Virtual Private Networks

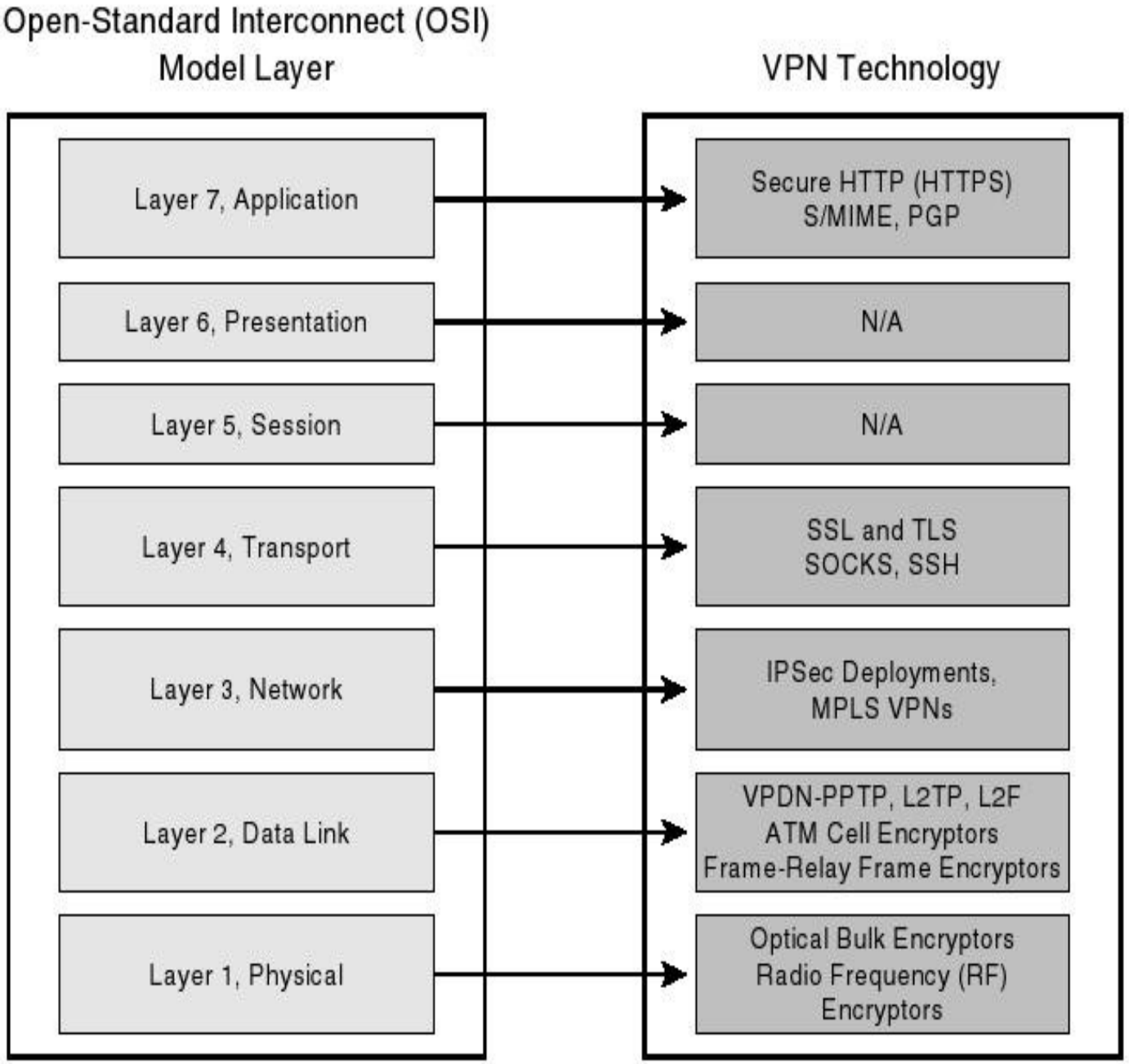
-Prekshu Ajmera

Virtual Private Network

- Internet runs on public lines that are insecure
  - Need to communicate securely
  - Private lines : costly option
- VPN
  - Secure private communications over public internet
  - Private IP packets encapsulated within public packets (tunnel)

VPN where and why?

Use	Application	Alternative To	Benefits
Remote Access VPN	Remote Connectivity	Dedicated Dial ISDN	Ubiquitous Access Lower Cost
IntranetVPN	Site-to-Site Internal Connectivity	Leased Line	Extend Connectivity Lower Cost
ExtranetVPN	Business-to-Business External Connectivity	Fax, Mail, EDI	Facilitates E-Commerce

