NFV 436-WBT Remote Access VPNs Using PPTP and L2TP

NFV 436-WBT AT&T Vyatta 5600 vRouter Remote Access VPNs Using PPTP and L2TP

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.

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

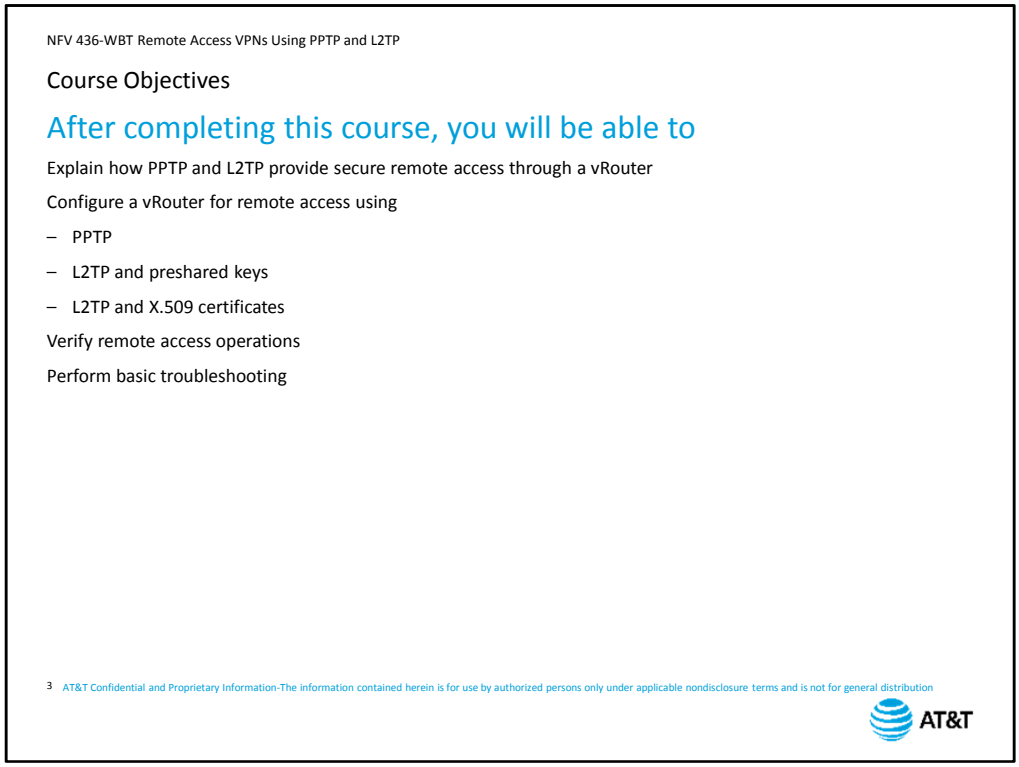
AT&T

1

Legal Disclaimer

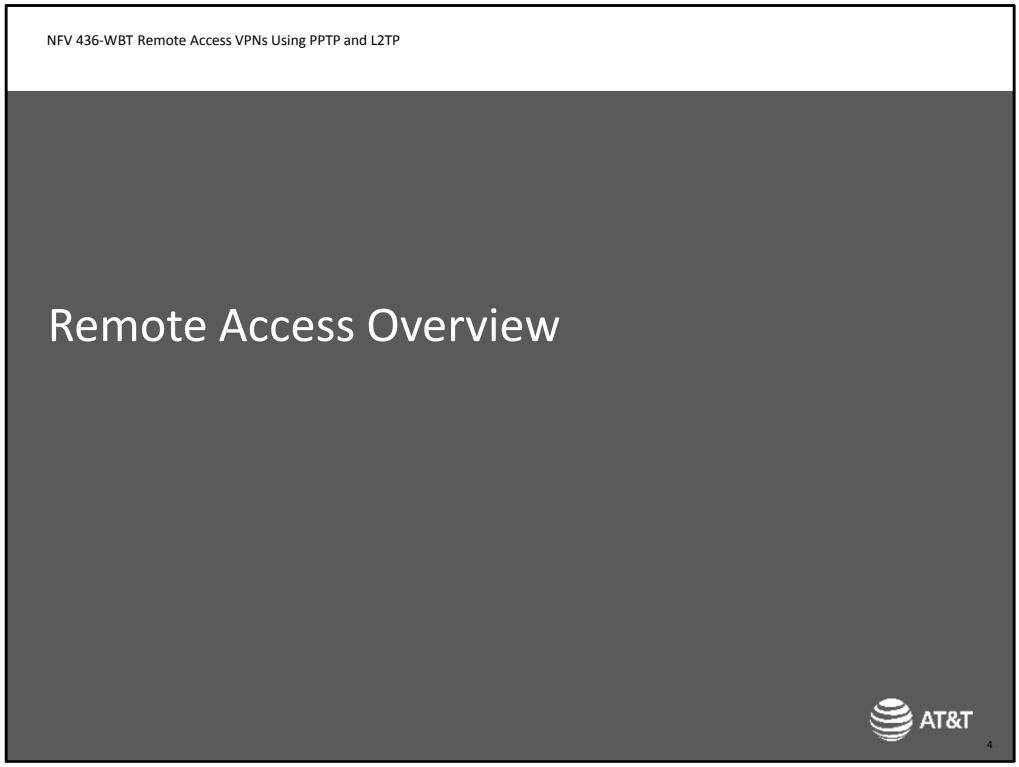
All or some of the products detailed in this presentation may still be under development and certain specifications may be subject to change. Nothing in this presentation shall be deemed to create a warranty of any kind.

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

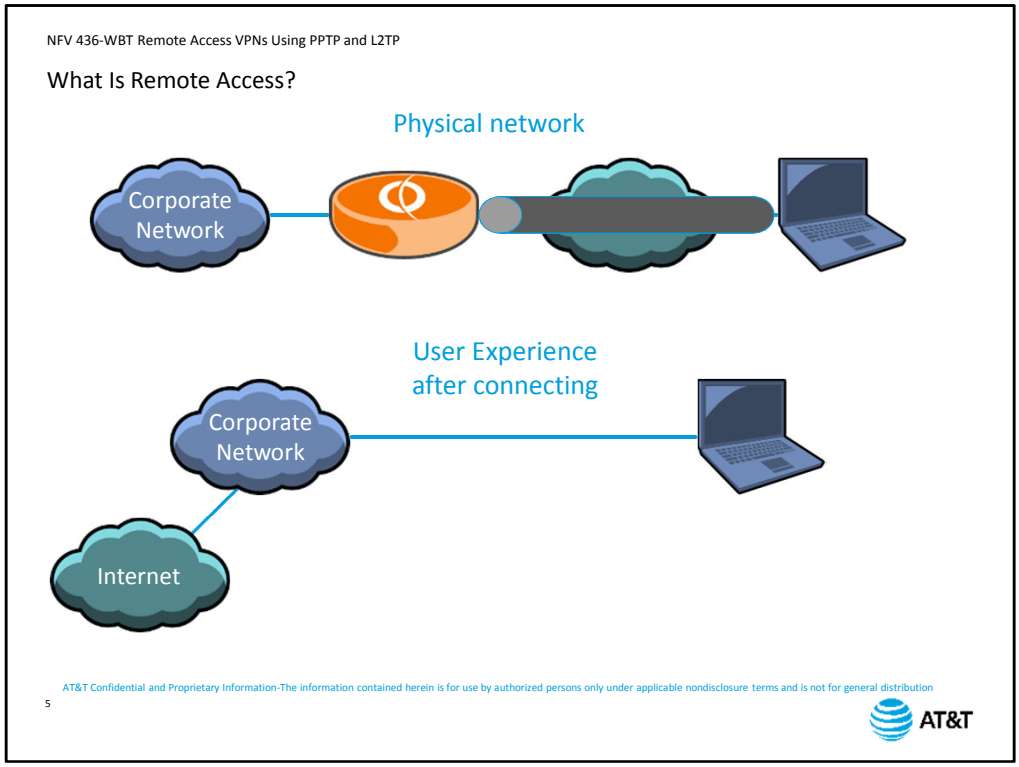


Welcome to the AT&T vRouter Remote Access using PPTP and L2TP.
After completing this course, you will be able to:

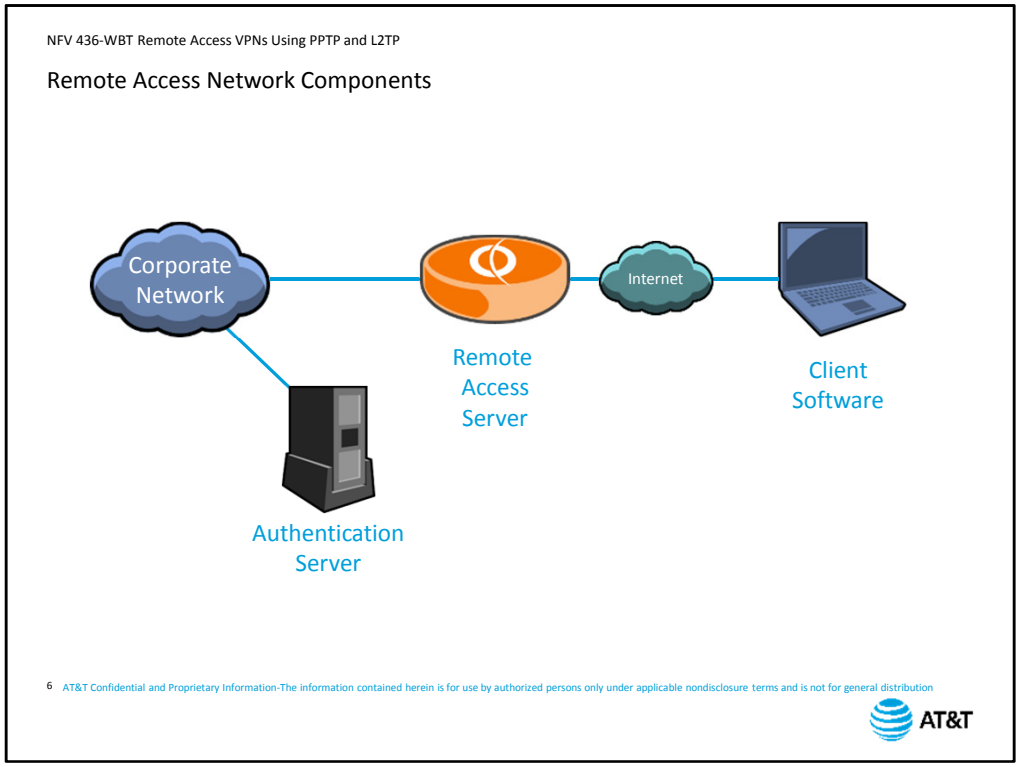
- Explain how PPTP and L2TP provide secure remote access through a vRouter
- Configure the vRouter for remote access using PPTP, L2TP and preshared keys, and L2TP and X.509 certificates
- Verify remote access operations
- Perform basic troubleshooting



