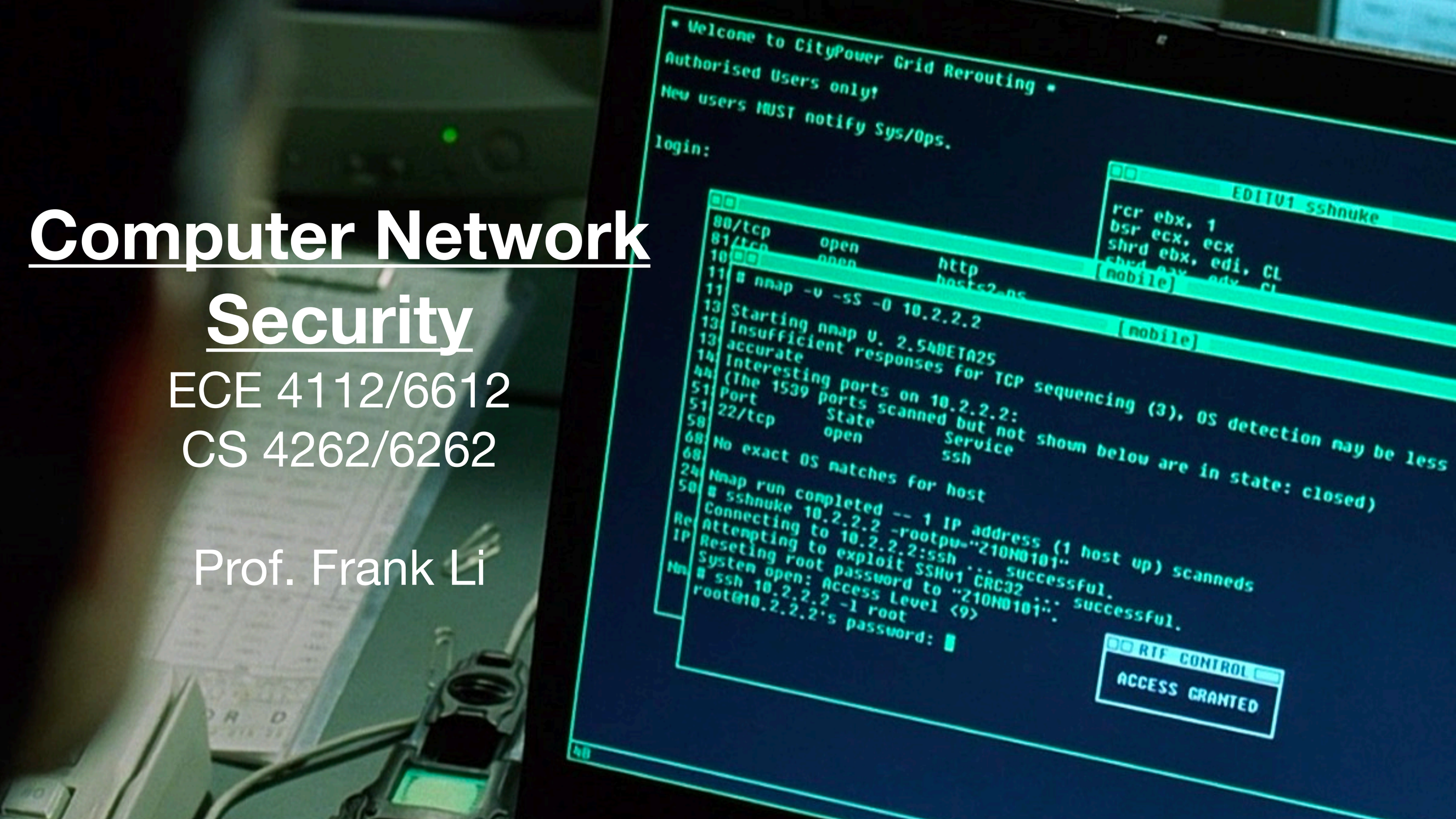
Computer Network Security

ECE 4112/6612
CS 4262/6262

Prof. Frank Li



Logistics

Date	Session Topic
Tue, Aug 22	Course Overview + Logistics
Thu, Aug 24	Network Protocols Overview
Tue, Aug 29	Cryptography: Symmetric Crypto
Thu, Aug 31	Cryptography: Hash + MACs
Tue, Sept 5	Cryptography: Public-Key Crypto
Thu, Sept 7	Link Layer: LAN + wireless security
Tue, Sept 12	Internet Layer: IP Security
Thu, Sept 14	Internet Layer: Routing / BGP Security
Tue, Sept 19	**Quiz 1**

Logistics

HW1 was due yesterday, solutions to be posted shortly

Who is turtle Tank?

Logistics

Project - Group Formation Survey due *__today__* at midnight!

Logistics

Quiz 1 next Tuesday:

- Covers anything before next Tuesday.

- Modes:

  - Atlanta Section: Taken in class (so 1 hour + 15 mins)
  - ShenZhen Section: 10:25 - 11:40 AM on Wednesday, Sept 20, Shenzhen time, Room 408
  - Q Section: I've sent a Canvas announcement about this

Logistics

Quiz 1 next Tuesday:

During the exam:

- Open paper notes (no electronic devices, including tablets, laptops, phones)

- One seat between each person (including diagonally)

- Atlanta section: If you need clarification on a question during the exam, can ask one of the course staff. (No questions about your reasoning/answer)

- All sections: **When in doubt**, write your full justification/explanation for your answer. Then, if you submit a regrade request later on, we can factor in your justification.

Logistics

Quiz 1 Format:

- Bunch of True/False Questions

- Bunch of Multiple Choice Questions

- A Few Short Response or Fill-in-the-Blank Questions

- 3-4 Longer Reponse Questions (answer + explain why)

Questions will be a mix of definition-based questions as well as questions about certain situations/scenarios

Finishing up from last lecture...

Quick note on WPA3

Still has Personal and Enterprise Mode

Recall: WPA2's symmetric key generation was vulnerable b/c the password could be easily obtained + the key counter (which introduces randomness) can be sniffed.

Recall: WPA3 fixes this issue through a Diffie-Hellman-like key exchange (instead of a key counter), so sniffing doesn't allow the attacker to figure out the key.

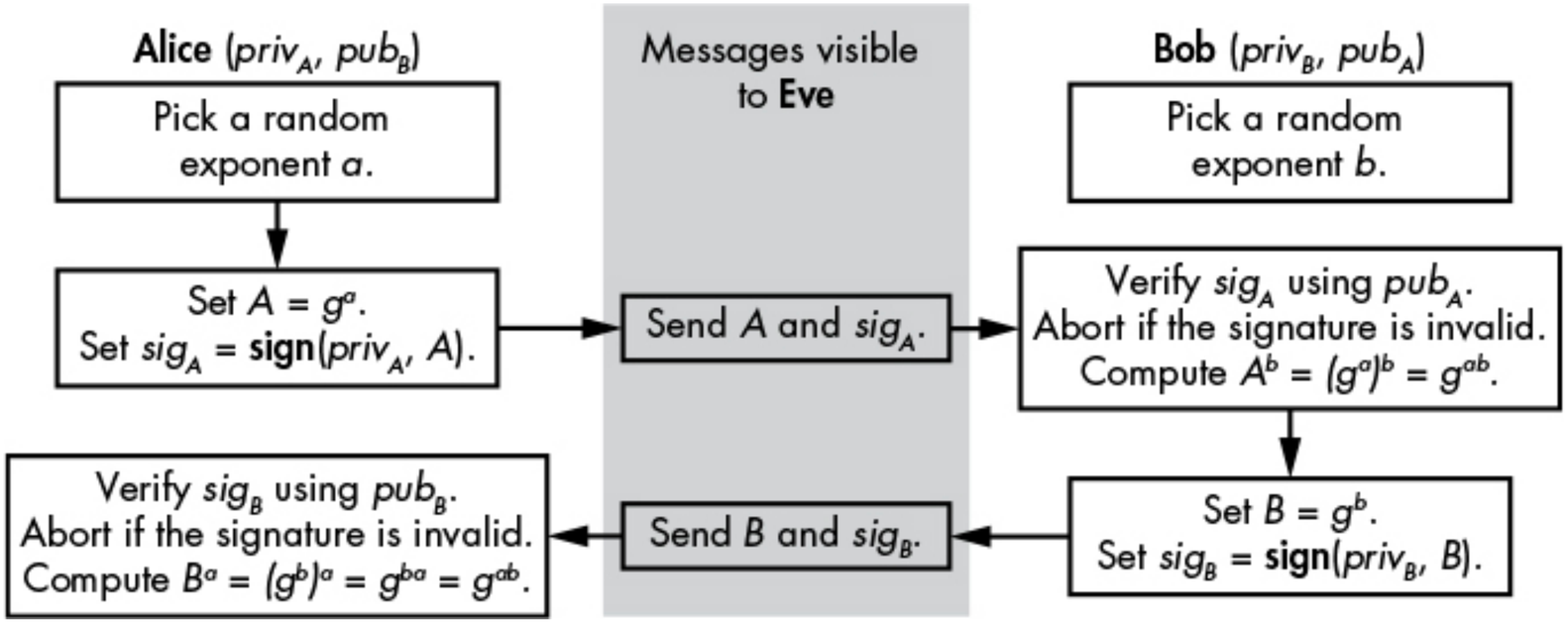
BUT: While DH allows for secure key exchange under an eavesdropper, it doesn't protect against MITM attack. Attacker can spoof being the AP to do MITM attack.

