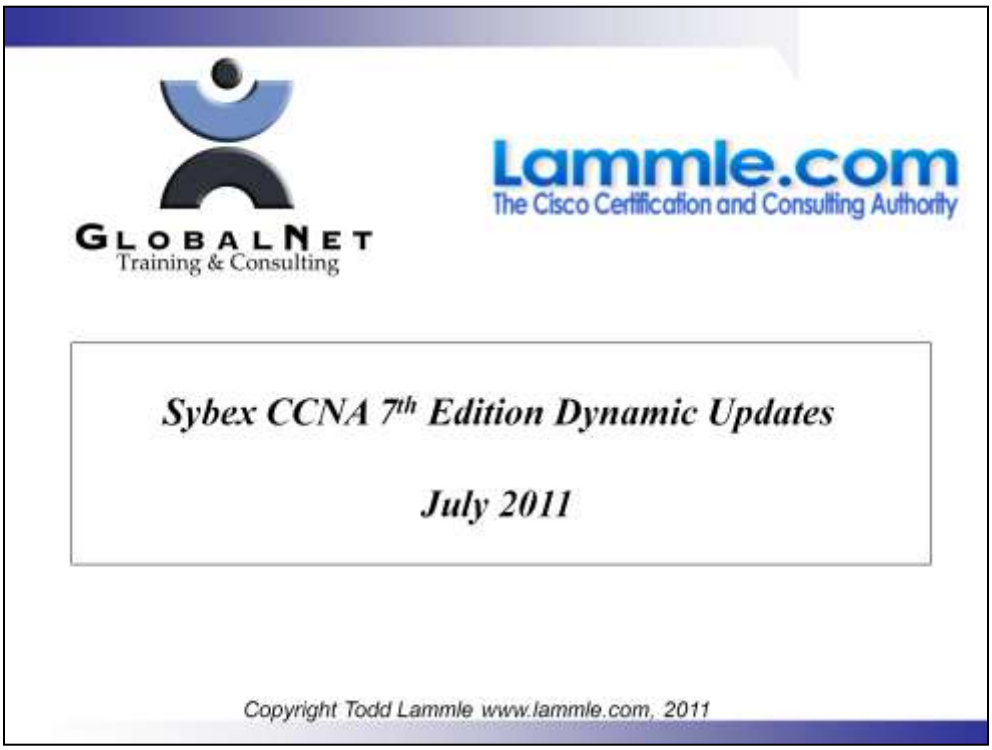
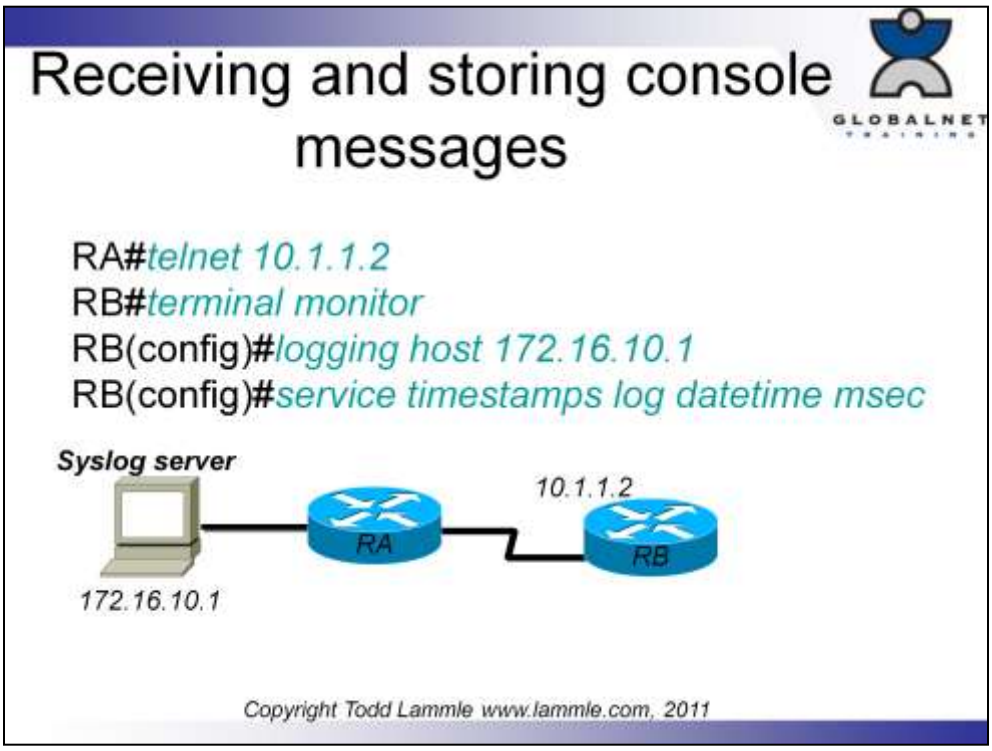

GLOBALNET
Training & Consulting
Lammle.com
The Cisco Certification and Consulting Authority
Sybex CCNA 7th Edition Dynamic Updates
July 2011
Copyright Todd Lammle www.lammle.com, 2011



If you telnet or SSH to a device, you will not receive console messages by default. To receive console messages, such as debug output, use the command:

#**terminal monitor**

from privileged exec mode

To send console messages to a syslog server from a router or switch, use the command:

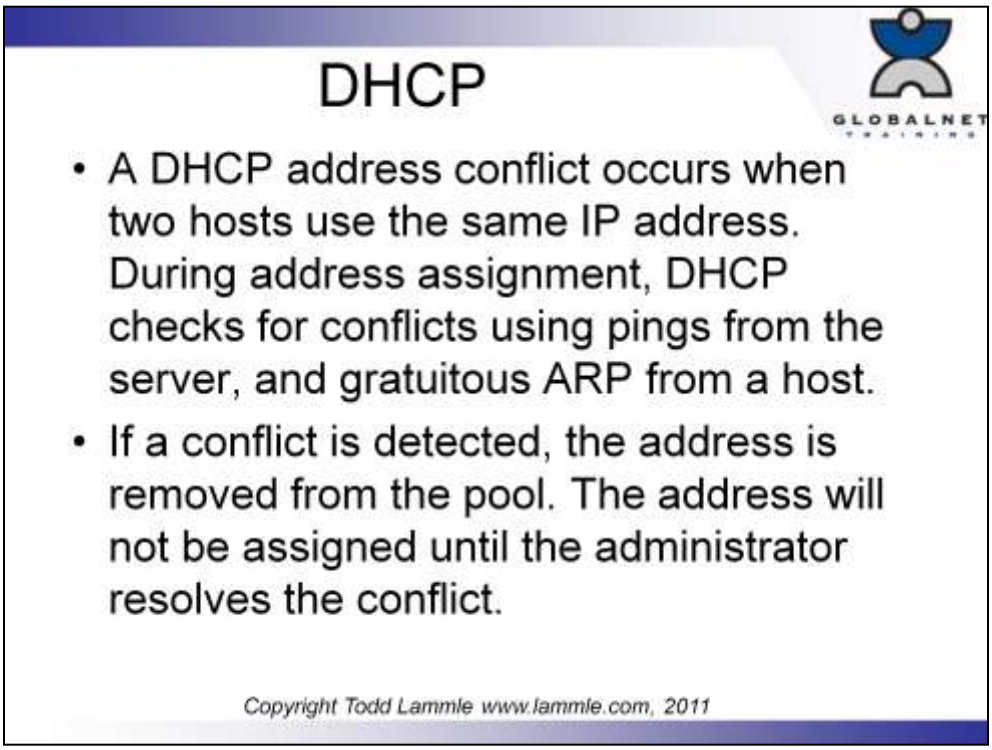
config t

logging host 1.2.3.4

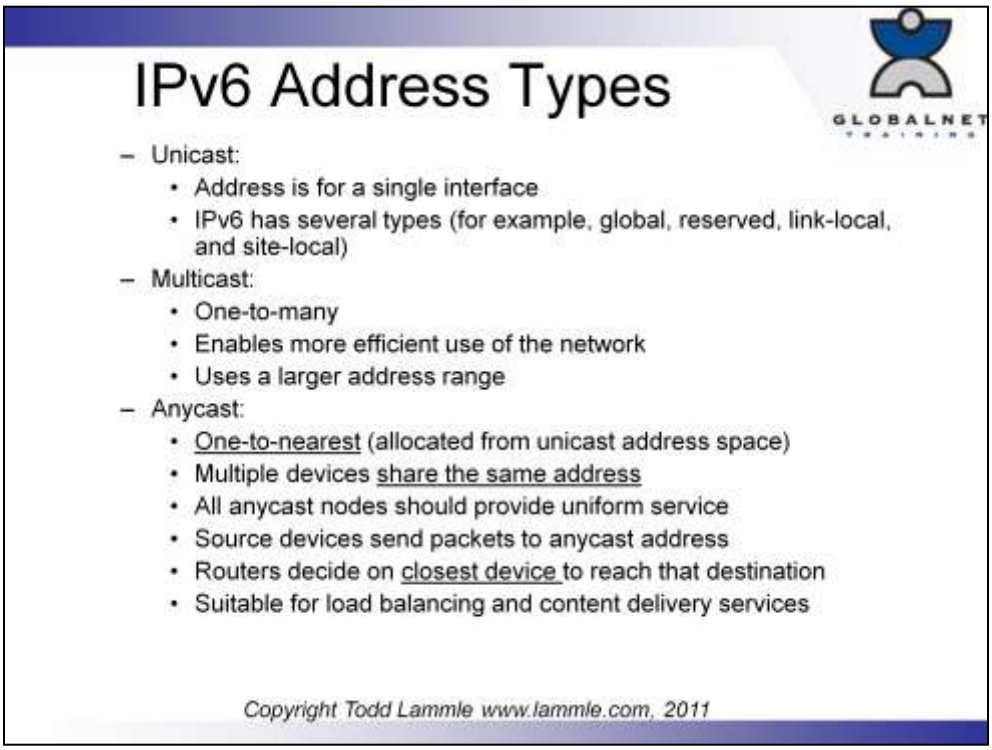
Determine the timing of various events, relative to each other when you are debugging a complicated router issue with the command:

config t

service timestamps log datetime msec



DHCP is covered in detail in pages 94-96 in my CCNA 7th Edition study guide. This slide was just to bring your attention to the fact that you need to read those pages!



RIPng is assigned on an interface, not global config, and uses the IPv6 address ff02::9 to send route updates

The EUI-64 format inserts the FFFE in the middle of the 48 bits of the MAC address

