Lecture 13: WPA2 & IP Security

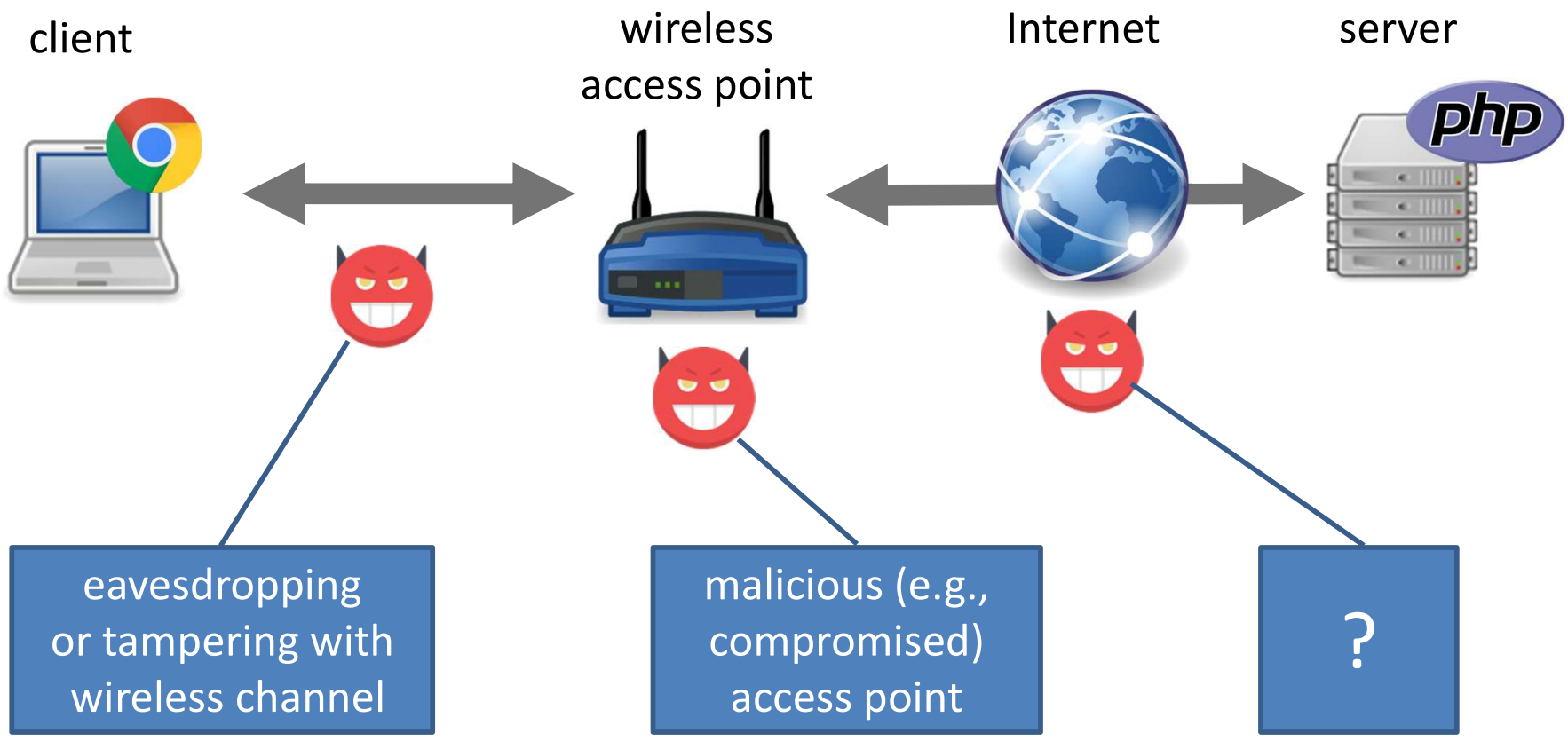
Stephen Huang

Content

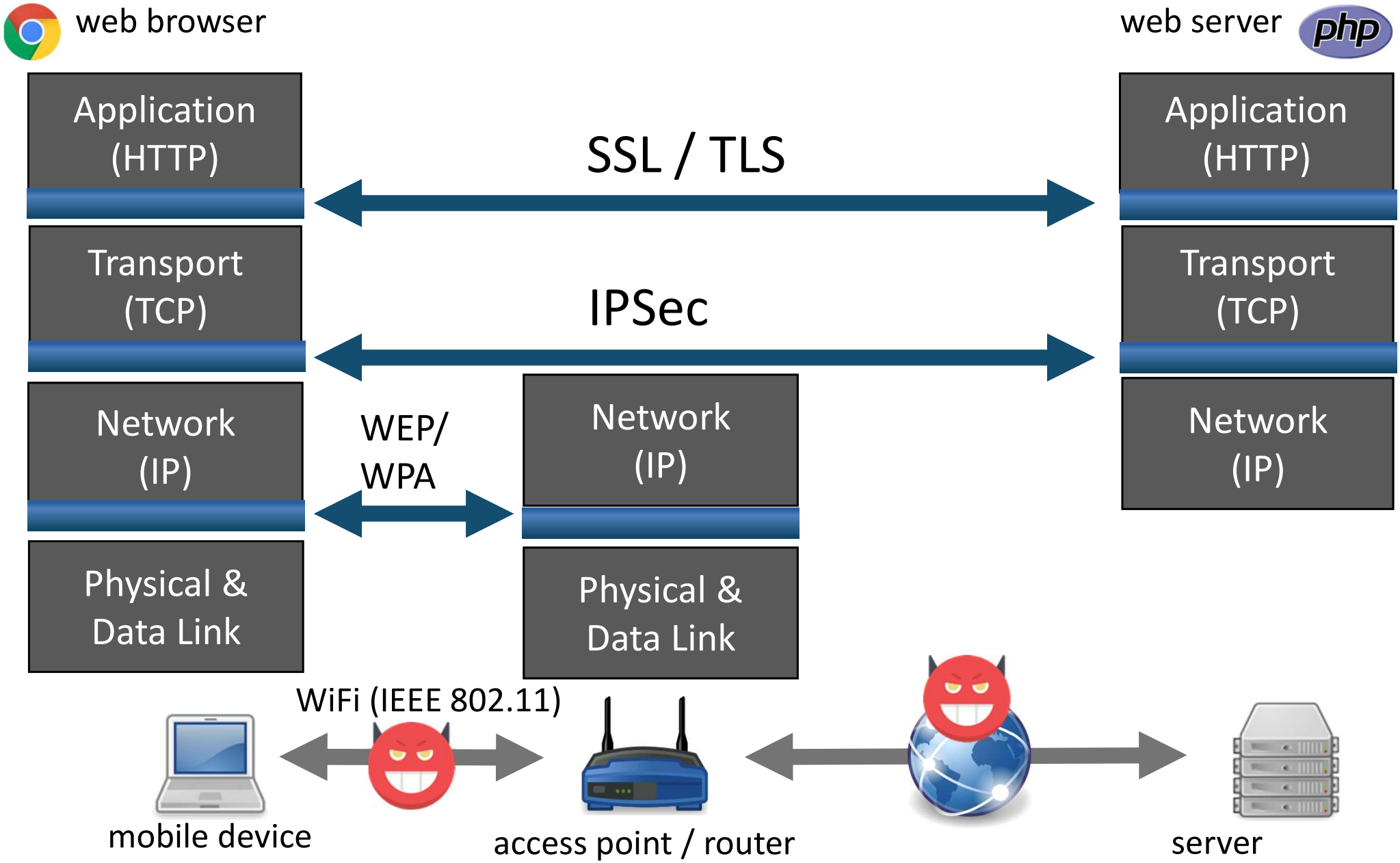
1. WiFi security: WPA2 and WPA3
   - WPA: WiFi Protected Access
2. IPSec
3. IPv4 Basics

Review

- Communication Threats in Practice



Review

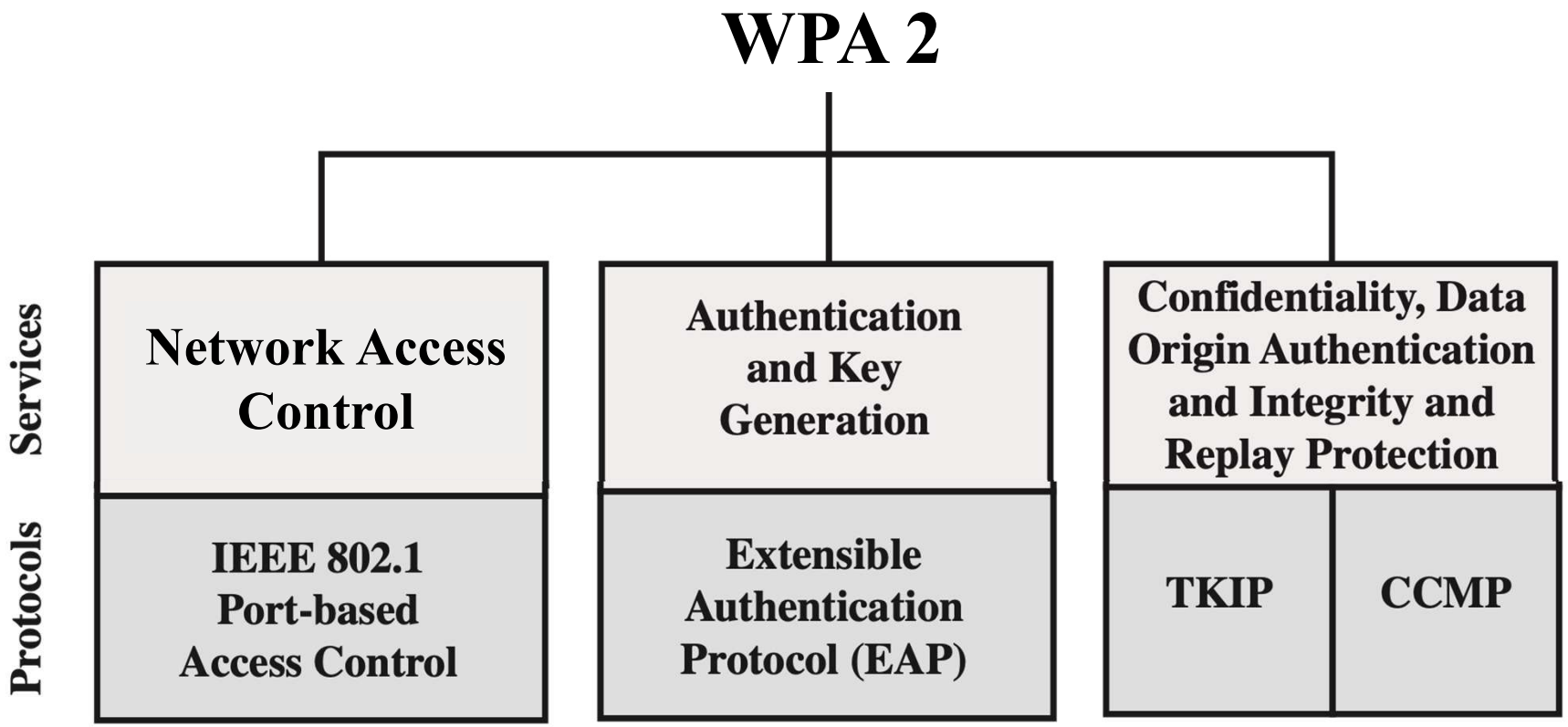

web browser
web server
Application (HTTP)
SSL / TLS
Application (HTTP)
Transport (TCP)
IPSec
Transport (TCP)
Network (IP)
WEP/ WPA
Network (IP)
Network (IP)
Physical & Data Link
Physical & Data Link
WiFi (IEEE 802.11)
mobile device
access point / router
server

