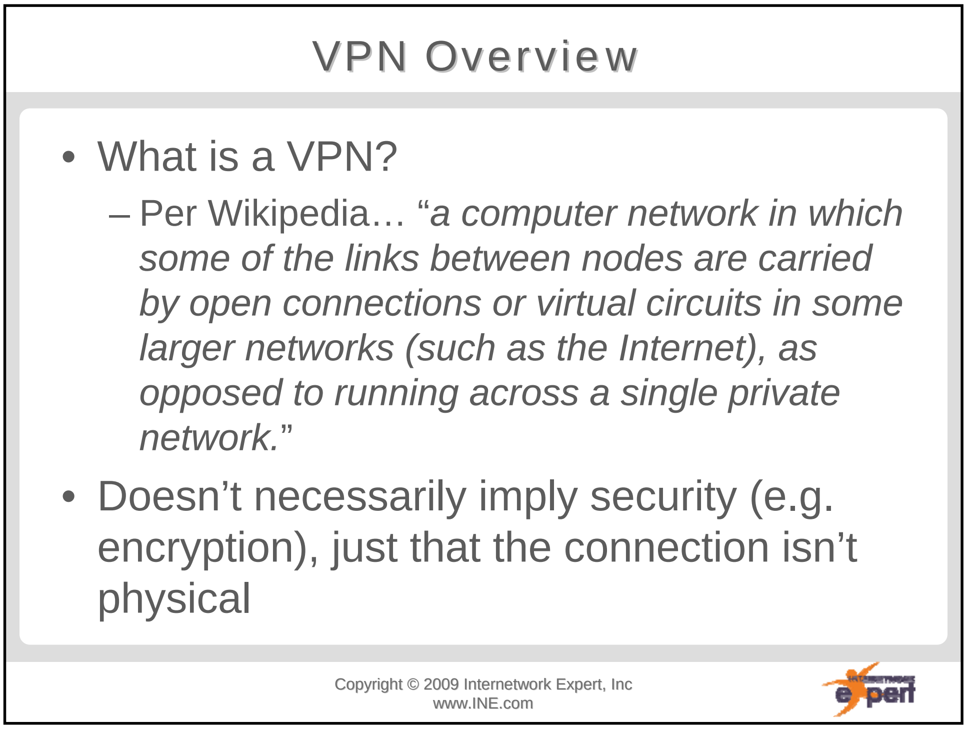
Implementing Secure Converged Wide Area Networks (ISCW)

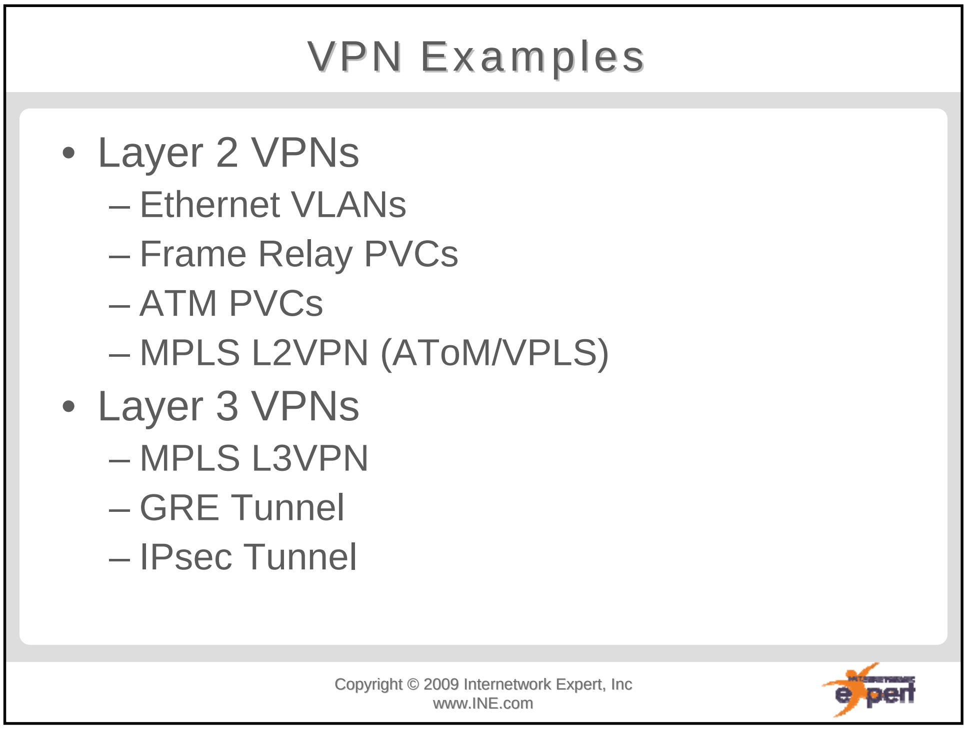
IPsec VPNs

http://www.INE.com



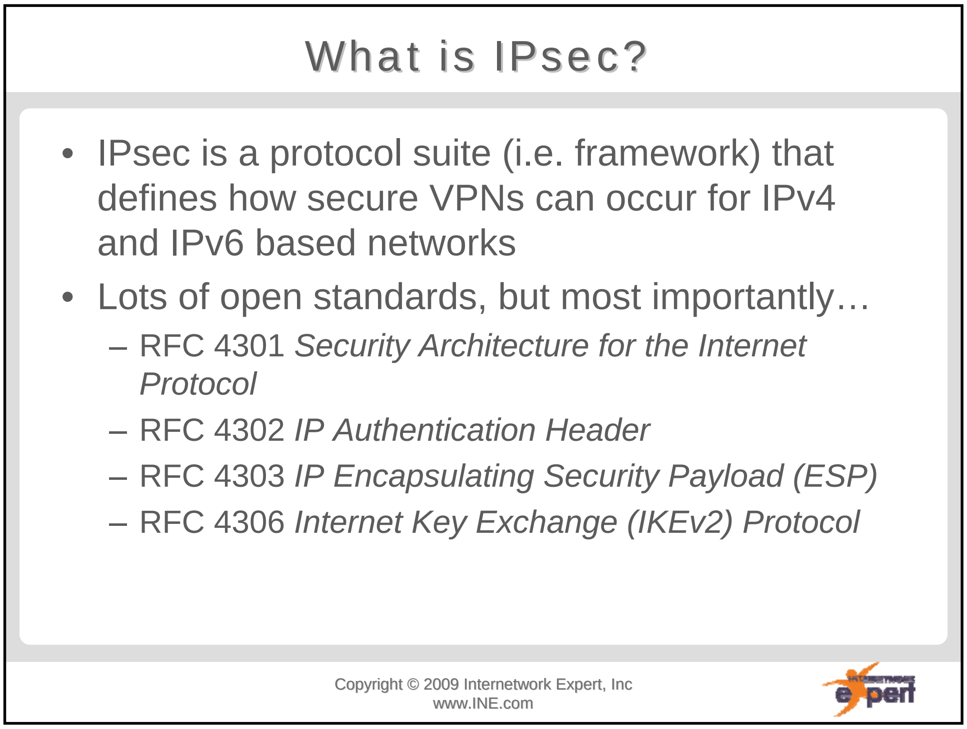
VPN Overview

- What is a VPN?
  - Per Wikipedia… "*a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger networks (such as the Internet), as opposed to running across a single private network.*"
- Doesn't necessarily imply security (e.g. encryption), just that the connection isn't physical



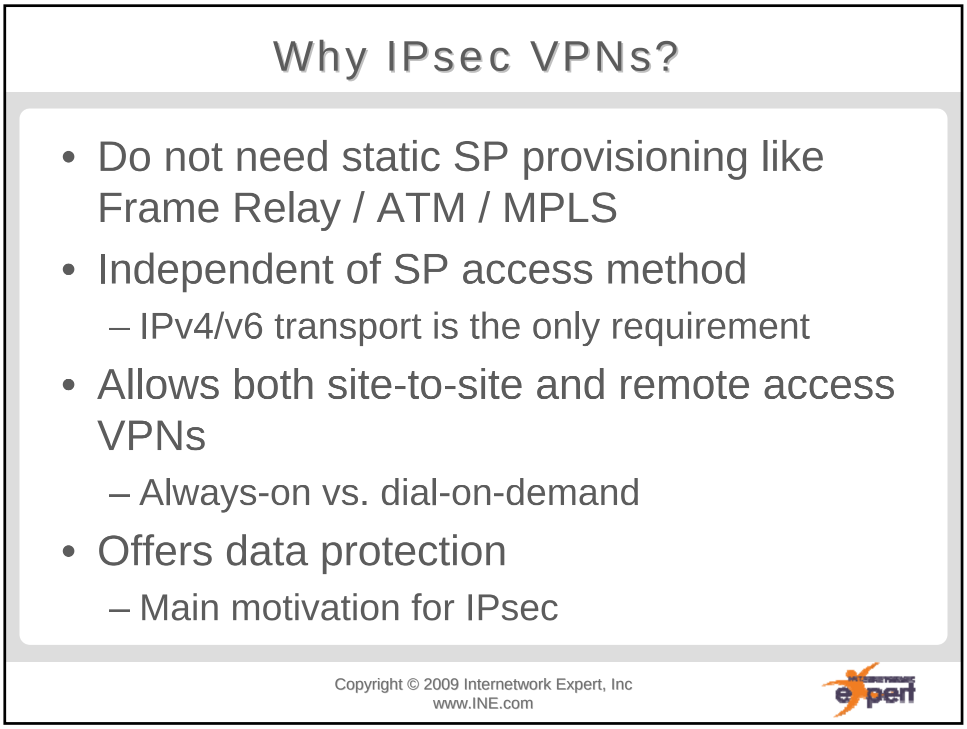
VPN Examples

- Layer 2 VPNs
  - Ethernet VLANs
  - Frame Relay PVCs
  - ATM PVCs
  - MPLS L2VPN (AToM/VPLS)
- Layer 3 VPNs
  - MPLS L3VPN
  - GRE Tunnel
  - IPsec Tunnel



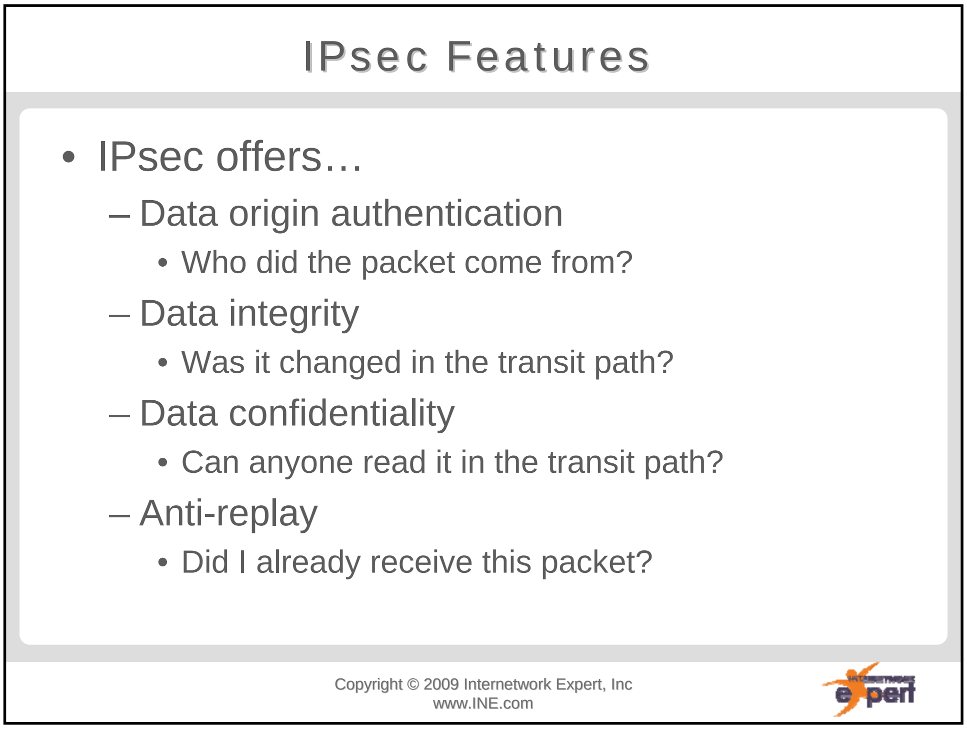
What is IPsec?

