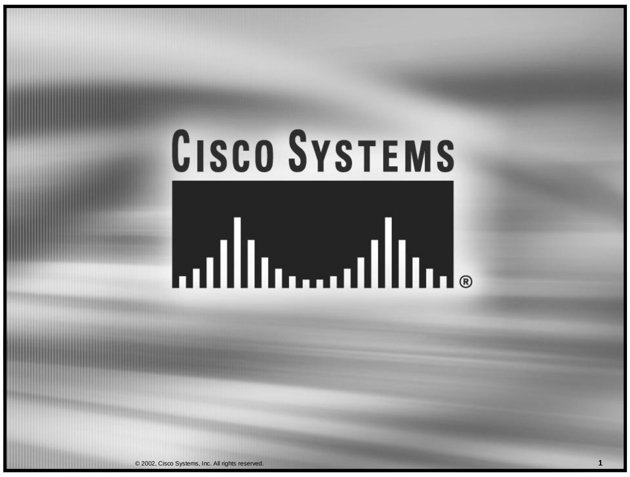
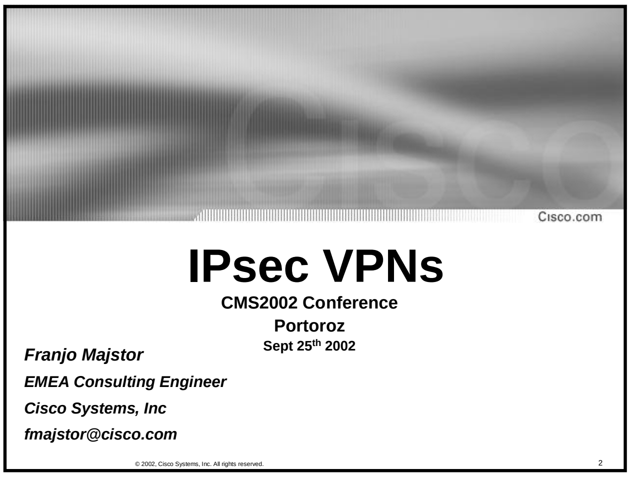
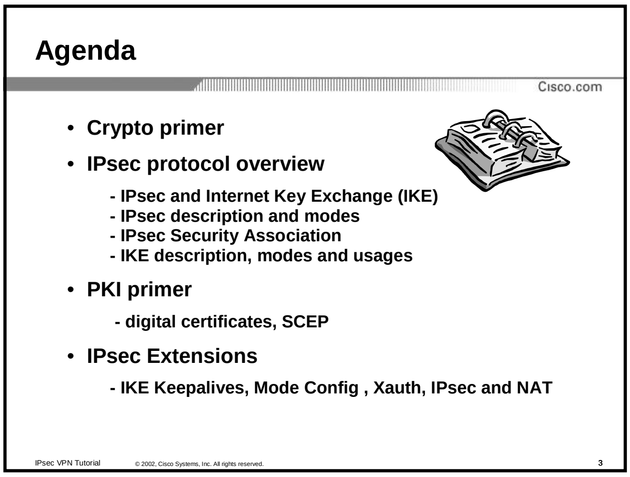




IPsec VPNs

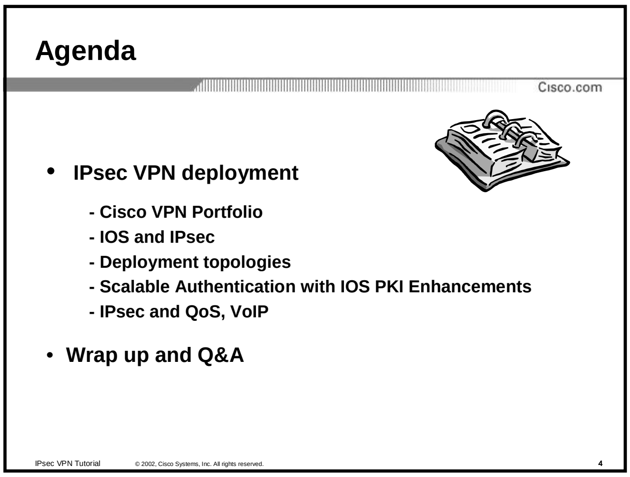
CMS2002 Conference
Portoroz
Sept 25th 2002

Franjo Majstor
EMEA Consulting Engineer
Cisco Systems, Inc
fmajstor@cisco.com



Agenda

- Crypto primer
- IPsec protocol overview
  - IPsec and Internet Key Exchange (IKE)
  - IPsec description and modes
  - IPsec Security Association
  - IKE description, modes and usages
- PKI primer
  - digital certificates, SCEP
- IPsec Extensions
  - IKE Keepalives, Mode Config , Xauth, IPsec and NAT

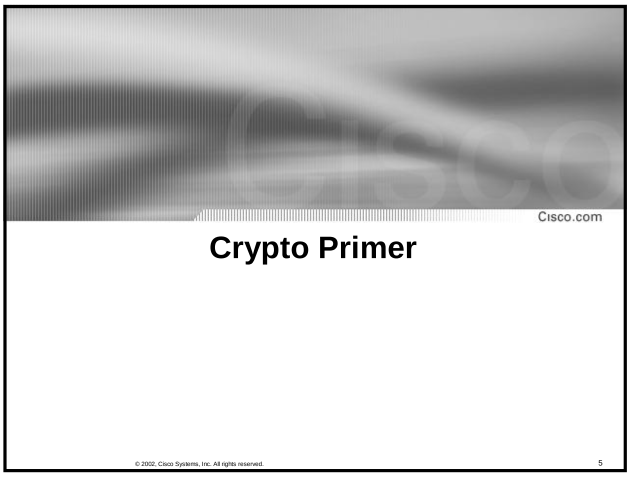


Agenda

Cisco.com

- IPsec VPN deployment
  - - Cisco VPN Portfolio
  - - IOS and IPsec
  - - Deployment topologies
  - - Scalable Authentication with IOS PKI Enhancements
  - - IPsec and QoS, VoIP
- Wrap up and Q&A

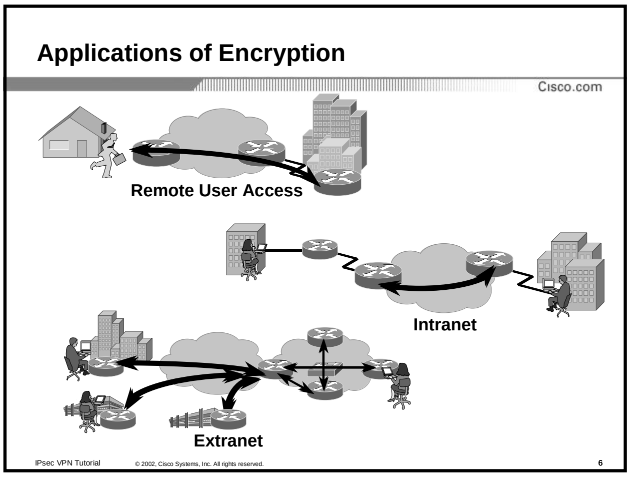
IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 4



Cisco.com

Crypto Primer

© 2002, Cisco Systems, Inc. All rights reserved. 5



Applications of Encryption

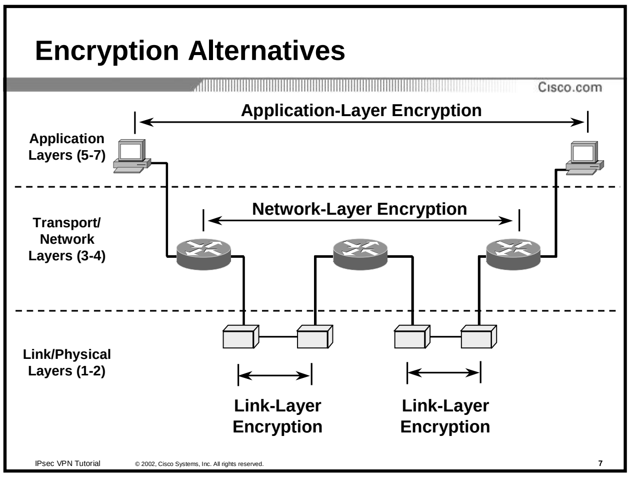
Cisco.com

Remote User Access

Intranet

Extranet

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 6



Encryption Alternatives

Application-Layer Encryption

Application Layers (5-7)

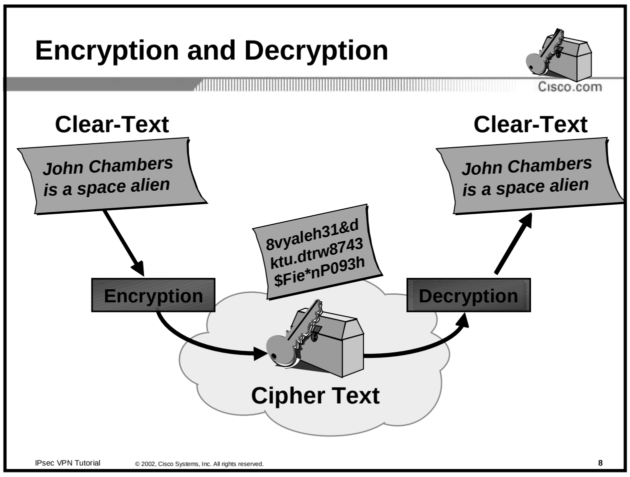
Network-Layer Encryption

Transport/ Network Layers (3-4)

Link/Physical Layers (1-2)

Link-Layer Encryption

Link-Layer Encryption



Encryption and Decryption

Clear-Text

John Chambers is a space alien

Clear-Text

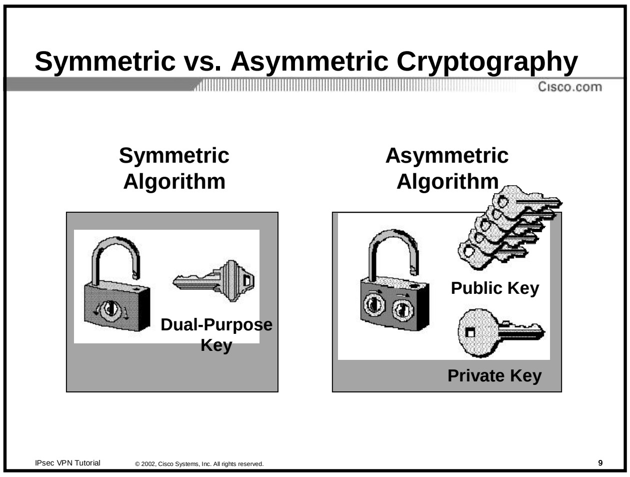
John Chambers is a space alien

8vyaleh31&d
ktu.dtrw8743
$Fie*nP093h

Encryption

Decryption

Cipher Text



Symmetric vs. Asymmetric Cryptography

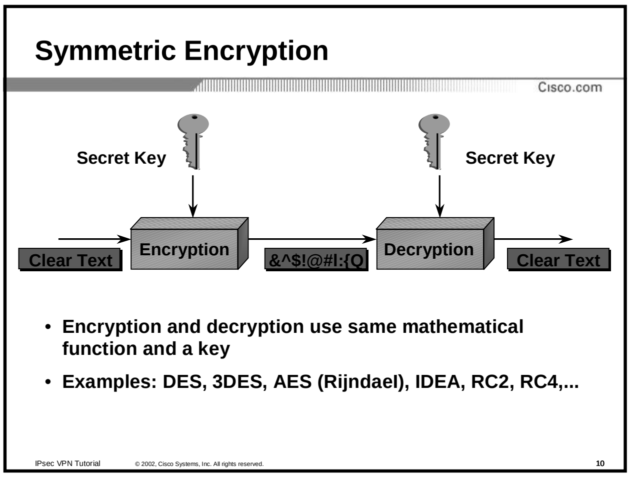
Symmetric Algorithm

Dual-Purpose Key

Asymmetric Algorithm

Public Key

Private Key



Symmetric Encryption

Cisco.com

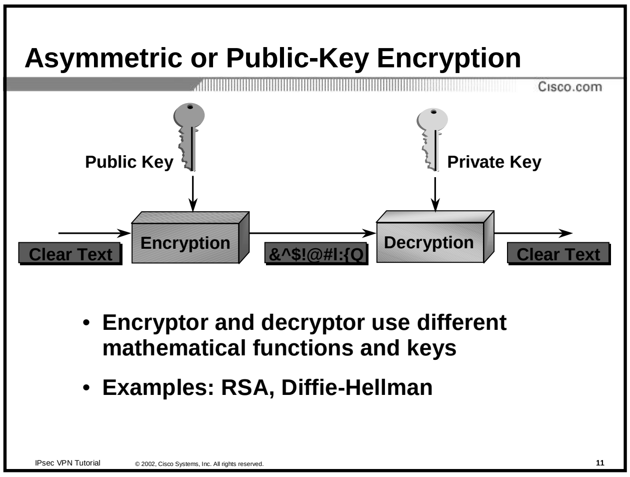
Secret Key

Secret Key

Clear Text → Encryption → &^$!@#l:{Q → Decryption → Clear Text

- Encryption and decryption use same mathematical function and a key
- Examples: DES, 3DES, AES (Rijndael), IDEA, RC2, RC4,...

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 10



Asymmetric or Public-Key Encryption

Cisco.com

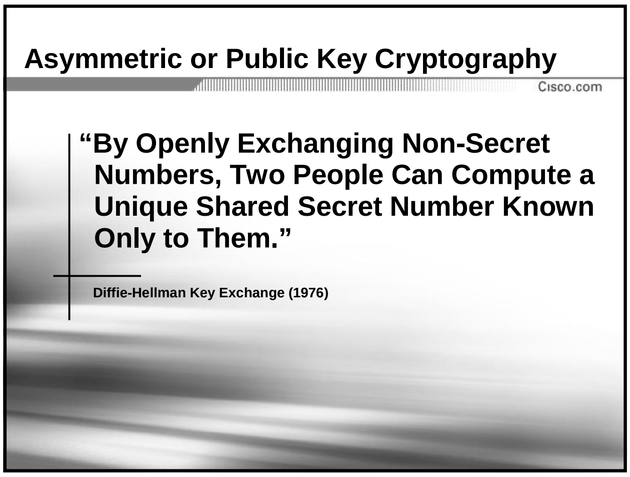
Public Key

Private Key

Clear Text → Encryption → &^$!@#l:{Q → Decryption → Clear Text

- Encryptor and decryptor use different mathematical functions and keys
- Examples: RSA, Diffie-Hellman

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 11



Asymmetric or Public Key Cryptography

Cisco.com

> "By Openly Exchanging Non-Secret Numbers, Two People Can Compute a Unique Shared Secret Number Known Only to Them."

Diffie-Hellman Key Exchange (1976)

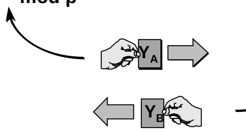
The Diffie-Hellman Public Key Exchange

Alice Secret Value, X_A
Public Value, Y_A

Secret Value, X_B
Public Value, Y_B **Bob**

$Y_A = g^{X_A} \bmod p$

$Y_B = g^{X_B} \bmod p$



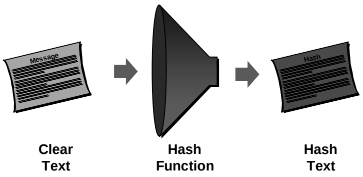
$$Y_B^{X_A} \bmod p = g^{X_A X_B} \bmod p = g^{X_B X_A} \bmod p = Y_A^{X_B} \bmod p$$

(Shared Secret)

p is a large prime
g size is based on D-H group

What is a Hash?

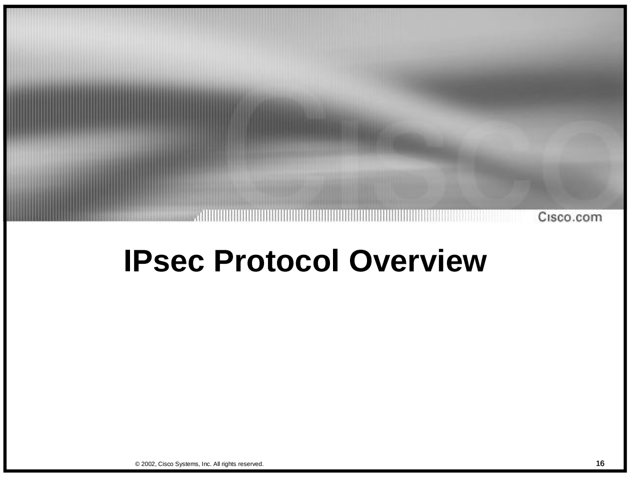
Hash – A one-way mathematical summary of a message such that the hash value cannot be (easily) reconstituted back into the original message – even with knowledge of the hash algorithm.



Hashing Algorithms

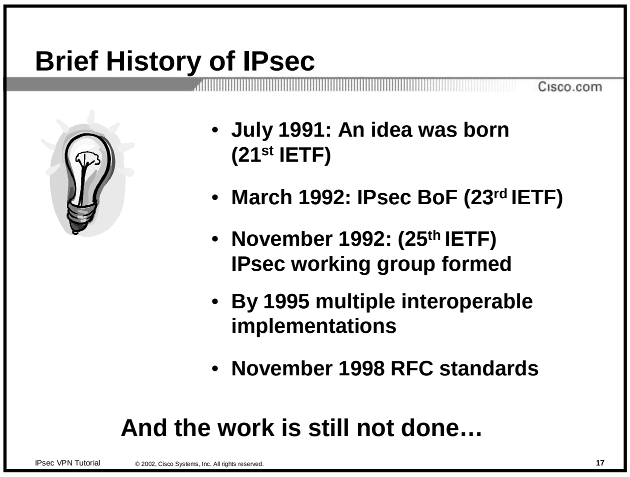
- MD5 (*Message Digest V5*): 128 bits hash
  Older but most widely supported hash algorithm
- SHA (*Secure Hash Algorithm*): 160 bits hash
  Newer and more secure hash than MD5
- HMAC (*Hash-based Message Authentication Code*): Further hash security through inclusion of a key with message in hash process (similar to MAC)

HMAC-MD5 and HMAC-SHA are used by IPSec for integrity checking



Cisco.com

IPsec Protocol Overview

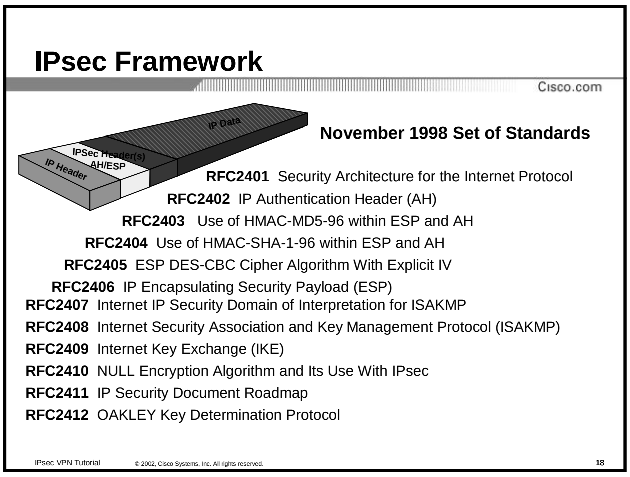


Brief History of IPsec

Cisco.com

- July 1991: An idea was born (21st IETF)
- March 1992: IPsec BoF (23rd IETF)
- November 1992: (25th IETF) IPsec working group formed
- By 1995 multiple interoperable implementations
- November 1998 RFC standards

And the work is still not done…



IPsec Framework

Cisco.com

November 1998 Set of Standards

RFC2401	Security Architecture for the Internet Protocol
RFC2402	IP Authentication Header (AH)
RFC2403	Use of HMAC-MD5-96 within ESP and AH
RFC2404	Use of HMAC-SHA-1-96 within ESP and AH
RFC2405	ESP DES-CBC Cipher Algorithm With Explicit IV
RFC2406	IP Encapsulating Security Payload (ESP)
RFC2407	Internet IP Security Domain of Interpretation for ISAKMP
RFC2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC2409	Internet Key Exchange (IKE)
RFC2410	NULL Encryption Algorithm and Its Use With IPsec
RFC2411	IP Security Document Roadmap
RFC2412	OAKLEY Key Determination Protocol

What is IPSec ?

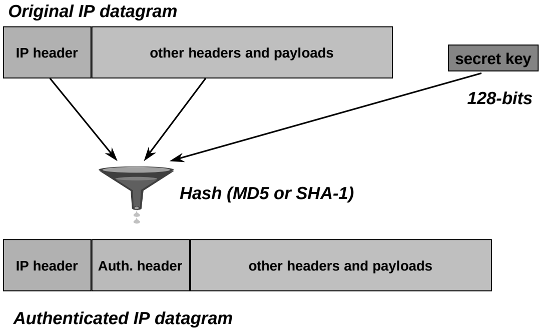
- RFC 2401-… Standards track
- This is a way to provide security services (confidentiality, integrity, …) through cryptography
- IPSec consists of 2 protocols:
  - Encapsulating Security Payload: confidentiality, authentication, integrity
  - Authentication Header: authentication, integrity
- IPSec defines
  - Packet format (encapsulation mainly)
  - Rules to be applied for packet processing

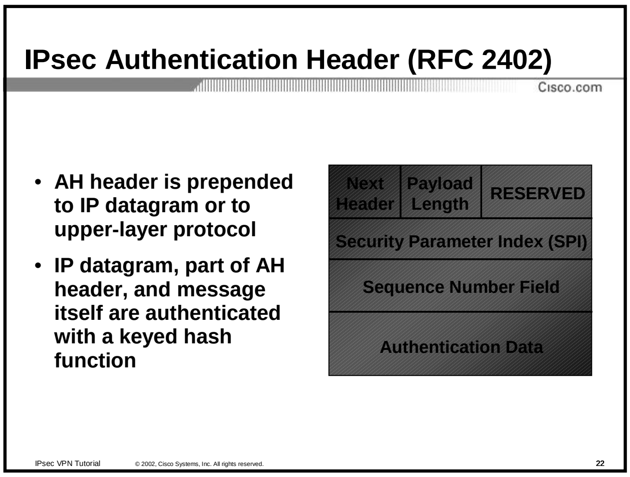
IPsec Authentication Header (RFC 2402)

Firewall
Router
All Data in Clear Text

- Data integrity - no twiddling of bits
- Origin authentication - definitely came from Router
- Uses keyed-hash mechanism
- Does not provide confidentiality
- Replay protection
- IP protocol type 51

IPsec Authentication Header (RFC 2402)

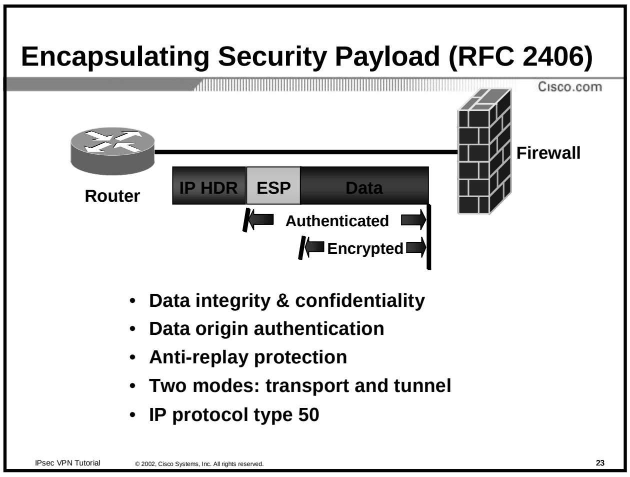




IPsec Authentication Header (RFC 2402)

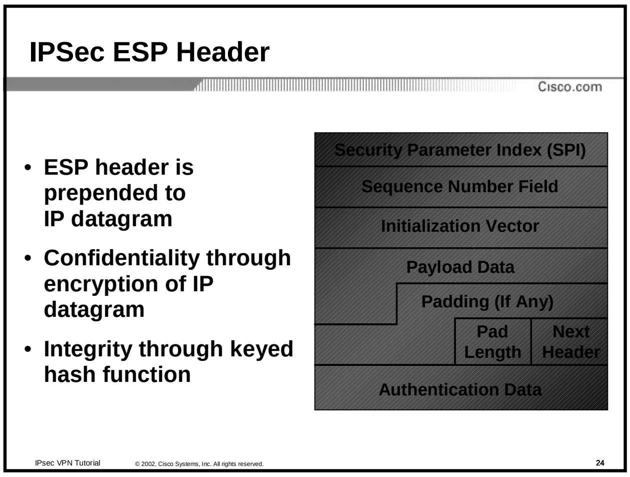
- **AH header is prepended to IP datagram or to upper-layer protocol**
- **IP datagram, part of AH header, and message itself are authenticated with a keyed hash function**

Next Header	Payload Length	RESERVED
Security Parameter Index (SPI)		
Sequence Number Field		
Authentication Data		



