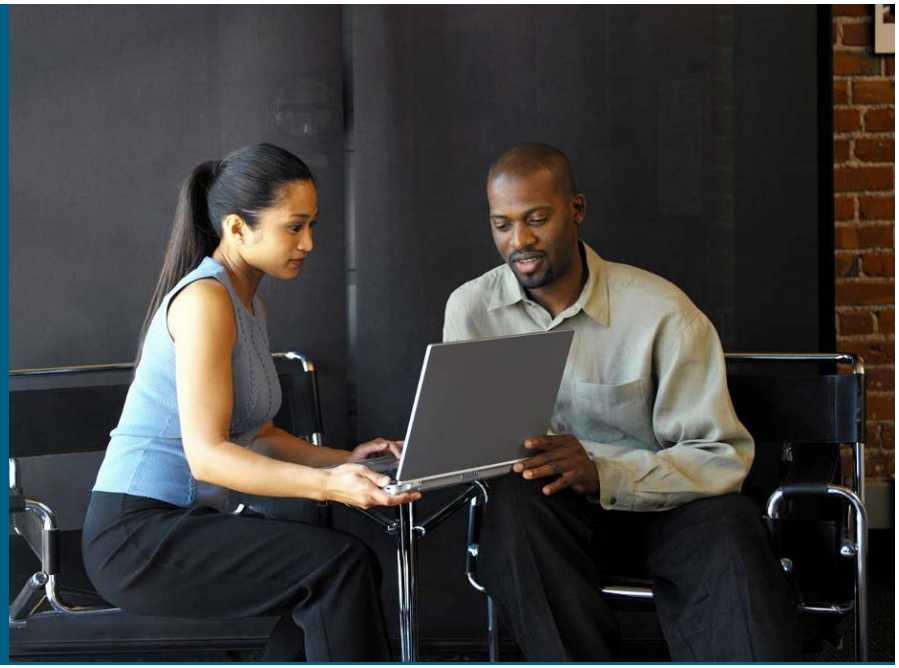
# Understanding IPsec

- Overview
- Two-Phase Connection
- Modes
- Configuration
- Debug Interpretation



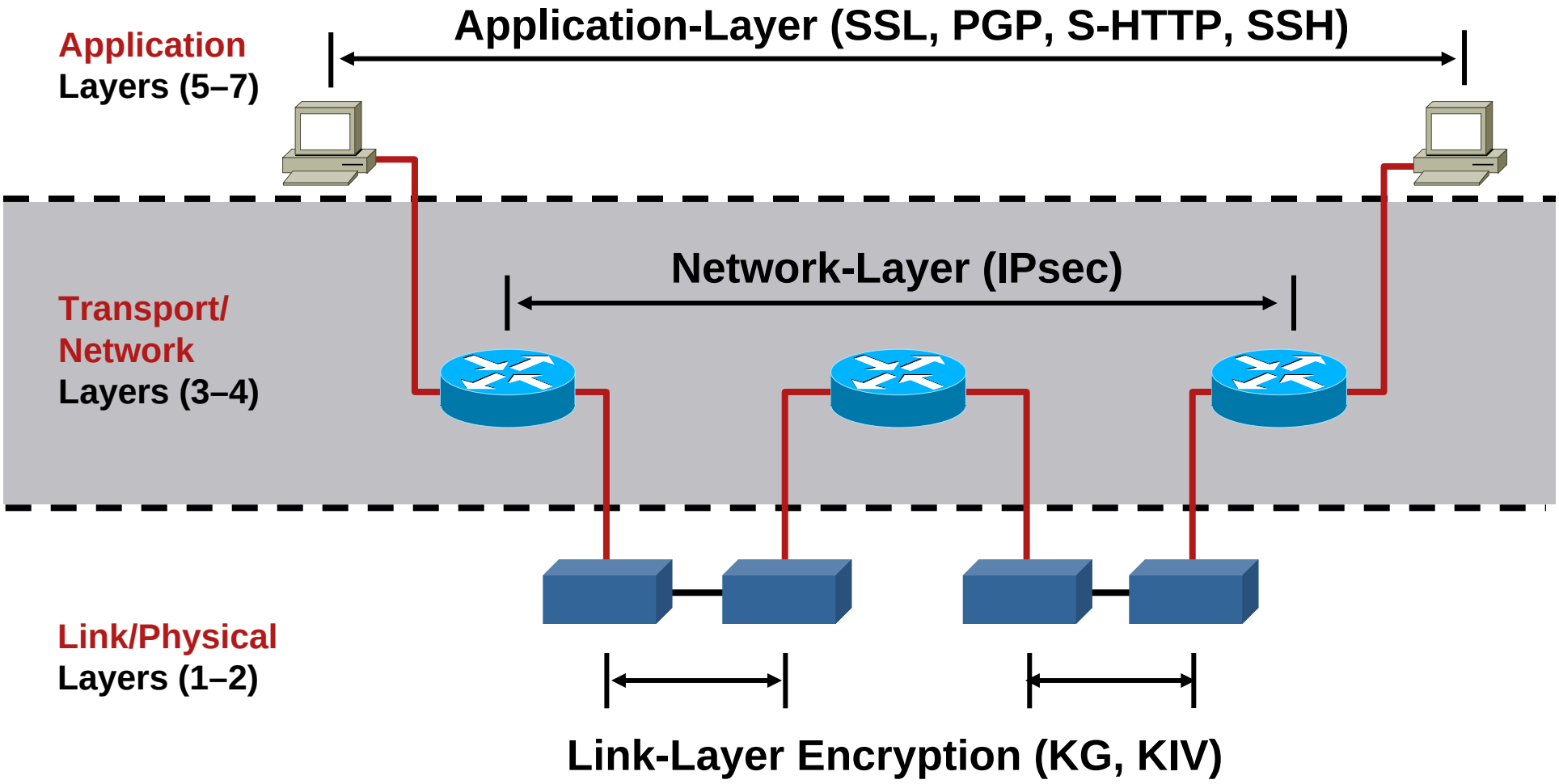
**Yusuf Bhaiji**
CCIE No. 9305

# What Is IPsec?

Internet Protocol Security

- IPsec is a set of security protocols and algorithms used to secure IP data at the network layer.
- IPsec provides data confidentiality (encryption), integrity (hash), and authentication (signatures and certificates) of IP packets while maintaining the ability to route them through existing IP networks.

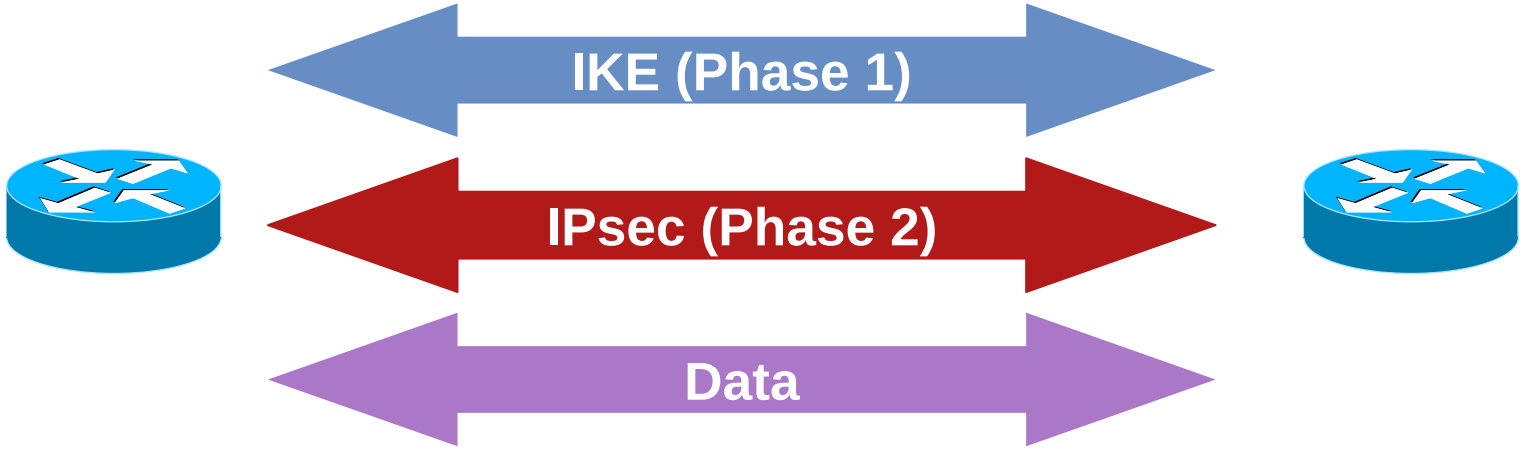
# Encryption Layers



# IPsec

- IPsec can ensure the confidentiality and authenticity of IP packets.
- These are the key points of IPsec:
  - Two modes of propagation (transport and tunnel)
  - Security associations (SAs)
  - Two types of header (ESP and AH)
- IPsec does not provide a key exchange mechanism.

# IPsec: Building a Connection




- Two-phase protocol:

  Phase 1 exchange: Two peers establish a secure, authenticated channel with which to communicate; Main mode or Aggressive mode accomplishes a Phase 1 exchange.

  There is also a Transaction Mode, that sits between Phase 1 and Phase 2; (Phase 1.5) which is used for Cisco Easy VPN (EzVPN) client scenario performing XAUTH or client attributes (mode config).

  Phase 2 exchange: Security associations are negotiated on behalf of IPsec services; Quick Mode accomplishes a Phase 2 exchange.

