# STUDENT ACTIVITY 3.4_KEY: PROTOCOL SECURITY

MTA Course: 98-367 Security Fundamentals
Lesson name: Protocol Security 3.4
Topic: Understand Protocol Security
File name: SecurityFund_SA_3.4_Key

## Lesson Objective

**3.4:** Understand protocol security. *This objective may include, but is not limited to:* protocol sniffing, tunneling, DNSsec, network sniffing, common attack methods.

## Resources, software, and additional files needed for this lesson

- Internet access
  *http://technet.microsoft.com/en-us/library/dd469817(WS.10).aspx*

## Directions to the student

Answer the following question.

## Content

### Choosing Between Tunneling Protocols

What factors should be considered when choosing between PPTP, L2TP/IPsec, SSTP, and IKEv2 remote access VPN solutions?

**a.** PPTP

**b.** L2TP/IPsec

**c.** SSTP

**d.** IKEv2

**Answers:**

**a.** PPTP can be used with a variety of Microsoft® clients, including Microsoft Windows® 2000 and later versions of Windows. Unlike L2TP/IPsec and IKEv2, PPTP does not require the use of a public key infrastructure (PKI). By using encryption, PPTP-based VPN connections provide data confidentiality (captured packets cannot be interpreted without the encryption key). PPTP-based VPN connections, however, do not provide data integrity (proof that the data was not modified in transit) or data origin authentication (proof that the data was sent by the authorized user).

**b.** L2TP can be used with client computers running Windows 2000 and later versions of Windows. L2TP supports either computer certificates or a preshared key as the authentication method for IPsec. Computer certificate authentication, the recommended authentication method, requires a PKI to issue computer certificates to the VPN server computer and all VPN client computers. By using IPsec, L2TP/IPsec VPN connections provide data confidentiality, data integrity, and data authentication.
Unlike PPTP and SSTP, L2TP/IPsec enables machine authentication at the IPsec layer and user level authentication at the PPP layer.

**c.** SSTP can be used only with client computers running Windows Vista® Service Pack 1 (SP1), Windows Server® 2008 R2, and later versions of Windows. By using SSL, SSTP VPN connections provide data confidentiality, data integrity, and data authentication.

**d.** IKEv2 is supported only on computers running Windows 7 and Windows Server 2008 R2. By using IPsec, IKEv2 VPN connections provide data confidentiality, data integrity, and data authentication. IKEv2 supports the latest IPsec encryption algorithms. Because of its support for mobility (MOBIKE), it is much more resilient to changing network connectivity, making it a good choice for mobile users who move between access points and even switch between wired and wireless connections.