IEEE 802.11 Security Standards

- WEP (Wired Equivalent Privacy)
  - introduced in 1997 as part of the original 802.11 standard
  - shown to be insecure in 2001
- WPA (WiFi Protected Access)
  - introduced in 2003, as a quick fix to WEP
  - subset of draft IEEE 802.11i
- WPA-2 (IEEE 802.11i)
  - standardized in 2004

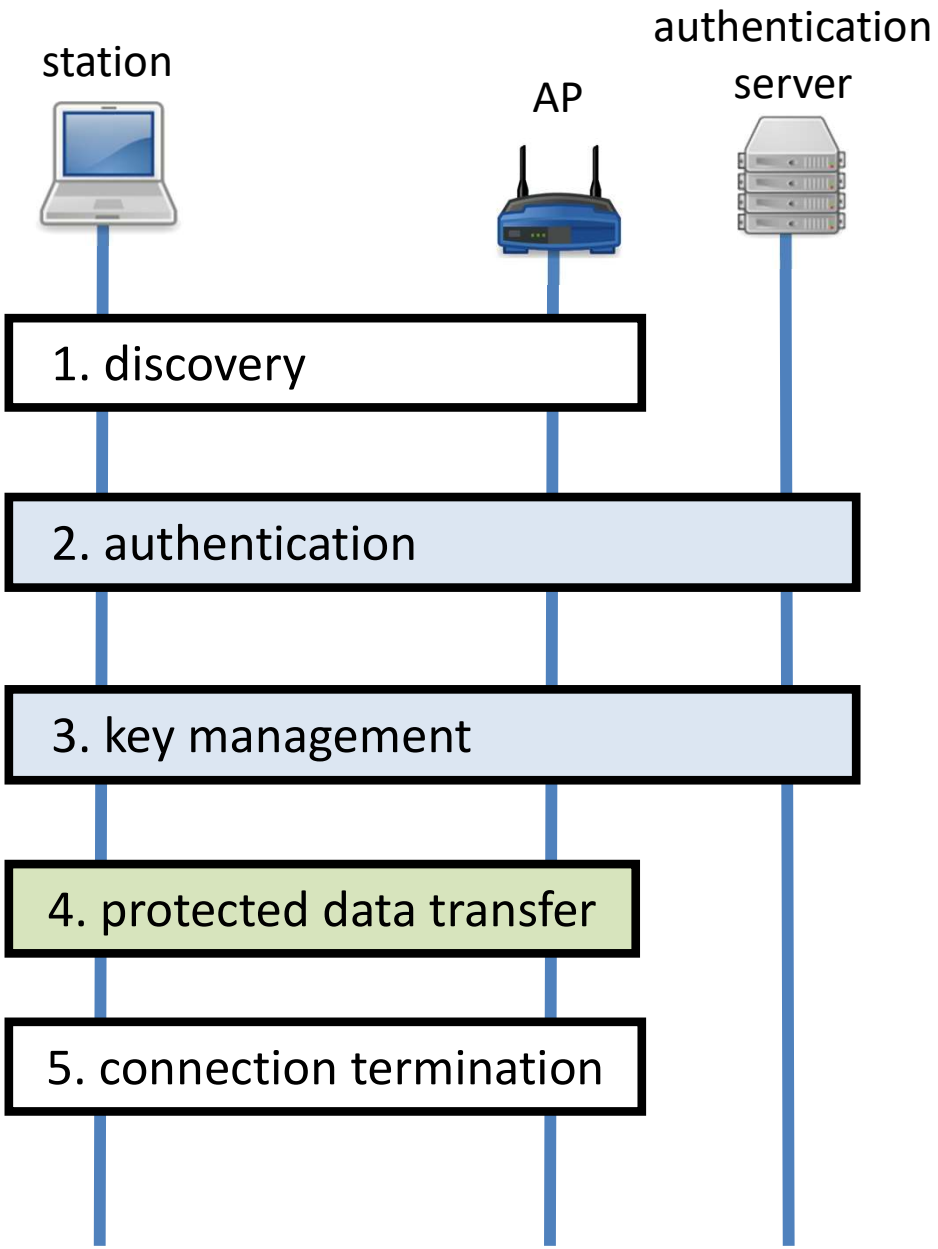
1. WiFi Security: WPA2

- Standard: IEEE 802.11i
  - WPA 2 devices can be certified by the Wi-Fi Alliance



Phases

1. Discovery
   - agree on what authentication method and ciphers to use
2. Authentication
   - may use an authentication server
   - create a pairwise master key
3. Key management
   - derive keys for various purposes
4. Protected data transfer
5. Connection termination



1.1 Discovery Phase

Goal: station and AP may support different authentication methods and ciphers → they need to agree on which ones they will use.

- Authentication and key-management suite: how to perform mutual authentication and derive fresh keys
  - IEEE 802.1X, pre-shared key (PSK), or vendor-specific
- Cipher suite: what ciphers to use for confidentiality and integrity
  - WEP, TKIP, CCMP, or vendor-specific
- Protocol
  - AP can periodically broadcast its security capabilities using a Beacon (or the station can ask for it using a Probe Request message)
  - Station specifies an authentication and cipher suite in an Association Request
  - if the AP accepts the specified suites, it sends an Association Response

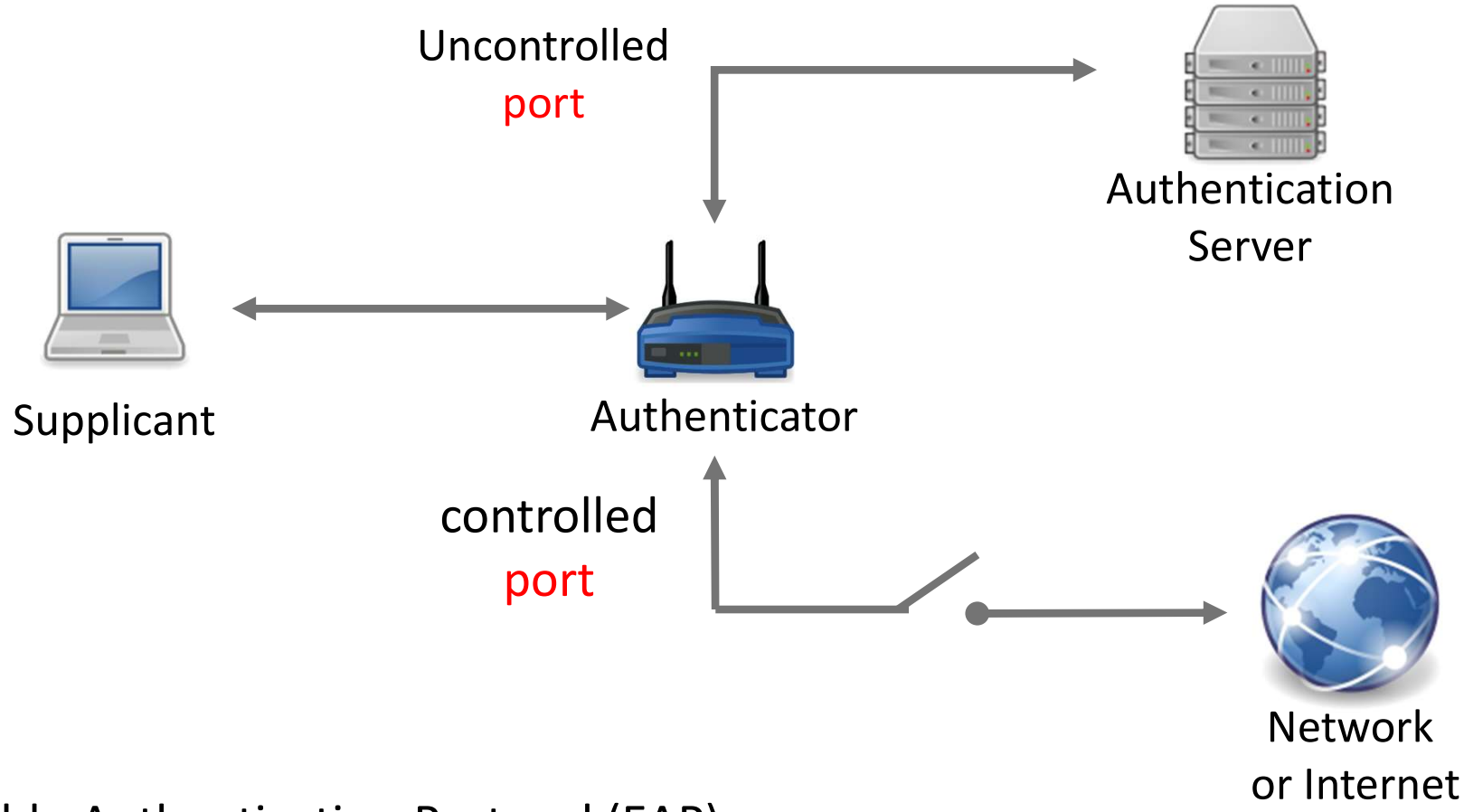
1.2 Authentication Phase

- Goals:
  - Mutual authentication:
    - Only authorized stations can use the network,
    - The station is assured that it communicates with a legitimate network
  - Generate a pairwise master key (PMK)
- Approaches
  - Pre-shared key (PSK)
    - Password is deployed on each station, and the AP manually
    - PMK = PSK = generated from the password using a hash function
    - Ideal for home and small office networks
  - IEEE 802.1X

Port-Based Access Control: IEEE 802.1X

- Standard for port-based network access control
- Entities
  - supplicant = station
  - authenticator = access point
  - authentication server
- Port-based: supplicant can access only the authentication server until the authentication succeeds
- Authentication server does not have to be implemented on the access point, little overhead for the access point.

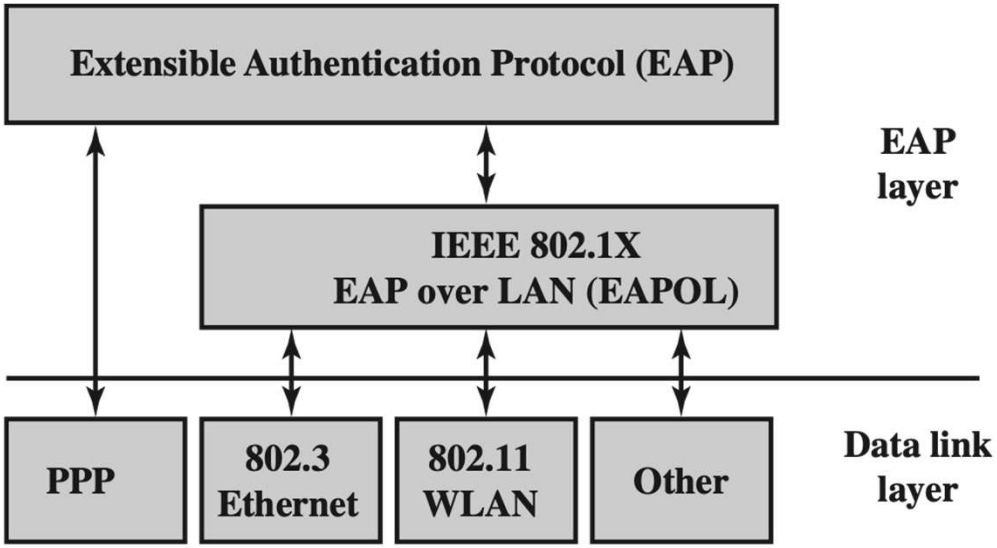
802.1X Access Control



The Extensible Authentication Protocol (EAP) specifies the structure of an authentication communication between a client and an authentication server

IEEE 802.1X and EAP

- *Reminder:*
  successful authentication enables access to a network and provides a fresh pairwise master key (PMK)
- IEEE 802.1X builds on IEEE 802 LAN (*e.g.*, WiFi or Ethernet)