Encapsulating Security Payload (RFC 2406)

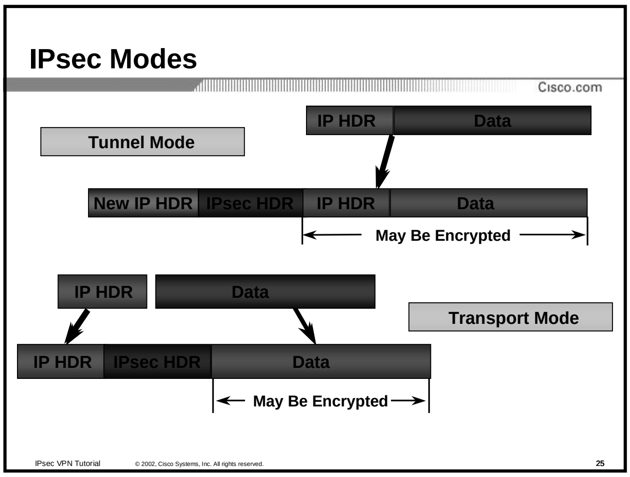
- **Data integrity & confidentiality**
- **Data origin authentication**
- **Anti-replay protection**
- **Two modes: transport and tunnel**
- **IP protocol type 50**



IPSec ESP Header

- **ESP header is prepended to IP datagram**
- **Confidentiality through encryption of IP datagram**
- **Integrity through keyed hash function**

Security Parameter Index (SPI)		
Sequence Number Field		
Initialization Vector		
Payload Data		
Padding (If Any)		
	Pad Length	Next Header
Authentication Data		



IPsec Modes

Cisco.com

Tunnel Mode

IP HDR | Data

New IP HDR | IPsec HDR | IP HDR | Data

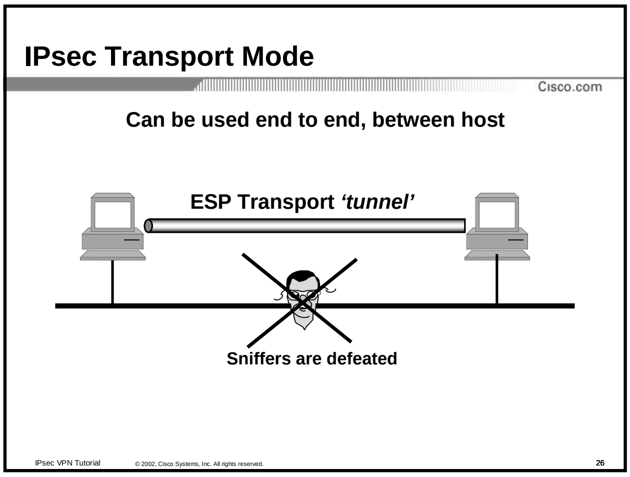
May Be Encrypted

Transport Mode

IP HDR | Data

IP HDR | IPsec HDR | Data

May Be Encrypted



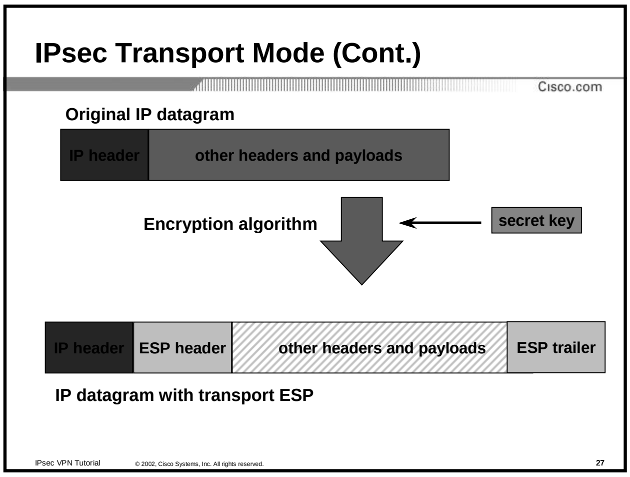
IPsec Transport Mode

Cisco.com

Can be used end to end, between host

ESP Transport *'tunnel'*

Sniffers are defeated



IPsec Transport Mode (Cont.)

Cisco.com

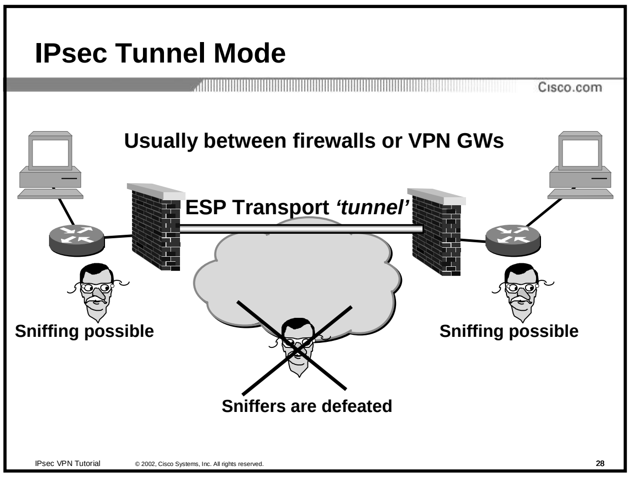
Original IP datagram

IP header | other headers and payloads

Encryption algorithm ← **secret key**

IP header | ESP header | other headers and payloads | ESP trailer

IP datagram with transport ESP



IPsec Tunnel Mode

Cisco.com

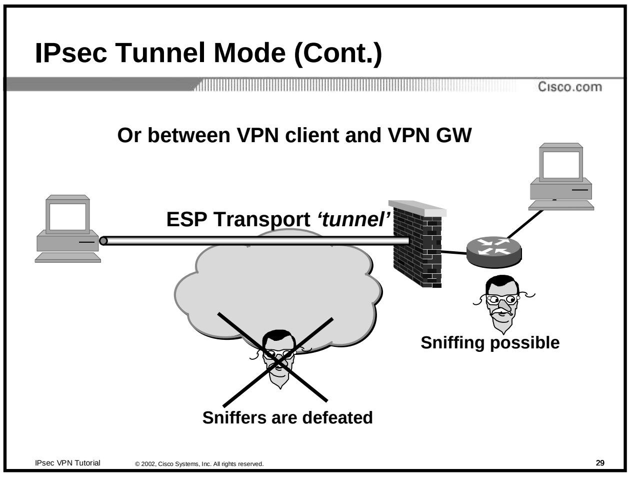
Usually between firewalls or VPN GWs

ESP Transport *'tunnel'*

Sniffing possible

Sniffing possible

Sniffers are defeated



IPsec Tunnel Mode (Cont.)

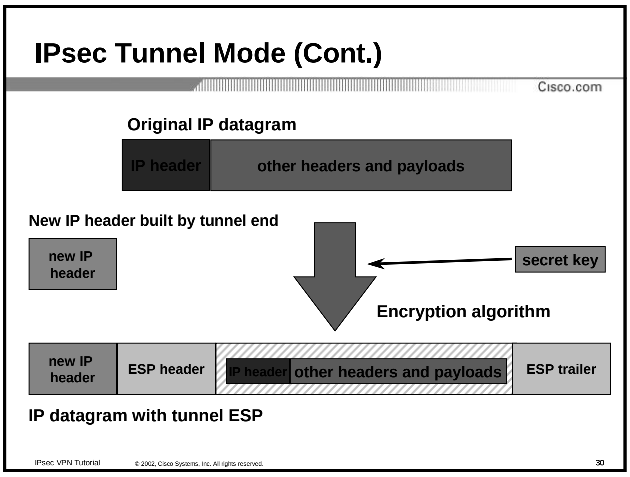
Cisco.com

Or between VPN client and VPN GW

ESP Transport *'tunnel'*

Sniffing possible

Sniffers are defeated



IPsec Tunnel Mode (Cont.)

Cisco.com

Original IP datagram

IP header | other headers and payloads

New IP header built by tunnel end

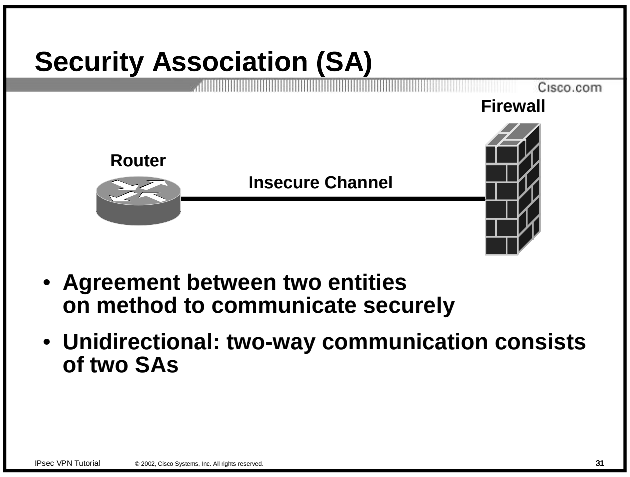
new IP header

secret key

Encryption algorithm

new IP header | ESP header | IP header | other headers and payloads | ESP trailer

IP datagram with tunnel ESP

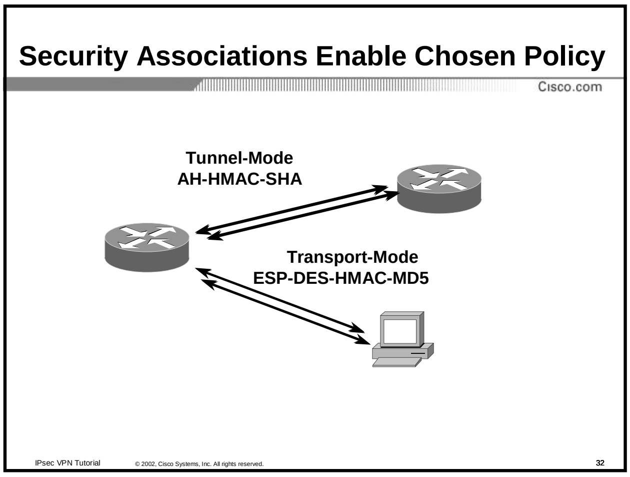


Security Association (SA)

Cisco.com

- **Agreement between two entities on method to communicate securely**
- **Unidirectional: two-way communication consists of two SAs**

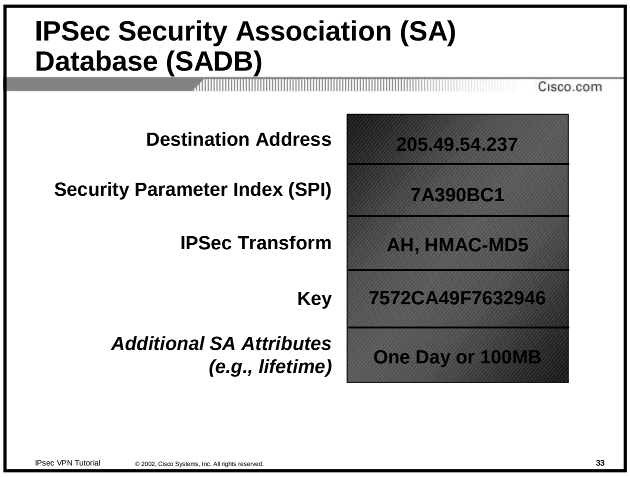
IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 31



Security Associations Enable Chosen Policy

Cisco.com

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 32

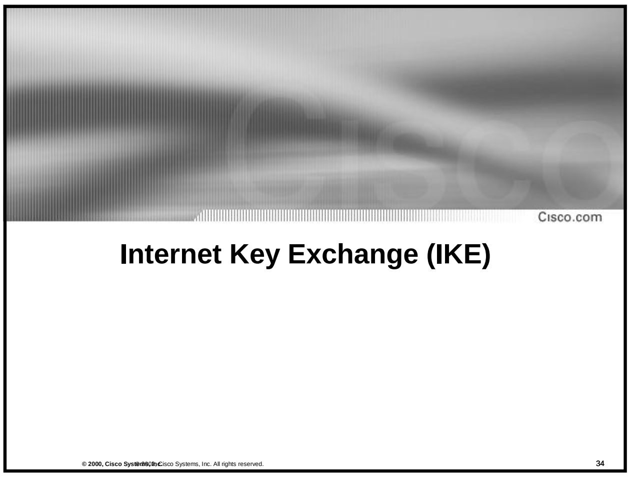


IPSec Security Association (SA) Database (SADB)

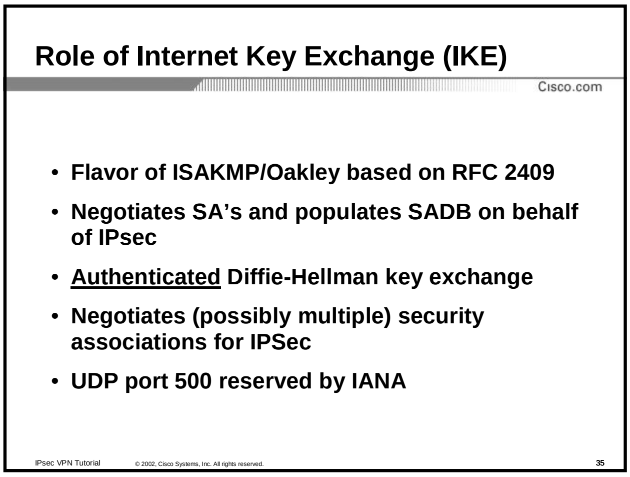
Cisco.com

Destination Address	**205.49.54.237**
Security Parameter Index (SPI)	**7A390BC1**
IPSec Transform	**AH, HMAC-MD5**
Key	**7572CA49F7632946**
Additional SA Attributes (e.g., lifetime)	**One Day or 100MB**

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 33

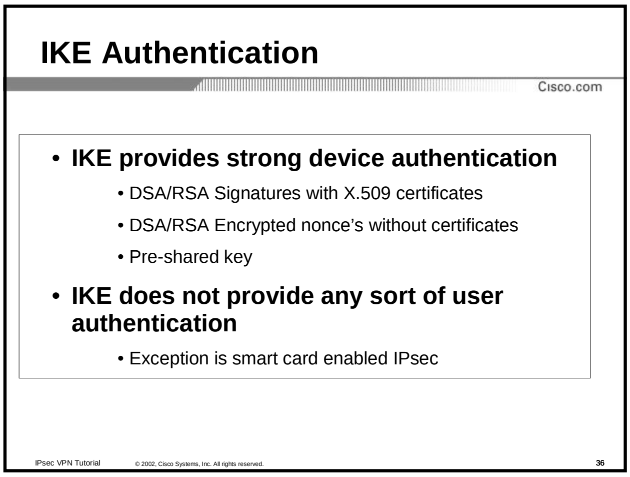


Internet Key Exchange (IKE)



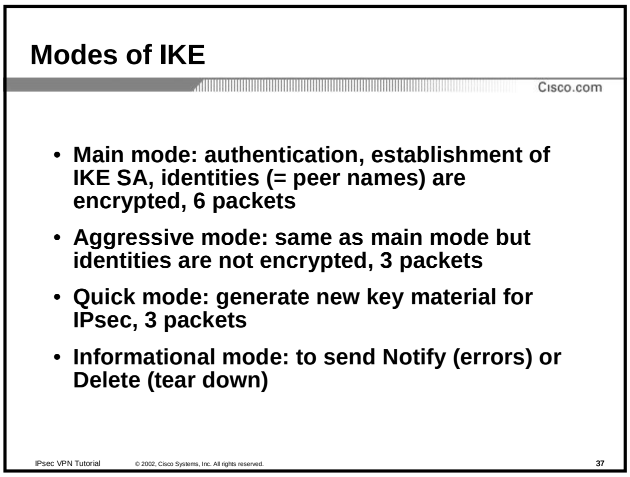
Role of Internet Key Exchange (IKE)

- **Flavor of ISAKMP/Oakley based on RFC 2409**
- **Negotiates SA's and populates SADB on behalf of IPsec**
- **Authenticated Diffie-Hellman key exchange**
- **Negotiates (possibly multiple) security associations for IPSec**
- **UDP port 500 reserved by IANA**



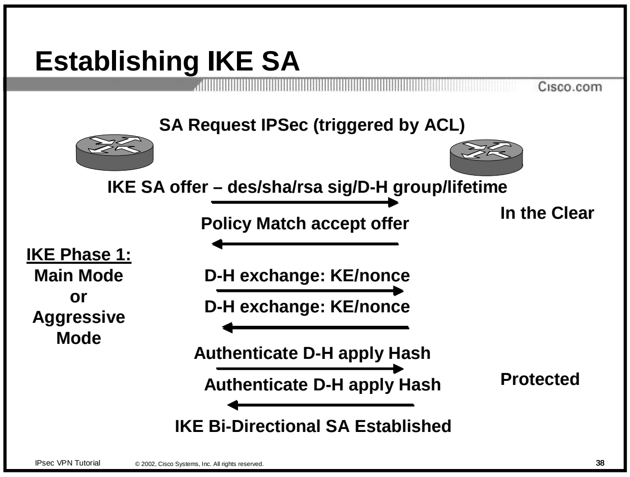
IKE Authentication

- **IKE provides strong device authentication**
  - DSA/RSA Signatures with X.509 certificates
  - DSA/RSA Encrypted nonce's without certificates
  - Pre-shared key
- **IKE does not provide any sort of user authentication**
  - Exception is smart card enabled IPsec



Modes of IKE

- Main mode: authentication, establishment of IKE SA, identities (= peer names) are encrypted, 6 packets
- Aggressive mode: same as main mode but identities are not encrypted, 3 packets
- Quick mode: generate new key material for IPsec, 3 packets
- Informational mode: to send Notify (errors) or Delete (tear down)



Establishing IKE SA

SA Request IPSec (triggered by ACL)

IKE SA offer – des/sha/rsa sig/D-H group/lifetime

In the Clear

Policy Match accept offer

IKE Phase 1:
Main Mode
or
Aggressive
Mode

D-H exchange: KE/nonce

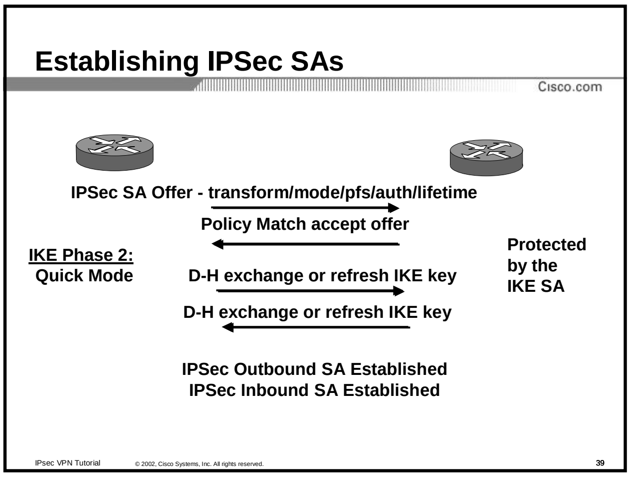
D-H exchange: KE/nonce

Authenticate D-H apply Hash

Authenticate D-H apply Hash

Protected

IKE Bi-Directional SA Established



Establishing IPSec SAs

IPSec SA Offer - transform/mode/pfs/auth/lifetime

Policy Match accept offer

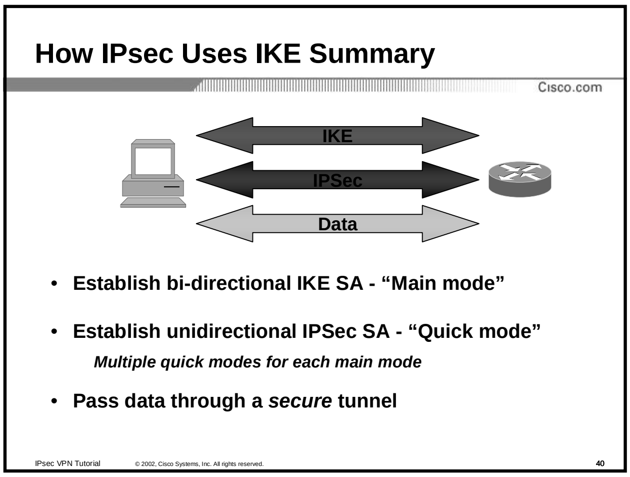
IKE Phase 2:
Quick Mode

Protected
by the
IKE SA

D-H exchange or refresh IKE key

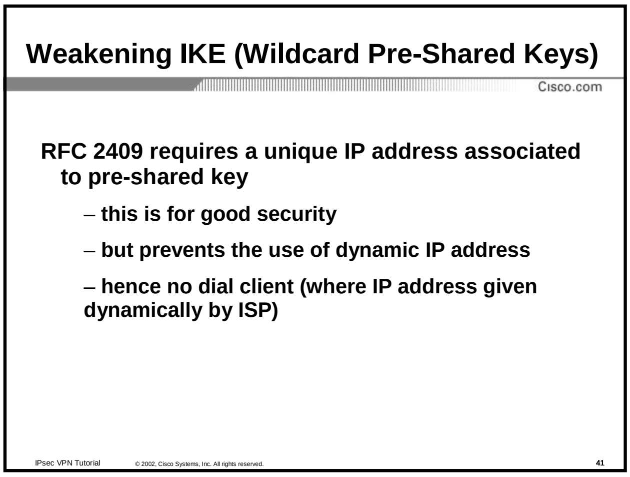
D-H exchange or refresh IKE key

IPSec Outbound SA Established
IPSec Inbound SA Established



How IPsec Uses IKE Summary

- Establish bi-directional IKE SA - “Main mode”
- Establish unidirectional IPSec SA - “Quick mode”
  - *Multiple quick modes for each main mode*
- Pass data through a *secure* tunnel



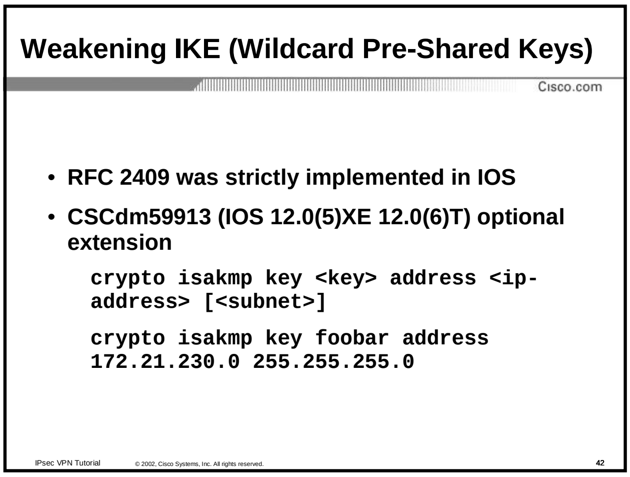
Weakening IKE (Wildcard Pre-Shared Keys)

RFC 2409 requires a unique IP address associated to pre-shared key

– this is for good security

– but prevents the use of dynamic IP address

– hence no dial client (where IP address given dynamically by ISP)

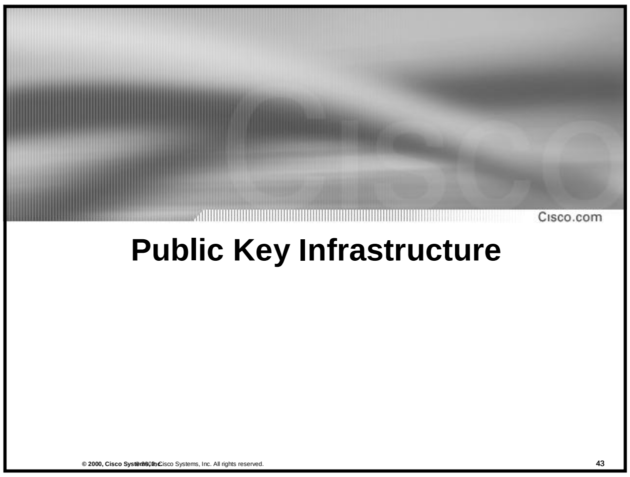


Weakening IKE (Wildcard Pre-Shared Keys)

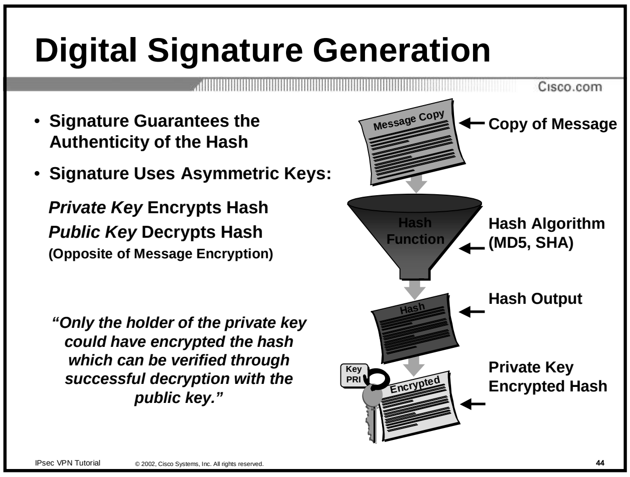
- RFC 2409 was strictly implemented in IOS
- CSCdm59913 (IOS 12.0(5)XE 12.0(6)T) optional extension

```
crypto isakmp key <key> address <ip-
address> [<subnet>]

crypto isakmp key foobar address
172.21.230.0 255.255.255.0
```



Public Key Infrastructure



Digital Signature Generation

- Signature Guarantees the Authenticity of the Hash
- Signature Uses Asymmetric Keys:

Private Key Encrypts Hash
Public Key Decrypts Hash
(Opposite of Message Encryption)

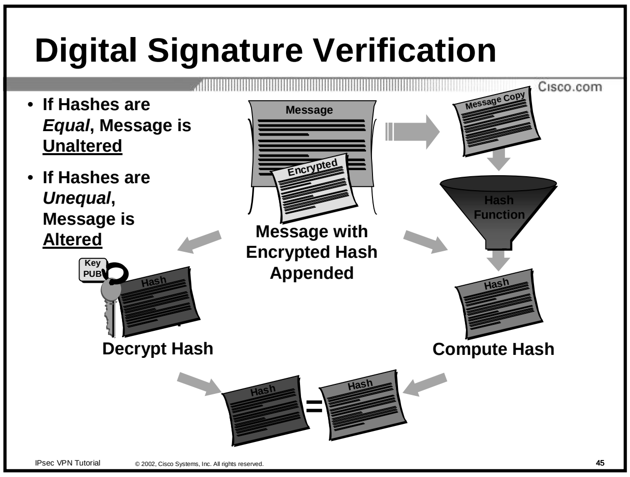
"Only the holder of the private key could have encrypted the hash which can be verified through successful decryption with the public key."