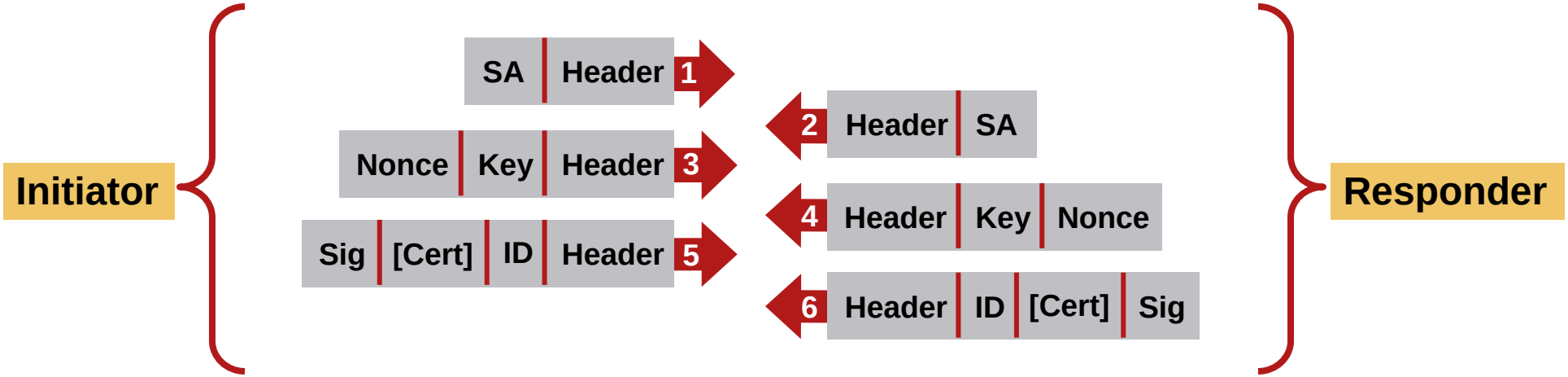
- Each phase has its SAs: ISAKMP SA (Phase 1) and IPsec SA (Phase 2).

# IKE and ISAKMP

- IKE is a key exchange mechanism.
- It is typically used for establishing IPsec sessions.
- There are five variations of an IKE negotiation:
  - –Two modes (aggressive mode and main mode)
  - –Three authentication methods (preshared, public key encryption, and public key signature)
- IKE is a sheer key exchange protocol.

# IKE: Main Mode (Phase 1)

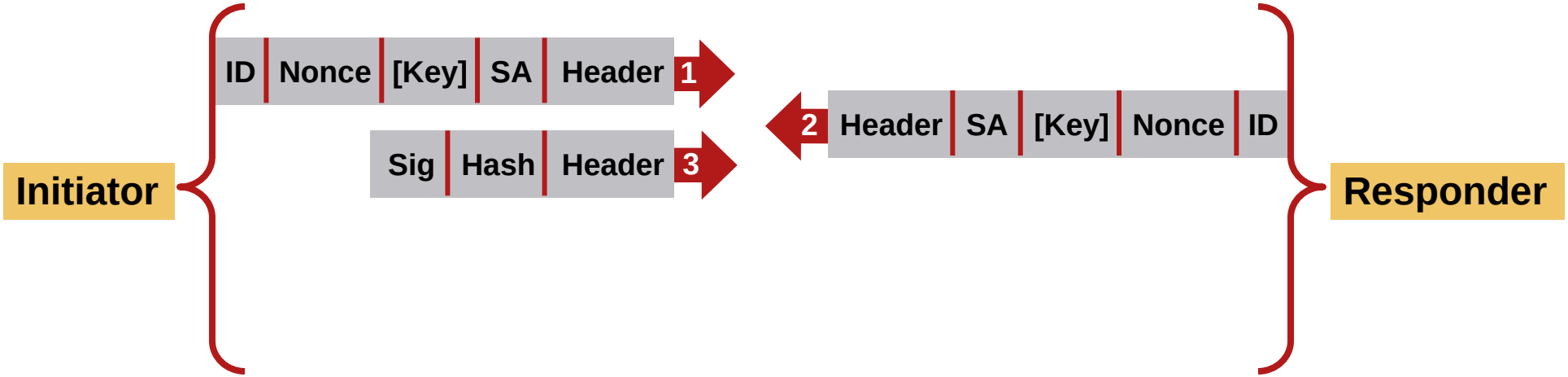
## ISAKMP Main Mode




- MSG 1: Initiator offers acceptable encryption and authentication algorithms (3DES, MD5, or RSA)—i.e., the transform-set.
- MSG 2: Responder presents acceptance of the proposal (or not).
- MSG 3: Initiator Diffie-Hellman key and nounce (key value is usually a number of 1024-bit length).
- MSG 4: Responder Diffie-Hellman key and nounce.
- MSG 5: Initiator signature, ID, and keys (maybe cert), i.e., authentication data.
- MSG 6: Responder signature, ID, and keys (maybe cert).

