3.6 Local Bridges

The local bridge is a function often used by the SoftEther VPN to make VPN connections. Local bridging is used to connect a virtual network and a physical network on the Ethernet level. This section will explain local bridge concepts, methods for setting them and precautions.

3.6.1 What is a Local Bridge?

The local bridge connection function (herein referred to as local bridge) can connect a Virtual Hub operating on the VPN Server or VPN Bridge and the physical network adapter connected to that server computer on a layer 2 connection, thereby joining two segments which originally operated as separate Ethernet segments into one.

Local bridging enables a computer connected to a Virtual Hub and a computer connected to a physical LAN to communicate freely on an Ethernet level connected, in theory, to the same Ethernet segment, regardless of whether each of them is physically linked to a separate network.

Using a local bridge makes it possible to easily construct a remote-access VPN and site-to-site VPN. For details, please refer to 10.4 Build a Generic Remote Access VPN, 10.5 Build a LAN-to-LAN VPN (Using L2 Bridge) and 10.6 Build a LAN-to-LAN VPN (Using L3 IP Routing).

Local Bridge function.

3.6.2 Local Bridge Settings & Operation

Authority Required to Create a Local Bridge

A local bridge is defined by designating a combination of a network adapter (Ethernet adapter) physically connected to a VPN Server or VPN Bridge and a Virtual Hub. The creation of a new local bridge or the removal of an existing local bridge can only be carried out by the entire VPN Server Administrator. A Virtual Hub Administrator cannot arbitrarily create a local bridge even if it is for their Virtual Hub.

Local Bridge Operations

Once a local bridge is defined, it is possible to send and receive Ethernet packets between the designated Virtual Hub and physical network adapter. The local bridge function automatically terminates when the designated Virtual Hub name does not exist or when the physical network adapter does not exist or has been disabled by the operating system. However, it restarts automatically once the cause of the termination is eliminated.

Creating a New Local Bridge

To define a new local bridge, click the [Local Bridge Settings] button in the VPN Server Manager. This displays the [Local Bridge Settings] dialog box, so select the Virtual Hub to be locally bridged from the [Virtual Hub] dropdown box and the name of the network adapter to bridge to said hub from the [network adapter] box, then click the [Add Local Bridge] button.

The same task can be carried out using the vpncmd utility's **[BridgeDeviceList]** and **[BridgeCreate]** commands.

The Virtual Hub name should be designated when creating a new local bridge, but even if a non-existent Virtual Hub name or an offline Virtual Hub is designated, the local bridge is correctly registered without an error occurring. However, the local bridge will remain in [Offline] status until the Virtual Hub with that name starts running.

Multiple local bridges can be created, although it is not possible to register the same Virtual Hub/ physical network adapter combination more than once.

3-6-2.png

Local bridge settings window.

Local Bridge Status

There are three types of local bridge status as follows.

- **Operating**
  The local bridge is functioning normally and Ethernet frames are being transceived between the Virtual Hub and the physical network adapter.
- **Error**
  An error occurs as a result of the request to the operating system to access the physical network adapter, such as a "device does not exist" error.
- **Offline**
  The Virtual Hub designated as the local bridge does not exist or is offline.

Local Bridging with a Virtual Network Adapter

When a VPN Client is installed on the computer on which the VPN Server or VPN Bridge is installed and a Virtual Network Adapter is registered on the system, this Virtual Network Adapter should appear in the physical network adapter list. In this case it is technically possible to configure a local bridge between the Virtual Hub and the Virtual Network Adapter, although there are almost no benefits to such a configuration from a practical perspective.

3.6.3 Preparing the Local Bridge network adapter

Adding a New Physical Network Adapter for use in a Local Bridge

Establishing a local bridge connection between a Virtual Hub and a physical network adapter enables the Virtual Hub, as well as VPN Clients and other Virtual Hubs which are remotely connected to that hub, to communicate directly with the locally bridged physical network as the same segment.

In this case, the physical LAN to be designated as the local bridging destination is often the same one used for regular communication by that VPN Server or VPN Bridge (i.e. for VPN communication with other VPN software). For example, when wishing to set up a VPN Bridge internally such as on an in-house LAN, and perform site-to-site connection via the Internet with a LAN in a separate location, the LAN used by that VPN Bridge to access the Internet and the LAN subject to the bridge connection would be one and the same.