DH: Man-in-the-Middle Attack

Alice-Eve
Shared Key
g^{ae} mod p

Bob-Eve
Shared Key
g^{eb} mod p

Back to Diffie-Hellman: Man-in-the-Middle Defense



The authenticated Diffie-Hellman protocol

Quick note on WPA3

Still has Personal and Enterprise Mode

Recall: WPA2's symmetric key generation was vulnerable b/c the password could be easily obtained + the key counter (which introduces randomness) can be sniffed.

Recall: WPA3 fixes this issue through a Diffie-Hellman-like key exchange (instead of a key counter), so sniffing doesn't allow the attacker to figure out the key.

BUT: While DH allows for secure key exchange under an eavesdropper, it doesn't protect against MITM attack. Attacker can spoof being the AP to do MITM attack.

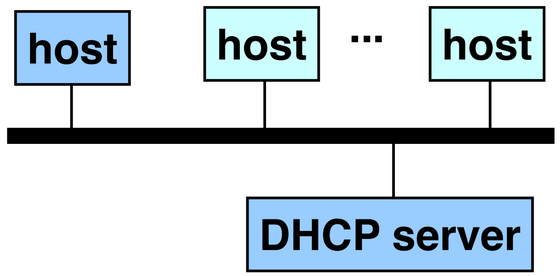
For MITM defense, we need authenticated DH, which requires public-key cryptography. Certificates provide this sort of public-key infrastructure (so Enterprise mode).

Internet Bootstrapping: DHCP

Newly joined host doesn't have an IP address yet, needs one (to use as the IP source address).

Also doesn't know who to ask for an IP address (i.e., doesn't know who to put in as IP destination)

Solution: Broadcast a link-layer packet (no IP addresses) to "discover" a server to help out.



DHCP = Dynamic Host Configuration Protocol

DHCP Protocol

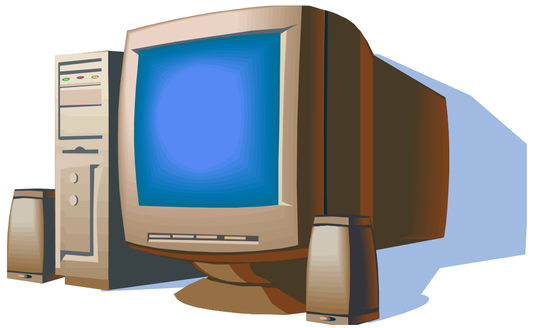
new client

DHCP discover (broadcast)

DHCP offer

DHCP request (broadcast)

DHCP ACK



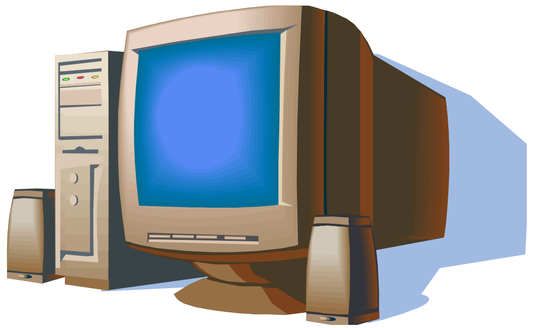
DHCP server

"**offer**" message includes IP address, DNS server, "gateway router", and how long client can have these ("lease" time)

DHCP Protocol

new client

DHCP discover (broadcast)



DHCP server

DHCP offer

DHCP request (broadcast)

DHCP ACK

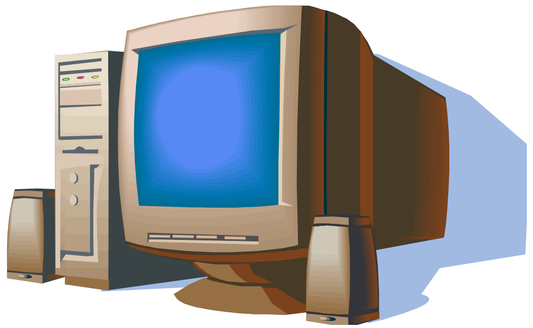
Local attacker on same network can **hear** new host's DHCP request

"**offer**" message includes IP address, DNS server, "gateway router", and how long client can have these ("lease" time)

DHCP Protocol

new client

DHCP discover (broadcast)



DHCP server

DHCP offer

DHCP request (broadcast)

DHCP ACK

This happens **even for WPA2-Enterprise**, since request is explicitly sent using broadcast

"**offer**" message includes IP address, DNS server, "gateway router", and how long client can have these ("lease" time)

DHCP Protocol

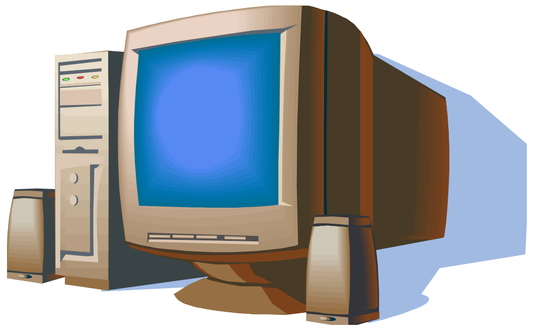
new client

DHCP discover (broadcast)

DHCP offer

DHCP request (broadcast)

DHCP ACK



DHCP server

"**offer**" message includes IP address, DNS server, "gateway router", and how long client can have these ("lease" time)

Attacker can **race** against the DHCP server to send a response; if attacker wins, can replace DNS server and/or gateway router

DHCP Threat

- Substitute a fake DNS server
  - Redirect any of a host's lookups to a machine of attacker's choice (e.g., `gmail.com` = **`6.6.6.6`**)
- Substitute a fake gateway router
  - Intercept all of a host's off-subnet traffic (even if not preceded by a DNS lookup)
  - This is one type of invisible ***Man In The Middle*** (MITM)
    - Victim host generally has no way of knowing it's happening! 😟
    - (Can't necessarily alarm on peculiarity of receiving multiple DHCP replies, since that can happen benignly)

DHCP Threat

- How can we fix this?

