

Outline of Master Thesis,
January 16, 2013.

Design and Implementation of SoftEther VPN

Daiyuu Nobori

*Department of Computer Science,
Graduate School of Systems and Information Engineering,
University of Tsukuba, Japan.*

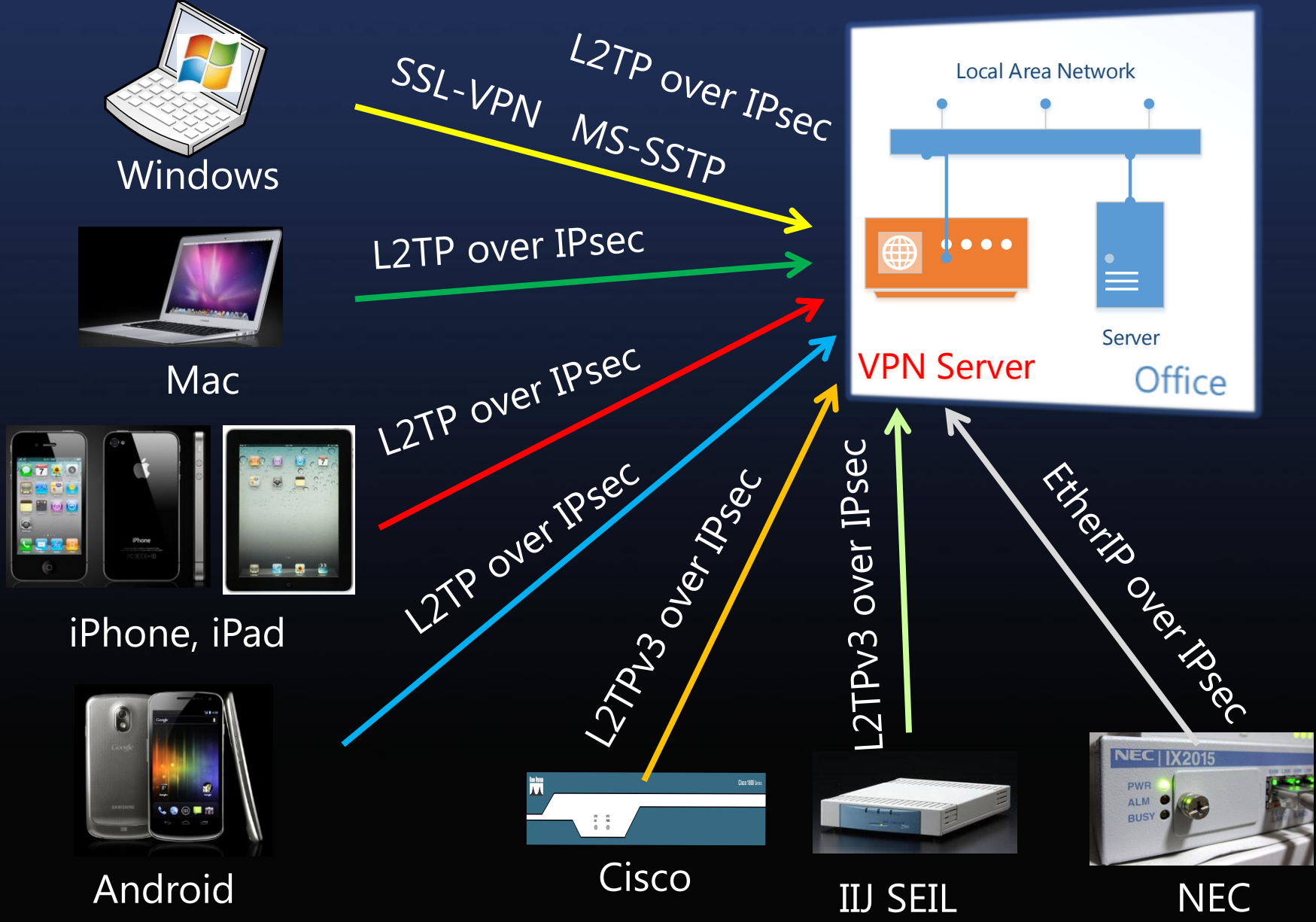
Background: Various VPN Protocols

- VPN Client Devices
 - PCs: Windows, Mac, iOS, Android, ...
 - Routers: Cisco, Juniper, NEC, IIJ, ...
- VPN Protocols
 - SoftEther VPN
 - L2TP/IPsec
 - SSTP
 - OpenVPN
 - L2TPv3/IPsec
 - EtherIP/IPsec
- System Administrators have to prepare multiple VPN Servers for each VPN protocol.



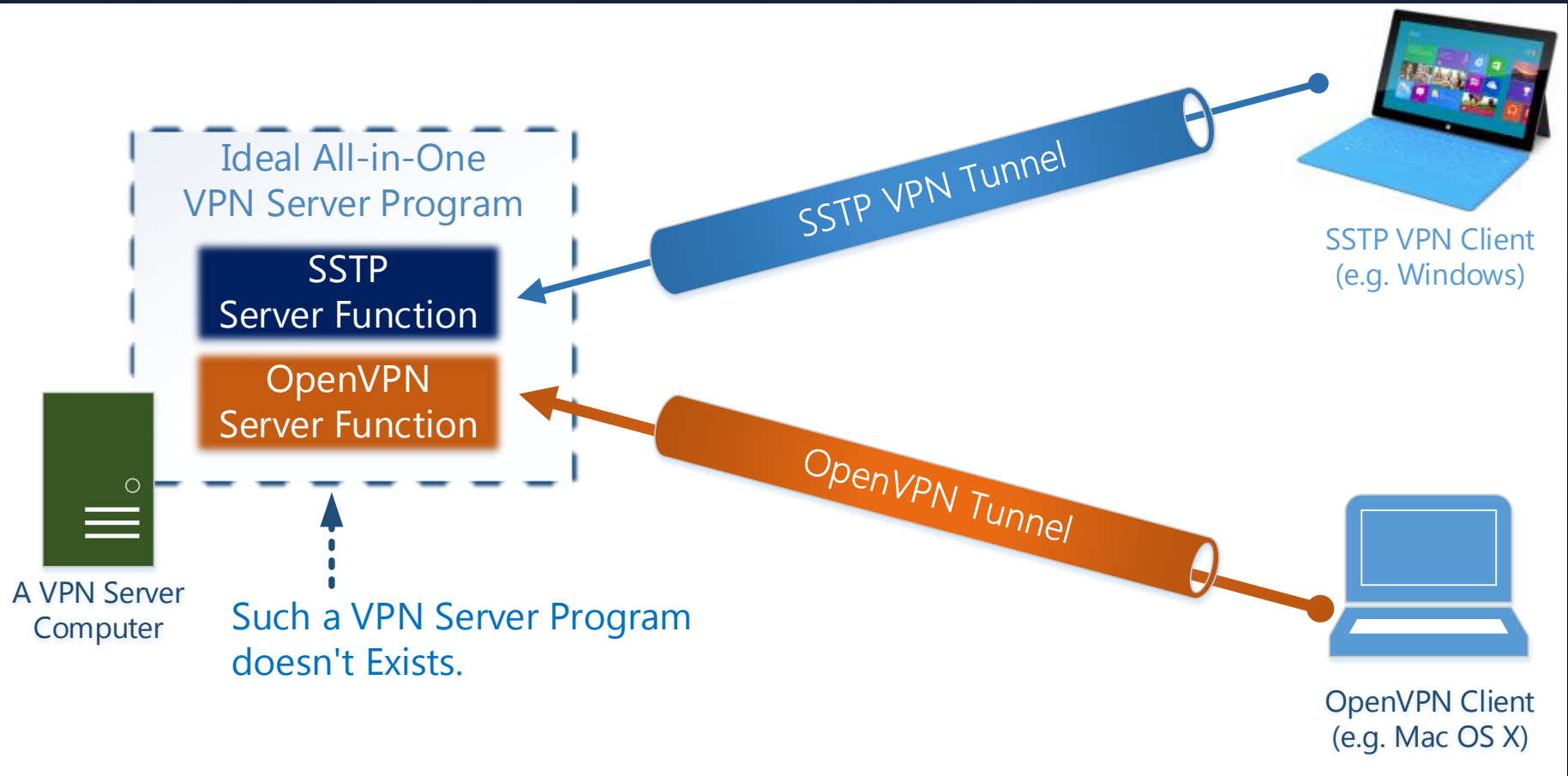
Characteristics of VPN Protocols

	L2TP	SSTP	PPTP	OpenVPN	L2TPv3	EtherIP	SoftEther VPN
Upper Protocol	IP	IP	IP	Ethernet	Ethernet	Ethernet	Ethernet
Transport Protocol	IPsec	HTTPS	GRE	Specific TCP/UDP	IPsec	IPsec	HTTPS
Proxy Support	NO	YES	NO	YES	NO	NO	YES
Restricted FW	Blocked	PASS	Blocked	Blocked	Blocked	Blocked	PASS
Client OS (PC)	Windows Linux Mac	Windows	Windows Linux Mac	Windows Linux Mac	-	FreeBSD	Windows Linux
Client OS (Smartphone)	iOS Android	-	iOS Android	-	-	-	-
Client OS (VPN Routers)	Cisco	-	-	-	Cisco IUI SEIL	NEC IX	-



Various VPN Protocols

Ideal All-in-One VPN Server Program



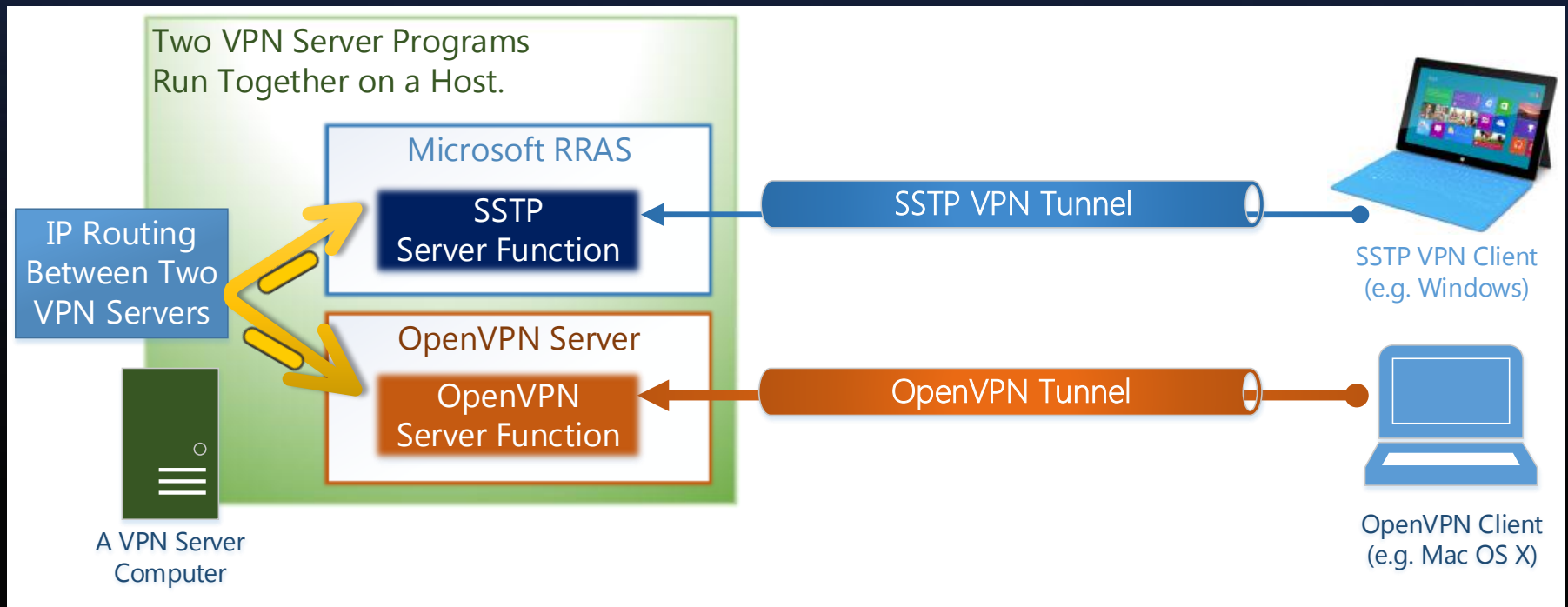
A Problem:

There is No Such an Ideal
VPN Server Program.

Existing VPN Server Programs Compatibles

	L2TP	SSTP	OpenVPN	L2TPv3	EtherIP
Microsoft RRAS	✓	✓	-	-	-
Mac OS X Server	✓	-	-	-	-
OpenVPN	-	-	✓	-	-
Cisco IOS	✓	-	-	✓	-
NEC IX Router OS	-	-	-	-	✓
IJ SEIL Router OS	✓	✓	-	✓	-

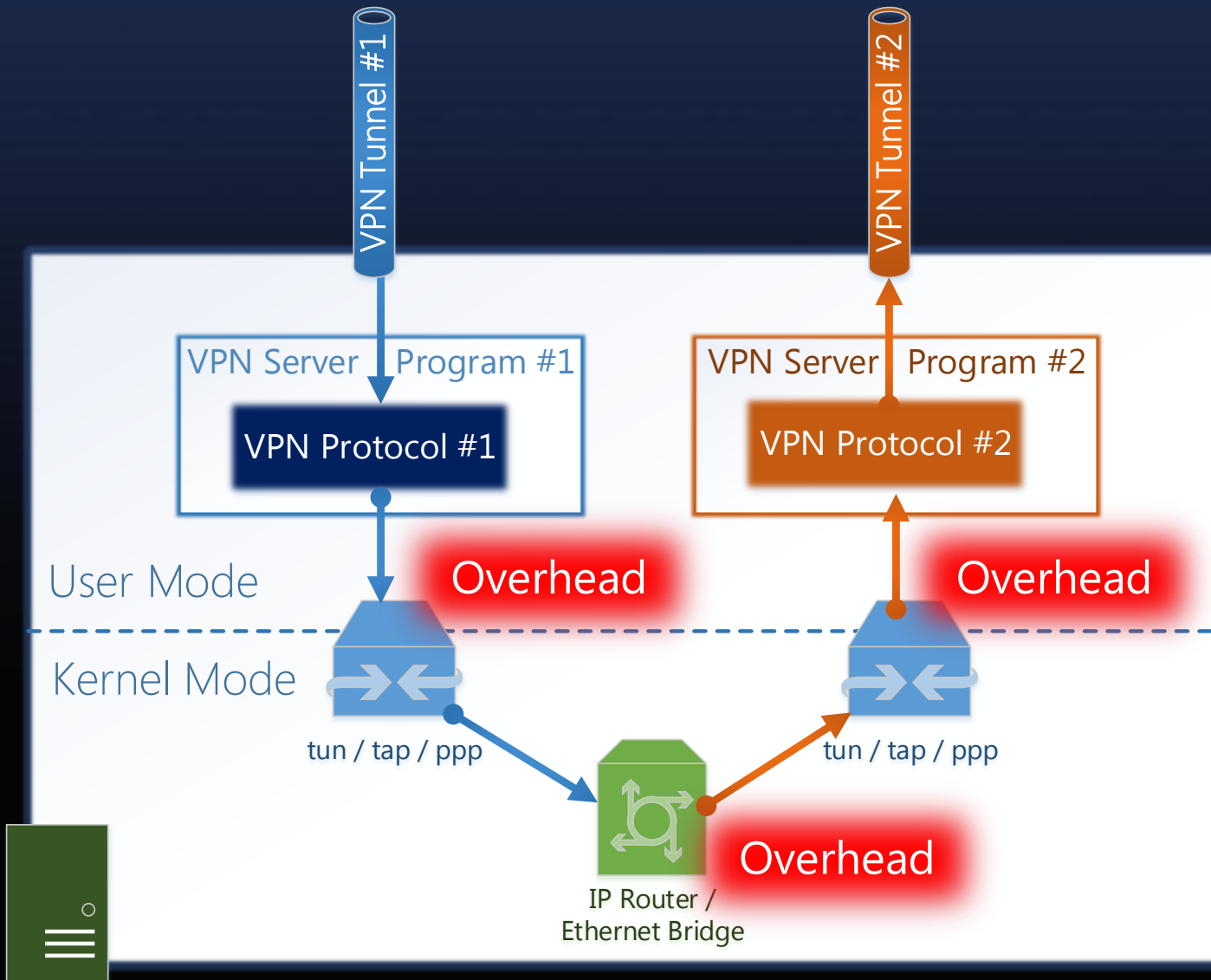
Supporting Multi VPN Protocols by Single VPN Server Computer



