AT&T

Remote Access IPsec VPN Configuration Guide, 17.2.0

November 2017

Supporting AT&T Vyatta Network Operating System

Contents

Copyright Statement

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.

About This Guide

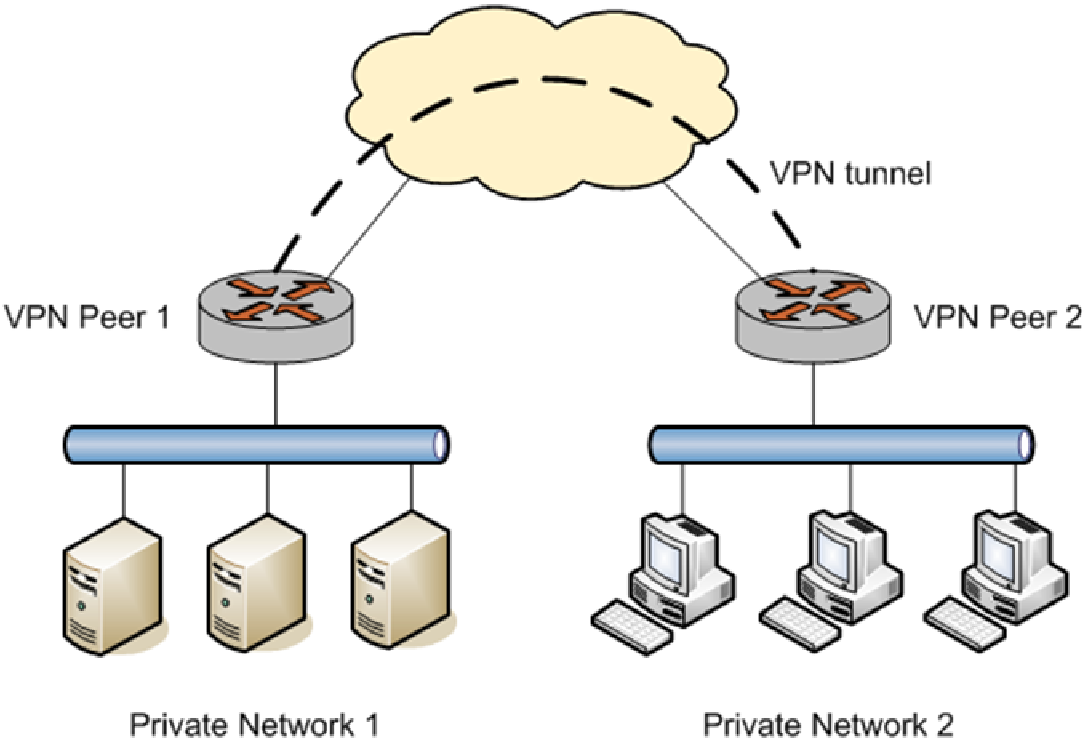
This guide describes how to configure Remote Access VPN on the AT&T Vyatta Network Operating System (referred to as a virtual router, vRouter, or router in the guide).

Remote Access VPN Overview

Remote access in the network

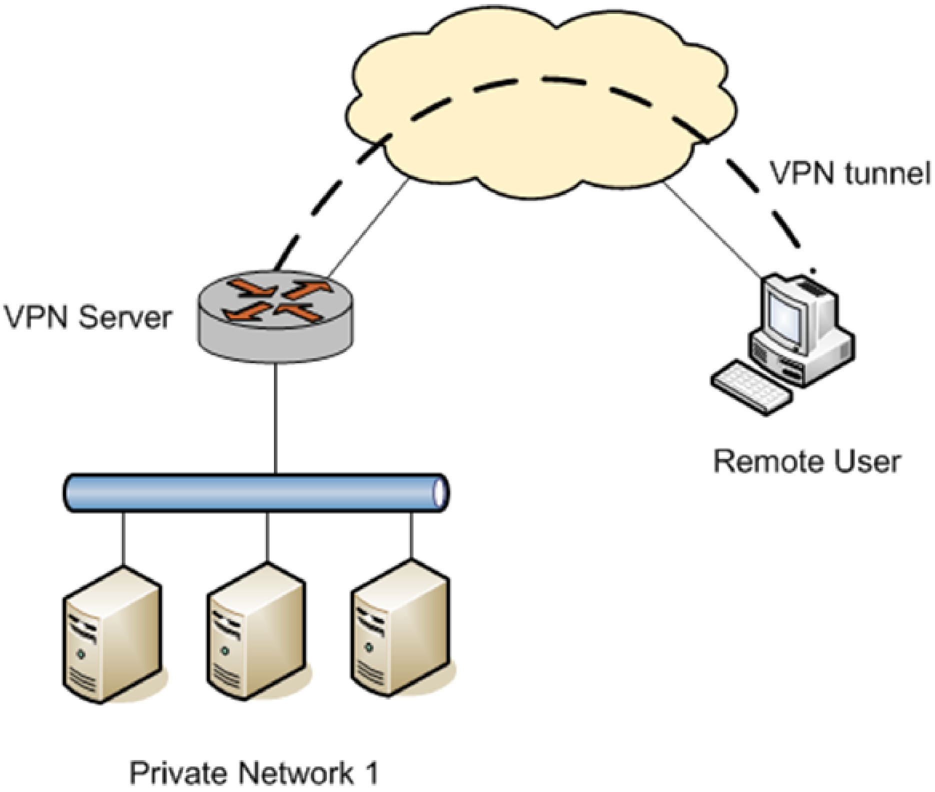
The AT&T Vyatta vRouter currently supports two main VPN mechanisms: site-to-site IPsec VPN, and Remote Access VPN (RA VPN). A site-to-site IPsec VPN connection allows two or more remote private networks to be "merged" into a single network as shown in the following figure.

Figure 1: Site-to-site IPsec VPN



With RA VPN, the AT&T Vyatta vRouter acts as a VPN server to a remote user with a client PC. A typical use for this capability is a traveling employee accessing the corporate network over the Internet. In this scenario, the remote employee's computer appears as another host on the corporate private subnet and is able to access all resources within that subnet. This scenario is shown in the following figure.

Figure 2: Remote access VPN



The AT&T Vyatta vRouter RA VPN implementation supports the built-in Windows VPN client: Layer 2 Tunneling Protocol (L2TP)/IPsec VPN.

The Windows L2TP/IPsec client supports two IPsec authentication mechanisms:

- Pre-shared key (PSK), where the two IPsec peers can use a PSK to authenticate each other based on the assumption that only the other peer knows the key.
- X.509 certificates, which are based on public key cryptography—specifically, digital signatures.

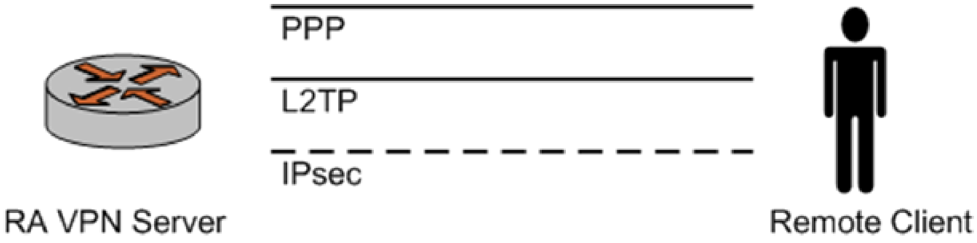
The AT&T Vyatta vRouter supports both pre-shared key and X.509 certificate authentication for L2TP/IPsec client; consequently, the AT&T Vyatta vRouter supports two different RA VPN deployments:

- L2TP/IPsec authenticated with pre-shared key
- L2TP/IPsec authenticated with X.509 certificates

RA VPN using L2TP/IPsec with pre-shared key

The following figure shows establishment of an L2TP/IPsec VPN session.

Figure 3: Remote access VPN-L2TP/IPsec with pre-shared key



1. The remote client first establishes an IPsec tunnel with the VPN server.
2. The L2TP client and server then establish an L2TP tunnel on top of the IPsec tunnel.
3. Finally, a PPP session is established on top of the L2TP tunnel, i.e., the PPP packets are encapsulated and sent/received inside the L2TP tunnel.