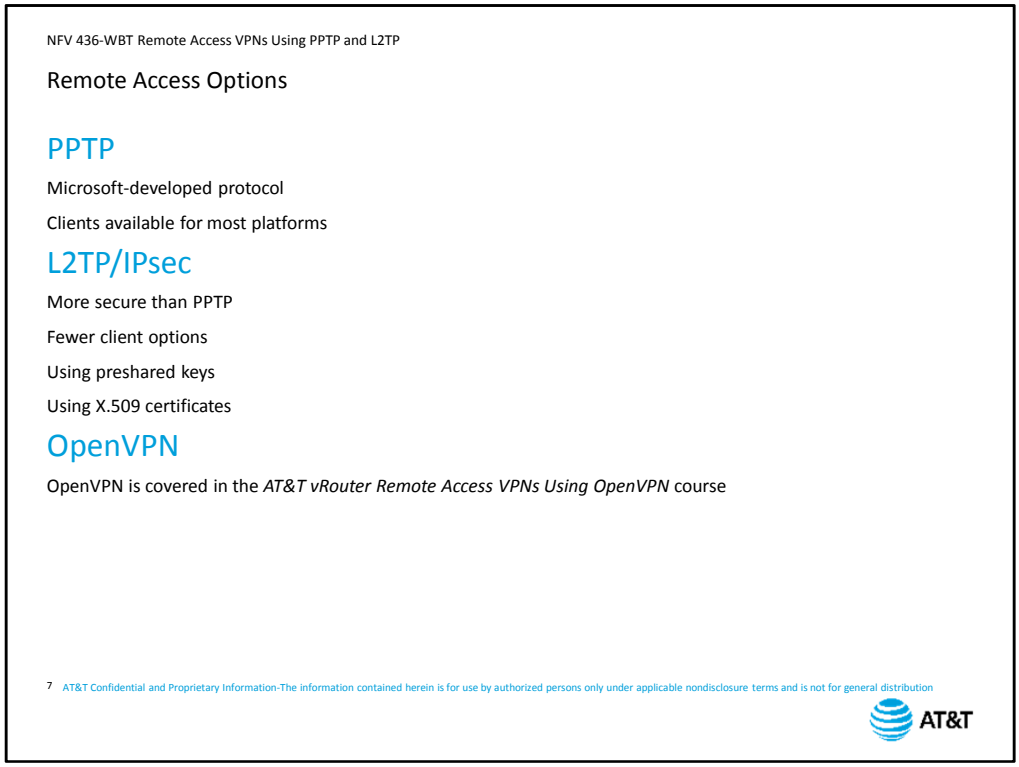
We begin with an overview of remote access technologies, focusing on PPTP and L2TP.



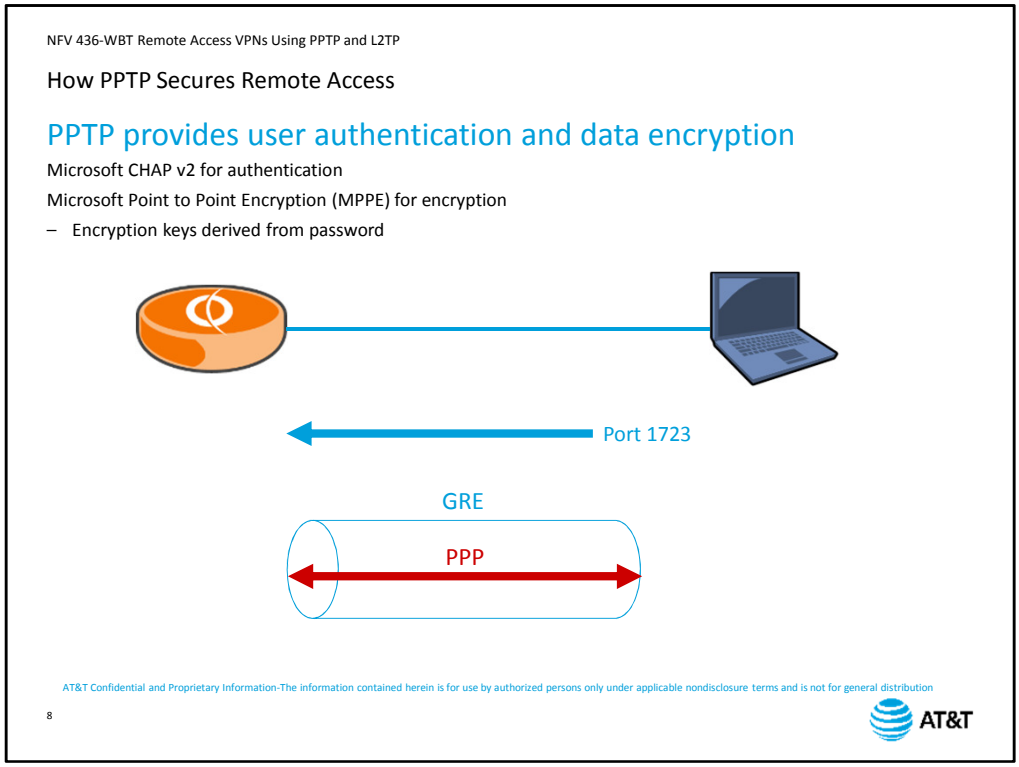
vRouter implementation of remote access allows individual users to establish a secure connection to a private network using the Internet. Users first connect to the Internet using any service provider,
Then establish a secured, encrypted connection to the vRouter. The vRouter then provides access to services located inside the private network.
Once the connection is established, the remote user appears to be directly connected to the corporate network. All traffic from the remote computer travels to the private network before being routed to its destination,
including traffic destined for resources outside the private network.



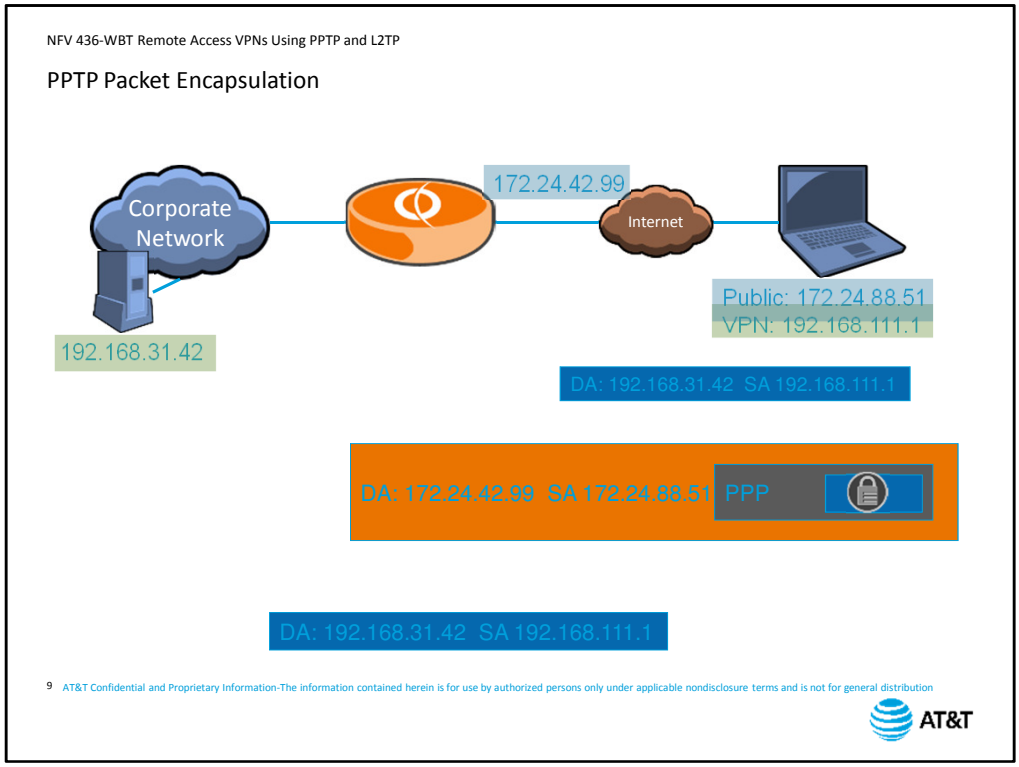
A remote access solution consists of several components.
The end user workstation needs to run client software to initiate the connection, authenticate the end user, and encrypt the data exchanges.
The remote access server is the terminus for the secured connection, providing user authentication and data encryption services. The vRouter is a remote access server.
A third component is the authentication server, which stores the individual username and password records.
This list of users can be configured on the vRouter itself if there are relatively few remote users.
More often, an administrator will maintain a separate user database on a RADIUS server.
RADIUS scales better for a large number of users.



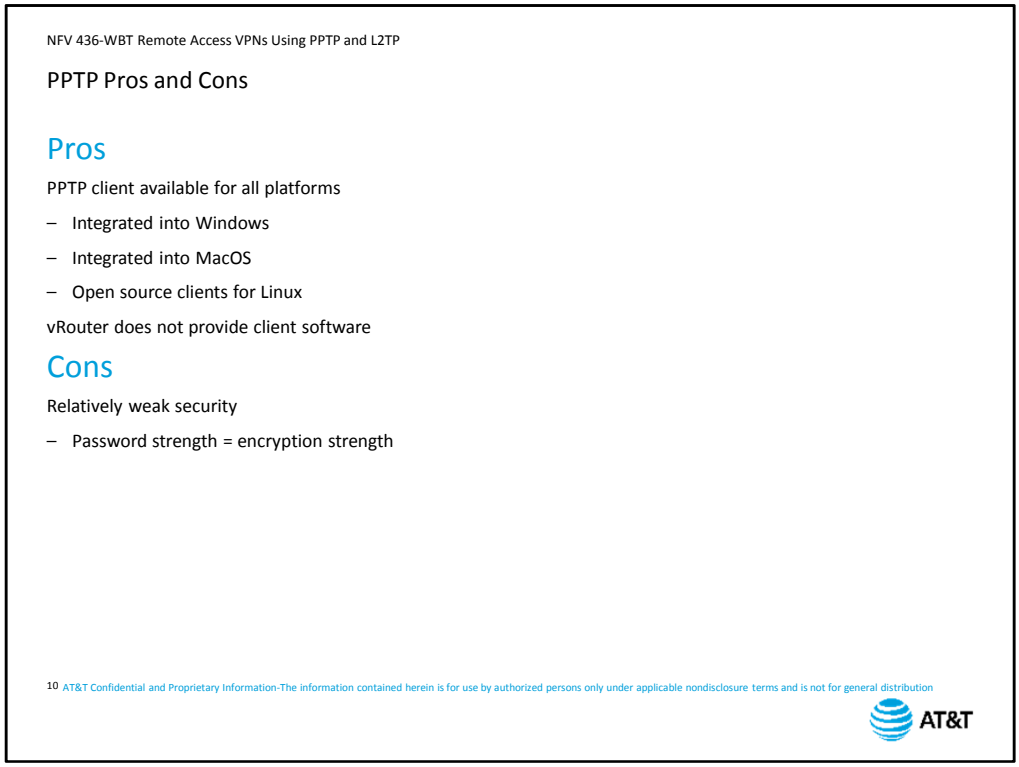
vRouter offers three options for remote access.
The first is PPTP, a remote access protocol developed by Microsoft and integrated into its Windows operating system. Although initially a Windows-only product, PPTP client software is now available for most end user platforms, including Mac and Linux.
The second remote access option is L2TP over IPsec. This option overcomes some of the security weaknesses of PPTP, but is not as widely supported on different operating systems. L2TP has two configuration options. You can secure the link using a preshared key, or you can use X.509 certificates. Each approach has its advantages and drawbacks, which we will discuss in detail later in this course.
The third remote access option is OpenVPN. We discuss this implementation in detail in the *AT&T vRouter Remote Access Using OpenVPN* course.



