NORTHFORGE

NETWORK SECURITY:
IPSEC AND SSL/TLS

NORTHFORGE

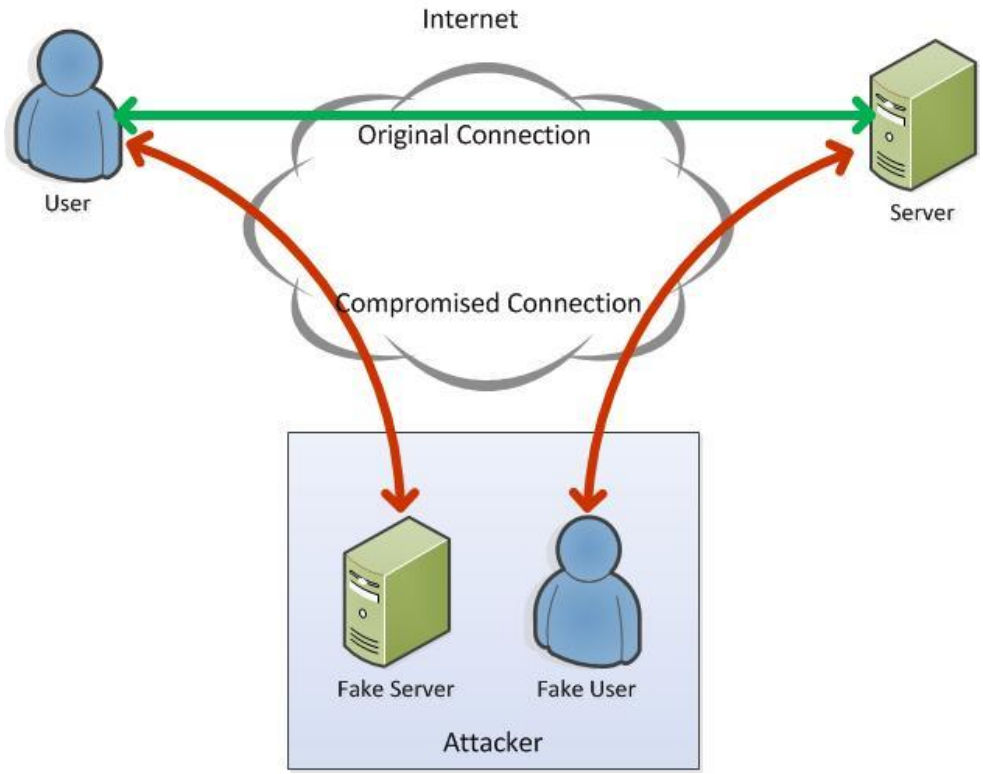
AGENDA

- Purpose of IPSec and SSL/TLS
- The whole picture with terminologies
- IPsec
- SSL/TLS
- Comparison