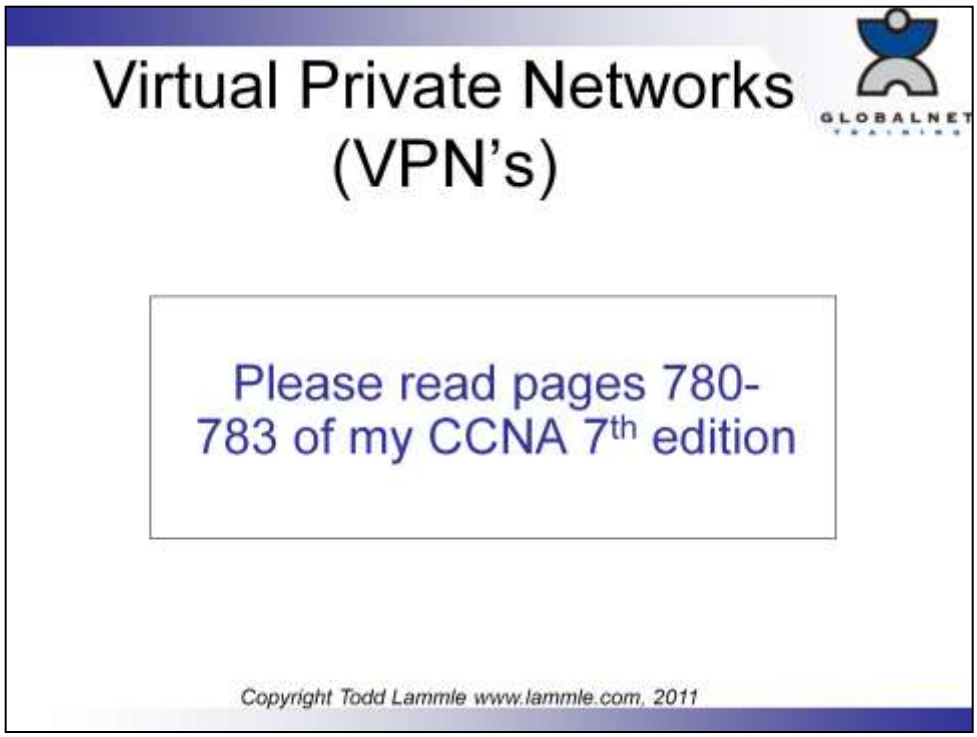
IPv6 provides no broadcasting, auto-configuration, and is considered plug & play

The best alternative to this IPv6 address:
B514:82C3:0000:0000:0029:EC7A:0000:EC72

“B514:82C3::29:EC7A:0:EC72”

This is covered in my Sybex CCNA 7th Edition, I am just trying to bring this command to your attention. Please read about this command on page 477.

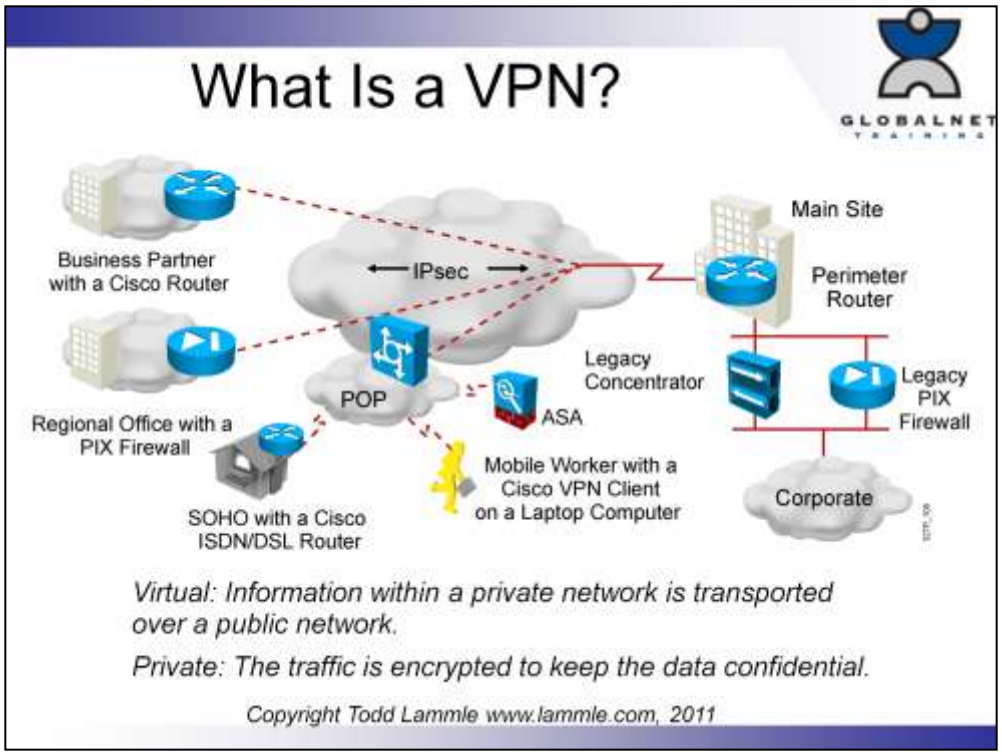
What would you say about adding a new RID for the router right under the router ospf *process-id* command instead? I'd say let's give it a shot! This slide is an example of doing that on the R3 router used in my books lab.



I'd be pretty willing to bet you've heard the term *VPN* more than once before – especially if you read pages 780-783 of my new Sybex CCNA 7th edition study guide! I need to make sure you have read this section, so let's do a review.

Maybe you even know what one is, but just in case, a *virtual private network (VPN)* allows the creation of private networks across the Internet, enabling privacy and tunneling of non-TCP/IP protocols.