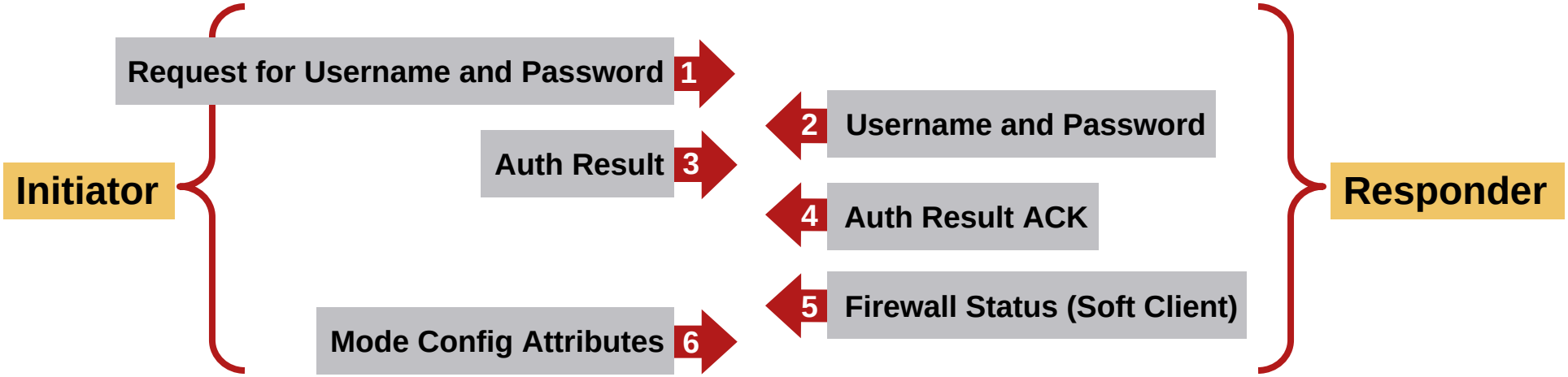
# IKE: Aggressive Mode (Phase 1)

## ISAKMP Aggressive Mode




- MSG 1: Initiator key exchange, ID, nonce, and parameter proposal
- MSG 2: Responder key exchange, ID, nonce, and acceptable parameters
- MSG 3: Initiator signature, hash, and ID

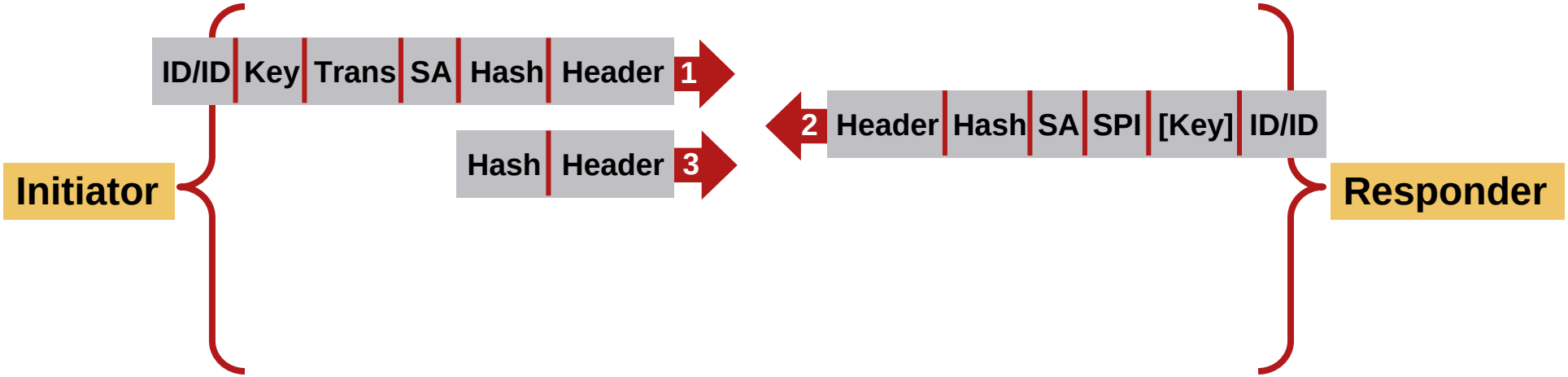
# IKE: Transaction Mode (Cisco Easy VPN Client)




- Transaction mode facilitates user authentication and the transfer of mode config attributes.
- Hardware and software clients only.
- The number of messages may vary depending on authentication protocol (RADIUS, SDI, etc.)