- IPsec is a protocol suite (i.e. framework) that defines how secure VPNs can occur for IPv4 and IPv6 based networks
- Lots of open standards, but most importantly…
  - RFC 4301 *Security Architecture for the Internet Protocol*
  - RFC 4302 *IP Authentication Header*
  - RFC 4303 *IP Encapsulating Security Payload (ESP)*
  - RFC 4306 *Internet Key Exchange (IKEv2) Protocol*



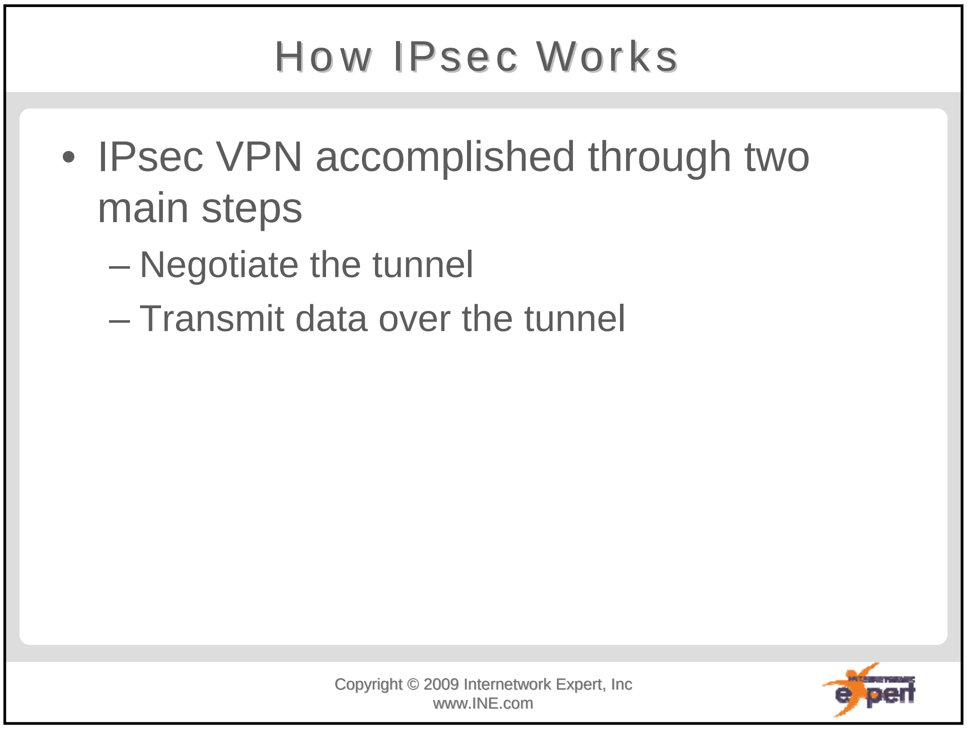
Why IPsec VPNs?

- Do not need static SP provisioning like Frame Relay / ATM / MPLS
- Independent of SP access method
  - IPv4/v6 transport is the only requirement
- Allows both site-to-site and remote access VPNs
  - Always-on vs. dial-on-demand
- Offers data protection
  - Main motivation for IPsec



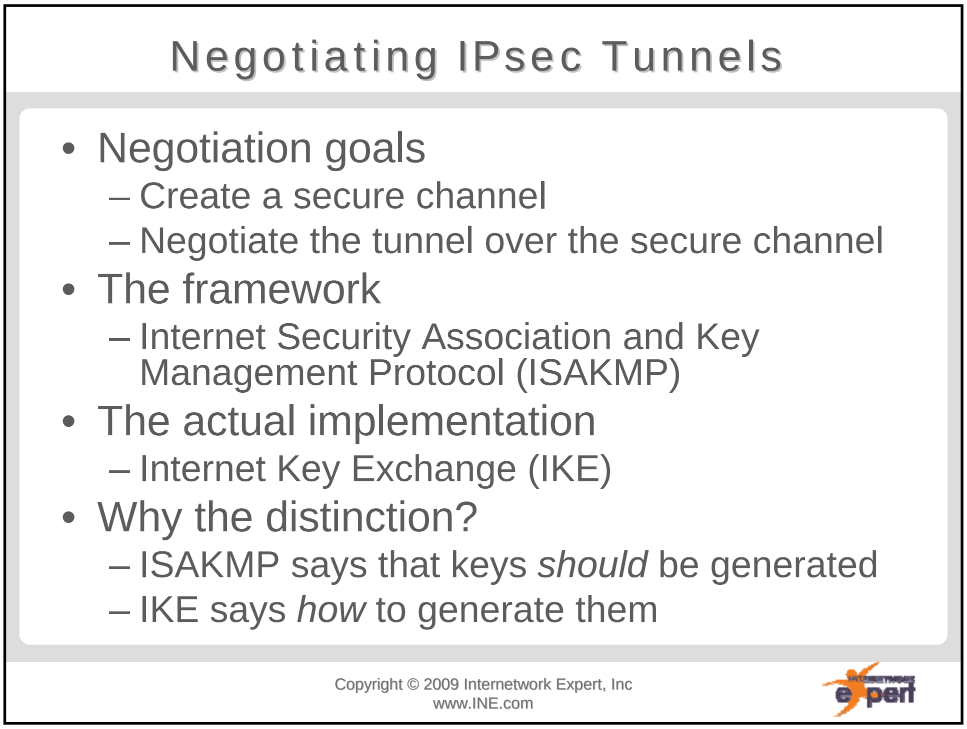
IPsec Features

- IPsec offers…
  - Data origin authentication
    - Who did the packet come from?
  - Data integrity
    - Was it changed in the transit path?
  - Data confidentiality
    - Can anyone read it in the transit path?
  - Anti-replay
    - Did I already receive this packet?



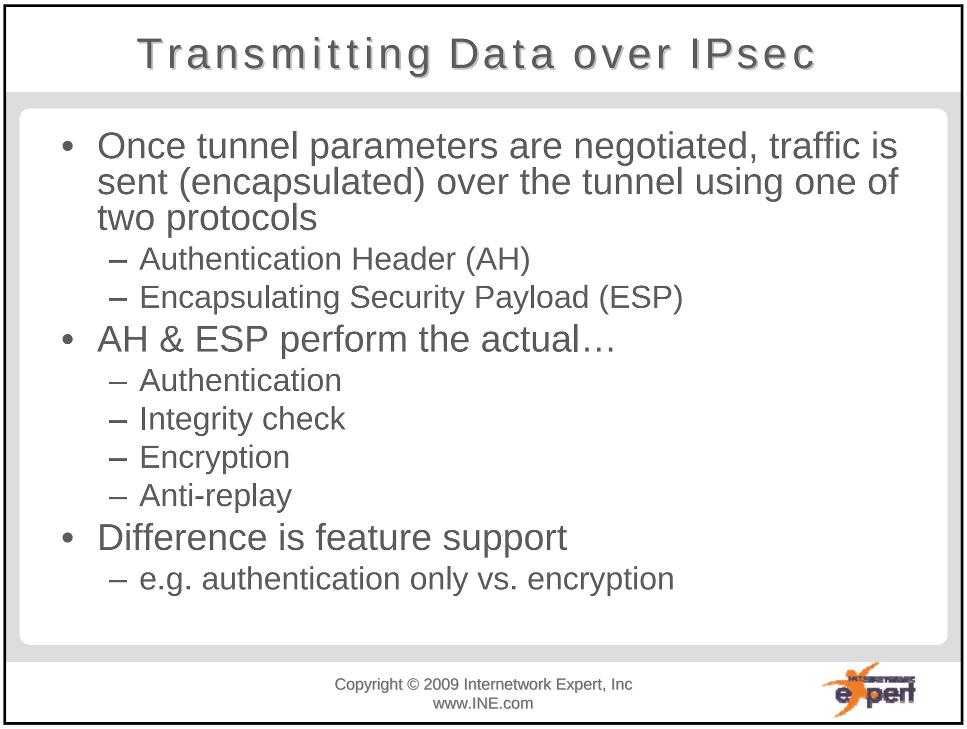
How IPsec Works

- IPsec VPN accomplished through two main steps
  - Negotiate the tunnel
  - Transmit data over the tunnel



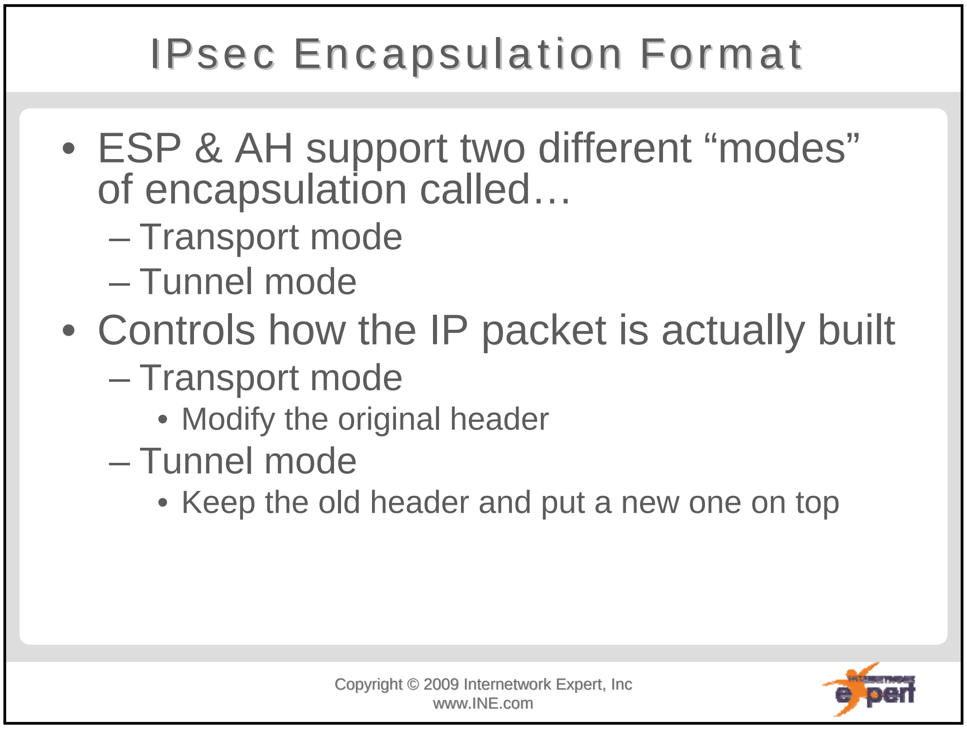
Negotiating IPsec Tunnels

- Negotiation goals
  - Create a secure channel
  - Negotiate the tunnel over the secure channel
- The framework
  - Internet Security Association and Key Management Protocol (ISAKMP)
- The actual implementation
  - Internet Key Exchange (IKE)
- Why the distinction?
  - ISAKMP says that keys *should* be generated
  - IKE says *how* to generate them