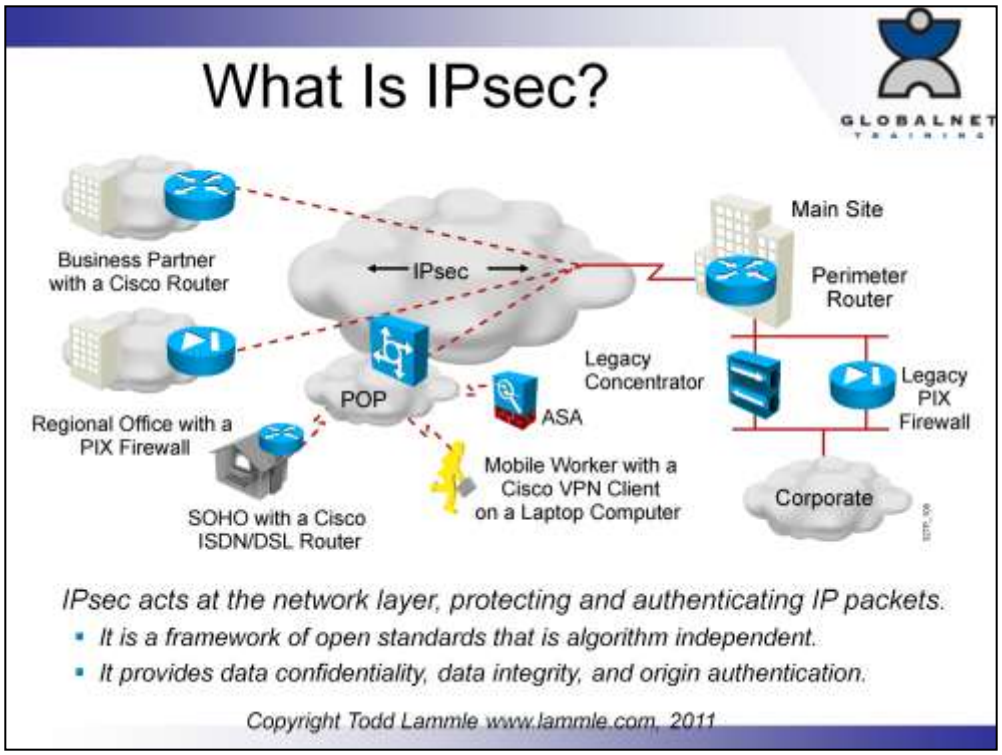
VPNs are used daily to give remote users and disjointed networks connectivity over a public medium like the Internet instead of using more expensive permanent means.



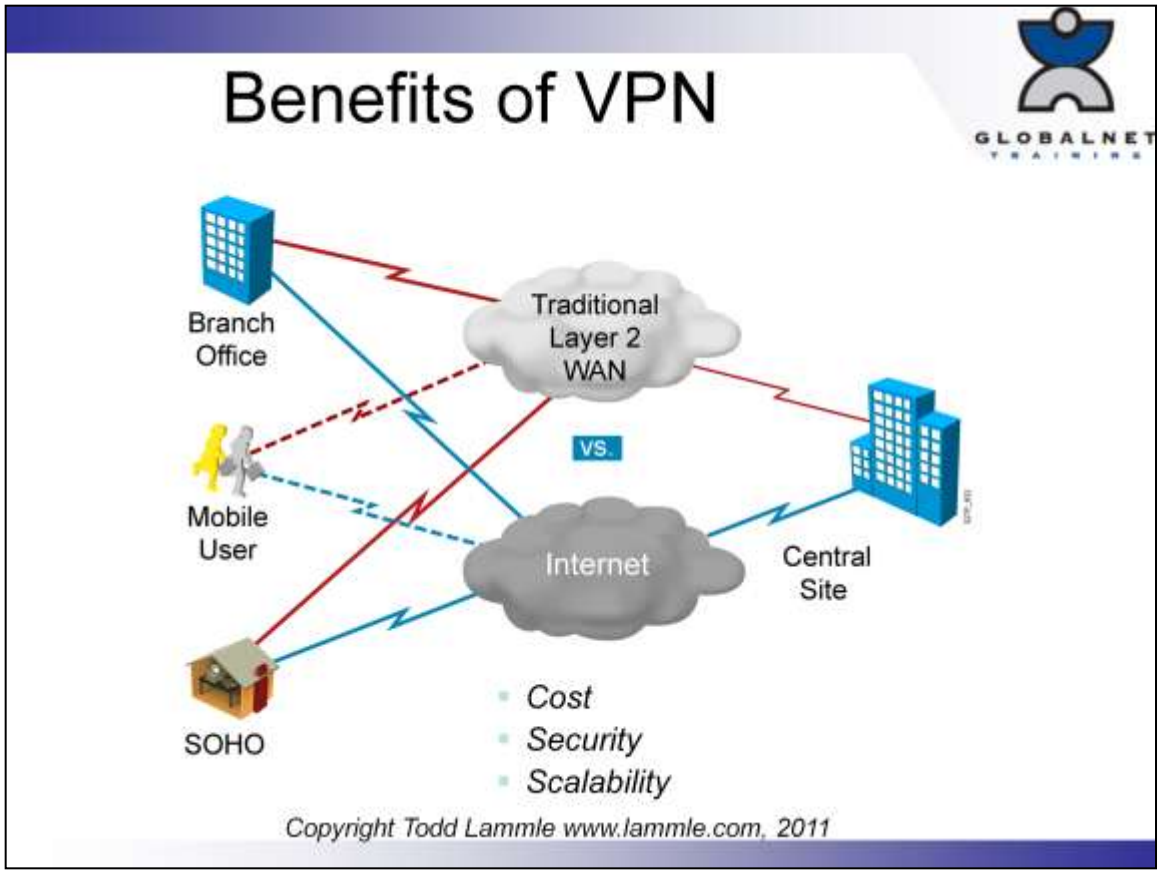
IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as other PIX or ASA Firewalls, Cisco routers, VPN 3000 Concentrator Series, Cisco Secure VPN Client, and other IPsec-compliant products.

IPsec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers at the IP layer. IPsec encompasses a suite of protocols. It is not bound to any specific encryption or authentication algorithms, key generation technique, or security association. IPsec supplies the rules while existing algorithms provide the encryption, authentication, key management, and so on. In this way, IPsec can allow the use of updated algorithms and key techniques