   Info:

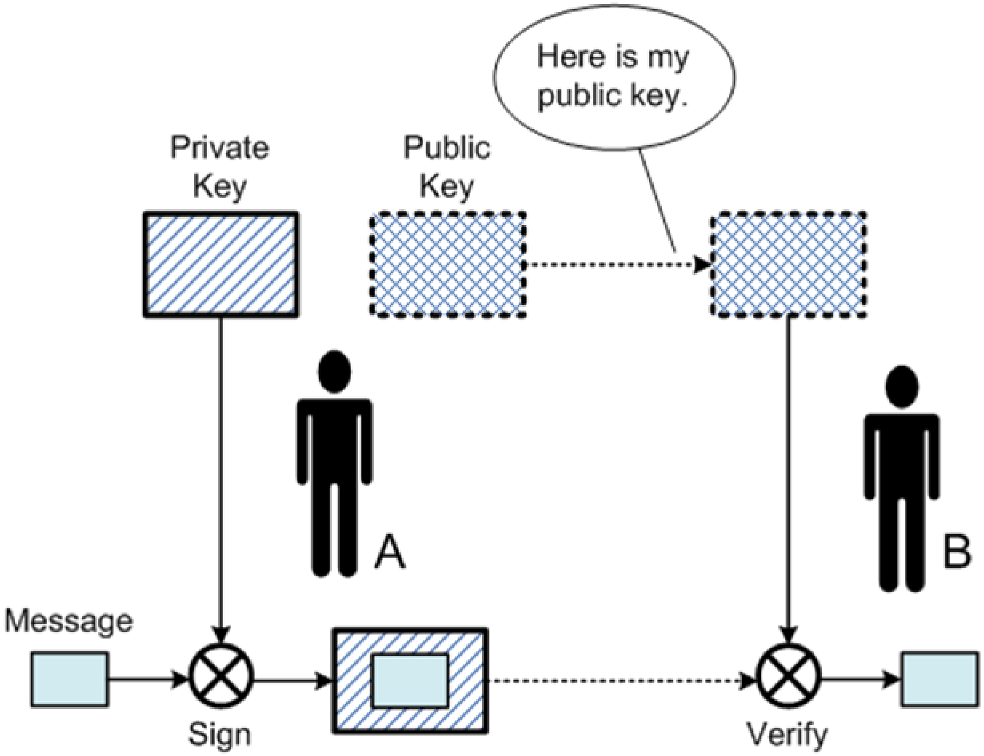
   With this solution, only user authentication is done at the PPP level (with username/password). Data encryption is provided by the IPsec tunnel. Furthermore, in order to perform encryption, IPsec also requires authentication (studies have shown that IPsec encryption-only mode is not secure) at the host level.

   When pre-shared key is used with L2TP/IPsec, all remote clients must be configured with the same PSK for IPsec authentication. This presents both a security challenge and an operations challenge, since when the key is changed, all remote clients must be re-configured. An alternative is to use L2TP/IPsec with X.509 certificates, as discussed in the next section.

RA VPN using L2TP/IPsec with X.509 certificates

The following figure shows a conceptual diagram of how digital signatures work.

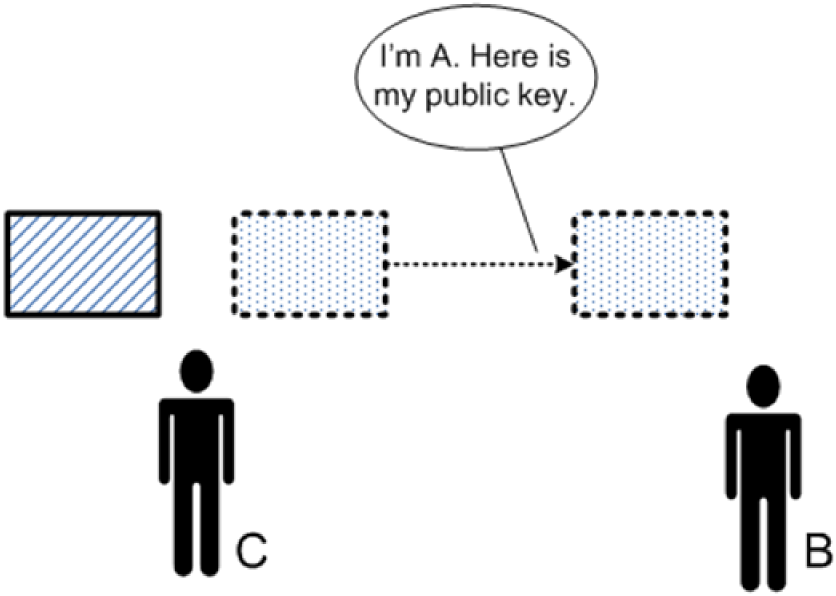
Figure 4: Digital signature



1. Peers A and B are communicating. A has a public key and a private key. A gives her public key to B.
2. A “signs” (encrypts) a message using her private key and sends the signed (encrypted) message to B.
3. B can “verify” the signature by decrypting it using A's public key and checking the result against the original message.
   Therefore, B can authenticate A by asking A to sign a message and then verifying the signature using A's public key. Since A's private key is only known to A, only A can create a signature that can be verified using A's public key.

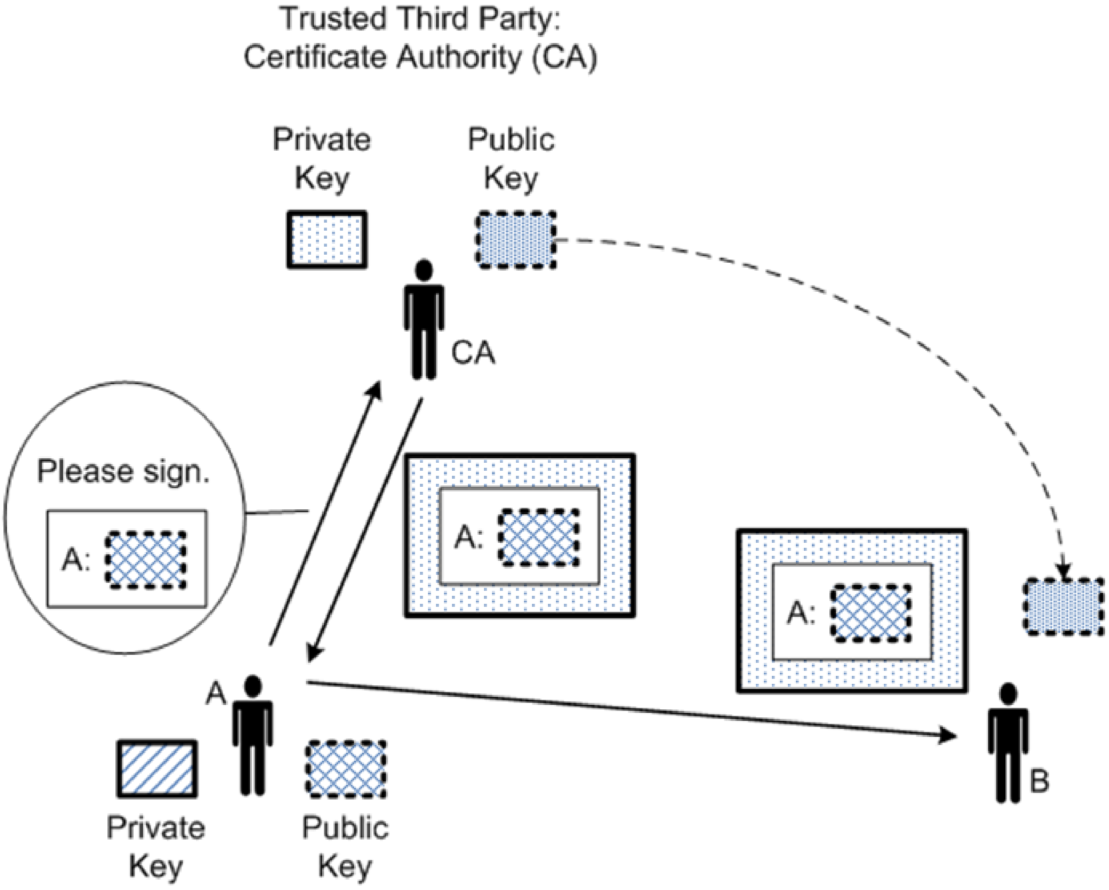
One problem with this authentication scheme is that B cannot know whether the public key he obtained is in fact A's public key. For example, in the following figure, a malicious attacker C pretends to be A and gives B a different public key.

Figure 5: Malicious attacker



In practice, this problem is solved by using a Public Key Infrastructure (PKI), which is based on a trusted third party, the Certificate Authority (CA). The CA can be either a commercial CA, such as Verisign, or a CA set up internal to the organization. The following figure illustrates conceptually how PKI works.

Figure 6: Trusted third party: certificate authority



1. Both A and B trust CA.
2. A asks the CA to sign a message verifying A's public key.
3. The CA signs the message using its private key, resulting in a "certificate."
4. A gives the certificate to B.
5. B can verify the certificate from A (and hence A's public key) using the CA's public key.

X.509 is a standard that defines public key certificate formats, revocation, and so on. Given the above scheme, L2TP/IPsec VPN with X.509 certificates works as follows.

1. The network admin obtains a certificate signed by a CA for each remote user (A in the example) and distributes it, along with public/private keys for the user, to the user through a secure channel.
2. The network admin configures the VPN server (B in the example) with the CA's public key, among other things.
3. When the remote client connects to the VPN server, it presents its certificate.
4. The VPN server verifies the certificate using the CA's public key. If the authentication is successful, the result tells the server the client's public key.
5. The server can then use the client's public key for authentication as described previously.
6. If authentication is successful, the IPsec tunnel is established between the client and server. Then the L2TP and PPP operations are identical to the PSK case described previously.

