Network Layer Security Protocol IPsec

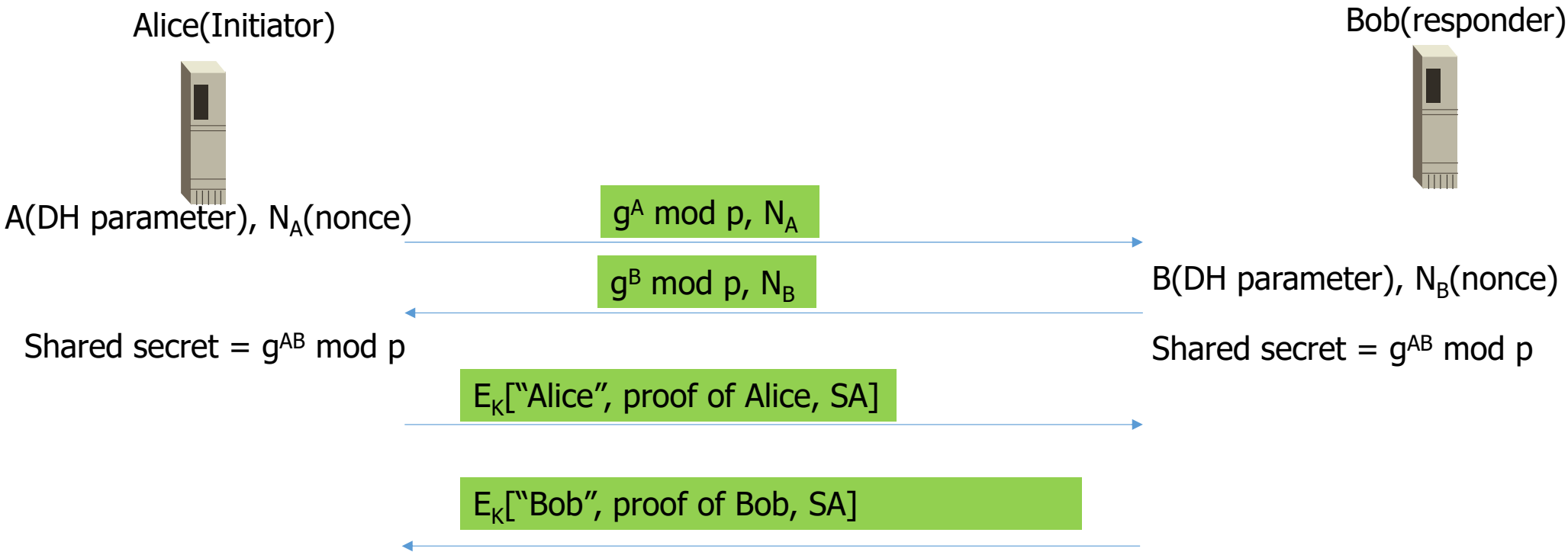
2019. 5. 13

Internet Key Exchange (IKE)

