

# IPv4 IPsec - IKE Phase II (Quick mode)

(An exchange of keys to determine how the data between the two will be encrypted)

The purpose of IKE phase two is to negotiate ISAKMP SAs to set up the IPsec tunnel. **IKE phase two** performs the following functions:

- Negotiates ISAKMP SA parameters protected by an existing IKE SA
- Establishes IPsec security associations
- Periodically renegotiates IPsec SAs to ensure security
- Optionally performs an additional Diffie-Hellman exchange ( $g^x/g^y$ ), or the keys may be derived from the phase 1 shared secret.

## ISAKMP Quick-mode – Phase II

*IKEv1 3-exchanges*

### Initiator

HDR\*, hash^1,[SA] proposal,NONCEi,( $g^x$ ),(ID^i)

To authenticate itself, to select a nonce, to propose security association(s) to execute an exchange of public Diffie-Hellman values.

### Responder

HDR\*, hash^2,[SA] proposal,NONCEr,( $g^y$ ),(ID^r)

After responder receives message 1 from the initiator and successfully authenticates it using HASH^1, it constructs a reply, message 2, to be sent back to initiator.

### Initiator

HDR\*,[SA] hash^3

**Hash transmitted** - that covers the message ID and both nonces that were exchanged in messages 1 and 2.

As a check against replay attacks, the responder waits until receipt of the next message. At this point, both initiator and responder have exchanged all the information necessary for them to derive the necessary keying material.

### Responder

HDR\*,[SA] notification

(This message is requested and sent between the initiator and responder in Windows Server 2003. Quick mode message 3. The payload is **not required by the IKE standard**. The initiator from sending IPsec-protected data, the responder is ready to receive the data.)

\* ISAKMP message payload

## Quick Mode Negotiation

When main mode negotiation completes or an existing quick mode SA expires, IKE begins quick mode negotiation. The quick mode negotiation process is implemented as defined in **RFC 2409**. All quick mode negotiations are protected with the main mode SA that was established during the main mode negotiation. Quick mode negotiation establishes two quick mode SAs. One SA is inbound and the other is outbound.

Quick mode **exchanges nonces** which are used to generate new shared keys to protect against replay attacks.

Quick mode is also used to renegotiate a new ISAKMP SA. Quick mode is used to refresh the keying material used to create the SA derived from the Diffie-Hellman exchange in phase one.

$g^x/g^y$  are the Diffie-Hellman ([DH]) public values.

**Identities, ID^i and ID^r, are optional.**

If not sent, it is assumed that the initiator is acting on behalf of the peer.

A common value for ID values used for the initiator and responder is the peer's IP address.

COPYRIGHT  
©ITcharts.com

## Perfect Forward Secrecy

If perfect forward secrecy is enabled, the Diffie-Hellman exchange is performed for each quick mode negotiation that has a payload. This means that the keys used for encryption are derived from the Diffie-Hellman exchange in phase one.