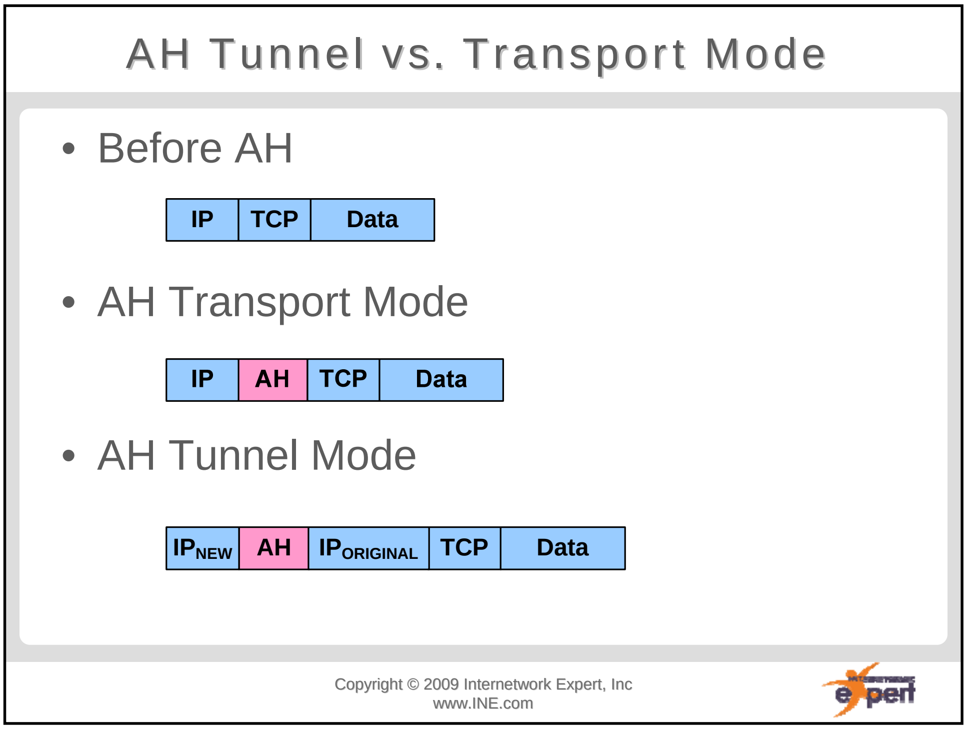
Transmitting Data over IPsec

- Once tunnel parameters are negotiated, traffic is sent (encapsulated) over the tunnel using one of two protocols
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- AH & ESP perform the actual…
  - Authentication
  - Integrity check
  - Encryption
  - Anti-replay
- Difference is feature support
  - e.g. authentication only vs. encryption



IPsec Encapsulation Format

- ESP & AH support two different “modes” of encapsulation called…
  - Transport mode
  - Tunnel mode
- Controls how the IP packet is actually built
  - Transport mode
    - Modify the original header
  - Tunnel mode
    - Keep the old header and put a new one on top



AH Tunnel vs. Transport Mode

- Before AH

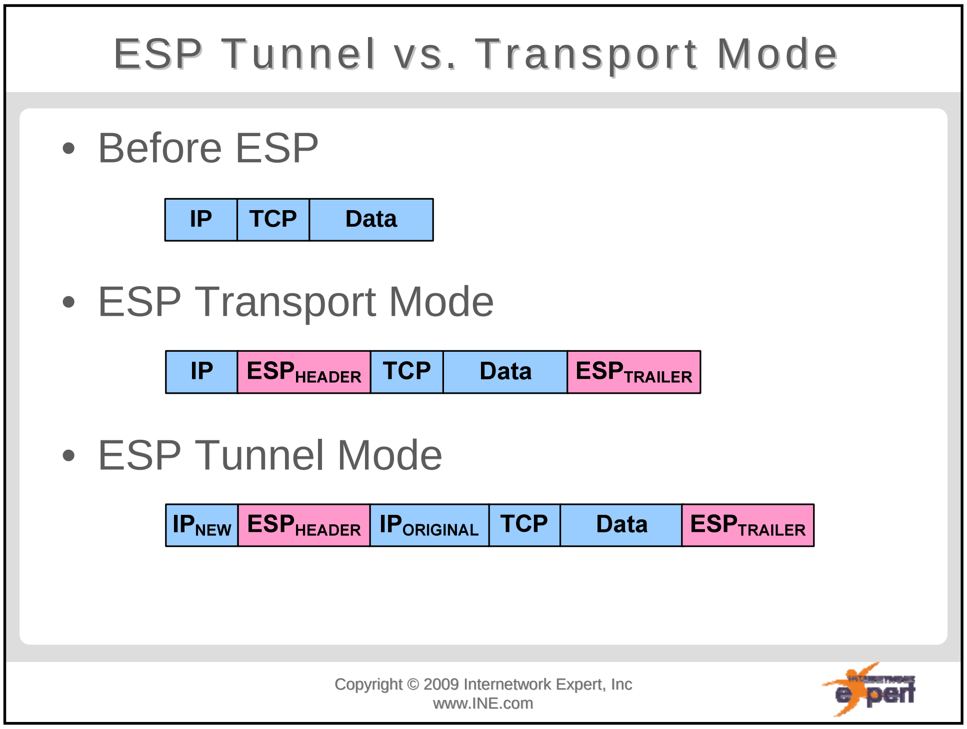
IP	TCP	Data

- AH Transport Mode

IP	AH	TCP	Data

- AH Tunnel Mode

IP_{NEW}	AH	$\text{IP}_{\text{ORIGINAL}}$	TCP	Data



ESP Tunnel vs. Transport Mode

- Before ESP

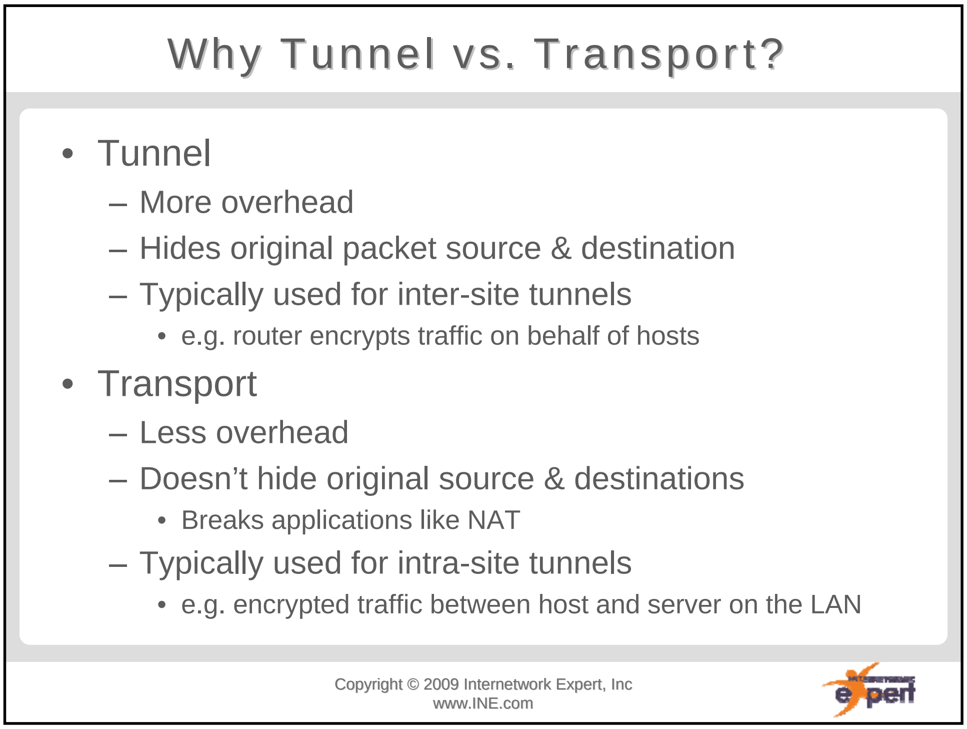
IP	TCP	Data

- ESP Transport Mode

IP	$\text{ESP}_{\text{HEADER}}$	TCP	Data	$\text{ESP}_{\text{TRAILER}}$

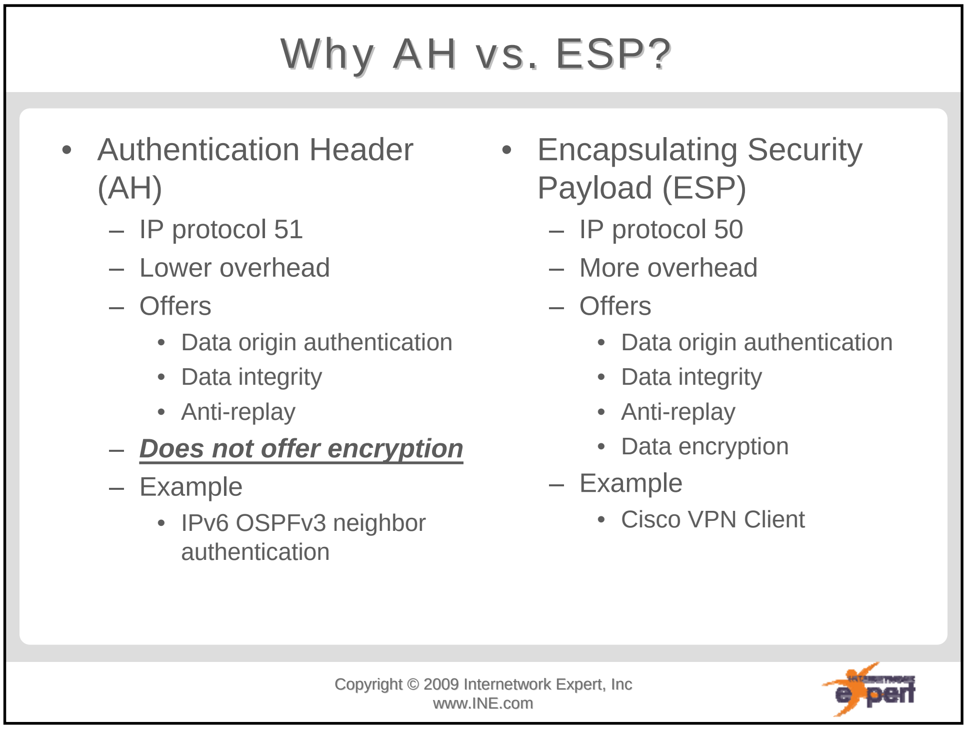
- ESP Tunnel Mode

IP_{NEW}	$\text{ESP}_{\text{HEADER}}$	$\text{IP}_{\text{ORIGINAL}}$	TCP	Data	$\text{ESP}_{\text{TRAILER}}$



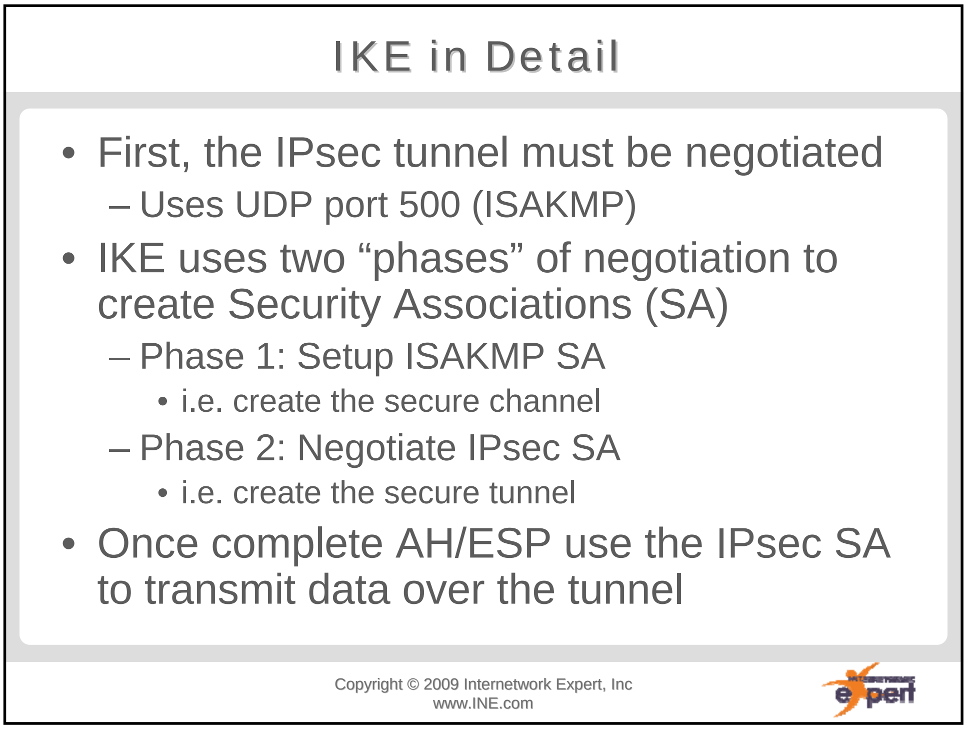
Why Tunnel vs. Transport?

