2. Layer-2 Ethernet-based VPN

2.1. Full Ethernet Virtualization

The key concept of the method of realizing VPN by SoftEther VPN is the full virtualization of Ethernet segments, layer-2 Ethernet switches and Ethernet adapters. In order to establish good VPN network, SoftEther VPN virtualizes Ethernet, which is widely used all over the World.

To understand the advantage of SoftEther VPN, please read the basis knowledge about Ethernet and it's limitation at first. And you will understand how SoftEther VPN resolves it in order to establish private communications between remote sites.

SoftEther VPN encapsulates Ethernet over HTTPS to transmit frames over Internet.

Ethernet is the Standard of LAN

As you know, Ethernet is a technology for using on LANs (Local Area Networks). Ethernet is very convenient and reliable standard in order to connect several computers mutual. With Ethernet, you can enjoy many network programs such as file sharing, printer sharing and accessing amounts of data on RDBMS (Relational Database Management Systems). Today there are no companies who have no LANs with Ethernet in their office.

Standard formation of Ethernet-using network is hub-and-spoke model. There are hubs (as know as Ethernet switches) central and each computers has a cable to the hub. Then

all computers can communicate mutually. The advantage of Ethernet is that you can understand the model very easily. This is a certain reason why Ethernet has been spread the world. Computers and hubs connected in order to enable them free communication consists an Ethernet Segment. It is also called as "Layer-2 Segment" or "Broadcast Domain" .

Ethernet has a Limit on Distance

But you cannot use Ethernet beyond the walls of office or building. In normal condition, you know you can connect computers mutual only in a room or a building. But you cannot make a computer on the site-A to communicate with another computer on the site-B with only Ethernet. The reason why you cannot is that Ethernet must need wired Ethernet network cables to connect between devices. Network cables can be laid only in the building. You cannot lay the cable between the separated two or more buildings, because you cannot place any cables across the road. Of course there are other limitations of Ethernet, for example maximum distance of cable. And these limitations cannot be solved by using other physical media as extensions of Ethernet lately invented, such as Wi-Fi and optical cables.

"Ethernet" is totally different to "Internet". The Internet is the interconnected network of a lot of private networks and ISPs mutually. It is certain that we can pay ISPs inexpensive money to enjoy the connection to the Internet. You can connect both offices of Tokyo and Beijing to the Internet. And computers on each office can now access to the Internet. But still you cannot enjoy any software written for LAN internal use between two sites, even if there are both two Internet connections. What you can do are only as follows; for example, to exchange emails, to use Skype and Messenger software in order to exchange short messages or voices, and to access the same groupware to exchange schedules and so on. You can do these things if you have two sites and both sites have each Internet connection. But you cannot enjoy any other profits which are came from software for LAN, for example file sharing, print sharing, database protocols, CRMs, ERPs, and other applications which are developed for specified purposes. Again, Ethernet is not Internet. Internet cannot become alternative to Ethernet. Even if you connect both sites to the Internet, two sites don't construct the single Ethernet segment at all. If you want to use application for LAN, you must construct a single Ethernet segment to surround every your computers.

Extend Your Ethernet Segment beyond any Distance by SoftEther VPN

SoftEther VPN is a tool to establish an Ethernet segment between two or more remote places, using the tunneling technology via the Internet.

You understood about the advantage of Ethernet and the difference between Ethernet and Internet, and also the limitation which is came from the difference. But you probably wonder if an Ethernet segment can be extended to other sites beyond any distance, for

example beyond roadways between two buildings. If it could, it might be possible to use any applications for purpose of LAN use between two or mote sites.

You can find that some telecom companies have provided such a distance-communication service as "Wide Area Ethernet Service" . You can establish the single Ethernet segment between two or more buildings with such services. But such dedicated line services costs much more than the cost of Internet (for example, 100 more times). And you cannot use this solution absolutely if your regions of at least one of your sites are not supported as service area.

Then you need any other solution. Fortunately, the cost to connect a site to the Internet is very cheap today. You can keep connection two or more sites to the Internet easily. Then if you install SoftEther VPN on each site, you can connect each segment of all sites mutually in order to build a single Ethernet segment. Before you establish the VPN tunnel, every site's network has its own Ethernet segment. Every segment is separated completely and mutually. After the VPN tunnel has been established, however, every segment is combined together and then unites to the single segment. After that, you can run any protocols between every remote site, crossing the physical distance. You can use this technique to both purposes of remote accessing and site-to-site connections.