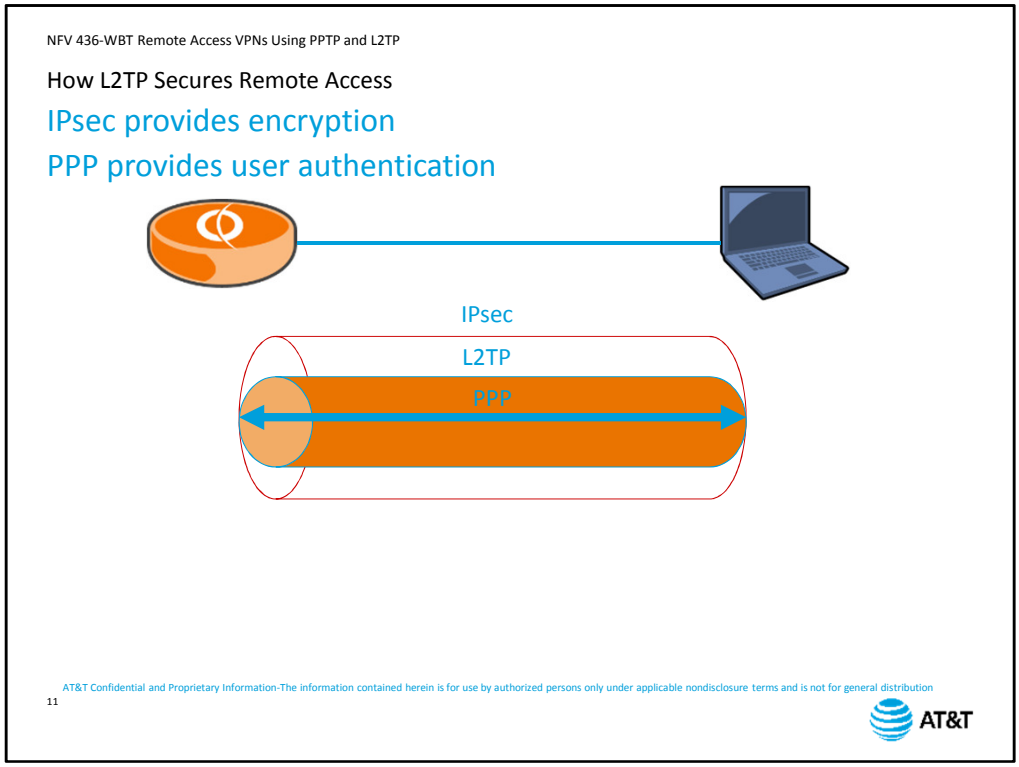
Let's look at the elements of a PPTP connection.
To establish a PPTP connection, the client software initiates a connection to the remote access server on port 1723.
The server then initiates a GRE tunnel between the two devices to encapsulate communications between the client and the server.
The client then initiates a PPP connection to the server. During this exchange, the client receives its private address for VPN use. When using PPTP,
PPP is the mechanism both for user authentication and data encryption.
For user authentication, PPTP uses Microsoft CHAP version 2, and for encryption, PPTP uses Microsoft's Point to Point Encryption algorithm.
The actual encryption keys are derived from the PPP password.



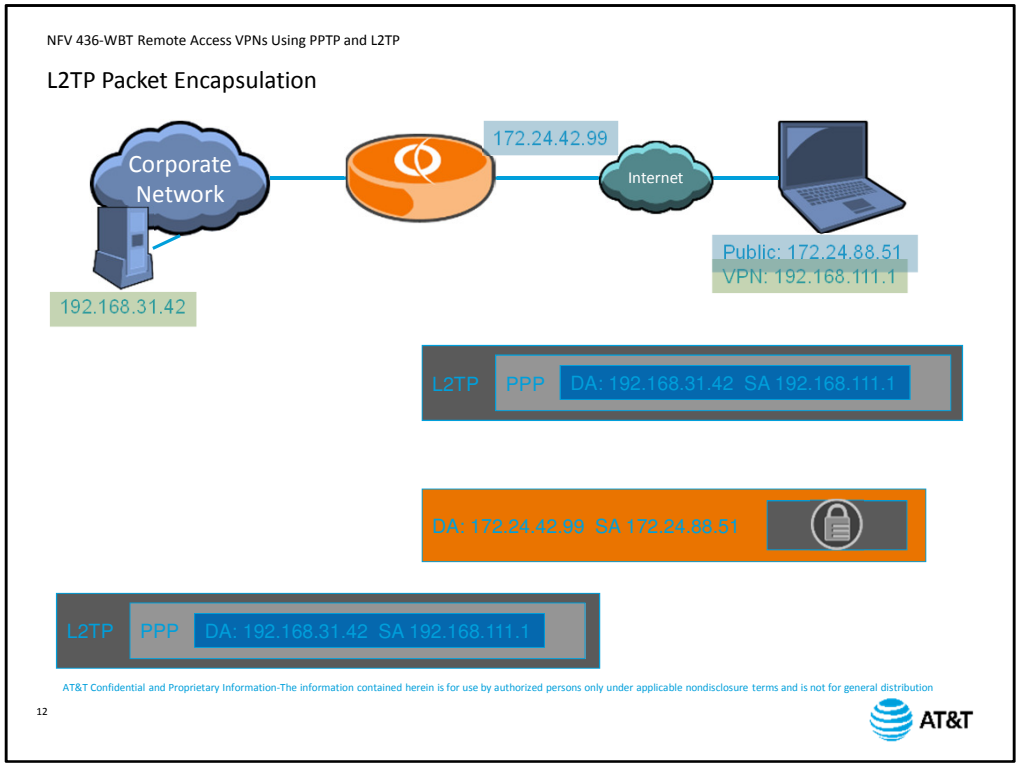
Let's look at the packets now that we have a secure connection.
The end station wants to send data to a server inside the corporate network.
The destination address of the packet is the address of the server.
The source address is the VPN address assigned to the client during the PPP exchange.
This packet is then encrypted
and encased in a PPP frame.
The PPP frame is then encapsulated in a GRE packet.
The destination address for the GRE packet is the address of the vRouter remote access server,
and the source address is the public IP address of the client workstation.
When the vRouter receives the packet, it first removes the GRE encapsulation,
then the PPP encapsulation,
then it decrypts the original packet,
and routes it to its destination.



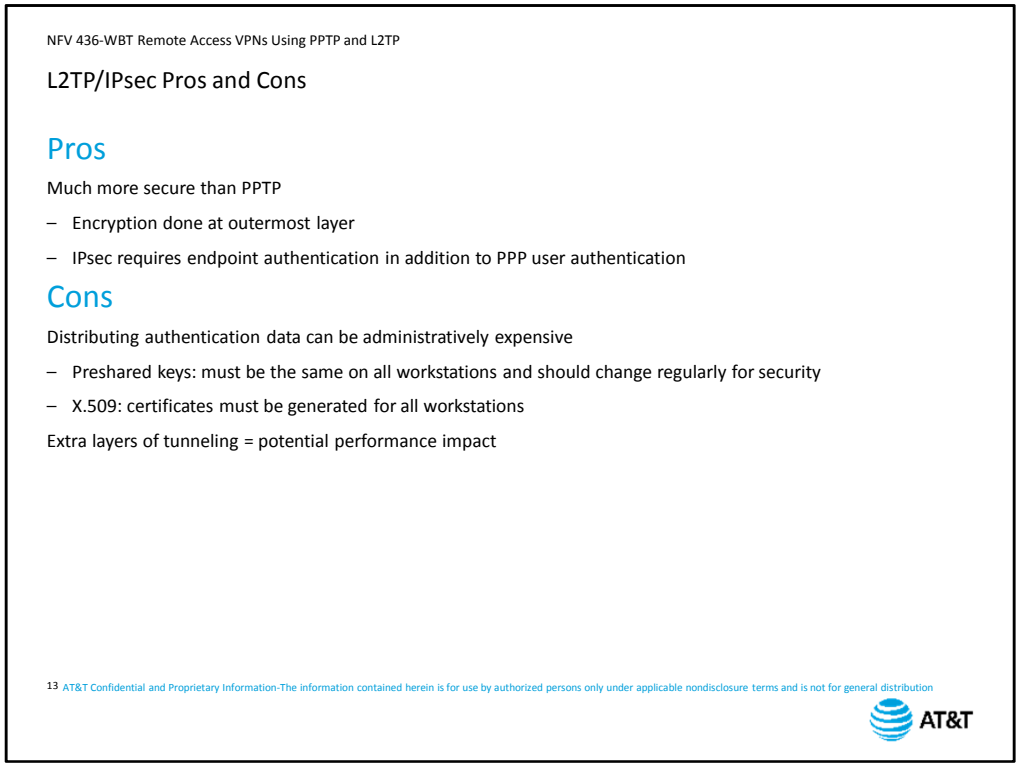
If you are considering using PPTP, you need to be aware of the following advantages and disadvantages.
The biggest advantage of using PPTP is that client software is available for all common end user operating systems.
Being a Microsoft-developed protocol, PPTP is fully integrated into Windows software.
Apple has fully integrated PPTP into its operating system, and there are several open-source options for Linux clients.
Note that, while vRouter supports standards-based PPTP clients, vRouter does not provide any client software.
The biggest disadvantage of PPTP is its relatively weak security. Because the encryption keys are derived directly from the user passwords, and because the encryption algorithms are relatively simple, PPTP is considered to be an easily-cracked protocol.



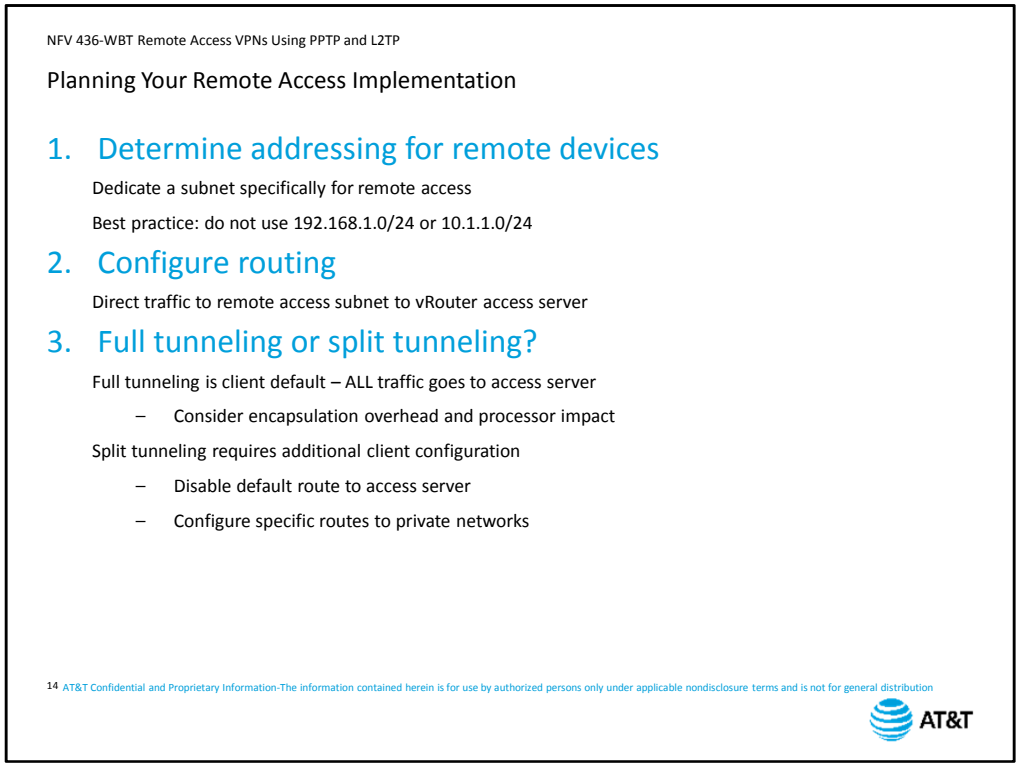
Now let's look at the elements of a vRouter L2TP remote access connection.
First, the client initiates an IPsec tunnel to the server. This establishes a secured, encrypted connection between the two endpoints.
Next, the client initiates an L2TP tunnel. Once this tunnel is established,
the client begins PPP authentication.
Unlike PPTP, using L2TP secures communications from the outset, using IPsec to encrypt all subsequent tunnel negotiations as well as the data exchange once the connection is established.
PPTP provides the user authentication piece of the connection.