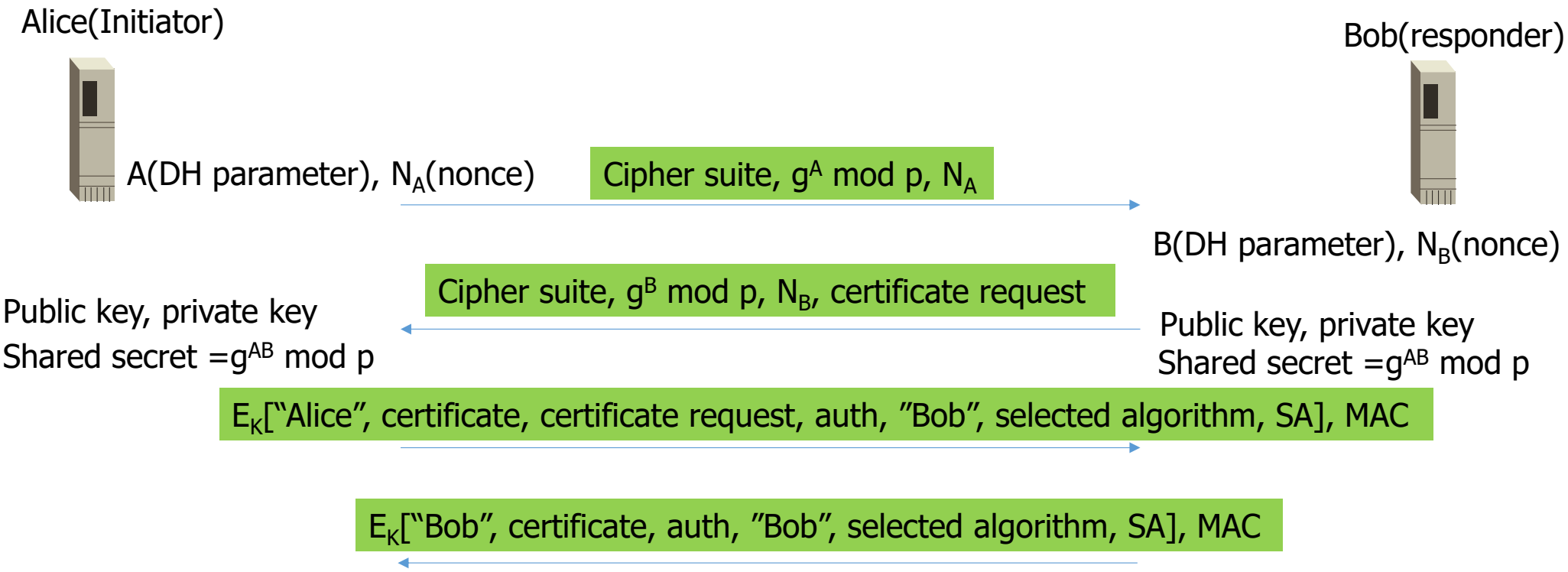
- Establish a secure session between two endpoints by doing:
  - Authentication
  - Key Establishment
- IKEv2
  - Greatly simplified IKEv1
  - IKEv1 is unnecessarily(?) complex (2 phases, 9 protocols)
  - IKEv2 is still complex

The First exchange of IKEv2

The initial exchanges authenticate each other and set up a special security association (SA).

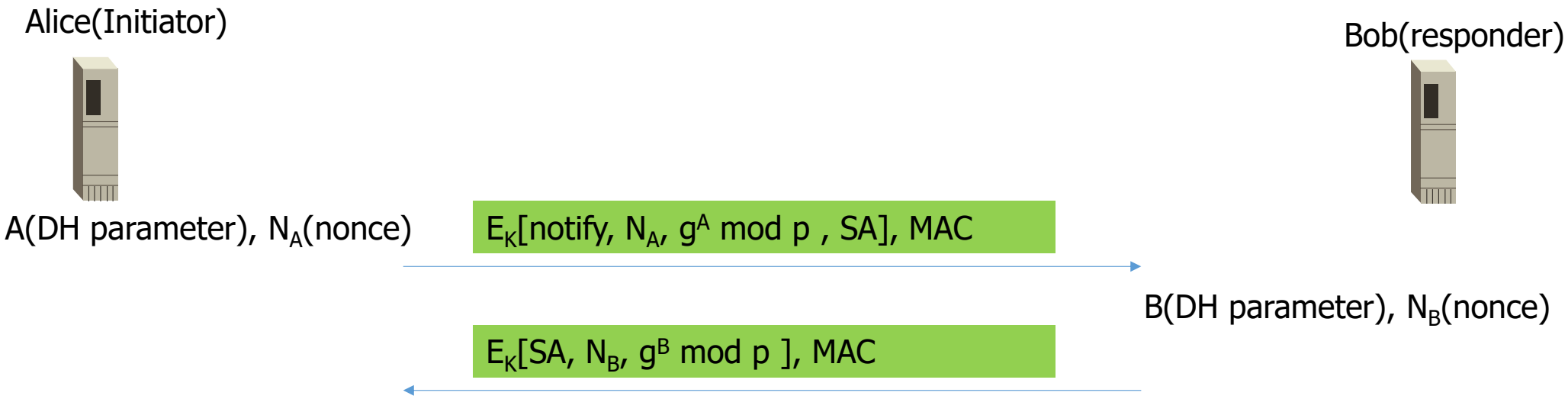


A little bit detailed procedure of IKEv2



Create Child SA

- CREAT_CHILD_SA exchange can be used to establish further SAs.