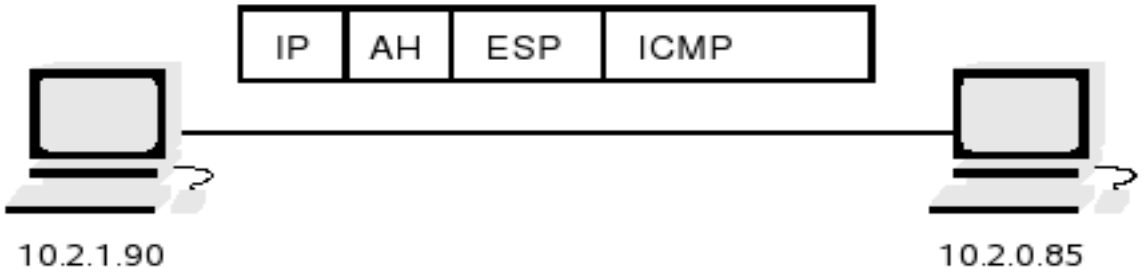

Open-Standard Interconnect (OSI) Model Layer
VPN Technology
Layer 7, Application
Secure HTTP (HTTPS)
S/MIME, PGP
Layer 6, Presentation
N/A
Layer 5, Session
N/A
Layer 4, Transport
SSL and TLS
SOCKS, SSH
Layer 3, Network
IPSec Deployments,
MPLS VPNs
Layer 2, Data Link
VPDN-PPTP, L2TP, L2F
ATM Cell Encryptors
Frame-Relay Frame Encryptors
Layer 1, Physical
Optical Bulk Encryptors
Radio Frequency (RF)
Encryptors

Types of VPN

- **Secure VPNs**
  - uses public lines
  - encryption / authentication methods
  - IPsec, SSL
- **Trusted VPNs**
  - service provider's private network
  - SLA to ensure QoS.
  - MPLS, L2VPN, L3VPN

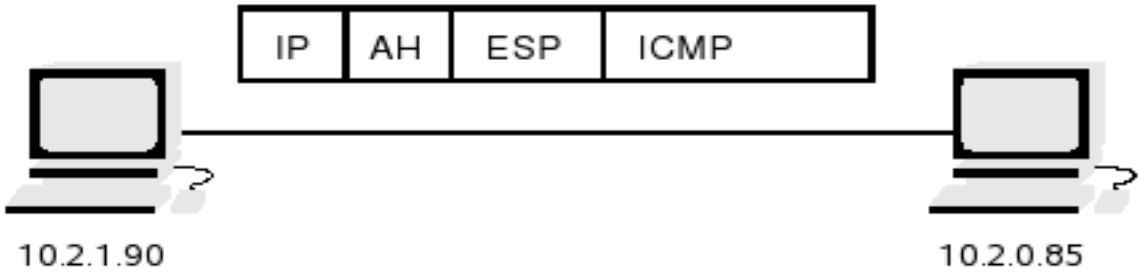
IPsec

- IPsec -standardized framework for securing IP communications
- Modes
  - Tunnel / Transport
- Protocols
  - AH - authentication, IP header integrity
  - ESP - data confidentiality, integrity, authentication.



Two machines in transport mode using AH and ESP

12 1.659707	10.2.0.85	10.2.1.90	TCP	56082 > auth [SYN] Seq=0 Len=0 MSS=1460 TSV=42499954 TSE
13 1.659837	10.2.1.90	10.2.0.85	TCP	auth > 56082 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
14 1.662712	10.2.0.85	10.2.1.90	FTP	Response: 220 ProFTPD 1.3.0 Server (Debian) [::ffff:10.2
15 1.662911	10.2.1.90	10.2.0.85	TCP	3516 > ftp [ACK] Seq=1 Ack=55 Win=5840 Len=0 TSV=1101437
17 3.274579	10.2.1.90	10.2.0.85	FTP	Request: USER amit
18 3.274592	10.2.0.85	10.2.1.90	TCP	ftp > 3516 [ACK] Seq=55 Ack=12 Win=5792 Len=0 TSV=425015
19 3.295449	10.2.0.85	10.2.1.90	FTP	Response: 331 Password required for amit.
20 3.295574	10.2.1.90	10.2.0.85	TCP	3516 > ftp [ACK] Seq=12 Ack=88 Win=5840 Len=0 TSV=110147
24 4.862908	10.2.1.90	10.2.0.85	FTP	Request: PASS amit
25 4.902132	10.2.0.85	10.2.1.90	TCP	ftp > 3516 [ACK] Seq=88 Ack=23 Win=5792 Len=0 TSV=425031
26 4.931350	10.2.0.85	10.2.1.90	FTP	Response: 230 User amit logged in.
27 4.931472	10.2.1.90	10.2.0.85	TCP	3516 > ftp [ACK] Seq=23 Ack=114 Win=5840 Len=0 TSV=11015
28 4.931524	10.2.1.90	10.2.0.85	FTP	Request: SYST
29 4.931531	10.2.0.85	10.2.1.90	TCP	ftp > 3516 [ACK] Seq=114 Ack=29 Win=5792 Len=0 TSV=42503
30 4.931654	10.2.0.85	10.2.1.90	FTP	Response: 215 UNIX Type: L8