Hard, because we lack a ***trust anchor***

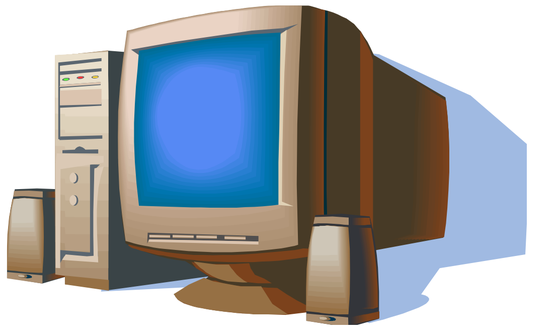
- Mitigations (not full fixes):
  - *DHCP Snooping*: configure LAN switches with trusted DHCP servers, and only forward their DHCP traffic
  - *Hard-code DHCP information* (i.e., don't use DHCP)

  These only work well for smaller/pre-configured networks :(

DHCP Protocol

new client

DHCP discover (broadcast)



DHCP server

DHCP offer

DHCP request (broadcast)

DHCP ACK

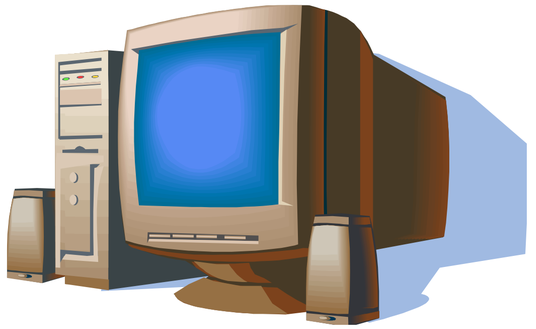
"**offer**" message includes IP address, DNS server, "gateway router", and how long client ~~can have~~ these ("lease" time)

These servers are all IP addresses. We may need to know their MAC address to reach locally.

Address Resolution Protocol (ARP)

new client

ARP probe:
who has IP address X
(broadcast)



Gateway Router

ARP response:
I have IP address X,
and my MAC address is Y

Same spoofing threat as with DHCP (attacker can spoof ARP response)

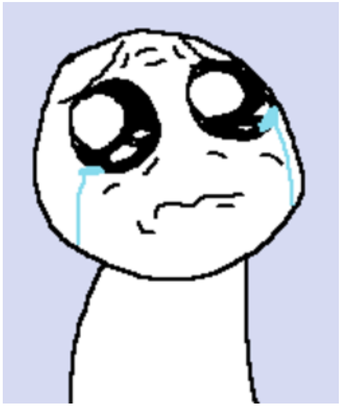
ARP Threat

- Spoof/substitute as another IP address
  - Redirect any traffic to another local IP to your (or another) device

- How to fix?
  - Still hard :(
  - Could hard-code IP/MAC mappings, or track known IP/MAC mappings and filter out ARP requests with unknown mappings. This only works at limited scales though.

LAN Threats Summary

- LAN relies on broadcast protocols
  - Broadcast protocols inherently at risk of **local** attacker sniffing and spoofing.
    - Attacker knows exactly what you're communicating… and can spoof valid responses at the right time
  - When initializing, systems are particularly vulnerable because they can *lack a trusted foundation* to build upon
  - Tension between wiring in trust vs. flexibility and convenience
  - MITM attacks **insidious** because no indicators they're occurring



Today: Network Layer Security

Certificates + Chain of Trust

Our crypto tool bag

Public key cryptography

- Alice can use Bob's public key to send an encrypted message that only Bob can decrypt (using his private key).

Digital signatures

- Alice can use her private key to sign a message that Bob can verify using Alice's public key.

But how does Alice know that a public key is Bob's, if Alice hasn't met Bob before?

Our crypto tool bag

Public key cryptography

- Alice can use Bob's public key to send an encrypted message that only Bob can decrypt (using his private key).

Digital signatures

- Alice can use her private key to sign a message that Bob can verify using Alice's public key.

But how does Alice know that a public key is Bob's, if Alice hasn't met Bob before?

Maybe get someone Alice trusts and can vouch for Bob's public key

Certificate Authorities

A **certificate** contains an entity's identity and public key.

Certificate authorities (CA) are entities that "vouch" for a certificate.

- Bob provides some "proof of identity" and his public key to a CA.
- CA creates a certificate containing Bob's identity and his public key.
- CA digitally signs the certificate (with the CA's secret key).
- Bob can now share this certificate, and anyone who has the CA's public key can trust the certificate content

Examples of identity: domain name, where proof of identity could be making a CA-requested change at the domain to prove ownership.

Certificate Authorities

A **certificate** contains an entity's identity and public key.

Certificate authorities (CA) are entities that "vouch" for a certificate.

- Bob provides some "proof of identity" and his public key to a CA.
- CA creates a certificate containing Bob's identity and his public key.
- CA digitally signs the certificate (with the CA's secret key).
- Bob can now share this certificate, and anyone who has the CA's public key can trust the certificate content

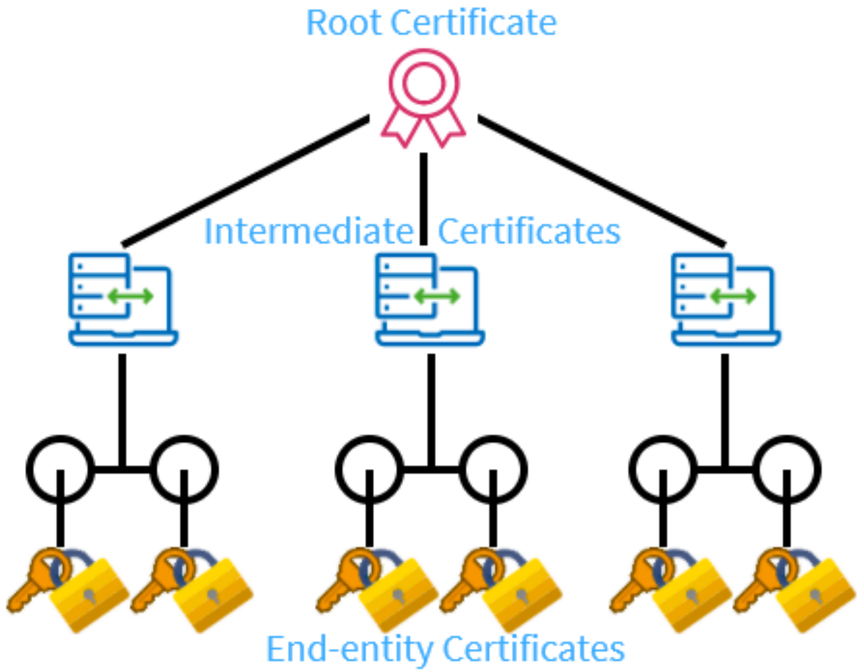
Examples of identity: domain name, where proof of identity could be making a CA-requested change at the domain to prove ownership.

But doesn't this just shift the question of trust to the CA?

Hierarchy of Trust

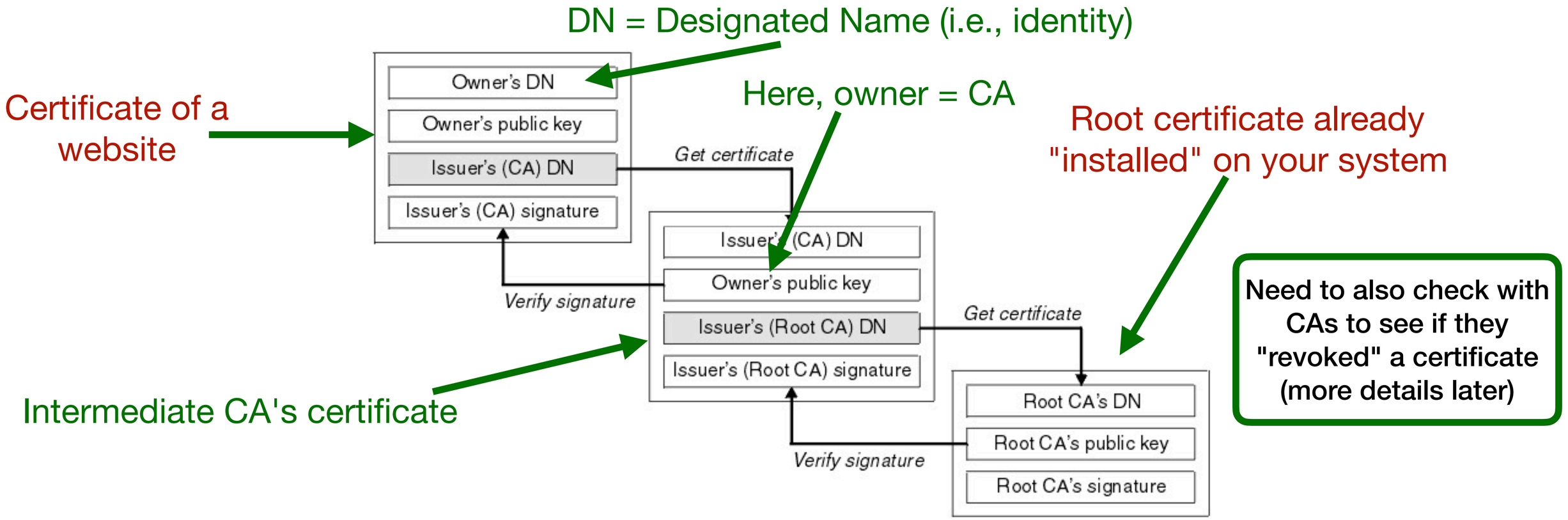
Need a trust anchor. These are the **root certificate authorities**. Their certificates come default in a system.