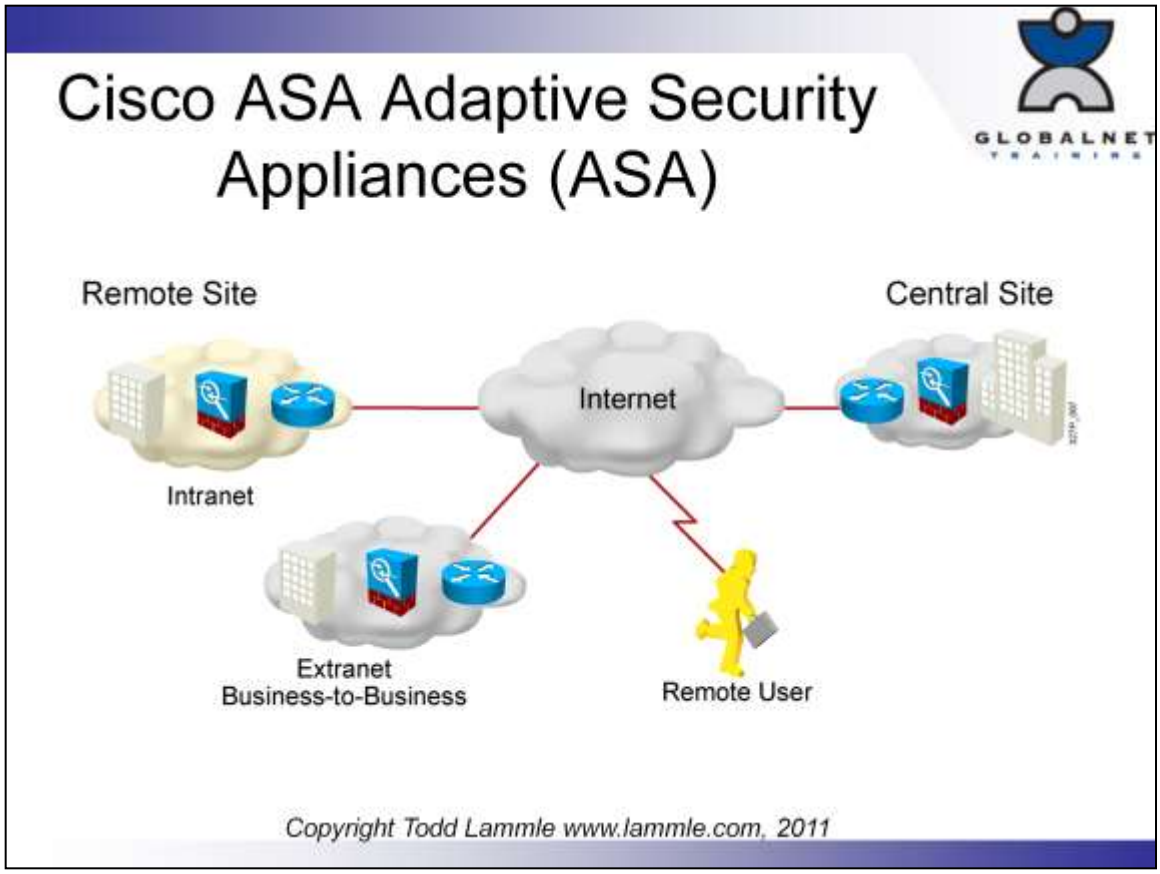
without patching the IPsec protocol. In this topic, we'll discuss how those open standards provide data confidentiality, integrity, and authentication.



IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as other PIX Firewalls, Cisco routers, VPN 3000 Concentrator Series, Cisco Secure VPN Client, and other IPsec-compliant products. IPsec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers at the IP layer. IPsec encompasses a suite of protocols. It is not bound to any specific encryption or authentication algorithms, key generation technique, or security association. IPsec supplies the rules while existing algorithms provide the encryption, authentication, key management, and so on.



The first VPN solution is remote access. Remote access is targeted to mobile user and Home telecommuters. Most people have access to the Internet from there homes, why not take advantage of it. In the past, corporations supported remote users via dial-in networks. This typically necessitated a toll, or 1-800, call to access the corporation. With the advent of VPNs, a mobile user can make a local call to their ISP to access corporation via Internet wherever they may be. It is an evolution of dial networks. Remote access VPN can support the needs of telecommuters, mobile users, extranet consumer-to-business, and so on.



Firewall is inherently a site-to-site solution. ASA Firewall is a key element in the overall Cisco end-to-end security solution. The ASA Firewall is a dedicated hardware and software security solution that delivers high security without impacting network performance. Firewall-based VPN solutions are not a technical issue but a security issue. The question is “who manages the VPN network”. If security manages the VPN, ASA may be VPN solution of choice. Customer may wish to enhance their existing Firewall equipment to support VPN services. Firewall based VPN solutions support intranet and extranet applications.

In VPN, the framework of open standards provides three critical functions: confidentiality, data integrity, and authentication.

Confidentiality (Encryption)

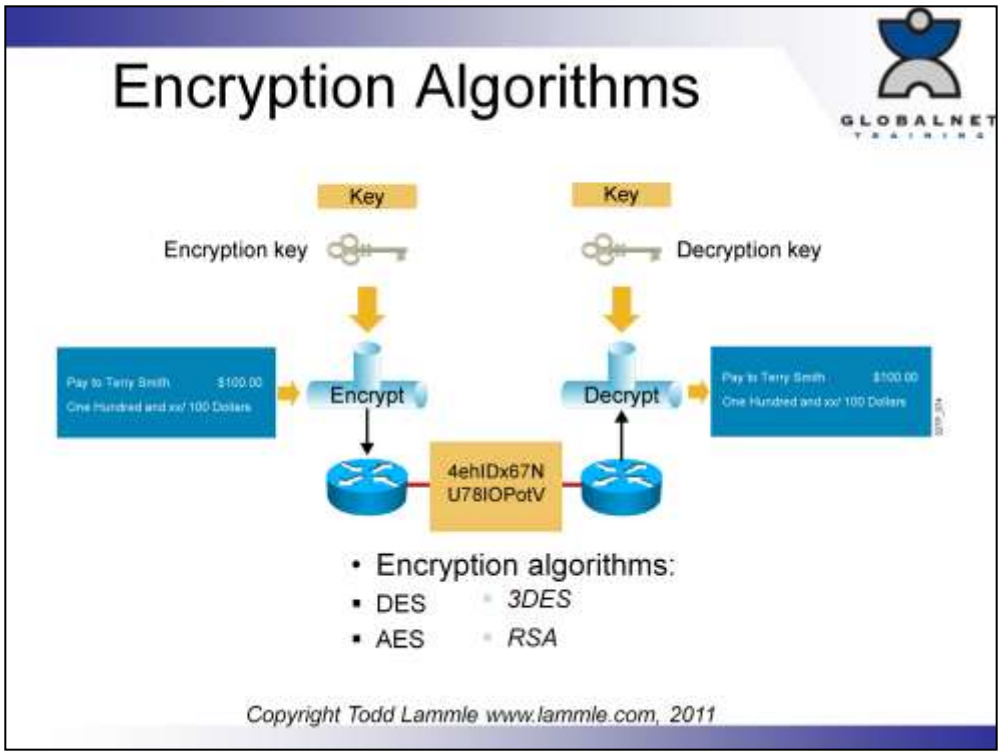
The sender can encrypt the packets before transmitting them across a network. By doing so, no one can eavesdrop on the communication If intercepted, the communications can not be read.