Two machines in transport mode using AH and ESP

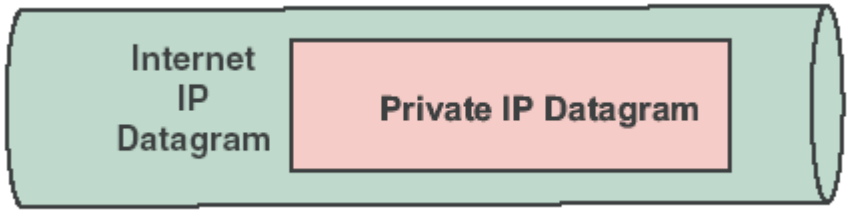
```
12 0.076444    10.2.0.85          10.2.1.90          ESP      ESP (SPI=0x00003d55)
13 0.077279    10.2.1.90          10.2.0.85          ESP      ESP (SPI=0x00005fb5)
14 0.077392    10.2.0.85          10.2.1.90          ESP      ESP (SPI=0x00003d55)
15 0.077474    10.2.0.85          10.2.1.90          ESP      ESP (SPI=0x00003d55)
16 0.077563    10.2.0.85          10.2.1.90          ESP      ESP (SPI=0x00003d55)
17 0.077646    10.2.0.85          10.2.1.90          ESP      ESP (SPI=0x00003d55)
18 0.077737    10.2.0.85          10.2.1.90          ESP      ESP (SPI=0x00003d55)
19 0.078211    10.2.1.90          10.2.0.85          ESP      ESP (SPI=0x00005fb5)
20 0.078318    10.2.0.85          10.2.1.90          ESP      ESP (SPI=0x00003d55)
21 0.078383    10.2.0.85          10.2.1.90          ESP      ESP (SPI=0x00003d55)
22 0.078591    10.2.1.90          10.2.0.85          ESP      ESP (SPI=0x00005fb5)
23 0.078913    10.2.0.85          10.2.1.90          ESP      ESP (SPI=0x00003d55)
```

```
00 11 2f 42 fc 52 00 11  09 fd 1c ad 08 00 45 10   ../B.R.. ......E.
05 dc 30 e4 40 00 40 33  ee 48 0a 02 00 55 0a 02   ..0.@.@3 .H...U..
01 5a 32 04 00 00 00 00  3d 54 00 01 7d 24 68 77   .Z2..... =T..}$hw
8e 2c df 43 81 fe cb 9d  71 6f 00 00 3d 55 00 01   .,.C.... qo..=U..
7d 24 e8 65 f7 de 14 ae  61 47 a2 a5 6a 7d 1a de   }$.e.... aG..j}..
bd 70 7b fa 32 e3 27 50  d1 37 87 56 1d c4 49 6a   .p{.2.'P .7.V..Ij
e8 7a 28 4b 2b fd 35 9d  46 a0 dc c6 e1 36 7e ec   .z(K+.5. F....6~.
34 25 5c a6 26 22 16 38  96 d8 6d ae 7e e9 a0 05   4%\.&".8 ..m.~...
```

```
#!/usr/sbin/setkey -f
# on 10.2.1.90

# AH
add 10.2.0.85 10.2.1.90 ah 15700 -A hmac-md5 "1234567890123456";
add 10.2.1.90 10.2.0.85 ah 24500 -A hmac-md5 "1234567890123456";

# ESP
add 10.2.0.85 10.2.1.90 esp 15701 -E 3des-cbc "123456789012123456789012";
add 10.2.1.90 10.2.0.85 esp 24501 -E 3des-cbc "123456789012123456789012";

spdadd 10.2.1.90 10.2.0.85 any -P out ipsec
        esp/transport//require
        ah/transport//require;

spdadd 10.2.0.85 10.2.1.90 any -P in ipsec
        esp/transport//require
        ah/transport//require;
```