Let's look at L2TP packet encapsulation.
Once again, the end station wants to send data to a server inside the corporate network.
The destination address is the address of the server,
and the source address is the assigned private address of the client.
The original packet is encapsulated in a PPP packet,
then in an L2TP packet.
the entire L2TP packet is encrypted,
Then placed inside an IPsec frame.
The destination address for the IPsec packet is the address of the vRouter remote access server,
and the source address is the public IP address of the client workstation.
When the vRouter receives the packet, it removes the IPsec encapsulation,
decrypts the L2TP frame,
then removes the L2TP encapsulation,
then the PPP encapsulation. Now that it has the original frame,
it can route it to its destination.



Like PPTP, L2TP has its own set of advantages and disadvantages.
The biggest advantage of using the vRouter L2TP implementation is security.
With IPsec securing the outermost layer of encapsulation, breaking into an L2TP/IPsec connection is much more difficult
Also, as part of the IPsec negotiation, the tunnel endpoints authenticate each other at the beginning of the connection process. This authentication occurs well before PPP user authentication, protecting username and password data from being intercepted by a bogus server.
One disadvantage has to do with distributing the authentication information necessary for IPsec.
If you are using preshared keys, all workstations must have the same key. Keys should be changed routinely to maintain security, which means distributing and installing new key information to remote workstations.
The alternative is to use X.509 certificates, but this requires the use of a Certificate Authority (CA), and the generation and distribution of unique certificates for each end station.
Finally, as the previous screen illustrated, L2TP over IPsec has several layers of encapsulation. Multiply the processing required to encapsulate and decapsulate packets by the number of remote connections and the amount of traffic generated over each link, and you potentially bog down the performance of your access server.


NFV 436-WBT Remote Access VPNs Using PPTP and L2TP

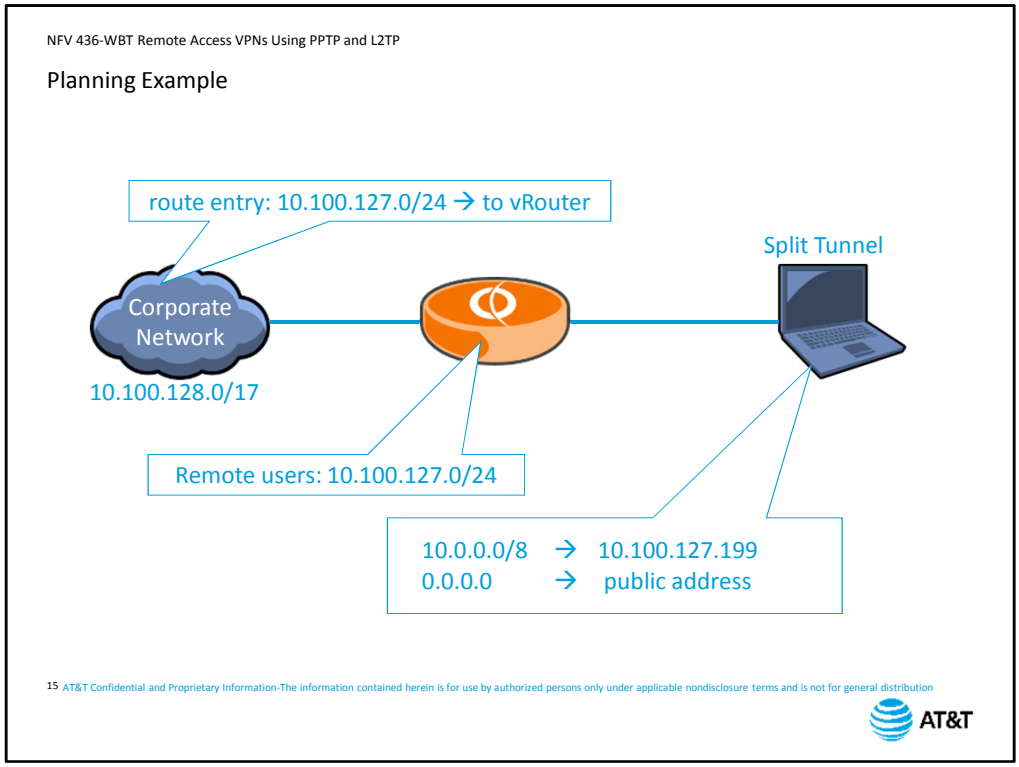
Planning Your Remote Access Implementation

1. Determine addressing for remote devices
   - Dedicate a subnet specifically for remote access
   - Best practice: do not use 192.168.1.0/24 or 10.1.1.0/24
2. Configure routing
   - Direct traffic to remote access subnet to vRouter access server
3. Full tunneling or split tunneling?
   - Full tunneling is client default – ALL traffic goes to access server
     - Consider encapsulation overhead and processor impact
   - Split tunneling requires additional client configuration
     - Disable default route to access server
     - Configure specific routes to private networks

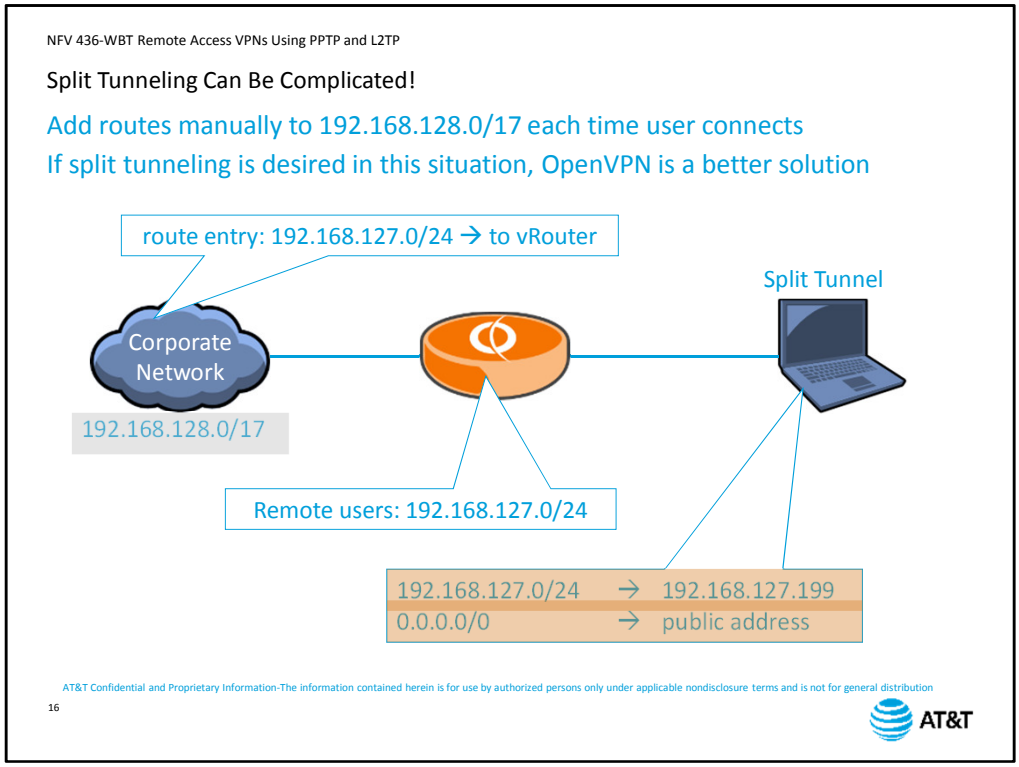
14 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

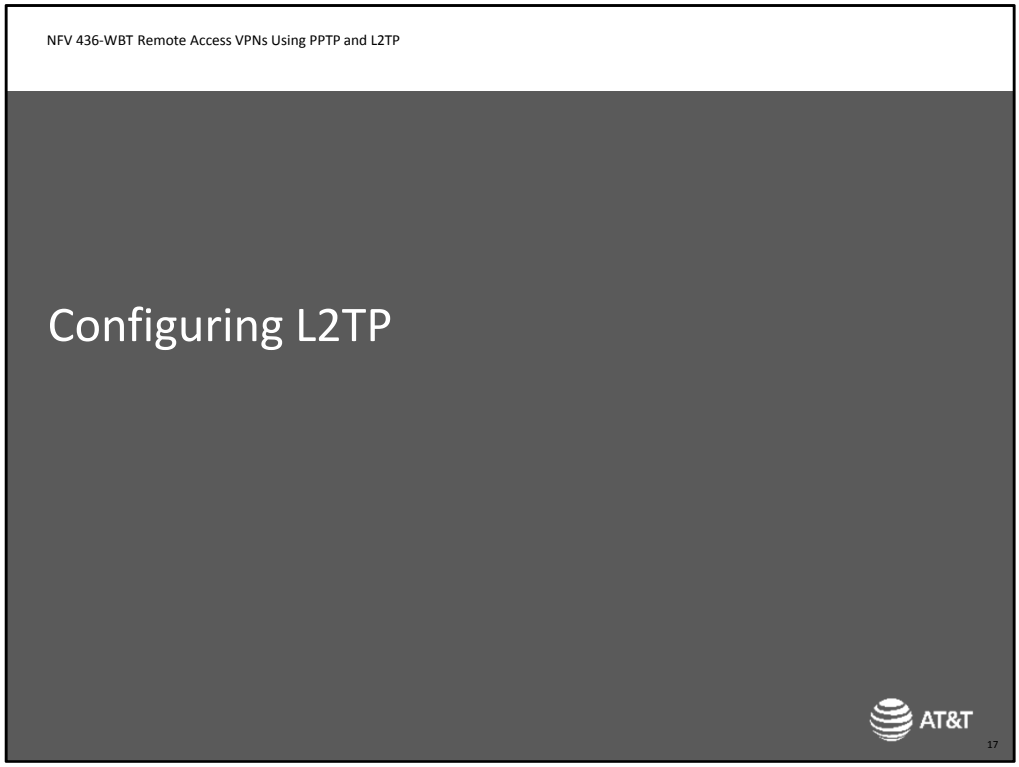
Regardless of which option you select, you need to do some planning and design before you begin configuring your vRouter.
First, you need to determine the range of addresses you will make available to remote users. This range of addresses should be a dedicated subnet of addresses and should not overlap with any subnets deployed within the private network.
In order to avoid conflicts with common default addressing schemes, you should also avoid using the subnets 192.168.1.0 or 10.1.1.0 for remote access devices.
Next, you need to configure routing within your network.
The subnet you dedicate for remote access is reachable via the vRouter. Upstream routers within the private network need to know to forward traffic for the remote access subnet to the vRouter. As this address range is not associated with a physical interface, you will need to configure static routing and route redistribution in order for upstream routers to learn about the remote access subnet.
Finally, you need to consider whether you want to use full tunneling or split tunneling.
With PPTP and L2TP, full tunneling is the client default. This means that once the end user's VPN is connected, ALL traffic from that device is sent over the VPN, even if its ultimate destination is not within the private network.
You need to consider the performance impact of handling all the encapsulation and encryption of traffic that ultimately turns around and heads back out to the Internet.