- Tunnel
  - More overhead
  - Hides original packet source & destination
  - Typically used for inter-site tunnels
    - e.g. router encrypts traffic on behalf of hosts
- Transport
  - Less overhead
  - Doesn’t hide original source & destinations
    - Breaks applications like NAT
  - Typically used for intra-site tunnels
    - e.g. encrypted traffic between host and server on the LAN



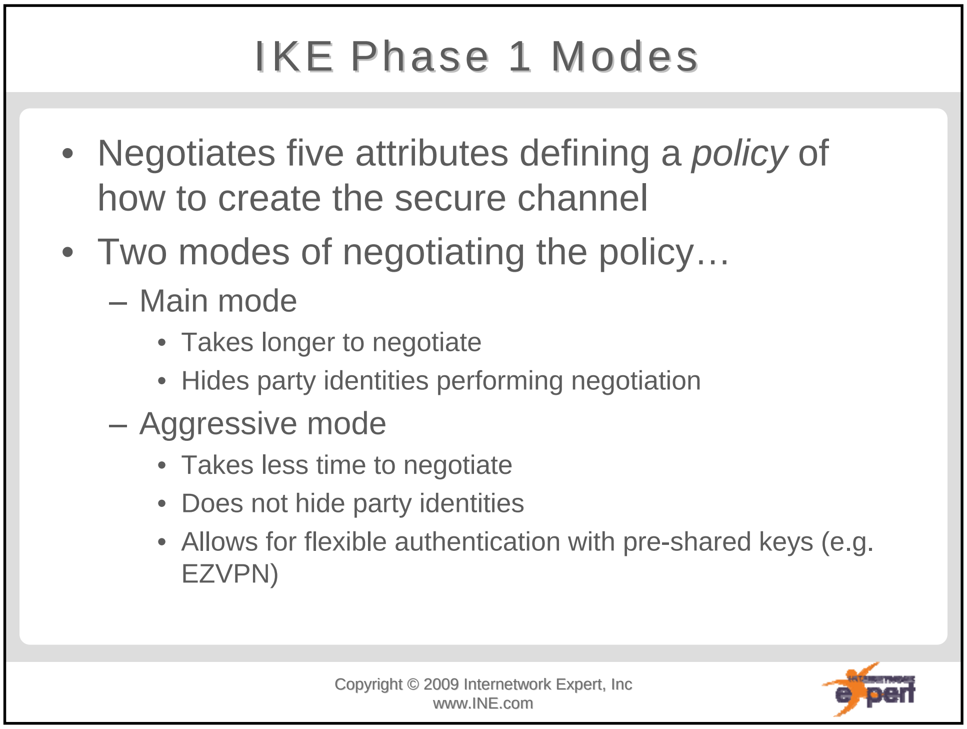
Why AH vs. ESP?

- Authentication Header (AH)
  - IP protocol 51
  - Lower overhead
  - Offers
    - Data origin authentication
    - Data integrity
    - Anti-replay
  - ***Does not offer encryption***
  - Example
    - IPv6 OSPFv3 neighbor authentication
- Encapsulating Security Payload (ESP)
  - IP protocol 50
  - More overhead
  - Offers
    - Data origin authentication
    - Data integrity
    - Anti-replay
    - Data encryption
  - Example
    - Cisco VPN Client



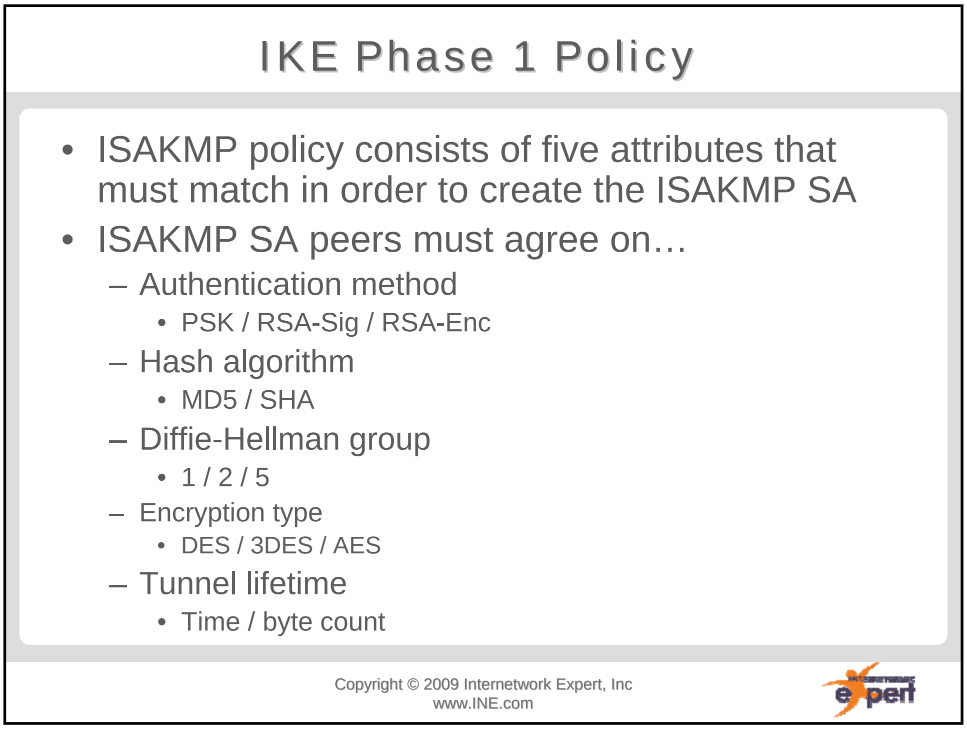
IKE in Detail

- First, the IPsec tunnel must be negotiated
  - Uses UDP port 500 (ISAKMP)
- IKE uses two “phases” of negotiation to create Security Associations (SA)
  - Phase 1: Setup ISAKMP SA
    - i.e. create the secure channel
  - Phase 2: Negotiate IPsec SA
    - i.e. create the secure tunnel
- Once complete AH/ESP use the IPsec SA to transmit data over the tunnel



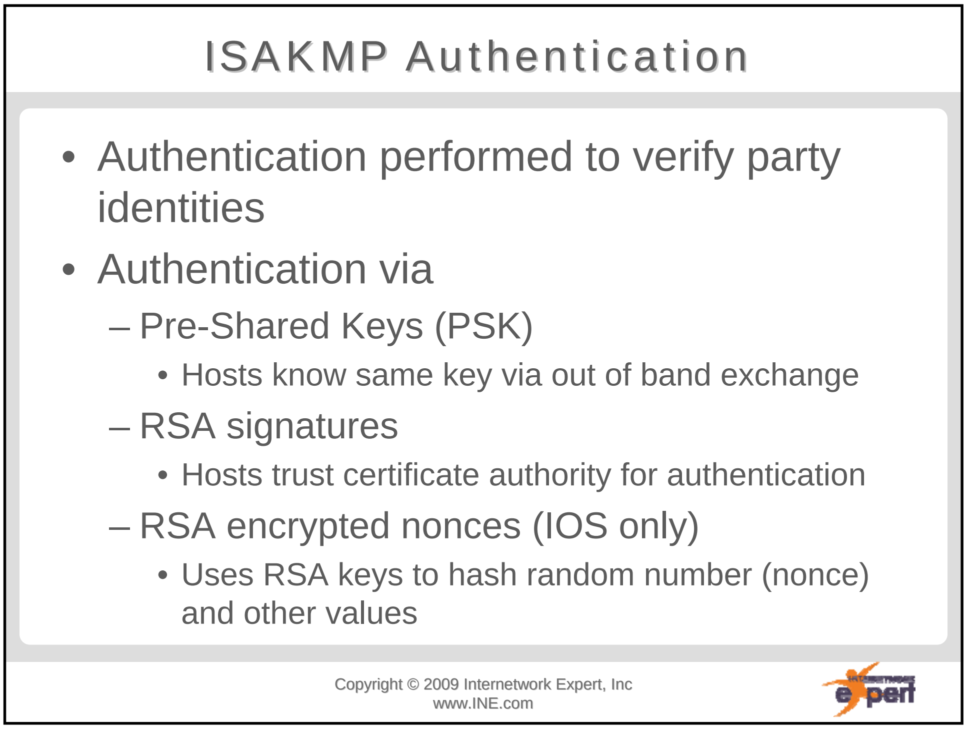
IKE Phase 1 Modes

- Negotiates five attributes defining a *policy* of how to create the secure channel
- Two modes of negotiating the policy…
  - Main mode
    - Takes longer to negotiate
    - Hides party identities performing negotiation
  - Aggressive mode
    - Takes less time to negotiate
    - Does not hide party identities
    - Allows for flexible authentication with pre-shared keys (e.g. EZVPN)



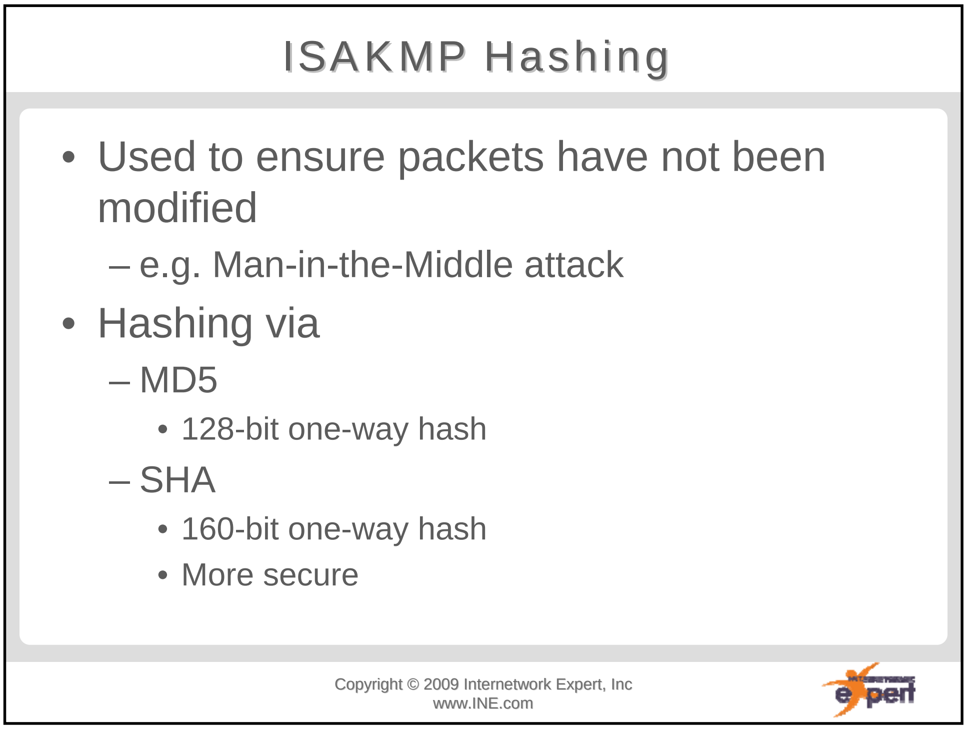
IKE Phase 1 Policy

- ISAKMP policy consists of five attributes that must match in order to create the ISAKMP SA
- ISAKMP SA peers must agree on…
  - Authentication method
    - PSK / RSA-Sig / RSA-Enc
  - Hash algorithm
    - MD5 / SHA
  - Diffie-Hellman group
    - 1 / 2 / 5
  - Encryption type
    - DES / 3DES / AES
  - Tunnel lifetime
    - Time / byte count