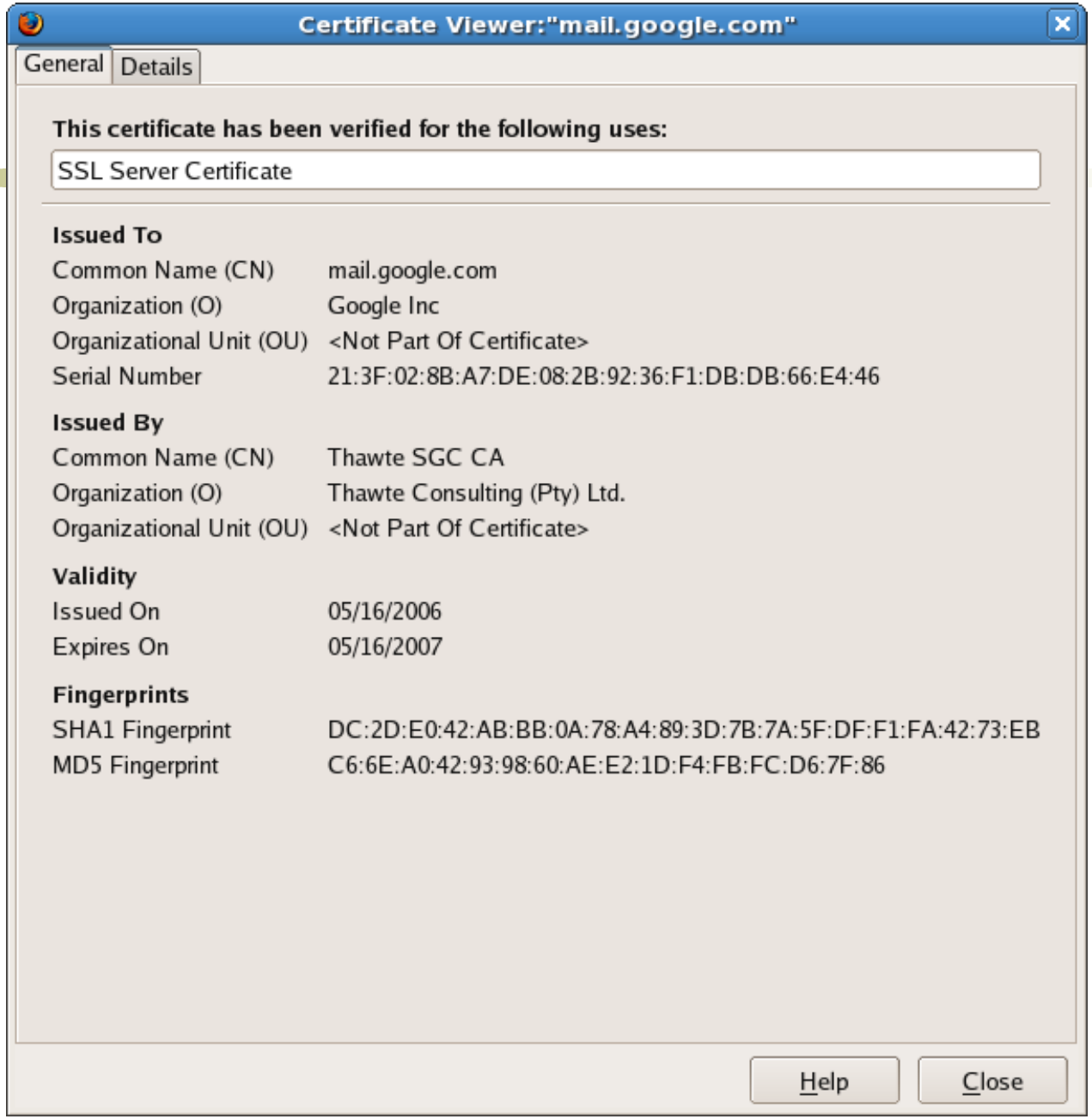
Tunnel vs Transport

- Transport
  - secure an end-to-end connection between two systems
  - only payload encrypted
- Tunnel
  - Encapsulation of original IP packet in another packet
  - between gateways (routers, firewalls)
  - End systems need not support this



SSL

- provides privacy using cryptography.
- end point authentication, typically -
  - server – certificates
  - client – passwords
- runs on layer beneath application layer protocols such as
  - https, sftp, smtp


Certificate Viewer:"mail.google.com"
General
Details
This certificate has been verified for the following uses:
SSL Server Certificate
Issued To
Common Name (CN) mail.google.com
Organization (O) Google Inc
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 21:3F:02:8B:A7:DE:08:2B:92:36:F1:DB:DB:66:E4:46
Issued By
Common Name (CN) Thawte SGC CA
Organization (O) Thawte Consulting (Pty) Ltd.
Organizational Unit (OU) <Not Part Of Certificate>
Validity
Issued On 05/16/2006
Expires On 05/16/2007
Fingerprints
SHA1 Fingerprint DC:2D:E0:42:AB:BB:0A:78:A4:89:3D:7B:7A:5F:DF:F1:FA:42:73:EB
MD5 Fingerprint C6:6E:A0:42:93:98:60:AE:E2:1D:F4:FB:FC:D6:7F:86
Help
Close