# IKE: Quick Mode (Phase 2)

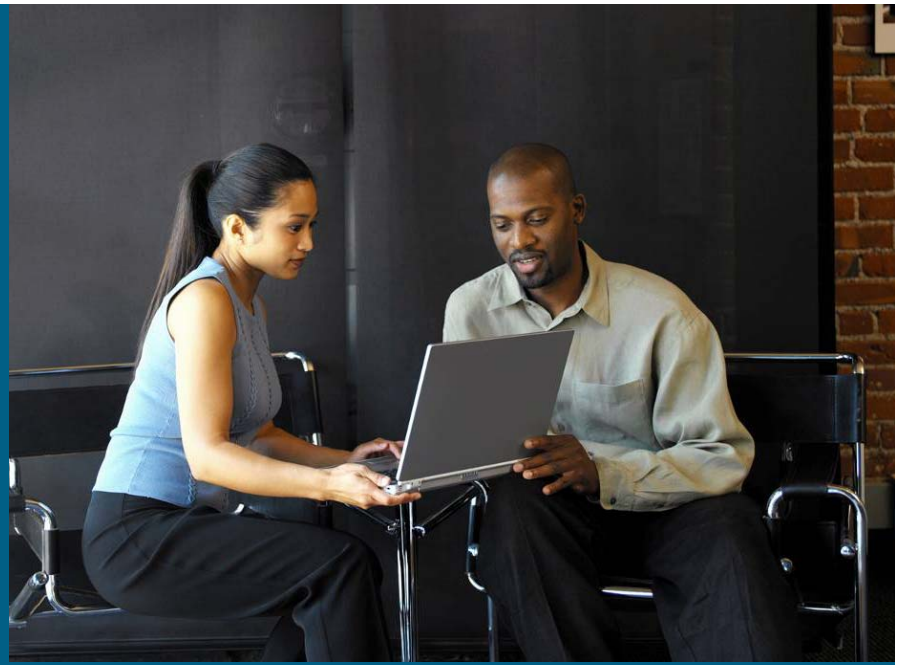
## Quick Mode



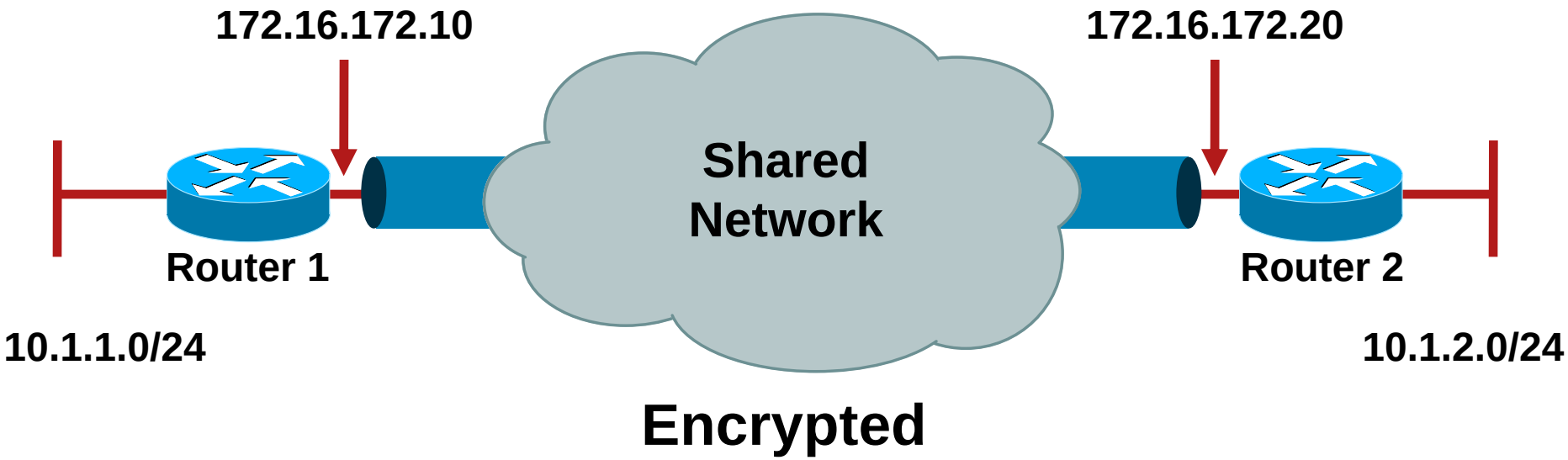

- MSG 1: Hash, SA proposal, IPsec transform, keying material, and ID (proxy identities, source, and destination)
- MSG 2: Responder hash, agreed to SA proposal, Responder SPI, and key
- MSG 3: Hash to verify current and live peer

Now passing encrypted traffic

# Basic IPsec Configuration



# Layout



# Router Configurations

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key C!scO address 172.16.172.20
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
 set peer 172.16.172.20
 set transform-set myset
 match address 101
```

**"crypto isakmp policy.." command defines the Phase 1 SA parameters**

**"crypto ipsec transform-set.." command defines IPsec encryption and authentication algorithm**

**"crypto map.." command defines the IPsec SA (Phase 2 SA) parameters**

# Router Configurations

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
!

interface Ethernet1/0
 ip address 172.16.172.10 255.255.255.240
 crypto map vpn
!

access-list 101 permit ip 10.1.1.0 0.0.0.255
10.1.2.0 0.0.0.255
```