Data Integrity

The receiver can verify the data was transmitted through the Internet without being changed or altered in anyway.

Origin Authentication

The receiver can authenticate the source of the packet. Can guarantee, certify, the source of the information



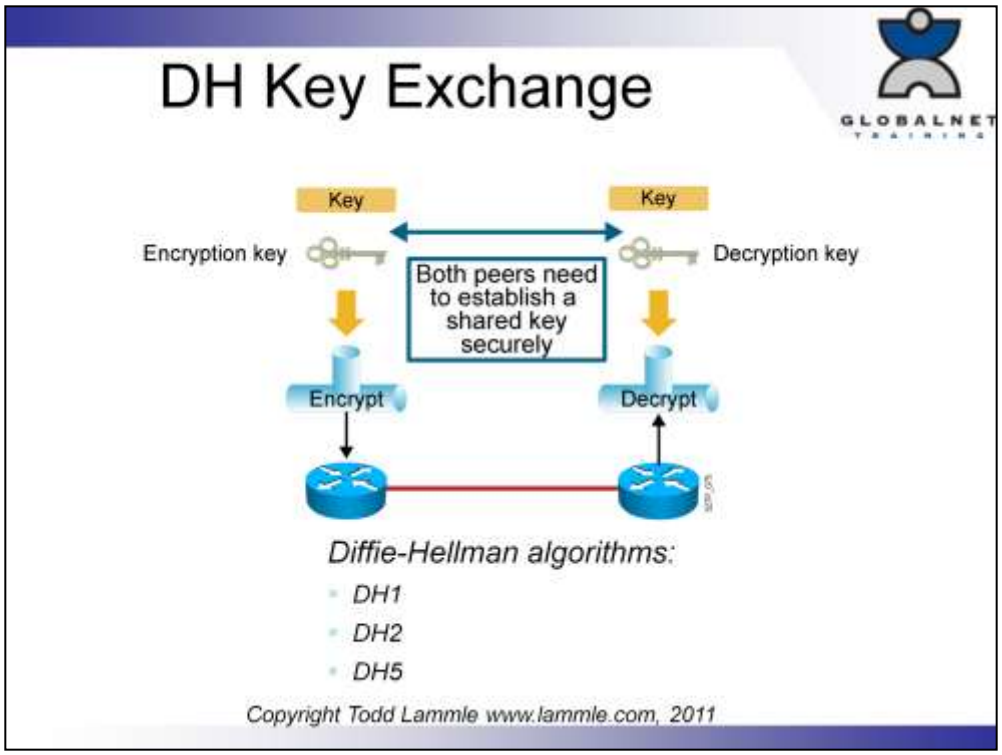
Degree of security is dependent on the length of the key. If one were to try and hack the key through a brute force attack, guessing every possible combination, the number of possibilities is a function of the length of the key. The time to process all the possibilities is a function of the computing power of the computer. Therefore, the shorter the key, the easier it is to break. A 64 bit key with a relatively sophisticated computer can take approximately 1 year to break. A 128 bit key with the same machine can take roughly 10e19 years to decrypt.

Some of the encryption algorithms are as follows:

DES Algorithm –DES was developed by IBM. DES uses a 56-bit key, ensuring high performance encryption. DES is a symmetric key cryptosystem.

Triple DES Algorithm (3DES) - The 3DES algorithm is a variant of the 56-bit DES. 3DES operates similarly to DES, in that data is broken into 64-bit blocks. 3DES then processes each block three times, each time with an independent 56-bit key. 3DES effectively doubles encryption strength over 56-bit DES. DES is a symmetric key cryptosystem

RSA – RSA is a asymmetrical key cryptosystem. It uses a key length of 512, 768, 1024, or larger. RSA is used for encryption or digital signatures. In software, DES is up to 100 times faster than RSA. We'll talk about digital signatures later in this topic.