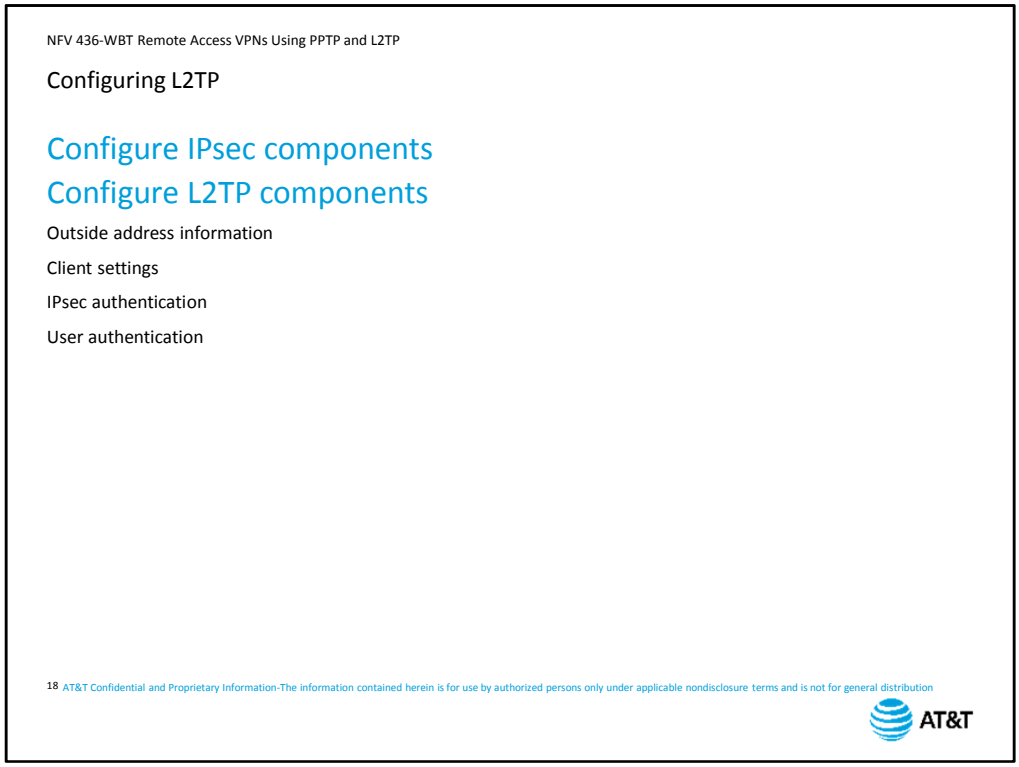


Let's look at one planning scenario.
We have decided to use subnet 10.100.127.0/24 for remote access users.
In order for devices within the corporate network to reach our remote users, we need to ensure that the routers know that hosts on subnet 10.100.127.0 are reachable through the vRouter.
When the client connects, it installs a default route sending all traffic to the VPN-assigned IP address.
If we choose to enable split tunneling,
the client will instead install a route to the classful private address boundary.
All other traffic will use the pre-existing default route to send traffic directly to the Internet.

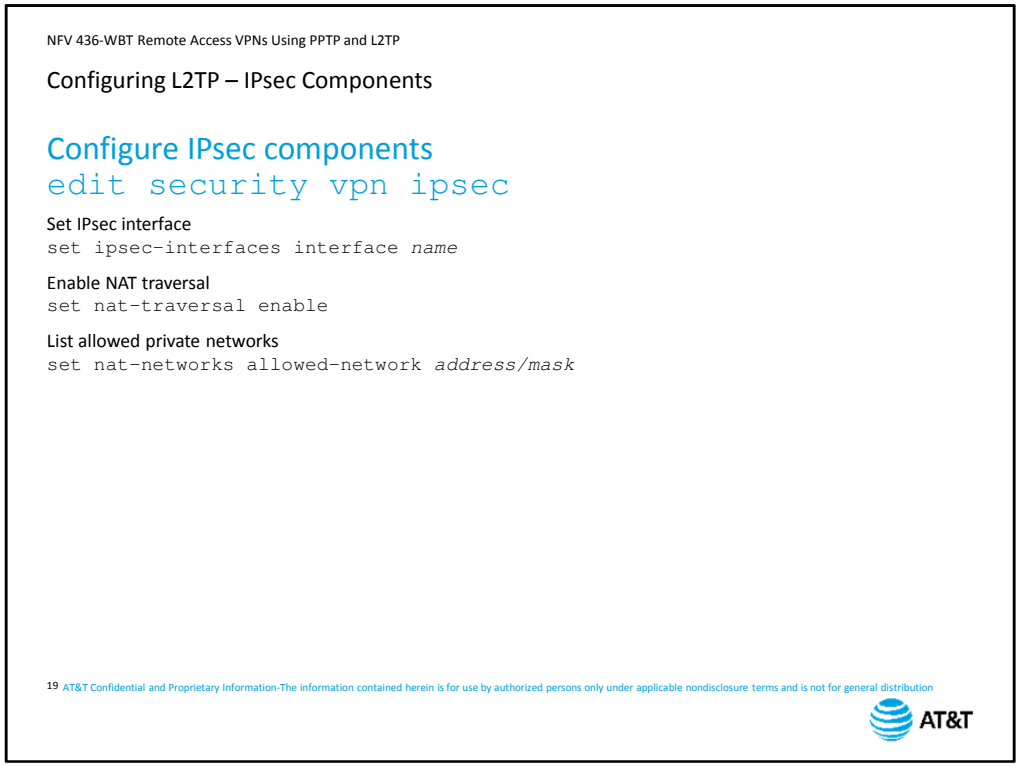


If we use the same planning scenario, but change the private addressing to use the 192.168 address space, split tunneling requires additional manual routing configuration.
The client will automatically install the classful route to the subnet that includes the assigned VPN address,
and direct all other traffic to the Internet.
This means that hosts inside the corporate network, which are on other networks in the 192.168 range, will not be reachable.
You need to add routes to the client manually, and will need to add these routes each time the user connects, since the client VPN IP address changes each time the connection is established.
Because this is difficult to implement, vRouter recommends using OpenVPN for remote access if you want to use split tunneling for networks using more complex addressing schemes.

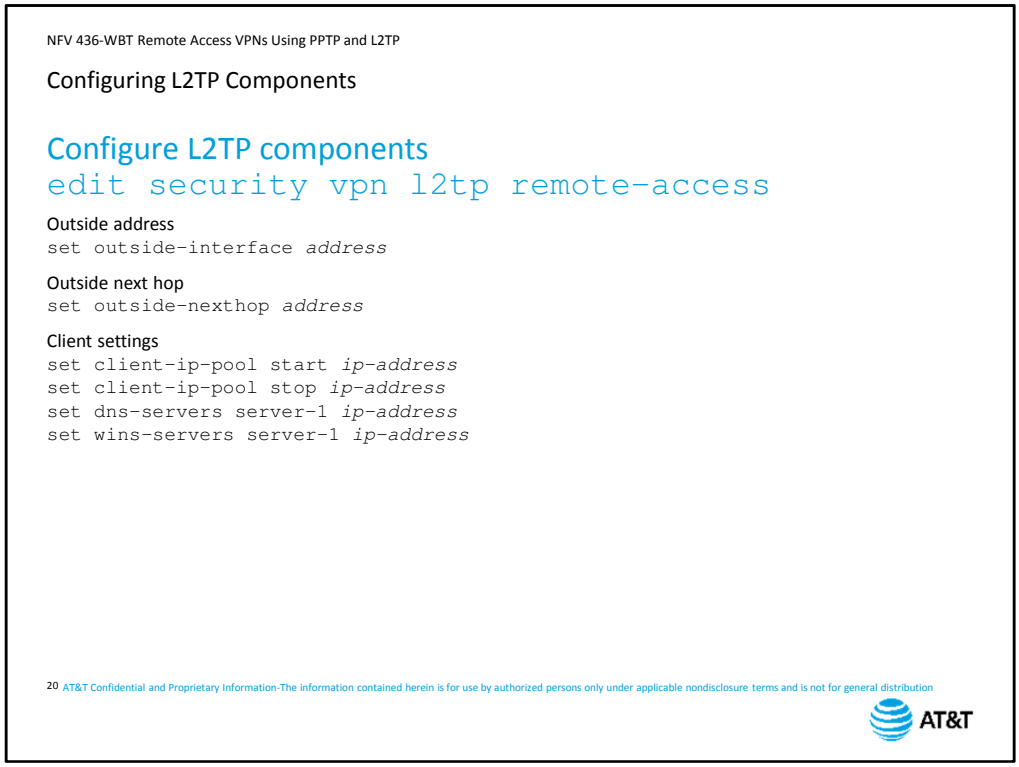




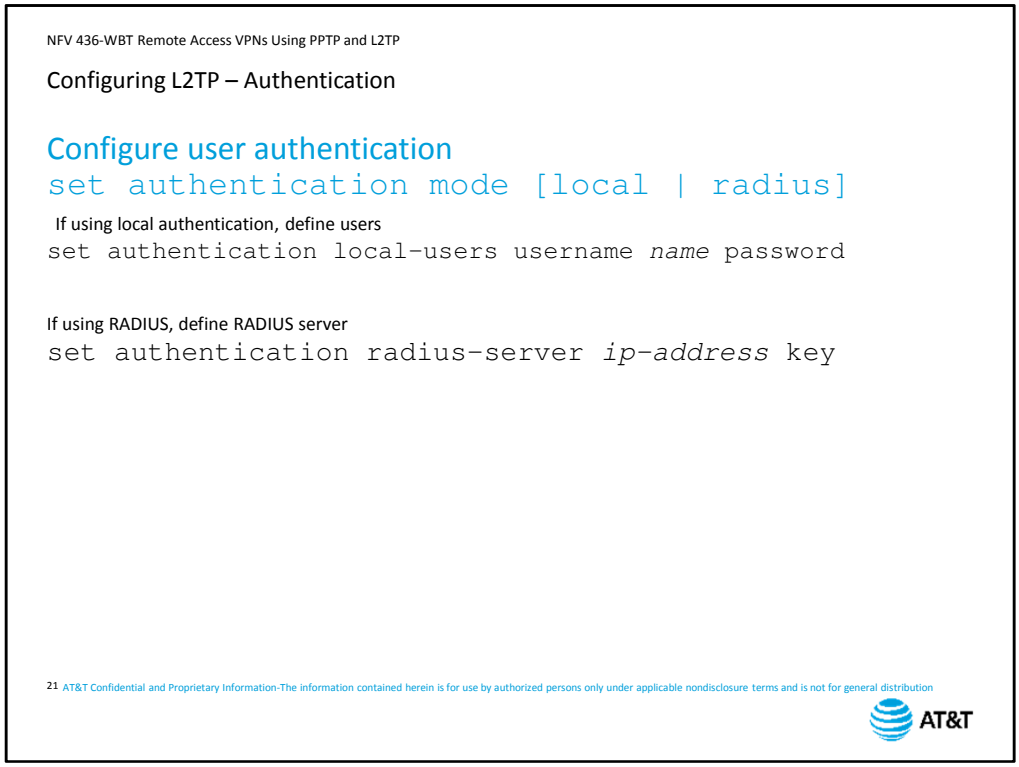
L2TP configuration has several components.
First you configure the components related to the IPsec tunnel.
Then you configure the L2TP settings, including the outside IP address information, client specific settings such as IP address and DNs server, IPsec tunnel authentication settings, and user authentication settings.