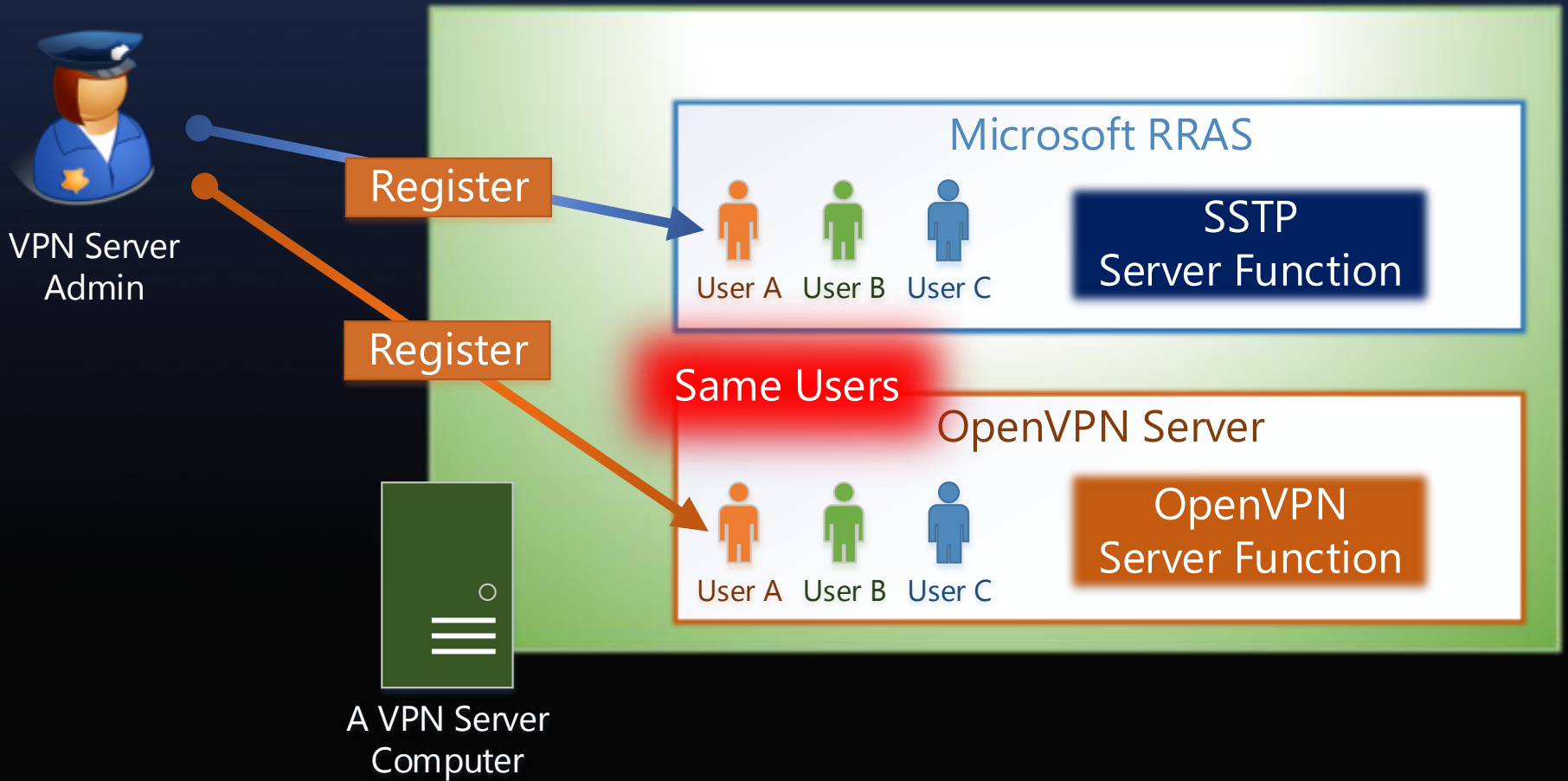
Supporting Multiple VPN Protocols by Single VPN Server

- Overhead Problem
 - Context Switching Costs
 - User-to-Kernel Switching Costs
 - Memory Copying Costs
- Management Problem
 - User Management Tasks
 - Log File Management Tasks
 - Inefficient IP Address Polls

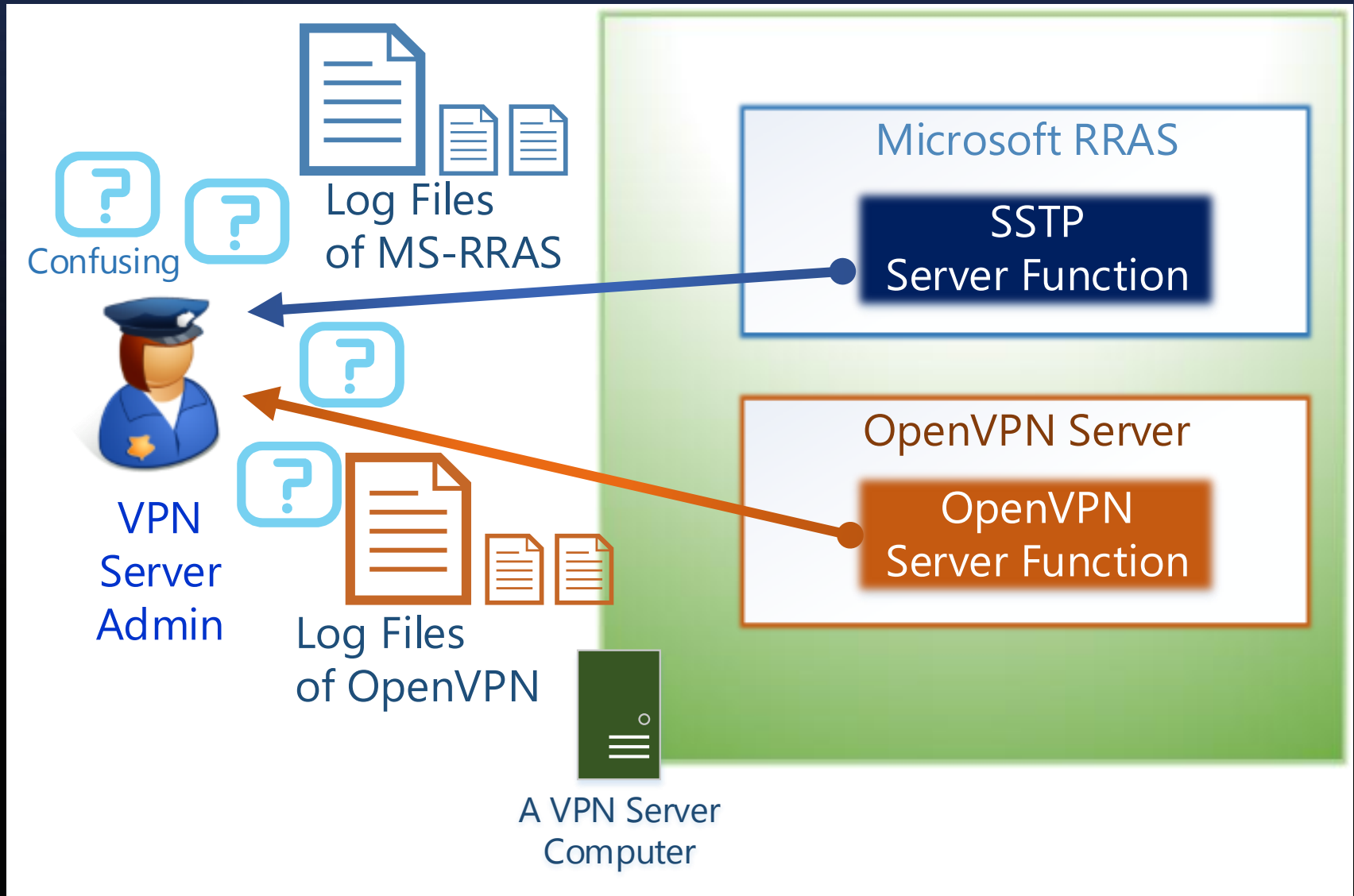
Overhead Problem



Management Problem



Log File Problem



IP Address Pool Duplication Problem

192.168.0.101-
192.168.0.150



Duplicate
IP Address Reserves

192.168.0.151-
192.168.0.200



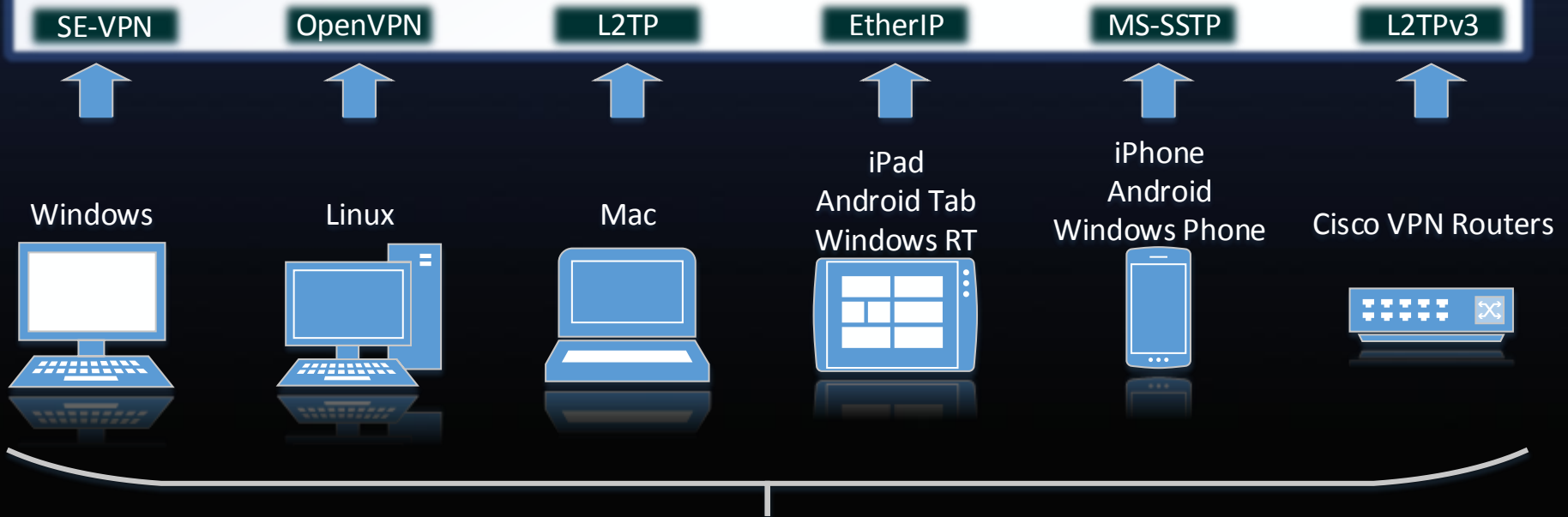
Goal of the Research

	L2TP	SSTP	OpenVPN	L2TPv3	EtherIP	SoftEther VPN
Microsoft RRAS	✓	✓	-	-	-	-
Mac OS X Server	✓	-	-	-	-	-
OpenVPN	-	-	✓	-	-	-
Cisco IOS	✓	-	-	✓	-	-
NEC IX Router OS	-	-	-	-	✓	-
IJ SEIL Router OS	✓	✓	-	✓	-	-
SoftEther VPN	✓	✓	✓	✓	✓	✓

"SoftEther" means Software Ethernet.

SoftEther VPN Server

A high-performance VPN server which supports multiple VPN protocols.



Supports various VPN client devices.

Difficulties of the Research

- 7 VPN protocols by one VPN server
 - Inter-VPN protocol packet exchange
 - Bridges between L2 (Ether) / L3 (IP)
- Management
 - User authentication
 - Dynamic IP address assignment to VPN clients
- Security
 - Security policy / Packet filter
 - Packet log
 - Isolation

How to Support 7 VPN Protocols?

L2 VPN Protocols	L3 VPN Protocols
SoftEther VPN	L2TP/IPsec
OpenVPN (L3)	SSTP/IPsec
EtherIP/IPsec	OpenVPN (L2)
L2TPv3/IPsec	

- Strategy #1

- Separate L2 VPN Ethernet / L3 VPN Router
- Layer-conversions between L2 / L3

Problem: Duplication of Security Implementations, Complicated Codes

- Strategy #2 [adopted]

- Treat all L3 VPN as L2 VPN
- All L3 packets will be descended to L2 Ether frames.

Benefit: Single Security Implementations, Simple Codes

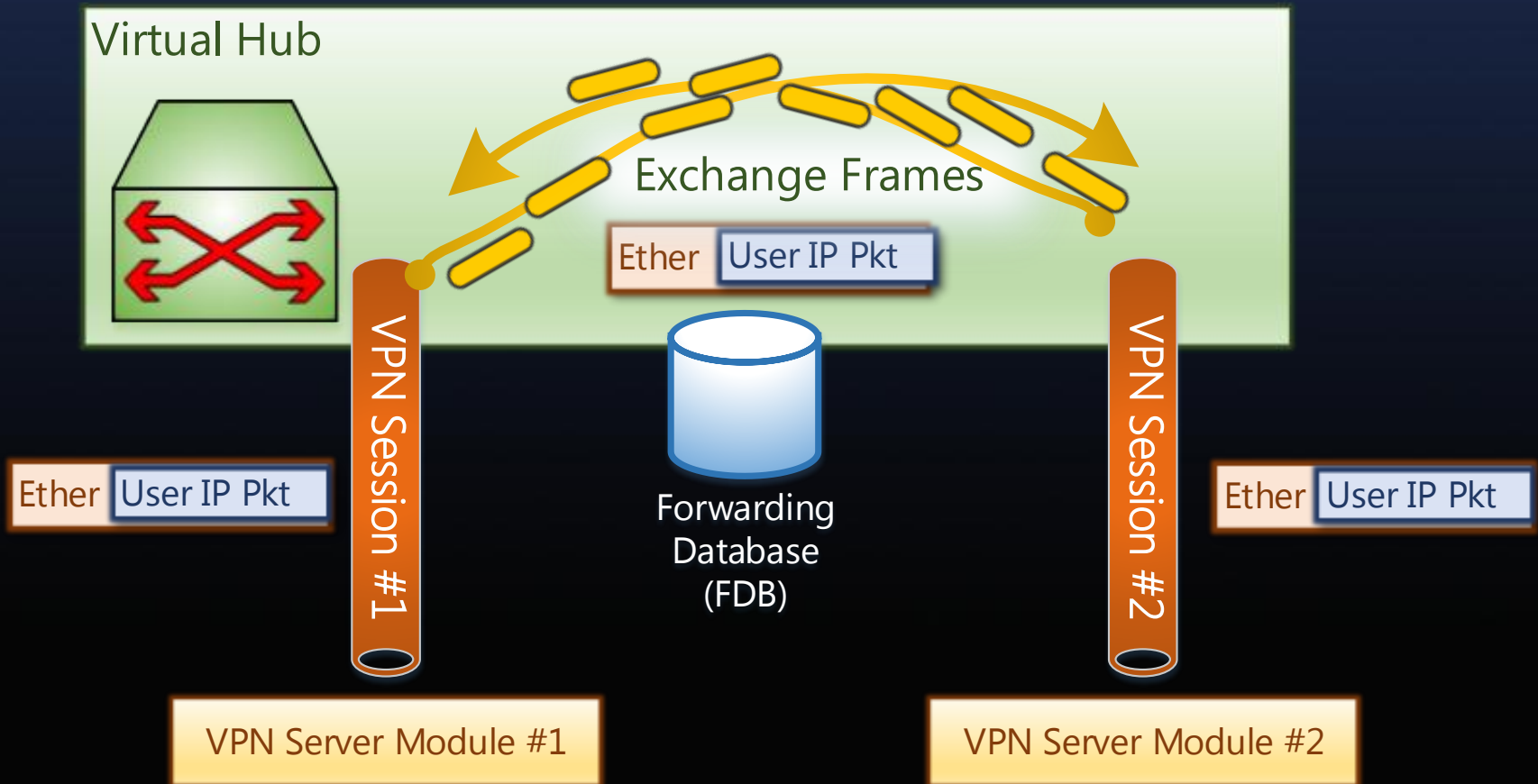
Design #1

- Ethernet (L2) as Common Bus.
 - Virtual Ethernet Switching Hub.
 - Layer conversion for IP-based VPN protocols (L2TP, SSTP, OpenVPN L3).
 - Virtual DHCP Client.