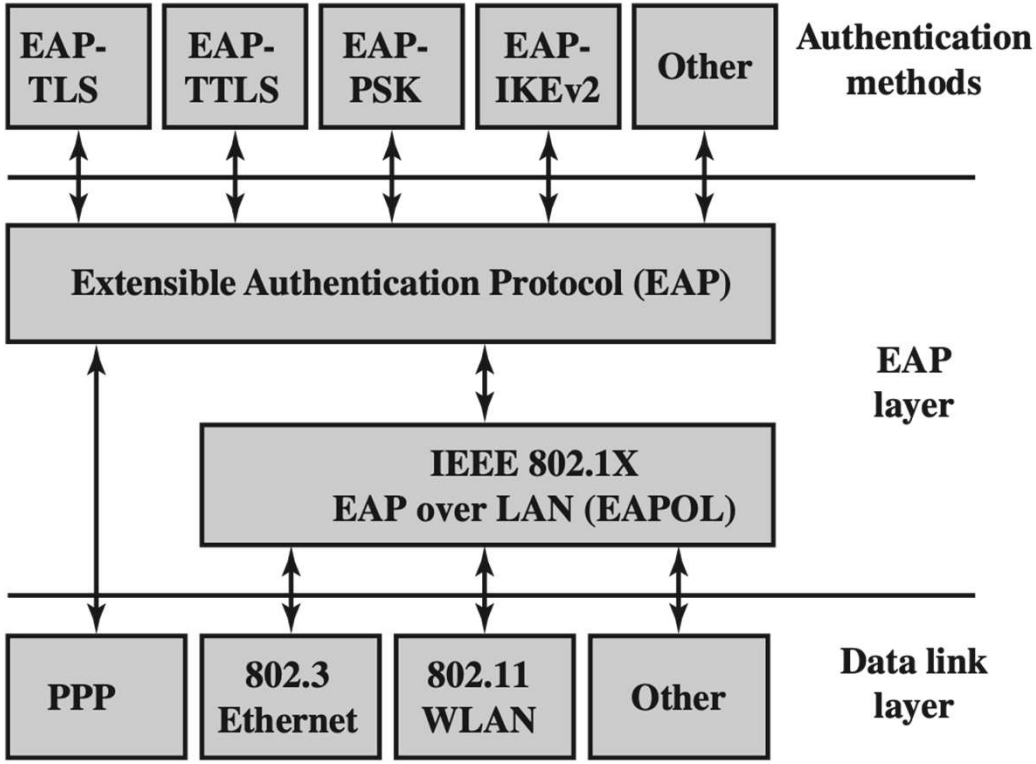


Point-to-Point Protocol (PPP) is a TCP/IP protocol that is used to connect one computer system to another.

- Authentication is performed using the Extensible Authentication Protocol (EAP)
  - EAPOL (EAP over LAN) protocol:
    enables the station to communicate with the authentication server

EAP Authentication Methods

- Extensible framework, not a specific authentication mechanism
- *Example methods*
  - EAP-TLS: based on public-key certificates
  - EAP-GPSK (Generalized Pre-Shared Key): based on secret keys shared by the client and the server, uses symmetric-key cryptography
  - …

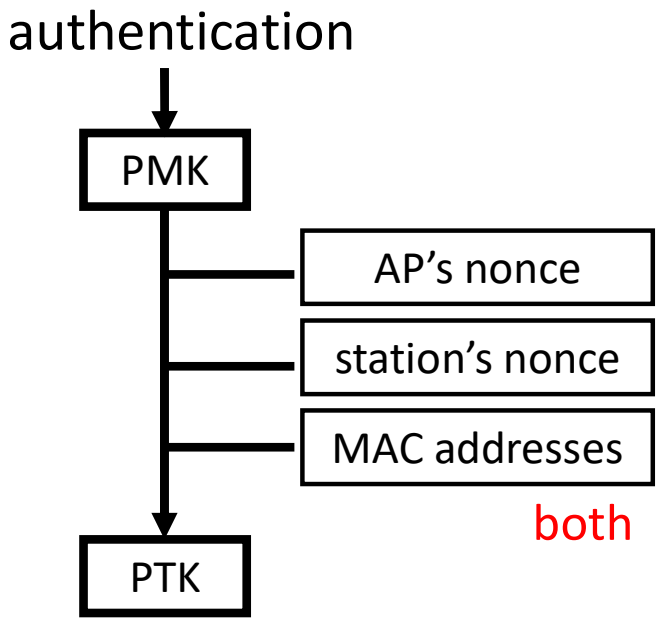


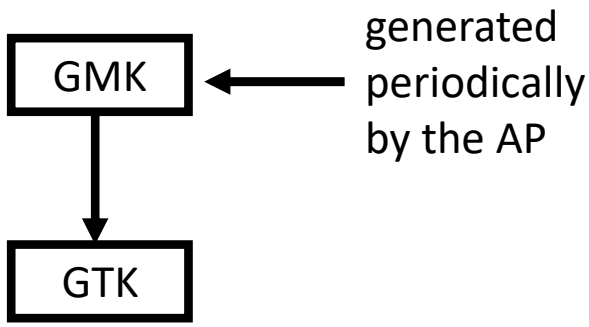
1.3 Key-Management Phase

Goals:

- derive pairwise transient keys from the Pairwise Master Key (PMK)
- distribute group keys

- Pairwise Transient Key (PTK)
  - protecting data between the station and AP
  - generated from PMK and the AP's and station's MAC addresses and nonces
- Group Temporal Key (GTK)
  - protecting multicast communication
  - group master key (GMK): generated randomly by the AP
  - distributed using the PTK





1.4 Protected Data Transfer Phase

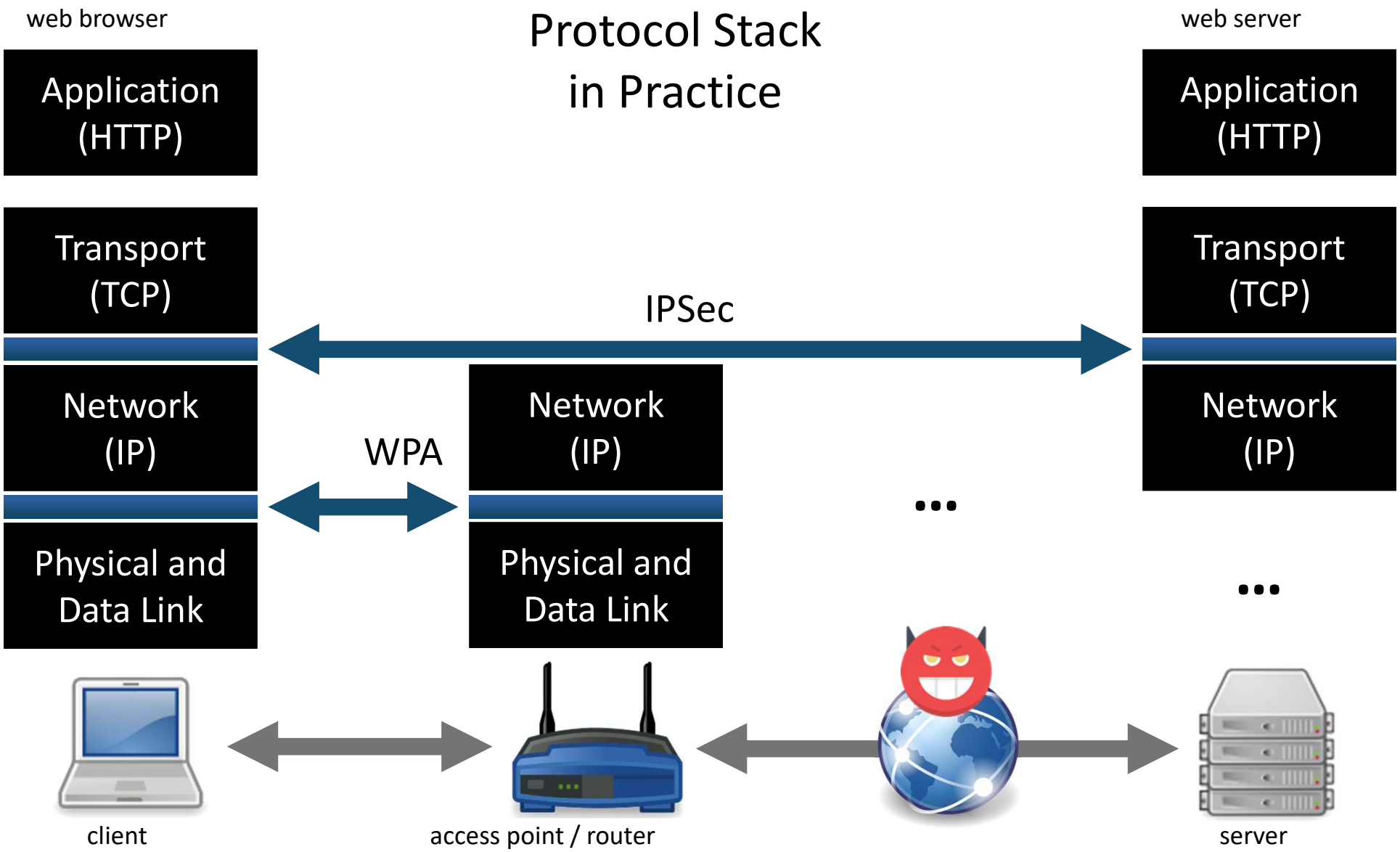
Standard defines two schemes: TKIP and CCMP

- TKIP (Temporal Key Integrity Protocol): same as WPA (Wi-Fi Protected Access)
- CCMP (Counter mode CBC-MAC Protocol)
  - based on the CCM (Counter with CBC-MAC) authenticated encryption mode
  - integrity: CBC-MAC based on AES encryption
  - confidentiality: AES encryption in counter (CTR) mode
  - same 128-bit key for integrity and confidentiality (from PTK)
  - 48-bit packet number to prevent replay attacks

IEEE 802.11i Conclusion

- Terminology
  - WPA ≈ subset of draft IEEE 802.11i (2003), deprecated
  - WPA 2 ≈ "full" IEEE 802.11i (2004)
  - WPA 3 (2018)
- Security: WPA 2 is generally secure with secure EAP methods, secure passwords, and CCMP
  - may be configured to be insecure, *e.g.*, weak pre-shared keys or WiFi Protected Setup (WPS)
- WPA 3 improvements
  - new algorithms (AES-256 in GCM mode, SHA-384 as HMAC)
  - replaces PSK with Simultaneous Authentication of Equals

2. IPSec

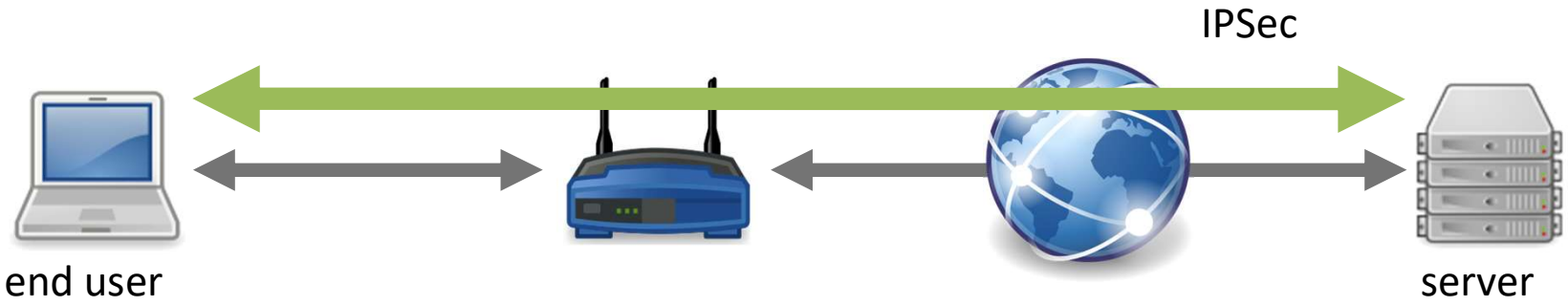

web browser
Protocol Stack
in Practice
web server
Application
(HTTP)
Application
(HTTP)
Transport
(TCP)
Transport
(TCP)
IPSec
Network
(IP)
WPA
Network
(IP)
Network
(IP)
Physical and
Data Link
Physical and
Data Link
client
access point / router
server