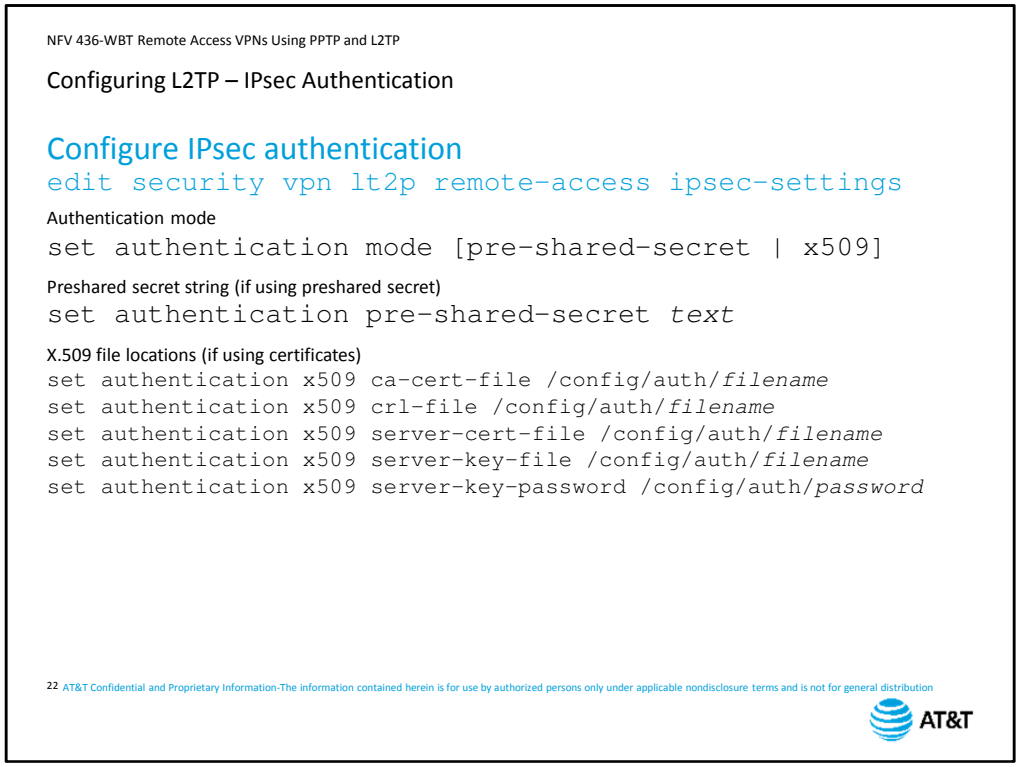
To edit the IPsec components, use the edit command to move into the IPsec part of the configuration hierarchy.
Set the interface that will receive incoming IPsec tunnel requests.
For L2TP, you need to enable NAT traversal in order to correctly support the encapsulated tunneled packets
You then need to list the private subnets used within the private network. You can use classful boundaries, or you can supernet networks as needed.



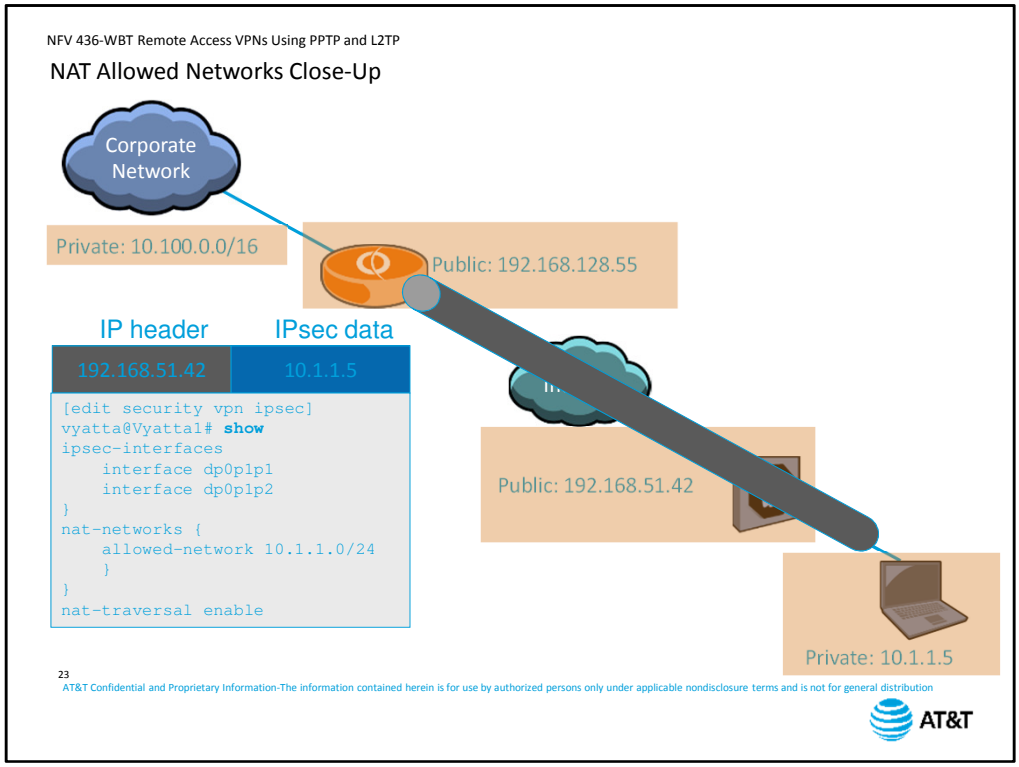
To set the L2TP components, use the `edit` command to move to the L2TP part of the configuration hierarchy.
First, set the IP address of the interface that will receive incoming L2TP connection requests. This is the address of the interface you configured as the IPsec interface previously.
Next, set the address of the next-hop address connected to the outside interface.
Next, set the client parameters. These commands are the same as we saw for PPTP.



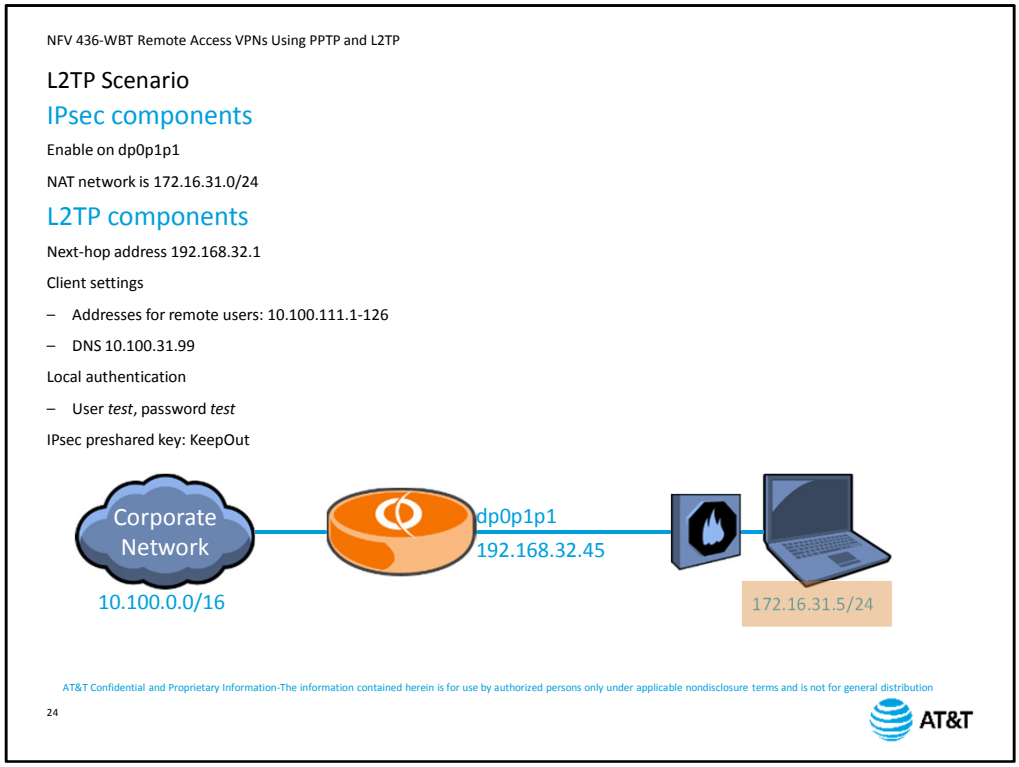
Next, set the authentication mode to use either the local username list or an external RADIUS server.
If you are using the local list, you then need to define all the users that will be connecting to your vRouter.
If you are using RADIUS, you need to tell the vRouter how to reach the RADIUS server, including the RADIUS server key.



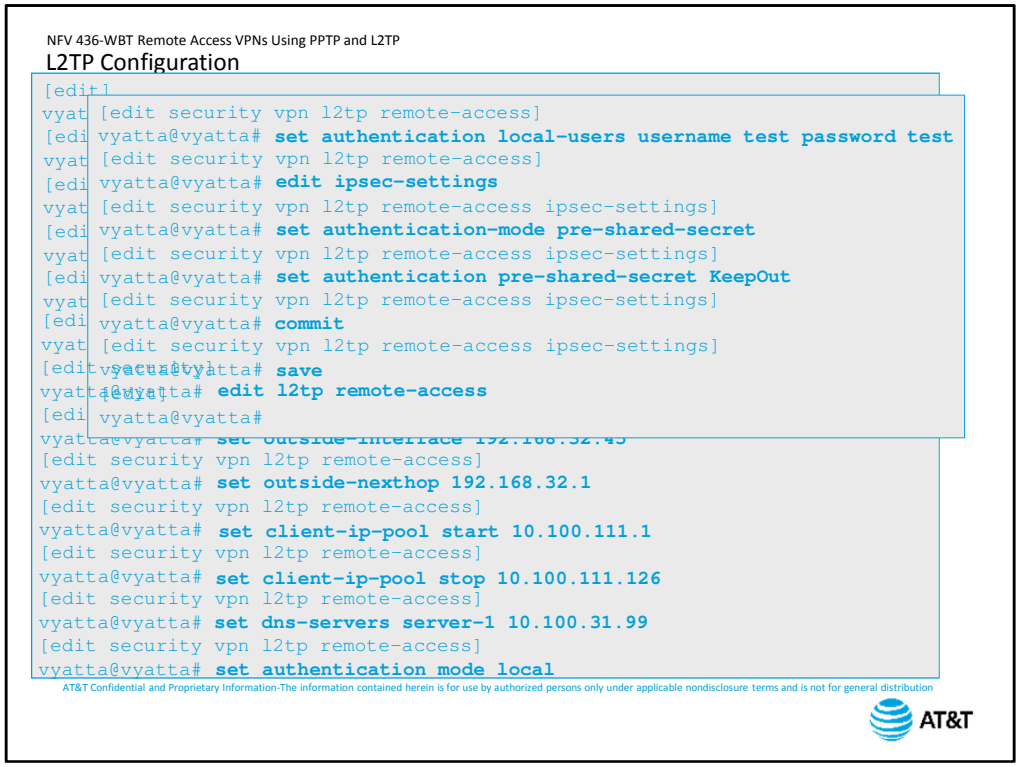
Next, set the authentication parameters for IPsec.
You can choose to use either a preshared key or x509 certificates.
If you use a preshared key, you need to set the key in the vRouter as well as on every remote client.
If you use x509 certificates, you need to specify the location of all the certificate files. You will get these files from your Certificate Authority and copy them to the vRouter into the */config/auth* directory.