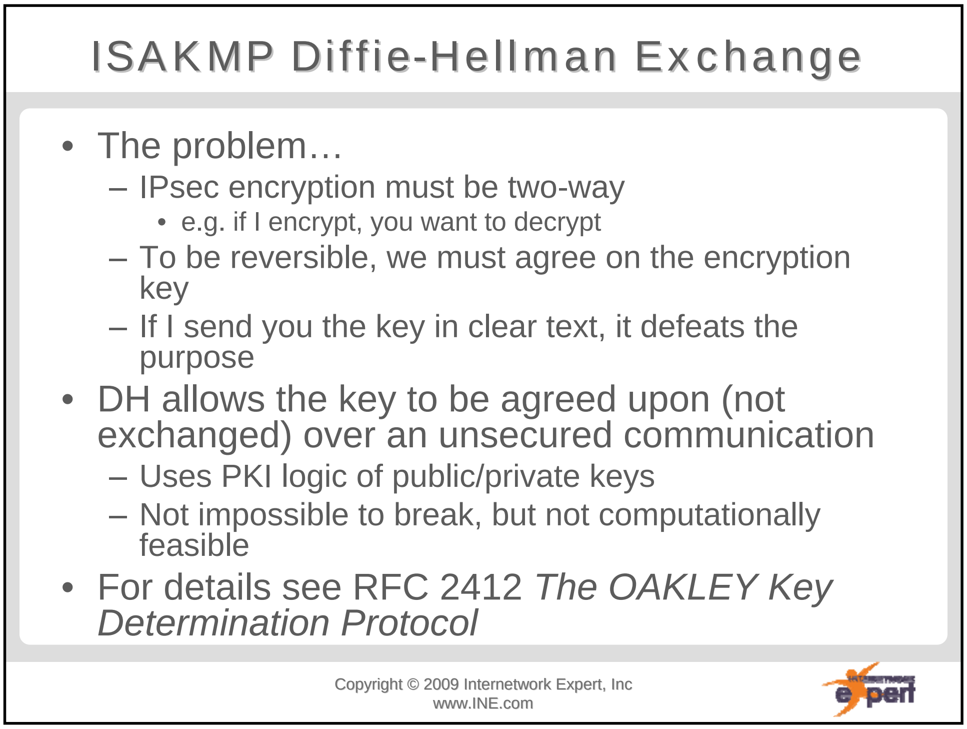
ISAKMP Authentication

- Authentication performed to verify party identities
- Authentication via
  - Pre-Shared Keys (PSK)
    - Hosts know same key via out of band exchange
  - RSA signatures
    - Hosts trust certificate authority for authentication
  - RSA encrypted nonces (IOS only)
    - Uses RSA keys to hash random number (nonce) and other values



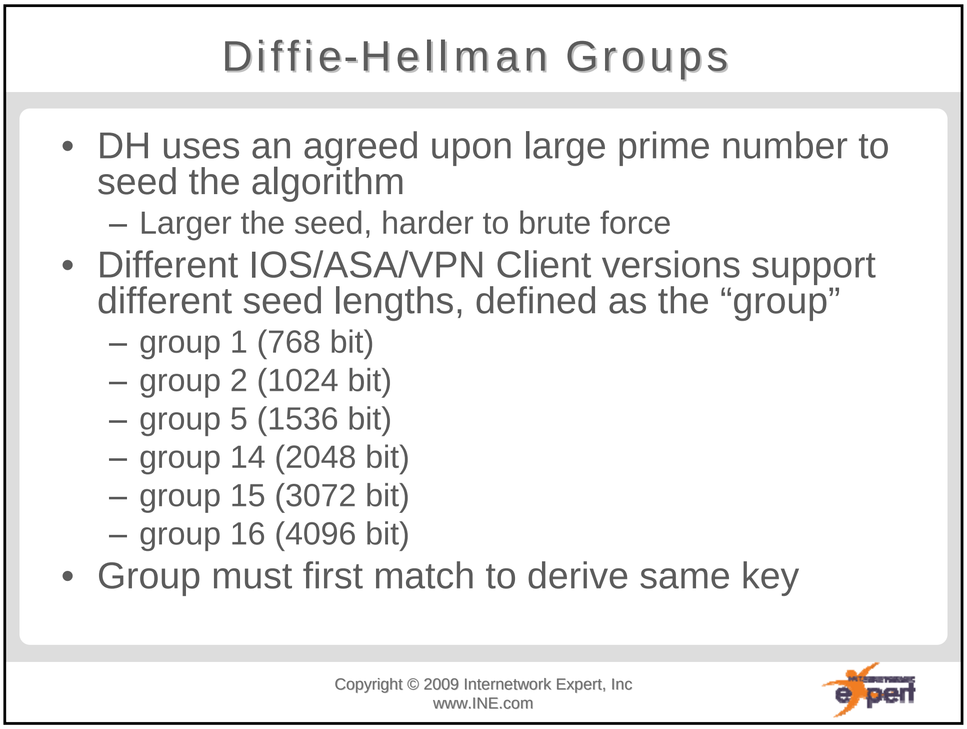
ISAKMP Hashing

- Used to ensure packets have not been modified
  - e.g. Man-in-the-Middle attack
- Hashing via
  - MD5
    - 128-bit one-way hash
  - SHA
    - 160-bit one-way hash
    - More secure



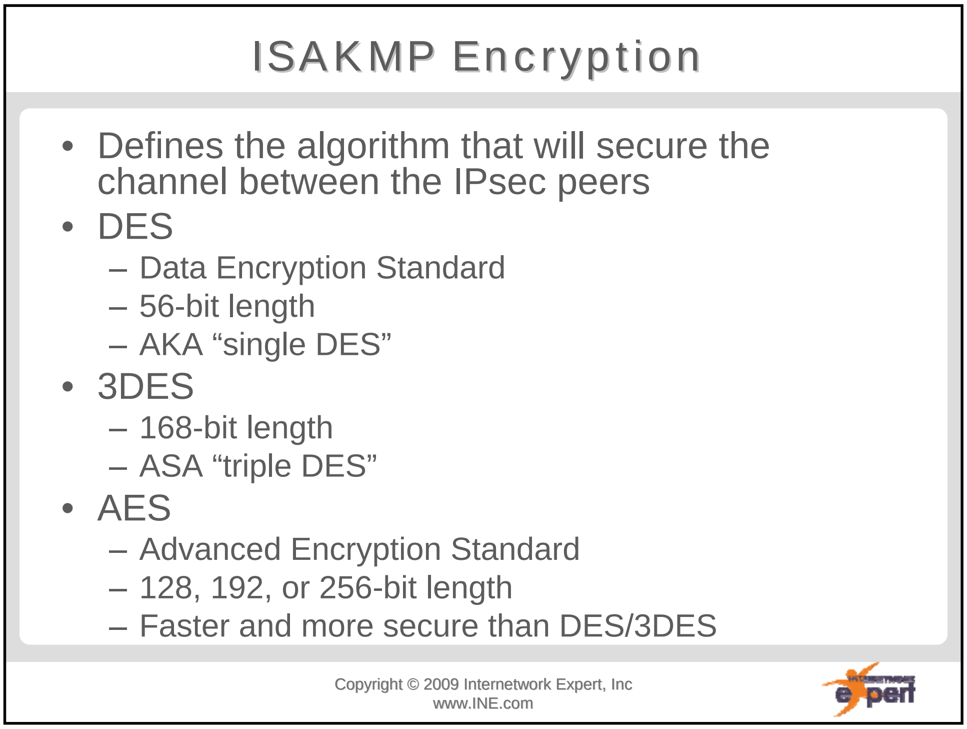
ISAKMP Diffie-Hellman Exchange

- The problem…
  - IPsec encryption must be two-way
    - e.g. if I encrypt, you want to decrypt
  - To be reversible, we must agree on the encryption key
  - If I send you the key in clear text, it defeats the purpose
- DH allows the key to be agreed upon (not exchanged) over an unsecured communication
  - Uses PKI logic of public/private keys
  - Not impossible to break, but not computationally feasible
- For details see RFC 2412 *The OAKLEY Key Determination Protocol*



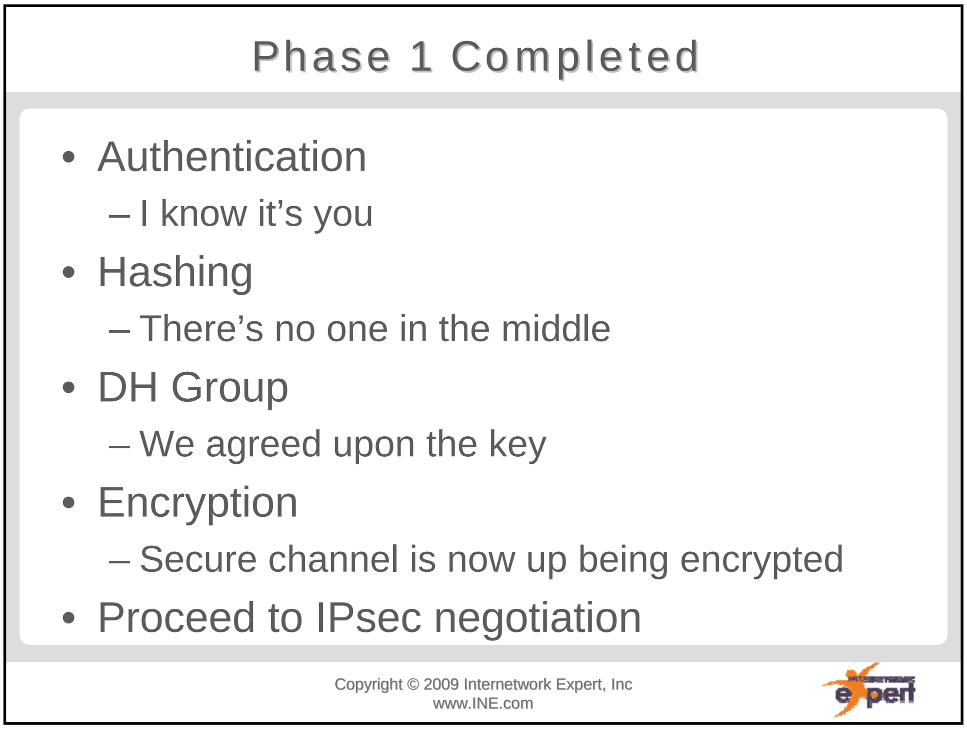
Diffie-Hellman Groups

- DH uses an agreed upon large prime number to seed the algorithm
  - Larger the seed, harder to brute force
- Different IOS/ASA/VPN Client versions support different seed lengths, defined as the “group”
  - group 1 (768 bit)
  - group 2 (1024 bit)
  - group 5 (1536 bit)
  - group 14 (2048 bit)
  - group 15 (3072 bit)
  - group 16 (4096 bit)
- Group must first match to derive same key