Interface that is connected to the private side of the network

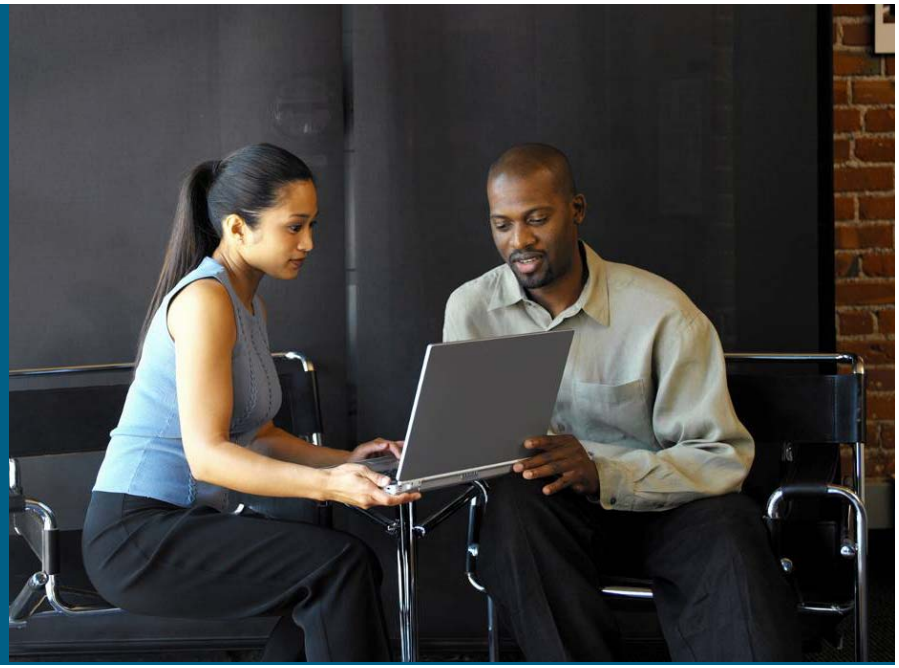
Crypto map is then applied to an outbound interface

Access-list defines interesting VPN traffic

# Router Configurations

```
R1#show crypto map
Crypto Map "vpn" 10 ipsec-isakmp
        Peer = 172.16.172.20
        Extended IP access list 101
          access-list 101 permit ip 10.1.1.0 0.0.0.255 10.1.2.0
          0.0.0.255
        Current peer: 172.16.172.20
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={ myset, }
        Interfaces using crypto map vpn:
                Ethernet1/0
```

# Interpreting Basic IPsec Debugs



# Debug Commands Explained

The next 10 slides show output of the debug commands listed below and explain how to interpret these debugs during each stage of tunnel establishment.

- debug crypto isakmp
- debug crypto ipsec
- debug crypto engine

# Tunnel Establishment

- ICMP source and destination addresses equal match address ACL for the crypto map vpn.

**Interesting Traffic Received**

```
00:04:10: IPsec(sa_request): ,
   (key eng. msg.) OUTBOUND local= 172.16.172.10, remote= 172.16.172.20,
   local_proxy = 10.1.1.0/255.255.255.0/0/0 (type=4),
   remote_proxy = 10.1.2.0/255.255.255.0/0/0 (type=4),
```

- 'local' is the local tunnel end-point; 'remote' is the remote crypto end point as configured in the map; local_proxy is the src interesting traffic as defined by the match address access list; and remote_proxy is the destination interesting traffic as defined by the match address access list.

```
protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x4A10F22E(1242624558), conn_id= 0, keysize= 0, flags= 0x400C
```

- The protocol and the transforms are specified by the crypto map, which has been hit, as are the lifetimes.

# IKE Main Mode Negotiation: Phase 1 SA Negotiation

- Begins main mode exchange; the first two packets negotiate Phase 1 SA parameters.


```
        ISAKMP: received ke message (1/1)
        ISAKMP: local port 500, remote port 500
        ISAKMP (0:1): Input = IKE_MESG_FROM_IPsec, IKE_SA_REQ_MM
  Old State = IKE_READY  New State = IKE_I_MM1


        ISAKMP (0:1): beginning Main Mode exchange
        00:04:10: ISAKMP (0:1): sending packet to 172.16.172.20 (I)
MM_NO_STATE
        00:04:10: ISAKMP (0:1): received packet from 172.16.172.20
(I) MM_NO_STATE
        00:04:10: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH
        Old State = IKE_I_MM1  New State = IKE_I_MM2
```

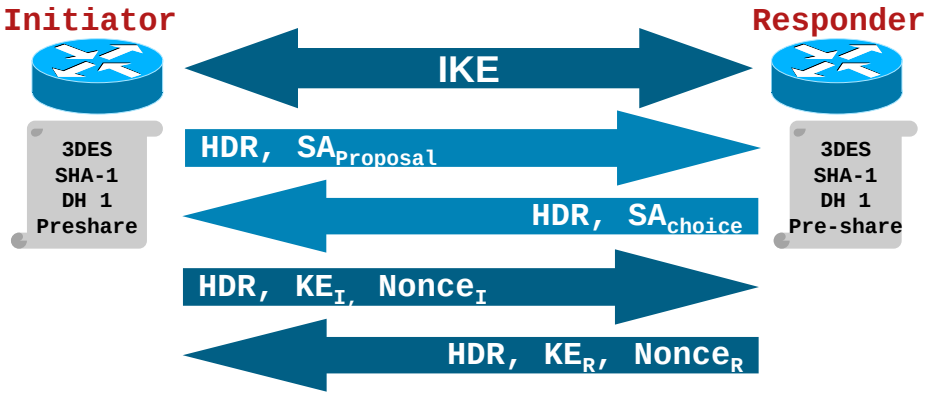
# IKE Main Mode Negotiation: Phase 1 SA Negotiation

```
00:04:10: ISAKMP (0:1): processing SA payload. message ID = 0
00:04:10: ISAKMP (0:1): found peer pre-shared key matching 172.16.172.20
00:04:10: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
00:04:10: ISAKMP:      encryption 3DES-CBC
00:04:10: ISAKMP:      hash SHA
00:04:10: ISAKMP:      default group 1
00:04:10: ISAKMP:      auth pre-share
00:04:10: ISAKMP:      life type in seconds
00:04:10: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
00:04:10: ISAKMP (0:1): atts are acceptable. Next payload is 0
00:04:10: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_I_MM2  New State = IKE_I_MM2
```

- The policy 1 on this router and the atts offered by the other side matched.