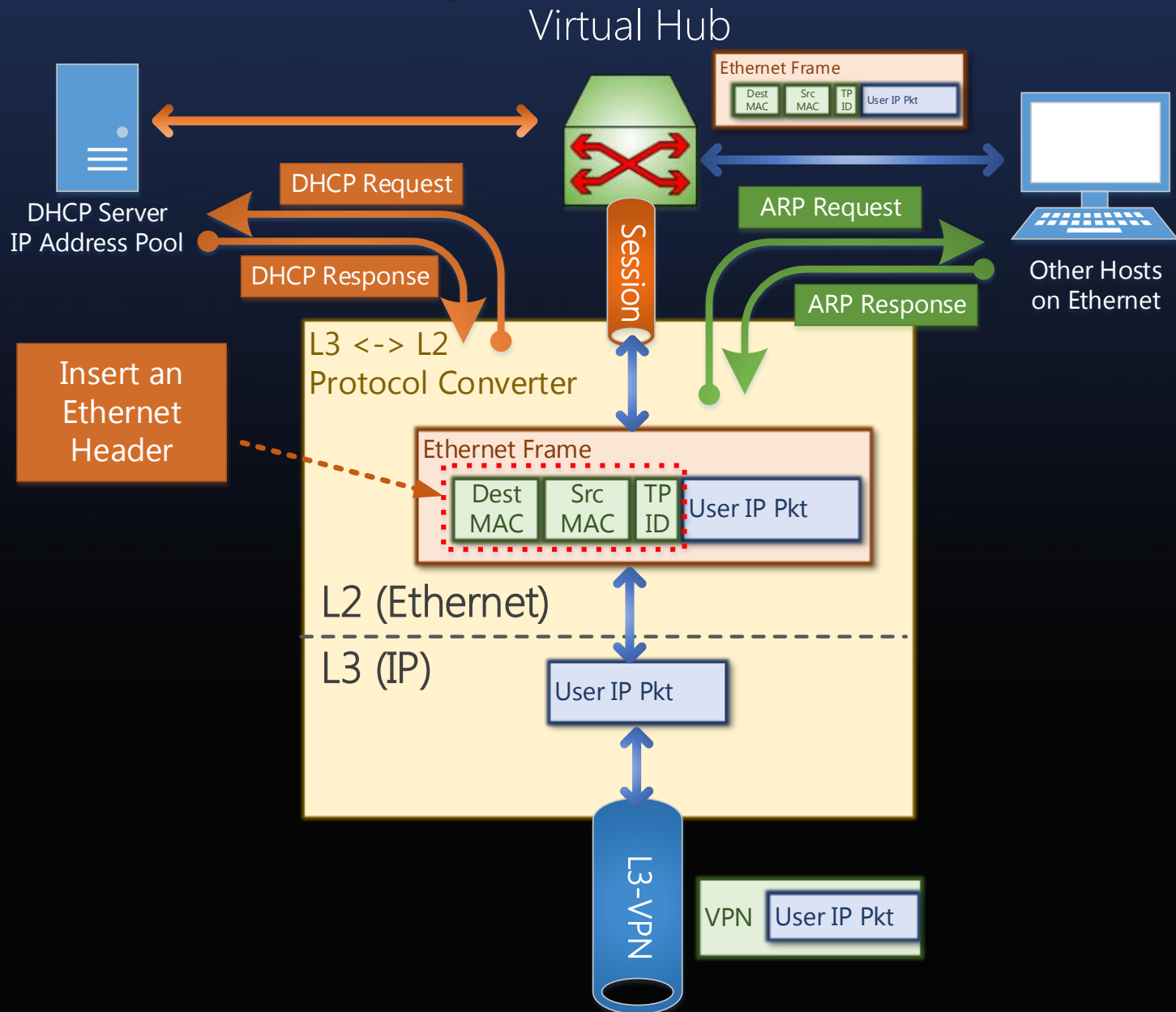
Design #2

- Kernel-mode
 - Difficult to debug
 - Lack of portability
- Multiple User-mode Process
 - Easy to implement
 - Overhead Problem still occurs
- Single User-mode process [adopted]
 - Easy to implement
 - Reduce overhead

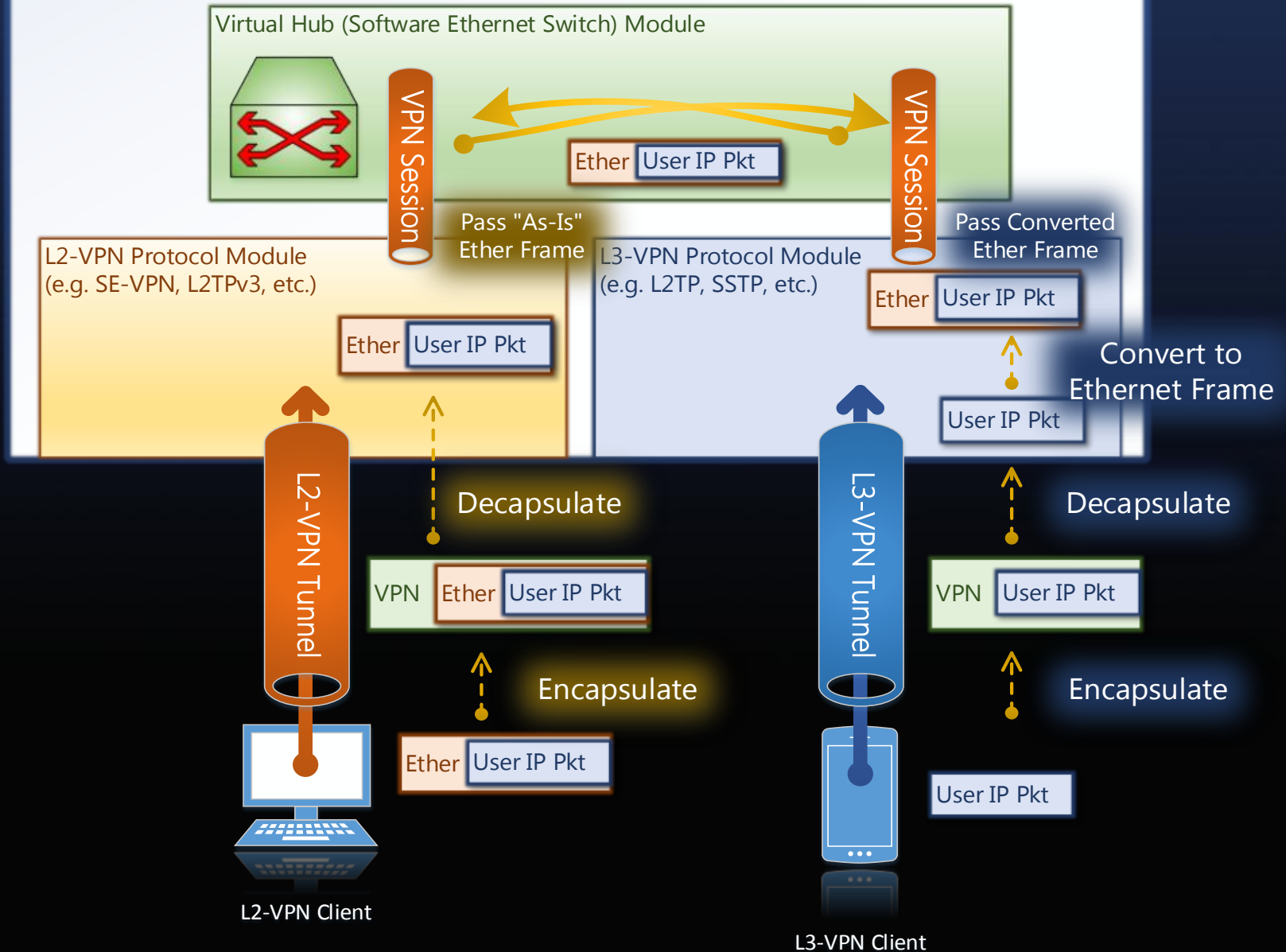
Virtual Ethernet Switching Hub



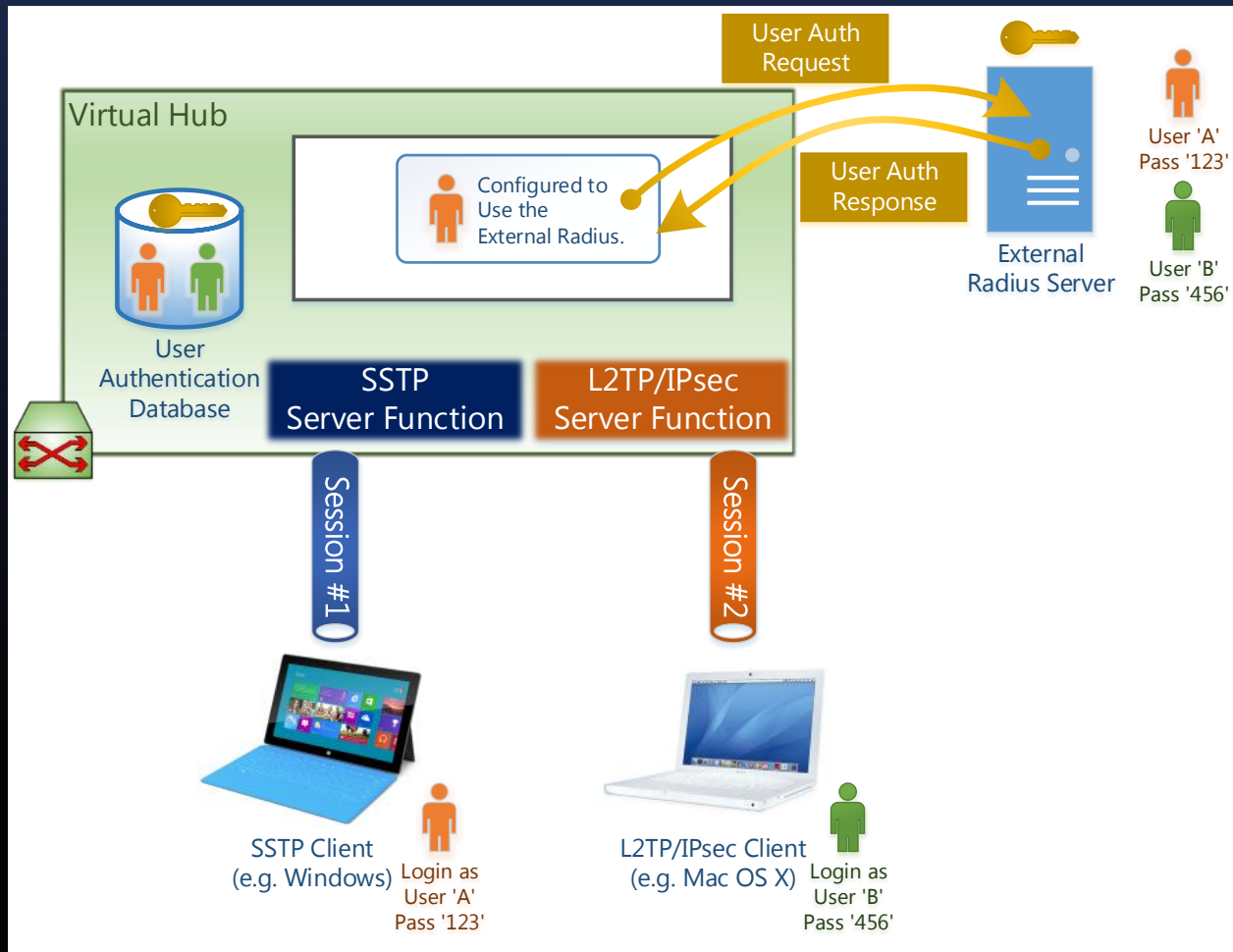
L3/L2 Transparent Conversion



All-in-One VPN Server

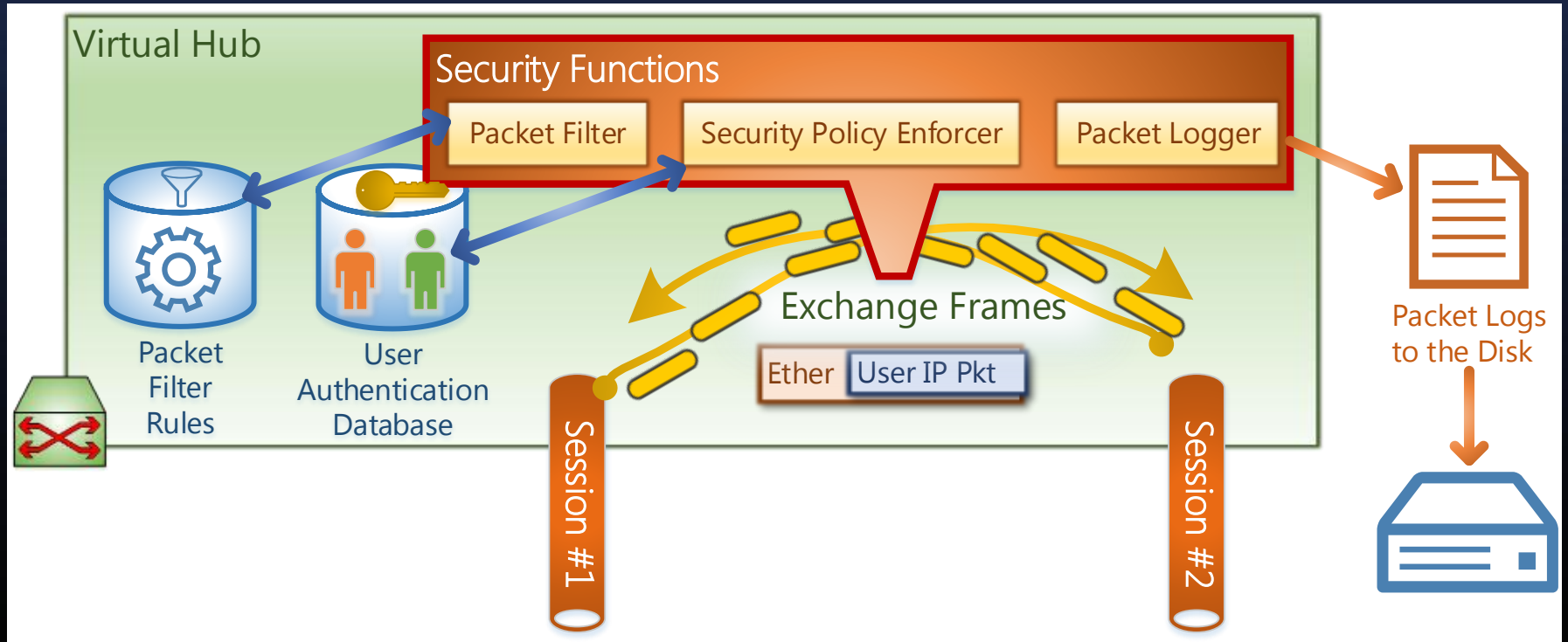


User Authentication

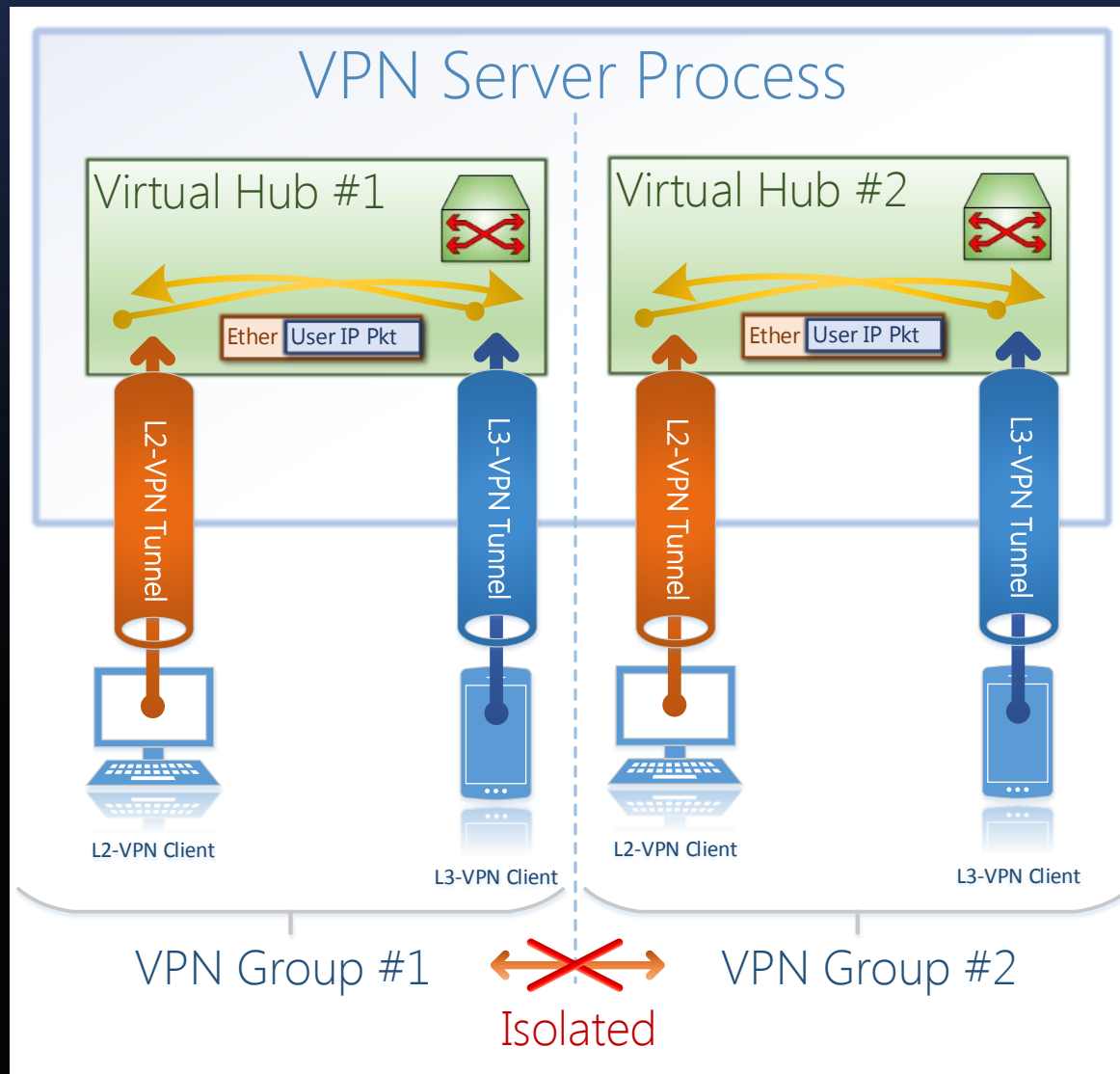


Supports PAP (Password Authentication Protocol) and MS-CHAPv2 (Microsoft Challenge-Handshake Authentication Protocol ver 2) via Local User-auth DB and External Radius/Active Directory Server.