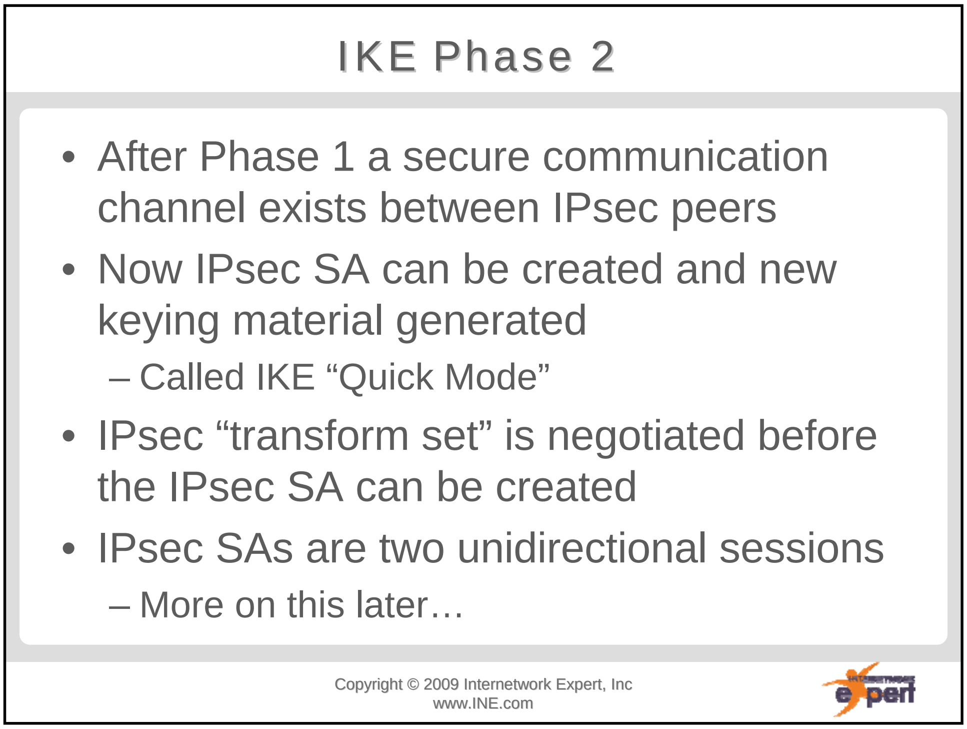
ISAKMP Encryption

- Defines the algorithm that will secure the channel between the IPsec peers
- DES
  - Data Encryption Standard
  - 56-bit length
  - AKA “single DES”
- 3DES
  - 168-bit length
  - ASA “triple DES”
- AES
  - Advanced Encryption Standard
  - 128, 192, or 256-bit length
  - Faster and more secure than DES/3DES



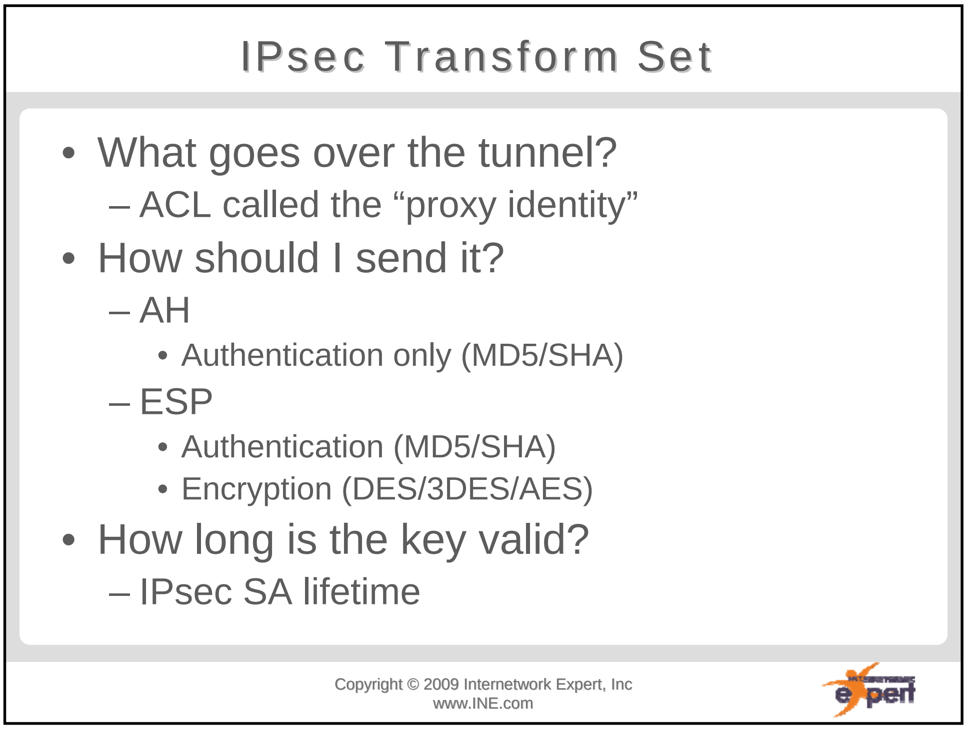
Phase 1 Completed

- Authentication
  - I know it’s you
- Hashing
  - There’s no one in the middle
- DH Group
  - We agreed upon the key
- Encryption
  - Secure channel is now up being encrypted
- Proceed to IPsec negotiation



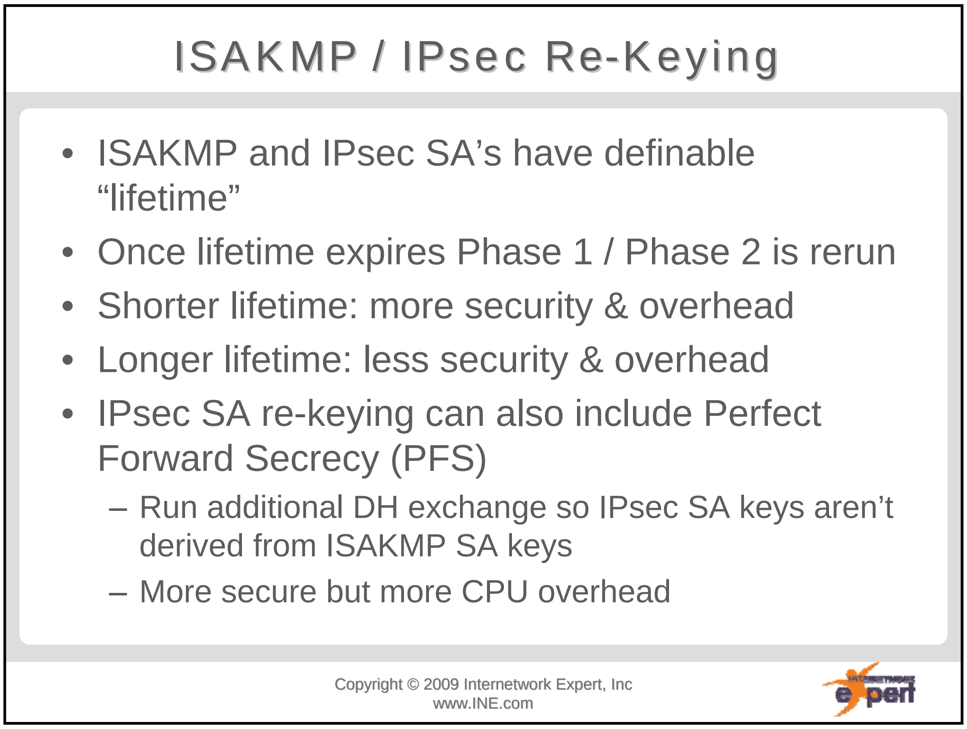
IKE Phase 2

- After Phase 1 a secure communication channel exists between IPsec peers
- Now IPsec SA can be created and new keying material generated
  - Called IKE “Quick Mode”
- IPsec “transform set” is negotiated before the IPsec SA can be created
- IPsec SAs are two unidirectional sessions
  - More on this later…



IPsec Transform Set

- What goes over the tunnel?
  - ACL called the “proxy identity”
- How should I send it?
  - AH
    - Authentication only (MD5/SHA)
  - ESP
    - Authentication (MD5/SHA)
    - Encryption (DES/3DES/AES)
- How long is the key valid?
  - IPsec SA lifetime



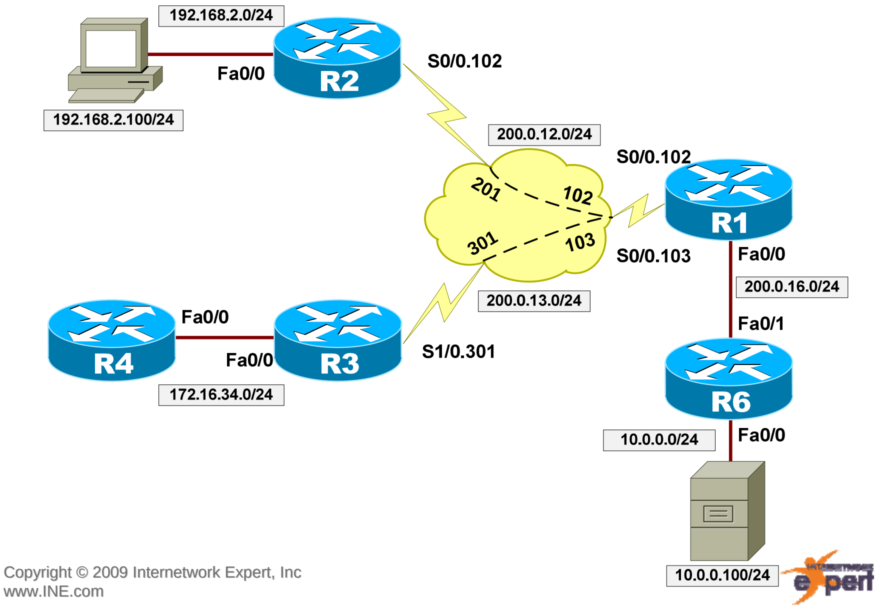
ISAKMP / IPsec Re-Keying

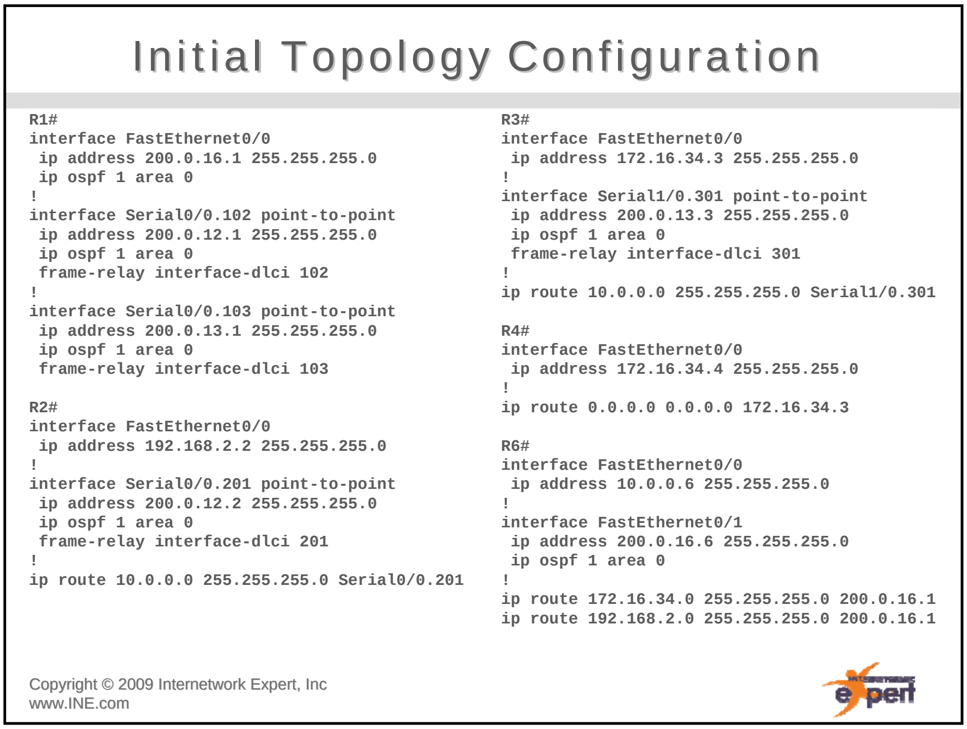
- ISAKMP and IPsec SA’s have definable “lifetime”
- Once lifetime expires Phase 1 / Phase 2 is rerun
- Shorter lifetime: more security & overhead
- Longer lifetime: less security & overhead
- IPsec SA re-keying can also include Perfect Forward Secrecy (PFS)
  - Run additional DH exchange so IPsec SA keys aren’t derived from ISAKMP SA keys
  - More secure but more CPU overhead