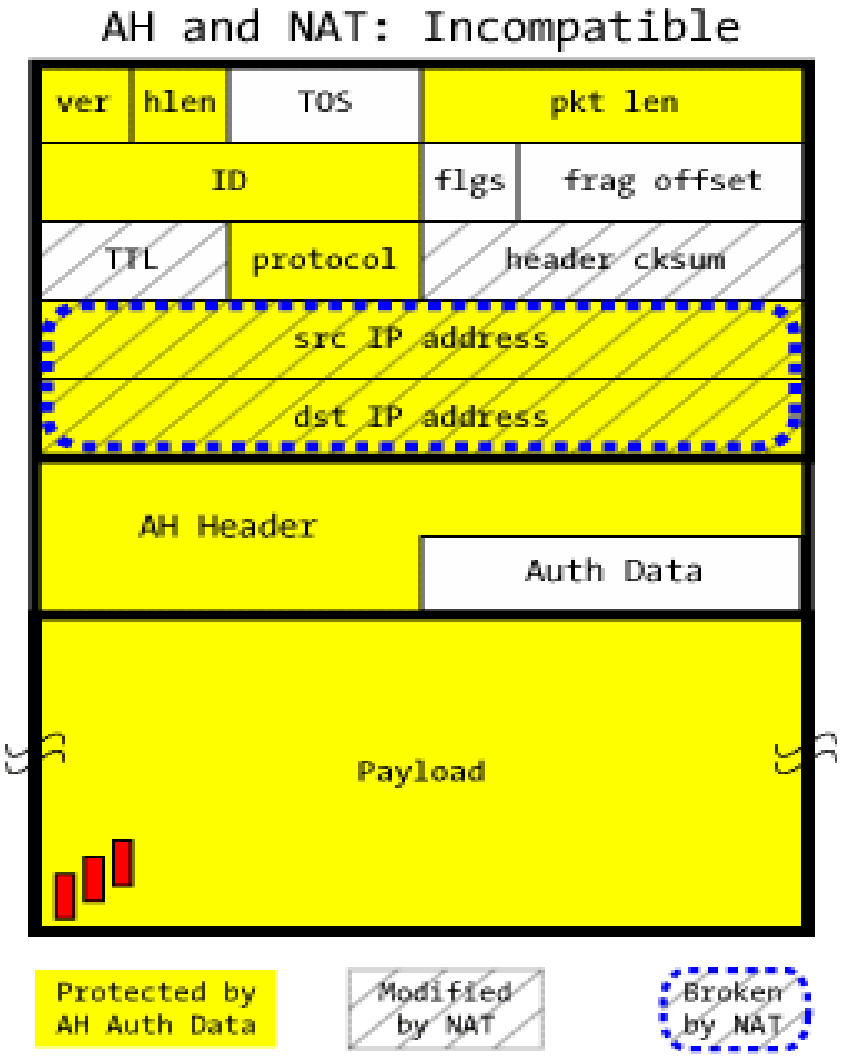
Comparison of IPSec & SSL

Comparisons...

- IPSec resides in the IP layer, SSL in the Application layer.
- The advantage of IPsec - elimination of overhead caused by each channel. SSL is one connection per one session type
- Disadvantage of ipsec - what if key was compromised.
- IPSec keys are exchanged over UDP (port 500 only).

Comparisons...

- SSL clients are not bound to a specific port as opposed to IPsec.
- IPsec suffers NAT traversal problem.
- NAT changes the source IP address, which is authenticated by AH.



Comparisons...

- IPsec doesn't integrate well among vendors. SSL is trouble free.
- IPsec has a high overhead in terms of header size(64 bytes, esp,ah tunnel mode) compared to SSL(21 bytes)
- SSL doesnt work with UDP, whereas IPsec avoids UDP problem by adding an IPsec header to the original packet's field

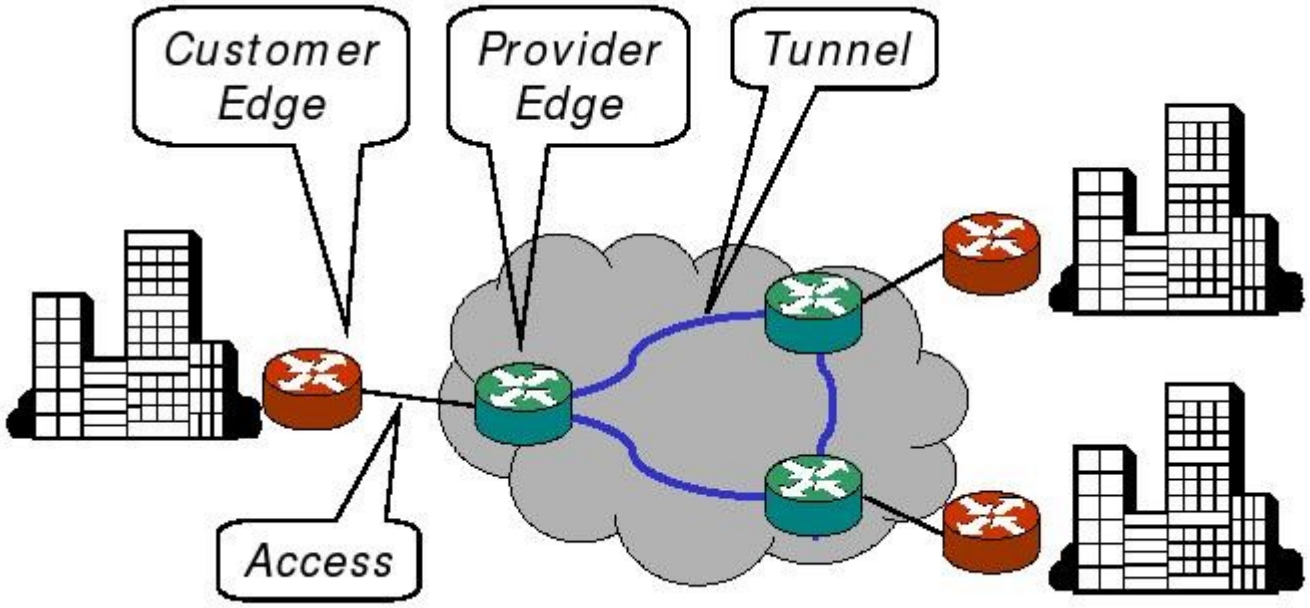
Conclusions...