While it is possible to designate the physically communicating network adapter used by the VPN Server or VPN Bridge for VPN communication as the physical network adapter to locally bridge to the physical LAN, the following problems may arise.

- The VPN Server or the VPN Bridge have to separate the frames used for VPN communication such as for cascade connection with another VPN Server, and the frames subject to local bridging, thereby consuming CPU time and slowing communication speed.
- The Ethernet frames inserted into the physical network adapter have to be copied by both the frame buffer to the TCP/IP protocol stack in the OS and the frame buffer required when inserting for local bridging, thereby placing a burden on CPU time and memory and slowing communication speed.

Accordingly, when local bridging with a physical LAN, a physically new LAN should be installed on the computer running the VPN Server or VPN Bridge and used exclusively for local bridging if possible. However, this does not apply when there are no available

PCI slots on the computer or physical installation of an Ethernet port is not possible due to embedded hardware.

3-6-3.png

Preparing the local bridge network adapter.

No Protocol Stack is Used for the Local Bridge Network Adapter

Where there is a network adapter prepared on the computer for use exclusively in local bridging, it is recommended that the TCP/IP protocol and other protocol stacks be disabled on that network adapter to enhance performance. The role of the local bridge network adapter is to release Ethernet frames between the Virtual Hub and the physical LAN, entirely without the need for intervention from the protocol stack of the OS running the Virtual Hub.

In the case of Windows, it is possible to remove all protocols and services from the local bridge network adapter including the TCP/IP protocol and other network protocols, and the Microsoft Network Client file sharing service. To perform this setting, open the network adapter property in the [Network connections] property and deselect all of the protocol and service checkboxes.

3-6-4.png

Removing protocol stacks from local bridge network adapter.

Even when it is not possible to disable protocol stacks on the local bridge network adapter for technical reasons, the TCP/IP protocol settings can be changed so that the network adapter does not obtain IP addresses from the DHCP Server. If this setting is not carried out, the local bridge network adapter automatically receives the assignment of one IP address from the DHCP Server and, as a result, problems arise such as VPN communication becoming unstable due to the collapse of the routing table.

3-6-5.png

Setting a fixed IP address for the Local bridge network adapter.

For Linux and Solaris, it is possible to use the [ifconfig] command to obtain a result equivalent to assigning an IP address of 0.0.0.0 to the local bridge network adapter.

3.6.4 Local Bridge Sessions

When a local bridge is associated with the Virtual Hub, displaying a list of that Virtual Hub's sessions indicates the presence of the local bridge sessions (sessions with the user name "Local Bridge"). Local bridge sessions are virtual sessions created automatically for the Virtual Hub by the VPN Server in order to connect the Virtual Hub and physical network adapter.

3-6-6.png

Local bridge session status window.

3.6.5 Supported Network Adapter Types

Requirements of Local Bridge Network Adapters

The local bridge function is compatible with network adapters satisfying the following criteria.

- Network adapter with a device driver recognizable by the operating system as an Ethernet (IEEE802.3) device.
- Able to send and receive MTU (excluding Ethernet header) of up to 1500 bytes without incident.
- Able to operate in promiscuous mode.
- Has sufficient hardware and device drive performance and FIFO buffer capacity, and able to withstand heavy loads without operating instability due to software or hardware crashes or overheating.

Recommended Network Adapters

In-house testing carried out at SoftEther VPN Project has shown the following network adapters to possess very high performance worthy of recommendation. Please note, however, that other network adapters generally pose no problems for use with a local bridge. We recommend considering a change to one of the following network adapters if the network adapter you are currently using lacks sufficient performance and is unable to function as required during local bridging.

Manufacturer	Product Series	Link Type
Intel	Intel PRO or Gigabit Adapter series	100Base-TX 1000Base-T 1000Base-SX 1000Base-LX 10GBase-SR 10GBase-LR
Broadcom	Broadcom NetXtreme series	100Base-TX 1000Base-T
3Com	3Com series	100Base-TX 1000Base-T

3.6.6 Use of network adapters not supporting Promiscuous Mode

network adapters not supporting Promiscuous Mode

Some network adapters and network adapter drivers may not support promiscuous mode. network adapters which do not support promiscuous mode cannot, in principle, be used for local bridging with the VPN Server / VPN Bridge.