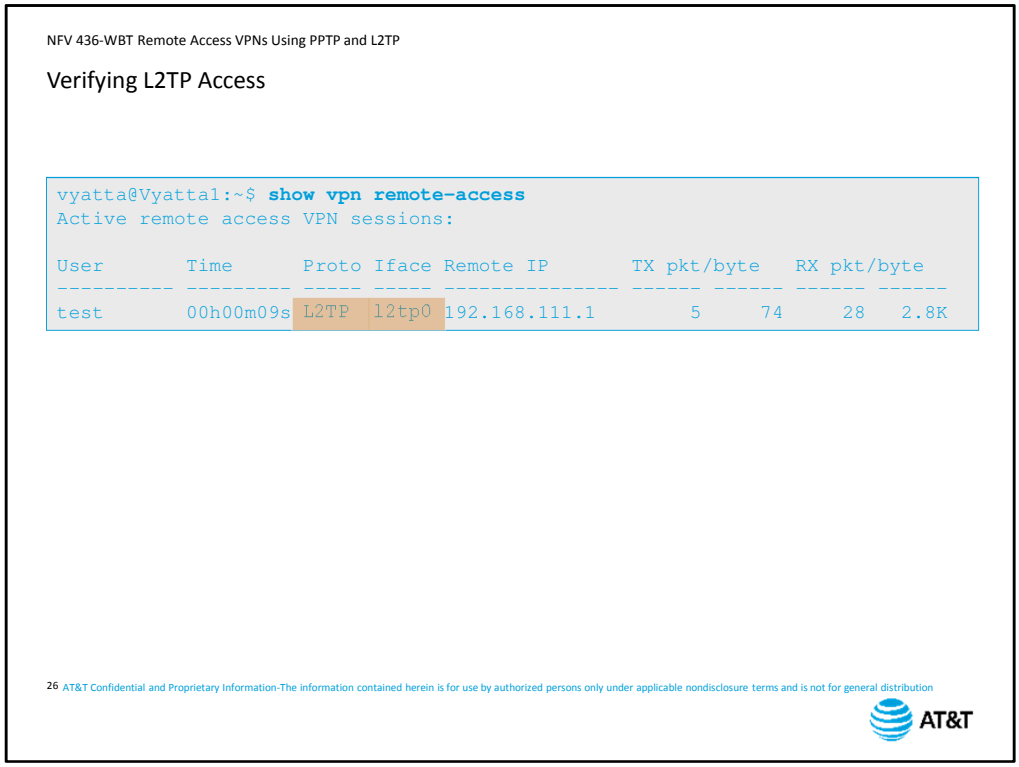
Before we begin our scenario, let's look more closely at the NAT allowed networks part of the IPsec configuration.
In this network, we have a range of private addresses in use in the corporate network.
The vRouter is providing NAT services, translating the private addressing into the public address assigned to the corporation.
The remote client also has a private IP address,
with a firewall providing NAT services, translating the private address to a public address.
All of this addressing and translation happens before we add L2TP to the network.
When we activate the IPsec tunnel, the NAT performed by the firewall causes a problem.
The IPsec internals will show packets originating from the client at 10.1.1.5, but the packet headers will show the public address of 192.168.51.42. This would normally cause IPsec to discard the packets as invalid.
In order to support the in-line NAT, we have to enable NAT traversal and explicitly allow the private network assigned to the client



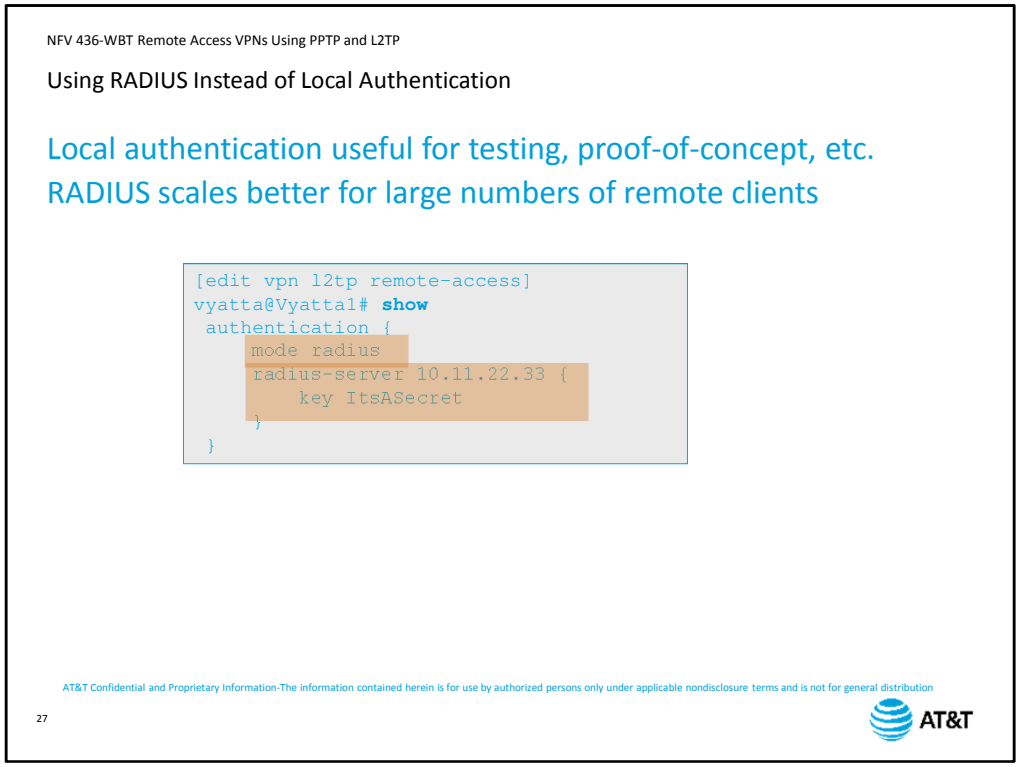
Let's apply these configuration commands to a scenario.
For IPsec, we enable IPsec on dataplane interface 1.
We define the NAT network to be 172.16.31.0/24. This includes the entire subnet of private addressing used inside the client home network.
For L2TP purposes the outside interface address is the address of interface 1.
The next-hop address – which is not shown in the diagram – is 192.168.32.1. This is the address of the upstream router inside the Internet.
The client settings include the address range for the end users and the DNS server address.
We are using local authentication so we will set up a user named *test* with the password of *test*.
The IPsec preshared key is *KeepOut.*



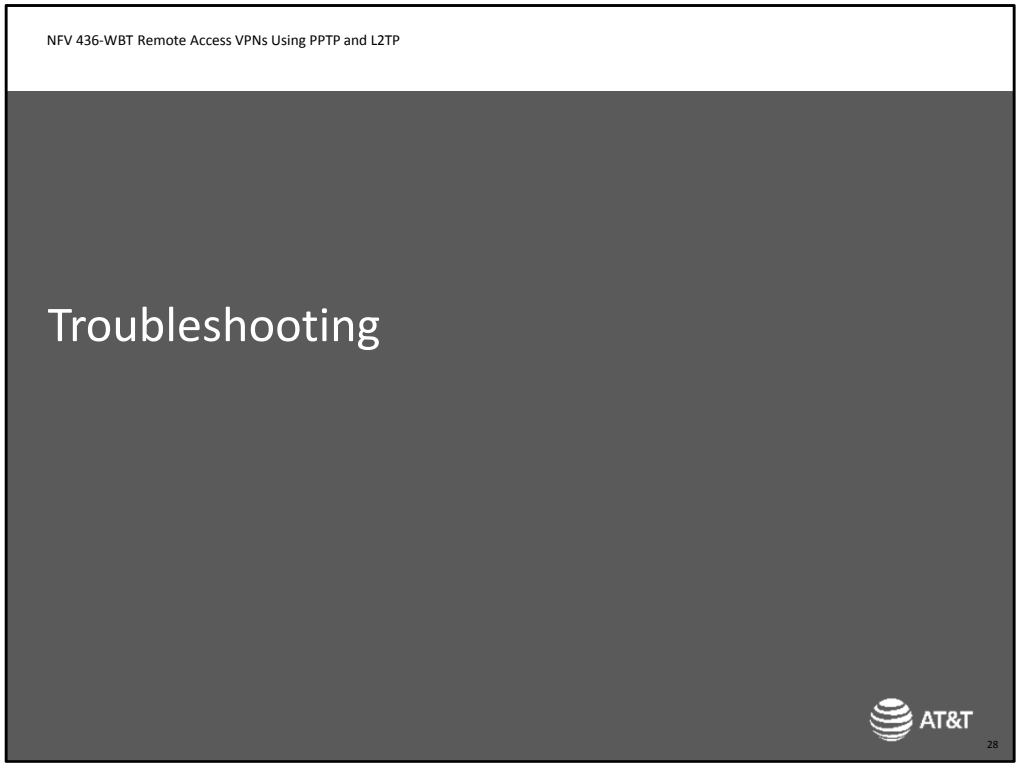
First, we edit the IPsec components.
Setting the IPsec interface,
enabling nat-traversal
and setting IPsec to accept the private addresses in use in our network.
We go up two levels, then edit the L2TP components.
We set the outside interface address
and the outside next-hop address.
Next we set the client parameters, defining the range of addresses for the clients,
and the DNS server address.
Next, we set the authentication to local mode,
Then create the local user.
Now we edit the IPsec settings for L2TP
setting the authentication mode to preshared secret
Then setting the preshared key.
Now we can commit and save our changes.



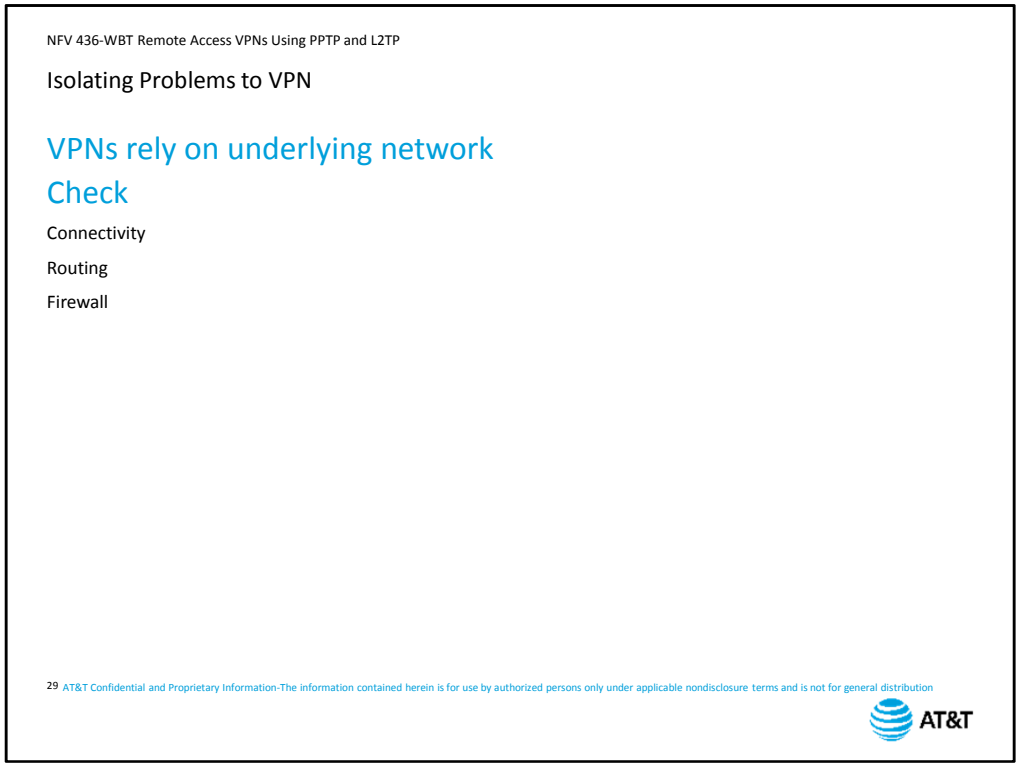
As with PPTP, the best way to verify your configuration is to make a connection and then use the `show vpn remote-access` command . Connected sessions will show up in the active sessions table.
Note that the protocol in this case is L2TP, not PPTP.
The interface name is *l2tp0*. As with PPTP, the vRouter will create an interface for each individual connection, then remove it when the connection is terminated.