Planning considerations

The following points should be taken into consideration when planning a Remote Access VPN configuration:

- `Dedicated subnet` - At least one dedicated subnet should be used for remote access VPN users. This subnet should not overlap with existing subnets on the private network.
- `Address pools must not overlap` - As it is possible to define multiple address pools, care must be taken to not overlap the address ranges in these pools. In addition, the address pool ranges must be unique with the router configuration.
- `Routes to VPN clients are required` - In addition to configuring the remote access VPN server and clients, routers on the corporate network must be made aware of the VPN client subnet so that they know to forward traffic destined for clients through the VPN server. This can be done using static routes and route redistribution in local routing protocols.
- `Concurrent use of site-to-site and L2TP remote access VPN` - The L2TP remote access server must not be configured if an IPsec site-to-site peer address is set to 0.0.0.0. Neither protocol will function properly in this scenario. This is a problem because it is unclear whether the incoming IKE connection requests are from a site-to-site client with a dynamic IP address, or an L2TP remote access client.
- `Full Tunneling vs. Split Tunneling` - Full Tunneling means that all traffic from the remote access VPN client (that is, traffic destined for the corporate network and traffic destined for the Internet) flows across the VPN. Split Tunneling means that only traffic destined for the corporate network flows across the VPN. Internet traffic goes directly from the client to the Internet. The advantage of Full Tunneling is that Internet access can be controlled centrally. The disadvantage is that it consumes more corporate bandwidth and VPN server resources to service the additional traffic. The advantage of Split Tunneling is that it it makes better use of network resources. The disadvantage is that Internet access control must be provided and maintained on the client. In addition, the routing configuration on the client becomes complicated and must be performed manually each time the client connects if the default classful route added by the client software (that is, a route to 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16) is insufficient (for example, if you need to reach both 10.1.0.0/24 and 172.16.1.0/24). If this is the case, and Split Tunneling is desired, OpenVPN is a better solution as it provides better Split Tunnel support. For more information on OpenVPN, see the AT&T Vyatta Network Operating System OpenVPN Configuration Guide.

  Full Tunneling is the default with Windows (L2TP) clients. Split Tunneling is the default with OpenVPN clients.

Remote access using OpenVPN

The AT&T Vyatta vRouter also supports remote access using OpenVPN. For more information on OpenVPN, see AT&T Vyatta Network Operating System OpenVPN Configuration Guide.

RA VPN with zone-based firewall

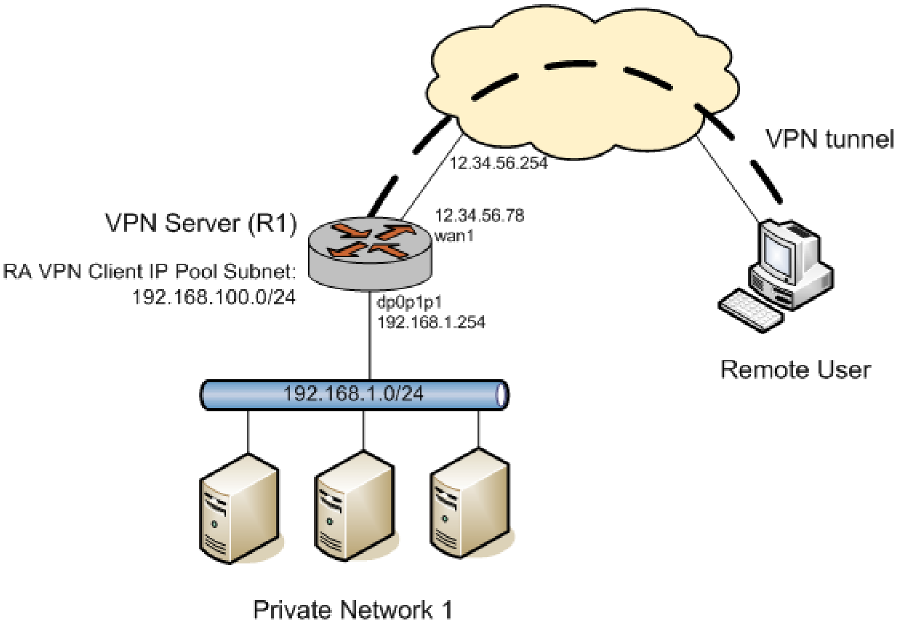
To configure the firewall to treat all Remote Access VPN users as a separate firewall zone, see documentation on zone-based firewall configuration in the AT&T Vyatta Network Operating System Firewall Configuration Guide.

Remote Access VPN Configuration

RA VPN configuration overview

This chapter provides configuration examples for three of the RA VPN scenarios supported: L2TP/IPsec with pre-shared key, and L2TP/IPsec with X.509 certificates. Each configuration example uses the diagram shown below as the deployment scenario:

Figure 7: Remote access VPN example



L2TP/IPsec with pre-shared key

The first step in configuring a basic remote access VPN setup using L2TP/IPsec with pre-shared key between R1 and a Windows XP client is to configure R1 as an L2TP/IPsec-based VPN server.

Table 1: Remote access VPN - L2TP/IPsec example

Step	Command
Enable NAT traversal. This is mandatory.	`vyatta@R1# set security vpn ipsec nat-traversal enable`
Set the allowed subnet.	`vyatta@R1# set security vpn ipsec nat-networks allowed-network 192.168.100.0/24`
Commit the change.	`vyatta@R1# commit`

Step	Command

Show the ipsec configuration.	`vyatta@R1# show security vpn ipsec`
	`ipsec {`
	`        nat-networks {`
	`                allowed-network 192.168.100.0/24`
	`        }`
	`        nat-traversal enable`
	`}`

Bind the L2TP server to the external address.	`vyatta@R1# set security vpn l2tp remote-access outside-address 12.34.56.78`
Set the nexthop address.	`vyatta@R1# set security vpn l2tp remote-access outside-nexthop 12.34.56.254`

Set up the pool of IP addresses that remote VPN connections will assume. In this case we make 10 addresses available (from .101 to .110) on subnet 192.168.100.0/24. Note that we do not use the subnet on the LAN.	`vyatta@R1# set security vpn l2tp remote-access client-ip-pool start 192.168.100.101`
	`vyatta@R1# set security vpn l2tp remote-access client-ip-pool stop 192.168.100.110`

(Optional) Set the server pool of IP addresses used at the router. In this example we make 10 server side addresses available (from .1 - .10) on subnet 10.22.0.0/24. Note that we do not use the subnet on the LAN.	`vyatta@R1# set security vpn l2tp remote-access server-ip-pool start 10.22.0.1`
	`vyatta@R1# set security vpn l2tp remote-access server-ip-pool stop 10.22.0.10`

Set the IPsec authentication mode to pre-shared secret.	`vyatta@R1# set security vpn l2tp remote-access ipsec-settings authentication mode pre-shared-secret`
Set the pre-shared secret.	`vyatta@R1# set security vpn l2tp remote-access ipsec-settings authentication pre-shared-secret !secrettext!`
Set the L2TP remote access authentication mode to local.	`vyatta@R1# set security vpn l2tp remote-access authentication mode local`
Set the L2TP remote access username and password.	`vyatta@R1# set security vpn l2tp remote-access authentication local-users username testuser password testpassword`
Commit the change.	`vyatta@R1# commit`

<table>
<tr><th>Step</th><th>Command</th></tr>
<tr><td>Show the l2tp remote access configuration.</td><td><pre>
vyatta@R1# show security vpn l2tp remote-
access
remote-access {
        authentication {
                local-users {
                        username testuser {
                                password
 "********"
                        }
                }
                mode local
        }
        client-ip-pool {
                start 192.168.100.101
                stop 192.168.100.110
        }
        ipsec-settings {
                authentication {
                        mode pre-shared-secret
                        pre-shared-secret
 "********"
                }
        }
        outside-address 12.34.56.78
        outside-nexthop 12.34.56.254
        server-ip-pool {
                start 10.22.0.1
                stop 10.22.0.10
        }
}
</pre></td></tr>
</table>

The next step is to configure the L2TP/IPsec VPN client on a Windows XP SP2 system (the remote user in the example). You can use the Windows **New Connection Wizard** as follows.

1. Select **Start#Control Panel#Network Connections**.
2. Click **Create a new connection**. The **New Connection Wizard** launches. Click **Next**.
3. Select **Connect to the network at my workplace**. Click **Next**.
4. Select **Virtual Private Network connection**. Click **Next**.
5. Enter a name for the connection; for example vRouter-L2TP. Click **Next**.
6. Select **Do not dial the initial connection**. Click **Next**.
7. Type the VPN server address (12.34.56.78 in the example). Click **Next**.
8. If asked, select **Do not use my smart card**. Click **Next**.
9. Click **Finish**.

By default, after the VPN configuration is created, a pre-shared key is not configured and must be added.

1. Go to **Network Connections** in the **Control Panel**.
2. Right-click the vRouter-L2TP (or whatever name you specified) icon. Select **Properties**.
3. Click the **Security** tab. Click **IPsec Settings...**.
4. Check the **Use pre-shared key for authentication** checkbox.
5. Type the pre-shared key (!secrettext! in our example) in the **Key** field.
6. Click **OK**. Click **OK**.

To connect to the VPN server, double-click the vRouter-L2TP icon, type the user name (testuser in our example) and password (testpassword in our example), and then click **Connect**. The `show interfaces` and `show vpn remote-access` operational commands will display the connected user on an interface named l2tp*x* where *x* is an integer.