Security



Isolation between Virtual Hubs



Implementation

- SoftEther VPN Server

Current features

- Virtual Ethernet Switching Hub
- Security Policy / Packet Filter Enforcement
- Packet Logging
- Internal and External User-authentication

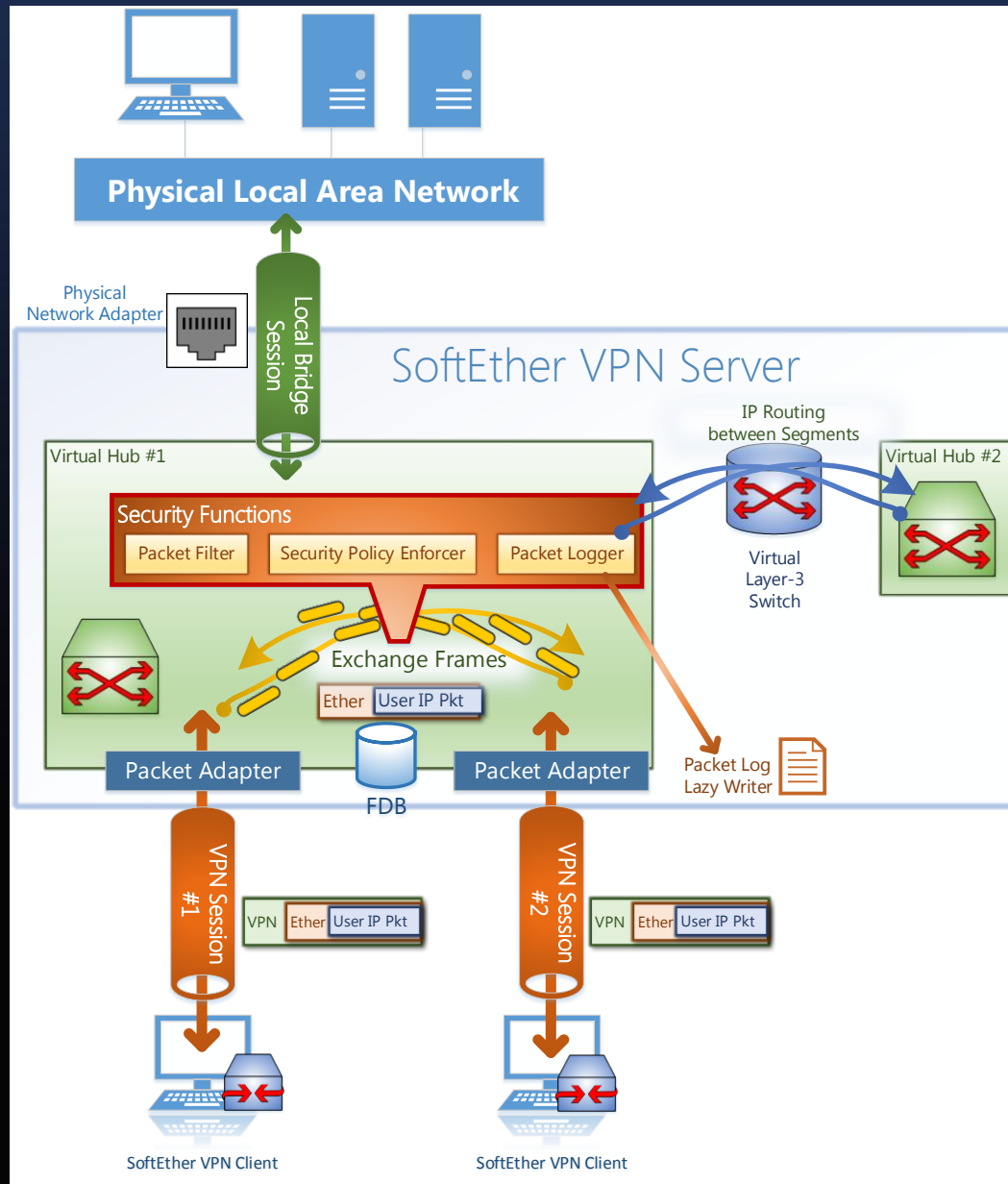
Language

- C / C++

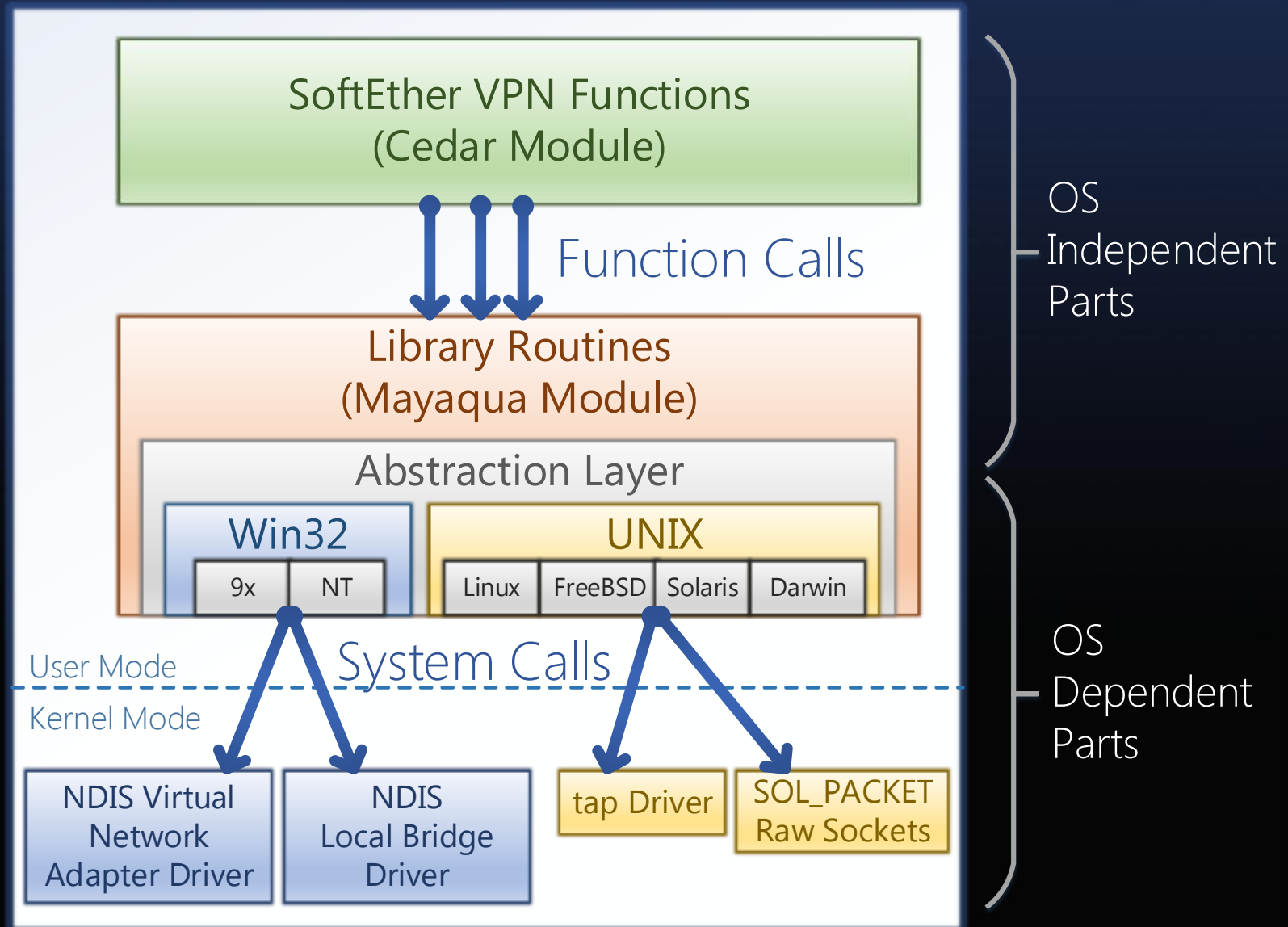
IPsec Modules based on

- BitVisor IPsec Client (Univ of Tsukuba)

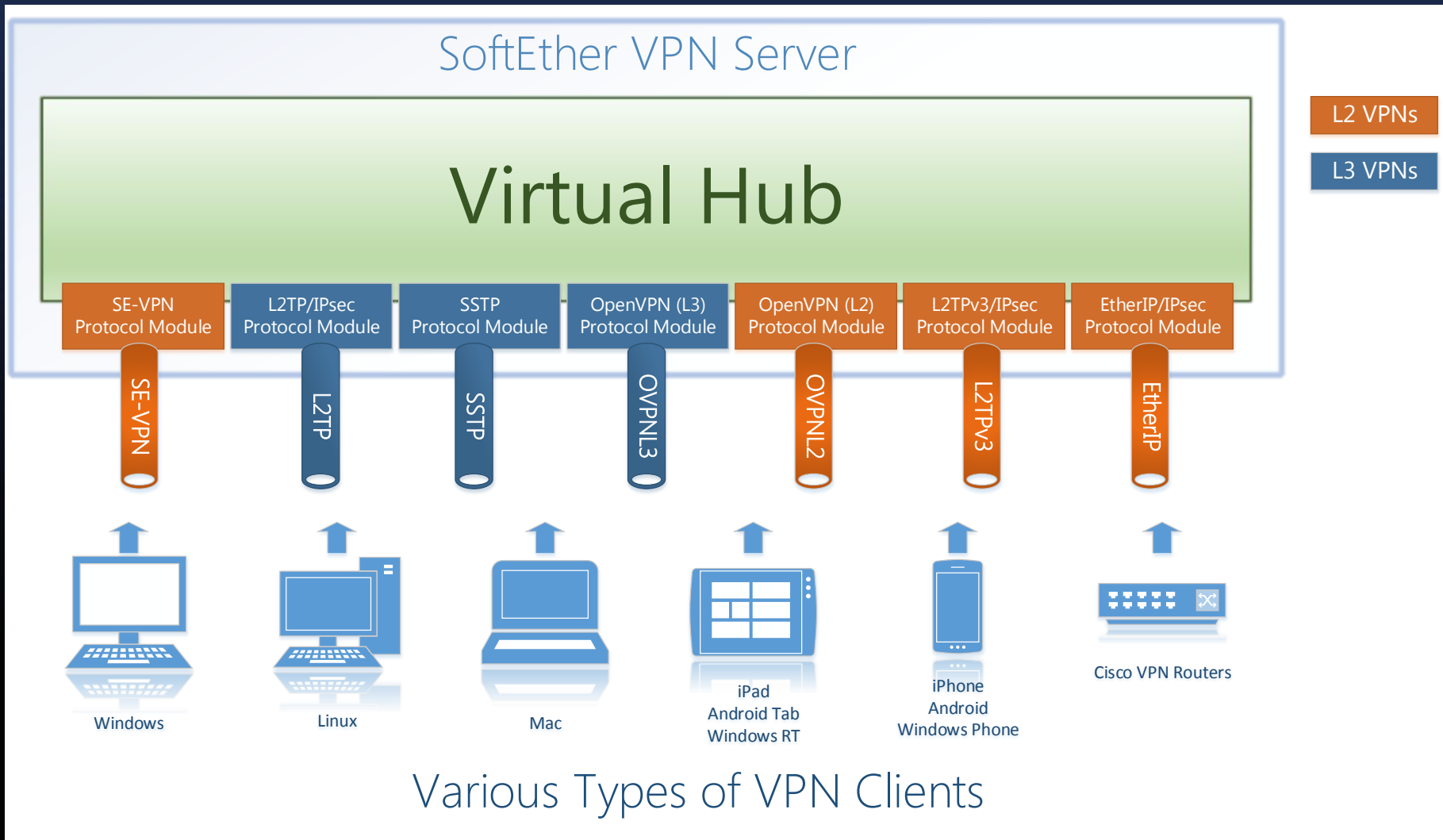
SoftEther VPN Architecture



OS Abstraction Layer



7 Protocol Modules

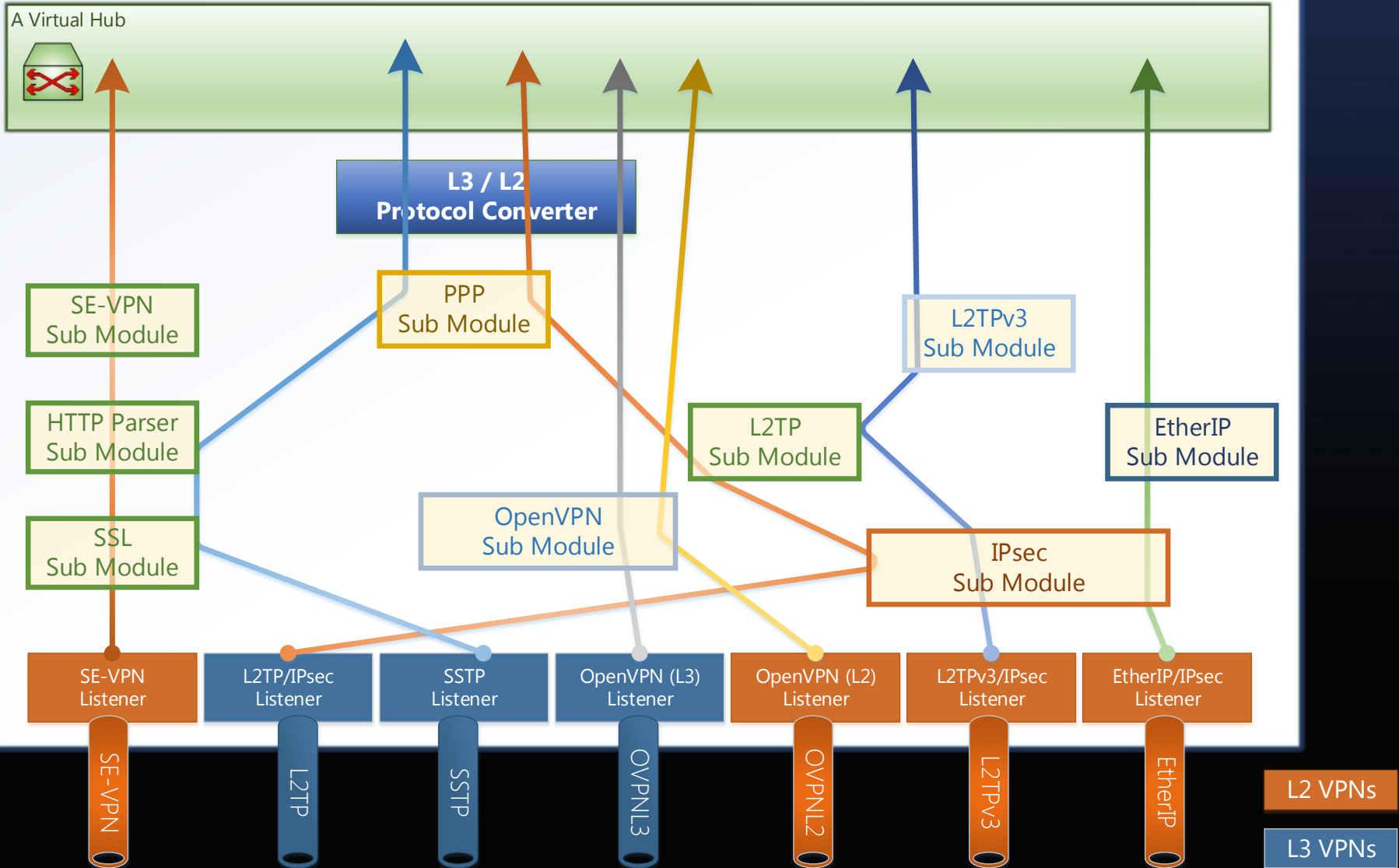


Divide 7 VPN Protocols into Sub Modules

- Overlapped Parts of Processing VPN Protocols
 - "PPP stack" is used by L2TP and SSTP.
 - "IPsec stack" is used by L2TP, L2TPv3 and EtherIP.
 - "OpenVPN stack" is used by OpenVPN L2 and L3.
 - A portion of "L2TP stack" is used by L2TPv3.
- Divide into Sub Modules
 - Minimize Volumes of Codes
 - Reduce Bugs
- Connections between Sub Modules
 - "Tube": A new fast in-process pipe
 - for Single-thread and Multi-thread inter-module communication.