Root CAs can sign the certificates of other trusted CAs (which can in turn sign certificates of other entities, including other domains and CAs). These CAs forms the **Public-Key Infrastructure (PKI).**



Certificate Chains

Each entity's certificate is **signed** by the parent entity in the hierarchy of trust (up until the root certificate)



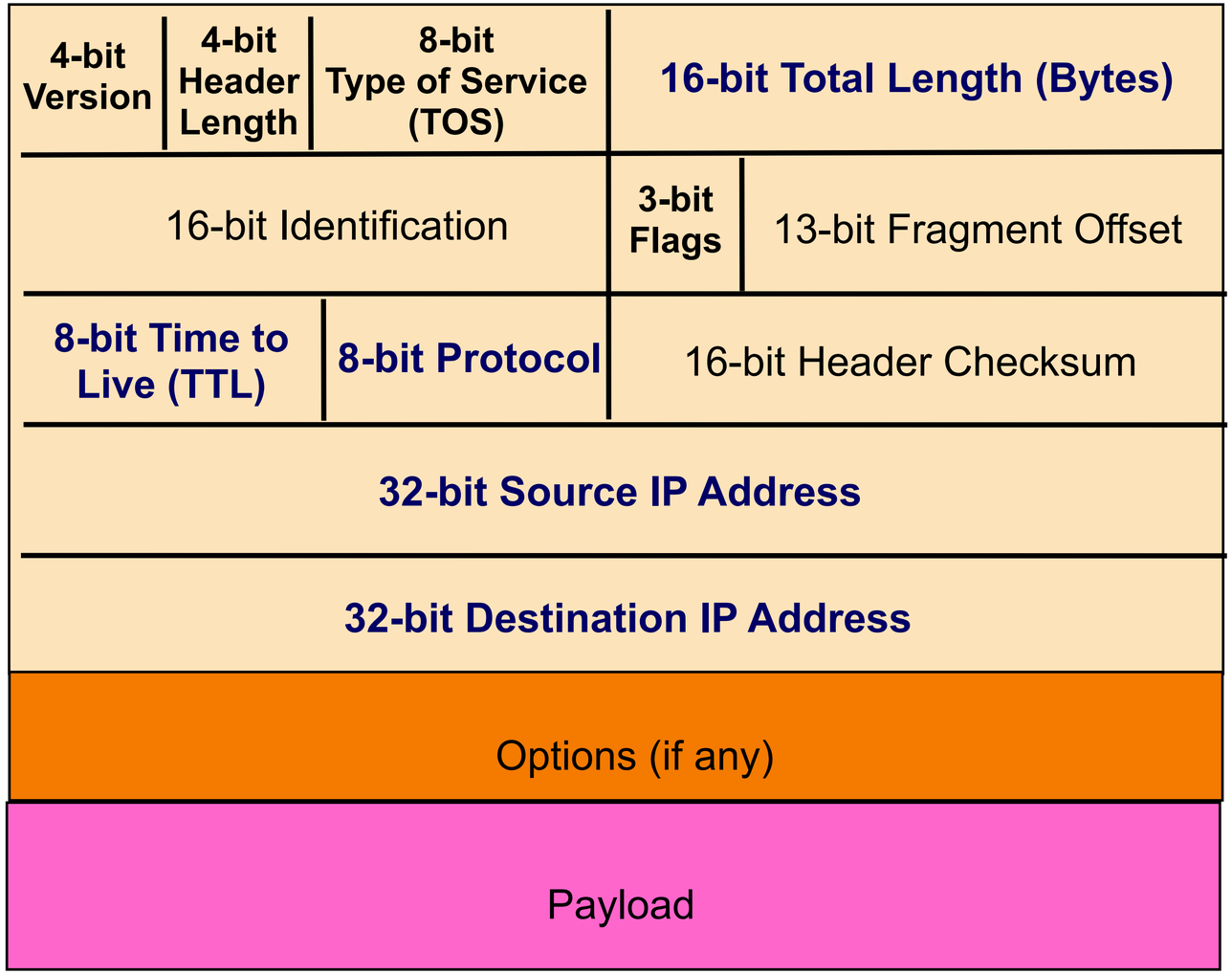
Today: Network Layer Security

IP Protocol

Sending packets b/w IP source to IP destination addresses (could be across the Internet)

