




# Chapter 6 - Key Terms

 Term	 Page	 Description
<u>Internet Key Exchange (IKE).</u>	582	Protocol used by IPsec to negotiate & establish secured site-to-site remote-access VPN tunnels. IKE is a framework provided by the Internet Security Association and Key Management Protocol (ISAKMP) and parts of two other key management protocols: namely, Oakley and Secure Key Exchange Mechanism (SKEME).
<u>Diffie-Hellman (DH).</u>	580	A key agreement protocol that enables two users or devices to authenticate each other's pre-shared keys without actually sending the keys over an unsecured medium.
<u>IKEv1 vs. IKv2</u>	582	There are two versions of the IKE protocol (IKEv1 and IKEv2). <b>Phase 1</b> - IKEv1 Phase 1 has two possible exchanges: main mode and aggressive mode. There is a single exchange of a message pair for IKEv2 IKE_SA. <b>Phase 2</b> - IKEv2 has a simple exchange of two message pairs for the CHILD_SA. IKEv1 uses an exchange of at least three message pairs for Phase 2.