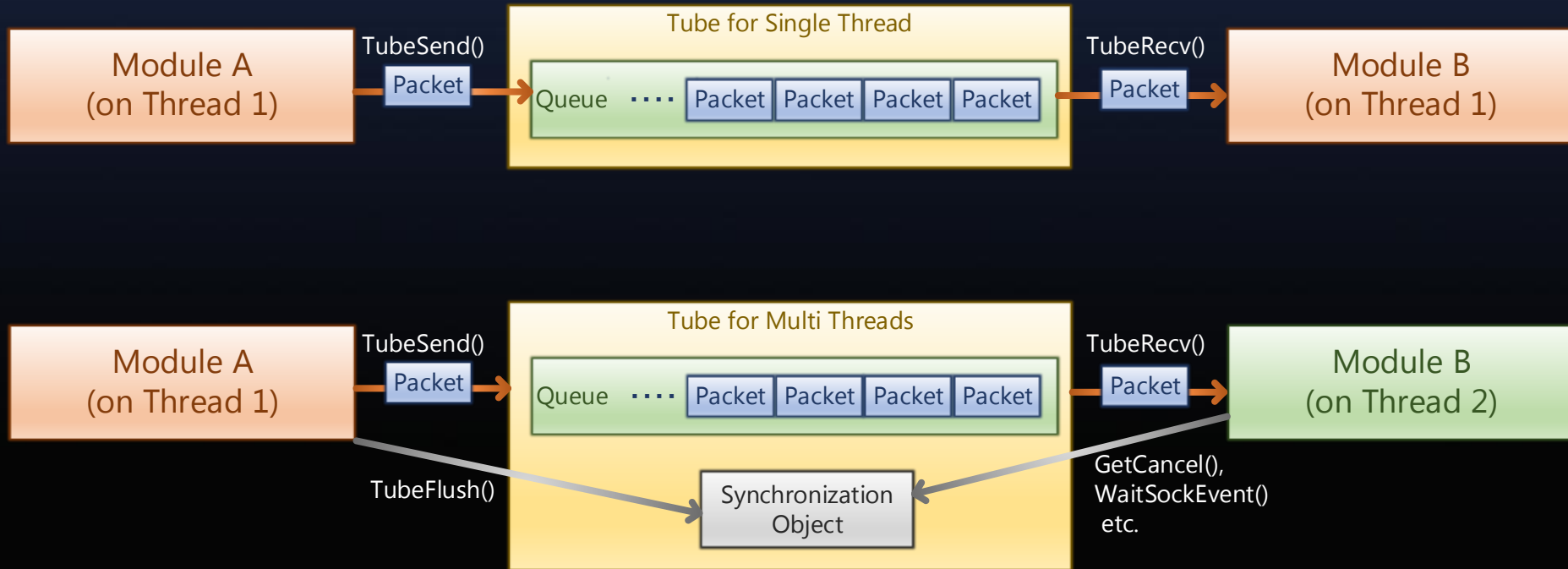
Sub Modules

SoftEther VPN Server



"Tube"

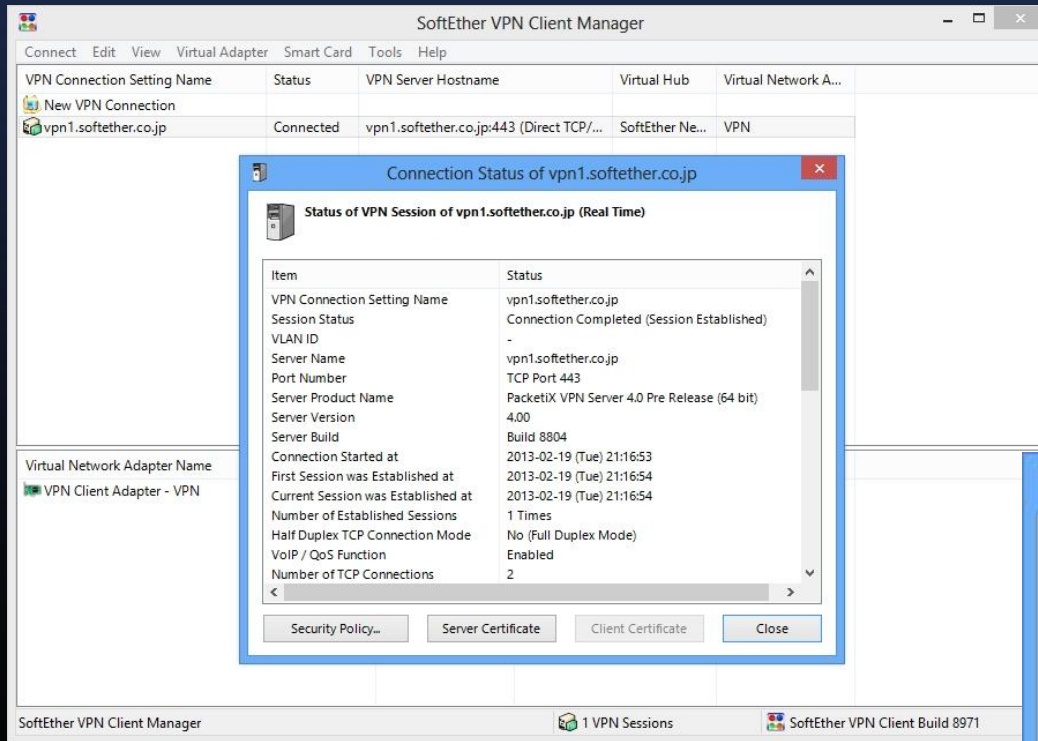
(fast lightweight pipe)



Programming

- C / C++ Source Codes
 - 396,867 Lines (11.5MB)
(including 31,686 comment lines)
- Compiler
 - Visual C++ 2008 for Windows Binaries
 - gcc (any version) for UNIX and Linux Binaries
- Planning to be Open Source (GPL) in Mid 2013.
 - Now translating a lot of comments into English before releasing the source.

Screen Shots



SoftEther VPN Client

Screen Shots

vpn1.softether.co.jp - SoftEther VPN Server Manager

Manage VPN Server "vpn1.softether.co.jp"

Virtual Hub Name	Status	Type	User	Group	Session	MAC Tables	IP Tables
BEIJING_SEGMENT	Online	Standalone	1	0	2	12	12
CHINATEST	Online	Standalone	4	0	3	0	0
moosta	Online	Standalone	3	0	2	2	4
Okkota	Online	Standalone	1	0	0	0	0
SoftEther Network	Online	Standalone	26	2	14	349	336
TEST1	Online	Standalone	1	0	0	0	0
UT	Online	Standalone	2	0	1	1	1

Management of Listeners:

Port Number	Status
TCP 443	Listening
TCP 992	Listening
TCP 993	Listening
TCP 1194	Listening
TCP 8888	Listening

VPN Server and Network Information and Settings:

- Encryption and Network
- Clustering Configuration
- View Server Status
- Clustering Status
- About this VPN Server
- Show List of TCP/IP Connections

Beta Version (Pre-release) Edit Config

Local Bridge Setting Layer 3 Switch Setting IPsec / L2TP Setting OpenVPN / MS-SSTP Setting


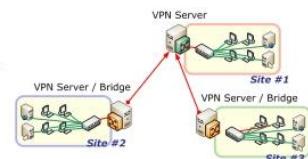
Dynamic DNS Setting VPN Azure Setting

Current DDNS Hostname: vpn1.softether.net VPN Azure Hostname: vpn1.vpnazure.net

SoftEther VPN Server / Bridge Easy Setup

By using this setup you can easily setup a SoftEther VPN Server or VPN Bridge for the following use and purpose. After exiting the setup, you can use the VPN Server Manager to freely configure more advanced settings.

Select the type of VPN server you want to build. Multiple types can be selected together.

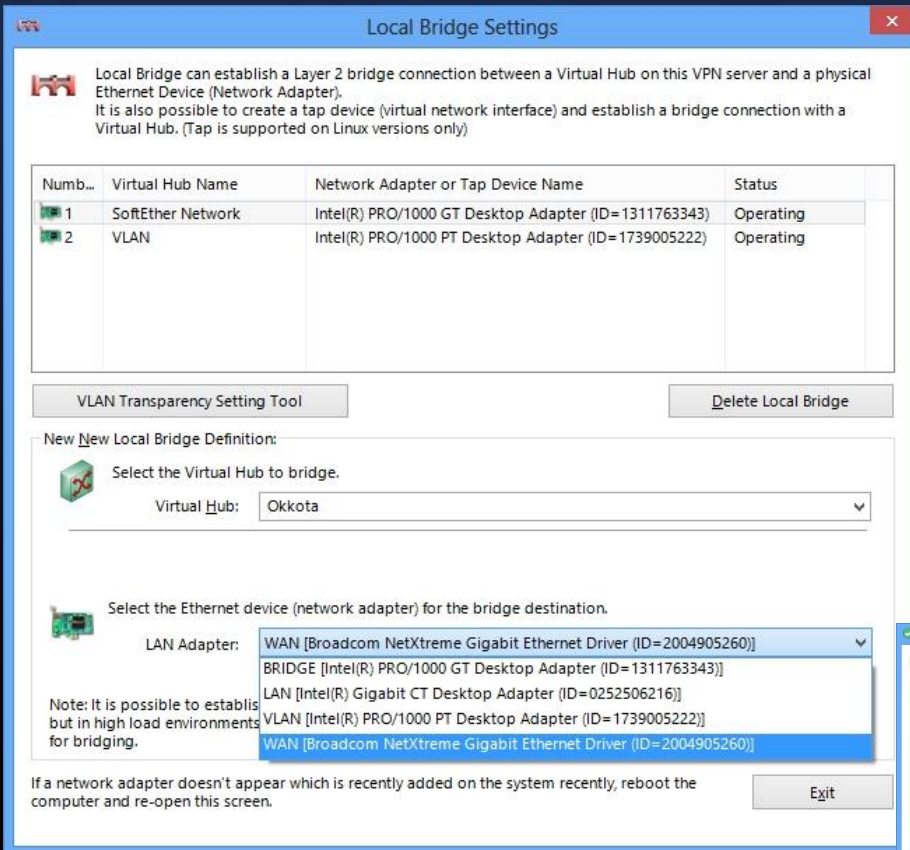
- Remote Access VPN Server**
The Remote Access VPN Server allows VPN Client computers in remote locations to access to the existing Ethernet segments, for example company LAN. Any VPN Clients who is connecting to the VPN Server will be able to access to the network as if they are connected directly and physically to the network.

- Site-to-site VPN Server or VPN Bridge**
Site-to-site VPN is a VPN configuration to connect between two or more remote Ethernet segments. Each of the sites are connected together, and become the same segment at Layer-2 level. It enables any computers of each sites to communicate to each other as if there is a single network.
Select the role of this VPN Server:
 - VPN Server that Accepts Connection from Other Sites (Center)
 - VPN Server or VPN Bridge at Each Site (Edge)
- Other Advanced Configuration of VPN**
Select this if you are planning to build a VPN system that provides advanced functions such as a clustering function and a Virtual Layer 3 Switch function.

Click Next to start Setup. Click Close if you want to exit the setup and manually configure all settings.

Next > Close

SoftEther VPN Server (GUI Config Tools)

Screen Shots



Local Bridge Settings

Local Bridge can establish a Layer 2 bridge connection between a Virtual Hub on this VPN server and a physical Ethernet Device (Network Adapter). It is also possible to create a tap device (virtual network interface) and establish a bridge connection with a Virtual Hub. (Tap is supported on Linux versions only)

Numb...	Virtual Hub Name	Network Adapter or Tap Device Name	Status
1	SoftEther Network	Intel(R) PRO/1000 GT Desktop Adapter (ID=1311763343)	Operating
2	VLAN	Intel(R) PRO/1000 PT Desktop Adapter (ID=1739005222)	Operating

VLAN Transparency Setting Tool Delete Local Bridge

New Local Bridge Definition:

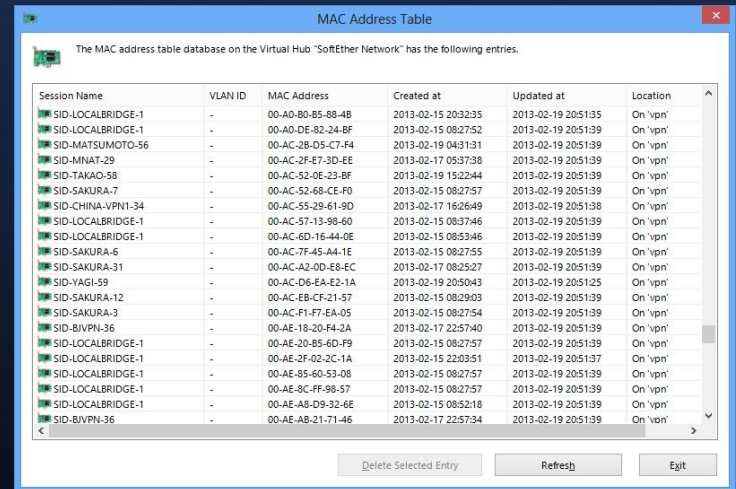
Select the Virtual Hub to bridge.
Virtual Hub: Okkota

Select the Ethernet device (network adapter) for the bridge destination.
LAN Adapter: WAN [Broadcom NetXtreme Gigabit Ethernet Driver (ID=2004905260)]
BRIDGE [Intel(R) PRO/1000 GT Desktop Adapter (ID=1311763343)]
LAN [Intel(R) Gigabit CT Desktop Adapter (ID=0252506216)]
WAN [Intel(R) PRO/1000 PT Desktop Adapter (ID=1739005222)]
WAN [Broadcom NetXtreme Gigabit Ethernet Driver (ID=2004905260)]

Note: It is possible to establish in high load environments for bridging.

If a network adapter doesn't appear which is recently added on the system recently, reboot the computer and re-open this screen.

Exit

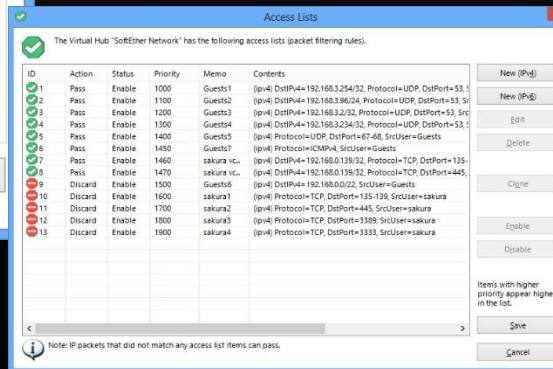


MAC Address Table

The MAC address table database on the Virtual Hub "SoftEther Network" has the following entries.

