WSA - HW – 10 :

2. Describe the idea of the Secure Socket Tunneling Protocl (SSTP). Provide details and different scenarious.

Secure Socket Tunneling Protocol (SSTP) is a form of VPN tunnel that provides a mechanism to transport PPP or L2TP traffic through an SSL 3.0 channel. SSL provides transport-level security with key-negotiation, encryption and traffic integrity checking. The use of SSL over TCP port 443 allows SSTP to pass through virtually all firewalls and proxy servers except for authenticated web proxies.

SSTP servers must be authenticated during the SSL phase. SSTP clients can optionally be authenticated during the SSL phase, and must be authenticated in the PPP phase. The use of PPP allows support for common authentication methods, such as EAP-TLS and MS-CHAP.

SSTP is available for Linux, BSD, and Windows.The Mikrotik RouterOS also includes an SSTP client and server.

SoftEther VPN Server, a cross-platform open-source VPN server, also supports SSTP as one of its multi-protocol capability.

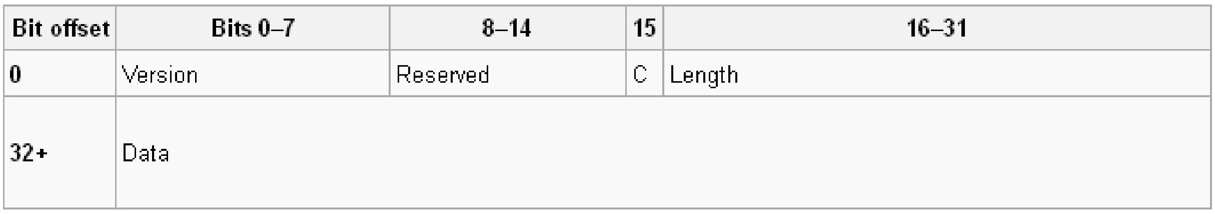
Similar functionality can be obtained by using open-source solutions like OpenVPN.

For Windows, SSTP is available on Windows Vista SP1 and later, in RouterOS, and in SEIL since its firmware version 3.50. It is fully integrated with the RRAS architecture in these operating systems, allowing its use with Winlogon or smart card authentication, remote access policies and the Windows VPN client. The protocol is also used by Windows Azure for Point-to-Site Virtual Network.

SSTP was intended only for remote client access, it generally does not support site-to-site VPN tunnels. The RouterOS version has no such restrictions.

SSTP suffers from the same performance limitations as any other IP-over-TCP tunnel. In general, performance will be acceptable only as long as there is sufficient excess bandwidth on the un-tunneled network link to guarantee that the tunneled TCP timers do not expire. If this becomes untrue, performance falls off dramatically. This is known as the "TCP meltdown problem"

The following header structure is common to all types of SSTP packets:



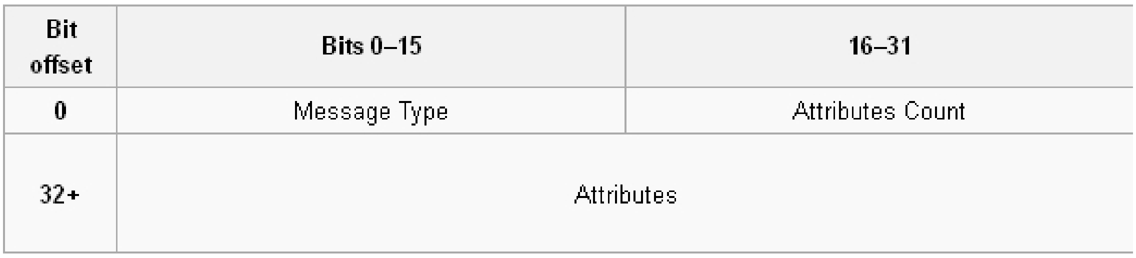
Bit offset	Bits 0–7	8–14	15	16–31
0	Version	Reserved	C	Length
32+	Data			

- Version (8 bits) – communicates and negotiates the version of SSTP that is used.
- Reserved (7 bits) – reserved for future use.
- C (1 bit) – Control bit indicating whether the SSTP packet represents an SSTP control packet or an SSTP data packet. This bit is set if the SSTP packet is a control packet.
- Length (16 bits) – packet length field, composed of two values: a Reserved portion and a Length portion.

    - Reserved (4 bits) – reserved for future use.
    - Length (12 bits) – contains the length of the entire SSTP packet, including the SSTP header.

- Data (variable) – when Control bit C is set, this field contains an SSTP control message. Otherwise, the data field would contain a higher level protocol. At the moment, this can only be PPP.

The data field of the SSTP header contains an SSTP control message only when the header's Control bit C is set.



Bit offset	Bits 0–15	16–31
0	Message Type	Attributes Count
32+	Attributes	

- Message Type (16 bits) – specifies the type of SSTP control message being communicated. This dictates the number and types of attributes that can be carried in the SSTP control packet.
- Attributes Count (16 bits) – specifies the number of attributes appended to the SSTP control message.
- Attributes (variable) – contains a list of attributes associated with the SSTP control message. The number of attributes is specified by the Attributes Count field.

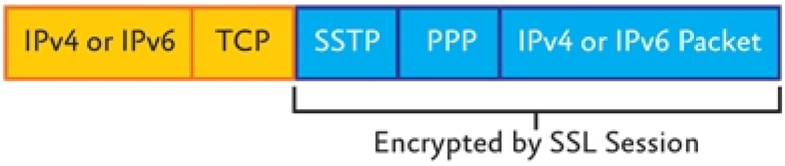
How SSTP Works

When a user on a computer running Windows Server 2008 or Windows Vista Service Pack 1 initiates an SSTP-based VPN connection, the following occurs:

1. The SSTP client establishes a TCP connection with the SSTP server between a dynamically-allocated TCP port on the client and TCP port 443 on the server.
2. The SSTP client sends an SSL Client - Hello message, indicating that the client wants to create an SSL session with the SSTP server.
3. The SSTP server sends its computer certificate to the SSTP client.
4. The SSTP client validates the computer certificate, determines the encryption method for the SSL session, generates an SSL session key and then encrypts it with the public key of the SSTP server’s certificate.
5. The SSTP client sends the encrypted form of the SSL session key to the SSTP server.

6. The SSTP server decrypts the encrypted SSL session key with the private key of its computer certificate. All future communication between the SSTP client and the SSTP server is encrypted with the negotiated encryption method and SSL session key.
7. The SSTP client sends an HTTP over SSL request message to the SSTP server.
8. The SSTP client negotiates an SSTP tunnel with the SSTP server.
9. The SSTP client negotiates a PPP connection with the SSTP server. This negotiation includes authenticating the user’s credentials with a PPP authentication method and configuring settings for IPv4 or IPv6 traffic.
10. The SSTP client begins sending IPv4 or IPv6 traffic over the PPP link.

The next figure shows the structure of IPv4 or IPv6 packets that are sent over an SSTP-based VPN connection.



Structure of SSTP packets

An IPv4 or IPv6 packet is first encapsulated with a PPP header and an SSTP header. The combination of the IPv4 or IPv6 packet, the PPP header, and the SSTP header is encrypted by the SSL session. A TCP header and an IPv4 header (for SSTP connections across the IPv4 Internet) or an IPv6 header (for SSTP connections across the IPv6 Internet) are added to complete the packet.

For more information about SSTP, see the Routing and Remote Access Blog at :

http://blogs.technet.com/b/rrasblog

More info about SSTP and VPN Tunneling Protocols:

http://technet.microsoft.com/en-us/library/cc771298%28v=ws.10%29.aspx