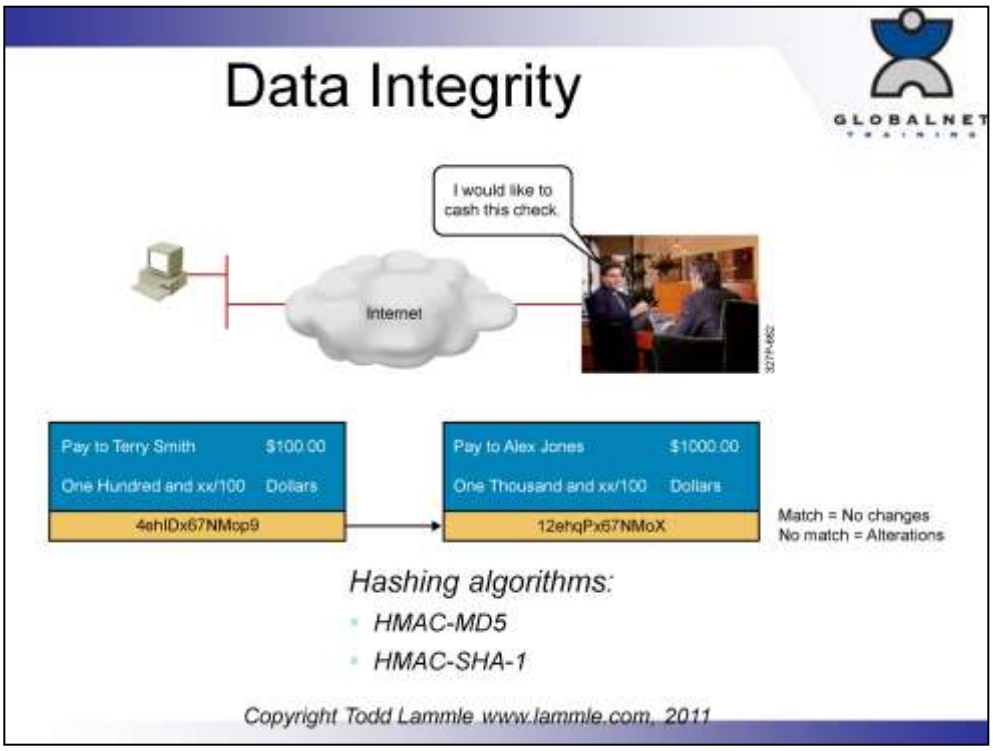
Degree of security is dependent on the length of the key. If one were to try and hack the key through a brute force attack, guessing every possible combination, the number of possibilities is a function of the length of the key. The time to process all the possibilities is a function of the computing power of the computer. Therefore, the shorter the key, the easier it is to break. A 64 bit key with a relatively sophisticated computer can take approximately 1 year to break. A 128 bit key with the same machine can take roughly 10e19 years to decrypt.

Some of the encryption algorithms are as follows:

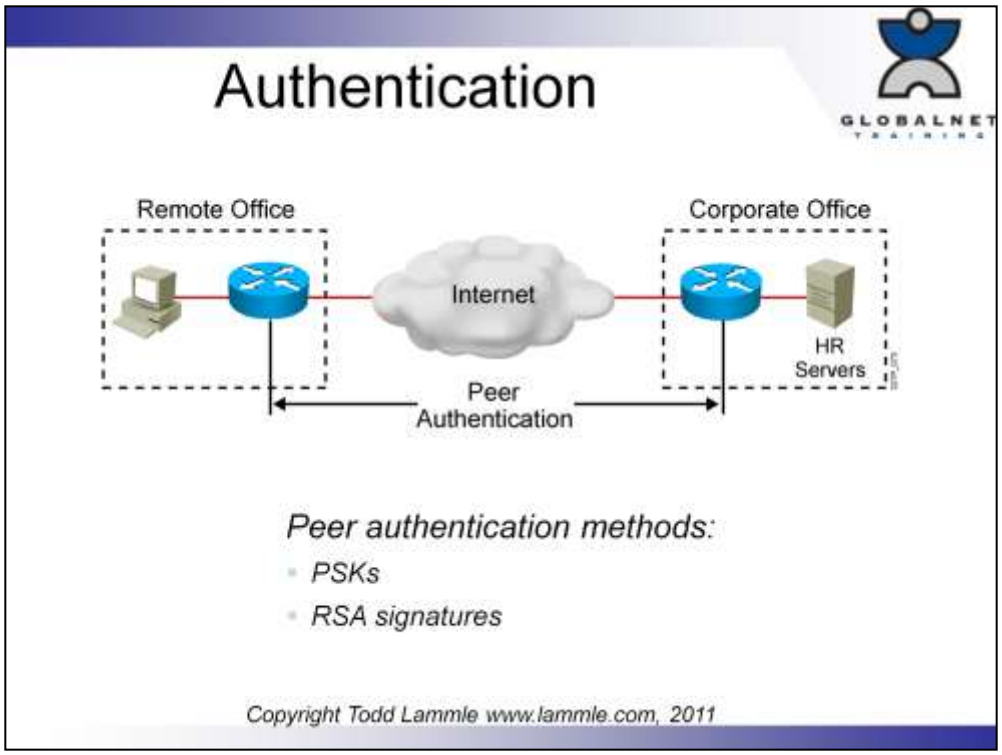
DES Algorithm –DES was developed by IBM. DES uses a 56-bit key, ensuring high performance encryption. DES is a symmetric key cryptosystem.

Triple DES Algorithm (3DES) - The 3DES algorithm is a variant of the 56-bit DES. 3DES operates similarly to DES, in that data is broken into 64-bit blocks. 3DES then processes each block three times, each time with an independent 56-bit key. 3DES effectively doubles encryption strength over 56-bit DES. DES is a symmetric key cryptosystem

RSA – RSA is a asymmetrical key cryptosystem. It uses a key length of 512, 768, 1024, or larger. RSA is used for encryption or digital signatures. In software, DES is up to 100 times faster than RSA. We'll talk about digital signatures later in this topic.



The next VPN critical function is data integrity. VPN data is transported over the public Internet. Potentially, this data could be intercepted, and modified. To guard against this from happening, each message has a hash attached to the message. A hash guarantees the integrity of the original message. If the transmitted hash matches the received hash, the message has not been tampered with. However, if there is no match, the message was altered.