Virtualization of Ethernet Switches, Adapters and Cables

To fulfill the above purpose, SoftEther VPN virtualizes Ethernet switches, cables and adapters.

Ethernet switch, as known as Hub or Layer-2 Switch, is a device to exchange packets between Ethernet hosts. A switch has a FDB (Forwarding Database) inside itself in order to determine the appropriate destination port of outgoing for a packet which came from incoming port. This behavior is called as "Switching" as a major function of switches.

Ethernet network cable, as known as Cat5e or Cat6 Copper Cable, is a device to connect between Ethernet devices, such as Ethernet switches and Ethernet adapters. Ethernet Adapters are also called "NIC (Network Interface Card)" and placed on computer. Nowadays a computer has an Ethernet adapter on its board. It is called "Onboard" . You know that you can insert more adapters on PCI or USB bus of the computer if you need.

SoftEther VPN virtualizes Ethernet switch and emulate it. The virtual Ethernet switch is called "Virtual Hub" in the software. And SoftEther VPN virtualizes Ethernet adapter and emulate it. The virtual Ethernet adapter is called "Virtual Network Adapter" in the software. SoftEther VPN also virtualizes Ethernet network cable and emulates it. The virtual Ethernet network cable is called "VPN Session" or "VPN Tunnel" in the software.

Above three elements are important to understand SoftEther VPN. For example, when you want to build a remote access VPN in order to accept VPN connections from remote site to the company LAN, you will create a Virtual Hub on the VPN Server in the

company LAN. That Virtual Hub constructs an Ethernet segment. And you connect both the Virtual Hub and the physical network adapter on the server computer mutually. Then both segments of the Virtual Hub and the existing physical LAN are now combined and united as the single Ethernet segment. And you will install VPN Client software on the remote client PC, for instance, laptop PC. VPN Client software can create a Virtual Network Adapter on the client PC. You will create a connection setting in order to connect the VPN Client to the Virtual Hub on the VPN Server in your company. When you ignite the connection, a new VPN Session will be established between the Virtual Network Adapter and the Virtual Hub. This situation is very similar that you attach the one-side of an Ethernet cable to the physical Hub and the other-side to the physical Ethernet adapter on the computer. Not only similar, but it is also exactly same in the logical aspect of behavior of Ethernet. After you established the VPN connection, you can send and receive any protocols suitable for Ethernet. All packets are transmitted on the virtual cable, as called as VPN Session or VPN Tunnel.

After once you understood the architecture of realizing method of SoftEther VPN, you will be able to understand that the potential possibilities for range of use of SoftEther VPN is almost infinite. The above example show you the way to construct a remote access VPN, but you can apply this way to make any other form of VPN. It is very easy to build a site-to-site VPN. Only difference to remote access VPN is the opposite ends from the VPN Server is not a VPN Client but a VPN Bridge.

A Virtual Hub is a software-implemented Ethernet Switch. It exchanges packets between devices.

ss2.1_1.jpg

You can create a lot of Virtual Hubs on SoftEther VPN Server. Each Virtual Hub is isolated to others.

ss2.1_2.jpg

You can create a lot of Virtual Network Adapter on the client-side PC with SoftEther VPN Client.
Each Virtual Network Adapter is regarded as a "real" Ethernet adapter as if it is

attached on the PC.

2.2. Transmit Any Ethernet Packets via VPN

Since SoftEther VPN tunnels the Internet and establish a VPN Session between remote sites with full capabilities to transmit any Ethernet packets, SoftEther VPN has unlimited protocol transparency as exact same as physical Ethernet segments. As you know, there are many of protocols which can be used on Ethernet. For example, IPv4 (TCP, UDP, ICMP, ESP, GRE etc.), IPv6 (the next generation of IP), NetBEUI, IPX/SPX, PPPoE, RIP, STP and so on. All protocols can be transmitted on the tunnel by SoftEther VPN.

Legacy VPNs, such as L2TP, IPsec or PPTP, can transmit virtually only IPv4. Because these VPN protocols can carry only the upper layer of equal or more than layer-3. Contrariwise, SoftEther VPN can carry any packets which are equal or more than layer-2.