- IPv4: 32-bit addresses
- IPv6: 128-bit addresses

IPv4 Packet Header

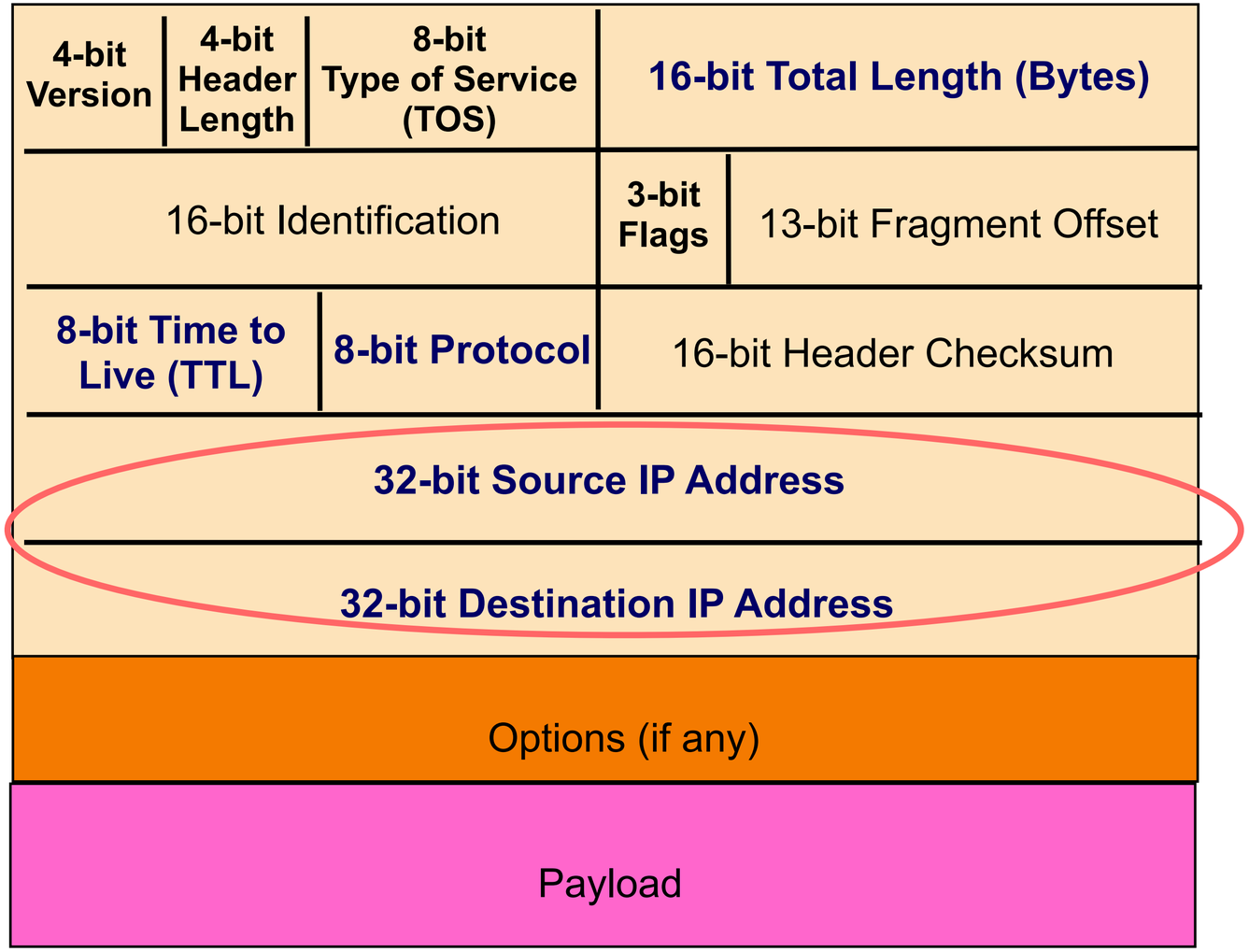


IP Protocol

Sending packets b/w IP source to IP destination addresses (could be across the Internet)

- IPv4: 32-bit addresses
- IPv6: 128-bit addresses

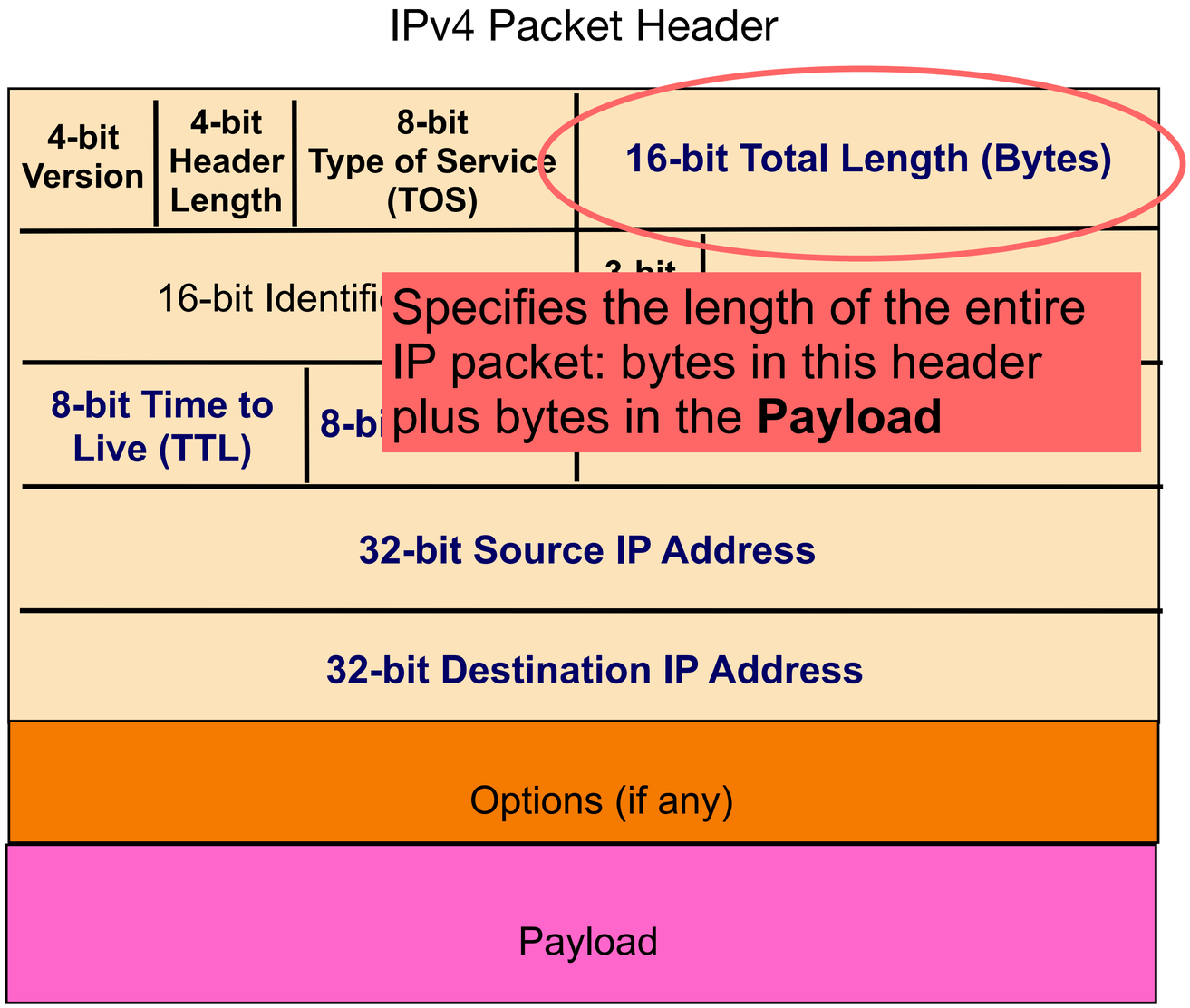
IPv4 Packet Header



IP Protocol

Sending packets b/w IP source to IP destination addresses (could be across the Internet)