NORTHFORGE

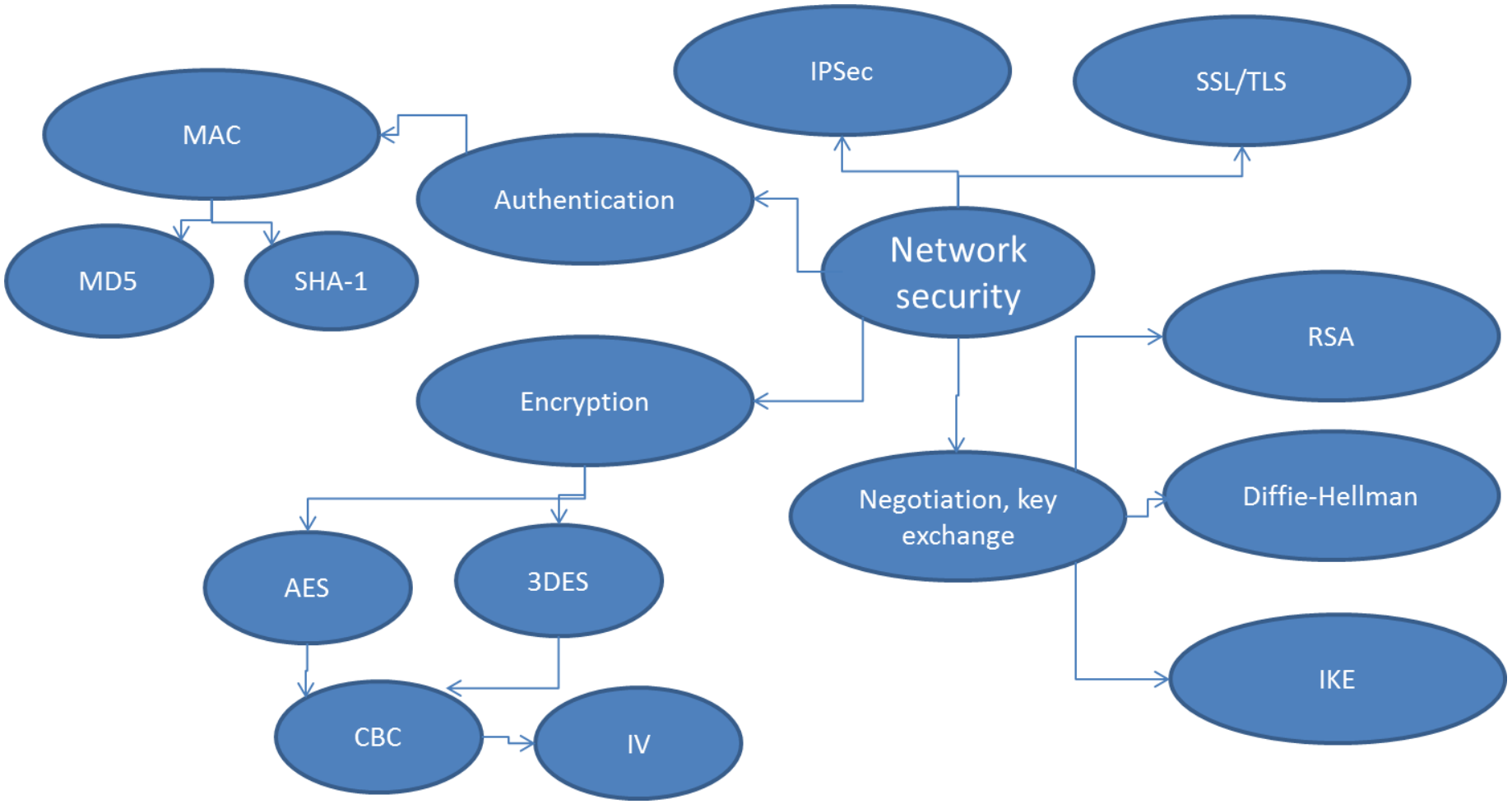
MOTIVATION: PROTECT USERS FROM ATTACKS

- Man in the middle attacks
  - Get user's sensitive information
  - Data forgery
  - Data replay