Note: You need to make sure that, between the remote client and the VPN server, nothing is blocking packets with protocol L2TP or UDP port 500. (Check firewall settings, home gateway, DSL modem, ISP, and so on.)

Configuring the L2TP/IPsec VPN client on a Windows XP SP2 system

The next step is to configure the L2TP/IPsec VPN client on a Windows XP SP2 system (the remote user in the example). You can use the Windows **New Connection Wizard** as follows.

1. Select **Start#Control Panel#Network Connections.**
2. Click **Create a new connection**. The **New Connection Wizard** launches. Click **Next**.
3. Select **Connect to the network at my workplace**. Click **Next**.
4. Select **Virtual Private Network connection**. Click **Next**.
5. Enter a name for the connection; for example vRouter-L2TP. Click **Next**.
6. Select **Do not dial the initial connection**. Click **Next**.
7. Type the VPN server address (12.34.56.78 in the example). Click **Next**.
8. If asked, select **Do not use my smart card**. Click **Next**.
9. Click **Finish**.

Connecting to the VPN server

1. Go to **Network Connections** in the **Control Panel**.
2. Right#click the vRouter#L2TP (or whatever name you specified) icon. Select **Properties**.
3. Click the **Security** tab. Click **IPsec Settings...**.
4. Check the **Use pre#shared key for authentication** checkbox.
5. Type the pre#shared key (!secrettext! in our example) in the **Key** field.
6. Click **OK**. Click **OK**.

Info:

To connect to the VPN server, double-click the vRouter-L2TP icon, type the user name (testuser in our example) and password (testpassword in our example), and then click **Connect**. The `show interfaces` and `show vpn remote-access` operational commands will display the connected user on an interface named l2tp*x* where *x* is an integer.

Note: You need to make sure that, between the remote client and the VPN server, nothing is blocking packets with protocol L2TP or UDP port 500. (Check firewall settings, home gateway, DSL modem, ISP, and so on.)

L2TP/IPsec with x.509 certificates

The first step in configuring a basic remote access VPN setup using L2TP/IPsec with X.509 certificates between R1 and a Windows XP client is to obtain the files necessary for authentication using X.509 certificates. In general, the procedure for doing this is as follows:

1. Generate the private key and a certificate signing request (CSR) (based on the public key). This can be accomplished using `generate vpn x509 key-pair` *name* (for example, `generate vpn x509 key-pair R1`, where `R1.key` is the private key and `R1.csr` is the certificate signing request file - both created in `/config/auth`).
2. Send the CSR file (for example, `R1.csr`) to the certificate authority (CA) and receive back a server certificate (for example, `R1.crt`), the CA certificate (for example, `ca.crt`), and potentially, a certificate revocation list (CRL) file. This procedure varies according to the CA being used.
3. The same procedure should be followed to obtain equivalent files for the Windows client machine (for example, `windows.crt` and `windows.key`). The same CA certificate (`ca.crt`) can be used on the Windows machine.

Note: If the CA can combine the `windows.crt` and `windows.key` files and export a PKCS #12 file (for example, `windows.p12`), it will save a step later on.

Once the X.509-related files have been generated or acquired, the next step is to configure R1 as an L2TP/IPsec-based VPN server.

Table 2: Remote access VPN - L2TP/IPsec example

Step	Command
Define the interface used for IPsec; in this case, dp0p1p1.	`vyatta@R1# set security vpn ipsec ipsec-interfaces interface dp0p1p1`
Enable NAT traversal. This is mandatory.	`vyatta@R1# set security vpn ipsec nat-traversal enable`
Set the allowed subnet.	`vyatta@R1# set security vpn ipsec nat-networks allowed-network 192.168.100.0/24`
Commit the change.	`vyatta@R1# commit`

Show the ipsec configuration.	`vyatta@R1# show vpn ipsec`
	`ipsec-interfaces {`
	`    interface dp0p1p1`
	`}`
	`nat-networks {`
	`    allowed-network 192.168.100.0/24 {`
	`    }`
	`}`
	`nat-traversal enable`

Bind the L2TP server to the external address.	`vyatta@R1# set security vpn l2tp remote-access outside-address 12.34.56.78`
Set the nexthop address.	`vyatta@R1# set security vpn l2tp remote-access outside-nexthop 12.34.56.254`

Set up the pool of IP addresses that remote VPN connections will assume. In this case we make 10 addresses available (from .101 to .110) on subnet 192.168.100.0/24. Note that we do not use the subnet on the LAN.	`vyatta@R1# set security vpn l2tp remote-access client-ip-pool start 192.168.100.101`
	`vyatta@R1# set security vpn l2tp remote-access client-ip-pool stop 192.168.100.110`

(Optional) Set the server pool of IP addresses used at the router. In this example we make 10 server side addresses available (from .1 - .10) on subnet 10.22.0.0/24. Note that we do not use the subnet on the LAN.	`vyatta@R1# set security vpn l2tp remote-access server-ip-pool start 10.22.0.1`
	
	`vyatta@R1# set security vpn l2tp remote-access server-ip-pool stop 10.22.0.10`

Set the IPsec authentication mode to x509.	`vyatta@R1# set security vpn l2tp remote-access ipsec-settings authentication mode x509`

Step	Command
Specify the location of the CA certificate.	`vyatta@R1# set security vpn l2tp remote-access ipsec-settings authentication x509 ca-cert-file /config/auth/ca.crt`
Specify the location of the server certificate.	`vyatta@R1# set security vpn l2tp remote-access ipsec-settings authentication x509 server-cert-file /config/auth/R1.crt`
Specify the location of the server key file.	`vyatta@R1# set security vpn l2tp remote-access ipsec-settings authentication x509 server-key-file /config/auth/R1.key`
Specify the password for the server key file.	`vyatta@R1# set security vpn l2tp remote-access ipsec-settings authentication x509 server-key-password testpwd-R1 testpwd-R1`
Set the L2TP remote access authentication mode to local.	`vyatta@R1# set security vpn l2tp remote-access authentication mode local`
Set theL2TP remote access username and password.	`vyatta@R1# set security vpn l2tp remote-access authentication local-users username testuser password testpassword`
Commit the change.	`vyatta@R1# commit`

<table>
<tr><th>Step</th><th>Command</th></tr>
<tr><td>Show the l2tp remote access configuration.</td><td><pre>
vyatta@R1# show security vpn l2tp remote-
access
authentication {
    local-users {
        username testuser {
            password testpassword
        }
    }
    mode local
}
client-ip-pool {
    start 192.168.100.101
    stop 192.168.100.110
}
server-ip-pool {
    start 10.22.0.1
    stop 10.22.0.10
}
ipsec-settings {
    authentication {
        mode x509
        x509 {
            ca-cert-file /config/auth/ca.crt
            server-cert-file /config/auth/
R1.crt
            server-key-file /config/auth/
R1.key
            server-key-password testpwd-R1
        }
    }
}
outside-address 12.34.56.78
outside-nexthop 12.34.56.254
</pre></td></tr>
</table>

Once R1 is configured, the next step is to configure the L2TP/IPsec VPN client on a Windows XP SP2 system (the remote user in the example). The first part of this is to import the key and certificate files created by the CA onto the Windows machine. Windows expects the key and server certificates to be wrapped into a single file in a PKCS #12 format (a .p12 file).

> **Note:** If the CA does not provide this, then you will need to use a tool (e.g. openssl) to combine the key file and the certificate file for the Windows machine into a .p12 file.

1. Copy the `ca.crt` and `windows.p12` files to the Windows machine.
2. On the Windows machine: Select **Start#Run...**. The **Run** dialog opens.
3. Enter **mmc** at the **Open:** prompt. Click **OK**. The **Console1** MMC console opens.
4. Select **File#Add/Remove Snap#in...**. The **Add/Remove Snap#in** dialog opens.
5. Click **Add...**. The **Add Standalone Snap#in** dialog opens.
6. Select **Certificates** in the list of Available standalone snap#ins. Click **Add**. The **Certificates snap#in** dialog opens.
7. Select **Computer account**. Click **Next**. The **Select Computer** dialog appears.
8. Select **Local computer** (the computer this console is running on). Click **Finish**. Click **Close**. Click **OK**.

Certificates (Local Computer) appears beneath **Console Root** in the **Console1** MMC console. Now you can import the certificate, as follows.

1. Expand **Certificates (Local Computer)**.
2. Right click **Personal** and select **All Tasks#Import...**. The **Certificate Import Wizard** opens.
3. Click **Next**. Specify the location of the `windows.p12` file. Click **Next**.

4. Enter the password for the private key. Click **Next**. Click **Finish**.
5. Right click **Trusted Root Certification Authorities** and select **All Tasks#Import...**. The **Certificate Import Wizard** opens.
6. Click **Next**. Specify the location of the ca.crt file. Click **Next**.
7. Click **Finish**. Close the **Console1** MMC console.

At this point, the necessary key and certificate files have been imported to the Windows machine. The next part of configuring the L2TP/IPsec VPN client on the Windows XP SP2 system is to specify the VPN connection. You can use the Windows **New Connection Wizard** as follows.