Session Name	VLAN ID	MAC Address	Created at	Updated at	Location
SID-LOCALBRIDGE-1	-	00-A0-80-B5-88-4B	2013-02-15 20:32:35	2013-02-19 20:51:35	On 'vpn'
SID-LOCALBRIDGE-1	-	00-A0-DE-82-24-BF	2013-02-15 08:27:52	2013-02-19 20:51:39	On 'vpn'
SID-MATSUMOTO-56	-	00-AC-28-D5-C7-F4	2013-02-19 04:31:31	2013-02-19 20:51:39	On 'vpn'
SID-MIAT-29	-	00-AC-2F-E7-2D-EE	2013-02-17 05:37:38	2013-02-19 20:51:39	On 'vpn'
SID-TAKAO-58	-	00-AC-52-0E-23-8F	2013-02-19 15:22:44	2013-02-19 20:51:39	On 'vpn'
SID-SAKURA-7	-	00-AC-52-68-CE-F0	2013-02-15 08:27:57	2013-02-19 20:51:39	On 'vpn'
SID-CHINA-VPN1-34	-	00-AC-55-29-61-90	2013-02-17 16:26:49	2013-02-19 20:51:38	On 'vpn'
SID-LOCALBRIDGE-1	-	00-AC-57-13-98-60	2013-02-15 08:37:46	2013-02-19 20:51:39	On 'vpn'
SID-LOCALBRIDGE-1	-	00-AC-6D-16-4A-0E	2013-02-15 08:53:46	2013-02-19 20:51:39	On 'vpn'
SID-LOCALBRIDGE-1	-	00-AC-7F-45-A4-1E	2013-02-15 08:27:55	2013-02-19 20:51:39	On 'vpn'
SID-SAKURA-31	-	00-AC-A2-0D-E8-EC	2013-02-17 08:25:27	2013-02-19 20:51:39	On 'vpn'
SID-YAGI-59	-	00-AC-D6-EA-E2-1A	2013-02-19 20:50:43	2013-02-19 20:51:25	On 'vpn'
SID-SAKURA-12	-	00-AC-EB-CF-21-57	2013-02-15 08:29:03	2013-02-19 20:51:39	On 'vpn'
SID-SAKURA-3	-	00-AC-F1-F7-EA-05	2013-02-15 08:27:54	2013-02-19 20:51:39	On 'vpn'
SID-BIVPN-36	-	00-AE-18-20-F4-2A	2013-02-17 22:57:40	2013-02-19 20:51:39	On 'vpn'
SID-LOCALBRIDGE-1	-	00-AE-20-B5-6D-F9	2013-02-15 08:27:57	2013-02-19 20:51:39	On 'vpn'
SID-LOCALBRIDGE-1	-	00-AE-2F-02-2C-1A	2013-02-15 22:03:51	2013-02-19 20:51:37	On 'vpn'
SID-LOCALBRIDGE-1	-	00-AE-85-60-53-08	2013-02-15 08:27:57	2013-02-19 20:51:39	On 'vpn'
SID-LOCALBRIDGE-1	-	00-AE-8C-FF-98-57	2013-02-15 08:27:57	2013-02-19 20:51:39	On 'vpn'
SID-LOCALBRIDGE-1	-	00-AE-AB-D9-32-6E	2013-02-15 08:52:18	2013-02-19 20:51:39	On 'vpn'
SID-BIVPN-36	-	00-AE-AB-21-71-46	2013-02-17 22:57:34	2013-02-19 20:51:39	On 'vpn'

Delete Selected Entry Refresh Exit

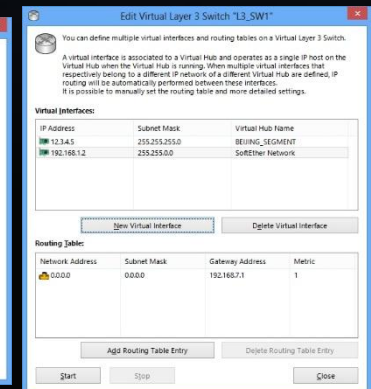


Access Lists

The Virtual Hub "SoftEther Network" has the following access lists (packet filtering rules).

ID	Action	Status	Priority	Memo	Contents
1	Pass	Enable	1000	Guests1	(ip4) DstIP=+ 192.168.3.254/32, Protocol=UDP, DstPort=53, SrcIP=+ 192.168.3.254/32, SrcPort=53
2	Pass	Enable	1100	Guests2	(ip4) DstIP=+ 192.168.3.254/32, Protocol=UDP, DstPort=53, SrcIP=+ 192.168.3.254/32, SrcPort=53
3	Pass	Enable	1200	Guests3	(ip4) DstIP=+ 192.168.3.254/32, Protocol=UDP, DstPort=53, SrcIP=+ 192.168.3.254/32, SrcPort=53
4	Pass	Enable	1300	Guests4	(ip4) DstIP=+ 192.168.3.254/32, Protocol=UDP, DstPort=53, SrcIP=+ 192.168.3.254/32, SrcPort=53
5	Pass	Enable	1400	Guests5	(ip4) Protocol=UDP, DstPort=+ 48, SrcUser=Guests
6	Pass	Enable	1450	Guests7	(ip4) Protocol=ICMP, SrcUser=Guests
7	Pass	Enable	1460	sakura v...	(ip4) DstIP=+ 192.168.0.139/32, Protocol=TCP, DstPort=135...
8	Pass	Enable	1470	sakura v...	(ip4) DstIP=+ 192.168.0.139/32, Protocol=TCP, DstPort=445...
9	Pass	Enable	1470	sakura v...	(ip4) DstIP=+ 192.168.0.139/32, Protocol=TCP, DstPort=445...
10	Discard	Enable	1500	Guests6	(ip4) DstIP=+ 192.168.0.0/22, SrcUser=Guests
11	Discard	Enable	1600	sakura1	(ip4) Protocol=TCP, DstPort=+ 135-139, SrcUser=sakura
12	Discard	Enable	1700	sakura2	(ip4) Protocol=TCP, DstPort=+ 445, SrcUser=sakura
13	Discard	Enable	1800	sakura3	(ip4) Protocol=TCP, DstPort=+ 3389, SrcUser=sakura
14	Discard	Enable	1900	sakura4	(ip4) Protocol=TCP, DstPort=+ 3333, SrcUser=sakura

Note: IP packets that did not match any access list items can pass.



Edit Virtual Layer 3 Switch "L3_SW1"

You can define multiple virtual interfaces and routing tables on a Virtual Layer 3 Switch.

A virtual interface is associated to a Virtual Hub and operates as a single IP host on the Virtual Hub when the Virtual Hub is running. When multiple virtual interfaces that respectively belong to a different IP network of a different Virtual Hub are defined, IP routing will be automatically performed between these interfaces. It is possible to manually set the routing table and more detailed settings.

Virtual Interfaces:

IP Address	Subnet Mask	Virtual Hub Name
13.14.5	255.255.255.0	BEIJING_SEGMENT
192.168.1.2	255.255.0.0	SoftEther Network

Routing Table:

Network Address	Subnet Mask	Gateway Address	Metric
0.0.0.0	0.0.0.0	192.168.1.1	1

A lot of VPN Server Setting Screens (total 70+ dialogs)

Screen Shots

IPsec / L2TP / EtherIP / L2TPv3 Server Settings
Virtual Hubs on the VPN Server can accept Remote-Access VPN connections from L2TP-compatible PCs, Mac OS X and Smartphones, and also can accept EtherIP / L2TPv3 Site-to-Site VPN Connection.

L2TP Server (Remote-Access VPN Server Function)
VPN Connections from Smartphones suchlike iPhone, iPad and Android, and also from built-in VPN Clients on Mac OS X and Windows can be accepted.

- Enable L2TP Server Function (L2TP over IPsec)**
Make VPN Connections from iPhone, iPad, Android, Windows, and Mac OS X acceptable.
- Enable L2TP Server Function (Raw L2TP with No Encryptions)**
It supports special VPN Clients which uses L2TP with no IPsec encryption.

Users should specify their username such as "Username@Target Virtual Hub Name" to connect this L2TP Server.
If designation of a Virtual Hub is omitted, the below Hub will be used as the target.

Default Virtual Hub in a case of omitting a name of Hub on the Username:

EtherIP Server Function (Site-to-Site VPN Connection)
Router products which are compatible with EtherIP / L2TPv3 over IPsec can connect to Virtual Hub on the VPN Server and establish Layer-2 (Ethernet) Bridging.

- Enable EtherIP / L2TPv3 over IPsec Server Function**

IPsec Common Settings
IPsec Pre-Shared Keys:

IPsec Pre-Shared Keys are also called "PSKs" or "Secrets". Specify it with almost eight ASCII characters, and let all VPN users know.

L2TP / L2TPv3 / EtherIP

OpenVPN / MS-SSTP VPN Clone Server Function Settings

OpenVPN Clone Server Function
This VPN Server has the clone functions of OpenVPN software products by OpenVPN Technologies, Inc.

Any OpenVPN Clients can connect to this VPN Server.

- Enable OpenVPN Clone Server Function**

UDP Ports to Listen for OpenVPN:

Multiple UDP ports can be specified with splitting by space or comma letters.
OpenVPN Server Function also runs on TCP ports. Any TCP ports which are defined as listeners on the VPN Server accepts OpenVPN Protocol respectively and equally.

Sample File Generating Tool for OpenVPN Clients
Making a OpenVPN Client configuration file is a very difficult job. You can use this tool to generate an appropriate OpenVPN Client configuration file. The generated configuration sample can be used immediately.

Microsoft SSTP VPN Clone Server Function
This VPN Server has the clone functions of MS-SSTP VPN Server which is on Windows Server 2008 / 2012 by Microsoft Corporation. Built-in MS-SSTP Clients on Windows Vista / 7 / 8 / RT can connect to this VPN Server.

- Enable MS-SSTP VPN Clone Server Function**

The value of CN (Common Name) on the SSL certificate of VPN Server must match to the hostname specified on the client, and that certificate must be in the trusted list on the client. For details refer the Microsoft's documents.

The manner to specify a username to connect to the Virtual Hub, and the selection rule of default Hub by using these clone server functions are same to the IPsec Server functions.

OpenVPN (L2 & L3) / SSTP

Screen Shots

VPN over ICMP / DNS Function Settings

VPN over ICMP / DNS Function

You can establish a VPN only with ICMP or DNS packets even if there is a firewall or routers which blocks TCP/IP communications. You have to enable the following functions beforehand.

- Enable VPN over ICMP Server Function
- Enable VPN over DNS Server Function (Uses UDP Port 53)

```

C:\>ping 219.219.219.154
Pinging 219.219.219.154 with 32 bytes of data:
Reply from 219.219.219.154: bytes=32 time=45ms TTL=67
Reply from 219.219.219.154: bytes=32 time=54ms TTL=67
Reply from 219.219.219.154: bytes=32 time=54ms TTL=67
Reply from 219.219.219.154: bytes=32 time=54ms TTL=67
Ping statistics for 219.219.219.154:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 54ms, Maximum = 55ms, Average = 54ms

```

Use Ping / DNS Packets to Establish a VPN Tunnel.

ICMP
DNS

VPN Server

Outbound Firewall

VPN Client

VPN over ICMP
VPN over DNS

ICMP Header / DNS Header
VPN Payload

Warning: Use this function for emergency only. It is helpful when a firewall or router is misconfigured to blocks TCP/IP, but either ICMP or DNS is not blocked. It is not for long-term stable using.

Requires VPN Client / VPN Bridge internal version 4.0 or greater.

OK Cancel

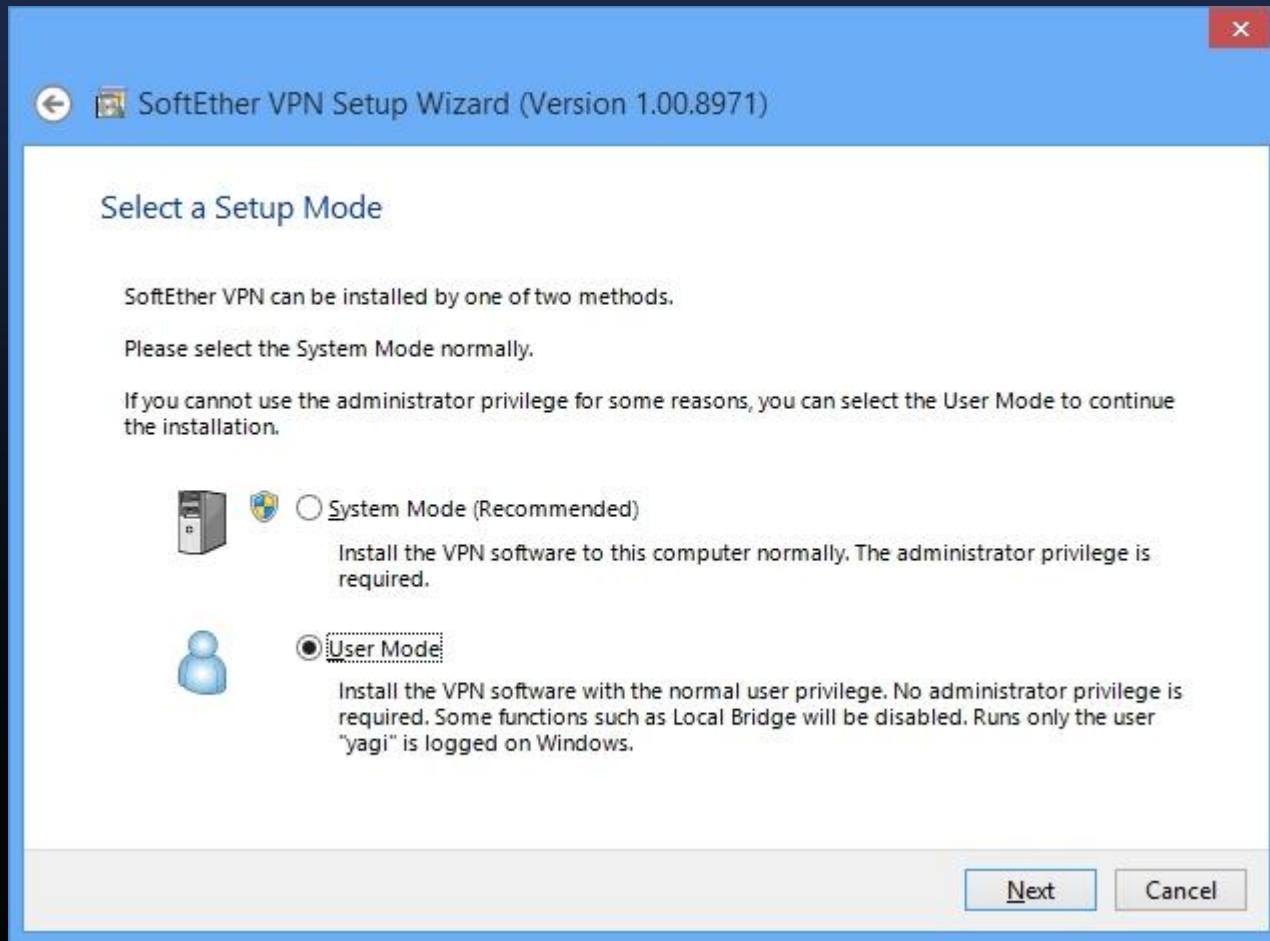
Ethernet over DNS, Ethernet over ICMP
(Enjoy your Wi-Fi Life!)

Screen Shots



Beautiful Installer for SoftEther VPN

Screen Shots



User-Mode Install Option
(System Admins will be Surprised!)