NORTHFORGE

MAP OF NETWORK SECURITY MECHANISM

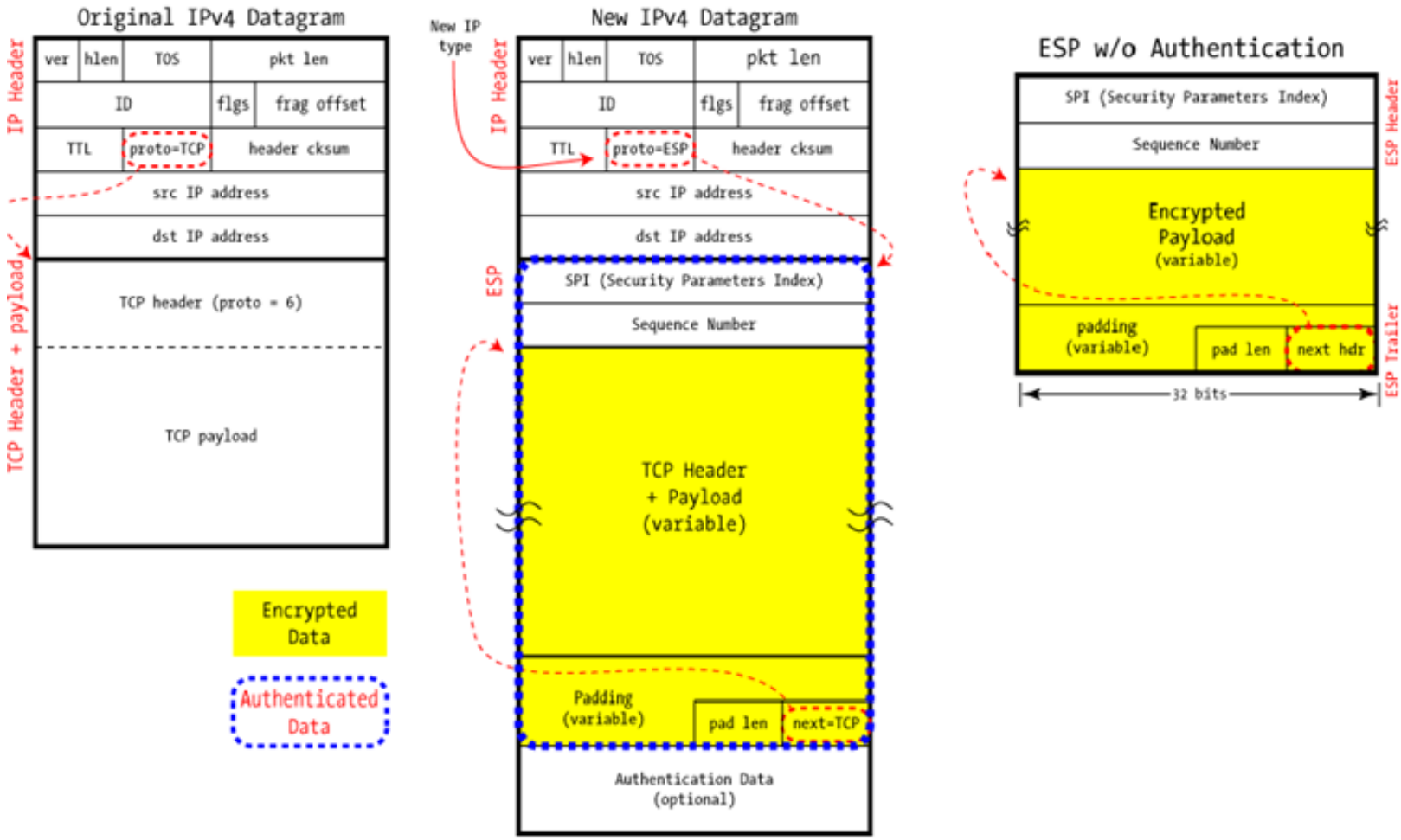


NORTHFORGE

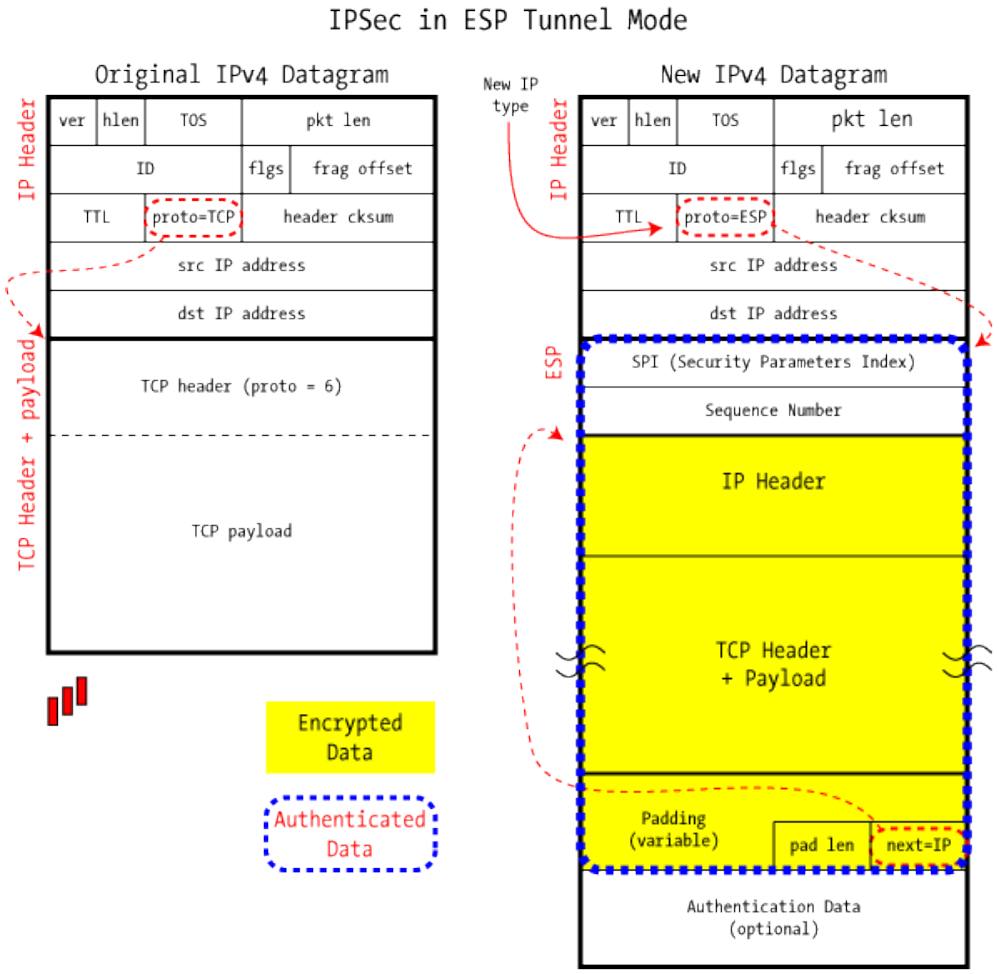
INTERNET PROTOCOL SECURITY- IPSEC

- Encapsulation
  - Authentication Header - AH
  - Encapsulating Security Payload - ESP
- Mode of operation
  - Transport mode
  - Tunnel mode