# IKE Main Mode Negotiation: DH Exchange

- The third and fourth packets complete the Diffie-Hellman exchange.

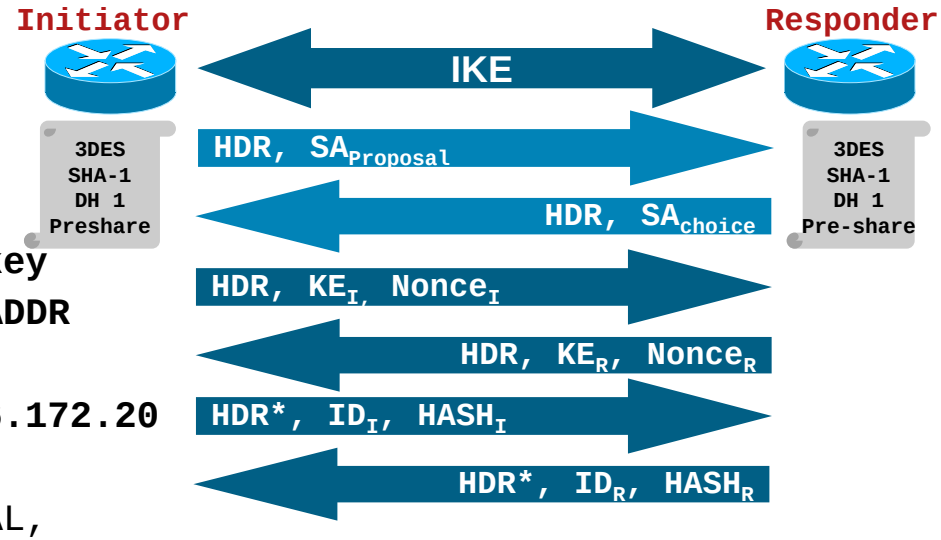



```
ISAKMP (0:1): sending packet to
172.16.172.20 (I) MM_SA_SETUP
ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
 IKE_PROCESS_COMPLETE Old State = IKE_I_MM2  New State = IKE_I_MM3
ISAKMP (0:1): received packet from 172.16.172.20 (I) MM_SA_SETUP
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_I_MM3  New State = IKE_I_MM4

ISAKMP (0:1): processing KE payload. message ID = 0
ISAKMP (0:1): processing NONCE payload. message ID = 0
ISAKMP (0:1): found peer pre-shared key matching 172.16.172.20
ISAKMP (0:1): SKEYID state generated
ISAKMP (0:1): processing vendor id payload
```

# IKE Main Mode Negotiation: Authentication

- The fifth and sixth packets complete IKE authentication; Phase 1 SA established.

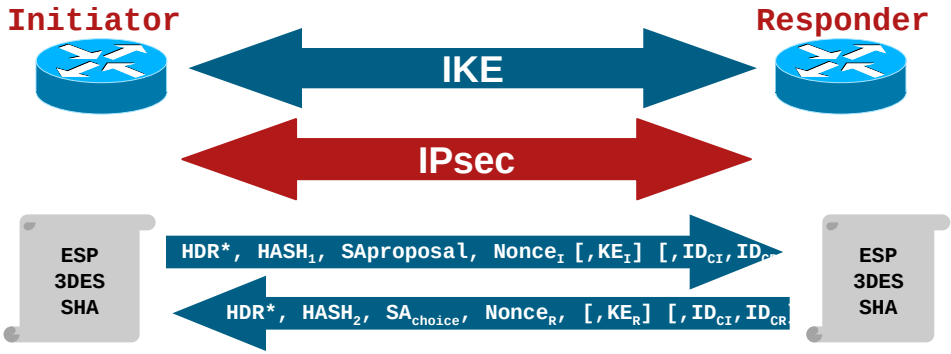



```
ISAKMP (0:1): SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR
……
ISAKMP (0:1): sending packet to 172.16.172.20
(I) MM_KEY_EXCH
ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETEOld State = IKE_I_MM4  New State = IKE_I_MM5

ISAKMP (0:1): received packet from 172.16.172.20 (I) MM_KEY_EXCH
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_I_MM5  New State = IKE_I_MM6
ISAKMP (0:1): processing ID payload. message ID = 0
ISAKMP (0:1): processing HASH payload. message ID = 0
ISAKMP (0:1): SA has been authenticated with 172.16.172.20
ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_I_MM6  New State = IKE_P1_COMPLETE
```