Internet Protocol Security (IPSec)

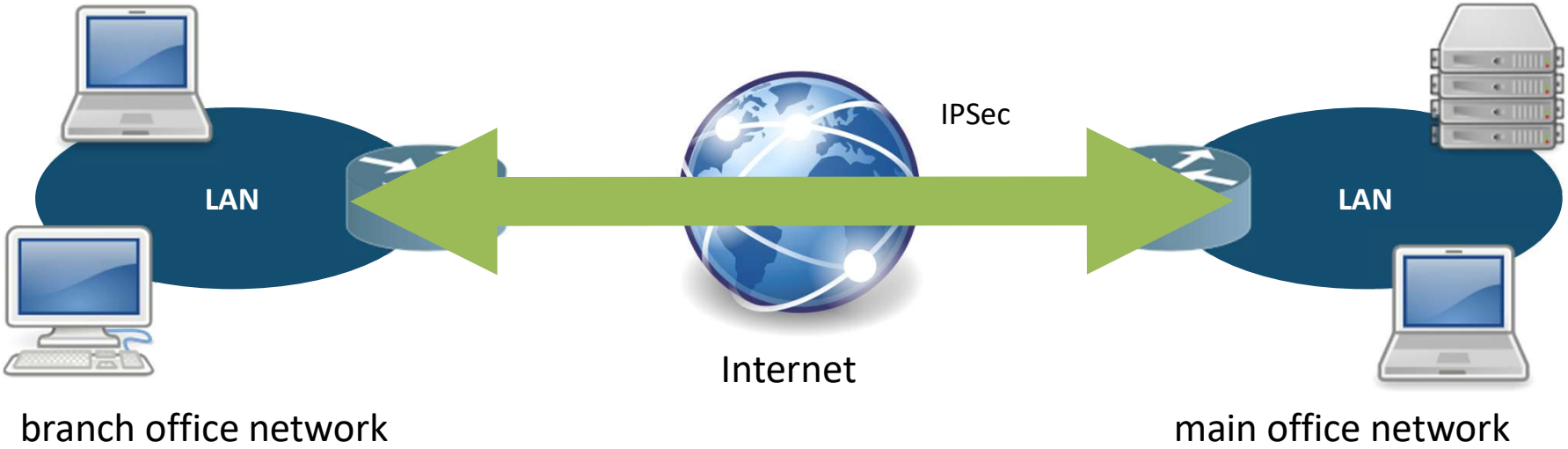
- Collection of protocols and mechanisms standardized by the Internet Engineering Task Force (IETF) in a series of publications.
- IPSec was a mandatory part of IPv6 (it is now optional)
  - optional to use with IPv4.
- Provides
  - data confidentiality and integrity (**encryption**)
  - source **authentication** (prevent address spoofing, i.e., sending from a fake address).
  - protection against packet replay.
- Below the transport layer (TCP or UDP) → transparent to applications.
- End-to-end security between two hosts, a host and a network, or between two networks.

Example Applications of IPSec

- Secure remote access over the Internet



- Secure virtual private network

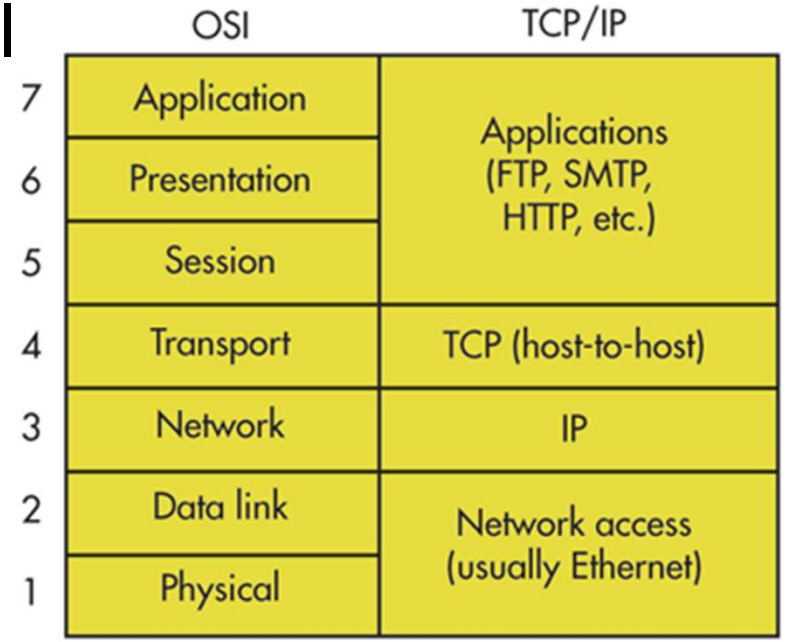


3. IPv4 Basics

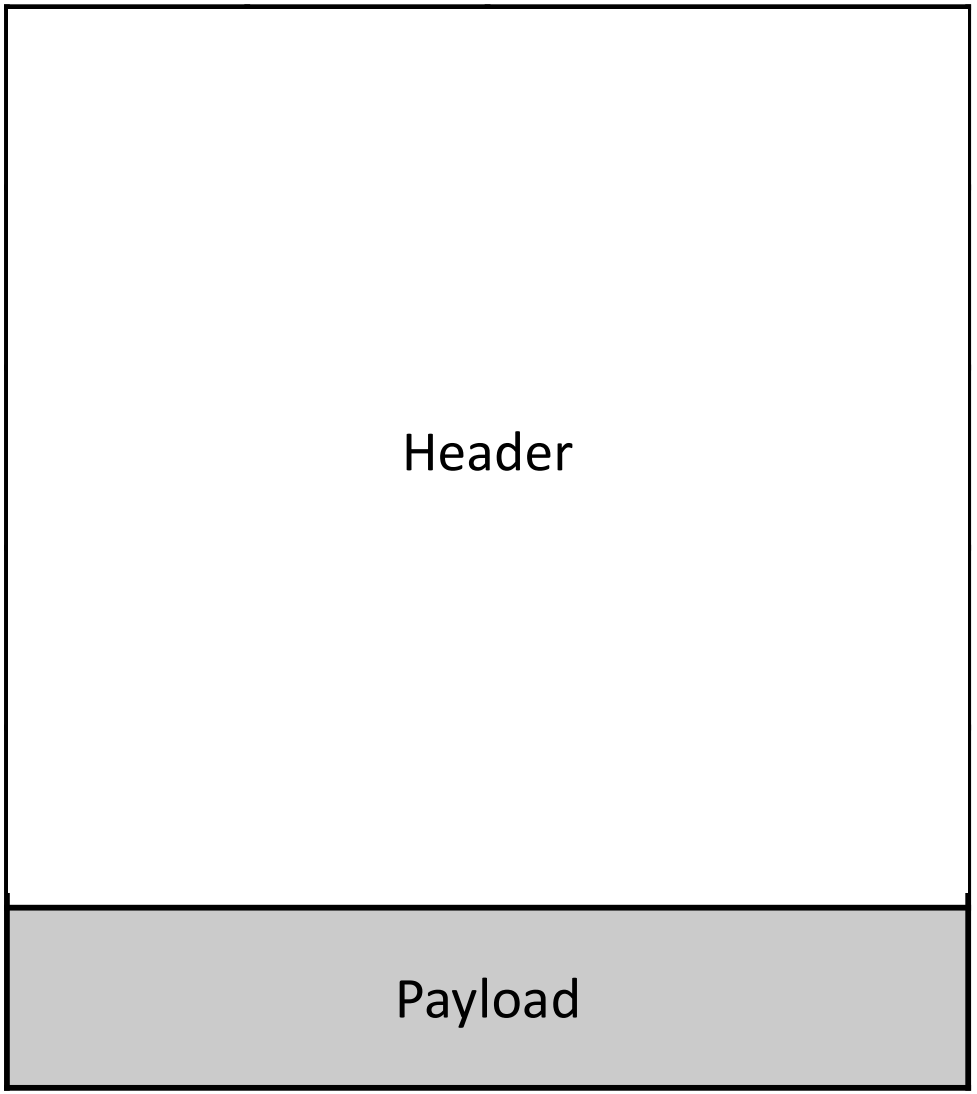
- Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP) and the first to be widely deployed.
  - IPv4 addresses are 32-bit integers that have to be expressed in Decimal, such as 189.123.10.123.
- IP version 6 is the new version, which is way better than IP version 4 in terms of complexity and efficiency.
  - IPv6 is written as a group of 8 hexadecimal numbers separated by colon (:). Example: `ABCD:EF01:2345:6789:ABCD:B201:5482:D023`.
  - IPSEC is an inbuilt security feature in the IPv6.

Reminder: TCP/IP

- Transmission Control Protocol (TCP) is a communications standard that enables application programs and computing devices to exchange messages over a network.
- The Internet Protocol (IP) is the method for sending data from one device to another across the internet.
- The four layers of the TCP/IP model
  - Datalink layer
  - Internet layer
  - Transport layer
  - Application layer