	IPSec	SSL
Configuration	hard	easy
Client Authentication	must	optional
Pre-Shared Key	yes	no
Interoperability Problem	yes	no
TCP Support	all	some
UDP Support	yes	no
Compression Support	yes	OpenSSL only
HandShake Time	slow	fast

Trusted VPNs

- Do not use cryptographic tunnelling
- Rely on single provider's network to protect the traffic. Thus QoS comes into picture.
- Classified by OSI layer at which access network operates
  - Layer3VPN
    - IP Service, Routing relationship between PE and CE
  - Layer2VPN
    - Data link service, Ethernet MAC

Basic Structure



- Data arrives from CE via access network
- Encapsulated by PE & sent over tunnel
- Decapsulated by receiving PE & sent over access network to CE

Layer2 VPNs

- L2VPN forwards customer packets based on layer-2 (MAC address) information.
- Types
  - •VPWS
  - •VPLS

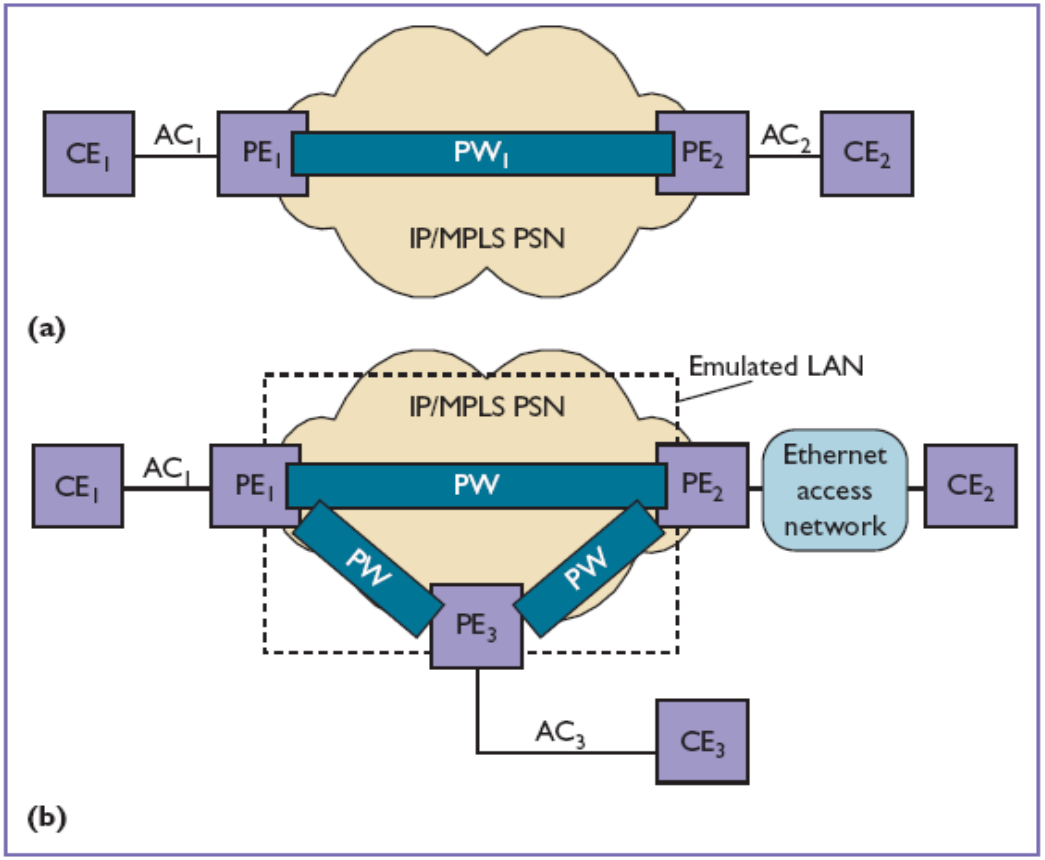


Figure 1. Layer-2 virtual private network (L2VPN) types. (a) A virtual private wire service (VPWS) supports point-to-point service. (b) A virtual private LAN service (VPLS) supports point-to-multipoint or multipoint service.