IPSEC IN ESP TRANSPORT MODE

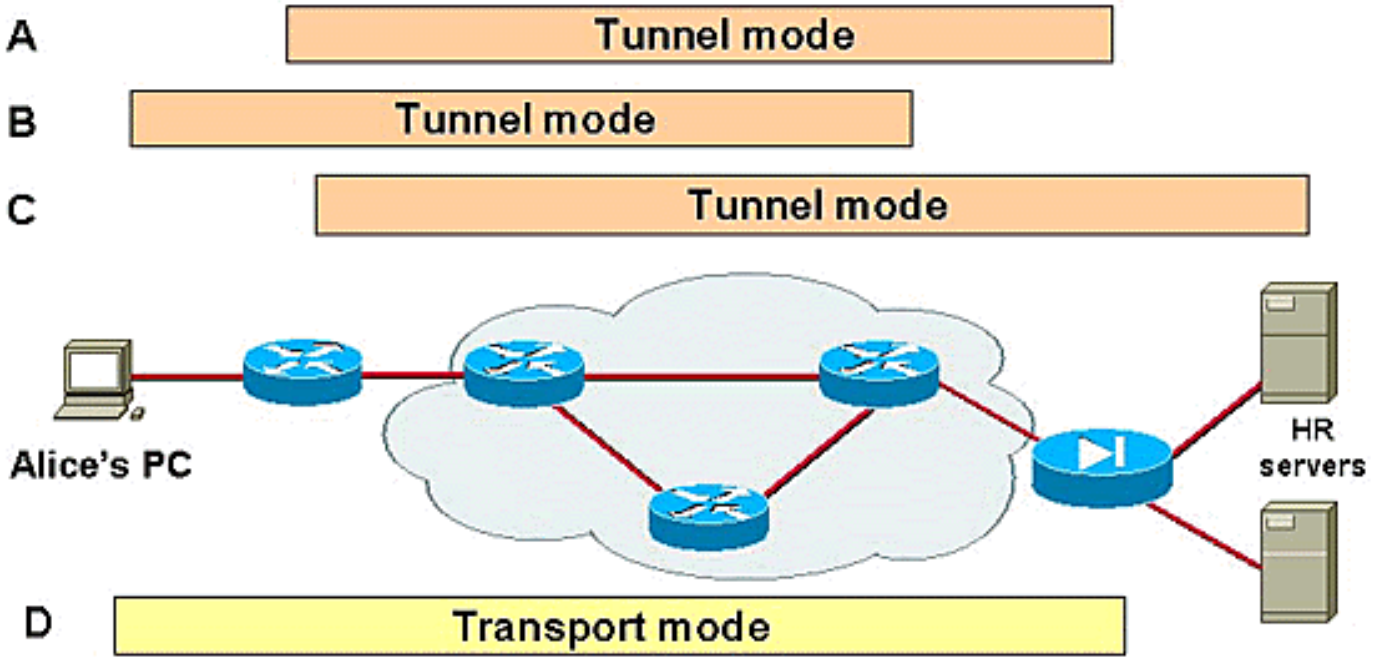


IPSEC IN ESP TUNNELING MODE

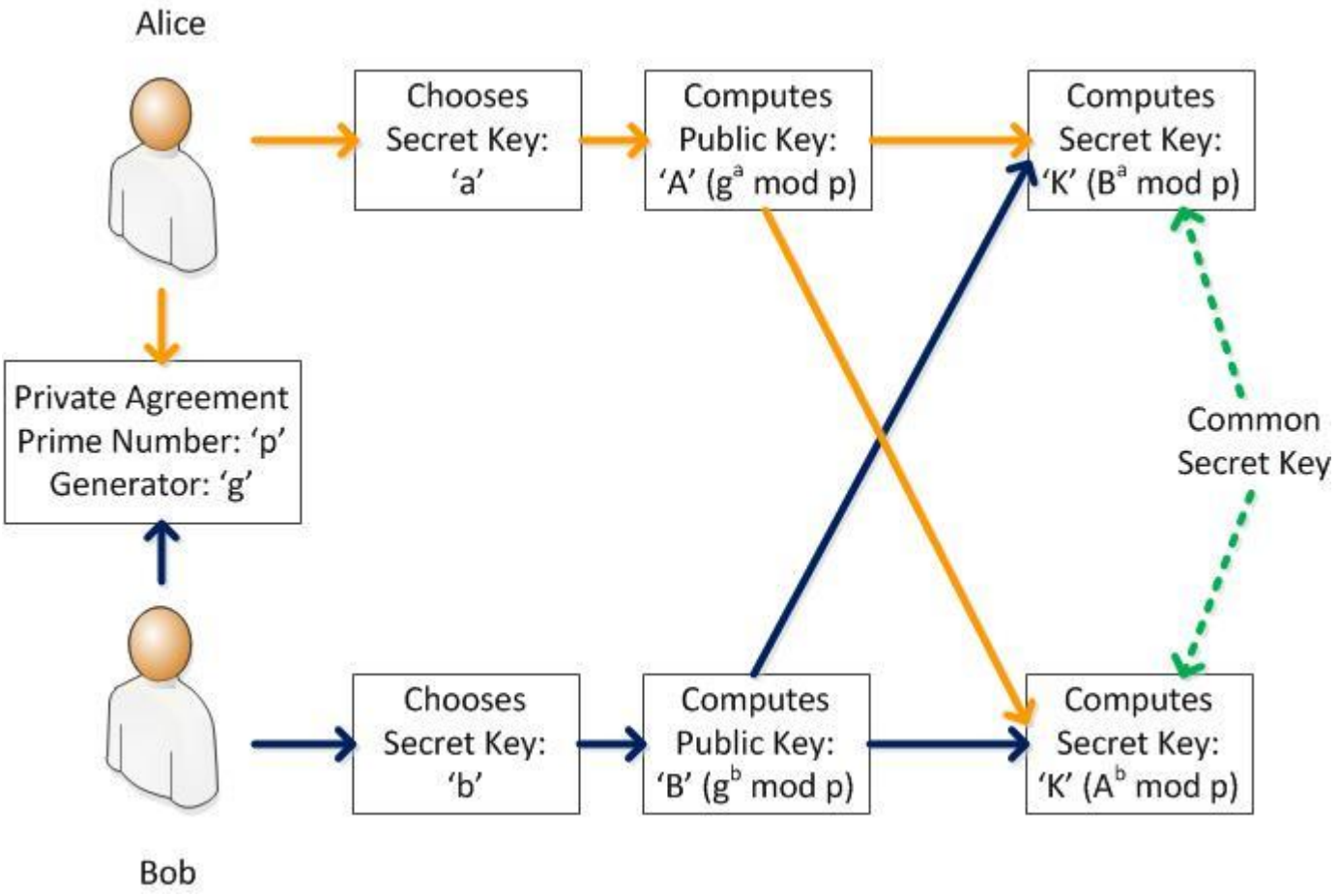


NORTHFORGE

TRANSPORT VS. TUNNEL MODE



INTERNET KEY EXCHANGE PROTOCOL (IKEV2) - DIFFIE HELLMAN ALGORITHM



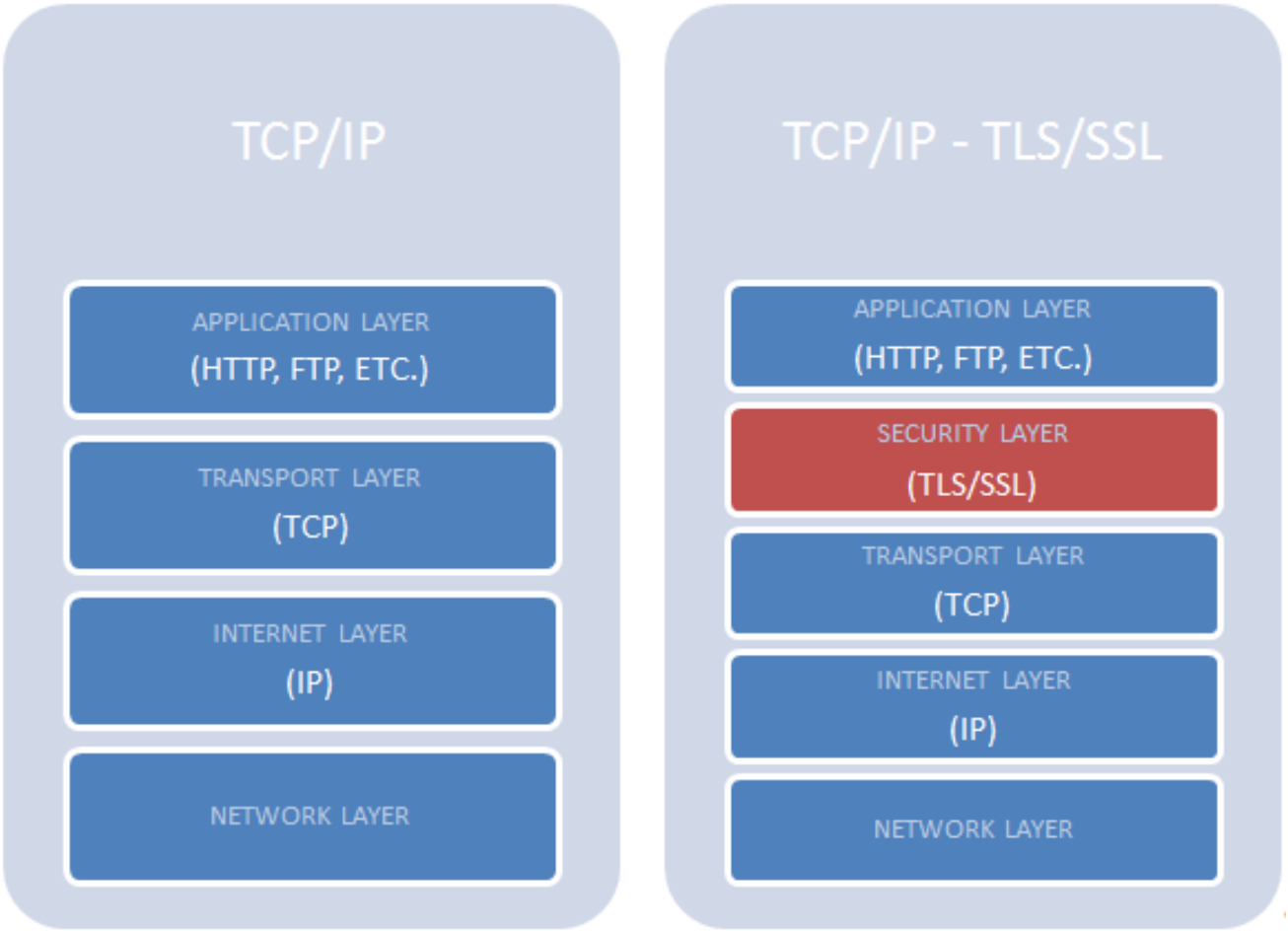
NORTHFORGE

SSL/TLS

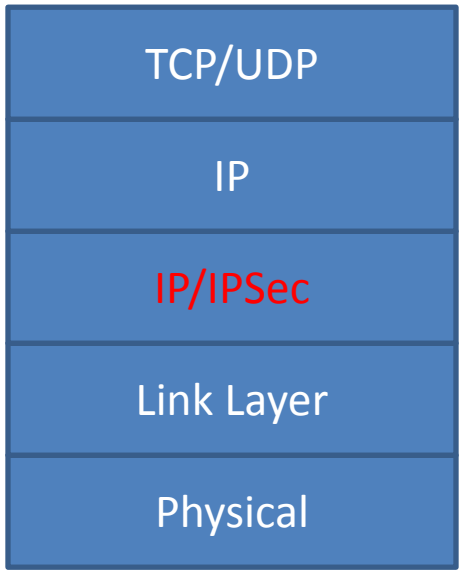
- SSL: Secure Sockets Layer (v2.0, v3.0)