IOS IPsec Configuration Steps

- Define ISAKMP policy / policies
  - Processed top down until a match occurs
  - Implies most secure policy should be first
- Define IPsec policy
  - Transform set
- Define traffic to be IPsec encapsulated
  - Access-lists should be mirror images
- Applied to the link level as **`crypto-map`**

Configuring L2L IPsec Example

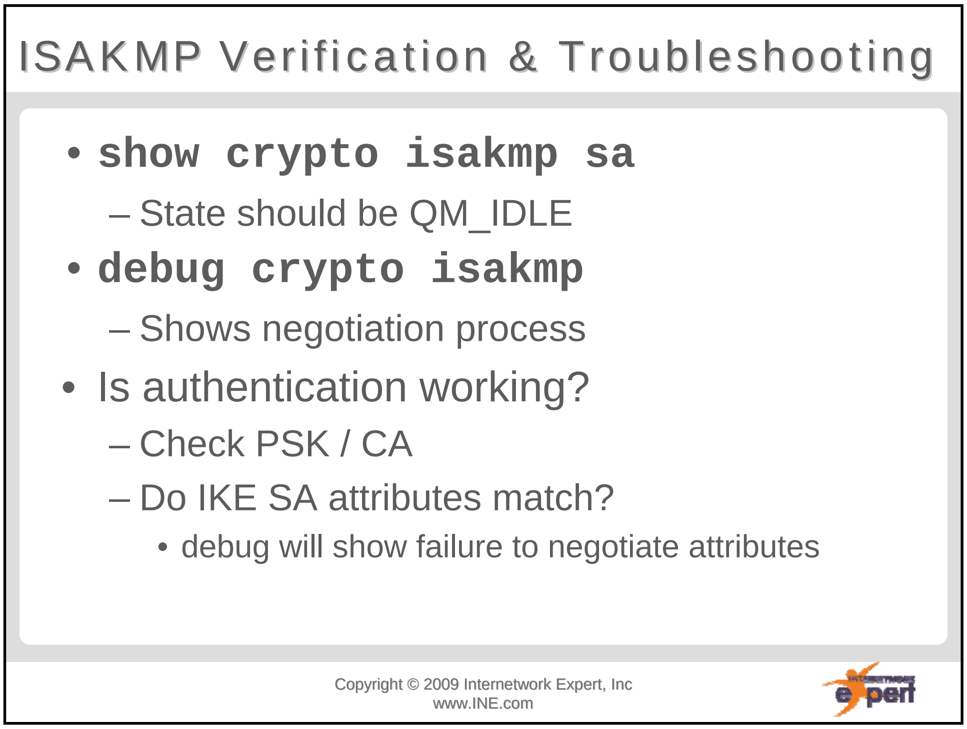




Initial Topology Configuration

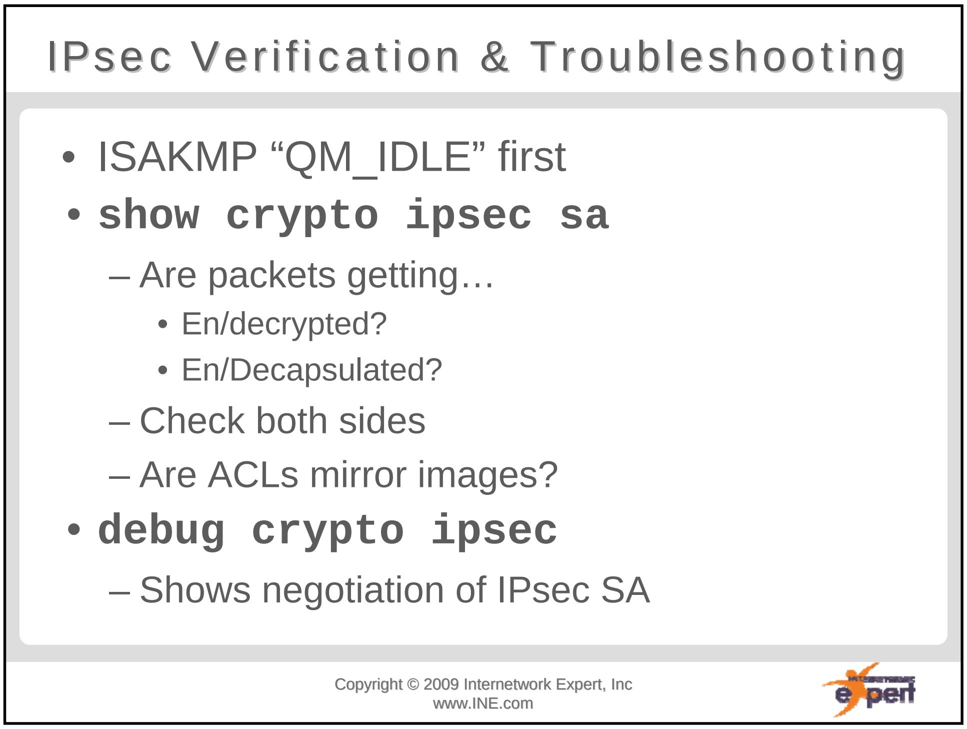
```
R1#
interface FastEthernet0/0
 ip address 200.0.16.1 255.255.255.0
 ip ospf 1 area 0
!
interface Serial0/0.102 point-to-point
 ip address 200.0.12.1 255.255.255.0
 ip ospf 1 area 0
 frame-relay interface-dlci 102
!
interface Serial0/0.103 point-to-point
 ip address 200.0.13.1 255.255.255.0
 ip ospf 1 area 0
 frame-relay interface-dlci 103

R2#
interface FastEthernet0/0
 ip address 192.168.2.2 255.255.255.0
!
interface Serial0/0.201 point-to-point
 ip address 200.0.12.2 255.255.255.0
 ip ospf 1 area 0
 frame-relay interface-dlci 201
!
ip route 10.0.0.0 255.255.255.0 Serial0/0.201
```

```
R3#
interface FastEthernet0/0
 ip address 172.16.34.3 255.255.255.0
!
interface Serial1/0.301 point-to-point
 ip address 200.0.13.3 255.255.255.0
 ip ospf 1 area 0
 frame-relay interface-dlci 301
!
ip route 10.0.0.0 255.255.255.0 Serial1/0.301

R4#
interface FastEthernet0/0
 ip address 172.16.34.4 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 172.16.34.3

R6#
interface FastEthernet0/0
 ip address 10.0.0.6 255.255.255.0
!
interface FastEthernet0/1
 ip address 200.0.16.6 255.255.255.0
 ip ospf 1 area 0
!
ip route 172.16.34.0 255.255.255.0 200.0.16.1
ip route 192.168.2.0 255.255.255.0 200.0.16.1
```



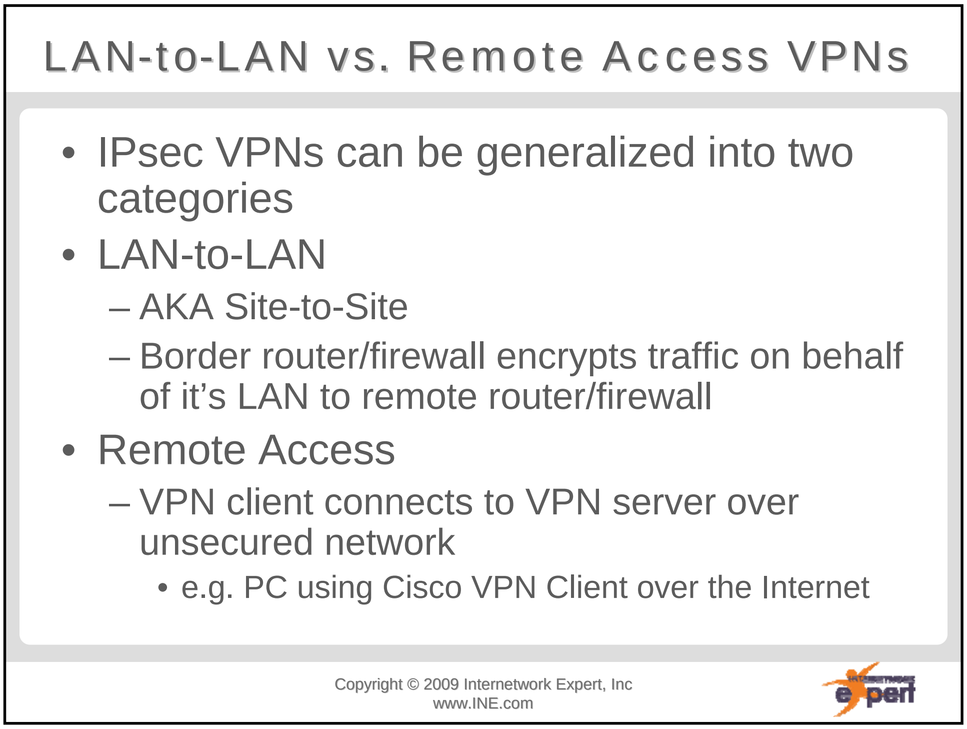
ISAKMP Verification & Troubleshooting

- **`show crypto isakmp sa`**
  - State should be QM_IDLE
- **`debug crypto isakmp`**
  - Shows negotiation process
- Is authentication working?
  - Check PSK / CA
  - Do IKE SA attributes match?
    - debug will show failure to negotiate attributes



IPsec Verification & Troubleshooting

- ISAKMP “QM_IDLE” first
- **`show crypto ipsec sa`**
  - Are packets getting…
    - En/decrypted?
    - En/Decapsulated?
  - Check both sides
  - Are ACLs mirror images?
- **`debug crypto ipsec`**
  - Shows negotiation of IPsec SA



LAN-to-LAN vs. Remote Access VPNs

- IPsec VPNs can be generalized into two categories
- LAN-to-LAN
  - AKA Site-to-Site
  - Border router/firewall encrypts traffic on behalf of it’s LAN to remote router/firewall
- Remote Access
  - VPN client connects to VPN server over unsecured network
    - e.g. PC using Cisco VPN Client over the Internet

Remote Access Challenges

- What if they go through NAT?
  - Modifying L3 header breaks AH/ESP integrity check
- What if they go through a firewall?
  - Most firewalls can’t inspect/block protocols 50/51
- How do I do per-user authentication?
  - PSK for all clients isn’t secure
- How do I give them per-user options?
  - DHCP / DNS / ACLs / etc.