1. Select **Start #Control Panel#Network Connections**.
2. Click **Create a new connection**. The **New Connection Wizard** launches. Click **Next**.
3. Select **Connect to the network at my workplace**. Click **Next**.
4. Select **Virtual Private Network connection**. Click **Next**.
5. Enter a name for the connection; for example vRouter#X509. Click **Next**.
6. Select **Do not dial the initial connection**. Click **Next**.
7. Type the VPN server address (12.34.56.78 in the example). Click **Next**.
8. If asked, select **Do not use my smart card**. Click **Next**.
9. Click **Finish**.

At this point, the configuration on the Windows machine is complete.

To connect to the VPN server, double#click the vRouter#X509 icon. Enter the User name and Password, then click **Connect** to establish the connection.

The `show interfaces` and `show vpn remote-access` operational commands will display the connected user on an interface named l2tp*x* where *x* is an integer.

> **Note:** You need to make sure that, between the remote client and the VPN server, nothing is blocking packets with protocol L2TP or UDP port 500. (Check firewall settings, home gateway, DSL modem, ISP, and so on.)

Split tunneling on a windows client

On a Windows client, by default, after the VPN configuration is created, the client is configured for Full Tunneling (all traffic flows across the VPN). If you want to configure the client for Split Tunneling (where Internet traffic does not flow across the VPN), you can modify the client VPN configuration as follows:

1. Select **Start #Control Panel#Network Connections**.
2. Right-click the icon for the VPN connection. Click **Properties**.
3. Click the **Networking** tab. Select **Internet Protocol (TCP/IP)**, then click **Properties**.
4. Click **Advanced**. Uncheck the **Use default gateway on remote network** checkbox.
5. Click **OK** three times.

Info:

Monitoring Remote Access VPN

Showing interface information

To see high-level interface information, you can use the `show interfaces` operational mode command, as shown in the following example. For Remote Access VPN connections, in addition to the local interface and the IP address it is bound to, you will see the remote user's name and the IP address assigned to the remote user.

Viewing interface information

```
vyatta@vyatta:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
dp0p2p1          10.224.66.52/25                   u/u
dp0p5p1          192.168.44.1/24                   u/u
dp0port2         23.23.23.23/24                    u/u
lo               127.0.0.1/8                       u/u
                 ::1/128
ppp0             10.22.0.1                         u/u  L2TP user3
                                                        192.168.101.1
ppp1             10.22.0.2                         u/u  L2TP user1
                                                        192.168.101.2
vyatta@vyatta:~$
```

Showing remote access VPN information

To see Remote Access VPN information specifically, you can use the `show vpn remote-access` operational mode command, as shown in the following example.

Viewing remote access VPN information

```
vyatta@vyatta:~$ show vpn remote-access
Active remote access VPN sessions:

User            Proto Iface  Tunnel IP       TX byte RX byte  Time
----            ----- -----  -----------     ------- -------  ----
bill           L2TP  ppp1   192.168.101.2       58    3.8K  00h02m09s
dave           L2TP  ppp0   192.168.101.1       58    3.8K  00h02m32s
vyatta@vyatta:~$
```

Remote Access VPN Commands

reset vpn remote-access all

Terminates all remote-access VPN tunnels.

Syntax:

`reset vpn remote-access all`

Operational mode

Use this command to terminate all remote access VPN tunnels.

The following example terminates all remote access VPN tunnels.

```
vyatta@vyatta# reset vpn remote-access all
vyatta@vyatta#
```

reset vpn remote-access interface <interface>

Terminates the specified active session.

Syntax:

`reset vpn remote-access interface` *interface*

interface

The interface associated with the session to be terminated.

Operational mode

Use this command to terminate a specific remote access VPN tunnel.

The following example terminates the active session on dp0p1p1.

```
vyatta@vyatta# reset vpn remote-access interface dp0p1p1
vyatta@vyatta#
```

reset vpn remote-access user <username>

Terminates the specified user's active sessions.

Syntax:

`reset vpn remote-access user` *username* [**`protocol`** { **`l2tp`** }]

username

The user name associated with the sessions to be terminated.

`l2tp`

Terminate the specified user's session that is using the l2tp protocol.

Operational mode

Use this command to terminate remote access VPN tunnels for the specified user. Use the **`l2tp`** option to specify a particular session. This is useful when a user has simultaneous sessions open on different protocols.

The following example terminates all active sessions for user robert.

```
vyatta@vyatta# reset vpn remote-access user robert
vyatta@vyatta#
```

security vpn l2tp

Creates the top-most configuration node for L2TP VPN, enabling L2TP VPN functionality.

Syntax:
`set security vpn l2tp`

Syntax:
`delete security vpn l2tp`

Syntax:
`show security vpn l2tp`

Configuration mode

```
security {
          vpn {
             l2tp
    }
}
```

Use this command to create the configuration node for Layer 2 Tunneling Protocol (L2TP) Virtual Private Network (VPN) functionality.

Use the `set` form of this command to create the L2TP VPN configuration node.

Use the `delete` form of this command to remove all L2TP VPN configuration.

Use the `show` form of this command to display L2TP VPN configuration.

security vpn l2tp remote-access authentication mode <mode>

Specifies user authentication mode for L2TP VPN remote access connections.

Syntax:
`set security vpn l2tp remote-access authentication mode` *mode*

Syntax:
`delete security vpn l2tp remote-access authentication mode`

Syntax:
`show security vpn l2tp remote-access authentication mode`

Users are authenticated using the system's local user database defined in the vpn l2tp configuration.

mode

The mode to be used for authenticating remote users. Supported values are as follows:

`local`: Authenticates users locally.

`radius`: Authenticates using a RADIUS server.

Configuration mode

```
security {
          vpn {
             l2tp {
                remote-access {
                authentication {
                          mode mode
             }
          }
       }
   }
}
```

Use this command to specify how L2TP VPN remote users are to be authenticated.

Users can be authenticated either locally, using login credentials specified using the `security vpn l2tp remote-access authentication local-users username` *username* command, or using one or more servers running the Remote Access Dial In User Service (RADIUS) protocol.

If you specify RADIUS authentication, you must specify the location of the RADIUS servers, and record the RADIUS login password, by using the `security vpn l2tp remote-access authentication radius-server ipv4 key` *key* command.

Use the `set` form of this command to configure the authentication mode for users.

Use the `delete` form of this command to remove the user authentication mode.

Use the `show` form of this command to display the user authentication mode.

security vpn l2tp remote-access authentication local-users username <username>

Specifies the login credentials for L2TP VPN remote users being authenticated locally.

Syntax:
set security vpn l2tp remote-access authentication local-users username *username* [**disable** | **password** *password* | **static-ip** *ipv4*]

Syntax:
delete security vpn l2tp remote-access authentication local-users username *username* [**disable** | **password** | **static-ip**]

Syntax:
show security vpn l2tp remote-access authentication local-users username *username* [**password** | **static-ip**]

username
The user name. Mandatory if **authentication** mode is local.

disable
Disables remote access for the user.

password
The login password for the specified user. Mandatory if **authentication** mode is local.

ipv4
The IPv4 address to assign the user when they connect. This address does not have to be part of the client-ip-pool.

Configuration mode

```
security {
          vpn {
             l2tp {
                remote-access {
                   authentication {
                          local-users {
                             username username {
                                 disable
                                 password password
                                 static-ip ipv4
                        }
                    }
                }
            }
        }
    }
}
```

Use this command to specify login credentials for L2TP VPN remote users and, optionally, to specify the IP address that will be assigned to a user when they connect.

Use the `set` form of this command to create the user name configuration node for the user.

Use the `delete` form of this command to remove a user's login credentials.

Use the `show` form of this command to display the user login authentication configuration.

security vpn l2tp remote-access authentication radius-server <ipv4> key <key>

Defines a RADIUS server authenticating L2TP VPN remote users.

Syntax:
`set security vpn l2tp remote-access authentication radius-server` *ipv4* **`key`** *key*

Syntax:
`delete security vpn l2tp remote-access authentication radius-server` *ipv4* [**`key`**]

Syntax:
`show security vpn l2tp remote-access authentication radius-server` *ipv4* [**`key`**]

ipv4

Multi-node. The IPv4 address of the RADIUS server. Mandatory if **`authentication`** `mode` is `radius`.

You can define more than one RADIUS server by creating multiple **`radius-server`** configuration nodes.

key

The password for the RADIUS server. This must be the same as that recorded on the RADIUS server. Mandatory if **`authentication`** `mode` is `radius`.

Supported characters are alphanumeric, space, and special characters. Strings containing spaces must be enclosed in double quotes.

Configuration mode

```
security {
          vpn {
             l2tp {
                    remote-access {
                       authentication {
                          radius-server ipv4 {
                                       key key
                }
             }
          }
       }
    }
}
```

Use this command to define one or more RADIUS servers for authenticating remote L2TP VPN and the login credentials required to access it.

At least one RADIUS server must be defined if RADIUS is set as the user authentication mode.

RADIUS servers are queried in the order they were configured. If the query to the first RADIUS server times out, the next RADIUS server in the list is queried. If no query is successful, the login attempt fails.