After IKE

- After IKE, two end points establishes a secure logical connection called security association(SA).
- SA identifies the identity number (SPI), the identities of two ends, and all security profiles.
- Below, one example is shown.

A

SPI: 12345
Source IP: 200.168.1.100
Dest IP: 193.68.2.23
Protocol: ESP
Encryption algorithm: 3DES-cbc
HMAC algorithm: MD5
Encryption key: 0x7aeaca…
HMAC key:0xc0291f…

B

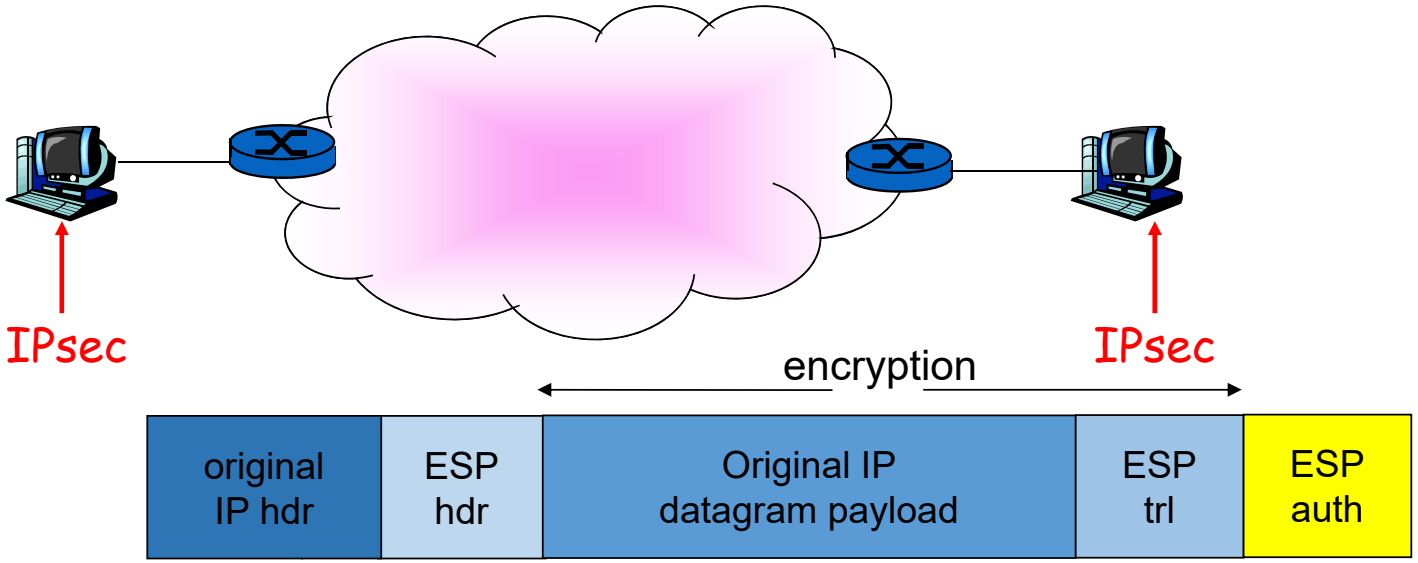
SPI: 12345
Source IP: 193.68.2.23
Dest IP: 200.168.1.100
Protocol: ESP
Encryption algorithm: 3DES-cbc
HMAC algorithm: MD5
Encryption key: 0x7aeaca…
HMAC key:0xc0291f…

Two headers

- Authentication Header (AH)
  - Sender authentication and data integrity
  - But not confidentiality
- Encapsulation Security Payload (ESP)
  - Sender authentication and data integrity
  - And also confidentiality
  - Commonly used in real deployment