Copy of Message

Hash Algorithm (MD5, SHA)

Hash Output

Private Key Encrypted Hash



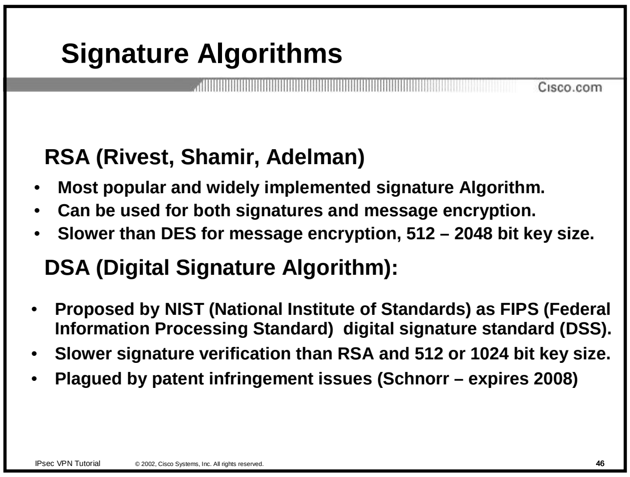
Digital Signature Verification

- If Hashes are *Equal*, Message is Unaltered
- If Hashes are *Unequal*, Message is Altered

Message with Encrypted Hash Appended

Decrypt Hash

Compute Hash



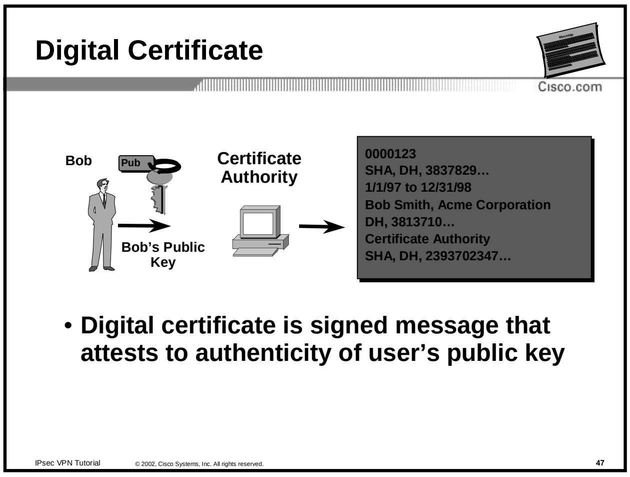
Signature Algorithms

RSA (Rivest, Shamir, Adelman)

- Most popular and widely implemented signature Algorithm.
- Can be used for both signatures and message encryption.
- Slower than DES for message encryption, 512 – 2048 bit key size.

DSA (Digital Signature Algorithm):

- Proposed by NIST (National Institute of Standards) as FIPS (Federal Information Processing Standard) digital signature standard (DSS).
- Slower signature verification than RSA and 512 or 1024 bit key size.
- Plagued by patent infringement issues (Schnorr – expires 2008)



Digital Certificate

Bob

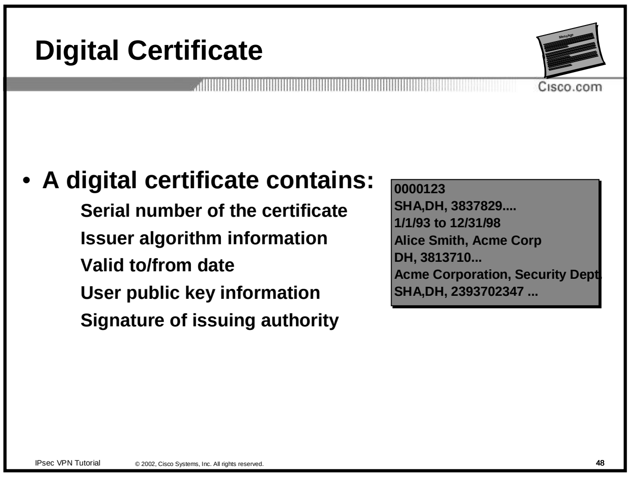
Pub

Bob's Public Key

Certificate Authority

0000123
SHA, DH, 3837829…
1/1/97 to 12/31/98
Bob Smith, Acme Corporation
DH, 3813710…
Certificate Authority
SHA, DH, 2393702347…

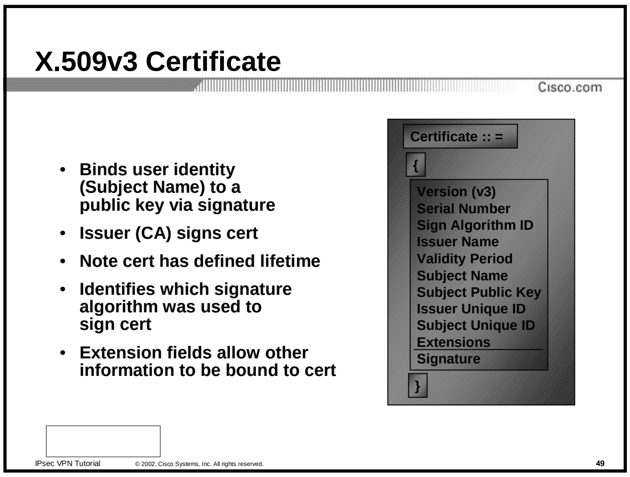
- Digital certificate is signed message that attests to authenticity of user's public key



Digital Certificate

- A digital certificate contains:
  - Serial number of the certificate
  - Issuer algorithm information
  - Valid to/from date
  - User public key information
  - Signature of issuing authority

0000123
SHA,DH, 3837829....
1/1/93 to 12/31/98
Alice Smith, Acme Corp
DH, 3813710...
Acme Corporation, Security Dept.
SHA,DH, 2393702347 ...



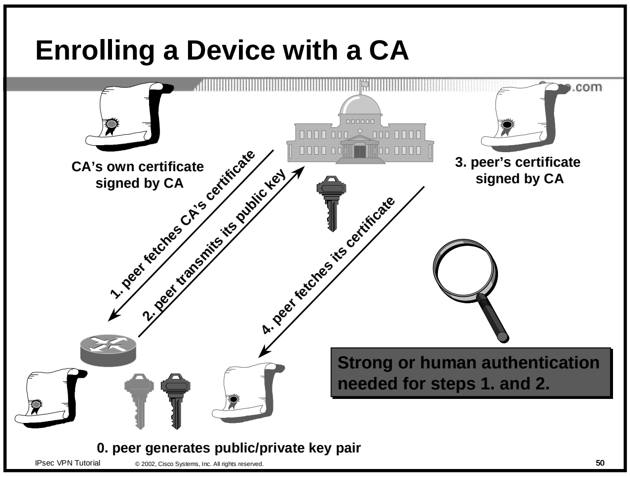
X.509v3 Certificate

Cisco.com

- Binds user identity (Subject Name) to a public key via signature
- Issuer (CA) signs cert
- Note cert has defined lifetime
- Identifies which signature algorithm was used to sign cert
- Extension fields allow other information to be bound to cert

Certificate :: =
{
Version (v3)
Serial Number
Sign Algorithm ID
Issuer Name
Validity Period
Subject Name
Subject Public Key
Issuer Unique ID
Subject Unique ID
Extensions
Signature
}

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 49



Enrolling a Device with a CA

.com

CA's own certificate signed by CA

3. peer's certificate signed by CA

1. peer fetches CA's certificate

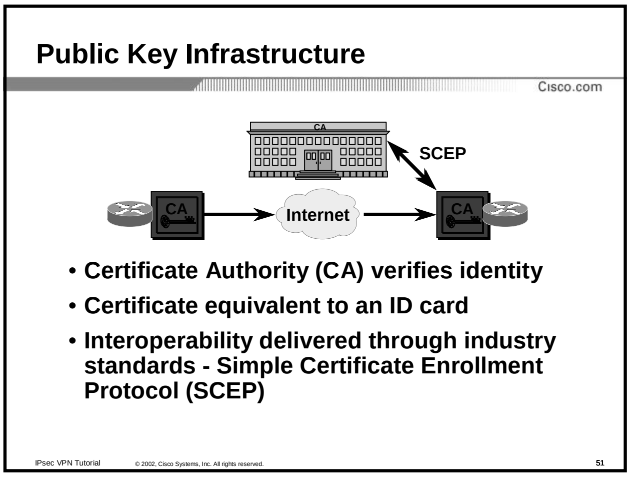
2. peer transmits its public key

4. peer fetches its certificate

Strong or human authentication needed for steps 1. and 2.

0. peer generates public/private key pair

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 50



Public Key Infrastructure

Cisco.com

- Certificate Authority (CA) verifies identity
- Certificate equivalent to an ID card
- Interoperability delivered through industry standards - Simple Certificate Enrollment Protocol (SCEP)

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 51

Simple Certificate Enrollment Protocol

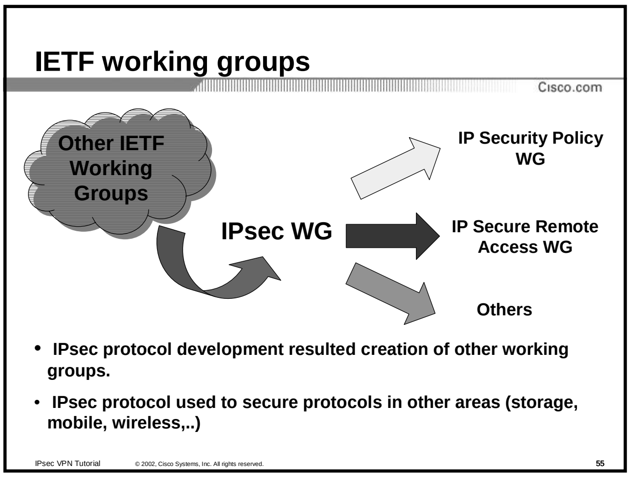
- **Based on CRS draft**
- **PKCS #7 for signing and enveloping**
- **PKCS #10 for certificate request**
- **HTTP and LDAP for transport**
- **Requires out of band authentication during enrollment**
- **CRL distribution is optional**

PKI and Cisco

- **Build open PKI aligned with PKIX**

  http://www.ietf.org/internet-drafts/draft-nourse-scep-06.txt
- **Support of leading CA vendors**
  - ✔ **Verisign summer 98**
  - ✔ **Entrust summer 98**
  - ✔ **Netscape CMS 3.1 end 99**
  - ✔ **Microsoft Windows 2000 February 00** *requires Windows Resource Kit*
  - – **Baltimore Technologies 00**
  - – **RSA Keon, XCert,…**

IPsec Extensions



IETF working groups

Other IETF Working Groups

IPsec WG

IP Security Policy WG

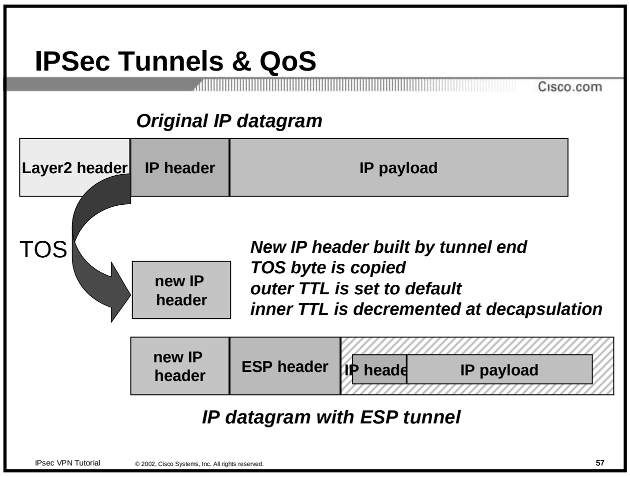
IP Secure Remote Access WG

Others

- IPsec protocol development resulted creation of other working groups.
- IPsec protocol used to secure protocols in other areas (storage, mobile, wireless,..)

IPsec Extensions

- IPsec and QoS
- IPsec and Keepalives
- IPsec and remote access VPNs
- IPsec and NAT
- IPsec future developments



IPSec Tunnels & QoS

Original IP datagram

Layer2 header | IP header | IP payload

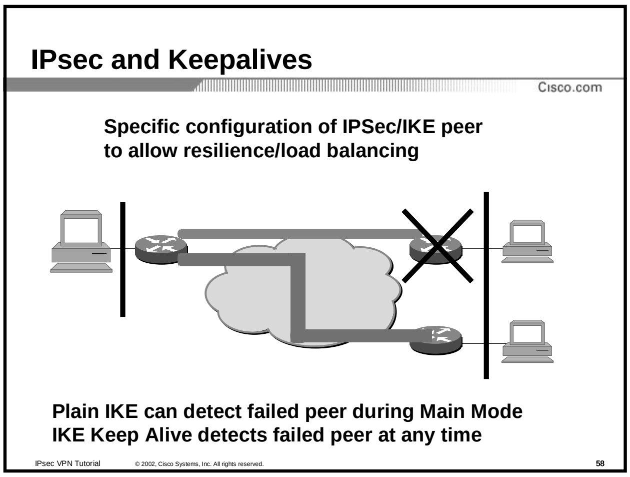
TOS

new IP header

New IP header built by tunnel end
TOS byte is copied
outer TTL is set to default
inner TTL is decremented at decapsulation

new IP header | ESP header | IP heade | IP payload

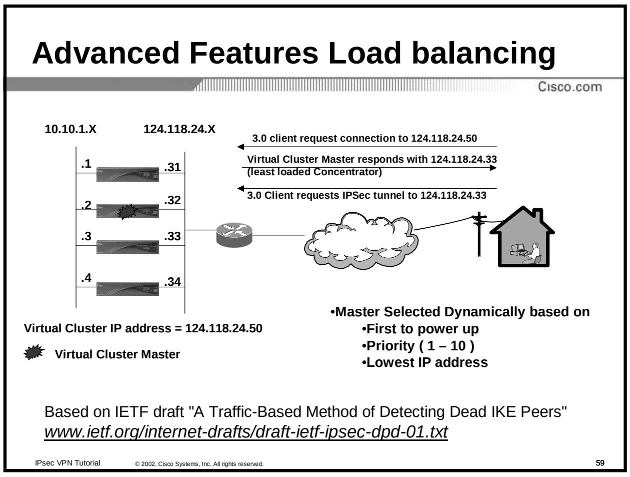
IP datagram with ESP tunnel



IPsec and Keepalives

Specific configuration of IPSec/IKE peer to allow resilience/load balancing

Plain IKE can detect failed peer during Main Mode
IKE Keep Alive detects failed peer at any time



Advanced Features Load balancing

Cisco.com
10.10.1.X
124.118.24.X
.1
.31
.2
.32
.3
.33
.4
.34

3.0 client request connection to 124.118.24.50

Virtual Cluster Master responds with 124.118.24.33 (least loaded Concentrator)

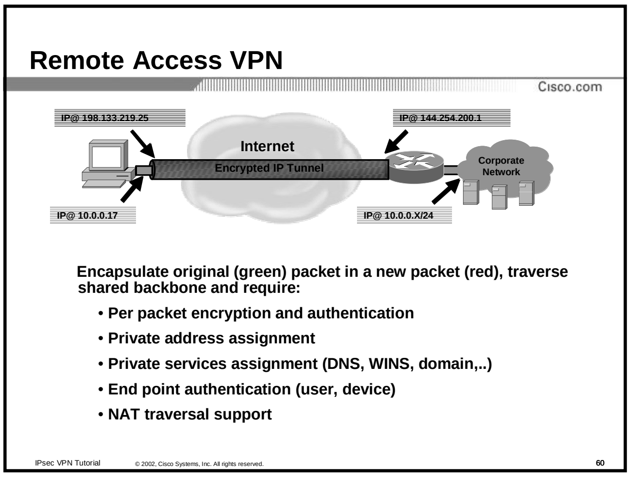
3.0 Client requests IPSec tunnel to 124.118.24.33

Virtual Cluster IP address = 124.118.24.50

Virtual Cluster Master

- **Master Selected Dynamically based on**
  - **First to power up**
  - **Priority (1 – 10)**
  - **Lowest IP address**

Based on IETF draft "A Traffic-Based Method of Detecting Dead IKE Peers"
www.ietf.org/internet-drafts/draft-ietf-ipsec-dpd-01.txt

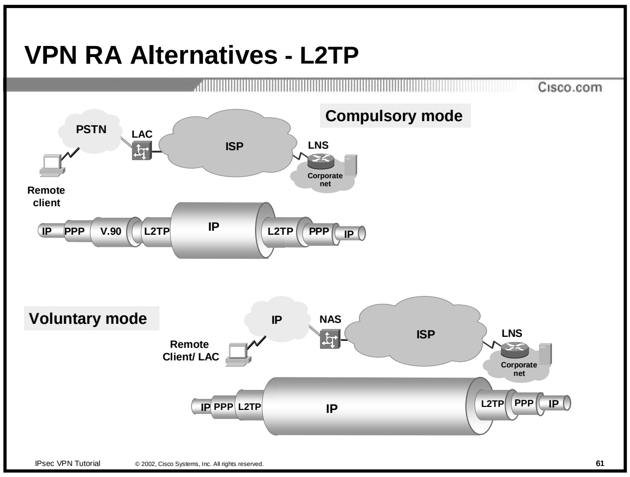


Remote Access VPN

Cisco.com
IP@ 198.133.219.25
IP@ 144.254.200.1
Internet
Encrypted IP Tunnel
Corporate Network
IP@ 10.0.0.17
IP@ 10.0.0.X/24

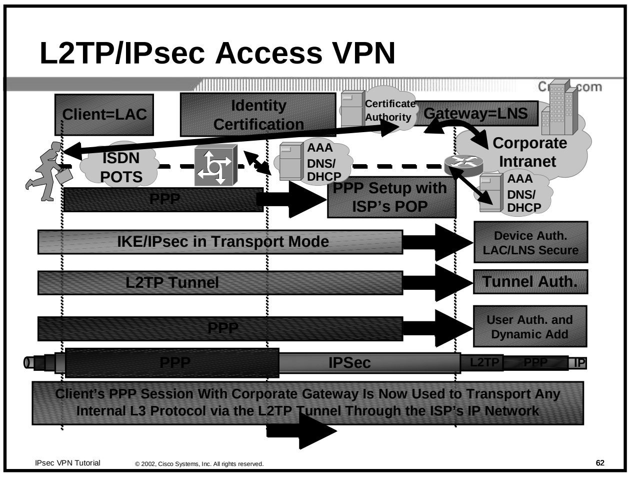
Encapsulate original (green) packet in a new packet (red), traverse shared backbone and require:

- **Per packet encryption and authentication**
- **Private address assignment**
- **Private services assignment (DNS, WINS, domain,..)**
- **End point authentication (user, device)**
- **NAT traversal support**



VPN RA Alternatives - L2TP

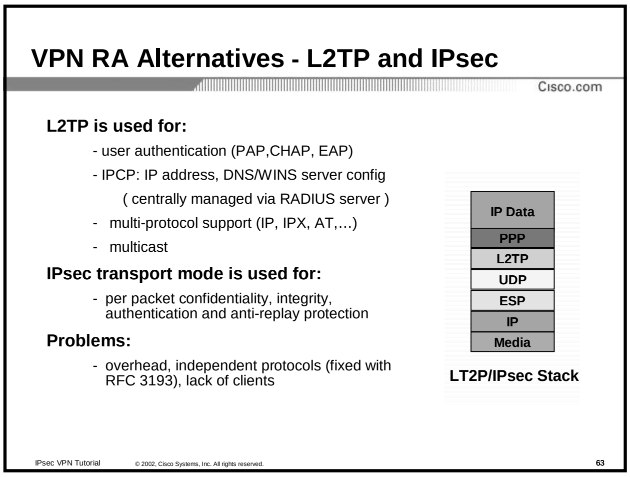
IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 61



L2TP/IPsec Access VPN

Client's PPP Session With Corporate Gateway Is Now Used to Transport Any Internal L3 Protocol via the L2TP Tunnel Through the ISP's IP Network

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 62



VPN RA Alternatives - L2TP and IPsec

L2TP is used for:

- user authentication (PAP,CHAP, EAP)
- IPCP: IP address, DNS/WINS server config
  (centrally managed via RADIUS server)
- multi-protocol support (IP, IPX, AT,…)
- multicast

IPsec transport mode is used for:

- per packet confidentiality, integrity, authentication and anti-replay protection

Problems:

- overhead, independent protocols (fixed with RFC 3193), lack of clients

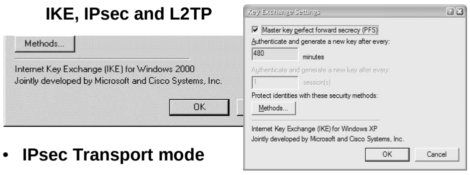
LT2P/IPsec Stack

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 63

Windows 2000/XP VPN Client

- Cisco and Microsoft Co-development

  IKE, IPsec and L2TP



Methods...

Internet Key Exchange (IKE) for Windows 2000
Jointly developed by Microsoft and Cisco Systems, Inc.

OK

Key Exchange Settings

☑ Master key perfect forward secrecy (PFS)

Authenticate and generate a new key after every:
480 minutes

Authenticate and generate a new key after every:
1 session(s)

Protect identities with these security methods:
Methods...

Internet Key Exchange (IKE) for Windows XP
Jointly developed by Microsoft and Cisco Systems, Inc.