The RADIUS secret is specified in plain text. RADIUS secrets are stored in plain text on the system, and used as part of a cryptographic operation for transferring authentication information securely over the network. When you view RADIUS secrets, they are displayed in plain text.

Use the `set` form of this command to define a RADIUS server. Note that you cannot use **`set`** to change the IP address of a defined server. To change the server's IP address, delete the server and create a new one.

Use the `delete` form of this command to remove the RADIUS server configuration node or the key. Note that the key is mandatory; if you delete the key, you must configure another one.

Use the `show` form of this command to display RADIUS server configuration.

security vpn l2tp remote-access client-ip-pool start <ipv4>

Specifies the beginning address of a pool of IP addresses for L2TP VPN remote clients.

Syntax:
`set security vpn l2tp remote-access client-ip-pool start` *ipv4*

Syntax:
`delete security vpn l2tp remote-access client-ip-pool start`

Syntax:
`show security vpn l2tp remote-access client-ip-pool start`

The default beginning address is 10.255.0.0.

ipv4

The IP address that designates the beginning of the address pool.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                client-ip-pool {
                          start ipv4
             }
          }
       }
    }
}
```

Use this command to specify the beginning address of an address pool for remote L2TP VPN clients. Each L2TP VPN connection requires a client address and a server address. Both the beginning and ending addresses must be specified for the remote L2TP VPN clients. Use the `security vpn 12tp remote-access client-ip-pool stop` *ipv4* command to specify the ending address for the L2TP VPN clients.

For information on how to specify the range of addresses for an L2TP server, refer to the `security vpn 12tp remote-access server-ip-pool start` *ipv4* and `security vpn 12tp remote-access server-ip-pool stop` *ipv4* commands.

Use the `set` form of this command to specify the beginning address.

Use the `delete` form of this command to delete the beginning address.

Use the `show` form of this command to display the beginning address.

security vpn l2tp remote-access client-ip-pool stop <ipv4>

Specifies the ending address of a pool of IP addresses for L2TP VPN remote clients.

Syntax:

```
set security vpn l2tp remote-access client-ip-pool stop ipv4
```

Syntax:

```
delete security vpn l2tp remote-access client-ip-pool stop
```

Syntax:

```
show security vpn l2tp remote-access client-ip-pool stop
```

The default ending address is 10.255.255.255.

ipv4

The IP address that designates the end of the address pool.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                client-ip-pool {
                          stop ipv4
             }
          }
       }
    }
}
```

Use this command to specify the ending address of an address pool for remote L2TP VPN clients. Each L2TP VPN connection requires a client address and a server address. Both the beginning and ending addresses must be specified for the remote L2TP VPN clients. Use the `security vpn 12tp remote-access client-ip-pool start` *ipv4* command to specify the beginning address for the L2TP VPN clients.

For information on how to specify the range of addresses for an L2TP server, refer to the `security vpn 12tp remote-access server-ip-pool start` *ipv4* and `security vpn 12tp remote-access server-ip-pool stop` *ipv4* commands.

Use the `set` form of this command to specify the ending address.

Use the `delete` form of this command to delete the ending address.

Use the `show` form of this command to display the ending address.

security vpn l2tp remote-access dhcp-interface <interface>

Specifies a DHCP client interface to use for remote access L2TP VPN connections.

Syntax:

```
set security vpn l2tp remote-access dhcp-interface interface
```

Syntax:

```
delete security vpn l2tp remote-access dhcp-interface
```

Syntax:

```
show security vpn l2tp remote-access dhcp-interface
```

interface

The interface to use for remote access L2TP VPN connections (for example, dp0p1p1). Note that the interface must already have IPsec VPN enabled, using the `security vpn ipsec ipsec-interfaces interface` *if-name* command (described in the AT&T Vyatta Network Operating System IPsec Site-to-Site VPN Configuration Guide), and must be configured as a DHCP client.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                dhcp-interface interface
             }
          }
       }
}
```

Use this command to specify a DHCP client interface to use for remote access L2TP VPN connections. Connections will be automatically restarted if the IP address changes.

The DHCP interface is the interface facing the external network. This is the interface to which the L2TP server binds, and only remote connections coming into this interface will be accepted.

> **Note:** This command cannot be used if the `security vpn 12tp remote-access outside-address` *ipv4* command is also set.

Use the `set` form of this command to specify a DHCP interface to use for remote access L2TP VPN connections.

Use the `delete` form of this command to remove the configuration.

Use the `show` form of this command to view the configuration.

security vpn l2tp remote-access dns-servers server-1 <ipv4>

Specifies the IP address for the primary DNS server for L2TP VPN remote clients.

Syntax:

`set security vpn l2tp remote-access dns-servers server-1` *ipv4*

Syntax:

`delete security vpn l2tp remote-access dns-servers server-1`

Syntax:

`show security vpn l2tp remote-access dns-servers server-1`

ipv4

The IP address of the primary DNS server for remote clients.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                dns-servers {
                   server-1 ipv4
             }
          }
       }
    }
}
```

Use this command to specify the primary DNS server to be associated with remote L2TP VPN clients.

Use the `set` form of this command to specify the primary DNS server IP address.

Use the `delete` form of this command to remove the primary DNS server IP address.

Use the `show` form of this command to display the primary DNS server IP address.

security vpn l2tp remote-access dns-servers server-2 <ipv4>

Specifies the IP address for the secondary DNS server for L2TP VPN remote clients.

Syntax:

`set security vpn l2tp remote-access dns-servers server-2` *ipv4*

Syntax:

`delete security vpn l2tp remote-access dns-servers server-2`

Syntax:

`show security vpn l2tp remote-access dns-servers server-2`

ipv4

The IP address of the secondary DNS server for remote clients.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                dns-servers {
                   server-2 ipv4
             }
          }
       }
    }
}
```

Use this command to specify the secondary DNS server to be associated with remote L2TP VPN clients.

Use the `set` form of this command to specify the secondary DNS server IP address.

Use the `delete` form of this command to remove the secondary DNS server IP address.

Use the `show` form of this command to display the secondary DNS server IP address.

security vpn l2tp remote-access ipsec-settings authentication mode <mode>

Sets the IPsec authentication mode to be used for IPsec authentication on remote access L2TP VPN connections.

Syntax:

`set security vpn l2tp remote-access ipsec-settings authentication mode` *mode*

Syntax:

`delete security vpn l2tp remote-access ipsec-settings authentication mode`

Syntax:

`show security vpn l2tp remote-access ipsec-settings authentication mode`

Pre-shared secret.

mode

Specifies the authentication mode to be used for IPsec authentication on L2TP VPN remote access connections. Supported values are as follows:

`pre-shared-secret`: Uses a pre-shared secret for authentication.

`x509`: Uses X.509 V.3 certificates for authentication.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                ipsec-settings {
                   authentication {
                      mode mode
                }
             }
          }
       }
   }
}
```

Use this command to set the authentication mode to be used for IPsec authentication on remote access L2TP VPN connections.

A pre-shared secret, or pre-shared key (PSK), is a method of authentication. The secret, or key, is a string agreed upon beforehand by both parties as key for authenticating the session. It is used to generate a hash such that each VPN endpoint can authenticate the other.

If the **`authentication`** `mode` is **`pre-shared-secret`**, you must configure the secret using the `security vpn l2tp remote-access ipsec-settings authentication pre-shared-secret` *secret* command.

The pre-shared secret is not passed from side to side. It is configured on both sides, and must match on both sides. Pre-shared secrets are less secure than X.509 certificates.

Note: You should restrict the use of pre-shared keys to smaller, low-risk environments.

X.509 v.3 certificates are certificates conforming to the ITU-T X.509 version 3 standard for public key infrastructure (PKI). The certificate is issued by a Certificate Authority (CA), and stored securely on the local AT&T Vyatta vRouter.

If the mode is X.509 certificates, you must configure all X.509 certificate information.

Use the `set` form of this command to specify the authentication mode for remote access L2TP VPN.

Use the `delete` form of this command to remove authentication mode configuration.

Use the `show` form of this command to display authentication mode configuration.

security vpn l2tp remote-access ipsec-settings authentication pre-shared-secret <secret>

Sets a pre-shared key for IPsec authentication on remote access L2TP VPN connections.

Syntax:

```
set security vpn l2tp remote-access ipsec-settings authentication pre-shared-secret secret
```

Syntax:

```
delete security vpn l2tp remote-access ipsec-settings authentication pre-shared-secret
```

Syntax:

```
show security vpn l2tp remote-access ipsec-settings authentication pre-shared-secret
```

secret

The password, or secret, to be used to authenticate the remote access connection. This parameter is mandatory if **`authentication`** `mode` is **`pre-shared-secret`**. The secret must be the same on both sides of the connection.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                ipsec-settings {
                   authentication {
                      pre-shared-secret secret
                }
             }
          }
       }
    }
}
```

Use this command to set a pre-shared secret to be used to authenticate the IPsec part of remote access L2TP VPN connections.

Use the `set` form of this command to specify the pre-shared secret.

Use the `delete` form of this command to remove pre-shared secret configuration.

Use the `show` form of this command to display pre-shared secret configuration.

security vpn l2tp remote-access ipsec-settings authentication x509 ca-cert-file <file-name>

Specifies the name of an X.509 Certificate Authority (CA) certificate file for IPsec authentication on remote access L2TP VPN connections.

Syntax:

```
set security vpn l2tp remote-access ipsec-settings authentication x509 ca-cert-file file-name
```

Syntax:

```
delete security vpn l2tp remote-access ipsec-settings authentication x509 ca-cert-file
```

Syntax:

```
show security vpn l2tp remote-access ipsec-settings authentication x509 ca-cert-file
```

file-name

The name of a certificate file. This parameter is mandatory if **`authentication`** `mode` is **`x509`**.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
             ipsec-settings {
                authentication {
                   x509 {
                      ca-cert-file file-name
                   }
                }
```

```
                  }
               }
            }
         }
}
```

Use this command to specify the name of an X.509 Certificate Authority (CA) certificate file. The X.509 CA certificate is used for IPsec authentication on remote access L2TP VPN connections.

