10.5 Build a LAN-to-LAN VPN (Using L2 Bridge)

This section will explain how to create a layer 2 connection between two or more remote networks with a bridge connection.

10.5.1 About Bridge-Connected LAN VPNs

By using VPN Server and VPN Bridge you can create a layer 2 connection between a layer 2 segment (such as an Ethernet LAN) and another point on a public IP network such as the Internet.

In the past, it proved physically difficult to connect two points together into a single segment via a layer 2 connection. Then, services such as Wide Area Ethernet appeared and it became possible to extend an Ethernet segment out to another location via common carrier networks.

By using VPN Server and VPN Bridge together you can achieve what Wide Area Ethernet offers through an inexpensive broadband connection to the Internet. Furthermore, through the use of SSL, data transmitted between LANs can be encrypted. This means improved security compared to currently available Wide Area Ethernet or frame relay services.

10.5.2 Local Bridge and Cascade Connection Functionality

To build a LAN-to-LAN VPN you will need to utilize both local bridges (see section 3.6 Local Bridges) and cascade connections (3.4 Virtual Hub Functions).

Local bridging, which appeared in section 10.4 Build a Generic Remote Access VPN, is a feature that allows you to make an Ethernet connection between a Virtual Hub and a physical network adapter. A cascade connection is a feature that allows you to connect Virtual Hubs running on different computers together at the Ethernet level. These two features allow you to use SoftEther VPN to build an extremely flexible VPN.

10.5.3 Pros and Cons of Bridging

This section will explain the pros and cons of using only bridge connections between multiple networks to create a VPN connection.

Bridging - Pros

Using SoftEther VPN to make a layer 2 (Ethernet) bridge connection between two or more LANs is an extremely convenient, yet simple way to construct a LAN-to-LAN VPN. The pros of connecting two LANs via a layer 2 bridge connection are as follows:

- All LANs will have a direct layer 2 connection to each other. Logically, it is the same as if multiple LANs' switching hubs were connected to each other in a cascade connection with an extremely long Ethernet cable.
- TCP/IP and even older protocols such as NetBEUI and IPX/SPX can be used. All protocols that run over Ethernet are supported.
- The devices you can communicate with over the VPN are not limited to only computers. Any device that can be connected to via Ethernet is compatible. Even devices that use a special or proprietary protocol such as security cameras, digital video recorders, home electronics, VoIP telephones, etc. can be connected to via a bridge connection and used across networks.
- Because you do not have to deal with IP routing, the process of communicating between multiple networks has been simplified. Utilizing bridging allows you to effectively expand the area of use of a network, rather than simply connect networks together.

Bridging - Cons

At the same time, the cons of connecting two LANs via a layer 2 bridge connection are as follows:

- Because the LANs will be linked via a layer 2 connection, when TCP/IP is used within the VPN all LANs will, as a rule, belong to the same IP network. When you want to add a new LAN to a remote site, you can simply bridge the new LAN with the old LAN effectively expanding the original LAN. However, if you want to connect two existing LANs together with a local bridge you will have to re-design the network topology and come up with new IP address assignment rules. This could be a costly operation especially in the case of networks where IP addresses are static or assigned by hand.
- When bridging multiple LANs together there could be an increase in broadcast packet traffic due to the increased number of computers on the network.

If you believe the cons listed above would result in problems for your network, we recommend connecting your LANs via layer 3 routing. This method is introduced in section 10.6 Build a LAN-to-LAN VPN (Using L3 IP Routing).

10.5.4 Network Layout

This section will explain the following type of network layout as an example.

10-5-1.png

Network Layout.

In the above example, two physically separated LANs, one in Tokyo and one in Osaka, are formed into a single segment via a layer 2 (Ethernet) bridge connection.

Tokyo is the main LAN, and Osaka is the sub-LAN. In Tokyo, a Virtual Hub is created on the VPN Server computer and a local bridge connection is made to the network adapter on the LAN we wish to connect to. In Osaka, a Virtual Hub with the name "BRIDGE" is created on a computer with VPN Bridge installed and a local bridge connection is made to the network adapter on the LAN we wish to connect to. A cascade connection is also made to Tokyo from Osaka. Now, the once separated network segments are formed into a single segment which can communicate between each other.

Once the segments have been combined the computers on both segments can communicate as if they were on the same segment. Thus, they can be configured and used as if they were all on the same LAN.

When connecting 3 or more LANs together you must install a VPN Server on the designated "main" LAN and VPN Bridge on the remaining LANs. Then, you will make a cascade connection from each VPN Bridge to the VPN Server to connect the LANs together. This allows the computers on all the LANs to communicate with each other through the VPN Server at a layer 2 level.

10.5.5 Installing VPN Server On the Main LAN

First, VPN Server will be installed on the main LAN in Tokyo.