OK Cancel

- IPsec Transport mode

  Caveats for remote access - no IKE extensions

IKE Configuration Method (IKE mode-cfg)

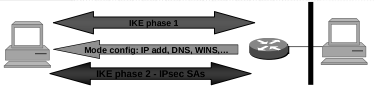
www.ietf.org/internet-drafts/draft-dukes-ike-mode-cfg-02.txt

- **IETF draft to allow the dynamic allocation of IP parameters to an IPSec client (a la DHCP or IPCP of PPP).**

- **Just after IKE phase I (main or aggressive mode)**

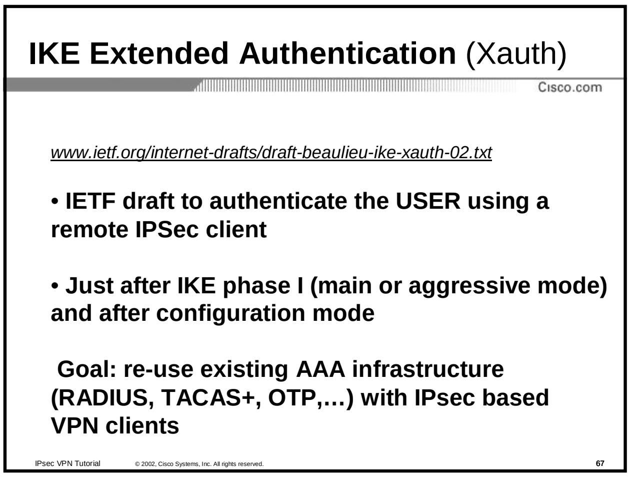
Goal: easy configuration of IPSec client

VPN RA Alternatives - IKE Mode Config



```
Attribute                Value   Type       Length
======================== ======= ========== ====================
INTERNAL_IP4_ADDRESS        1     Variable   0 or 4 octets
INTERNAL_IP4_NETMASK        2     Variable   0 or 4 octets
INTERNAL_IP4_DNS            3     Variable   0 or 4 octets
INTERNAL_IP4_NBNS           4     Variable   0 or 4 octets
INTERNAL_ADDRESS_EXPIRY     5     Variable   0 or 4 octets
INTERNAL_IP4_DHCP           6     Variable   0 or 4 octets
APPLICATION_VERSION         7     Variable   0 or more
INTERNAL_IP4_SUBNET        13     Variable   0 or 8 octets
...                     ...
Reserved for future use  16-16383
Reserved for private use 16384-32767
```

draft-dukes-ike-mode-cfg-02.txt

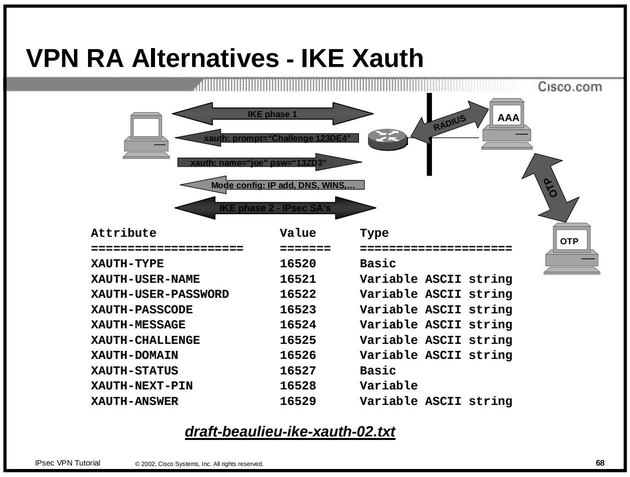


IKE Extended Authentication (Xauth)

www.ietf.org/internet-drafts/draft-beaulieu-ike-xauth-02.txt

- **IETF draft to authenticate the USER using a remote IPSec client**
- **Just after IKE phase I (main or aggressive mode) and after configuration mode**

Goal: re-use existing AAA infrastructure (RADIUS, TACAS+, OTP,…) with IPsec based VPN clients

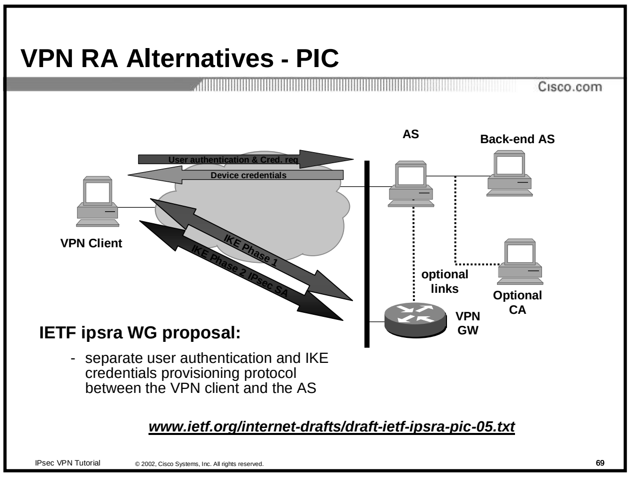


VPN RA Alternatives - IKE Xauth

Cisco.com
IKE phase 1
xauth: prompt="Challenge 123DE4"
xauth: name="joe" psw="13ZD3"
Mode config: IP add, DNS, WINS,…
IKE phase 2 - IPsec SA's
RADIUS
AAA
OTP
OTP

```
Attribute                Value      Type
=====================    =======    =====================
XAUTH-TYPE               16520      Basic
XAUTH-USER-NAME          16521      Variable ASCII string
XAUTH-USER-PASSWORD      16522      Variable ASCII string
XAUTH-PASSCODE           16523      Variable ASCII string
XAUTH-MESSAGE            16524      Variable ASCII string
XAUTH-CHALLENGE          16525      Variable ASCII string
XAUTH-DOMAIN             16526      Variable ASCII string
XAUTH-STATUS             16527      Basic
XAUTH-NEXT-PIN           16528      Variable
XAUTH-ANSWER             16529      Variable ASCII string
```

draft-beaulieu-ike-xauth-02.txt



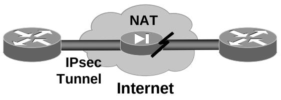
VPN RA Alternatives - PIC

IETF ipsra WG proposal:

- separate user authentication and IKE credentials provisioning protocol between the VPN client and the AS

www.ietf.org/internet-drafts/draft-ietf-ipsra-pic-05.txt

Network Address Translation and IPsec



- PAT breaks IPsec
- NAT works with ESP and tunnel mode
- NAT with AH breaks IPsec
- Fixing this in remote access: one further encapsulations (TCP or UDP)

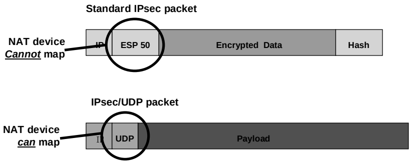
IPsec VPN and NAT/PAT Transparency

- IPsec/UDP

  Allows clients to operate behind a NAT device

  Provides the security of IPsec/ESP

  Requires no user intervention



IPsec over NAT

- IPsec UDP encapsulation:

  – defines methods to encapsulate and decapsulate ESP packets inside UDP packets for the purpose of traversing NATs.

- IPsec NAT-T:

  - describes how to detect one or more NATs between IPsec hosts, and how to negotiate the use of UDP encapsulation of the IPsec packets through the NAT boxes in IKE

NAT Traversal (NAT-T)

- **Cisco, Microsoft, SSH, F-Secure, and Nortel have merged their own proposals into a single draft set:**

www.ietf.org/internet-drafts/draft-ietf-ipsec-udp-encaps-03.txt

www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-t-ike-03.txt

- **IETF meetings confirmed that there will not be any major modifications to the existing drafts. At Helsinki IPsec bakeoff , Microsoft, SSH, F-Secure, Netscreen, and PGP already tested their own implementations of the IETF UDP wrapper successfully.**

IPsec future developments

- **Reduce complexity of existing framework**
- **Standardize method of IPsec traversing firewalls and NAT boxes**
- **Standardize method for peer detection**
- **New algorithms support (AES,SHA-256,...)**
- **New protocols support (SCTP,iSCSI,…)**
- **New Key Exchange protocol**

Two proposals at the IETF:

- **IKEv2**
- **JFK**

Advanced Encryption Standard (AES)

> **"December 4, 2001 - FIPS 197,**
>
> **Advanced Encryption Standard (AES) became a Federal standard on November 26, 2001 and was announced in a Federal Register Notice and in a press release today.**
>
> **AES was developed to replace the Data Encryption Standard (DES) in a multi-year effort that began in 1997. The AES specifies a cryptographic algorithm that can be used to protect electronic data by encrypting (enciphering) and decrypting (deciphering) information."**

Source NIST: *www.nist.gov/public_affairs/releases/g01-111.htm*

ESP/AH revisions

- **ESP Sequence numbers extended**
  - new option for a 64-bit sequence number for high-speed communications.
- **ESP TFC (traffic flow confidentiality) padding**
  - added requirement to be able to add bytes after the end of the IP Payload
- **ESP Algorithms**
  - AES in CBC mode, MUST implement: HMAC-MD5, HMAC-SHA-1, NULL Encryption algorithm

www.ietf.org/internet-drafts/draft-ietf-ipsec-esp-v3-03.txt

- **AH** - Sequence numbers extended - 64 bits

www.ietf.org/internet-drafts/draft-ietf-ipsec-rfc2402bis-01.txt

IPsec and AES usage drafts

- **AES in CBC mode draft:**
  - **must 128 and MAY for 192 and 256 keys**

www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-aes-cbc-04.txt

- **AES in IPsec for hashing**
  - **AES XCBC - MAC**

www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-aes-xcbc-mac-02.txt

- **New DH mode groups**
  - **documents the used 1536 bits group-5 (RFC-2409), and also defines new 2048, 3072, 4096, 6144, and 8192 bits (15430?)**

www.ietf.org/internet-drafts/draft-ietf-ipsec-ike-modp-groups-04.txt

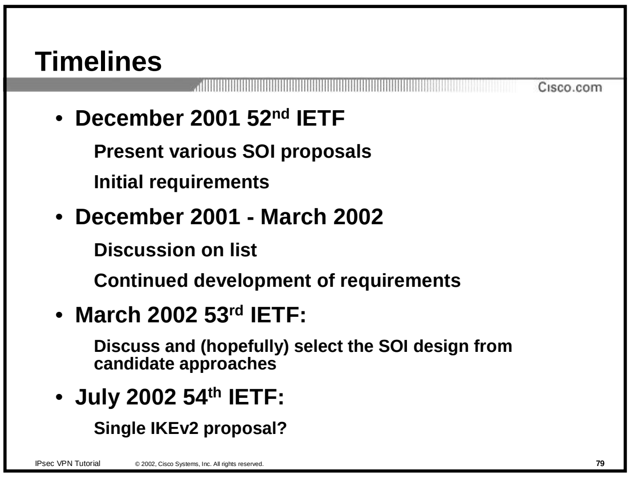
51st IETF - Security Area Director Position

Formal and semi-formal analyses by Meadows, Schneier et al, and Simpson, have shown that the security problems in IKE stem directly from its *complexity*… It seems also, only a matter of time, before serious **implementation* problems* become apparent…

Security Area directors in the IETF… hereby place a *temporary moratorium* on the addition of new features to IKE

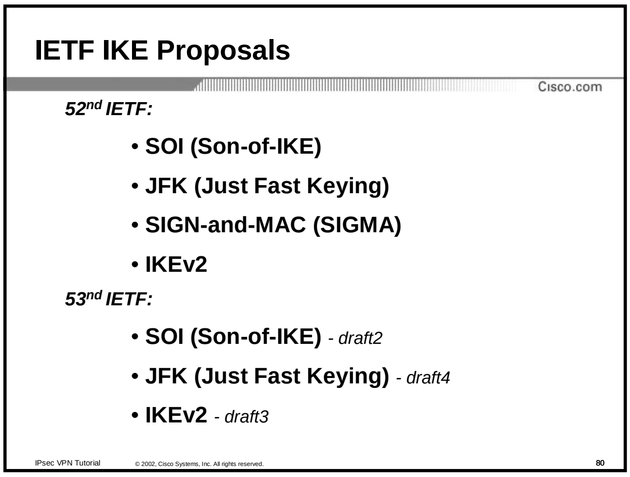
Marcus Leech (IESG) Jeff Schiller (IESG) Steve Bellovin (IAB)

11 ESP Encryption
4 ESP Integrity
6 IKE Encryption
3 IKE Integrity
1 IKE PFS
5 Ph1 DH Grp
5 Ph2 DH Grp
5 Authentication
--
99000 possible combinations



Timelines

- December 2001 52nd IETF
  - Present various SOI proposals
  - Initial requirements
- December 2001 - March 2002
  - Discussion on list
  - Continued development of requirements
- March 2002 53rd IETF:
  - Discuss and (hopefully) select the SOI design from candidate approaches
- July 2002 54th IETF:
  - Single IKEv2 proposal?



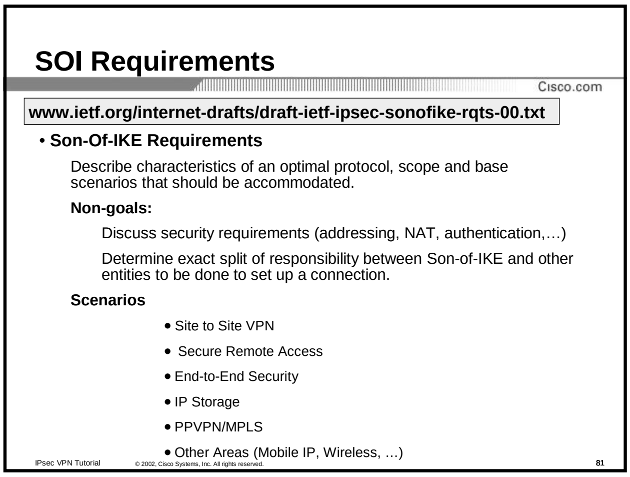
IETF IKE Proposals

52nd IETF:

- SOI (Son-of-IKE)
- JFK (Just Fast Keying)
- SIGN-and-MAC (SIGMA)
- IKEv2

53nd IETF:

- SOI (Son-of-IKE) *- draft2*
- JFK (Just Fast Keying) *- draft4*
- IKEv2 *- draft3*



SOI Requirements

www.ietf.org/internet-drafts/draft-ietf-ipsec-sonofike-rqts-00.txt

- **Son-Of-IKE Requirements**

  Describe characteristics of an optimal protocol, scope and base scenarios that should be accommodated.

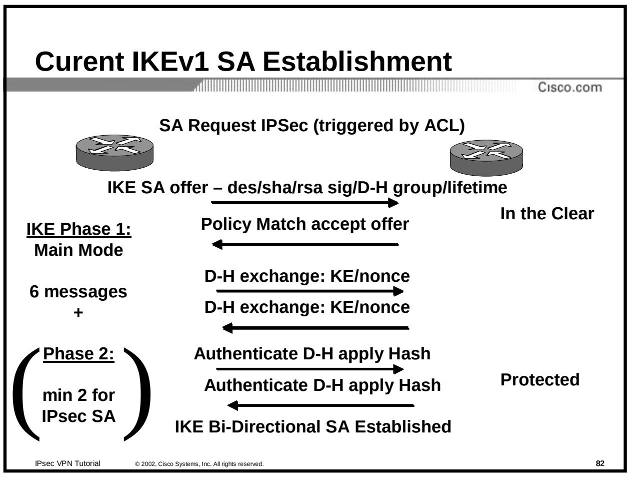
  Non-goals:

  Discuss security requirements (addressing, NAT, authentication,…)

  Determine exact split of responsibility between Son-of-IKE and other entities to be done to set up a connection.

  Scenarios

  - Site to Site VPN
  - Secure Remote Access
  - End-to-End Security
  - IP Storage
  - PPVPN/MPLS
  - Other Areas (Mobile IP, Wireless, …)



Curent IKEv1 SA Establishment

SA Request IPSec (triggered by ACL)

IKE SA offer – des/sha/rsa sig/D-H group/lifetime

In the Clear

IKE Phase 1:
Main Mode

6 messages
+

(Phase 2:

min 2 for
IPsec SA)

Policy Match accept offer

D-H exchange: KE/nonce

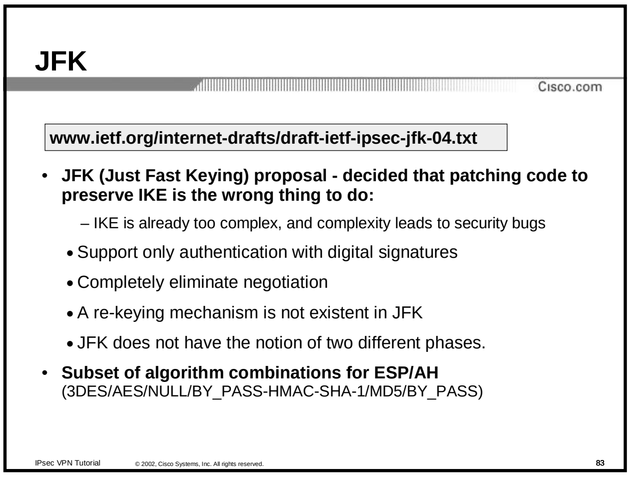
D-H exchange: KE/nonce

Authenticate D-H apply Hash

Authenticate D-H apply Hash

Protected

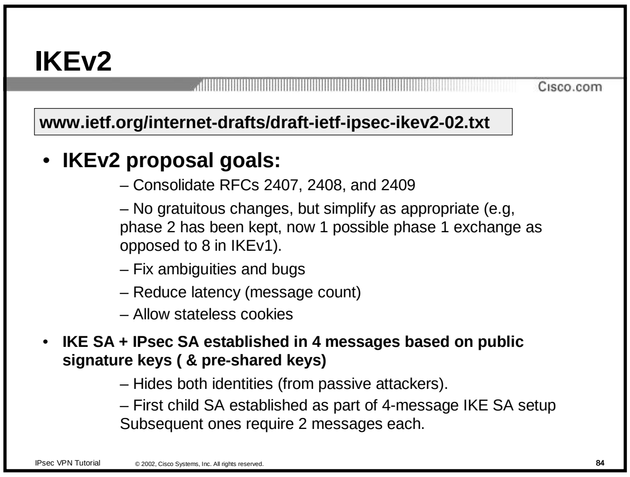
IKE Bi-Directional SA Established



JFK

www.ietf.org/internet-drafts/draft-ietf-ipsec-jfk-04.txt

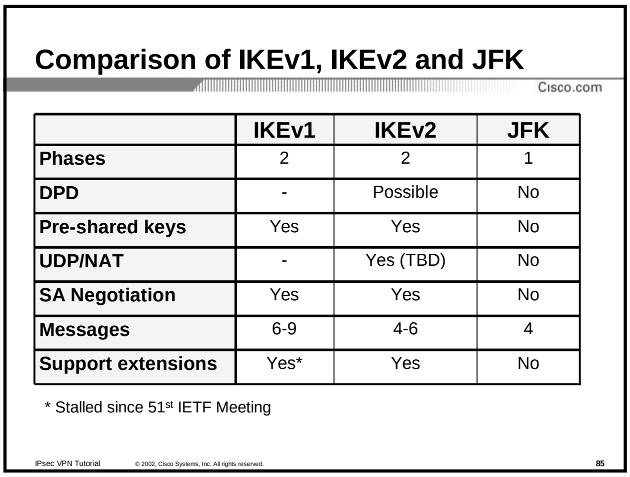
- **JFK (Just Fast Keying) proposal - decided that patching code to preserve IKE is the wrong thing to do:**
  - IKE is already too complex, and complexity leads to security bugs
  - Support only authentication with digital signatures
  - Completely eliminate negotiation
  - A re-keying mechanism is not existent in JFK
  - JFK does not have the notion of two different phases.
- **Subset of algorithm combinations for ESP/AH** (3DES/AES/NULL/BY_PASS-HMAC-SHA-1/MD5/BY_PASS)



IKEv2

www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-02.txt

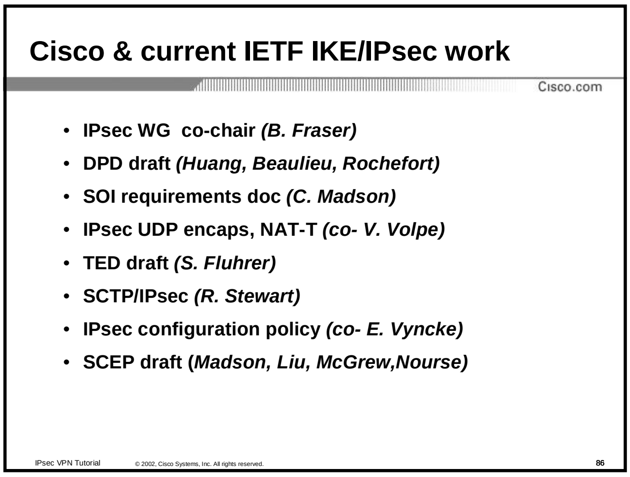
- **IKEv2 proposal goals:**
  - Consolidate RFCs 2407, 2408, and 2409
  - No gratuitous changes, but simplify as appropriate (e.g, phase 2 has been kept, now 1 possible phase 1 exchange as opposed to 8 in IKEv1).
  - Fix ambiguities and bugs
  - Reduce latency (message count)
  - Allow stateless cookies
- **IKE SA + IPsec SA established in 4 messages based on public signature keys (& pre-shared keys)**
  - Hides both identities (from passive attackers).
  - First child SA established as part of 4-message IKE SA setup Subsequent ones require 2 messages each.



Comparison of IKEv1, IKEv2 and JFK

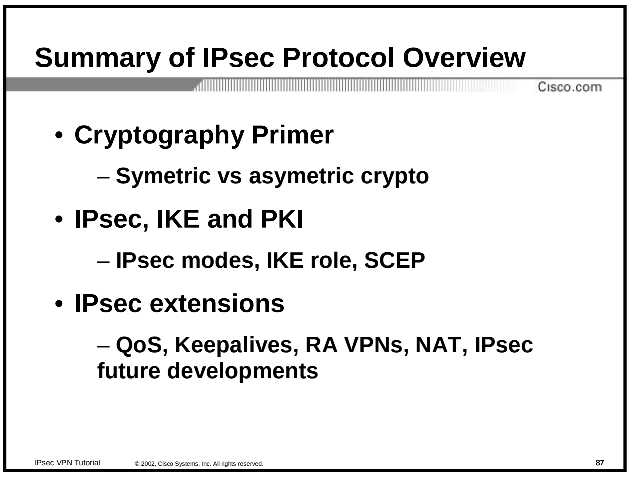
	IKEv1	IKEv2	JFK
Phases	2	2	1
DPD	-	Possible	No
Pre-shared keys	Yes	Yes	No
UDP/NAT	-	Yes (TBD)	No
SA Negotiation	Yes	Yes	No
Messages	6-9	4-6	4
Support extensions	Yes*	Yes	No

* Stalled since 51st IETF Meeting



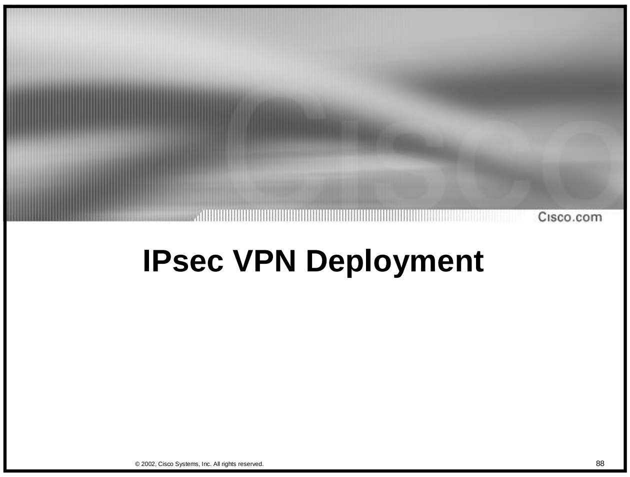
Cisco & current IETF IKE/IPsec work

- **IPsec WG co-chair *(B. Fraser)***
- **DPD draft *(Huang, Beaulieu, Rochefort)***
- **SOI requirements doc *(C. Madson)***
- **IPsec UDP encaps, NAT-T *(co- V. Volpe)***
- **TED draft *(S. Fluhrer)***
- **SCTP/IPsec *(R. Stewart)***
- **IPsec configuration policy *(co- E. Vyncke)***
- **SCEP draft (*Madson, Liu, McGrew,Nourse)***



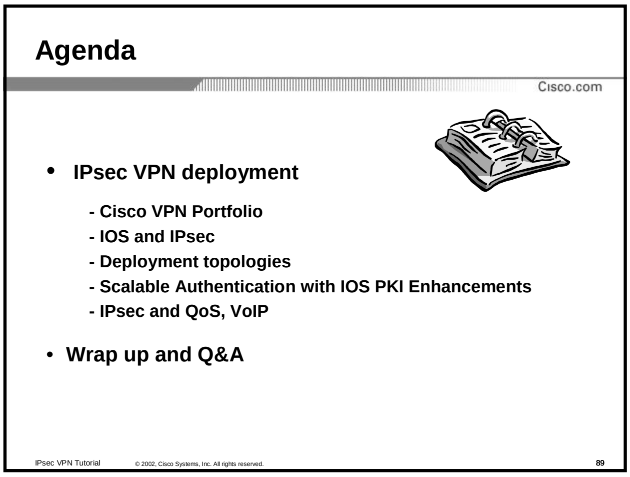
Summary of IPsec Protocol Overview

- **Cryptography Primer**
  - **Symetric vs asymetric crypto**
- **IPsec, IKE and PKI**
  - **IPsec modes, IKE role, SCEP**
- **IPsec extensions**
  - **QoS, Keepalives, RA VPNs, NAT, IPsec future developments**