You can derive a benefit from this advantage. You can use any legacy and latest protocols within the VPN session of SoftEther VPN, not possible for any other VPNs. If your company uses some specified protocol for controlling a manufacturing machine, you can use it on the SoftEther VPN Session. No modifications on the software are needed to use such a protocol on the layer-2 VPN.

Unlike legacy IPsec or PPTP VPNs, SoftEther VPN Protocol can carry any kinds of packets.
You can enjoy any applications which are "local-network oriented" without no modifications.

2.3. Benefits of Layer-2 VPN for Remote Access Users

Almost all legacy VPN products with IPsec, PPTP or L2TP need to define a virtual IP subnet inside the VPN server, because these protocols are virtually layer-3 VPN protocols. If your company's existing LAN has an IP subnet as 192.168.3.0/24, you cannot connect the remote PC directly to that IP subnet. At first you have to create a virtual IP subnet, for example 192.168.100.0/24 on the VPN server. And then you can

connect VPN Client PC to the VPN server. And the VPN server is always processing the routing between two different IP subnets. This method of remote accessing VPN is complicated because sometimes the network administrator has to design and modify the routing policy of the LAN. It might cause a troublesome. For example, many protocols and applications are designed on the assumption that any broadcast IP packets can be passed between nodes. In the legacy VPN's situation, such applications cannot work normally. The good instance is the file sharing protocol of Windows, everyone knows about it. This protocol, as knows as CIFS (Common Internet File System) or SMB (Server Message Block), is virtually depended on the method of resolving the computer name by broadcast packets of IP. No broadcast IP packets can be broadcasted beyond the differences of IP subnets. So such a mechanism for browsing the computer by Windows doesn't work well on the legacy VPNs. You need more costs to patch this problem, such as building WINS or DNS server for Windows name browsing. Moreover than mentioned above, you might have a trouble to use any protocols from remotely since legacy VPN protocols are lack of transparency of any kind of packets. Some legacy VPN devices, such as Cisco's, patched this problem with attempting to adopt Proxy-ARP mechanism. But it is a rare case and lack of compatibilities for any situation.

SoftEther VPN gives you a benefit that you can transmit any packets between the VPN Client PC and the VPN Server's LAN segments. You create a layer-2 VPN Session between the VPN Client and the VPN Server, and you will take no trouble about using any applications which have been designed for LAN inside use. Because the circumstances of such a VPN Session are exactly same in the logical layer as the situation that you connect the Ethernet adapter on the laptop PC to a port of the Ethernet switch in the company. It can be said that SoftEther VPN realizes a virtual and very long network cable over the Internet. Because of this characteristic you can use your laptop PC from anywhere and anytime as exactly same as you are taking a seat just in front of the company's desk.

2.3.jpg

SoftEther VPN Client behaves as same as the computer is physically connected to the local area network.

For example, unlike layer-3 based VPNs, Windows Client PC in your home will enumerate computers on the office network.

2.4. Benefits of Layer-2 VPN between Site-to-Site

Not only building a remote accessing VPN, but you can also establish the reliable link between or more sites. It is called "Site-to-Site VPN" . You can use such a link as a dedicated line, even if the physical underlay layer is a cheap Internet connection provided by ISPs. It is no matter of kinds of connection media to the Internet. Once you have established a VPN link between sites, after that, everyone on both sites can transmit any kinds of packets from a side to other sides.

With legacy VPNs such as IPsec or L2TP, you cannot connect two or more sites by layer-2 tunnel. You have to establish layer-3 tunnel due to limitation of such legacy VPN protocols. Then almost same problems always occur as similar to the situation of creating remote accessing VPN with legacies. The IP subnets must be different between each site. For example, Tokyo has to have 192.168.1.0/24, Beijing has to have 192.168.2.0/24, and Shanghai has to have 192.168.3.0/24. You cannot use any protocols which are depended on the broadcast packet, such as name browsing functions of Windows File Sharing implemented on SMB or CIFS. And you cannot use any non-IP protocols, neither. Not only such limitations, but also you have to design to separate IP subnets on each site. An IP subnet of a site cannot be overlapped to other sites. If you are a small company, it might become extra costs because such a designation of IP subnetting needs an adequate faculty to be conducted to prevent any trouble. And if you are a big company and want to connect many sites mutually, it will be a nightmare situation. You have to manage a lot of subnets with an effort to keep preventing to collide against any other subnets. Legacy VPN has requires us special pain to satisfy the demands of legacy VPNs if you want to adopt it for creating site-to-site VPN.