- IPv4: 32-bit addresses
- IPv6: 128-bit addresses

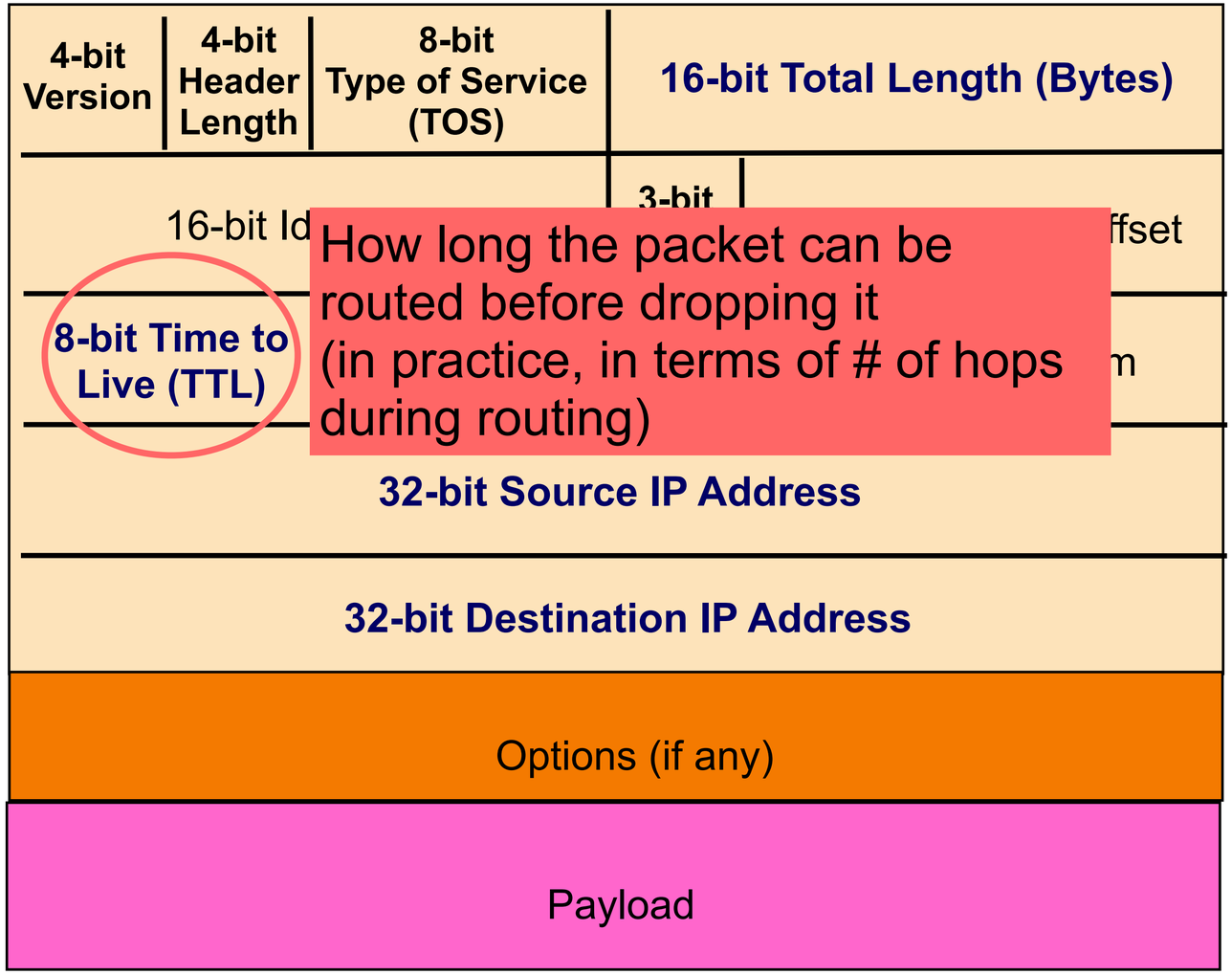


IP Protocol

Sending packets b/w IP source to IP destination addresses (could be across the Internet)

- IPv4: 32-bit addresses
- IPv6: 128-bit addresses

IPv4 Packet Header

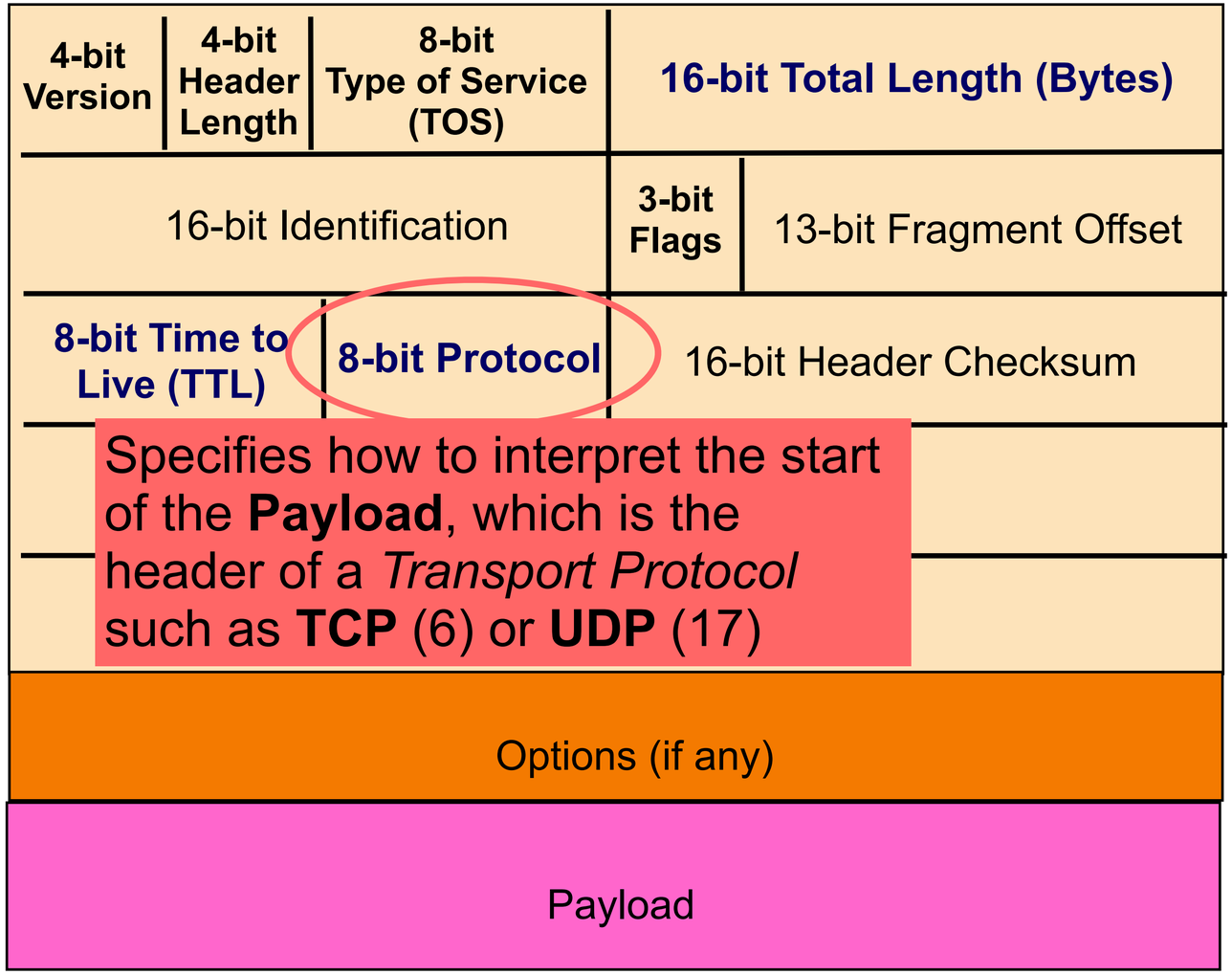


IP Protocol

Sending packets b/w IP source to IP destination addresses (could be across the Internet)