Cisco.com

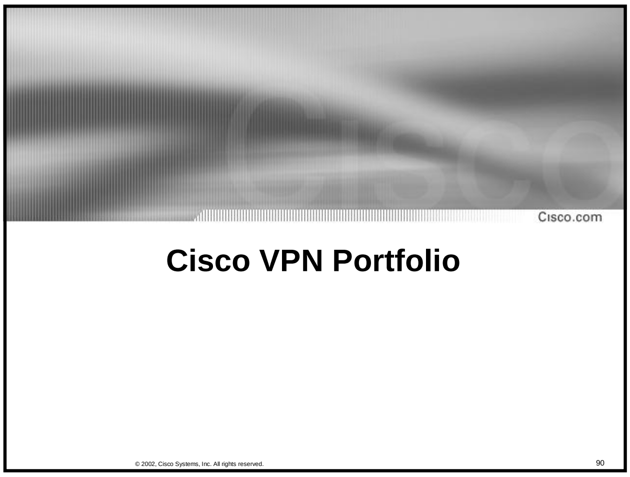
IPsec VPN Deployment



Agenda

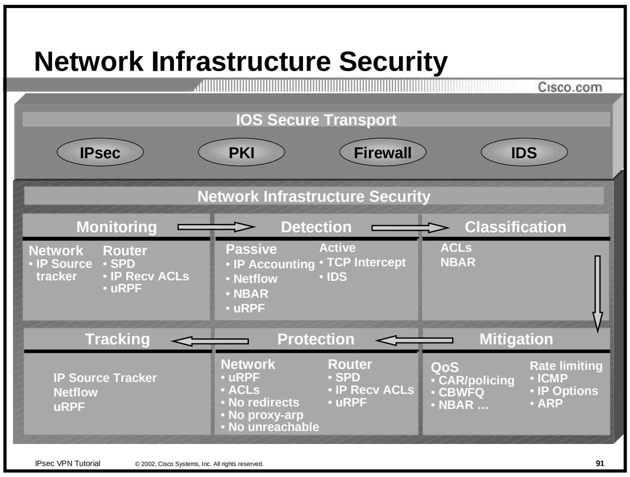
Cisco.com

- IPsec VPN deployment
  - - Cisco VPN Portfolio
  - - IOS and IPsec
  - - Deployment topologies
  - - Scalable Authentication with IOS PKI Enhancements
  - - IPsec and QoS, VoIP
- Wrap up and Q&A



Cisco.com

Cisco VPN Portfolio



Network Infrastructure Security

Cisco.com

IOS Secure Transport

IPsec | PKI | Firewall | IDS

Network Infrastructure Security

Monitoring → **Detection** → **Classification** → **Mitigation** → **Protection** → **Tracking**

Monitoring
- Network
  - IP Source tracker
- Router
  - SPD
  - IP Recv ACLs
  - uRPF

Detection
- Passive
  - IP Accounting
  - Netflow
  - NBAR
  - uRPF
- Active
  - TCP Intercept
  - IDS

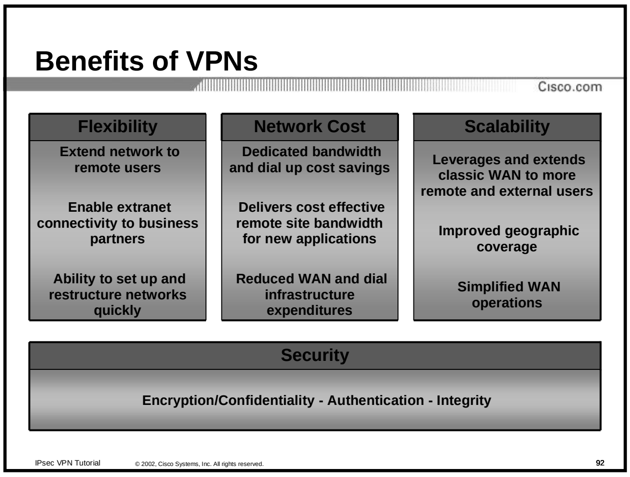
Classification
- ACLs
- NBAR

Mitigation
- QoS
  - CAR/policing
  - CBWFQ
  - NBAR ...
- Rate limiting
  - ICMP
  - IP Options
  - ARP

Protection
- Network
  - uRPF
  - ACLs
  - No redirects
  - No proxy-arp
  - No unreachable
- Router
  - SPD
  - IP Recv ACLs
  - uRPF

Tracking
- IP Source Tracker
- Netflow
- uRPF

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 91



Benefits of VPNs

Cisco.com

Flexibility
- Extend network to remote users
- Enable extranet connectivity to business partners
- Ability to set up and restructure networks quickly

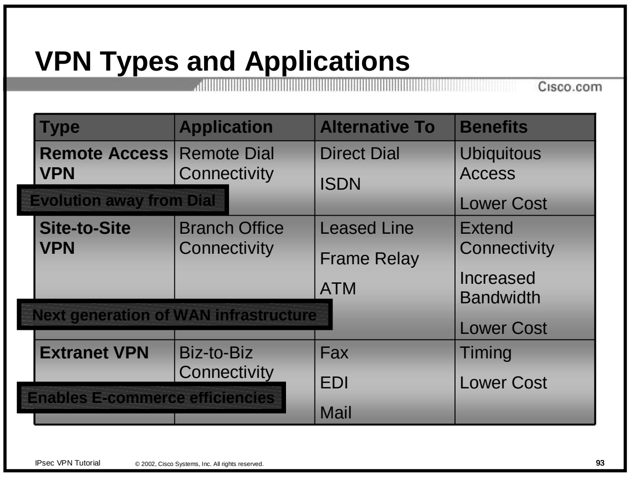
Network Cost
- Dedicated bandwidth and dial up cost savings
- Delivers cost effective remote site bandwidth for new applications
- Reduced WAN and dial infrastructure expenditures

Scalability
- Leverages and extends classic WAN to more remote and external users
- Improved geographic coverage
- Simplified WAN operations

Security

Encryption/Confidentiality - Authentication - Integrity

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 92



VPN Types and Applications

Cisco.com

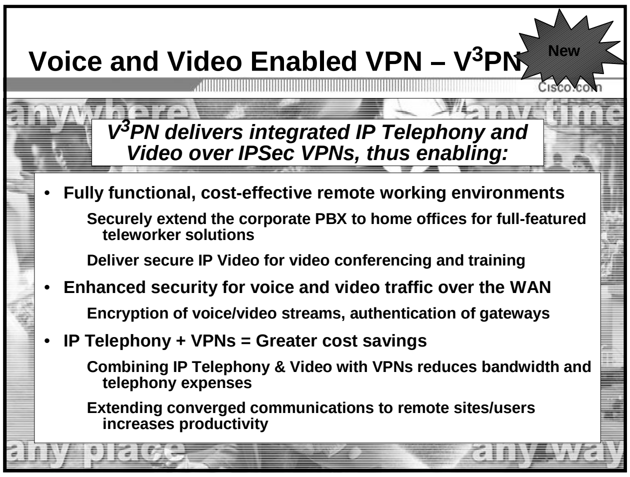
Type	Application	Alternative To	Benefits
Remote Access VPN	Remote Dial Connectivity	Direct Dial ISDN	Ubiquitous Access Lower Cost
Site-to-Site VPN	Branch Office Connectivity	Leased Line Frame Relay ATM	Extend Connectivity Increased Bandwidth Lower Cost
Extranet VPN	Biz-to-Biz Connectivity	Fax EDI Mail	Timing Lower Cost

Evolution away from Dial

Next generation of WAN infrastructure

Enables E-commerce efficiencies

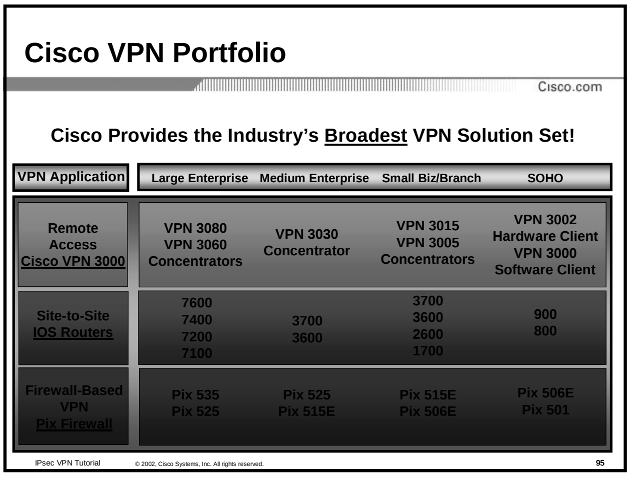
IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 93


New
Cisco.com
anywhere
any time
any place
any way

Voice and Video Enabled VPN – V^{3}PN

V^{3}PN delivers integrated IP Telephony and Video over IPSec VPNs, thus enabling:

- **Fully functional, cost-effective remote working environments**
  - **Securely extend the corporate PBX to home offices for full-featured teleworker solutions**
  - **Deliver secure IP Video for video conferencing and training**
- **Enhanced security for voice and video traffic over the WAN**
  - **Encryption of voice/video streams, authentication of gateways**
- **IP Telephony + VPNs = Greater cost savings**
  - **Combining IP Telephony & Video with VPNs reduces bandwidth and telephony expenses**
  - **Extending converged communications to remote sites/users increases productivity**

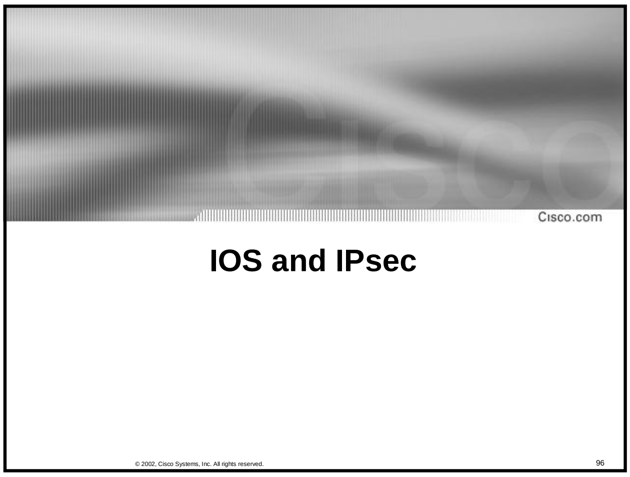


Cisco VPN Portfolio

Cisco Provides the Industry's Broadest VPN Solution Set!

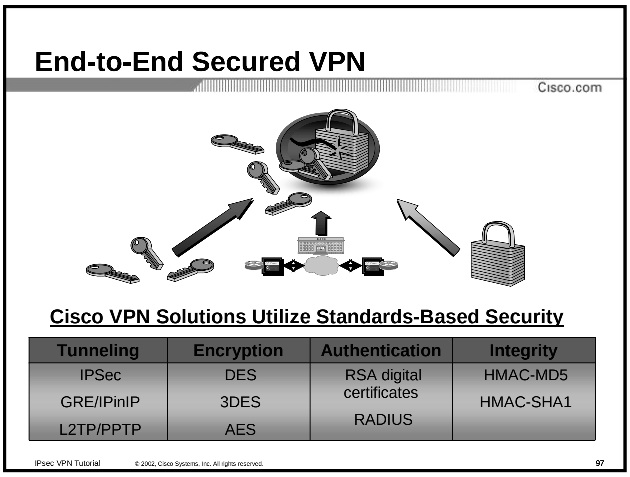
VPN Application	Large Enterprise	Medium Enterprise	Small Biz/Branch	SOHO
Remote Access Cisco VPN 3000	VPN 3080 VPN 3060 Concentrators	VPN 3030 Concentrator	VPN 3015 VPN 3005 Concentrators	VPN 3002 Hardware Client VPN 3000 Software Client
Site-to-Site IOS Routers	7600 7400 7200 7100	3700 3600	3700 3600 2600 1700	900 800
Firewall-Based VPN Pix Firewall	Pix 535 Pix 525	Pix 525 Pix 515E	Pix 515E Pix 506E	Pix 506E Pix 501

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 95


Cisco
Cisco.com

IOS and IPsec

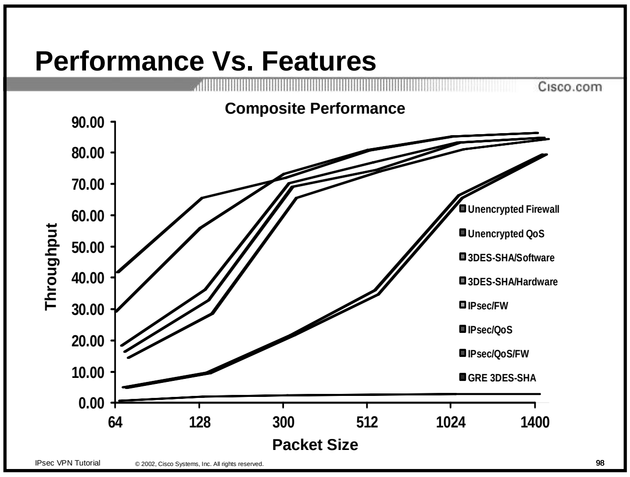
© 2002, Cisco Systems, Inc. All rights reserved. 96



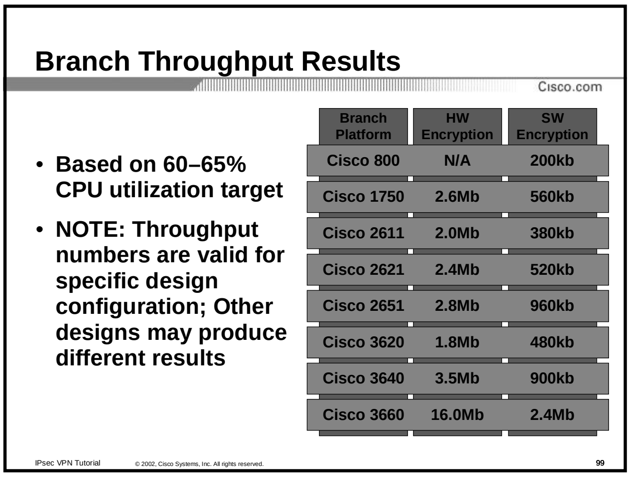
End-to-End Secured VPN

Cisco VPN Solutions Utilize Standards-Based Security

Tunneling	Encryption	Authentication	Integrity
IPSec GRE/IPinIP L2TP/PPTP	DES 3DES AES	RSA digital certificates RADIUS	HMAC-MD5 HMAC-SHA1



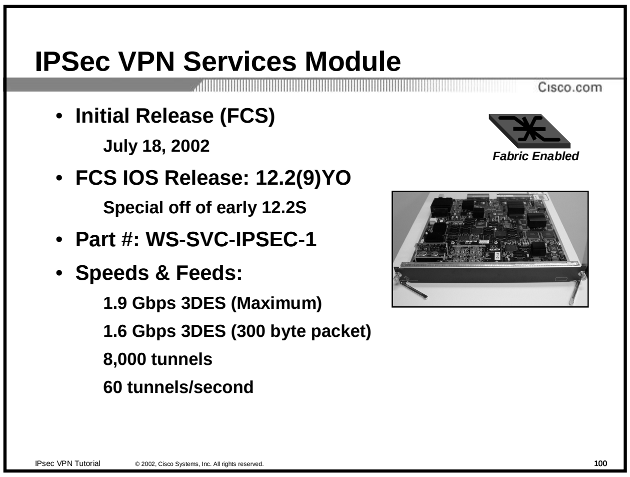
Performance Vs. Features



Branch Throughput Results

- Based on 60–65% CPU utilization target
- NOTE: Throughput numbers are valid for specific design configuration; Other designs may produce different results

Branch Platform	HW Encryption	SW Encryption
Cisco 800	N/A	200kb
Cisco 1750	2.6Mb	560kb
Cisco 2611	2.0Mb	380kb
Cisco 2621	2.4Mb	520kb
Cisco 2651	2.8Mb	960kb
Cisco 3620	1.8Mb	480kb
Cisco 3640	3.5Mb	900kb
Cisco 3660	16.0Mb	2.4Mb

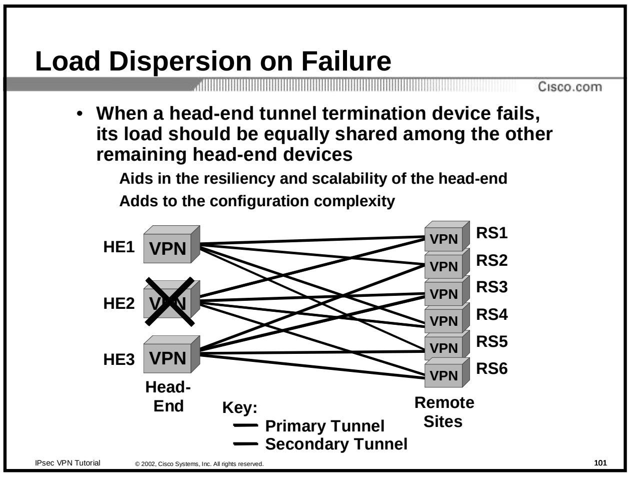


IPSec VPN Services Module

Cisco.com

- Initial Release (FCS)
  - July 18, 2002
- FCS IOS Release: 12.2(9)YO
  - Special off of early 12.2S
- Part #: WS-SVC-IPSEC-1
- Speeds & Feeds:
  - 1.9 Gbps 3DES (Maximum)
  - 1.6 Gbps 3DES (300 byte packet)
  - 8,000 tunnels
  - 60 tunnels/second

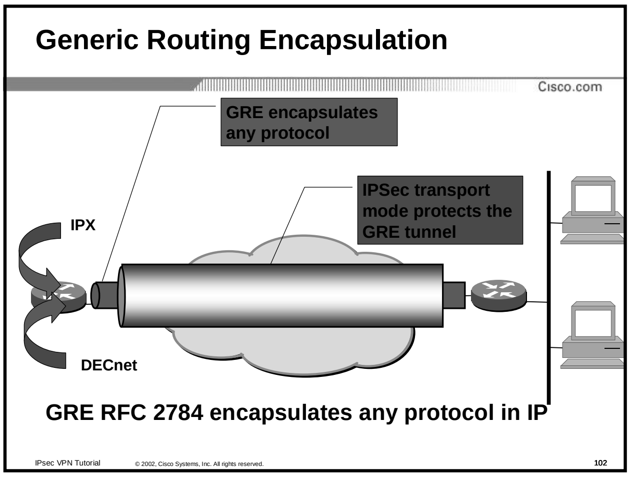
Fabric Enabled



Load Dispersion on Failure

Cisco.com

- When a head-end tunnel termination device fails, its load should be equally shared among the other remaining head-end devices
  - Aids in the resiliency and scalability of the head-end
  - Adds to the configuration complexity

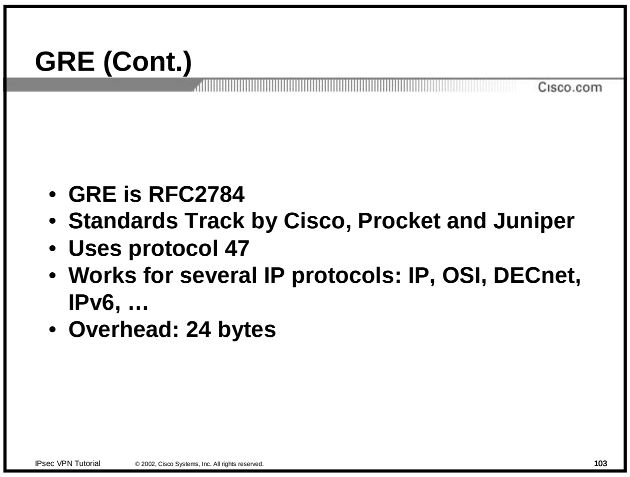


Generic Routing Encapsulation

Cisco.com

GRE encapsulates any protocol
IPSec transport mode protects the GRE tunnel
IPX
DECnet

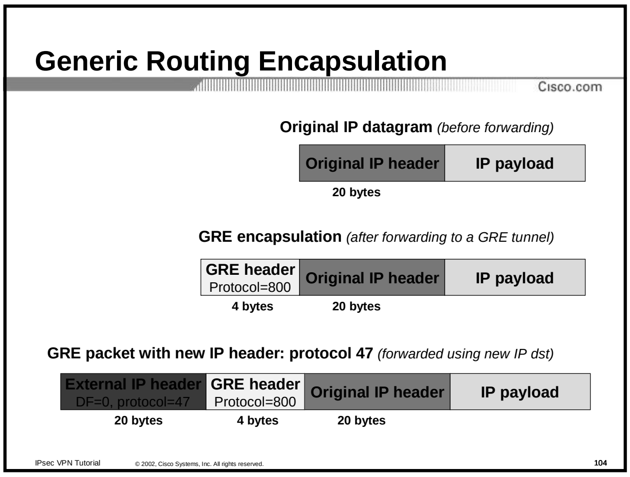
GRE RFC 2784 encapsulates any protocol in IP



GRE (Cont.)

- GRE is RFC2784
- Standards Track by Cisco, Procket and Juniper
- Uses protocol 47
- Works for several IP protocols: IP, OSI, DECnet, IPv6, …
- Overhead: 24 bytes

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 103



Generic Routing Encapsulation

Original IP datagram *(before forwarding)*

Original IP header	IP payload
20 bytes	

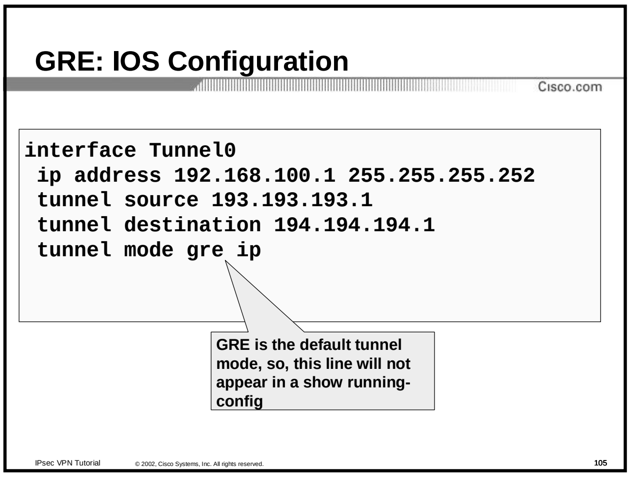
GRE encapsulation *(after forwarding to a GRE tunnel)*

GRE header Protocol=800	Original IP header	IP payload
4 bytes	20 bytes	

GRE packet with new IP header: protocol 47 *(forwarded using new IP dst)*

External IP header DF=0, protocol=47	GRE header Protocol=800	Original IP header	IP payload
20 bytes	4 bytes	20 bytes	

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 104

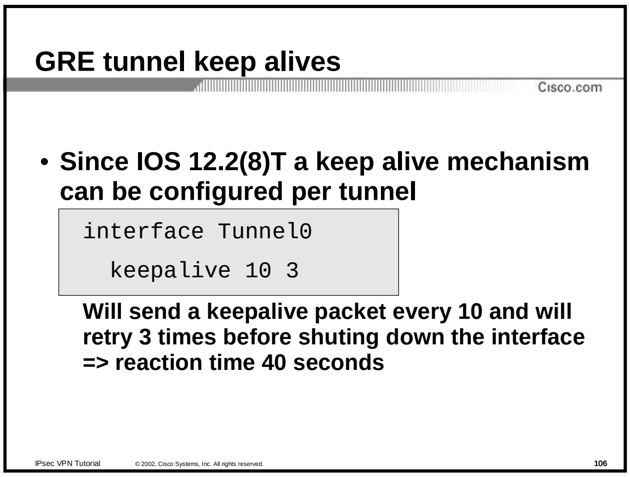


GRE: IOS Configuration

```
interface Tunnel0
 ip address 192.168.100.1 255.255.255.252
 tunnel source 193.193.193.1
 tunnel destination 194.194.194.1
 tunnel mode gre ip
```

GRE is the default tunnel mode, so, this line will not appear in a show running-config

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 105



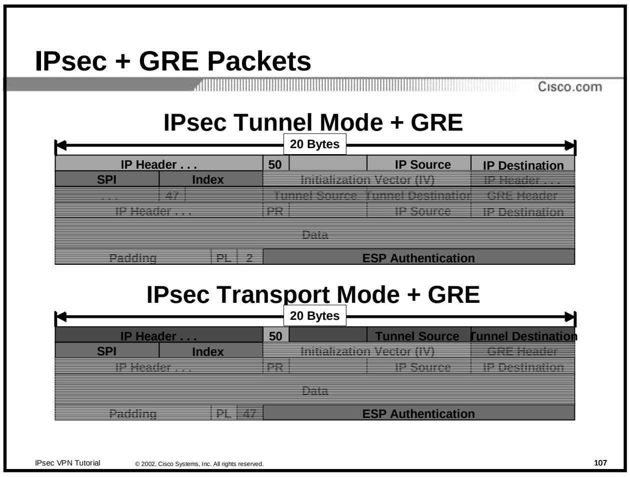
GRE tunnel keep alives

Cisco.com

- **Since IOS 12.2(8)T a keep alive mechanism can be configured per tunnel**

```
interface Tunnel0
  keepalive 10 3
```

Will send a keepalive packet every 10 and will retry 3 times before shuting down the interface => reaction time 40 seconds