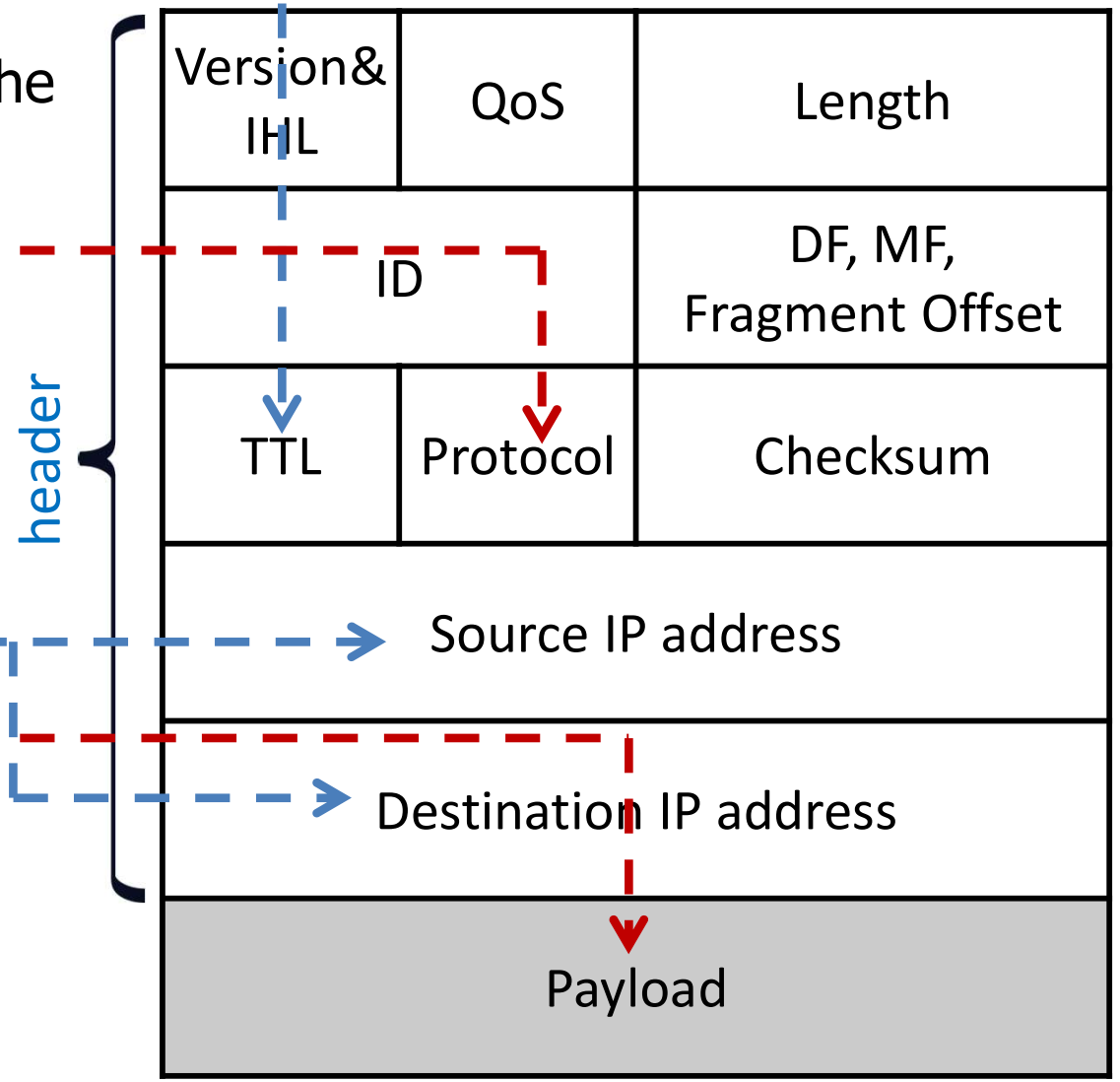


IPv4 Packet

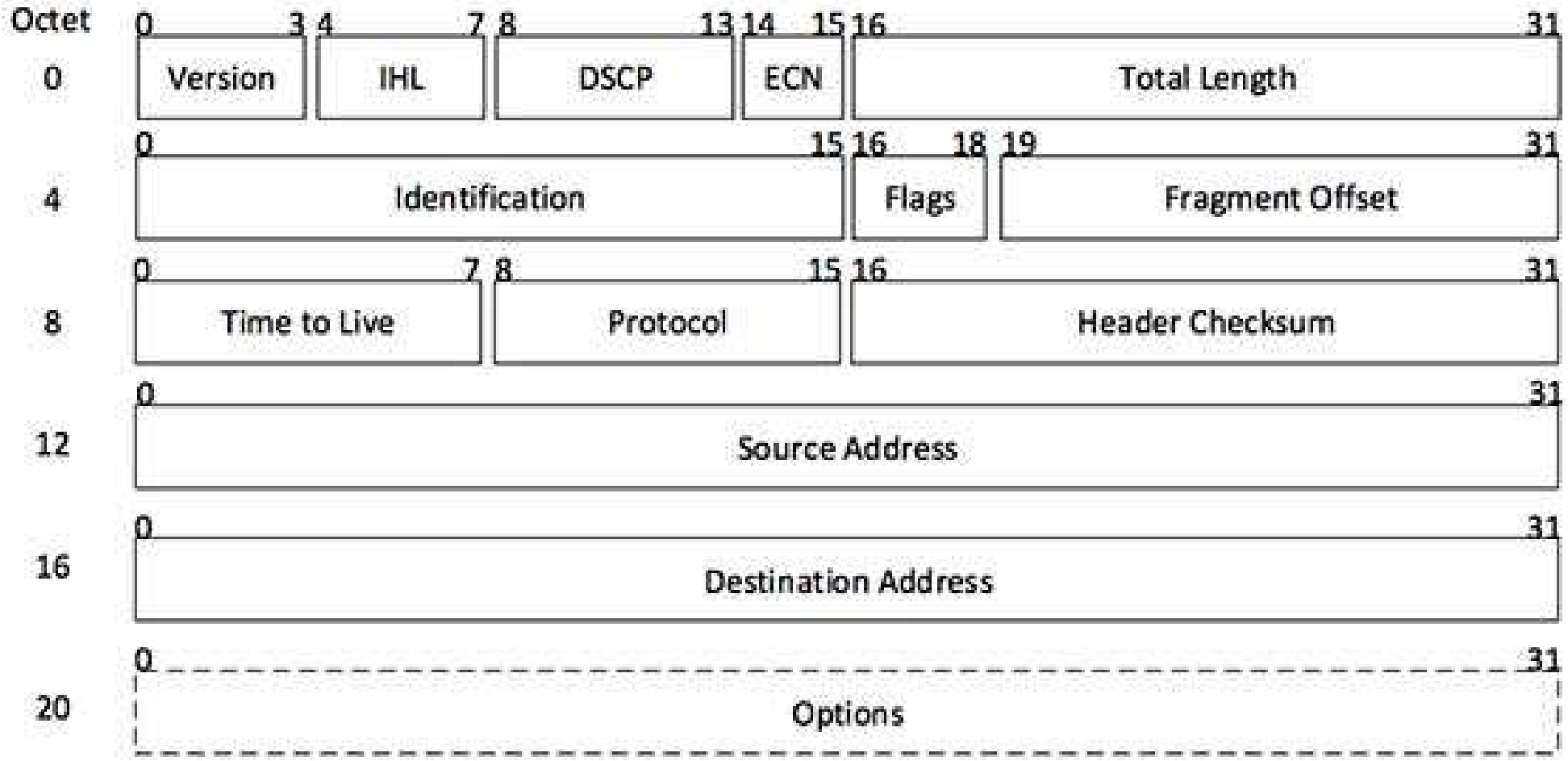


IPv4 Packet

- TTL: number of hops (i.e., intermediate nodes) that the packet is allowed to pass
- Protocol: identifies the higher-level protocol (*e.g.*, TCP, UDP)
- Source and destination IP: identifies the sender and recipient of the packet
- Payload: data from higher-level protocol

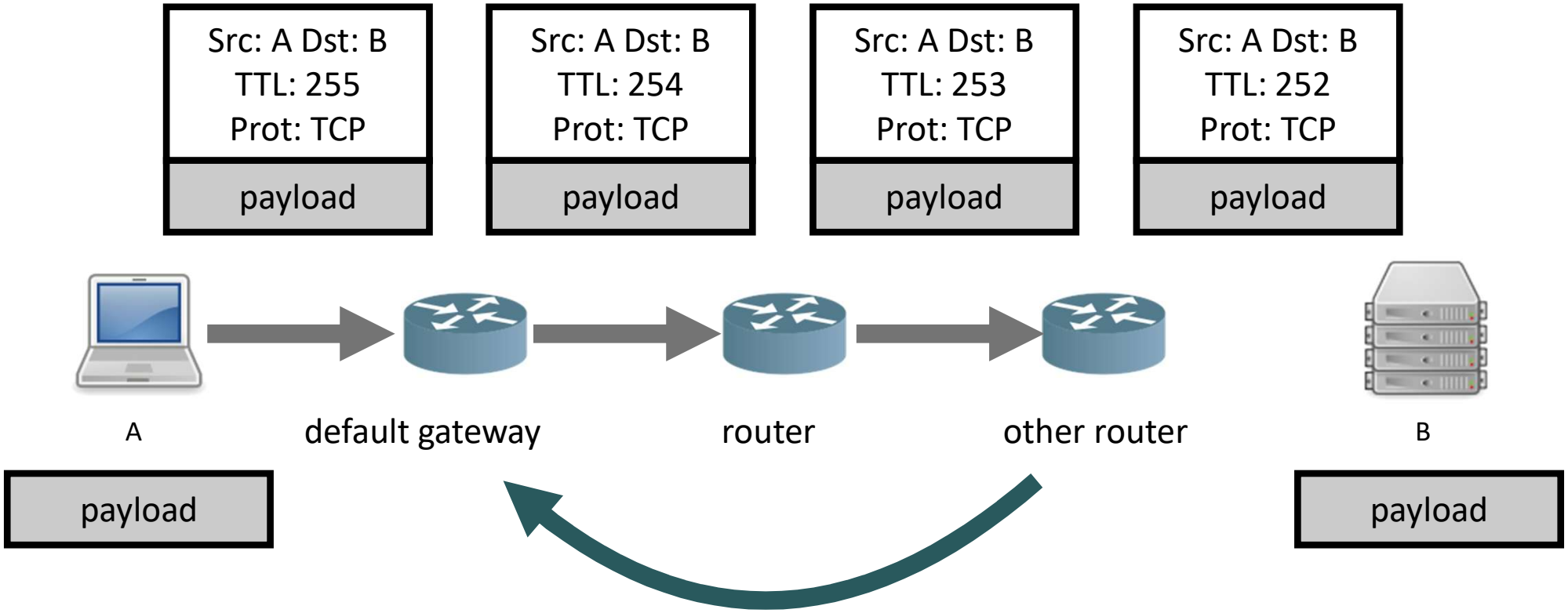


Detailed View



[Image: IP Header]

IP Packet Forwarding



- Challenges for security
  - some fields need to be read by intermediate nodes ↔ confidentiality
  - some fields need to be changed by intermediate nodes ↔ integrity

IP forwarding algorithm

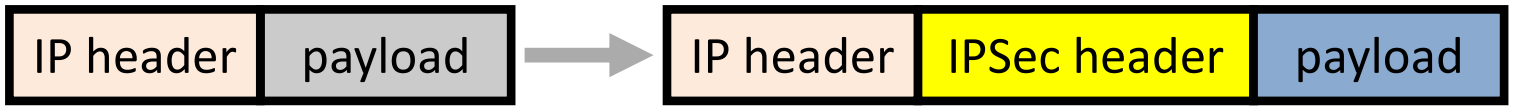
Given a destination IP address, D, and network prefix, N:

```
if (N matches a directly connected network address)
        Deliver datagram to D over that network link;
else if (The routing table contains a route for N)
        Send datagram to the next-hop address
        listed in the routing table;
else if (a default route exists)
        Send datagram to the default route;
else
        Send a forwarding error message to the
        originator;
```

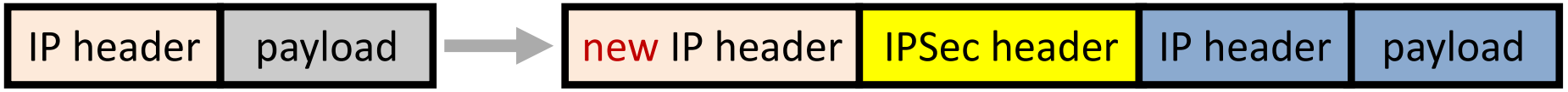
the entry with the longest subnet mask is chosen

IPSec Transport Mode and Tunnel Mode

- Transport mode
  - protects the payload of the IP packet
  - typically host-to-host communication