- IPv4: 32-bit addresses
- IPv6: 128-bit addresses

IPv4 Packet Header

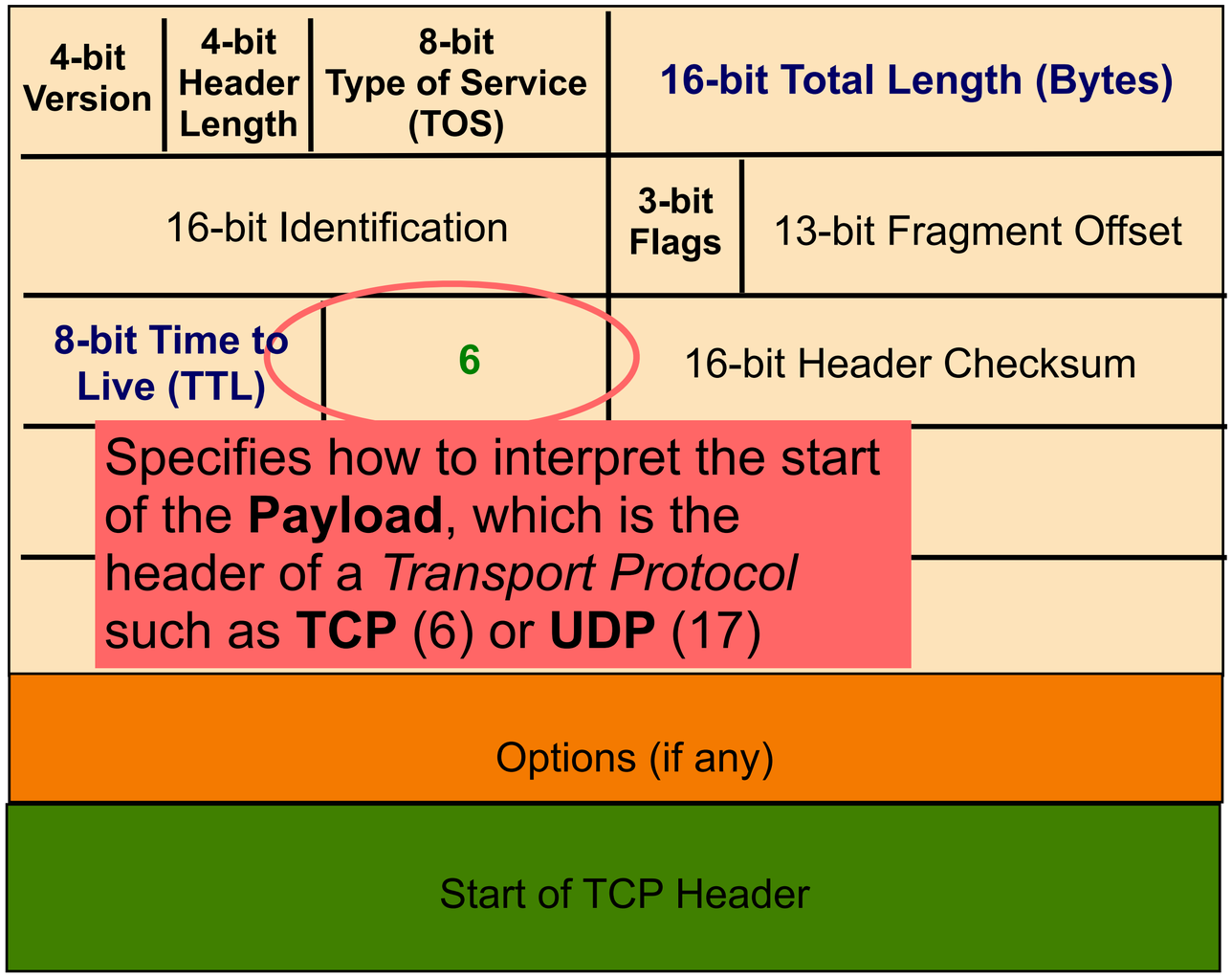


IP Protocol

Sending packets b/w IP source to IP destination addresses (could be across the Internet)

- IPv4: 32-bit addresses
- IPv6: 128-bit addresses

IPv4 Packet Header

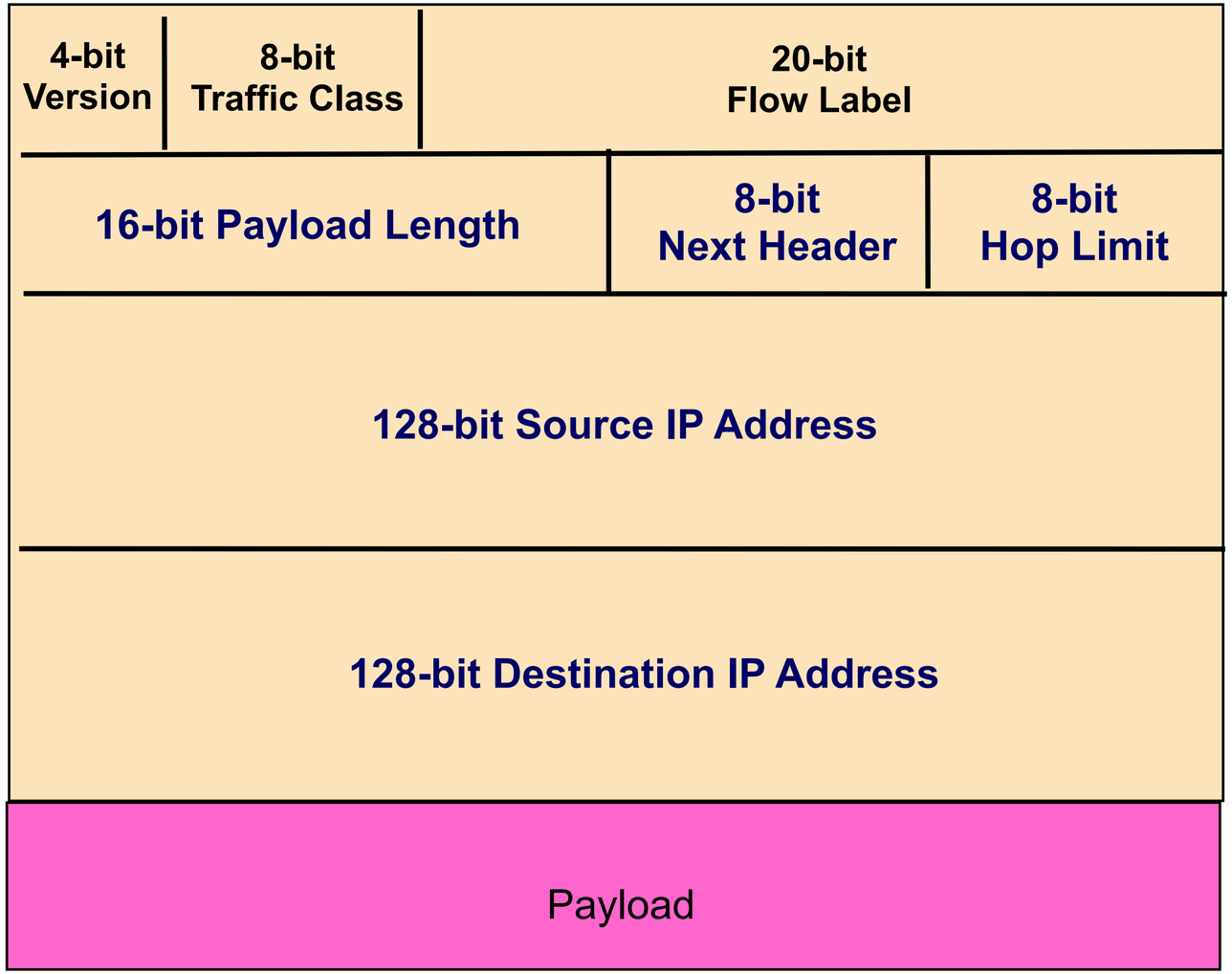


IP Protocol

Sending packets b/w IP source to IP destination addresses (could be across the Internet)