IPsec + GRE Packets

Cisco.com

IPsec Tunnel Mode + GRE

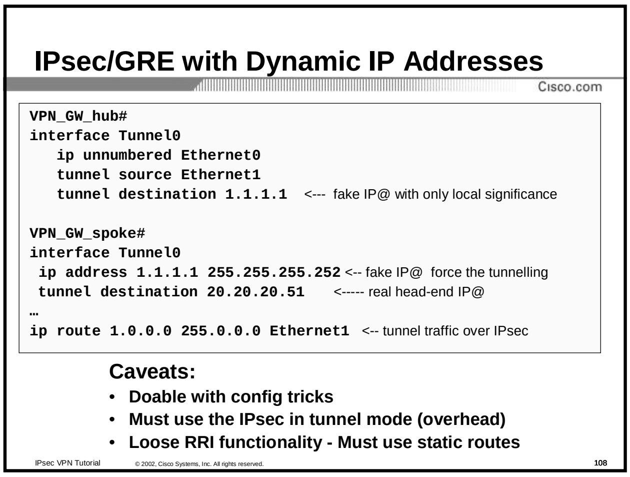
20 Bytes

IP Header . . . | 50 | | IP Source | IP Destination
SPI | Index | Initialization Vector (IV) | IP Header . . .
. . . | 47 | | Tunnel Source | Tunnel Destination | GRE Header
IP Header . . . | PR | | IP Source | IP Destination
Data
Padding | PL | 2 | ESP Authentication

IPsec Transport Mode + GRE

20 Bytes

IP Header . . . | 50 | | Tunnel Source | Tunnel Destination
SPI | Index | Initialization Vector (IV) | GRE Header
IP Header . . . | PR | | IP Source | IP Destination
Data
Padding | PL | 47 | ESP Authentication



IPsec/GRE with Dynamic IP Addresses

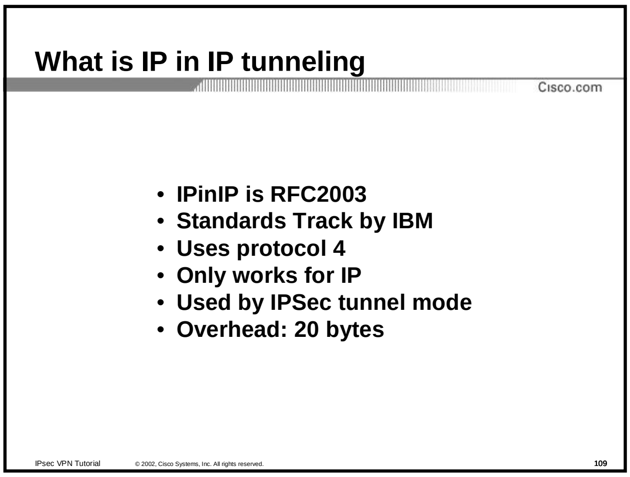
Cisco.com

```
VPN_GW_hub#
interface Tunnel0
   ip unnumbered Ethernet0
   tunnel source Ethernet1
   tunnel destination 1.1.1.1  <---  fake IP@ with only local significance

VPN_GW_spoke#
interface Tunnel0
 ip address 1.1.1.1 255.255.255.252 <-- fake IP@  force the tunnelling
 tunnel destination 20.20.20.51    <----- real head-end IP@
…
ip route 1.0.0.0 255.0.0.0 Ethernet1  <-- tunnel traffic over IPsec
```

Caveats:

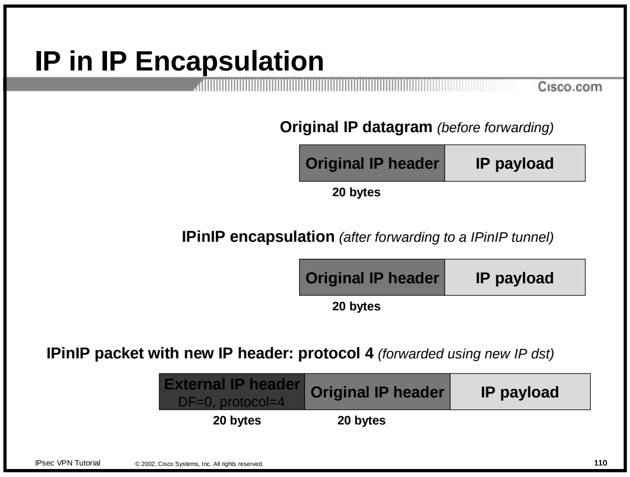
- **Doable with config tricks**
- **Must use the IPsec in tunnel mode (overhead)**
- **Loose RRI functionality - Must use static routes**



What is IP in IP tunneling

Cisco.com

- IPinIP is RFC2003
- Standards Track by IBM
- Uses protocol 4
- Only works for IP
- Used by IPSec tunnel mode
- Overhead: 20 bytes



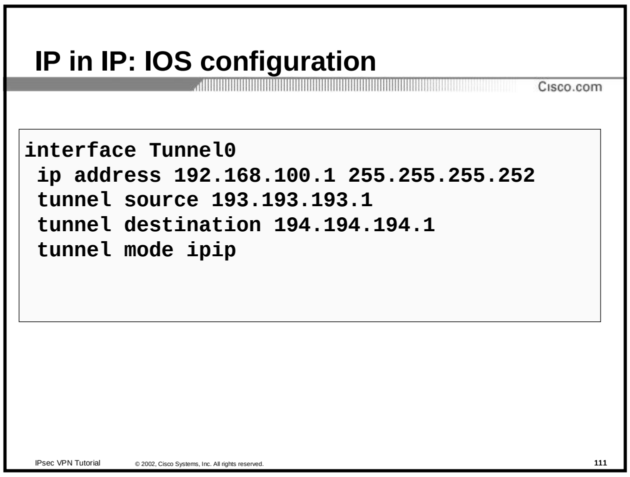
IP in IP Encapsulation

Cisco.com

Original IP datagram *(before forwarding)*

IPinIP encapsulation *(after forwarding to a IPinIP tunnel)*

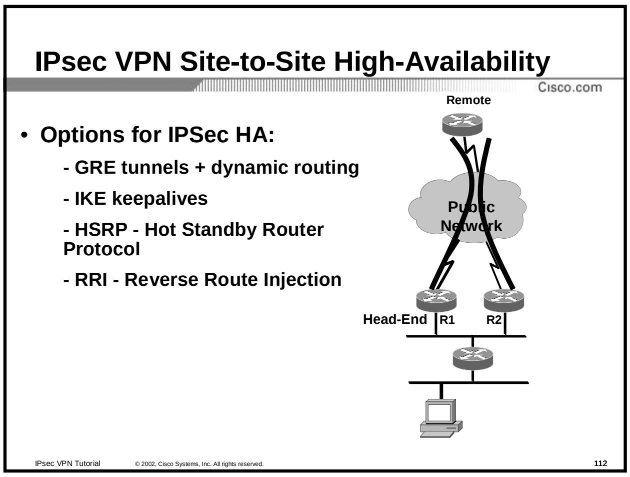
IPinIP packet with new IP header: protocol 4 *(forwarded using new IP dst)*



IP in IP: IOS configuration

Cisco.com

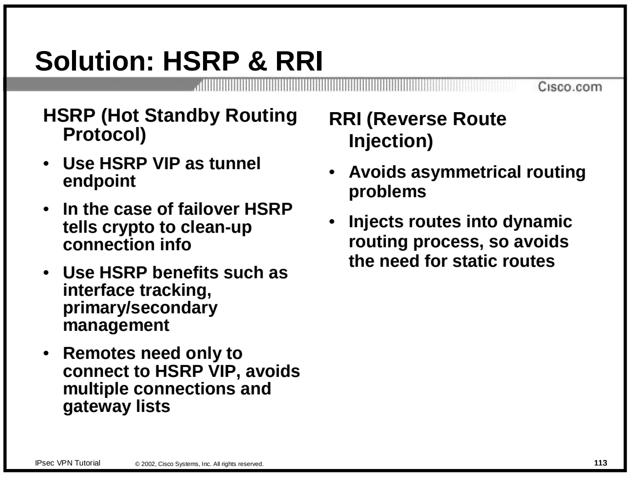
```
interface Tunnel0
 ip address 192.168.100.1 255.255.255.252
 tunnel source 193.193.193.1
 tunnel destination 194.194.194.1
 tunnel mode ipip
```



IPsec VPN Site-to-Site High-Availability

- **Options for IPSec HA:**
  - - GRE tunnels + dynamic routing
  - - IKE keepalives
  - - HSRP - Hot Standby Router Protocol
  - - RRI - Reverse Route Injection

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 112



Solution: HSRP & RRI

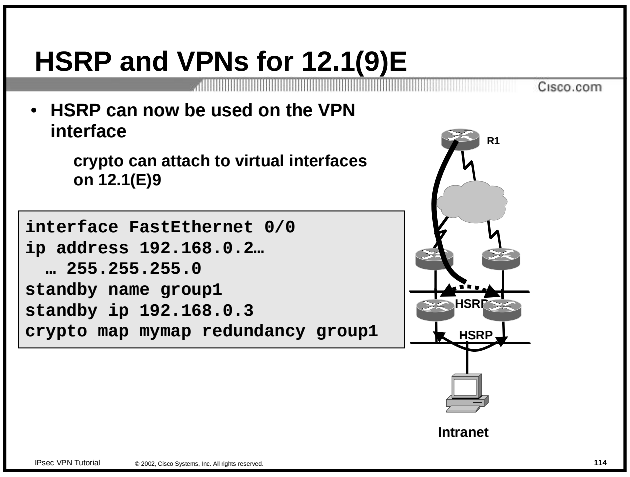
HSRP (Hot Standby Routing Protocol)

- Use HSRP VIP as tunnel endpoint
- In the case of failover HSRP tells crypto to clean-up connection info
- Use HSRP benefits such as interface tracking, primary/secondary management
- Remotes need only to connect to HSRP VIP, avoids multiple connections and gateway lists

RRI (Reverse Route Injection)

- Avoids asymmetrical routing problems
- Injects routes into dynamic routing process, so avoids the need for static routes

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 113



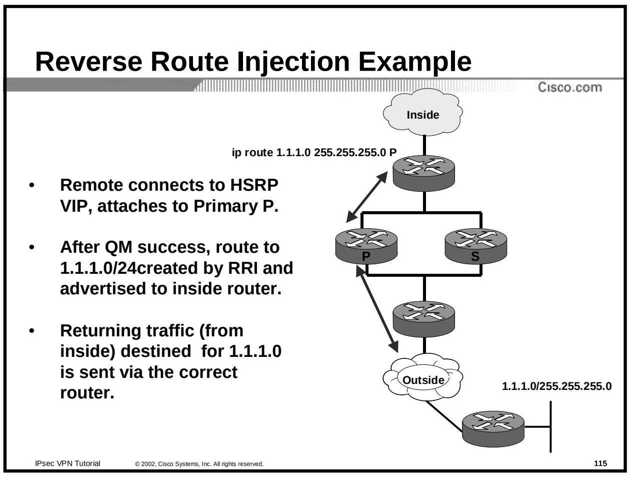
HSRP and VPNs for 12.1(9)E

- HSRP can now be used on the VPN interface

  crypto can attach to virtual interfaces on 12.1(E)9

```
interface FastEthernet 0/0
ip address 192.168.0.2…
  … 255.255.255.0
standby name group1
standby ip 192.168.0.3
crypto map mymap redundancy group1
```

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 114

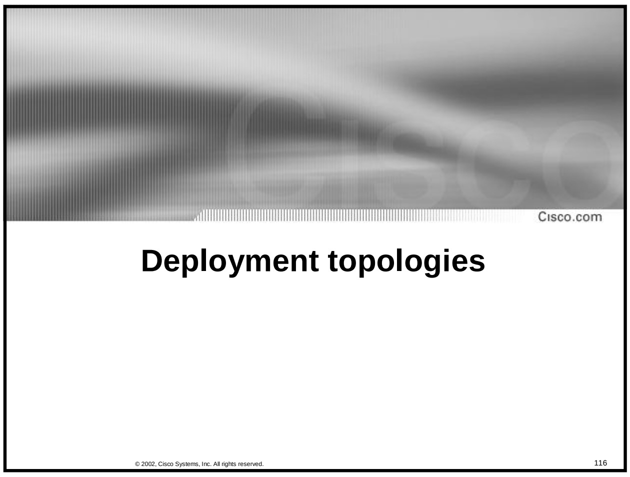


Reverse Route Injection Example

Cisco.com

- Remote connects to HSRP VIP, attaches to Primary P.
- After QM success, route to 1.1.1.0/24created by RRI and advertised to inside router.
- Returning traffic (from inside) destined for 1.1.1.0 is sent via the correct router.

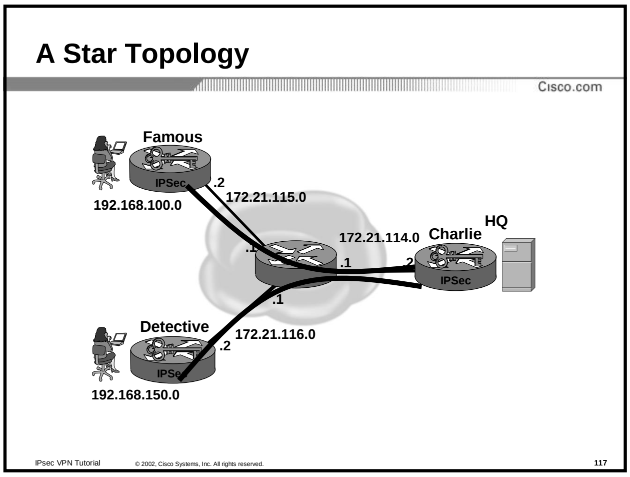
IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 115



Cisco.com

Deployment topologies

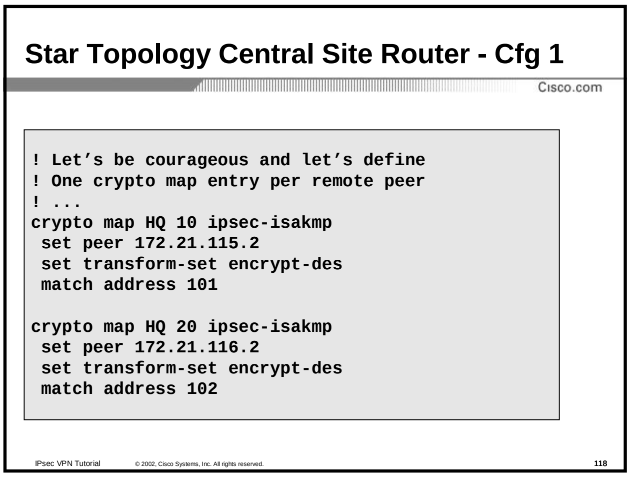
© 2002, Cisco Systems, Inc. All rights reserved. 116



A Star Topology

Cisco.com

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 117



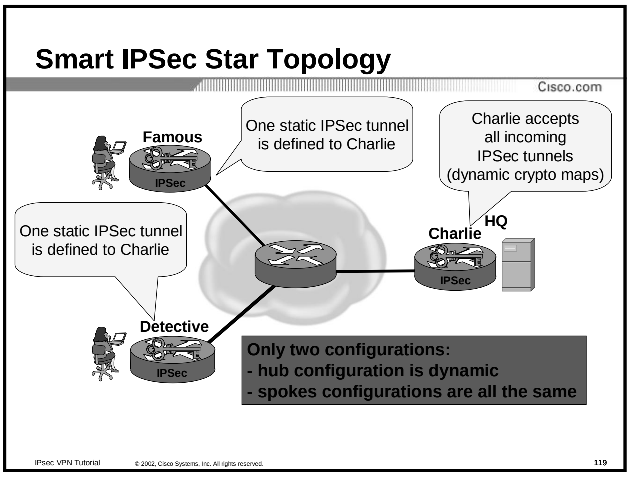
Star Topology Central Site Router - Cfg 1

Cisco.com

```
! Let’s be courageous and let’s define
! One crypto map entry per remote peer
! ...
crypto map HQ 10 ipsec-isakmp
 set peer 172.21.115.2
 set transform-set encrypt-des
 match address 101

crypto map HQ 20 ipsec-isakmp
 set peer 172.21.116.2
 set transform-set encrypt-des
 match address 102
```

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 118



Smart IPSec Star Topology

Cisco.com

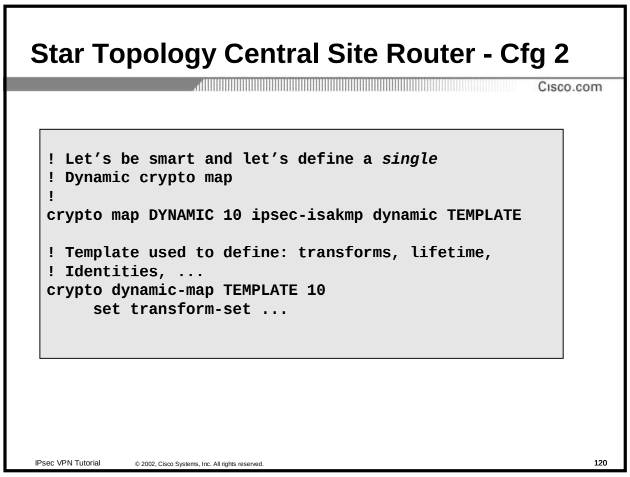
One static IPSec tunnel is defined to Charlie

Charlie accepts all incoming IPSec tunnels (dynamic crypto maps)

One static IPSec tunnel is defined to Charlie

Only two configurations:
- hub configuration is dynamic
- spokes configurations are all the same

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 119



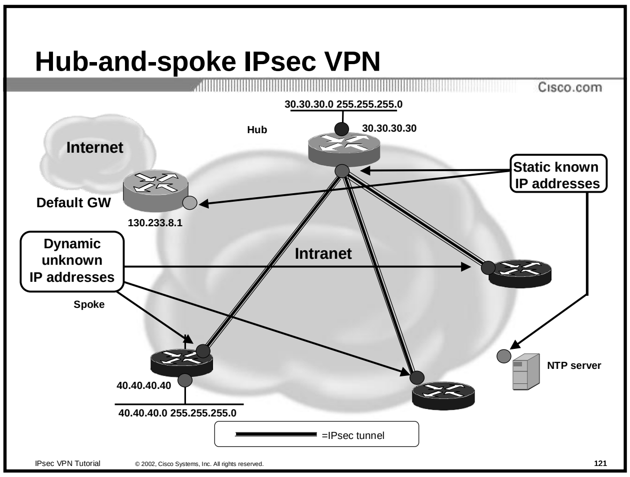
Star Topology Central Site Router - Cfg 2

Cisco.com

```
! Let’s be smart and let’s define a single
! Dynamic crypto map
!
crypto map DYNAMIC 10 ipsec-isakmp dynamic TEMPLATE

! Template used to define: transforms, lifetime,
! Identities, ...
crypto dynamic-map TEMPLATE 10
     set transform-set ...
```

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 120



Hub-and-spoke IPsec VPN

Cisco.com

30.30.30.0 255.255.255.0

Hub

30.30.30.30

Internet

Static known IP addresses

Default GW

130.233.8.1

Dynamic unknown IP addresses

Intranet

Spoke

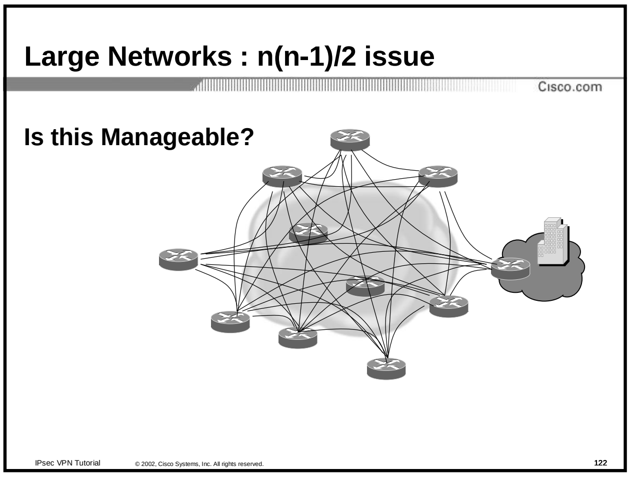
NTP server

40.40.40.40

40.40.40.0 255.255.255.0

=IPsec tunnel

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 121

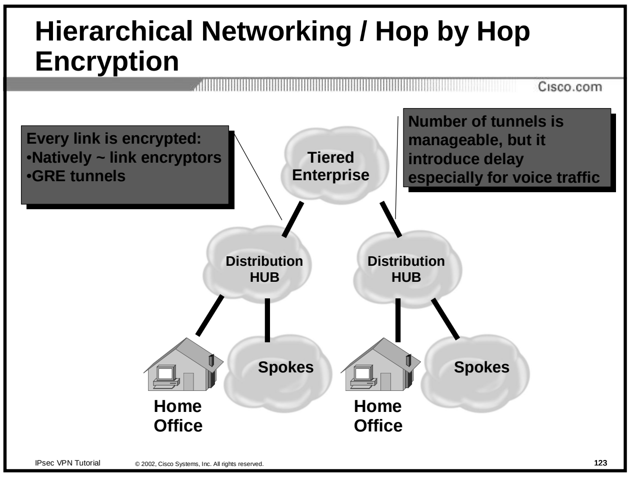


Large Networks : n(n-1)/2 issue

Cisco.com

Is this Manageable?

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 122



Hierarchical Networking / Hop by Hop Encryption

Cisco.com

Every link is encrypted:
- Natively ~ link encryptors
- GRE tunnels

Tiered Enterprise

Number of tunnels is manageable, but it introduce delay especially for voice traffic

Distribution HUB

Distribution HUB

Home Office

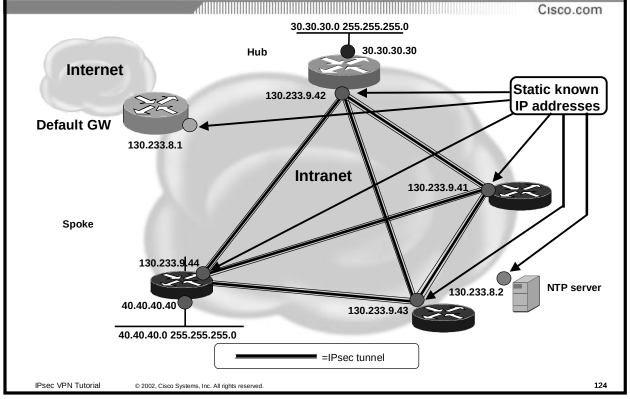
Spokes

Home Office

Spokes

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 123

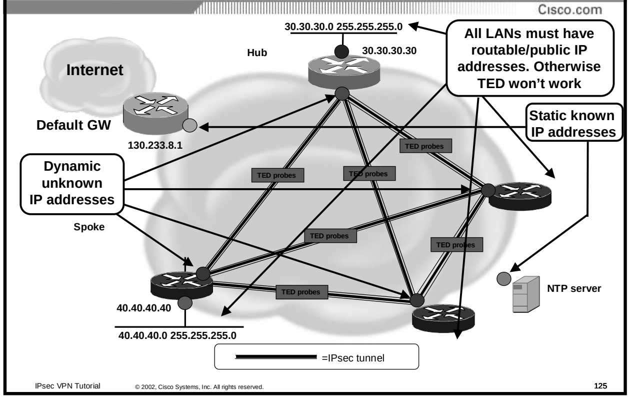
Site-to-Site (Full Mesh) IPsec VPN



Static known IP addresses

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 124

Full Mesh with TED IPsec VPN



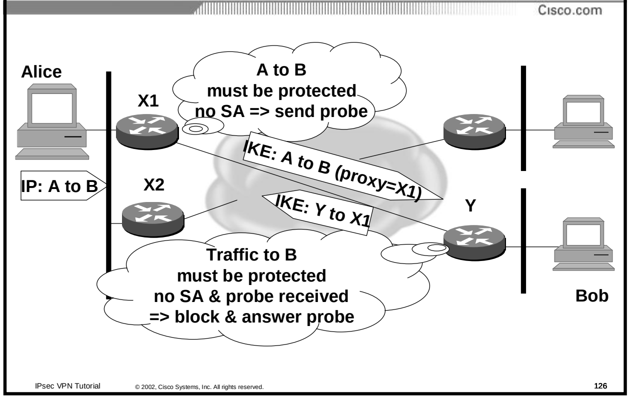
All LANs must have routable/public IP addresses. Otherwise TED won't work

Static known IP addresses

Dynamic unknown IP addresses

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 125

Fully Meshed - Tunnel Endpoint Discovery



A to B must be protected no SA => send probe

Traffic to B must be protected no SA & probe received => block & answer probe

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 126

Caveats of TED

- **Addressing**

  As the probe uses the protected entities address (A, B)

  these address MUST be routable

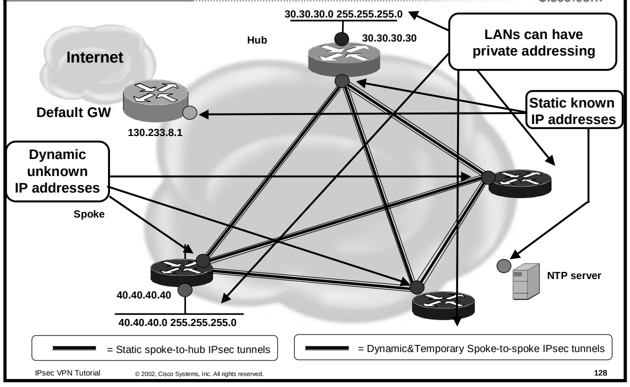
  TED is thus not applicable for VPN over Internet

- **Deployment**

  All IPSec routers must have TED enabled

  deployment on ALL routers SIMULTANEOUSLY...