Most network adapters, however, do support promiscuous mode and can be used without any problems.

Below are some typical examples of network adapters which do not support promiscuous mode.

- Wireless LAN (IEEE802.11) network adapters.
- All other network adapters with device drivers incapable of moving to promiscuous mode.

Forced Use of Network Adapters not Supporting Promiscuous Mode

It is possible to coercively use network adapters which do not support promiscuous mode, although this method is not recommended as it gives rise to numerous limitations. This

method should only be used when compelled to use a network adapter which does not support promiscuous mode for local bridging.

In order to perform this setting, it is necessary to open the **[LocalBridgeList]** node in the VPN Server Configuration file after defining the local bridge, then open the local bridge definition entry designating the intended network adapter defined by the name **[LocalBridge0]** or so on, and overwrite **[NoPromiscuousMode]** to **true**. The specific setting is described below.

```
declare LocalBridgeList
{
        declare LocalBridge0
        {
                string DeviceName Intel(R)$20PRO/1000$20MT
                bool FullBroadcastMode false
                string HubName SoftEther$20Network
                bool MonitorMode false
                bool NoPromiscuousMode true
        }
}
```

3.6.7 Tagged VLAN Frames

SoftEther VPN supports the use of tagged VLAN frames. However, this support is dependent upon the type of network adapter and the features of the device driver used for the local bridge. In addition, SoftEther VPN Project does not guarantee the correct handling of the VLAN frames. Bridging a network handling tagged VLAN frames to a Virtual Hub involves the following.

When the Local Bridge Network Adapter Supports Tagged VLAN Frames

Perform the network adapter's device driver settings followed by the relevant tagged VLAN settings. Please refer to your network adapter hardware manual for settings methods.

When the Local Bridge Network Aadapter does not Support Tagged VLAN Frames

When the network adapter hardware does not support tagged VLAN frames, the tagged portion is able to be read by software as part of a normal Ethernet frame even when the tagged VLAN frame is inserted from the network adapter. In this case, the SoftEther VPN virtualizes and encapsulates the Ethernet frame in which this frame is physically

flowing as is and sends its over the VPN. However, all frames including the tagged VLAN frames cannot exceed 1514 bytes including the MAC header.

3.6.8 Outputting all Communication Data in the Virtual Hub to the Network Adapter

Setting the Local Bridge to Monitor Mode

Using a function like the one described in 3.4 Virtual Hub Functions enables users making a VPN connection to a Virtual Hub to receive (intercept) all virtual Ethernet frames flowing within that Virtual Hub. A similar operation can be performed for locally bridged Virtual Network Adapters.

Enabling monitor mode with a local bridging definition results in all Ethernet frames flowing within that Virtual Hub being output from the locally bridged network adapter. Setting up local bridging in monitor mode is not a normal task and may be hazardous from a security perspective and as such, it is not able to be performed from the VPN Server Manager or vpncmd utility as a precaution. To set up local bridging in monitor mode, open the **[LocalBridgeList]** node in the VPN Server Configuration file after defining the local bridge, then open the local bridge definition entry designating the intended network adapter defined by the name **[LocalBridge0]** or so on, and overwrite **[MonitorMode]** to **true**. The specific setting is described below.

```
declare LocalBridgeList
{
        declare LocalBridge0
        {
                string DeviceName Intel(R)$20PRO/1000$20MT
                bool FullBroadcastMode false
                string HubName SoftEther$20Network
                bool MonitorMode true
                bool NoPromiscuousMode false
        }
}
```

Connecting a separate device to the LAN port of a network adapter set up in monitor mode enables that device to intercept all packets flowing over that the Virtual Hub. As is the case in monitoring mode (see 3.4 Virtual Hub Functions), packets cannot be transmitted within the virtual LAN.

Using a Network Adapter in Monitor Mode

By connecting external hardware to capture and log all Ethernet frames flowing over the network and a security device such as IDS or IDP to the network adapter locally bridged to the Virtual Hub in monitor mode, it is possible to monitor the contents of all communication flowing within a Virtual Hub.

3-6-7.png

This figure shows a normal VPN session in monitor mode, but network adapters in this mode are able to physically receive all Ethernet frames within the Virtual Hub in the same way as this System Administrator.