Layer3 VPNs

- L3VPN works on network layer.
- Two Headers
  - Tunnel Label
  - VPN Label

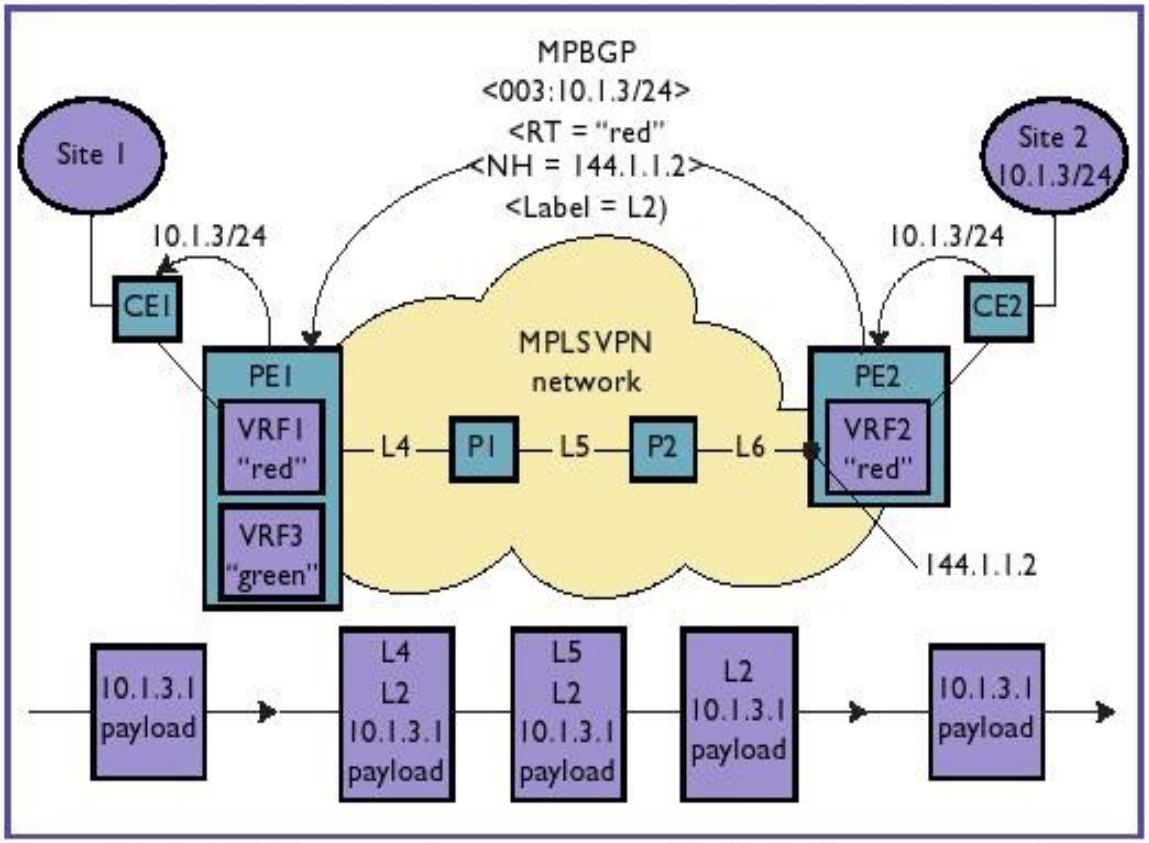
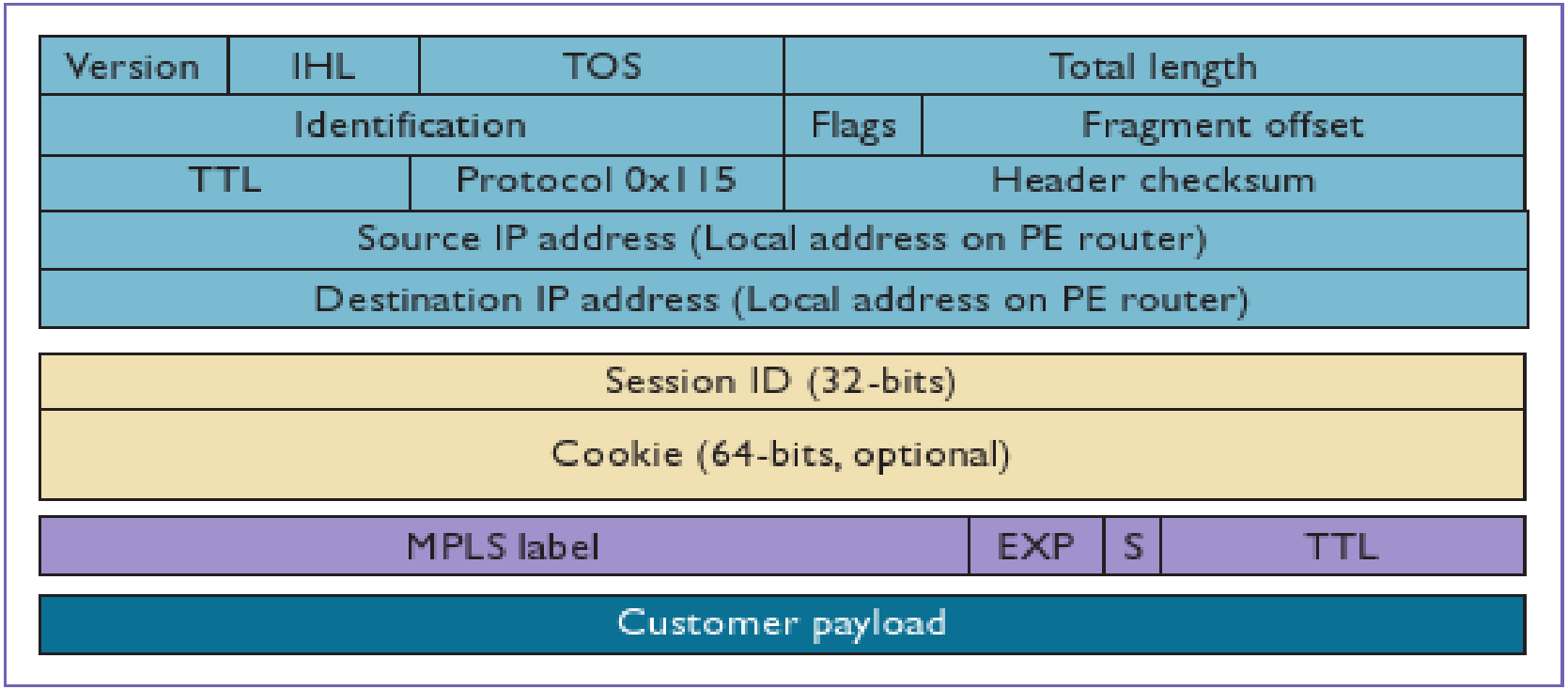


Figure 2. An MPLS virtual private network. MPBGP propagates VPN routes and labels between PEs. MPLS label switching is used to forward VPN data packets across the provider network.