# IKE Quick Mode: Phase 2 SA Begins

- Begin Quick Mode exchange; IPsec SA will be negotiated in QM.




```
ISAKMP (0:1): beginning Quick Mode exchange,
 M-ID of 965273472
ISAKMP (0:1): sending packet to 172.16.172.20 (I) QM_IDLE
ISAKMP (0:1): Node 965273472, Input = IKE_MESG_INTERNAL,
IKE_INIT_QM Old State = IKE_QM_READY  New State = IKE_QM_I_QM1
ISAKMP (0:1): received packet from 172.16.172.20 (I) QM_IDLE
```

- The IPsec SA proposal offered by the far end will be checked against local crypto map configuration.

```
ISAKMP (0:1): processing HASH payload. message ID = 965273472
ISAKMP (0:1): processing SA payload. message ID = 965273472
```

# IKE Quick Mode: Phase 2 SA Negotiation

```
ISAKMP (0:1): Checking IPsec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 3600
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-MD5
ISAKMP (0:1): atts are acceptable.
IPsec(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 172.16.172.10, remote= 172.16.172.20,
    local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
```

# IKE Quick Mode: Phase 2 SA (Inbound and Outbound SA)

## Two IPsec SAs have been negotiated:

- An incoming SA with the SPI generated by the local machine
- An outbound SA with the SPI proposed by the remote end

```
ISAKMP (0:1): Creating IPsec SAs

inbound SA from 172.16.172.20 to 172.16.172.10(proxy 10.1.2.0 to 10.1.1.0)
has spi 0x8EAB0B22 and conn_id 2029 and flags 4
 lifetime of 3600 seconds lifetime of 4608000 kilobytes

outbound SA from 172.16.172.10   to 172.16.172.20 (proxy 10.1.1.0 to 10.1.2.0)
has spi -343614331 and conn_id 2030 and flags C
  lifetime of 3600 seconds lifetime of 4608000 kilobytes
```

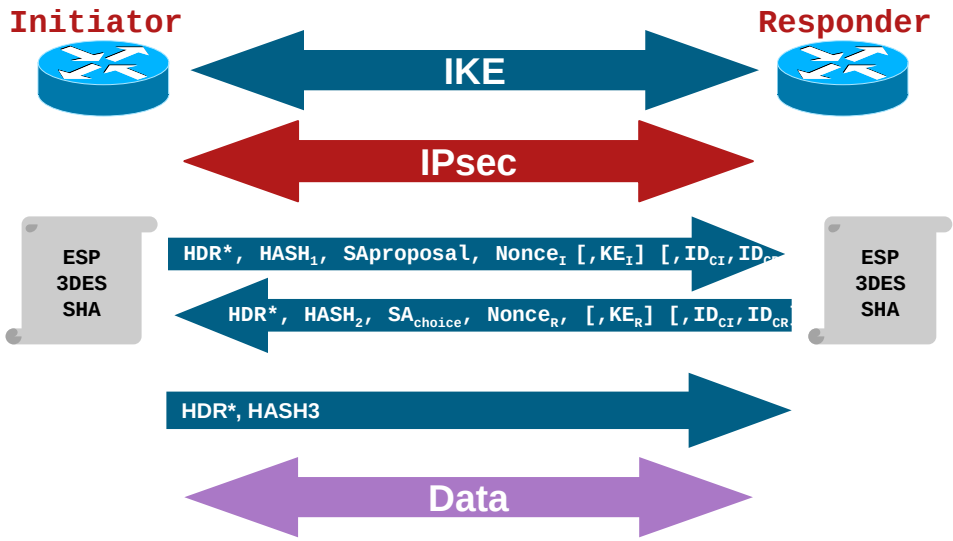
# IKE Quick Mode: Phase 2 SA Negotiated

- The IPsec SA info negotiated by IKE will be populated into the router SADB.

```
00:04:10: IPsec(key_engine): got a queue event...
00:04:10: IPsec(initialize_sas): ,
  (key eng. msg.) INBOUND local= 172.16.172.10, remote= 172.16.172.20,
    local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x8EAB0B22(2393574178), conn_id= 2029, keysize= 0, flags= 0x4
00:04:10: IPsec(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 172.16.172.10, remote= 172.16.172.20,
    local_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 10.1.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xEB84DC85(3951352965), conn_id= 2030, keysize= 0, flags= 0xC
```

# IKE Quick Mode: Phase 2 SA Created in SADB

- IPsec SA is created in SADB, sent out last packet with commit bit set, and the IPsec tunnel is established.




```
IPsec(create_sa): sa created,
 (sa) sa_dest= 172.16.172.10,
 sa_prot= 50,
 sa_spi= 0x8EAB0B22(2393574178),
 sa_trans= esp-3des esp-md5-hmac ,
 sa_conn_id= 2029
IPsec(create_sa): sa created,
 (sa) sa_dest= 172.16.172.20, sa_prot= 50, sa_spi= 0xEB84DC85(3951352965),
 sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2030
ISAKMP (0:1): sending packet to 172.16.172.20 (I) QM_IDLE
ISAKMP (0:1): Node 965273472, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_I_QM1  New State = IKE_QM_PHASE2_COMPLETE
```

# Recommended Reading

Network Security Technologies and Solutions (CCIE Professional Development Series)

ISBN: 1587052466

By Yusuf Bhaiji