Dynamic Multipoint VPN (MGRE - Q4CY02)



LANs can have private addressing

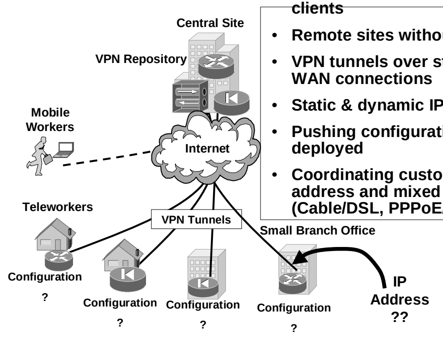
Static known IP addresses

Dynamic unknown IP addresses

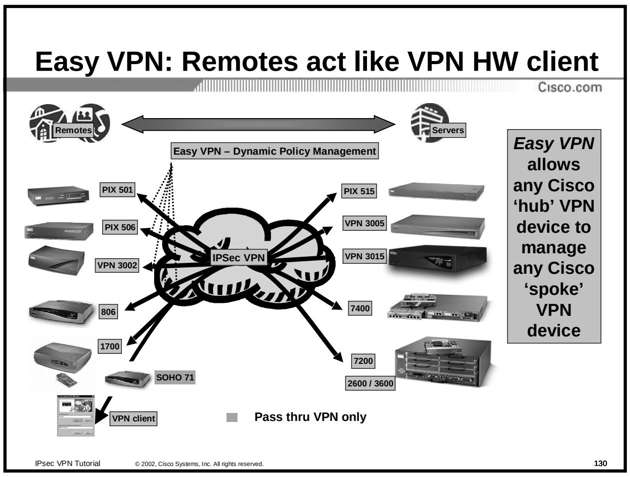
= Static spoke-to-hub IPsec tunnels

= Dynamic&Temporary Spoke-to-spoke IPsec tunnels

VPN Deployment & Management Challenges



- Heterogeneous CPE devices and clients
- Remote sites without on-site support
- VPN tunnels over static and dynamic WAN connections
- Static & dynamic IP addresses
- Pushing configuration changes once deployed
- Coordinating custom configuration, IP address and mixed WAN environment (Cable/DSL, PPPoE/hostname)

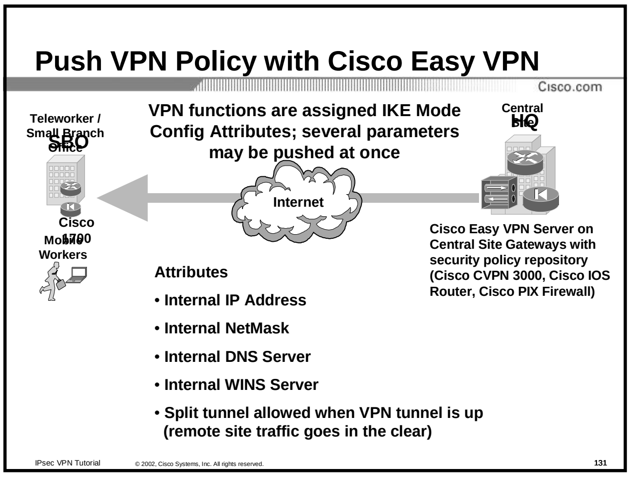


Easy VPN: Remotes act like VPN HW client

Easy VPN allows any Cisco ‘hub’ VPN device to manage any Cisco ‘spoke’ VPN device

▨ Pass thru VPN only

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 130



Push VPN Policy with Cisco Easy VPN

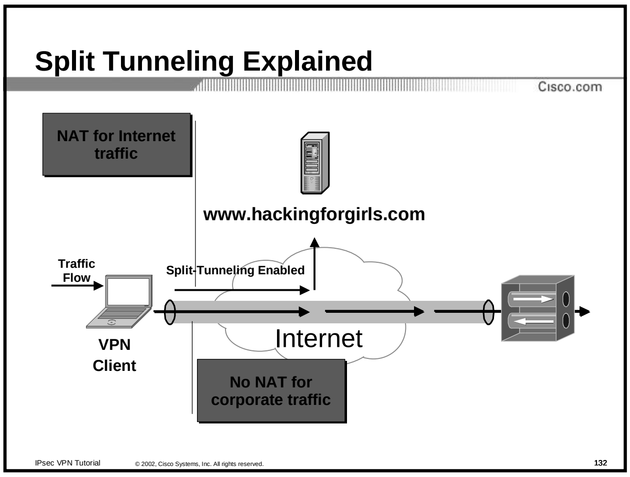
VPN functions are assigned IKE Mode Config Attributes; several parameters may be pushed at once

Cisco Easy VPN Server on Central Site Gateways with security policy repository (Cisco CVPN 3000, Cisco IOS Router, Cisco PIX Firewall)

Attributes

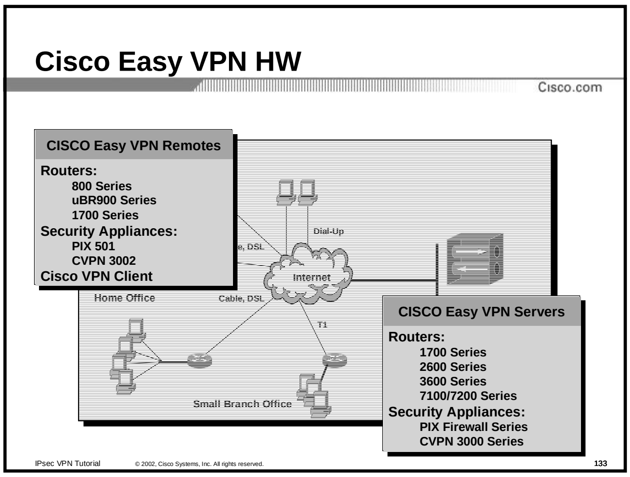
- Internal IP Address
- Internal NetMask
- Internal DNS Server
- Internal WINS Server
- Split tunnel allowed when VPN tunnel is up (remote site traffic goes in the clear)

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 131



Split Tunneling Explained

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 132



Cisco Easy VPN HW

CISCO Easy VPN Remotes

Routers:
- 800 Series
- uBR900 Series
- 1700 Series

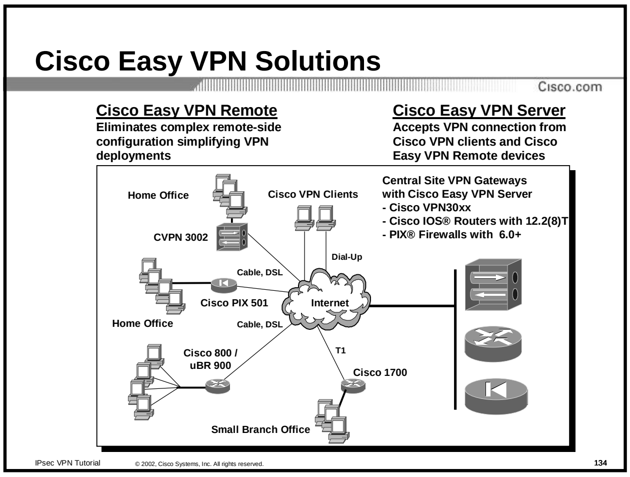
Security Appliances:
- PIX 501
- CVPN 3002

Cisco VPN Client

CISCO Easy VPN Servers

Routers:
- 1700 Series
- 2600 Series
- 3600 Series
- 7100/7200 Series

Security Appliances:
- PIX Firewall Series
- CVPN 3000 Series

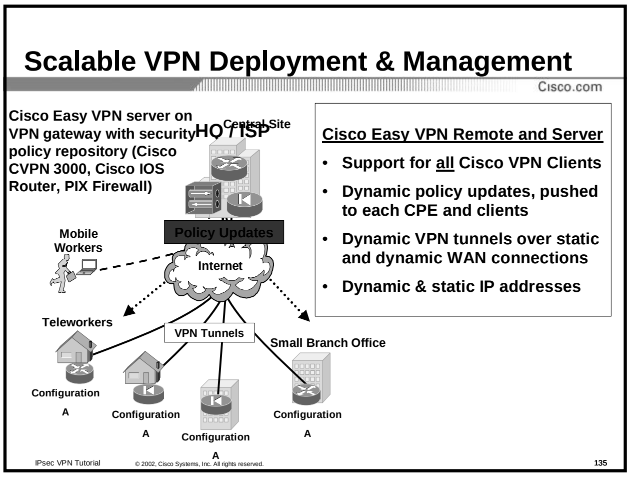


Cisco Easy VPN Solutions

Cisco Easy VPN Remote
Eliminates complex remote-side configuration simplifying VPN deployments

Cisco Easy VPN Server
Accepts VPN connection from Cisco VPN clients and Cisco Easy VPN Remote devices

Central Site VPN Gateways with Cisco Easy VPN Server
- Cisco VPN30xx
- Cisco IOS® Routers with 12.2(8)T
- PIX® Firewalls with 6.0+

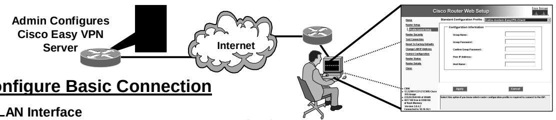


Scalable VPN Deployment & Management

Cisco Easy VPN server on VPN gateway with security policy repository (Cisco CVPN 3000, Cisco IOS Router, PIX Firewall)

Cisco Easy VPN Remote and Server
- Support for all Cisco VPN Clients
- Dynamic policy updates, pushed to each CPE and clients
- Dynamic VPN tunnels over static and dynamic WAN connections
- Dynamic & static IP addresses

Cisco Easy VPN Remote - Initiation


Admin Configures Cisco Easy VPN Server
Internet
Optional user initiation of Cisco Easy VPN Connection

1. Configure Basic Connection
   - LAN Interface
   - WAN Interface
   - DNS Address
   - DHCP Address
   - NAT / PAT Configuration (optional)
2. Configure Cisco Easy VPN Specifics
   - Mode (client or network ext.)
   - Peer address
   - VPN tunnel interface
   - Group name and password
   - User name and password

Initiate Dynamic VPN

100% pre-configured and automated initiation

Optional: admin final set up
with CLI, Telnet or console port

Optional: user final set up
(Cisco 800 & uBR900, CVPN 3002 and Cisco PIX 501 FW only)

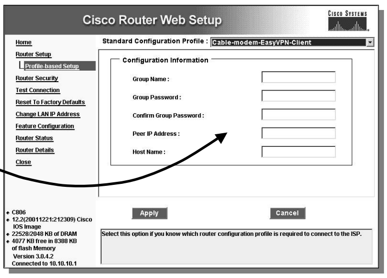
- Group Name, Group Password, Peer IP Address, Host Name

•Optional: dynamic/ongoing device authentication

Easy VPN Example - Cisco 800 Series

Setting up Cisco Easy VPN Remote

- Non-technical users can enable Easy VPN with simple login information provided by IT
- No pre-configuration required, standard router configuration can be used



Standard Configuration Profile : Cable-modem-EasyVPN-Client

Configuration Information

Group Name :

Group Password :

Confirm Group Password :

Peer IP Address :

Host Name :

- C806
- 12.2(20011221:212309) Cisco IOS Image
- 22528/2048 KB of DRAM
- 4077 KB free in 8388 KB of flash Memory

Version 3.0.4.2
Connected to 10.10.10.1

Select this option if you know which router configuration profile is required to connect to the ISP.

Cisco Easy VPN Remote GUI support on Cisco 800, 900, Cisco PIX Firewalls, and CVPN 3002

Where to use what

	IPsec	IPsec/GRE
Dynamic addresses	Yes	Q4CY02*
Full mesh	Yes (TED)	Partial mesh
Easy VPN	Yes	No
HSRP/RRI	Yes	IPsec only
	IP only	Multiprotocol, multicast

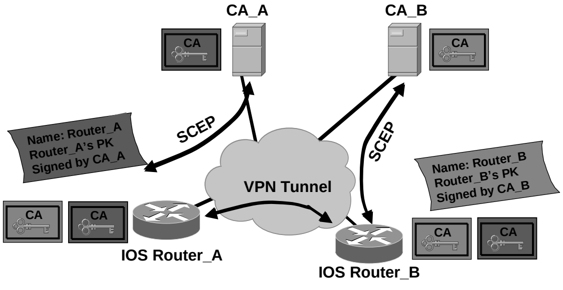
Scalable Authentication
with
IOS PKI Enhancements

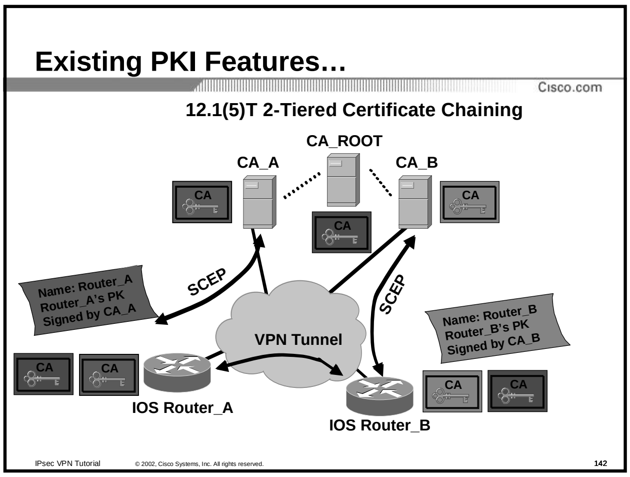
PKI Features in Cisco IOS 12.2T

- 12.1(5)T 2-Tiered Certificate Chaining
- 12.2(2)T Multiple Certificates per Router (one key pair)
- 12.2(4)T Distinguished Name (DN) Based Crypto Maps
- 12.2(8)T Separate Key-Pair per Identity
- 12.2(8)T Certificate Auto-Enrollment
- 12.2(8)T Multi-Certs per Router (multiple key pair)

Existing PKI Features…

12.1(4)/12.1(1)T Multi Root Support



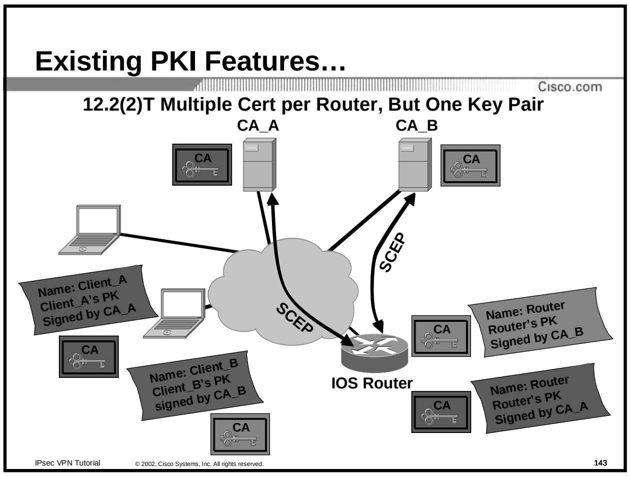


Existing PKI Features…

Cisco.com

12.1(5)T 2-Tiered Certificate Chaining

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 142

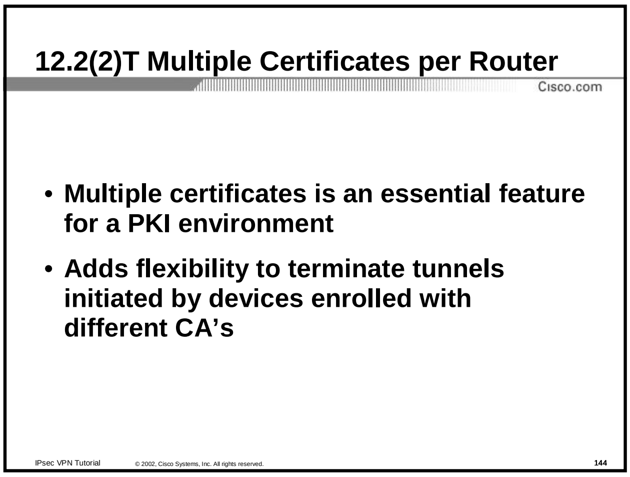


Existing PKI Features…

Cisco.com

12.2(2)T Multiple Cert per Router, But One Key Pair

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 143

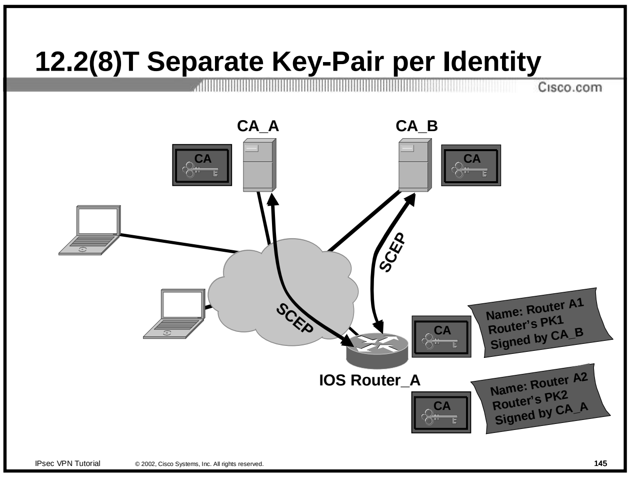


12.2(2)T Multiple Certificates per Router

Cisco.com

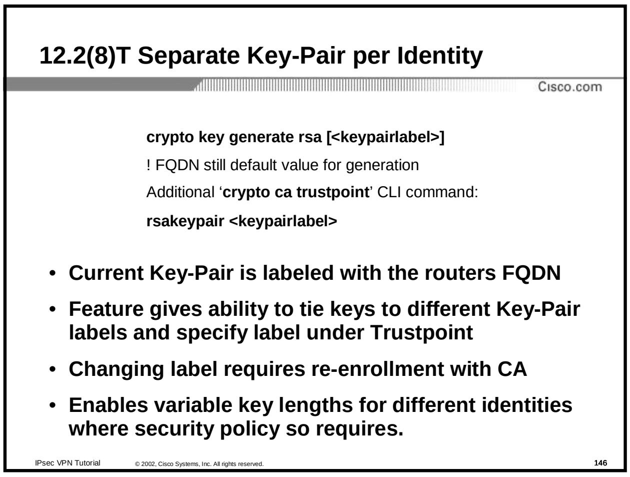
- **Multiple certificates is an essential feature for a PKI environment**
- **Adds flexibility to terminate tunnels initiated by devices enrolled with different CA's**

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 144



12.2(8)T Separate Key-Pair per Identity

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 145

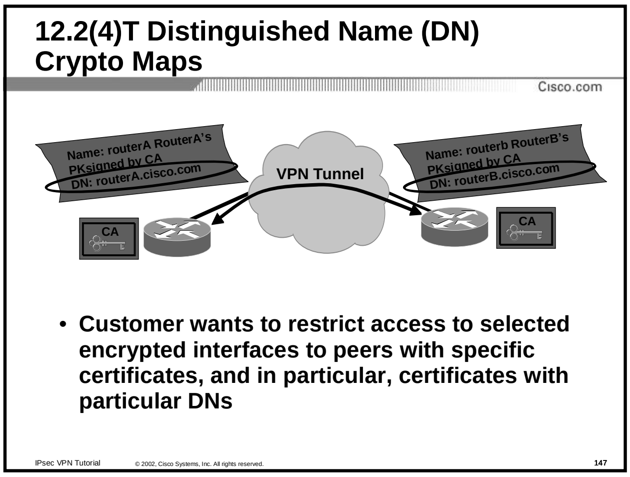


12.2(8)T Separate Key-Pair per Identity

```
crypto key generate rsa [<keypairlabel>]
! FQDN still default value for generation
Additional 'crypto ca trustpoint' CLI command:
rsakeypair <keypairlabel>
```

- **Current Key-Pair is labeled with the routers FQDN**
- **Feature gives ability to tie keys to different Key-Pair labels and specify label under Trustpoint**
- **Changing label requires re-enrollment with CA**
- **Enables variable key lengths for different identities where security policy so requires.**

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 146

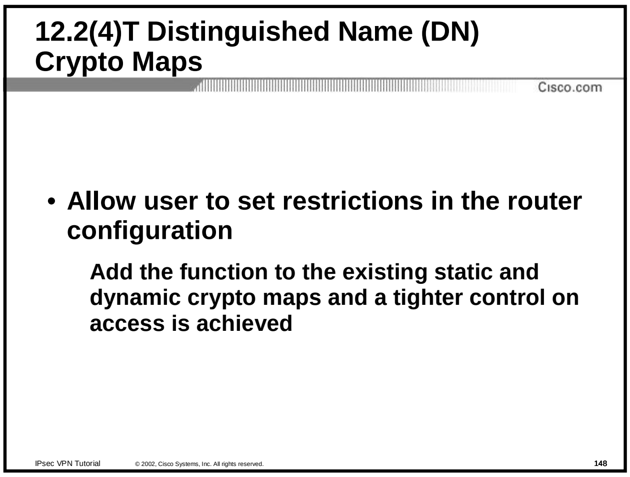


12.2(4)T Distinguished Name (DN) Crypto Maps

Cisco.com
Name: routerA RouterA's PKsigned by CA
DN: routerA.cisco.com
VPN Tunnel
Name: routerb RouterB's PKsigned by CA
DN: routerB.cisco.com
CA
CA

- **Customer wants to restrict access to selected encrypted interfaces to peers with specific certificates, and in particular, certificates with particular DNs**

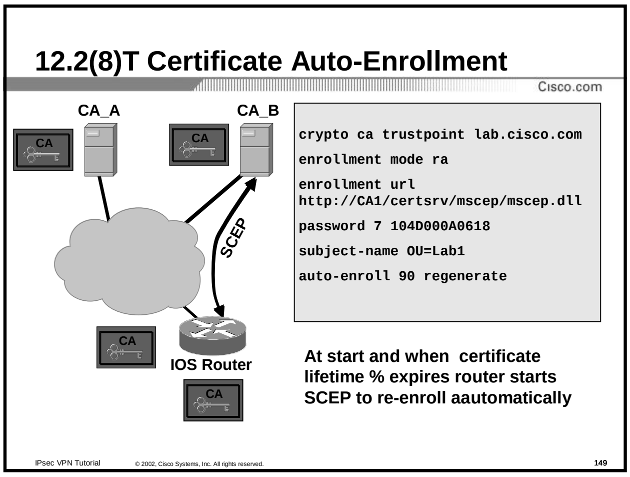
IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 147



12.2(4)T Distinguished Name (DN) Crypto Maps

- **Allow user to set restrictions in the router configuration**

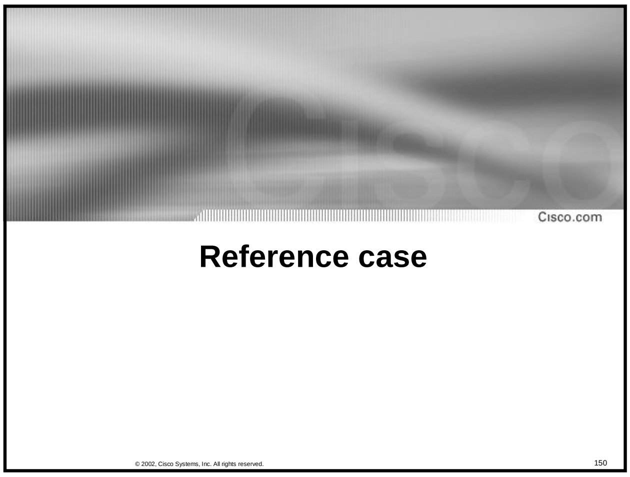
  Add the function to the existing static and dynamic crypto maps and a tighter control on access is achieved



12.2(8)T Certificate Auto-Enrollment

```
crypto ca trustpoint lab.cisco.com
enrollment mode ra
enrollment url
http://CA1/certsrv/mscep/mscep.dll
password 7 104D000A0618
subject-name OU=Lab1
auto-enroll 90 regenerate
```

At start and when certificate lifetime % expires router starts SCEP to re-enroll aautomatically