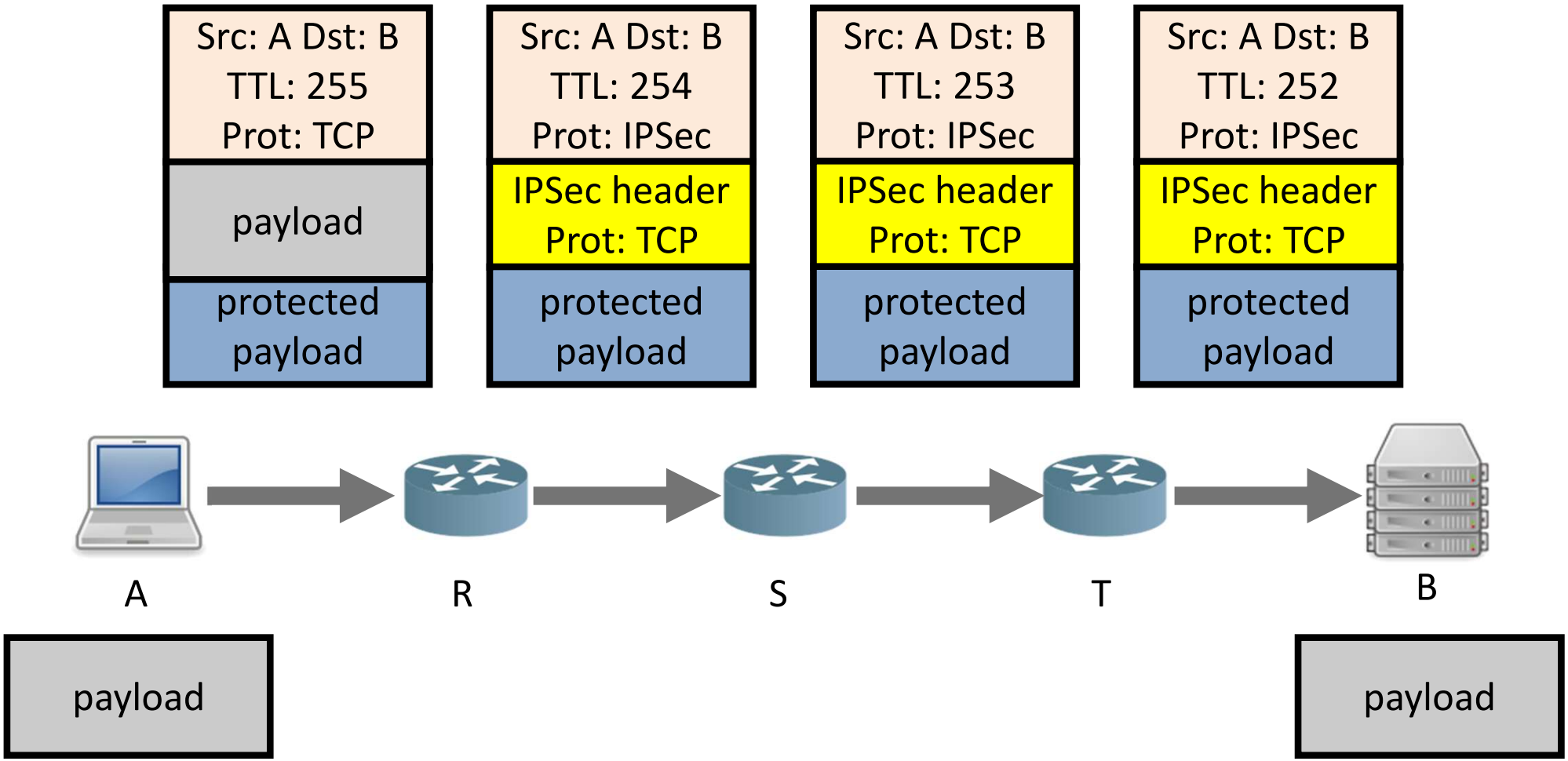


- Tunnel mode
  - protects the entire IP packet by encapsulating it in the payload of a new IP packet
  - typically host-to-network or network-to-network communication



Transport Mode Example

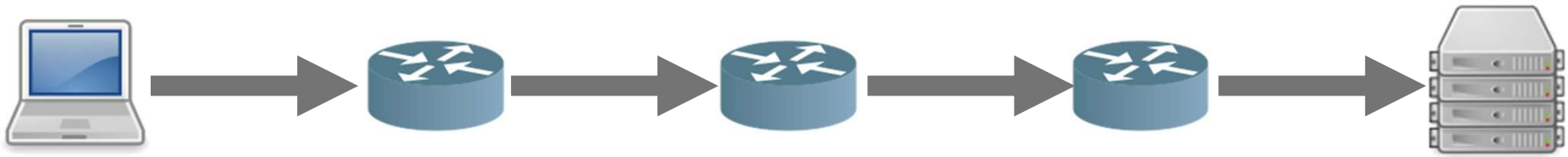
- Transport between A and B:



Tunnel Mode Example

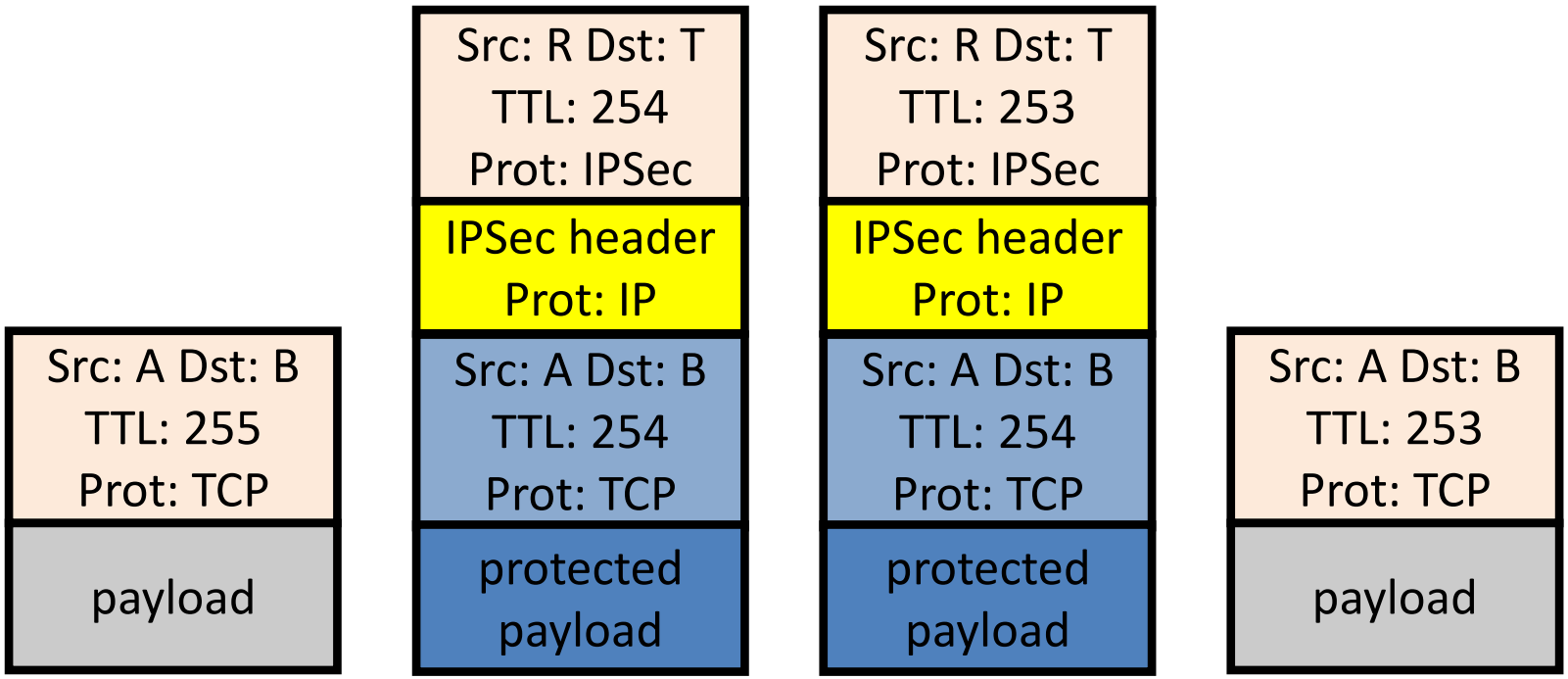
- Tunnel between A and B:

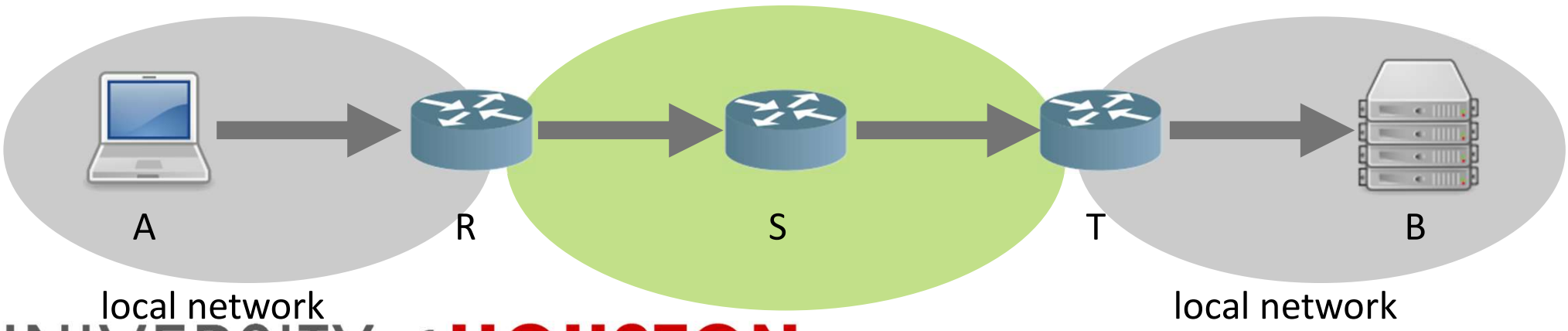
Src: A Dst: B TTL: 255 Prot: IPSec	Src: A Dst: B TTL: 254 Prot: IPSec	Src: A Dst: B TTL: 253 Prot: IPSec	Src: A Dst: B TTL: 252 Prot: IPSec
IPSec header Prot: IP	IPSec header Prot: IP	IPSec header Prot: IP	IPSec header Prot: IP
Src: A Dst: B TTL: 255 Prot: TCP	Src: A Dst: B TTL: 255 Prot: TCP	Src: A Dst: B TTL: 255 Prot: TCP	Src: A Dst: B TTL: 255 Prot: TCP
payload	protected payload	protected payload	protected payload



Tunnel Mode VPN Example

- Tunnel between R and T:





IPSec Protocols

	Protocol	
	Authentication Header (AH)	**Encapsulating Security Payloads (ESP)**
Modes	both transport and tunnel	
Provides	integrity, replay prevention	integrity, confidentiality, replay prevention
Protects	payload and IP header	payload

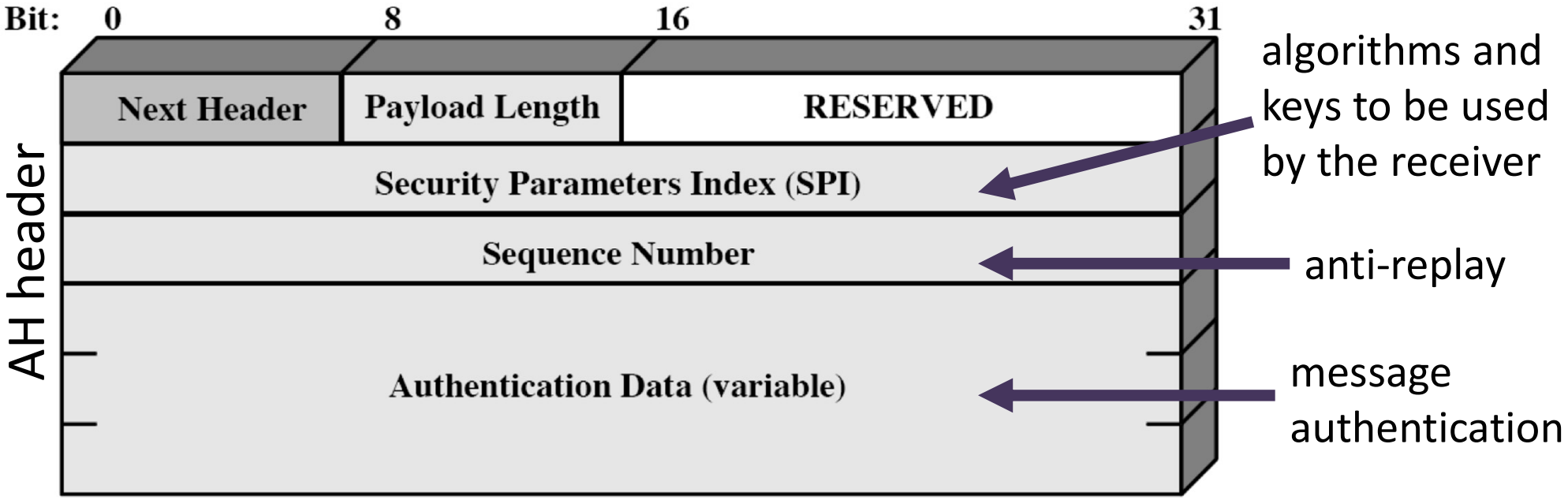
Authentication Header

- Services
  - data and origin integrity
  - replay-prevention
- Message authentication
  - computed from immutable fields of the IP header, AH header (except ICV), and original payload
  - algorithms: HMAC-MD5, HMAC-SHA-1, HMAC-SHA-2, …