But if you use SoftEther VPN to link up the site-to-site VPN, it is very easy and reduce your effort to coop against several troublesome which might be occur when you use legacy VPNs. As mentioned former, the link between sites are always emulating as the Ethernet network cable of long distance. You have no need to design anything special to fulfill your simple demand that you want to connect remote sites. You can simply think and design your network with VPN, as exactly same as you design traditional Ethernet network topology with hub-and-spoke mode. All your knowledge known by you as common sense can be work in the VPN Session consists of SoftEther VPN. You can imagine the situation that there are three sites; Tokyo, Beijing and Shanghai, and every site have an Ethernet switch. You can connect Ethernet network cables between them. Then every computer of each sites take an access to any computer of other sites. Establishing site-to-site VPN is very simple as that example. You can connect virtual VPN Sessions between sites, instead of physical Ethernet network cables. You will enjoy VPN communication between sites, without any modification of any settings of the server computers and so on. All kinds of server services and inter-client-PC-

communication applications will work well, with no difference between inside the same site and beyond the distance.

2.4.jpg

You can treat a Site-to-Site VPN as "very-long Ethernet cable between remote sites".

2.5. Virtual Hubs, Cascades and Local Bridges

SoftEther VPN Server and SoftEther VPN Bridge has the concepts of Virtual Hubs, Cascades and Local Bridges.

Virtual Hub

A Virtual Hub is an entity on the VPN Server and VPN Bridge which emulates a behavior of Ethernet switches in the real world. A Virtual Hub has its own FDB (Forwarding Database). Many of VPN Sessions will be connected to a Virtual Hub. Then every endpoint of VPN sessions can send and receive any Ethernet packets.

Any Virtual Hub can accept connections from both of VPN Clients and other Virtual Hubs. VPN Client is a software program which is running on the user's client-endpoint PC.

2.1.2.jpg

Virtual Hub has many connected VPN sessions and Forwarding Database (FDB) to learn MAC addresses.

ss2.5_1.jpg

Like physical Ethernet Switch products, Virtual Hub learns MAC addresses of each VPN sessions automatically.

Cascade Connection

On SoftEther VPN Server, you can create multiple Virtual Hubs as you wish (up to 4096). Every Virtual Hub constructs own Ethernet segment and totally separated to other Hubs even they are located on the same VPN Server computer. It is similar to a situation that there are some Ethernet switches on the same desk. Each Ethernet switch is not connected mutually so each Ethernet segment is independent. But if you connect an Ethernet network cable between any ports of every switch, Ethernet segments will be united as you did. As same as that, you can create a link between virtual Hubs on the same computer if necessary. It is called "Cascade Connection" or simply "Cascade" . Cascade is a popular technical term of Ethernet. If a cascade connection is established, then every Ethernet segment on each Virtual Hub is now united as a single segment.

And you can also create a cascade connection between remote VPN Servers. So if you have VPN Server on both side of Tokyo and Beijing, and each VPN Server has a Virtual Hub, then you can establish a cascade connection between two Hubs. Then each Hub is now united as a single segment. A computer which is belonging to Tokyo's Hub is now able to communicate to another computer which is belonging to Beijing's Hub.

You can also define multiple cascade connections on a Virtual Hub.

ss2.5_2.jpg

Define a cascade connection with GUI. It is very easy.

Local Bridge

Only the situation of existences of Virtual Hubs, cascades and VPN Clients is not so convenient, because every computers have to be installed VPN Client each and have to connect to a Virtual Hub in order to make a communication between computers mutually. In that usage, any computers which are outside of the Virtual Hub's segment cannot participate in the communication circle. It is possible but not good for company use of VPN.

The Local Bridge function can be used to extend an Ethernet segment in Virtual Hubs to the outside physical Ethernet segments.