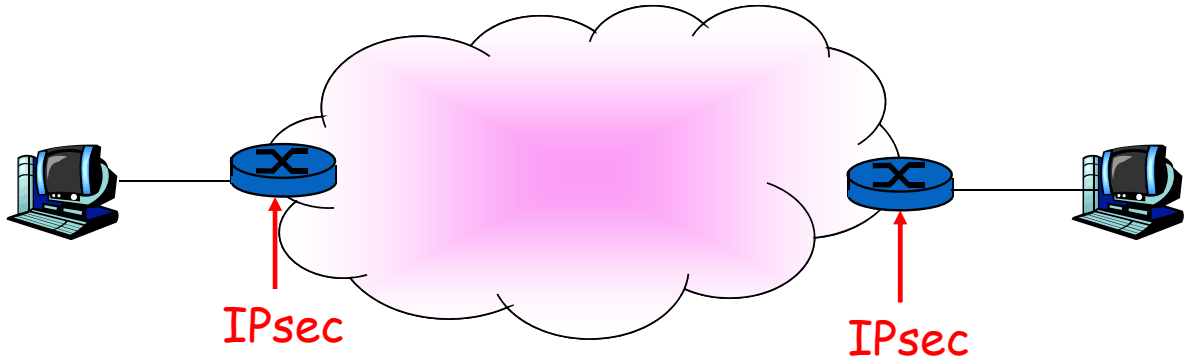
Two modes: Transport mode

- Transport mode
  - Provide the protection of the payload of an IP packet
  - Used for end-to-end communication



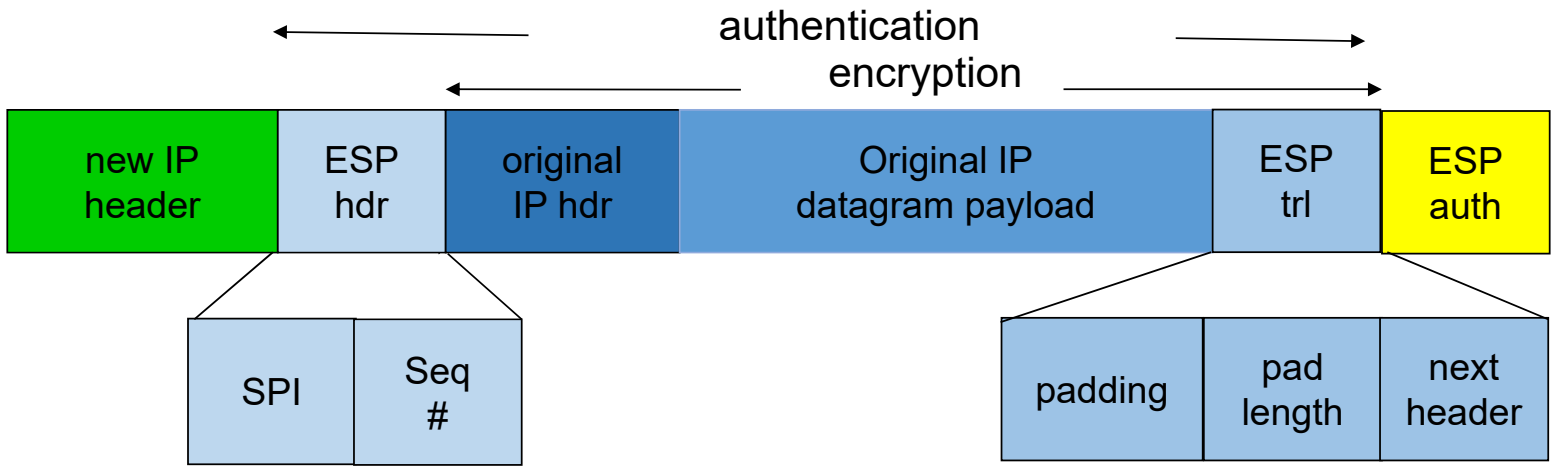
Two modes: Tunnel mode

- Tunnel mode
  - Provide the protection to the entire IP packet



Tunnel mode with ESP

- ESP trailer: appended to align with the length of block ciphers
- ESP header:
  - SPI (Security parameter index) : identify a security association (SA)
  - Sequence number: prevent replay attacks
- ESP auth : MAC (eg, HMAC)