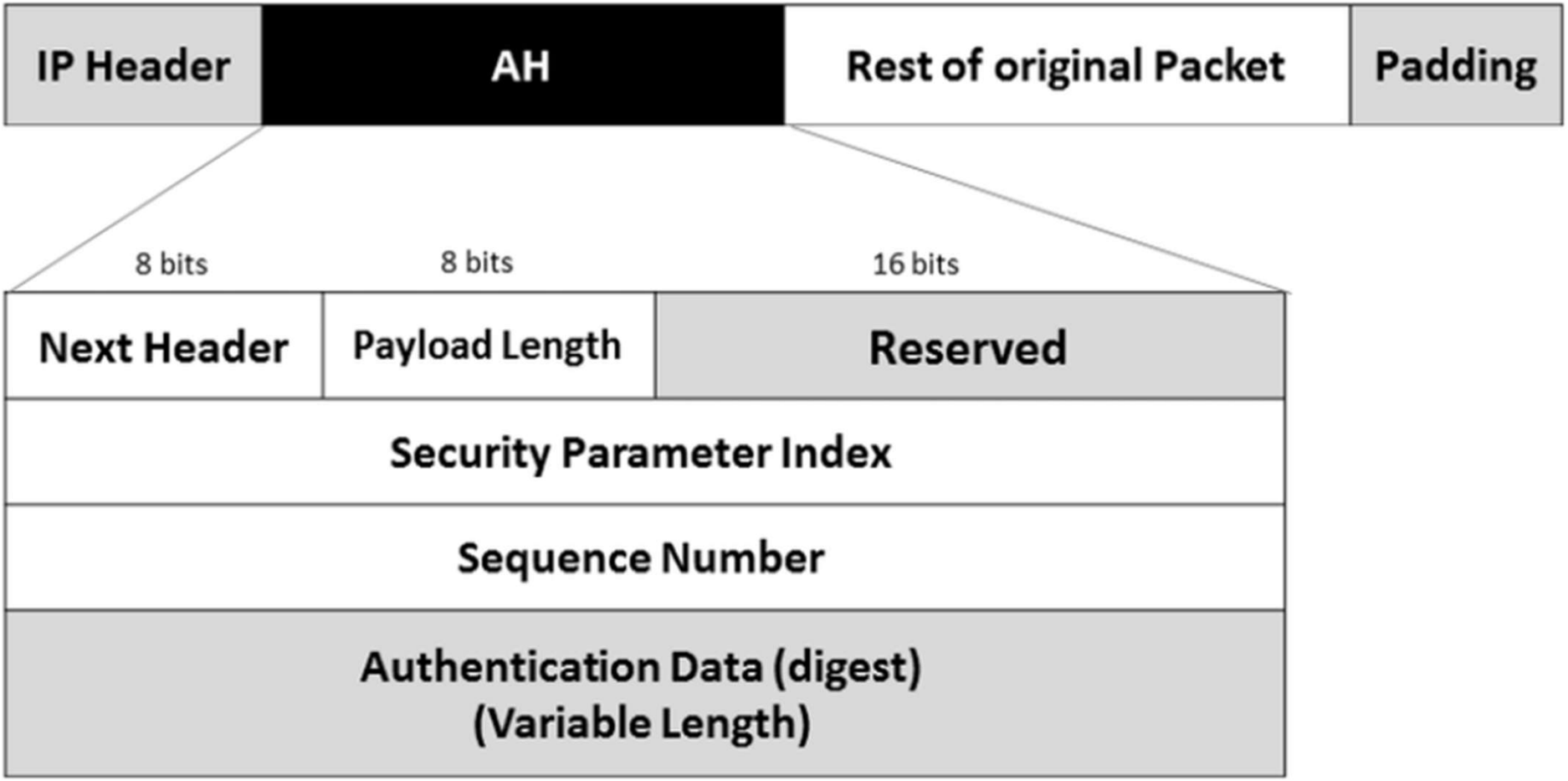
Authentication Header

Original IP packet

Version	QoS	Length
ID		DF, MF, Frag. Offset
TTL	Protocol	Checksum
Source IP address		
Destination IP address		
Payload		

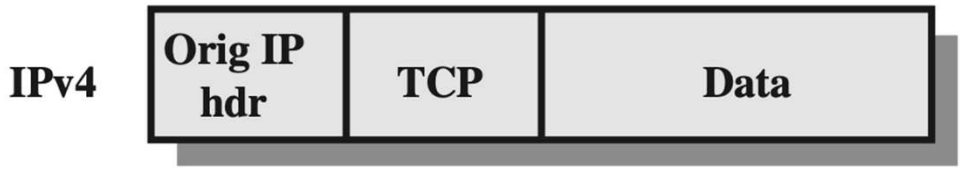


Authentication Header

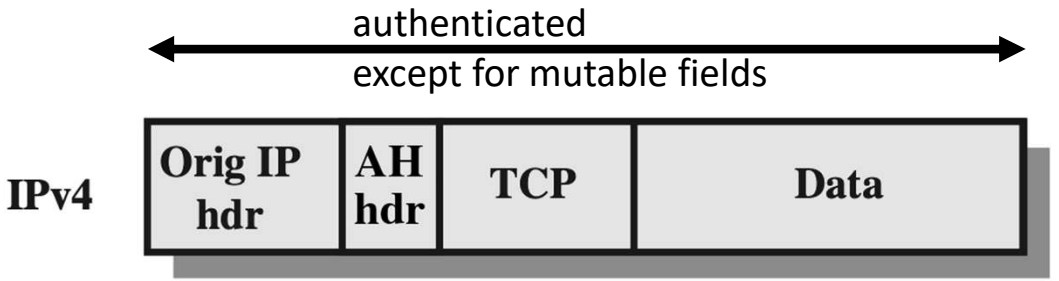


AH in Transport & Tunnel Modes

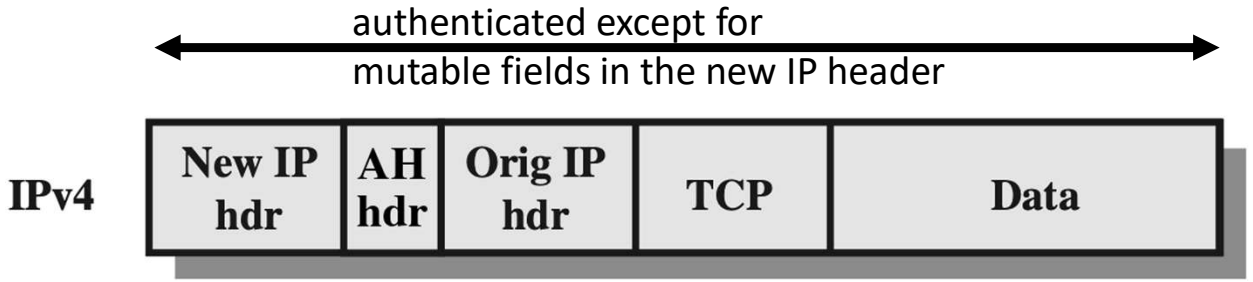
- Original IP Packet



- Transport Mode

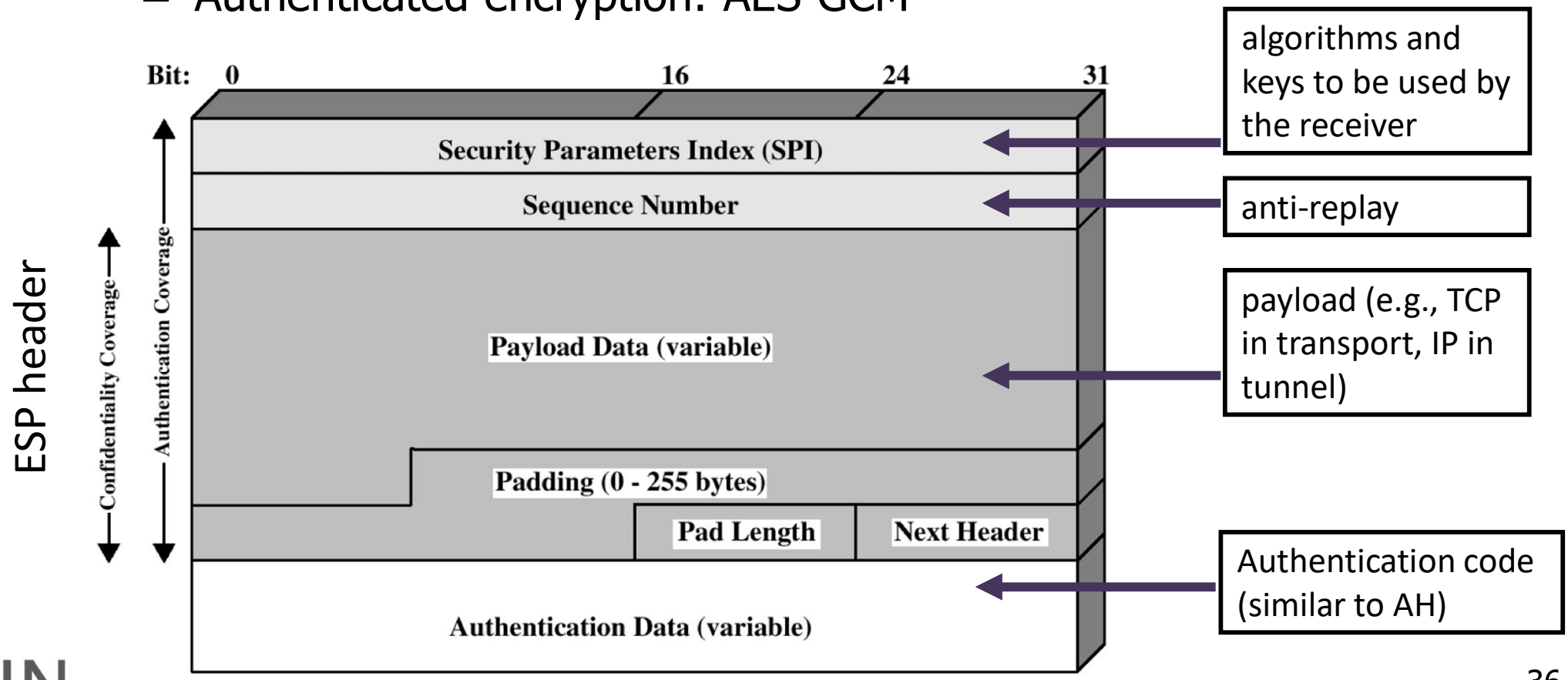


- Tunnel Mode



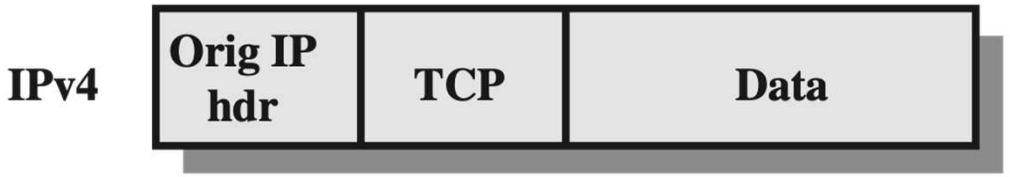
Encapsulating Security Payload

- Services: confidentiality, integrity (optional), replay prevention
  - Encryption: AES-CBC, 3DES-CBC, …
  - Message authentication: HMAC-SHA-1, AES-GMAC, …
  - Authenticated encryption: AES-GCM