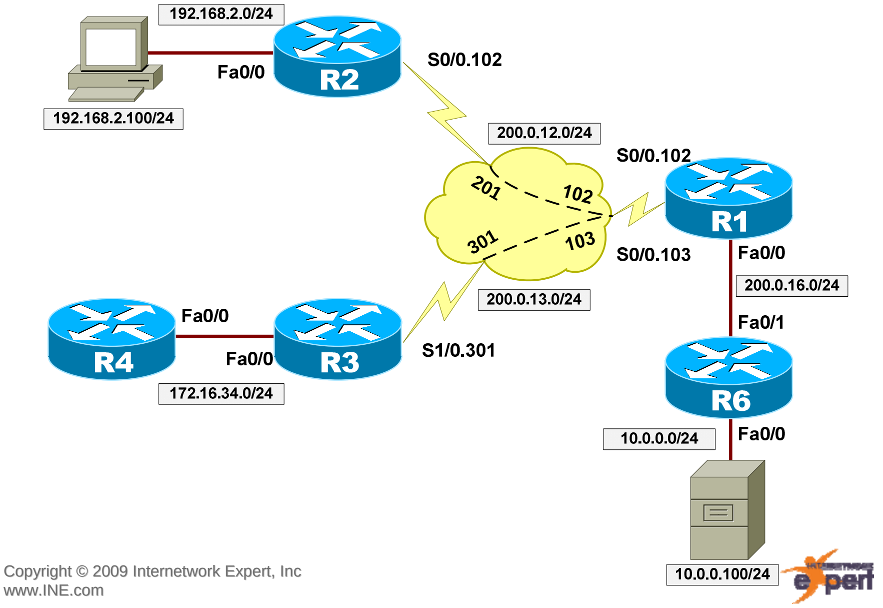
IPsec NAT-T

- AKA NAT Transparency or NAT Traversal
- ISAKMP uses UDP port 500, can go through NAT/PAT
- ESP/AH use protocols 50/51, no NAT/PAT support
- During IKE, VPN sever detects “identity” is different in IKE payload vs. IP packet source
- Workaround is ESP is tunneled inside UDP with port 4500
- Fixes problem with stateful firewalls
  - e.g. UDP usually inspected by default
- Cisco also has proprietary workarounds to tunnel over arbitrary UDP/TCP port
  - UDP 4500 may be blocked, but is TCP 80?

IKE Phase 1.5

- Once an IPsec RA peer connects to the server, optional “phase 1.5” can run to negotiate…
- Extended Authentication
  - AKA “Xauth”
  - Per user authentication in addition to Phase 1 authentication
- Mode Configuration
  - Per user attributes such as DHCP address for VPN, split DNS, split tunnel proxy ACL, etc.

Configuring RA IPsec Example



GRE and IPsec

- IPsec tunnels are not “interfaces”
  - No IP address associated with them
  - Implies that dynamic routing not supported
- Routing + IPsec requires GRE
  - e.g. DMVPN
- Protocol 47 (GRE) should be matched in proxy ACL
- Multiple tunnels (backup tunnels) can be used in redundancy designs

GRE and IPsec Overhead

- GRE packet format
  - 20 byte IP + ~4 byte GRE
  - ~24 bytes overhead

IP_{GRE}	GRE	$\text{IP}_{\text{ORIGINAL}}$	TCP	Data

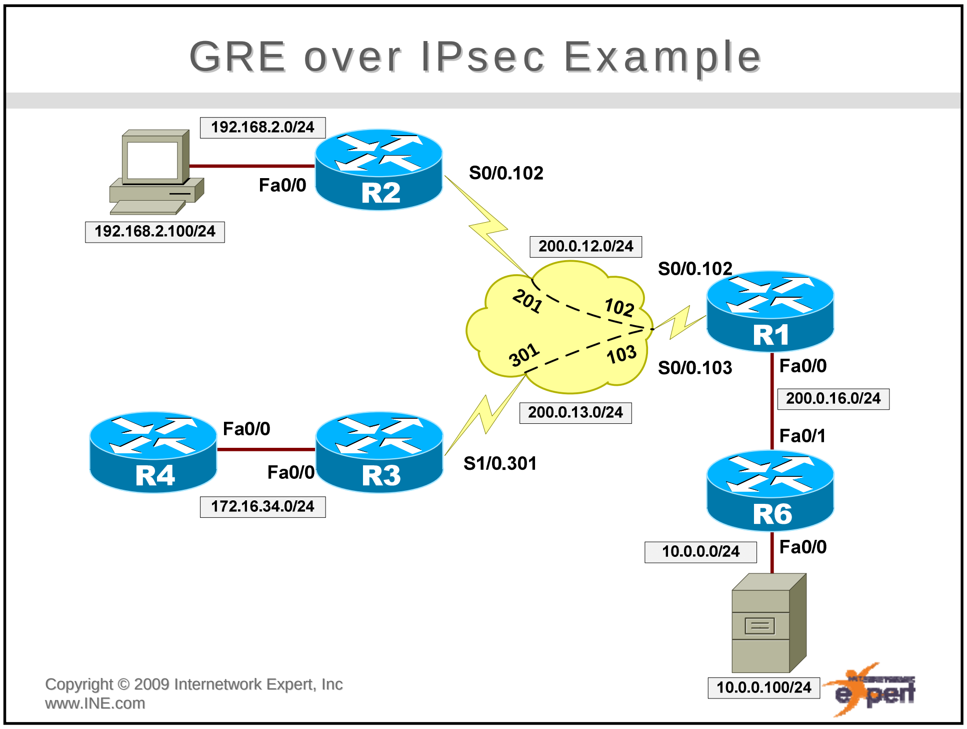
- GRE over ESP Transport Mode
  - 20 byte IP + ~31 ESP + ~4 byte GRE
  - ~55 bytes overhead

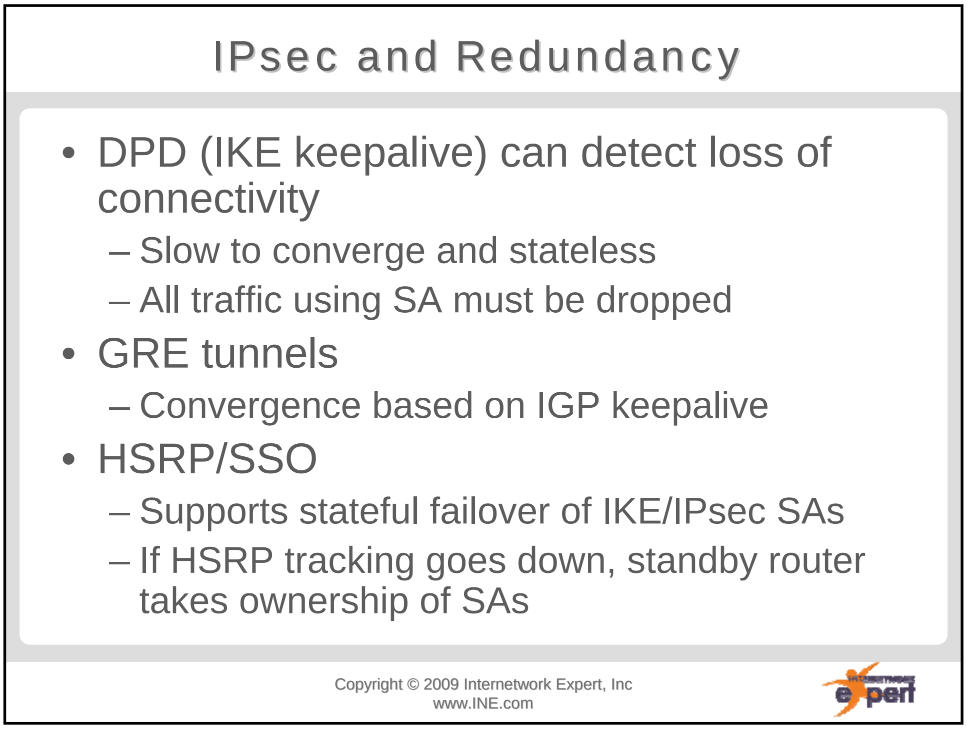
IP_{GRE}	$\text{ESP}_{\text{HEADER}}$	GRE	$\text{IP}_{\text{ORIGINAL}}$	TCP	Data	$\text{ESP}_{\text{TRAILER}}$

- GRE over ESP Tunnel Mode
  - 20 byte IP + ~31 ESP + 20 byte IP + ~4 byte GRE
  - ~75 bytes overhead
  - ***3 IP headers per packet!!!***

IP_{NEW}	$\text{ESP}_{\text{HEADER}}$	IP_{GRE}	GRE	$\text{IP}_{\text{ORIGINAL}}$	TCP	Data	$\text{ESP}_{\text{TRAILER}}$

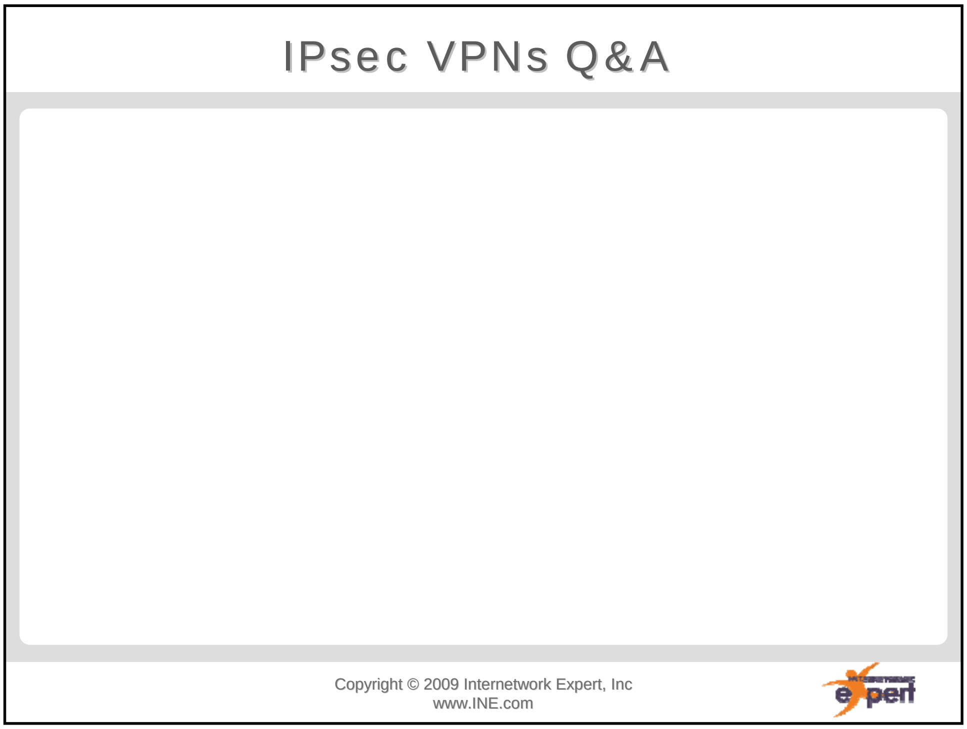
GRE over IPsec Example





IPsec and Redundancy

- DPD (IKE keepalive) can detect loss of connectivity
  - Slow to converge and stateless
  - All traffic using SA must be dropped
- GRE tunnels
  - Convergence based on IGP keepalive
- HSRP/SSO
  - Supports stateful failover of IKE/IPsec SAs
  - If HSRP tracking goes down, standby router takes ownership of SAs



IPsec VPNs Q&A