Screen Shots



Multi-languages Support

Evaluation

1. Functional Tests

- Self Test
- Beta Test

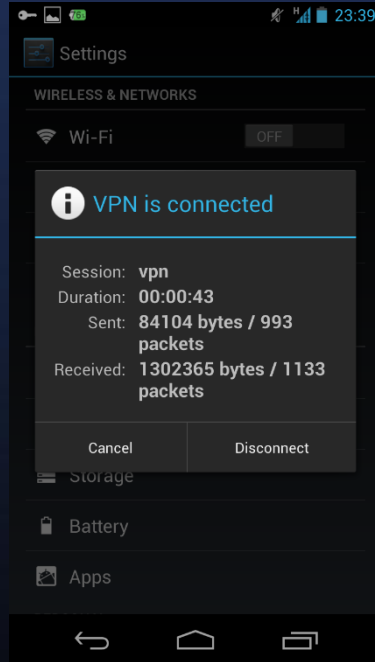
2. Performance Tests

- Simple throughput test
- Comparison to existing methods

L2TP/IPsec



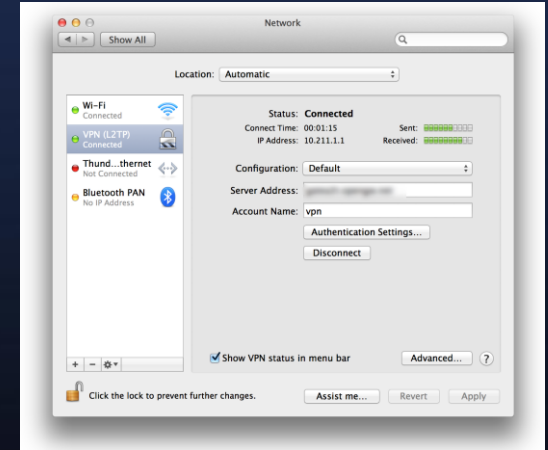
iOS



Android

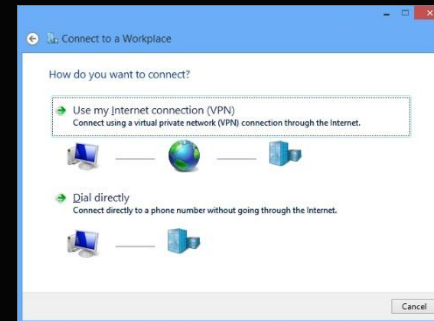
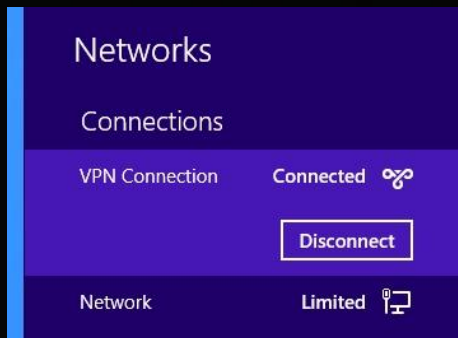


Windows

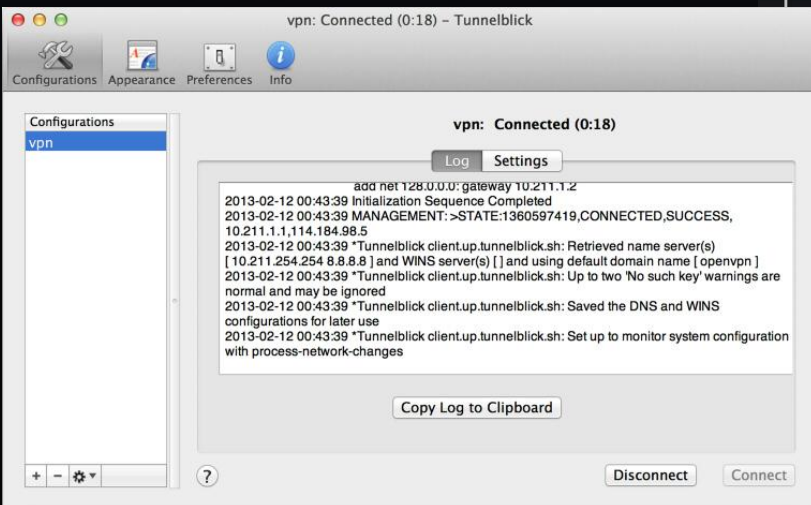
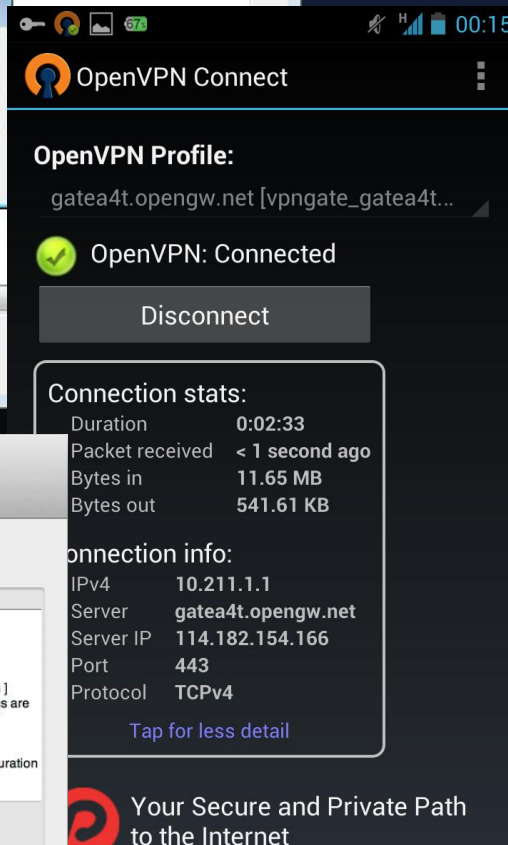
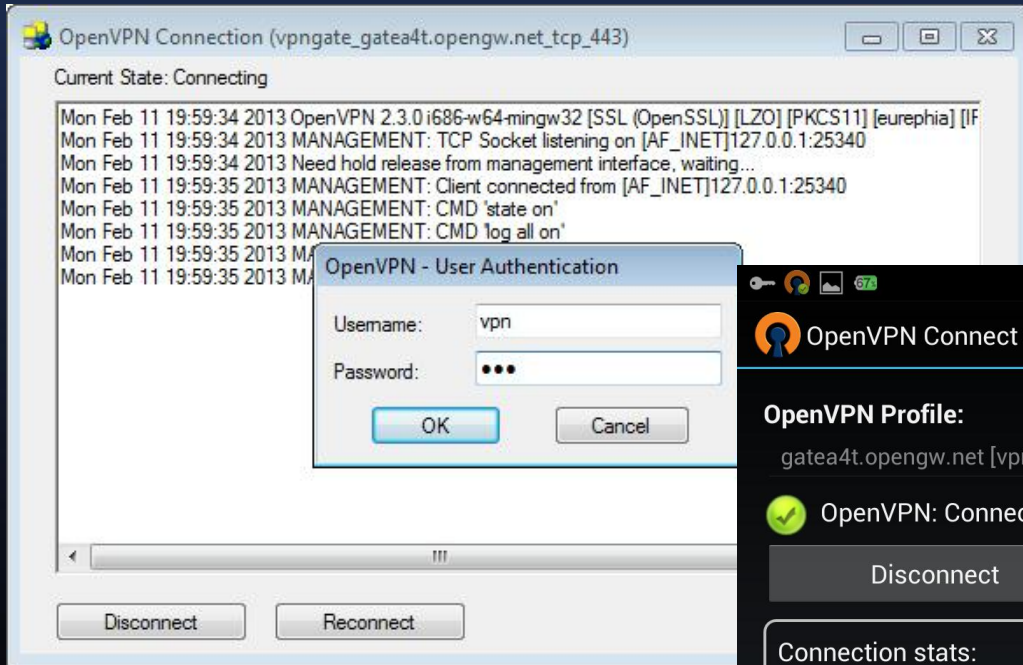


Mac OS X

SSTP



OpenVPN



L2TPv3/IPsec, EtherIP/IPsec

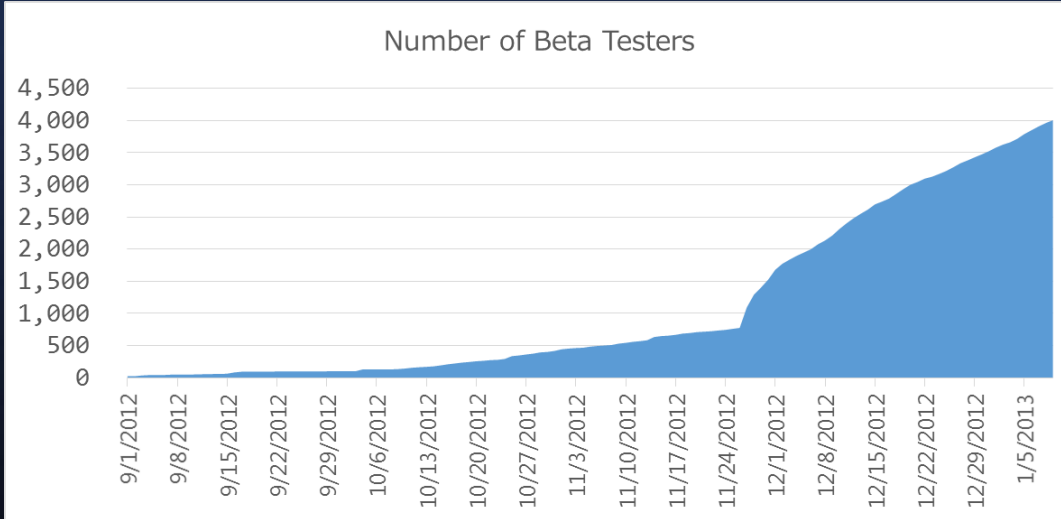


L2TPv3: Cisco IOS, IJ SEIL
EtherIP: NEC IX

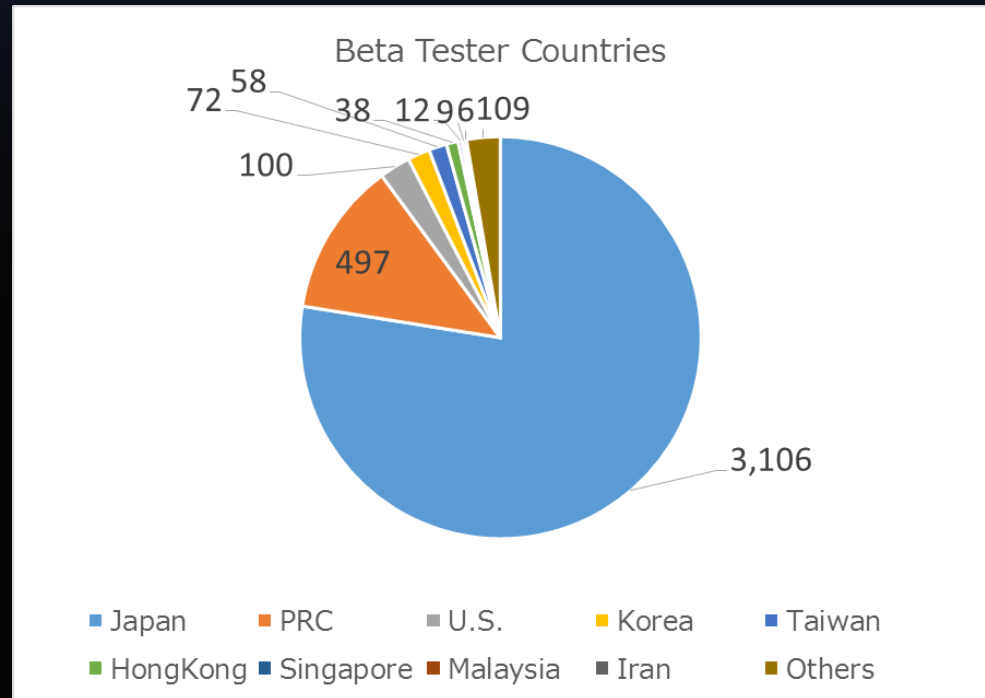
Results of Self Functional Tests

VPN Protocol	VPN Client Software / Device	Results
L2TP/IPsec	iPhone (iOS 4.x, 5.x, 6.x)	✓
	iPad (iOS 4.x, 5.x, 6.x)	✓
	Android (2.x, 3.x, 4.x)	✓
	Windows XP, Vista, 7, 8, RT	✓
	Mac OS X (10.6, 10.7, 10.8)	✓
SSTP	Windows Vista, 7, 8, RT	✓
OpenVPN (L3)	Windows, Linux, Mac, iPhone, Android	✓
L2TPv3/IPsec	Cisco 892J	✓
	Cisco 1812J	✓
EtherIP/IPsec	NEC IX2015	✓
OpenVPN (L2)	OpenVPN 2.2 for Windows, Linux	✓

Results of Beta Tests



4,007 Users on
Jan 09, 2013.



Achievement

	L2TP	SSTP	OpenVPN	L2TPv3	EtherIP	SoftEther VPN
Microsoft RRAS	✓	✓	-	-	-	-
Mac OS X Server	✓	-	-	-	-	-
OpenVPN	-	-	✓	-	-	-
Cisco IOS	✓	-	-	✓	-	-
NEC IX Router OS	-	-	-	-	✓	-
IJ SEIL Router OS	✓	✓	-	✓	-	-
SoftEther VPN (Old)	-	-	-	-	-	✓
SoftEther VPN (New)	✓	✓	✓	✓	✓	✓

Performance Tests

Computer	Fujitsu PRIMERGY TX100 S3 (3 Pieces)
CPU	Intel Xeon E3-1230 3.2GHz 8M
RAM	16GB (4GB 1333MHz DDR3 ECC CL9 DIMM x 4)
Chipset	Intel C202
NIC #1, #2	Intel 10 Gigabit CX4 Dual Port Server Adapter
OS	Windows Server 2008 R2 x64 Windows Server 2003 R2 x64 (for OS abstraction-layer performance tests) Linux 2.6.32 x64 (for OS abstraction-layer performance tests)



Target Protocols

- SoftEther VPN Protocol
- L2TP/IPsec
- SSTP
- OpenVPN (L3)
- OpenVPN (L2)

Test 1. Each Protocol (Solo)

Our Implementation vs. Vendor's Original Implementation

for L2TP,
for SSTP,
for OpenVPN



vs.

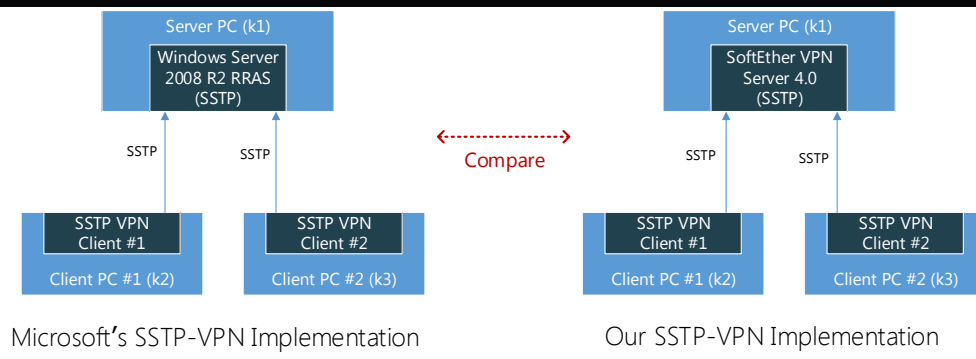


for L2TP,
for SSTP

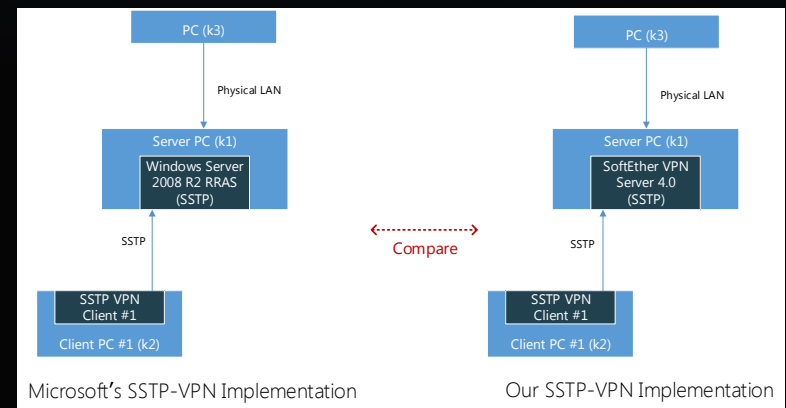


for OpenVPN

Examples (for SSTP)



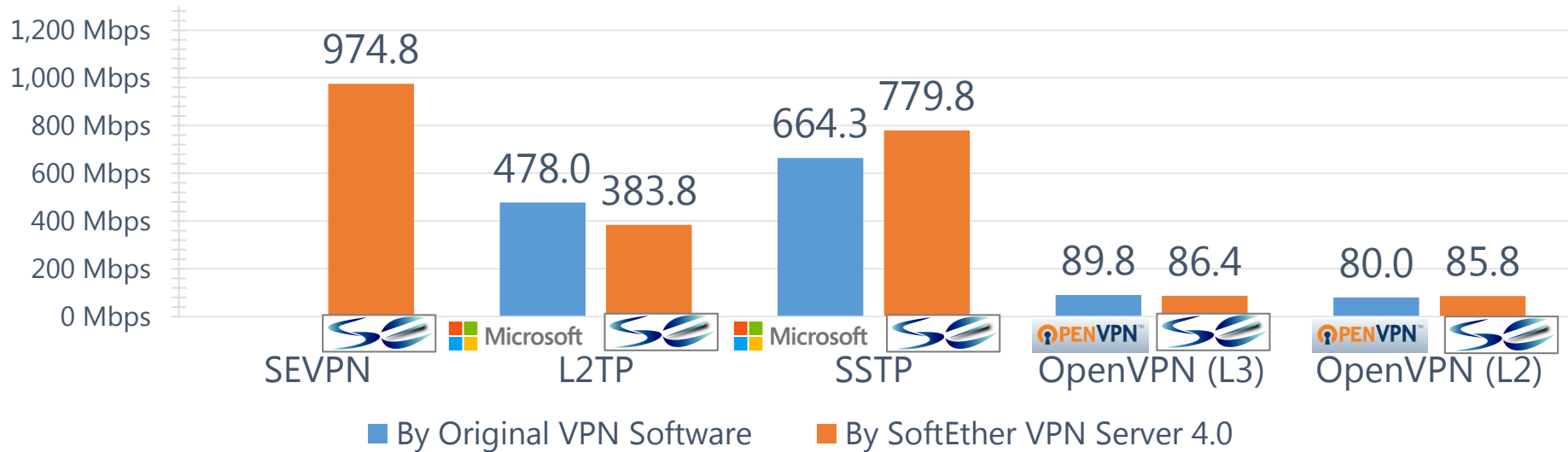
PC-to-PC VPN



PC-to-LAN VPN

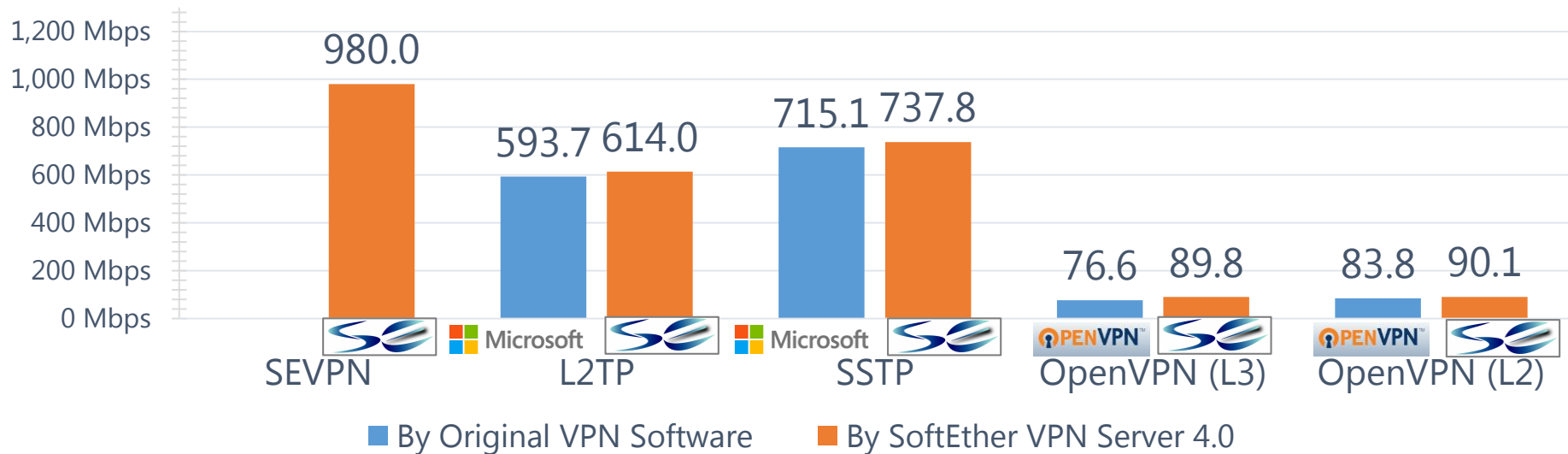
Test 1 Results (PC-to-PC)