The file is assumed to be in `/config/auth` unless an absolute path is specified.

Use the `set` form of this command to specify the name of the CA certificate file.

Use the `delete` form of this command to remove the name of the CA certificate file.

Use the `show` form of this command to display CA certificate file configuration.

security vpn l2tp remote-access ipsec-settings authentication x509 crl-file <file-name>

Specifies the name of an X.509 Certificate Revocation List (CRL) file for IPsec authentication on L2TP VPN remote access connections.

Syntax:

```
set security vpn l2tp remote-access ipsec-settings authentication x509 crl-file file-name
```

Syntax:

```
delete security vpn l2tp remote-access ipsec-settings authentication x509 crl-file
```

Syntax:

```
show security vpn l2tp remote-access ipsec-settings authentication x509 crl-file
```

file-name

The name of the CRL file.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                ipsec-settings {
                   authentication {
                      x509 {
                         crl-file file-name
                   }
                }
             }
          }
       }
    }
}
```

Use this command to specify the name of a Certificate Revocation List (CRL) file.

A CRL is a time-stamped signed data structure issued by the Certificate Authority (CA) identifying revoked certificates. When the remote user attempts to log on to the system, the system checks both the remote user's certificate signature and also the CRL to make sure that the remote user's certificate serial number is not on the CRL.

The file is assumed to be in `/config/auth` unless an absolute path is specified.

Use the `set` form of this command to specify the location of the CRL file.

Use the `delete` form of this command to remove the location of the CRL file.

Use the `show` form of this command to display CRL file configuration.

security vpn l2tp remote-access ipsec-settings authentication x509 server-cert-file <file-name>

Specifies the name of VPN server's certificate file for IPsec authentication on L2TP VPN remote access connections.

Syntax:

```
set security vpn l2tp remote-access ipsec-settings authentication x509 server-cert-file file-name
```

Syntax:

```
delete security vpn l2tp remote-access ipsec-settings authentication x509 server-cert-file
```

Syntax:

```
show security vpn l2tp remote-access ipsec-settings authentication x509 server-cert-file
```

file-name

The name of the VPN server's certificate file. This parameter is mandatory if **`authentication`** `mode` is **`x509`**.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                ipsec-settings {
                   authentication {
                      x509 {
                         server-cert-file file-name
                   }
                }
             }
          }
       }
    }
}
```

Use this command to specify the name of the VPN server's certificate file.

VPN server's certificate certifies the identity of the VPN server.

The file is assumed to be in `/config/auth` unless an absolute path is specified.

Use the `set` form of this command to specify the name of the VPN server's certificate file.

Use the `delete` form of this command to remove the name of the VPN server's certificate file.

Use the `show` form of this command to display VPN server certificate file configuration.

security vpn l2tp remote-access ipsec-settings authentication x509 server-key-file <file-name>

Specifies the name of VPN server's private key file for IPsec authentication on L2TP VPN remote access connections.

Syntax:

```
set security vpn l2tp remote-access ipsec-settings authentication x509 server-key-file file-name
```

Syntax:

```
delete security vpn l2tp remote-access ipsec-settings authentication x509 server-key-file
```

Syntax:

```
show security vpn l2tp remote-access ipsec-settings authentication x509 server-key-file
```

file-name

The name of the VPN server's private key file. This parameter is mandatory if **`authentication`** `mode` is **`x509`**.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                ipsec-settings {
                   authentication {
                      x509 {
                         server-key-file file-name
                      }
                   }
                }
             }
          }
       }
}
```

Use this command to specify the name of the VPN server's private key file.

VPN server's private key certifies the identity of the VPN server.

The file is assumed to be in `/config/auth` unless an absolute path is specified.

Use the `set` form of this command to specify the name of the VPN server's private key file.

Use the `delete` form of this command to remove the name of the VPN server's private key file.

Use the `show` form of this command to display VPN server private key file configuration.

security vpn l2tp remote-access ipsec-settings authentication x509 server-key-password <password>

Specifies the password that protects the L2TP VPN server's private key.

Syntax:

```
set security vpn l2tp remote-access ipsec-settings authentication x509 server-key-password password
```

Syntax:

```
delete security vpn l2tp remote-access ipsec-settings authentication x509 server-key-password
```

Syntax:

```
show security vpn l2tp remote-access ipsec-settings authentication x509 server-key-password
```

password

The password protecting the VPN server's private key file.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                ipsec-settings {
                   authentication {
                      x509 {
                         server-key-password password
                   }
                }
             }
          }
       }
    }
}
```

Use this command to specify a password that protects the VPN server's private key.

Use the `set` form of this command to specify the password for the VPN server's private key.

Use the `delete` form of this command to remove the password for the VPN server's private key.

Use the `show` form of this command to display VPN servers private key password configuration.

security vpn l2tp remote-access ipsec-settings ike-lifetime <lifetime>

Specifies the IKE lifetime of an L2TP connection.

Syntax:
`set security vpn l2tp remote-access ipsec-settings ike-lifetime` *lifetime*

Syntax:
`delete security vpn l2tp remote-access ipsec-settings ike-lifetime`

Syntax:
`show security vpn l2tp remote-access ipsec-settings ike-lifetime`

The IKE lifetime is 3600 seconds (1 hour).

lifetime

The length of time (in seconds) the IKE connection will remain active after the last traffic from the remote end is received. The range is 30 to 86400 (that is, 24 hours). The default is 3600 (1 hour).

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                ipsec-settings {
                   ike-lifetime lifetime
             }
          }
       }
    }
}
```

Use this command to specify the IKE lifetime of an L2TP connection. The IKE lifetime is used to terminate a connection when the remote end has not been heard from for a period of time.

Use the `set` form of this command to specify the IKE lifetime of an L2TP connection.

Use the `delete` form of this command to return the IKE lifetime to its default.

Use the `show` form of this command to display IKE lifetime configuration.

security vpn l2tp remote-access mtu <mtu>

Specifies the MTU for an L2TP connection.

Syntax:

```
set security vpn l2tp remote-access mtu mtu
```

Syntax:

```
delete security vpn l2tp remote-access mtu
```

Syntax:

```
show security vpn l2tp remote-access mtu
```

If this value is not set, fragmentation is never performed.

mtu

Sets the MTU, in octets, for the interface as a whole, including any logical interfaces configured for it. The range is 128 to 16384.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                mtu mtu
          }

       }
    }
}
```

Use this command to set the maximum transmission unit (MTU) for an L2TP connection.

When forwarding, IPv4 packets larger than the MTU will be fragmented unless the DF bit is set. In that case, the packets will be dropped and an ICMP “Packet too big” message is returned to the sender.

Use the `set` form of this command to specify the MTU.

Use the `delete` form of this command to remove MTU value and disable fragmentation.

Use the `show` form of this command to view MTU configuration.

security vpn l2tp remote-access outside-address <ipv4>

Sets the IP address to be bound to the L2TP server.

Syntax:

```
set security vpn l2tp remote-access outside-address ipv4
```

Syntax:

```
delete security vpn l2tp remote-access
```

Syntax:

```
show security vpn l2tp remote-access
```

ipv4

The IPv4 address to which the L2TP server should bind.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                outside-address ipv4
          }

       }
    }
}
```

Use this command to set the outside address for a remote access L2TP VPN connection.

The outside address is the address of the interface facing the external network. This is the address to which the L2TP server binds, and only remote connections coming into this address will be accepted.

> **Note:** This command cannot be used if the `security vpn 12tp remote-access dhcp-interface` *interface* command is also set.

Use the `set` form of this command to set the L2TP VPN outside address.

Use the `delete` form of this command to remove the L2TP VPN outside address.

Use the `show` form of this command to display L2TP VPN outside address configuration.

security vpn l2tp remote-access outside-nexthop <ipv4>

Sets the IP address of the next hop on the external network.

Syntax:
`set security vpn l2tp remote-access outside-nexthop` *ipv4*

Syntax:
`delete security vpn l2tp remote-access outside-nexthop` *ipv4*

Syntax:
`show security vpn l2tp remote-access outside-nexthop`

ipv4
The IPv4 address of the next hop on the outside network.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                outside-nexthop ipv4
          }

       }
     }
}
```

Use this command to set the next hop on the external network for a remote access L2TP VPN connection.