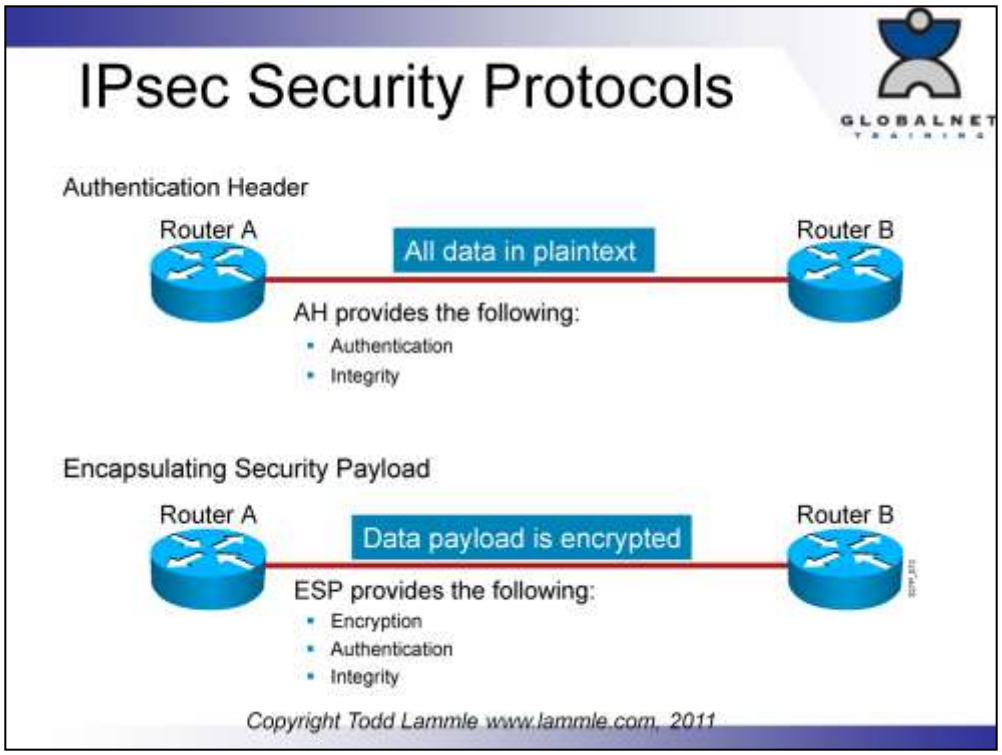


When conducting business long distance, its necessary to know who is at the other end of the phone, email, or FAX. The same is true of VPN networking. The device on the other end of the VPN tunnel must be authenticated before the communications path is considered secure. There are three data origin authentication methods:

• Pre-shared Keys – A secret key value entered into each peer manually used to authenticate the peer.

• RSA Signatures – Use the exchange of digital certificates to authenticate the peers

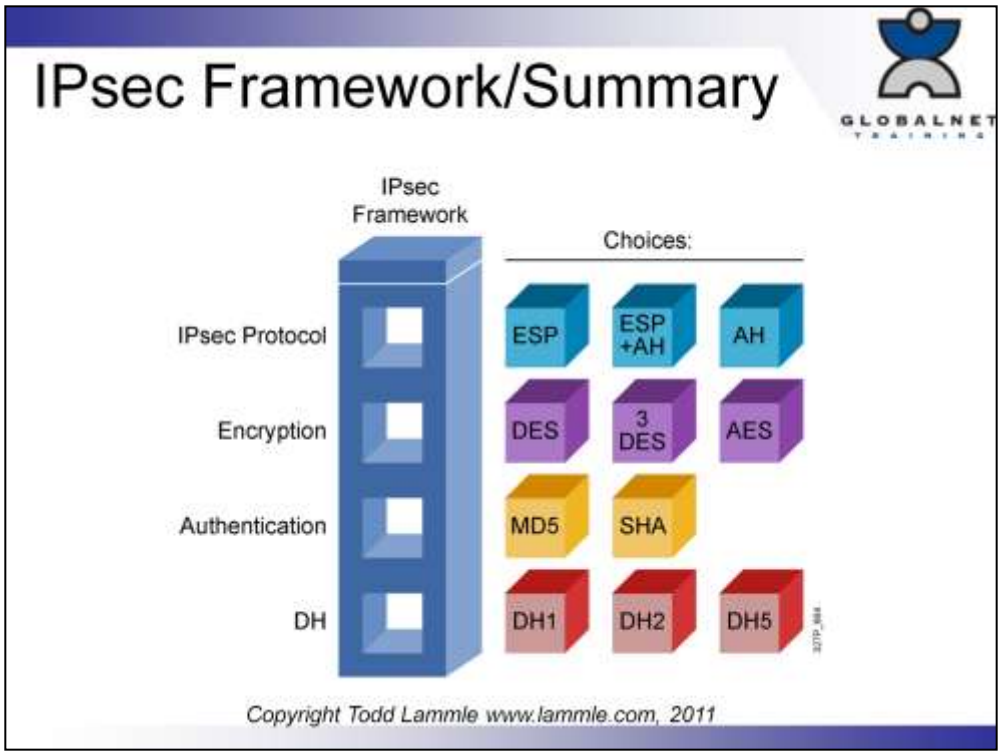
• RSA Encrypted Nonces – Nonces (a random number generated by each peer) are encrypted then exchanged between peers. The two nonces are used during peer authentication process.



IPsec consists of the following two main protocols:

Authentication Header (AH) provides data authentication and integrity for IP packets passed between two systems. It is a means of verifying any message passed from Router A to B has not been modified during transit. All text is transported in the clear. AH does not provide data confidentiality (encryption) of packets.

Encapsulating Security Payload (ESP) is a security protocol used to provide confidentiality (encryption), data origin authentication, integrity, and optional anti-replay service. ESP provides confidentiality by performing encryption at the IP packet layer. All ESP traffic is encrypted between Router A and B.



- HMAC-SHA-1 and RSA are two data integrity algorithms are commonly

used in vpn solutions

- When confidentiality is required the Encapsulating Security Payload (ESP) IPSec security protocol should be used

- You would install a Cisco Adaptive Security Appliance at a branch office to enable and mange an IPsec site-to-site VPN

- The Data Integrity component of VPN technology will ensure that data is unaltered between the sender and recipient

- The IPSec protocol suite is an open standard protocol framework that is commonly used in VPN's, to provide secure end-to-end connections

- The Authentication component of VPN technology ensures that data can be read only by its intended recipient