The computer you install VPN Server on must make a local bridge connection the company LAN in Tokyo. Therefore, it must be installed physically close enough to the LAN to connect to the layer 2 segment via a network cable.

Because the VPN Server must receive incoming VPN connections from the VPN Bridges over the Internet, it must have a public IP address or be able to receive TCP/IP communication through NAT, a firewall, or a reverse proxy system as described in section 10.2 Common Concepts and Knowledge. Please consult with your network administrator if you are unsure about any of these issues.

Now create a Virtual Hub in the VPN Server on the main LAN and name it whatever you like. You may use the default name of "DEFAULT" or name it something like "TOKYO" for easier management. The functionality will not be affected either way.

10.5.6 Installing VPN Bridge to the Sub-LAN

Next, a VPN Bridge will be configured on the sub-LAN in Osaka.

The computer you install VPN Bridge on must make a local bridge connection the company LAN in Osaka. Therefore, it must be installed physically close enough to the LAN to connect to the layer 2 segment via a network cable.

The VPN Bridge must also make a VPN connection to the VPN Server on the Tokyo LAN via the Internet, and thus must also be connected to the Internet. However, unlike the VPN Server the Osaka VPN Bridge will be making the VPN connection (cascade connection) to the VPN Server which is sitting on the Internet. Therefore, even if it is behind NAT, a firewall, or a proxy server and has a private IP address it will still be able

to make the connection. (However, be sure to take note of your NAT, firewall, or proxy server's load handling capabilities. The devices you send data through may become a bottleneck, lowering the overall communication speed of your VPN.)

10.5.7 Configuring the Local Bridges

Local bridges will be configured at both the VPN Server in Tokyo, and the VPN Bridge in Osaka. Refer to section 3.6 Local Bridges and create a local bridge connection from the Virtual Hub to the LAN.

You should be aware of the following things when making connections via a local bridge.

- As explained in detail in section 3.6 Local Bridges, if possible, try to set aside network adapters strictly for local bridging when making your local bridge connection. We recommend that you do not use a protocol stack for your local bridge network adapters, and do not assign TCP/IP IP addresses to them.
- We also recommend that you use a high quality network adapter from a trusted maker for your local bridge connections. For more information please refer to 3.6 Local Bridges.

10.5.8 Configuring Cascade Connections

Setting up the Osaka VPN Bridge's Virtual Hub to make a continuous cascade connection to the Tokyo LAN's VPN Server is the last step in configuring this LAN-to-LAN network.

First we'll make a new user for the cascade connection on the Virtual Hub on the Virtual Server in Tokyo. The username could be "osaka" or any other appropriate name. Password authentication (with a long enough password) should be a secure enough authentication method since the cascade connection configuration will most likely be done by the system administrator and not the end user. (For a more secure solution we recommend using X.509 certificate authentication for both the client and server.)

Next we'll make a cascade connection from the Osaka VPN Bridge's Virtual Hub to the Virtual Hub on the Tokyo LAN. For user authentication, we'll enter the username and password we registered to the Virtual Hub on the Tokyo LAN. (Or provide the X.509 authentication certificate and private key if using client certificate authentication.) Now we'll set our created cascade connection to "online" status. At this point, confirm that the cascade connection's connection status is set to "Online (Connection Established)".

10.5.9 Connecting to the LAN-to-LAN VPN/Performing a Communication Test

Once you have established a connection to a LAN-to-LAN VPN, both LANs should logically function as a single layer 2 (Ethernet) segment. To test if this is true, try some type of communication between both LANs that would be impossible unless they were both connected as a single LAN.

10.5.10 Supplementary Information

Take note of the following things when using a layer 2 bridge to make a bridged connection (by combining a cascade connection and a local bridge) between remote LANs.

- The multiple LANs that make up the LAN-to-LAN VPN will be logically connected as a single Ethernet network (broadcast domain segment) once they are connected via bridge connections. Thus, they will be able to communicate with each other as such. Therefore, computers will use the VPN to communicate between these networks exactly as if they were connected together as one big physical LAN.
- If there are DHCP servers running on the original LANs then once they are logically connected as a single segment it will be as if multiple DHCP servers are running on the same Ethernet network. As explained in section 10.2 Common Concepts and Knowledge, this causes protocol conflicts and overall network instability.
- When dealing with LANs that already have a fairly large amount of computers on them, you may have to make some changes to the network layout when building them into a LAN-to-LAN VPN using only bridge connections. (Especially when each computer is being assigned a static IP address.) If you are dealing with multiple LANs made up of multiple IP networks, we recommend also using IP routing (explained in section 10.6 Build a LAN-to-LAN VPN (Using L3 IP Routing)) when setting up your LAN-to-LAN VPN.

See Also

LAN to LAN Bridge

Geologically distributed branches are isolated as networks by default. SoftEther VPN lays virtual Ethernet cables between your all branches. Then all computers of all branches are connected to the single LAN.