Use the `set` form of this command to set the L2TP VPN outside next hop.

Use the `delete` form of this command to remove the L2TP VPN outside next hop.

Use the `show` form of this command to display L2TP VPN outside next-hop configuration.

security vpn l2tp remote-access server-ip-pool start <ipv4>

Specifies the beginning address of a pool of IP addresses for an L2TP server.

Syntax:
`set security vpn l2tp remote-access server-ip-pool start` *ipv4*

Syntax:
`delete security vpn l2tp remote-access server-ip-pool start`

Syntax:
`show security vpn l2tp remote-access server-ip-pool start`

The default beginning address is 10.255.0.0.

ipv4

The IP address that designates the beginning of the address pool.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                server-ip-pool {
                       start ipv4
             }
          }
       }
    }
}
```

Use this command to specify the beginning address of a pool of IP addresses for an L2TP server. Each L2TP VPN connection requires a client address and a server address. Both the beginning and ending addresses for the L2TP server must be specified. Use the `security vpn 12tp remote-access server-ip-pool stop` *ipv4* command to specify the ending address for the L2TP server.

For information on how to specify the range of addresses for L2TP VPN clients, refer to the `security vpn 12tp remote-access client-ip-pool start` *ipv4* and `security vpn 12tp remote-access client-ip-pool stop` *ipv4* commands.

> **Note:** The number of addresses that are used in the range for the L2TP server must be equal to or greater than the number of addresses that are used in the range for the L2TP VPN clients. And the address range that is used for L2TP server must be unique within your router configuration.

> **Note:** If you do not specify the beginning and ending addresses of a pool of IP addresses for an L2TP server, the AT&T Vyatta vRouter uses a default address range from 10.255.0.0 through 10.255.255.255. If you use the default range, ensure that this range is unique within your router configuration.

Use the `set` form of this command to specify the beginning address.

Use the `delete` form of this command to delete the beginning address.

Use the `show` form of this command to display the beginning address.

security vpn l2tp remote-access server-ip-pool stop <ipv4>

Specifies the ending address of a pool of IP addresses for an L2TP server.

Syntax:
`set security vpn l2tp remote-access server-ip-pool stop` *ipv4*

Syntax:
`delete security vpn l2tp remote-access server-ip-pool stop`

Syntax:
`show security vpn l2tp remote-access server-ip-pool stop`

The default ending address is 10.255.255.255.

ipv4
The IP address that designates the end of the address pool.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                server-ip-pool {
                       stop ipv4
             }
          }
       }
    }
}
```

Use this command to specify the ending address of a pool of IP addresses for an L2TP server. Each L2TP VPN connection requires a client address and a server address. Both the beginning and ending addresses for the L2TP server must be specified. Use the `security vpn 12tp remote-access server-ip-pool start` *ipv4* command to specify the beginning address for the L2TP server.

For information on how to specify the range of addresses for L2TP VPN clients, refer to the `security vpn 12tp remote-access client-ip-pool start` *ipv4* and `security vpn 12tp remote-access client-ip-pool stop` *ipv4* commands.

> **Note:** The number of addresses that are used in the range for the L2TP server must be equal to or greater than the number of addresses that are used in the range for the L2TP VPN clients. And the address range that is used for L2TP server must be unique within your router configuration.

> **Note:** If you do not specify the beginning and ending addresses of a pool of IP addresses for an L2TP server, the AT&T Vyatta vRouter uses a default address range from 10.255.0.0 through 10.255.255.255. If you use the default range, ensure that this range is unique within your router configuration.

Use the `set` form of this command to specify the ending address.

Use the `delete` form of this command to delete the ending address.

Use the `show` form of this command to display the ending address.

security vpn l2tp remote-access wins-servers server-1 <ipv4>

Specifies the IP address for the primary WINS server for L2TP VPN remote clients.

Syntax:
`set security vpn l2tp remote-access wins-servers server-1` *ipv4*

Syntax:
`delete security vpn l2tp remote-access wins-servers server-1`

Syntax:

`show security vpn l2tp remote-access wins-servers server-1`

ipv4

The IP address of the primary WINS server for remote clients.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                wins-servers {
                       server-1 ipv4
             }
          }
       }
    }
}
```

Use this command to specify a primary WINS server to be associated with remote L2TP VPN clients.

The Windows Internet Net Service (WINS) is used to support environments in which users access resources that have NetBIOS names.

Use the `set` form of this command to specify the primary WINS server IP address.

Use the `delete` form of this command to remove the primary WINS server IP address.

Use the `show` form of this command to display the primary WINS server IP address.

security vpn l2tp remote-access wins-servers server-2 <ipv4>

Specifies the IP address for the secondary WINS server for L2TP VPN remote clients.

Syntax:

`set security vpn l2tp remote-access wins-servers server-2` *ipv4*

Syntax:

`delete security vpn l2tp remote-access wins-servers server-2`

Syntax:

`show security vpn l2tp remote-access wins-servers server-2`

ipv4

The IP address of the secondary WINS server for remote clients.

Configuration mode

```
security {
       vpn {
          l2tp {
             remote-access {
                wins-servers {
                       server-2 ipv4
             }
          }
       }
    }
}
```

Use this command to specify the secondary WINS server to be associated with remote L2TP VPN clients.

The Windows Internet Net Service (WINS) is used to support environments in which users access resources that have NetBIOS names.

Use the `set` form of this command to specify the secondary WINS server IP address.

Use the `delete` form of this command to remove the secondary WINS server IP address.

Use the `show` form of this command to display the secondary WINS server IP address.

show vpn remote-access

Shows information about currently active remote access VPN sessions.

Syntax:

`show vpn remote-access`

Operational mode

Use this command to see information about the currently active remote access VPN sessions.

The following example shows the output of the `show vpn remote-access` command.

```
vyatta@vyatta# show vpn remote-access
Active remote access VPN sessions:
User            Proto Iface  Tunnel IP       TX byte RX byte  Time
----            ----- -----  -----------     ------- -------  ----
bill           L2TP  ppp1   192.168.101.2        58    3.8K  00h02m09s
dave           L2TP  ppp0   192.168.101.1        58    3.8K  00h02m32s
vyatta@vyatta#
```

List of Acronyms

Acronym	Description
ACL	access control list
ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
AMI	Amazon Machine Image
API	Application Programming Interface
AS	autonomous system
ARP	Address Resolution Protocol
AWS	Amazon Web Services
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BPDU	Bridge Protocol Data Unit
CA	certificate authority
CCMP	AES in counter mode with CBC-MAC
CHAP	Challenge Handshake Authentication Protocol
CLI	command-line interface
DDNS	dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DLCI	data-link connection identifier
DMI	desktop management interface
DMVPN	dynamic multipoint VPN
DMZ	demilitarized zone
DN	distinguished name
DNS	Domain Name System
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
eBGP	external BGP
EBS	Amazon Elastic Block Storage
EC2	Amazon Elastic Compute Cloud
EGP	Exterior Gateway Protocol
ECMP	equal-cost multipath
ESP	Encapsulating Security Payload
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HDLC	High-Level Data Link Control
I/O	Input/Output
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers

Acronym	Description
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IPS	Intrusion Protection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPOA	IP over ATM
IPsec	IP Security
IPv4	IP Version 4
IPv6	IP Version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISM	Internet Standard Multicast
ISP	Internet Service Provider
KVM	Kernel-Based Virtual Machine
L2TP	Layer 2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
MAC	medium access control
mGRE	multipoint GRE
MIB	Management Information Base
MLD	Multicast Listener Discovery
MLPPP	multilink PPP
MRRU	maximum received reconstructed unit
MTU	maximum transmission unit
NAT	Network Address Translation
NBMA	Non-Broadcast Multi-Access
ND	Neighbor Discovery
NHRP	Next Hop Resolution Protocol
NIC	network interface card
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OSPFv2	OSPF Version 2
OSPFv3	OSPF Version 3
PAM	Pluggable Authentication Module
PAP	Password Authentication Protocol
PAT	Port Address Translation
PCI	peripheral component interconnect
PIM	Protocol Independent Multicast
PIM-DM	PIM Dense Mode
PIM-SM	PIM Sparse Mode
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM

Acronym	Description
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PTMU	Path Maximum Transfer Unit
PVC	permanent virtual circuit
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
RHEL	Red Hat Enterprise Linux
RIB	Routing Information Base
RIP	Routing Information Protocol
RIPng	RIP next generation
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RSA	Rivest, Shamir, and Adleman
Rx	receive
S3	Amazon Simple Storage Service
SLAAC	Stateless Address Auto-Configuration
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
SPT	Shortest Path Tree
SSH	Secure Shell
SSID	Service Set Identifier
SSM	Source-Specific Multicast
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TBF	Token Bucket Filter
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
ToS	Type of Service
TSS	TCP Maximum Segment Size
Tx	transmit
UDP	User Datagram Protocol
VHD	virtual hard disk
vif	virtual interface
VLAN	virtual LAN
VPC	Amazon virtual private cloud
VPN	virtual private network
VRRP	Virtual Router Redundancy Protocol
WAN	wide area network
WAP	wireless access point
WPA	Wired Protected Access