Original VPN Software v.s. SoftEther VPN Server 4.0 (1 VPN Protocol, PC to PC)



Test 1 Results (PC-to-LAN)

Original VPN Software v.s. SoftEther VPN Server 4.0 (1 VPN Protocol, PC to LAN)



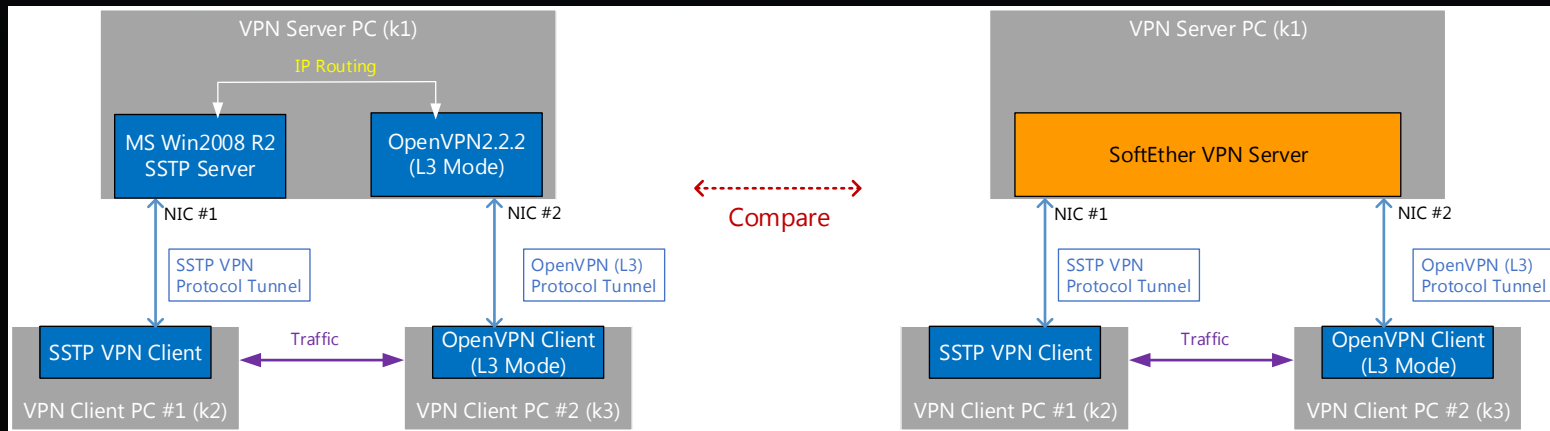
Test 2.

Combination of 2 Protocols

Our Implementation (New) vs. Mixture of 2 VPN Programs (Traditional)



Example (for SSTP+OpenVPN L3)



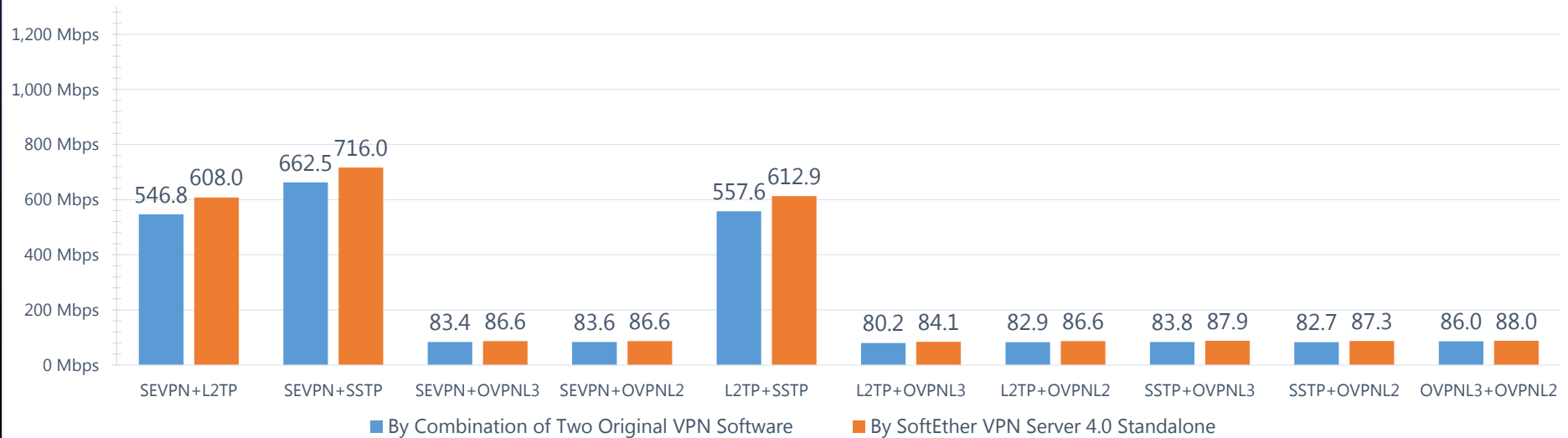
Combination Matrix

No.	Protocol 1	Protocol 2	Bridge / Routing
1	SEVPN	L2TP/IPsec	IP Routing
2	SEVPN	SSTP	IP Routing
3	SEVPN	OpenVPN_L3	IP Routing
4	SEVPN	OpenVPN_L2	Ethernet Bridging
5	L2TP/IPsec	SSTP	IP Routing
6	L2TP/IPsec	OpenVPN_L3	IP Routing
7	L2TP/IPsec	OpenVPN_L2	IP Routing
8	SSTP	OpenVPN_L3	IP Routing
9	SSTP	OpenVPN_L2	IP Routing
10	OpenVPN_L3	OpenVPN_L2	IP Routing

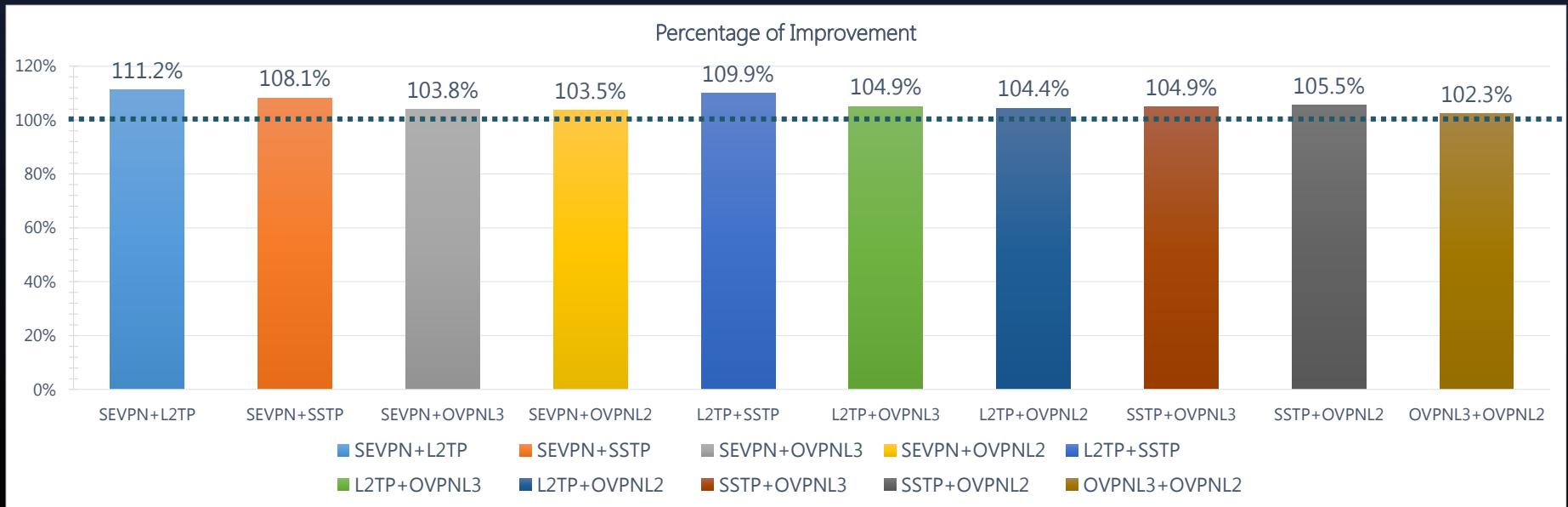
Total 10 Tests

Test2 Results (Throughput)

Original VPN Software v.s. SoftEther VPN Server 4.0 (2 VPN Protocols)

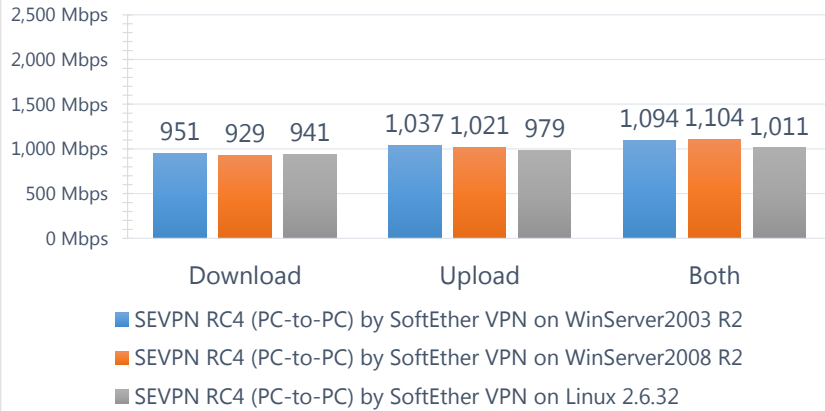


Test2 Results (Percentage of Improvement)

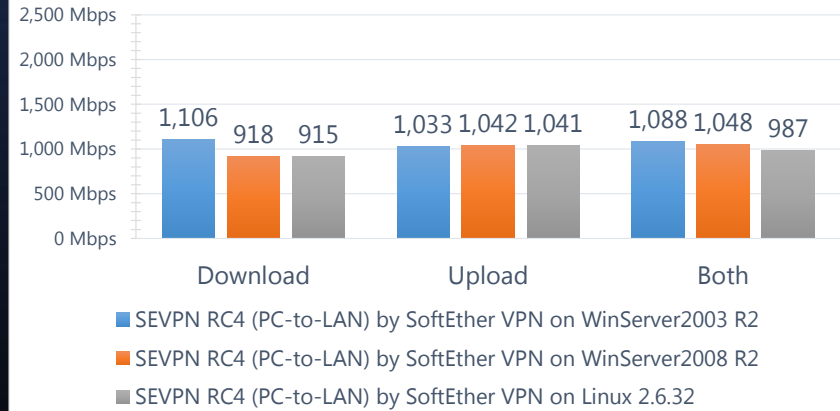


Test 3. Evaluation of OS-Abstraction Layer

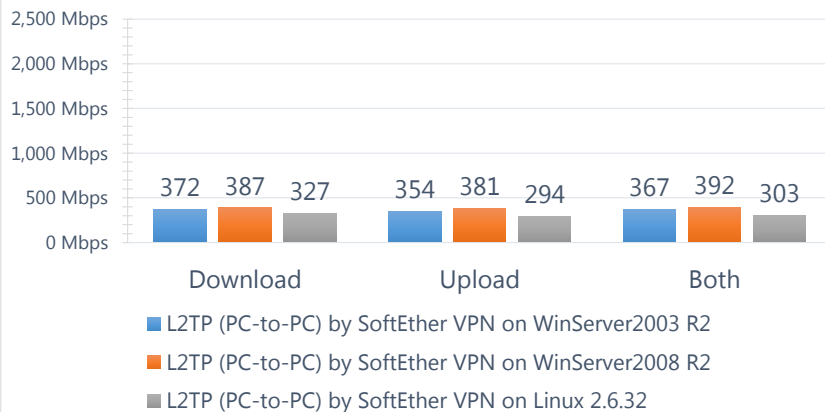
4.1.1. SEVPN RC4 PC-to-PC OS Comparison (Throughput)



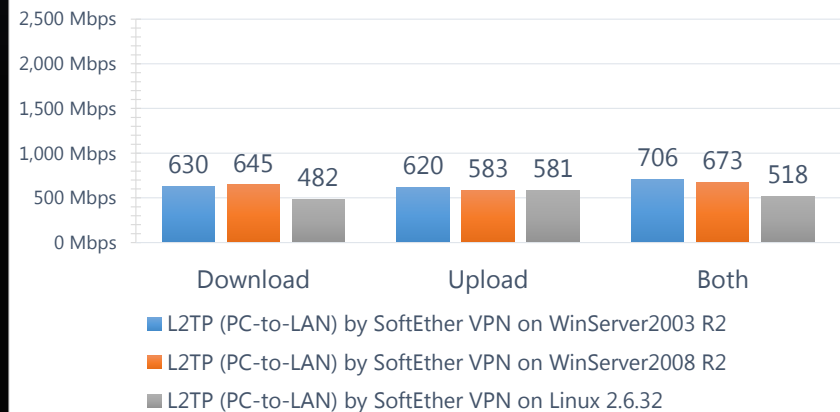
4.1.3. SEVPN RC4 PC-to-LAN OS Comparison (Throughput)



4.1.5. L2TP PC-to-PC OS Comparison (Throughput)



4.1.6. L2TP PC-to-LAN OS Comparison (Throughput)



Conclusions #1

- This Research Designs and Implements a New VPN Server Program.
 - Supports 7 VPN Protocols.
 - SoftEter VPN, L2TP over IPsec, SSTP, OpenVPN (L3, L2), EtherIP over IPsec and L2TPv3 over IPsec.
- The World's First VPN Server Program for Support All of Above VPN Protocols.
- Runs on Windows, Linux, Mac, FreeBSD and Solaris.
 - Unified Management, Security, User-auth and IP Address Assignment.

Conclusions #2

- Results of Performance Tests show:
 - Generally better throughputs, compare to Microsoft and OpenVPN's implementations.
 - Overheads of combination of different VPN protocols are reduced.
(Performance Improvements: 102.3% - 111.2%)
 - OS Abstraction Layer works well.

Future Works

- More Improvements of Performance.
- Additional VPN Protocols.
 - IKEv2, PPTP and IPsec Tunnel Mode
- Release as Open-Source Software (GPL license).
 - "SoftEther VPN", <http://www.softether.org/>
Estimated release date: by end of March 2013.
(First, close-source with binaries. Translate all Japanese comments to English and release it in middle 2013.)
- Enable third-Developers to Add More VPN Protocol Modules Easily.

Outline of Master Thesis,
January 16, 2013.

Design and Implementation of SoftEther VPN

Daiyuu Nobori

*Department of Computer Science,
Graduate School of Systems and Information Engineering,
University of Tsukuba, Japan.*