Local Bridge is a technology to unite the virtual Ethernet segment and the physical Ethernet segment. You company has an existing Ethernet segment on the psychical Ethernet switch. To realize a usable remote either accessing VPN or site-to-site VPN, you have to connect between the Ethernet segment on the Virtual Hub and the Ethernet segment on the physical Ethernet switch somehow. The answer is to use Local Bridge. Local Bridge can be created for a purpose to make two segments to exchange Ethernet packets mutually. If you have a Local Bridge between the physical Ethernet segment and the Virtual Hub's segment, then all computers who are connecting on the Virtual Hub can communicate to all computers on the physical existing network. Practically, Local Bridges must be applied between a Virtual Hub and an Ethernet network adapter which is connected to the physical Ethernet switch. So in order to use Local Bridge you need dedicated physical Ethernet adapter. (In fact, the Ethernet adapter can be shared with other purpose, such as transmitting packets physically to the Internet in order to keep the VPN Session, but it is highly recommended to prepare a dedicated one due to performance matter.)

Therefore, Local Bridge is a key function to fulfill the demands of creating both of remote accessing VPN and site-to-site VPN.

2.5.1.jpg

Local Bridge is a function to link between Virtual Segments and Physical Segments.

2.5.2.jpg

Combination of Local Bridge and Cascade Connection can build widely-spreaded Site-to-Site VPNs.
You can bind a lot of branches around the world.

ss2.5_3.jpg

To define a local bridge, select a Virtual Hub and a Physical Ethernet Adapter, and just click a button.

2.6. IEEE802.1Q VLAN Supports

Some large-scale enterprises adopt IEEE802.1Q VLAN for separating IP subnets on the single physical Ethernet equipment in order to reduce both administration costs and cable-wiring costs. It can also reduce the necessary number of ports on the each Ethernet switch.

SoftEther VPN is a layer-2 VPN technology, and it fully supports IEEE802.1Q Tagged VLAN packet transmitting. It is very useful feature if your company has many Ethernet segments on each site. By IEEE802.1Q VLAN technology, all Ethernet packets from each segment can be multiplexed by attaching VLAN tag on each packet. SoftEther VPN is capable to transmit any tagged VLAN packets in the case of site-to-site VPN. Thus your company can extend the tagged VLAN segments to other sites.

And as an additional function related on the VLAN transmission support, SoftEther VPN has also a function to insert and remove a VLAN tag on the packet automatically. It can be configured on each user object's security policy individually. So you can make a policy such as user-A can access to only VLAN 123, and user-B can access to only VLAN 456. All raw packets from a user will be added a tag of specified VLAN ID transparently, and all tagged toward to a user will filtered and tag will be removed transparently.

2.6.jpg

Virtual Hub can insert or remove IEEE802.1Q VLAN tag. VLAN settings is per user or group.

ss2.6_1.jpg

Define a "VLAN ID (IEEE802.1Q)" security policy per a user or per a group.

ss2.6_2.jpg

Virtual Hub learns both MAC addresses and VLAN IDs association.

2.7. Virtual Layer-3 Switch Function

You can create not only virtual layer-2 switch (Virtual Hub) on the VPN Server, but also you can create Virtual Layer-3 Switch on the VPN Server. Layer-3 switch is an entity acts with behavior same as IP router. Current version of SoftEther VPN supports only IPv4 protocol on any Layer-3 Switches. Same as Virtual Hubs, you can create multiple Virtual Layer-3 Switches on a VPN Server.

A Virtual Layer-3 Switch has multiple virtual interfaces and each interface can be connected to the Virtual Hubs on the same VPN Server. Then you can organize IPv4 subnet routing for inter-Virtual Hubs. If you want to create separated several Virtual Hubs for any reason, for example security or management convenience, but you want to enable them to be routed by IPv4 traditional routing mechanisms, it is a simple way to create Virtual Layer-3 Switches to fulfill your demand rather than placing the physical IP routers or expensive layer-3 switch products on the physical network.

A Virtual Layer-3 Switch can have a static routing table with unlimited lines. People, who have knowledge to configure IP routing design on any IP router products or layer-3 switching products, can easily configure and exploit it for any purpose.

Virtual Layer-3 Switch is a software-based IP router.

ss2.7.jpg

You can create unlimited number of Virtual Layer-3 Switches.
You can define unlimited number of Virtual Interfaces and Routing Table Entries.