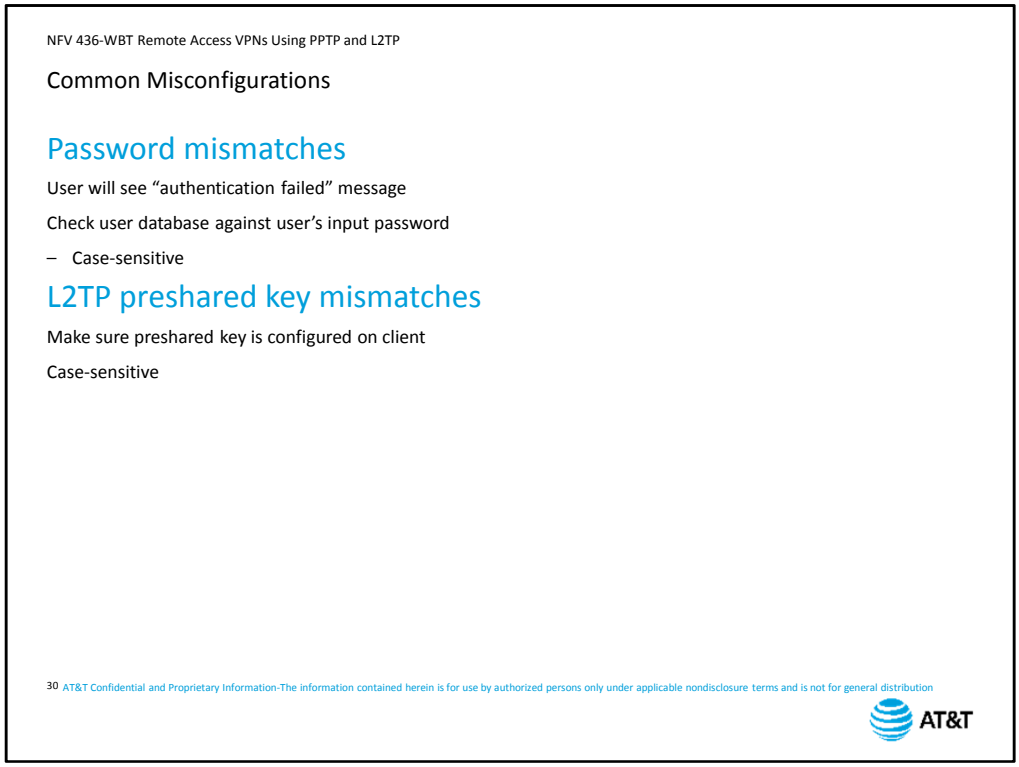
Both the PPTP and L2TP examples use local authentication. This is typical when you are first setting up your remote access network and want to quickly test connectivity without the complication of an external server.
In production environments, however, RADIUS is a better choice for handling large numbers of remote clients. You can get open-source RADIUS servers from several sources.
To implement RADIUS on the vRouter, set the authentication mode to `radius` instead of local,
then specify the address and key string for the RADIUS server. Although this example shows the configuration for L2TP, the command syntax is identical for PPTP.



Let’s take a moment to discuss troubleshooting remote access VPNs.



This may sound obvious, but when you are troubleshooting a VPN problem, you should first make sure it is really a VPN problem.
VPNs rely on connectivity provided by the underlying network. If, for example, the end user's Internet connection is experiencing performance problems, the VPN is going to experience the same performance problems.
You need to verify basic connectivity from the client to the Internet. Make sure the client has an active connection.
You need to verify routing and reachability from the client to the vRouter. Use ping and trace-route from the client to ensure that basic IP traffic can pass.
Next, you need to verify that there are no firewalls blocking VPN traffic.



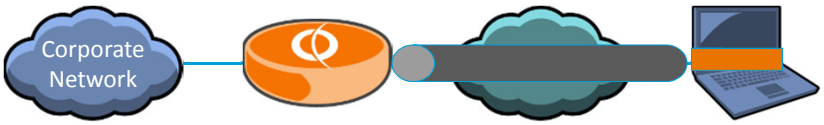
Password mismatches are the most common VPN misconfiguration.
The end user will see an authentication error. If the user continues to experience the error, you need to check the user’s input password against the password stored in the user database.
Remember that passwords are case-sensitive.
The IPsec preshared key is another opportunity for mismatching data.
To begin with, setting the preshared key is often buried in the client software, but it must be set in order for the IPsec tunnel to come up.
Again, the preshared key is case-sensitive.

NFV 436-WBT Remote Access VPNs Using PPTP and L2TP

Operational Issue – Problem 1

Problem: Some tunnel traffic gets dropped

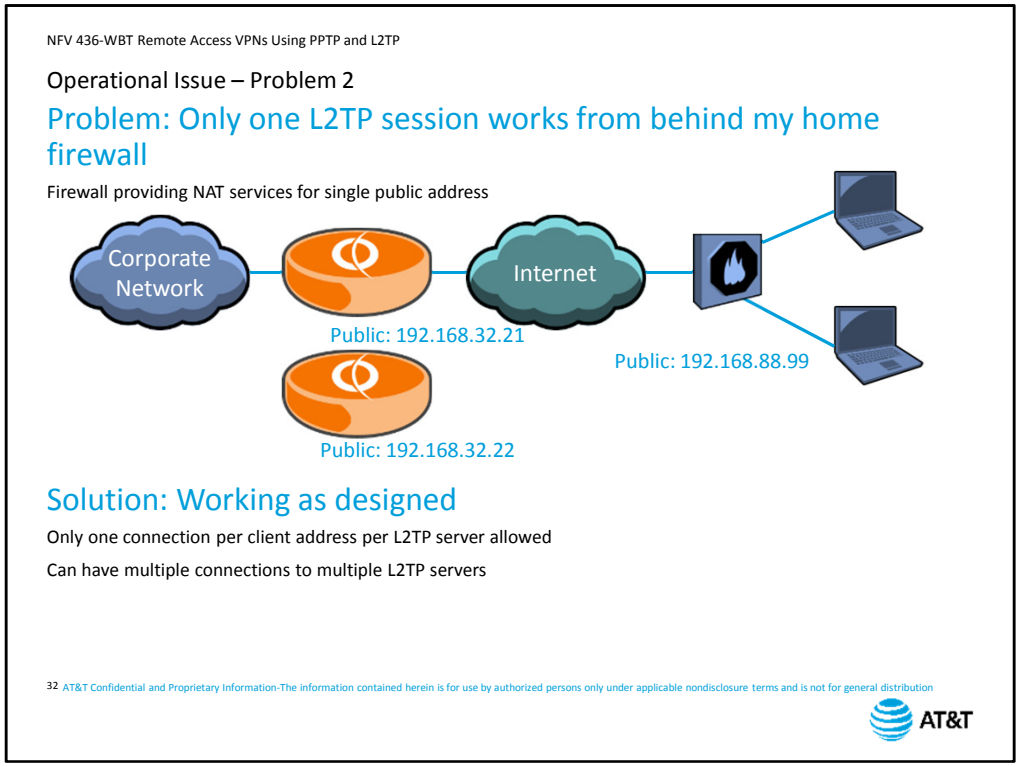
Small packets succeed; large packets fail



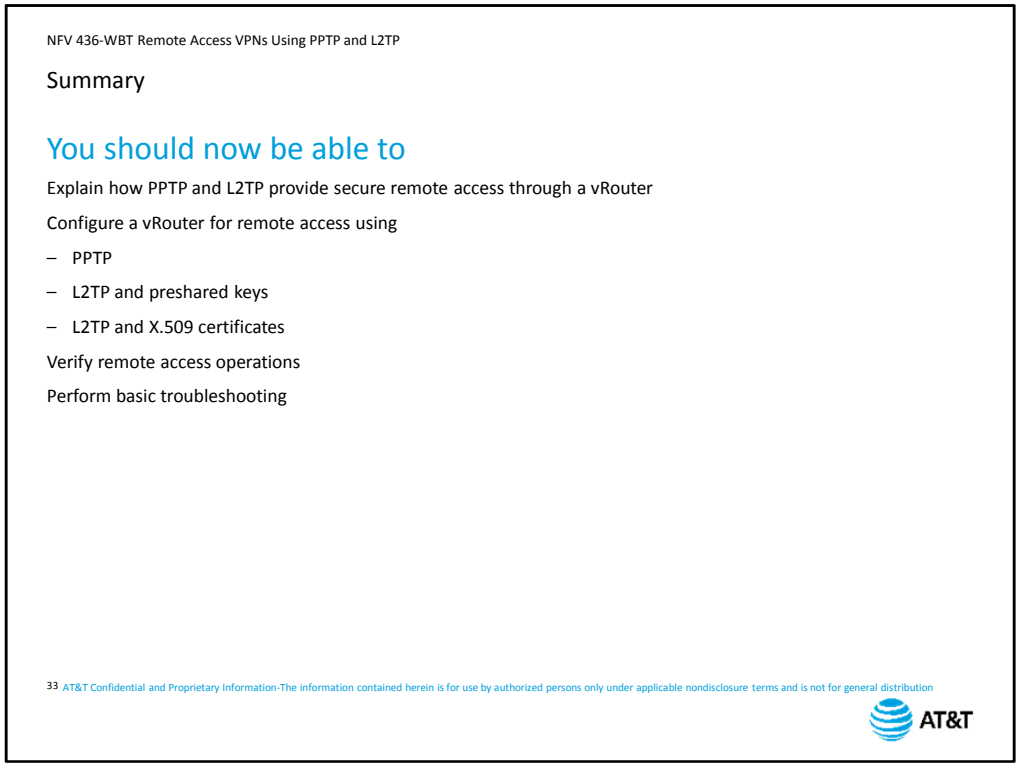
Solution: Lower MTU to <1400

`set interfaces dataplane dpxpypz mtu size`

Now let's look at some operational issues you may encounter, and discuss how to resolve them.
One problem often encountered by end users is that some tunnel traffic gets dropped. Specifically, smaller size packets traverse the VPN successfully, but larger packets cannot. The problem is due to packet fragmentation and subsequent dropping of fragments. You need to reconfigure both sides of the connection so that the maximum transmission unit (MTU) is under 1400 bytes. On the vRouter, you set this as part of the dataplane interface configuration.



Another known issue occurs.
When you try to connect multiple remote workstations behind a firewall to a single L2TP access server.
The firewall is providing NAT services, so that even though there are multiple workstations behind the firewall, they are all sharing a single public address.
This is working as designed.
L2TP can only support a single tunnel session from any given IP address. As far as L2TP is concerned, there is only one address at the home site - the public address.
If you need multiple simultaneous connections, you need to have multiple L2TP servers available. The first client will connect to the first server, the second client to the second server, and so on.



Congratulations! You have completed the AT&T vRouter Remote Access Using PPTP and L2TP course.

You should now be able to:

- Explain how PPTP and L2TP provide secure remote access through a vRouter
- Configure the vRouter for remote access using
  - PPTP
  - L2TP and preshared keys
  - L2TP and X.509 certificates
- Verify remote access operations
- Perform basic troubleshooting

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

End of Course – Remote Access VPNs Using PPTP and L2TP