  - Initializes handshakes to exchange key and information right away
  - Needs separate port number (HTTPS on port 443, LDAPS on port 636, IMAPS on port 993, instead of 80, 389, 143 respectively)

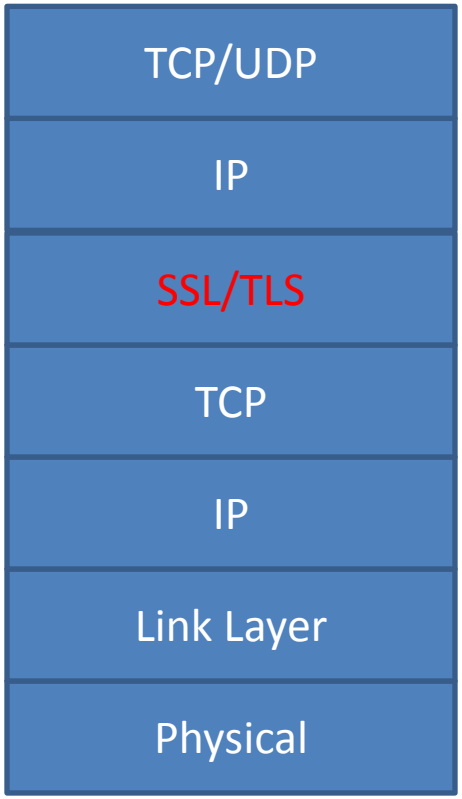
- TLS: Transport Layer Security (v1.1, v1.2)
  - Successor of SSL
  - Use the same port as the unsecured protocols

SSL/TLS IN THE PROTOCOL STACK



IPSEC OR SSL/TLS FROM VPN'S POINT OF VIEW





NORTHFORGE

IPSEC OR SSL/TLS FROM VPN'S POINT OF VIEW

IPsec

- Needs to be implemented at the kernel level
  -> applications using IPsec are not easily portable
- Can be deployed and easily used with other protocols such as IPComp (compression)
- Favored by standard bodies such as 3GPP

SSL/TLS

- Implementation does not need to be in the kernel
- Applications are easily portable