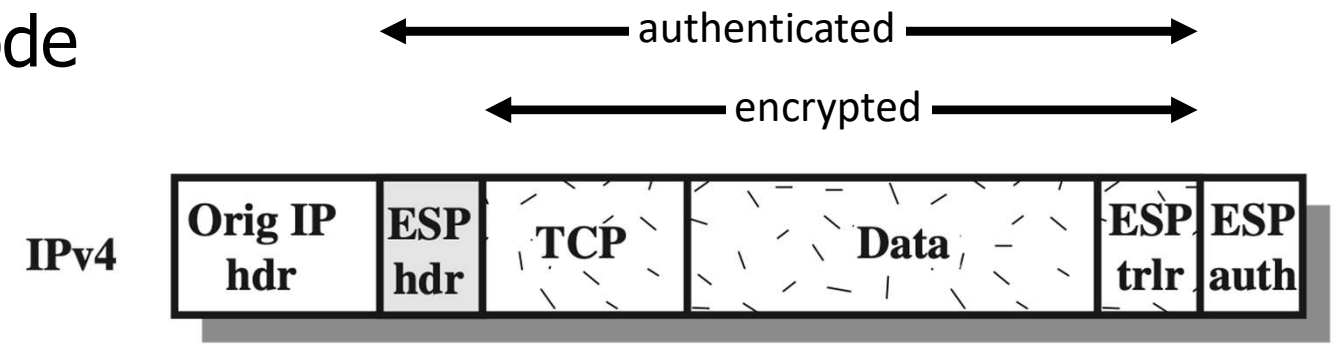


ESP in Transport & Tunnel Modes

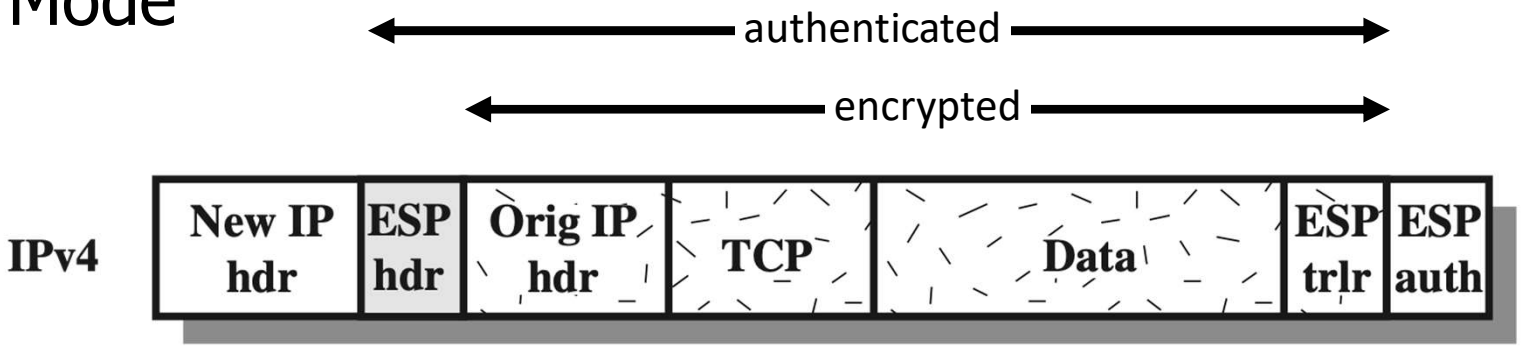
- Original IP Packet



- Transport Mode



- Tunnel Mode

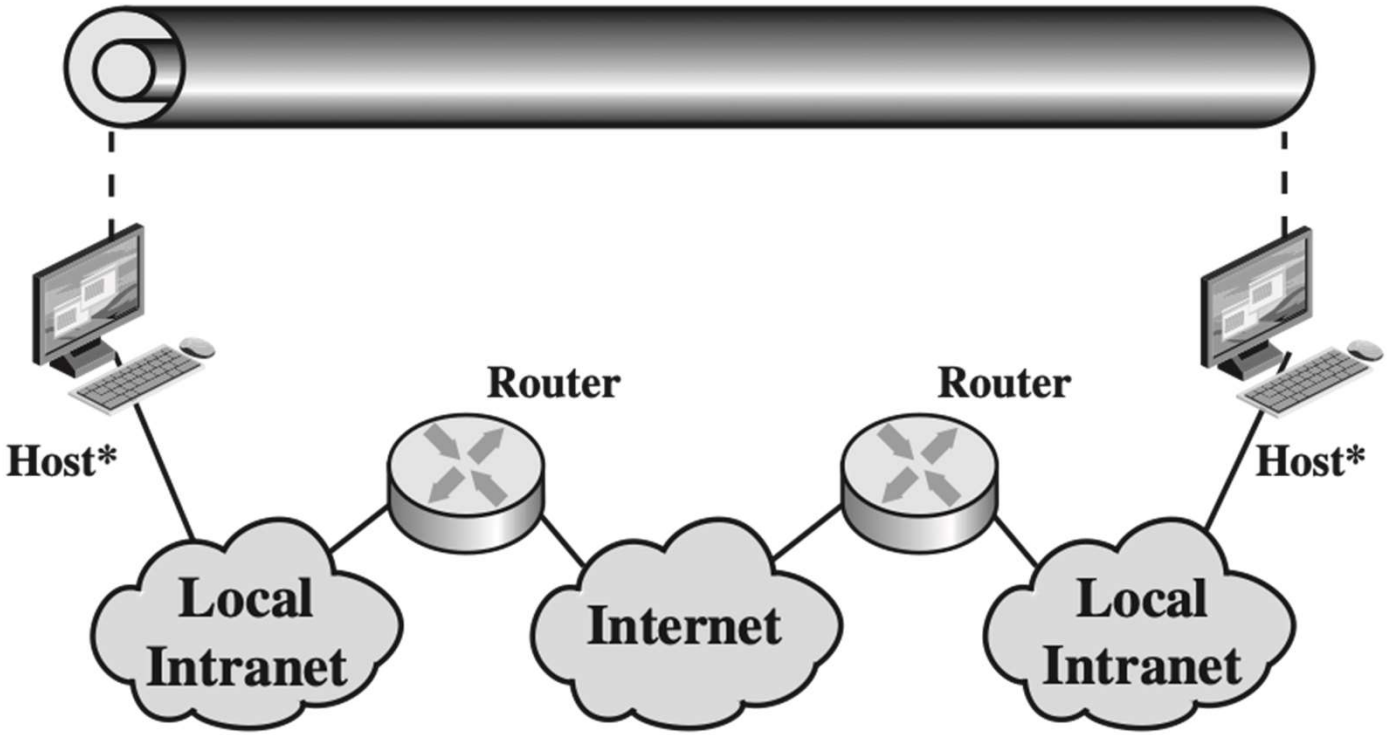


Combining Modes and Protocols

- Mode comparison
  - Tunnel: requires support only at the gateways, vs.
  - Transport: requires support only at the hosts
- Header comparison
  - AH: authenticates some elements of the original header, vs.
  - ESP: protects both integrity and confidentiality
- Combining modes
  - IPSec tunnel can carry any IP packet
    → IPSec transport or tunnel packets can be sent through an IPSec tunnel
  - IPSec transport can protect any IP packet
    → IPSec transport or tunnel packets can be protected by outer IPSec transport
  - may be nested to any depth

Combination Examples

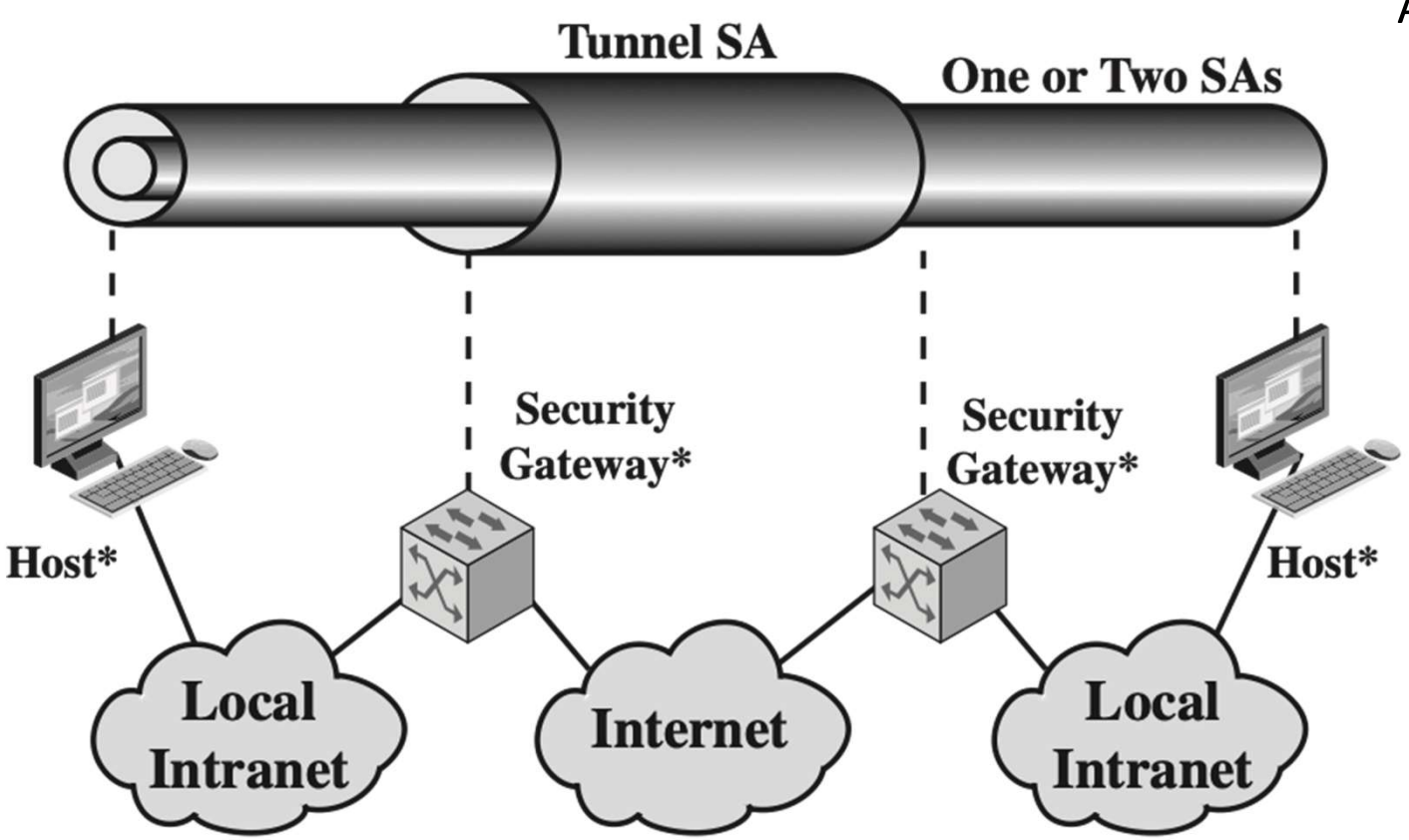
1. AH in transport (for integrity) + ESP in transport (for confidentiality)



Combination Examples

2. IPSec packets over tunnel

SA: Security Association



IPSec Conclusion

- Between network and transport layers (e.g., IP and TCP)
  - works over any IP network
  - transparent to applications
- Applications
  - host-to-host, host-to-network, network-to-network (VPN)
- Modes:
  - traffic and
  - tunnel
- Protocols:
  - Authentication Header and
  - Encapsulating Security Payload
- Provides confidentiality, integrity, source authentication, anti-replay

Next Topic

- IPSec
- Transport-Layer Security (SSL/TLS)