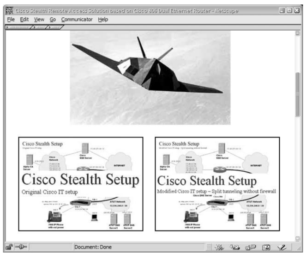
Reference case

Cisco Internal VPN Deployment Pilot

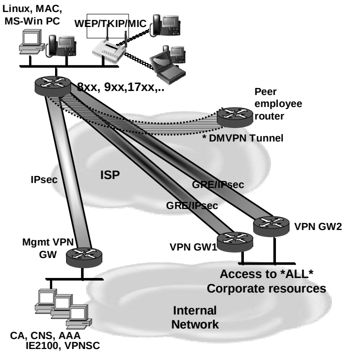
Cisco Internal Deployment of:

- IKE/IPsec with PKI
- IOS Firewall
- GRE for static and dynamic IP@
- NAT Overload [PAT]
- QoS-MQC based CBFWQ and PQ
- Split tunneling
- Multicast [IP/TV]
- MGRE + NHRP
- Nat traversal
- Pre-provisioning
- …

~ 350 sites in USA and EMA


Cisco Stealth Remote Access Solution based on Cisco 806 Dual Ethernet Router - Netscape
File Edit View Go Communicator Help
Cisco Stealth Setup
Original Cisco IT setup
Cisco Stealth Setup
Modified Cisco IT setup – Split tunneling without firewall
Document: Done

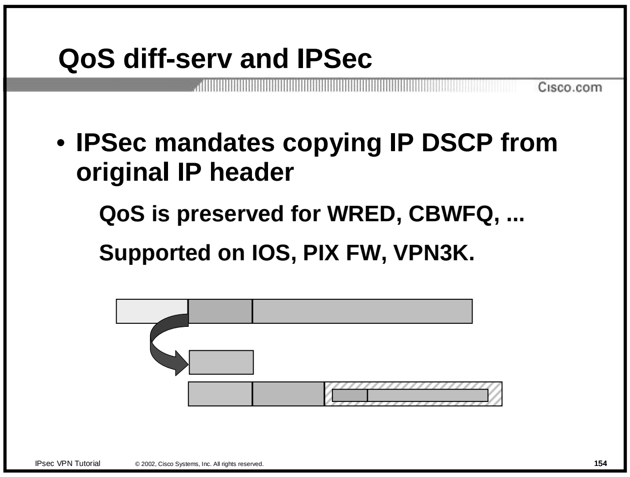
Cisco Telecommuter Office Pilot Test Bed



- **VPN Client – "Dial" VPN**
- **IOS FW – Security**
- **IPsec tunnel - Always on VPN**
- **GRE/IPsec tunnel - IP/TV**
- **2nd GW tunnel - Uptime**
- **Mgmt tunnel - Provisioning**
- **MGRE/IPsec - DM VPN***
- **Wireless WEP/TKIP/MIC**
- **VoIP**
- **...**

*** DM VPN = Dynamic Multipoint VPN**

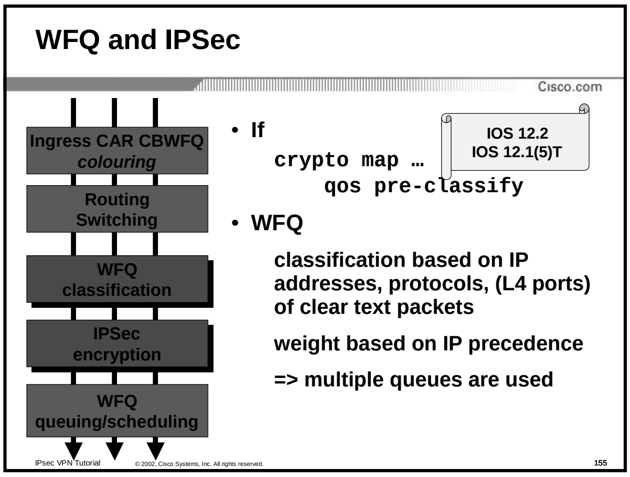
IPsec and QoS



QoS diff-serv and IPSec

Cisco.com

- IPSec mandates copying IP DSCP from original IP header
  - QoS is preserved for WRED, CBWFQ, ...
  - Supported on IOS, PIX FW, VPN3K.



WFQ and IPSec

Cisco.com

Ingress CAR CBWFQ *colouring*

Routing Switching

WFQ classification

IPSec encryption

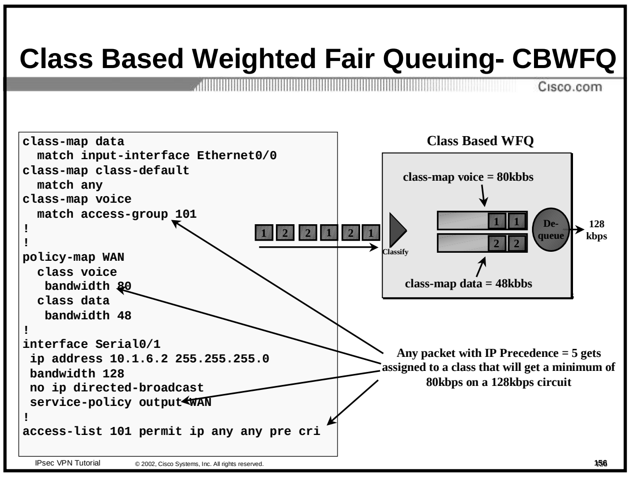
WFQ queuing/scheduling

- If

```
crypto map …
    qos pre-classify
```

IOS 12.2
IOS 12.1(5)T

- WFQ
  - classification based on IP addresses, protocols, (L4 ports) of clear text packets
  - weight based on IP precedence
  - => multiple queues are used

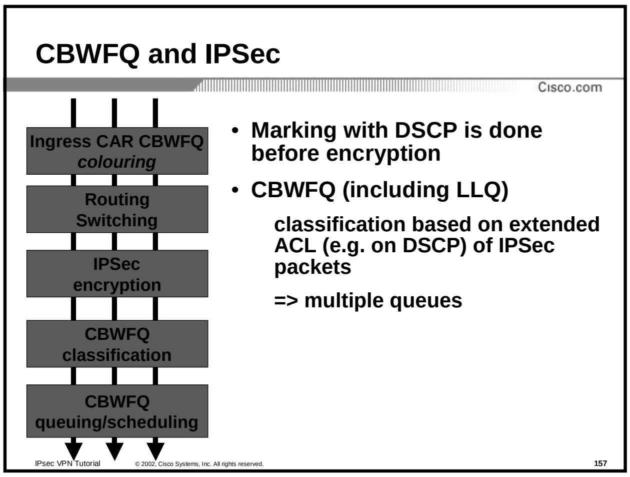


Class Based Weighted Fair Queuing- CBWFQ

Cisco.com

```
class-map data
  match input-interface Ethernet0/0
class-map class-default
  match any
class-map voice
  match access-group 101
!
!
policy-map WAN
  class voice
   bandwidth 80
  class data
   bandwidth 48
!
interface Serial0/1
 ip address 10.1.6.2 255.255.255.0
 bandwidth 128
 no ip directed-broadcast
 service-policy output WAN
!
access-list 101 permit ip any any pre cri
```

Any packet with IP Precedence = 5 gets assigned to a class that will get a minimum of 80kbps on a 128kbps circuit



CBWFQ and IPSec

Cisco.com

Ingress CAR CBWFQ *colouring*

Routing Switching

IPSec encryption

CBWFQ classification

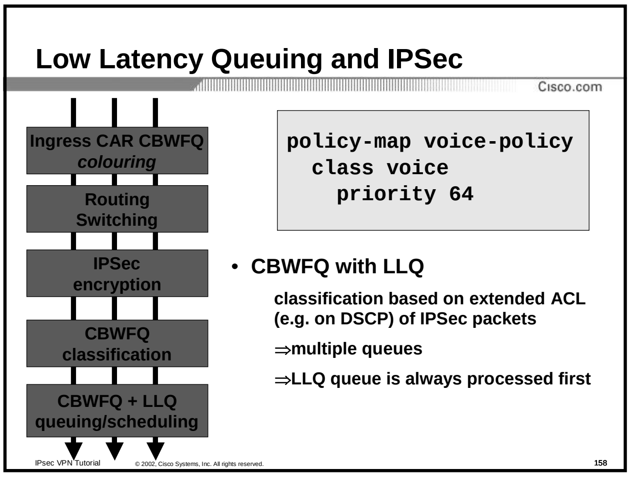
CBWFQ queuing/scheduling

- **Marking with DSCP is done before encryption**
- **CBWFQ (including LLQ)**

  classification based on extended ACL (e.g. on DSCP) of IPSec packets

  => multiple queues

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 157



Low Latency Queuing and IPSec

Cisco.com

Ingress CAR CBWFQ *colouring*

Routing Switching

IPSec encryption

CBWFQ classification

CBWFQ + LLQ queuing/scheduling

```
policy-map voice-policy
  class voice
    priority 64
```

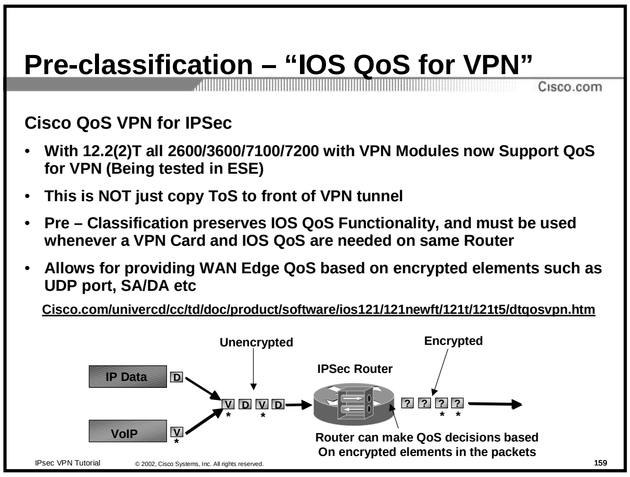
- **CBWFQ with LLQ**

  classification based on extended ACL (e.g. on DSCP) of IPSec packets

  ⇒multiple queues

  ⇒LLQ queue is always processed first

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 158



Pre-classification – "IOS QoS for VPN"

Cisco.com

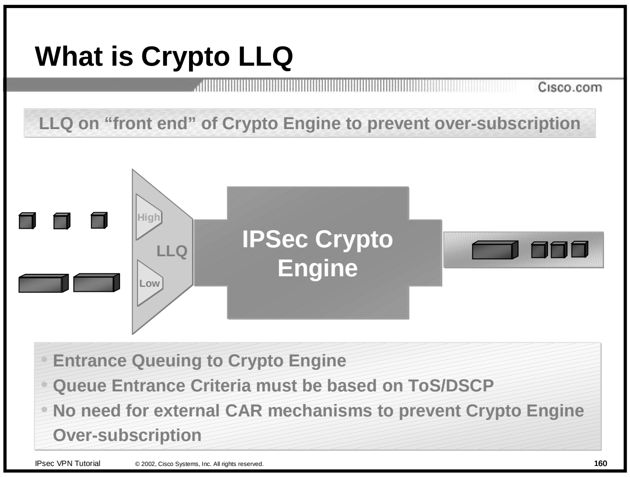
Cisco QoS VPN for IPSec

- **With 12.2(2)T all 2600/3600/7100/7200 with VPN Modules now Support QoS for VPN (Being tested in ESE)**
- **This is NOT just copy ToS to front of VPN tunnel**
- **Pre – Classification preserves IOS QoS Functionality, and must be used whenever a VPN Card and IOS QoS are needed on same Router**
- **Allows for providing WAN Edge QoS based on encrypted elements such as UDP port, SA/DA etc**

Cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtqosvpn.htm

Router can make QoS decisions based On encrypted elements in the packets

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 159



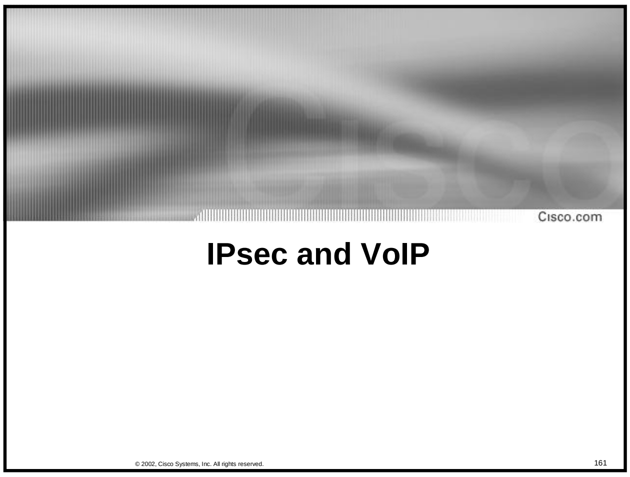
What is Crypto LLQ

Cisco.com

LLQ on "front end" of Crypto Engine to prevent over-subscription

- Entrance Queuing to Crypto Engine
- Queue Entrance Criteria must be based on ToS/DSCP
- No need for external CAR mechanisms to prevent Crypto Engine Over-subscription

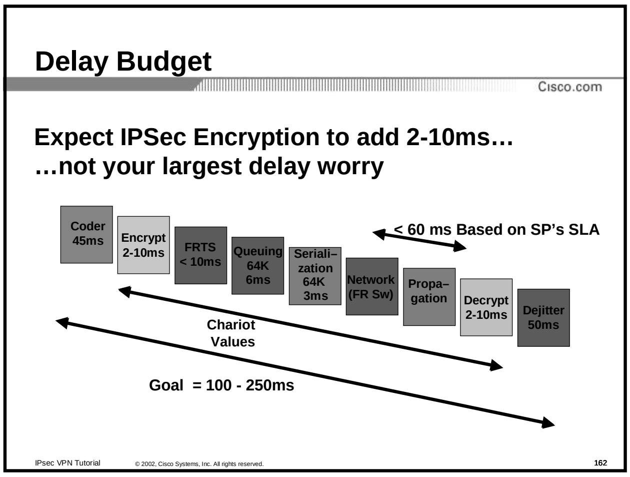
IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 160



Cisco.com

IPsec and VoIP

© 2002, Cisco Systems, Inc. All rights reserved. 161



Delay Budget

Cisco.com

Expect IPSec Encryption to add 2-10ms…
…not your largest delay worry

IPsec VPN Tutorial © 2002, Cisco Systems, Inc. All rights reserved. 162

VoIP & RTP

Cisco.com

	IP	UDP	RTP	Voice
Length (bytes)	20	8	12	20

Payload (voice):	20 bytes
Overhead:	40 bytes
Total packet:	60 bytes

If codec = 8 kbps, actual line utilization is 24 kbps !

VoIP & Compressed RTP *RFC 2508*

Cisco.com

	cRTP	Voice
Length (bytes)	~3	20

Payload (voice):	20 bytes
Overhead:	~3 bytes
Total packet:	~23 bytes

If codec = 8 kbps, actual line utilization is 9 kbps
cRTP compress IP+UDP+RTP only
cRTP works only link-by-link over PPP, …

VoIP & RTP & IPSec = Adding Headers

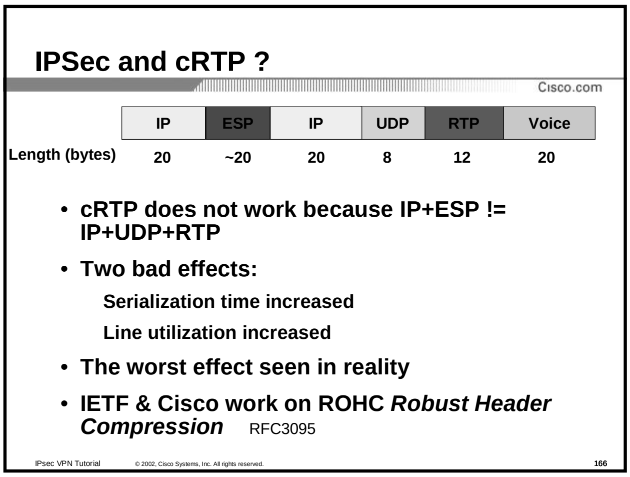
Cisco.com

encrypted (ESP through Voice)

	IP	ESP	IP	UDP	RTP	Voice
Length (bytes)	20	~20	20	8	12	20

Payload:	20 bytes
Overhead:	80 bytes
Total packet:	100 bytes

If codec = 8 kbps, actual line utilization is 40 kbps !

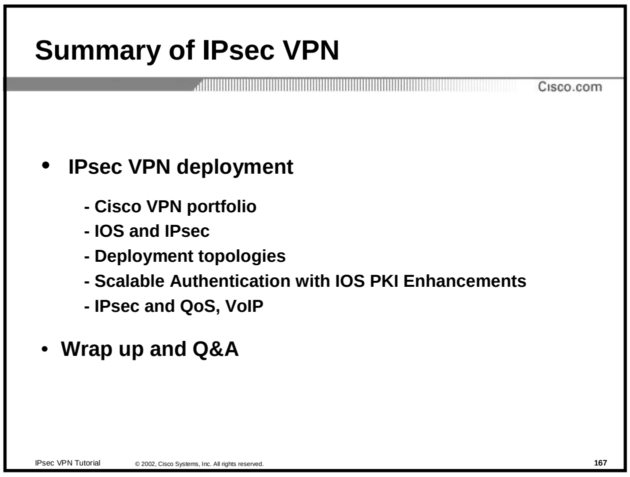


IPSec and cRTP ?

Cisco.com

	IP	ESP	IP	UDP	RTP	Voice
Length (bytes)	20	~20	20	8	12	20

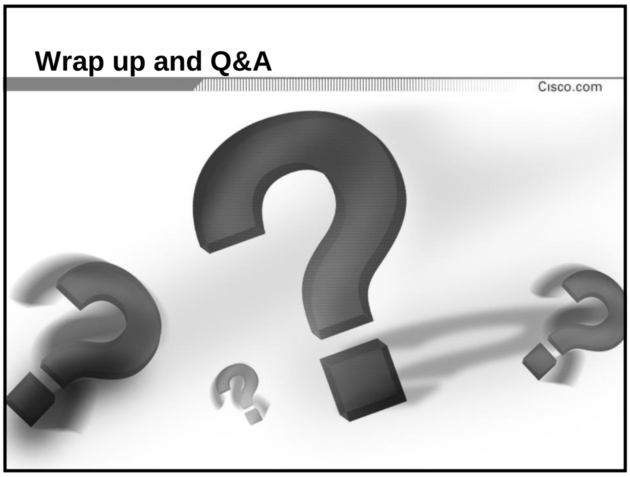
- cRTP does not work because IP+ESP != IP+UDP+RTP
- Two bad effects:
  - Serialization time increased
  - Line utilization increased
- The worst effect seen in reality
- IETF & Cisco work on ROHC *Robust Header Compression* RFC3095



Summary of IPsec VPN

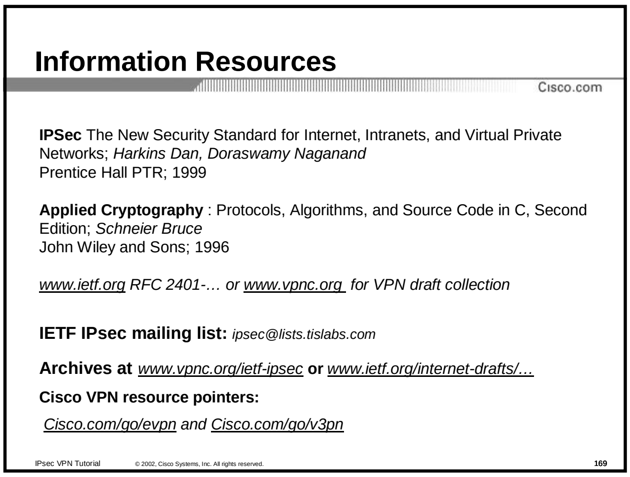
Cisco.com

- IPsec VPN deployment
  - - Cisco VPN portfolio
  - - IOS and IPsec
  - - Deployment topologies
  - - Scalable Authentication with IOS PKI Enhancements
  - - IPsec and QoS, VoIP
- Wrap up and Q&A



Wrap up and Q&A

Cisco.com



Information Resources

IPSec The New Security Standard for Internet, Intranets, and Virtual Private Networks; *Harkins Dan, Doraswamy Naganand*
Prentice Hall PTR; 1999

Applied Cryptography : Protocols, Algorithms, and Source Code in C, Second Edition; *Schneier Bruce*
John Wiley and Sons; 1996

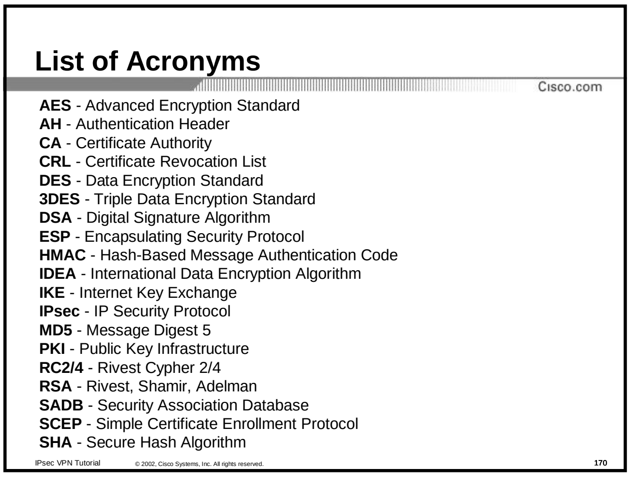
www.ietf.org RFC 2401-… or www.vpnc.org for VPN draft collection

IETF IPsec mailing list: *ipsec@lists.tislabs.com*

Archives at *www.vpnc.org/ietf-ipsec* **or** *www.ietf.org/internet-drafts/…*

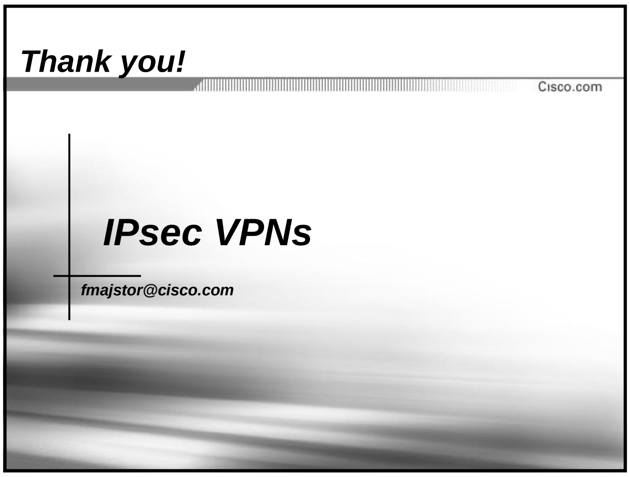
Cisco VPN resource pointers:

Cisco.com/go/evpn and Cisco.com/go/v3pn



List of Acronyms

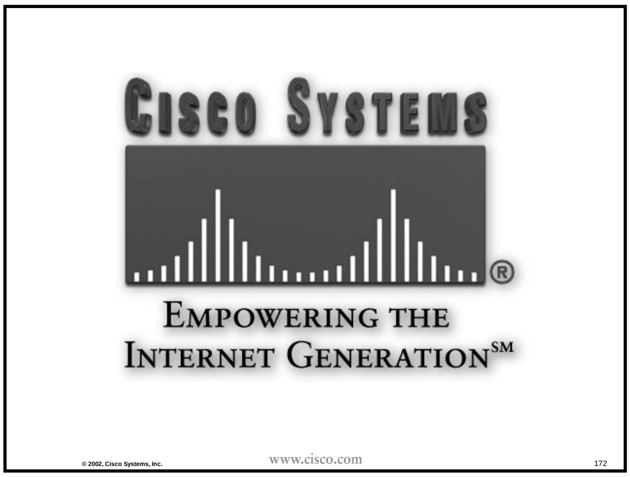
AES - Advanced Encryption Standard
AH - Authentication Header
CA - Certificate Authority
CRL - Certificate Revocation List
DES - Data Encryption Standard
3DES - Triple Data Encryption Standard
DSA - Digital Signature Algorithm
ESP - Encapsulating Security Protocol
HMAC - Hash-Based Message Authentication Code
IDEA - International Data Encryption Algorithm
IKE - Internet Key Exchange
IPsec - IP Security Protocol
MD5 - Message Digest 5
PKI - Public Key Infrastructure
RC2/4 - Rivest Cypher 2/4
RSA - Rivest, Shamir, Adelman
SADB - Security Association Database
SCEP - Simple Certificate Enrollment Protocol
SHA - Secure Hash Algorithm



Thank you!

IPsec VPNs

fmajstor@cisco.com



CISCO SYSTEMS

EMPOWERING THE
INTERNET GENERATION℠

www.cisco.com