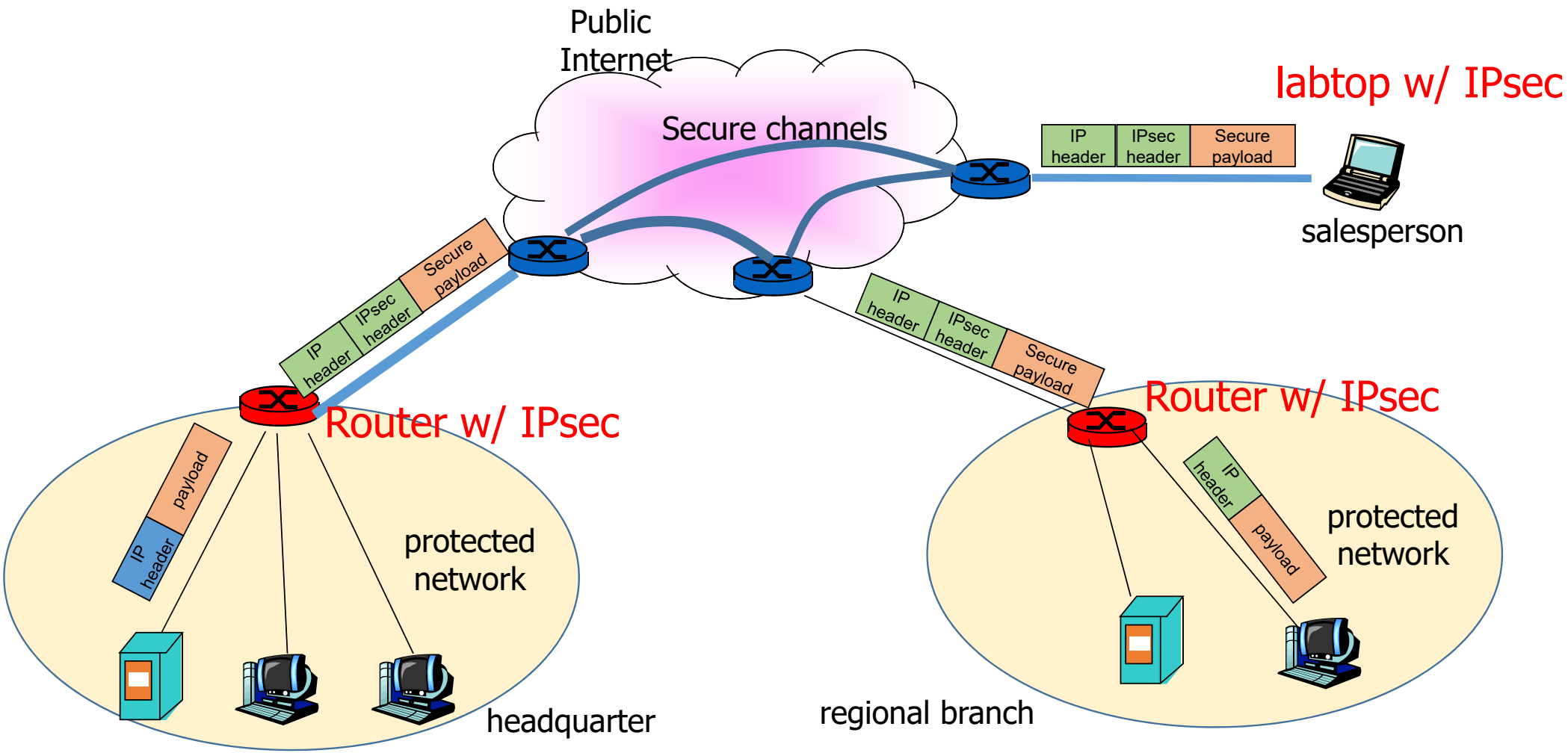
IPsec vs. TLS

- IPsec philosophy
  - Only change OS, don’t change applications or API
- TLS philosophy
  - Don’t change OS
  - Deploy as user process, so work on top of TCP
- Pros and Cons
  - …

IPsec application: VPN

- IPsec envisioned to replace TLS and be a standard way of protecting all communications, but the reality is not.
- One typical application of IPsec is VPN.
- VPN(virtual Private Network)
  - A private network is owned and administered by a private owner(ex, a company), and is allowed to be used by only members.
  - VPN is a way of constructing private networks on top of public networks.
  - Two essential requirements of VPN are the security and QoS.

VPN


Public Internet
Secure channels
Router w/ IPsec
Router w/ IPsec
Ilabtop w/ IPsec
salesperson
IP header
IPsec header
Secure payload
payload
protected network
protected network
headquarter
regional branch