MPLS



- MPLS-over-L2TPv3 encapsulation
- Not necessary for whole IP backbone to be MPLS compatible

VPN Toplogies

- The topology for a VPN consists of a set of nodes interconnected via tunnels.
- Types :
  - Full Mesh - tunnel exists between every pair of VPN edge devices.(Fig 1)
  - Hub and Spoke - single-spoke connectivity to a hub router at a central facility. (Fig 2)

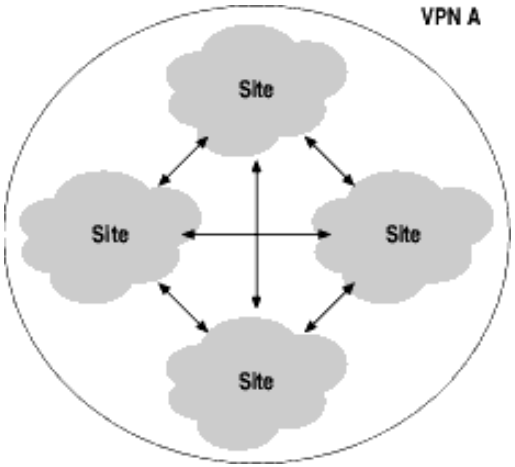


Fig1

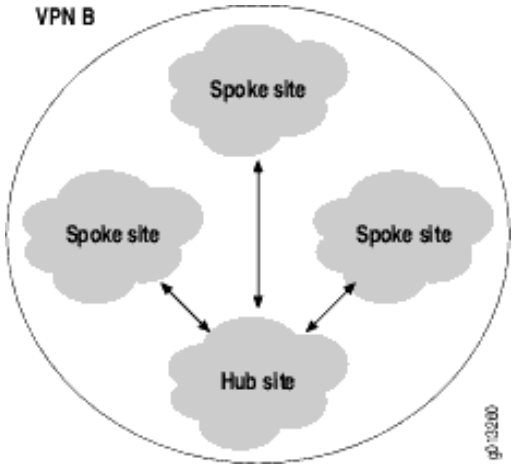
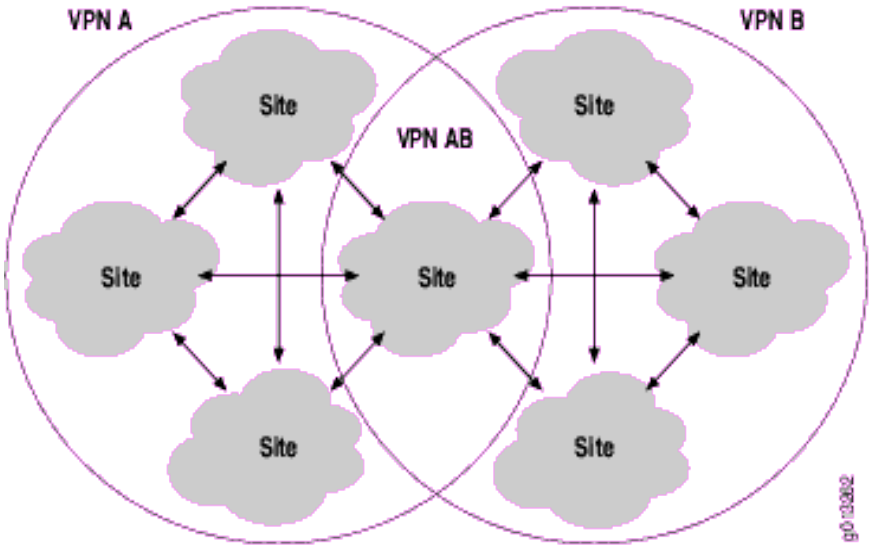


Fig2

VPN Toplogies (cont..)

- Using Partial Mesh :
  - reduce the number of tunnels
  - to force traffic through a firewall, or for monitoring or accounting purposes.



Disadvantages

- Potential pitfalls in the VPN model
  - VPNs require an in-depth understanding of public network security issues.
  - VPN technologies from different vendors may not work well together.
  - Can expose a company to potential security risks.
  - Scalability issues.

References

- C. Metz, “The Latest in Virtual Private Networks: Part I,”IEEE - 2003
- C. Metz, “The Latest in Virtual Private Networks: Part II,”IEEE - 2004
- B. Daugherty and C. Metz, “Multiprotocol Label Switching and IP,” IEEE - 2005
- A. Alshamsi, T Saito, “A Technical Comparison of SSL and IPsec,” IEEE – 2004
- http://www.ipsec-howto.org/ipsec-howto.pdf

Thanks

?