When the number of virtual Ethernet frames flowing through virtual Hub has lacked a case and the space capacity of the frame buffer that are beyond the processing capacity of a computer and neighboring devices, there is the case that the SoftEther VPN software cancels the frame, and is going to keep stability of the whole system. Therefore, depending on the situation, there is the case that cannot receive all frames.

3.6.9 Using Tap Devices

Rather than designating an existing physical network adapter as the local bridge destination network device, the Linux version VPN Server / VPN Bridge allow the creation of a new tap device and bridging to that device. In this case the Universal TUN/ TAP device needs to be embedded in the kernel and accessible as a /dev/net/tun file.

The tap device generated by this function acts as a Virtual Network Adapter directly connected to the Virtual Hub. The tap device should only be used when it has sufficiently advanced knowledge of the virtual network.

Use the [ifconfig] command to display a registered tap device and perform its IP address and other settings. The tap device name is recognized as a network interface in the Linux kernel starting with the name **"tap_"**.

```
# ifconfig
tap_test Link encap:Ethernet HWaddr 00:AC:11:9F:E2:8F
inet6 addr: fe80::2ac:11ff:fe9f:e28f/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:500
RX bytes:0 (0.0 b) TX bytes:308 (308.0 b)
```

3.6.10 Points to Note when Local Bridging in Windows

The following precautions should be noted when using the local bridge function on a Windows operating system.

- To use the local bridge function it is necessary to launch the VPN Server / VPN Bridge in service mode (Administrators authority is required when launching in user mode).
- The local bridge function is disabled when the VPN Server / VPN Bridge is launched with general user authority.
- For users of old Windows versions (Windows 98 / Windows 98 Second Edition / Windows Millennium Edition / Windows NT 4.0 Workstation / Windows NT 4.0 Server / Windows NT 4.0 Server, Enterprise Edition), WinPcap software must be installed when making a local bridge connection. Using the VPN Server Manager automatically launches the WinPcap installer and performs the installation.
- WinPcap installation is not required for the Windows 2000 and later versions. Instead, the SoftEther VPN performs the necessary local bridge processing by running a local bridge program inside the kernel.
- It is recommended that the computer be rebooted after configuring the local bridge connection when using a network adapter which supports hardware offloading to make the local bridge connection. Although the local bridge operates even without rebooting, communication may become unstable, in which case the computer should be rebooted. A setting to disable hardware offloading is applied upon rebooting, after which operation becomes stable.
- The device name which can be designated in the local bridge destination network adapter list is displayed as the name reported by that device's hardware device driver. When two or more devices of the same type are connected, the second and subsequent device names are distinguished by attaching (2), (3) and so on to the end of their name. While it is generally not defined as to which network adapter name corresponds to which physical network adapter, once the settings have been correctly performed, the order of the devices is typically not altered even after re-launching.

3.6.11 Points to Note when Local Bridging in Linux, FreeBSD, Solaris or Mac OS X

The following precautions should be noted when using the local bridge function on a Linux / UNIX operating system.

- To use the local bridge function it is necessary to launch the VPN Server / VPN Bridge in Service Mode (root authority is required when launching in User Mode).
- The local bridge function is disabled when the VPN Server / VPN Bridge is launched with general user authority.
- It is necessary to embed a socket interface for low level access to the network adapter (also referred to as a packet socket) in the Linux kernel if one is not already present. This is not a problem for most of the recent Linux kernels.
- When communication instability occurs as a result of using a network adapter which supports hardware floating to make the local bridge connection, disable said hardware floating. Please refer to your hardware manual for details.
- Limitations within the Linux or UNIX operating system prevent communication with IP addresses assigned to the network adapter locally bridged from the VPN side (Virtual Hub side). The cause of this restriction lies with OS's internal kernel codes rather than with the SoftEther VPN. When wishing to communicate in any form with a UNIX computer used for local bridging from the VPN side (Virtual Hub side), (for instance, when running both the VPN Server / VPN Bridge service & the HTTP Server service and wishing to grant access to the server service from the VPN side as well), prepare and connect a local bridge network adapter and physically connect both it and the existing network adapter to the same segment (as explained in **3.6 Local Bridges**, it is recommended to prepare a network adapter for exclusive use in local bridging for this and other situations).
- While Windows enables device names to be designated for all network adapter names, in UNIX, network device names such as eth0, eth1 and so on are designated. These device names can be obtained using the **[ifconfig -a]** command.