- IPv4: 32-bit addresses
- IPv6: 128-bit addresses

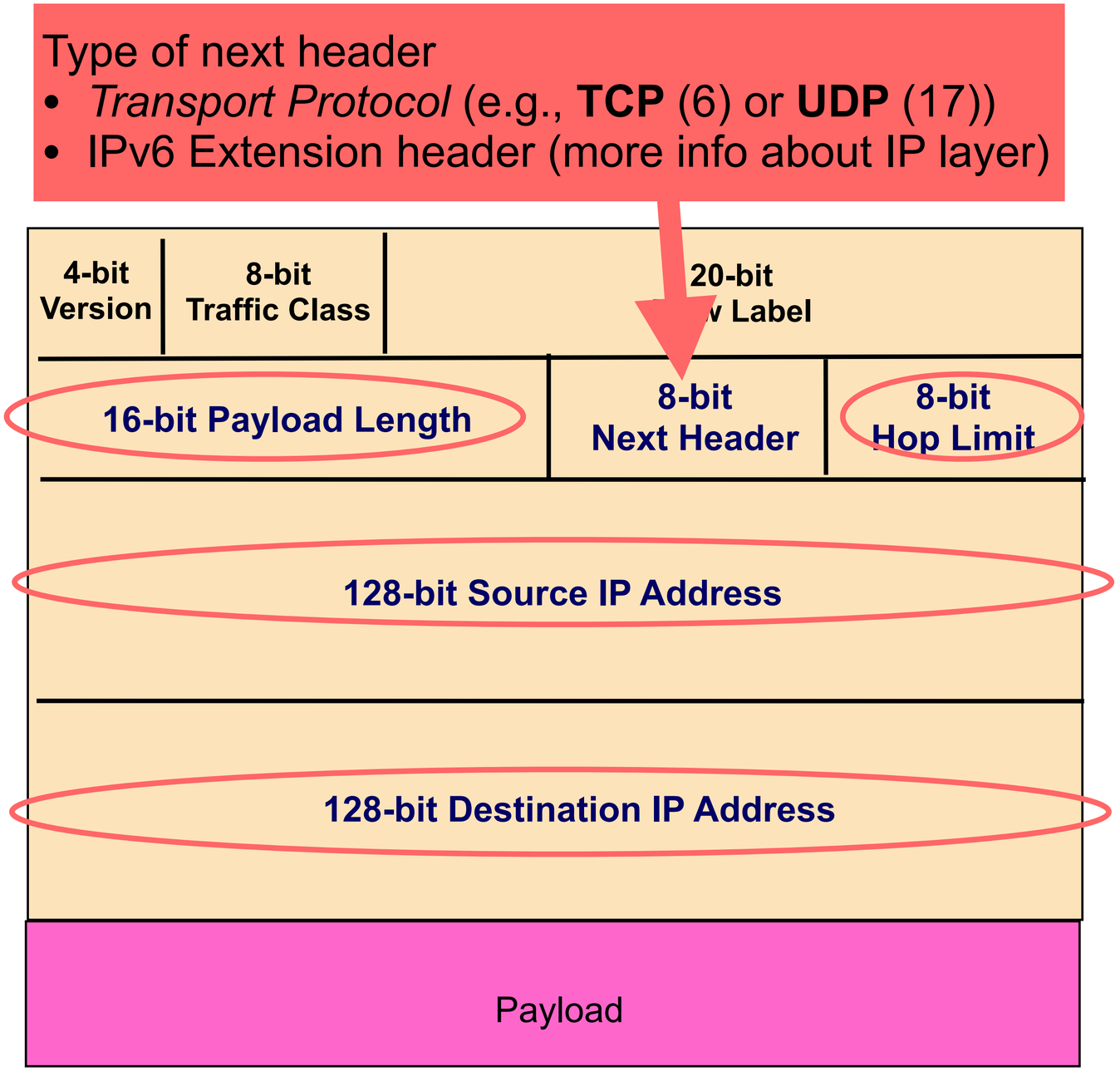
IPv6 Packet Header



IP Protocol

Sending packets b/w IP source to IP destination addresses (could be across the Internet)

- IPv4: 32-bit addresses
- IPv6: 128-bit addresses



IP Protocol

IP addresses of a network can be grouped together into **subnets** that start with the same prefix.

- 108.8.0.0/24 -> subnet starting with the same 24-bit prefix: 108.8.0.*

Within a subnet, special broadcast addresses are those ending in all 1-bits.

- 108.8.0.255 is a broadcast address within 108.8.0.0/24.

Special subnets reserved for use by private networks/LANs (not meant to be Internet routable)

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

IP Packet Vulnerability #1

IP header + payload is unencrypted (no confidentiality/integrity built in)

IPSec

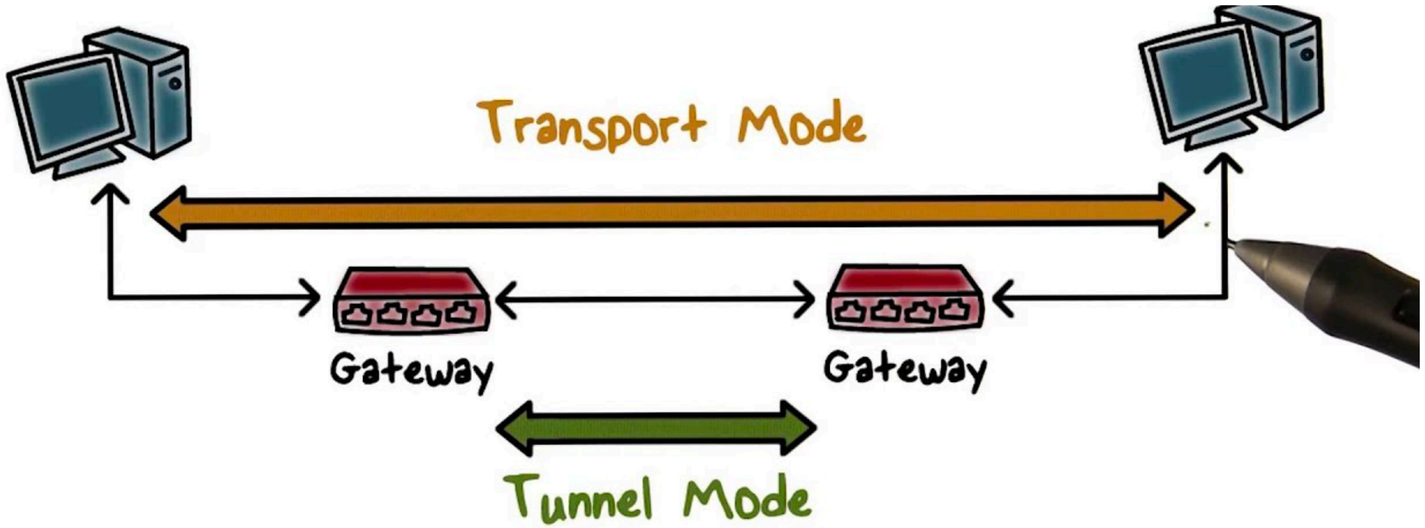
IPSec: Use encryption/MACs for confidentiality/integrity.

- Requires key exchange/establishment b/w IPSec endpoints
- Adopted in certain situations (e.g., b/w networks of the same company)
- Two IPSec modes:
  - Transport Mode (host <-> host)
  - Tunnel Mode (gateway <-> gateway, VPN-like)

IPSec

IPSec: Use encryption/MACs for confidentiality/integrity.

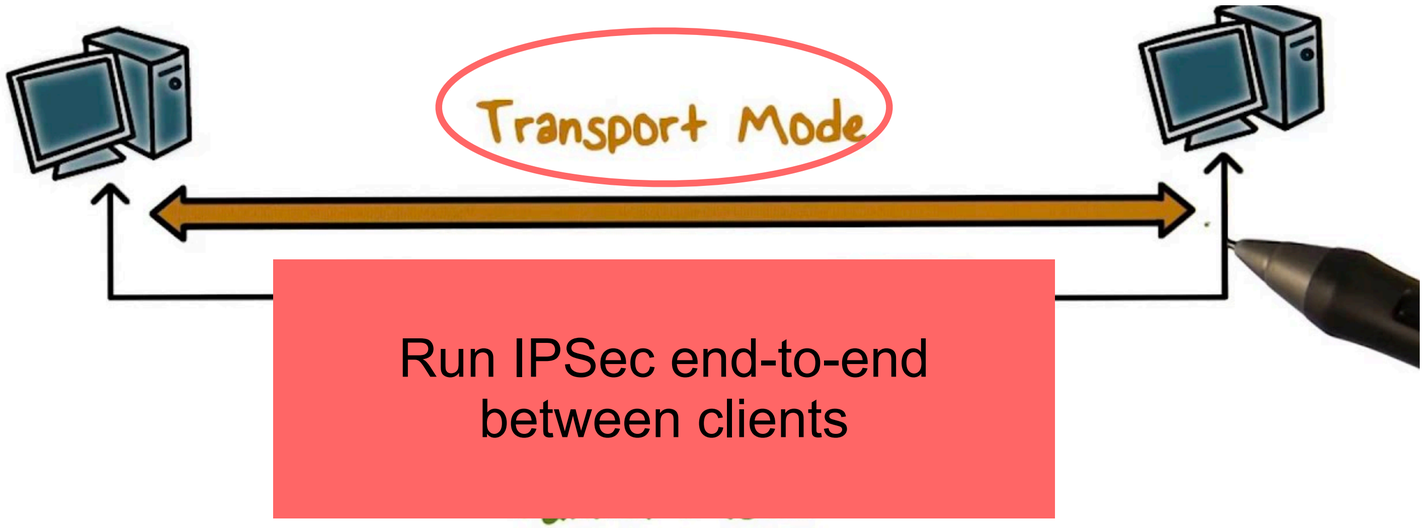
- Requires key exchange/establishment b/w IPSec endpoints
- Adopted in certain situations (e.g., b/w networks of the same company)
- Two IPSec modes:
  - Transport Mode (host <-> host)
  - Tunnel Mode (gateway <-> gateway, VPN-like)



IPSec

IPSec: Use encryption/MACs for confidentiality/integrity.

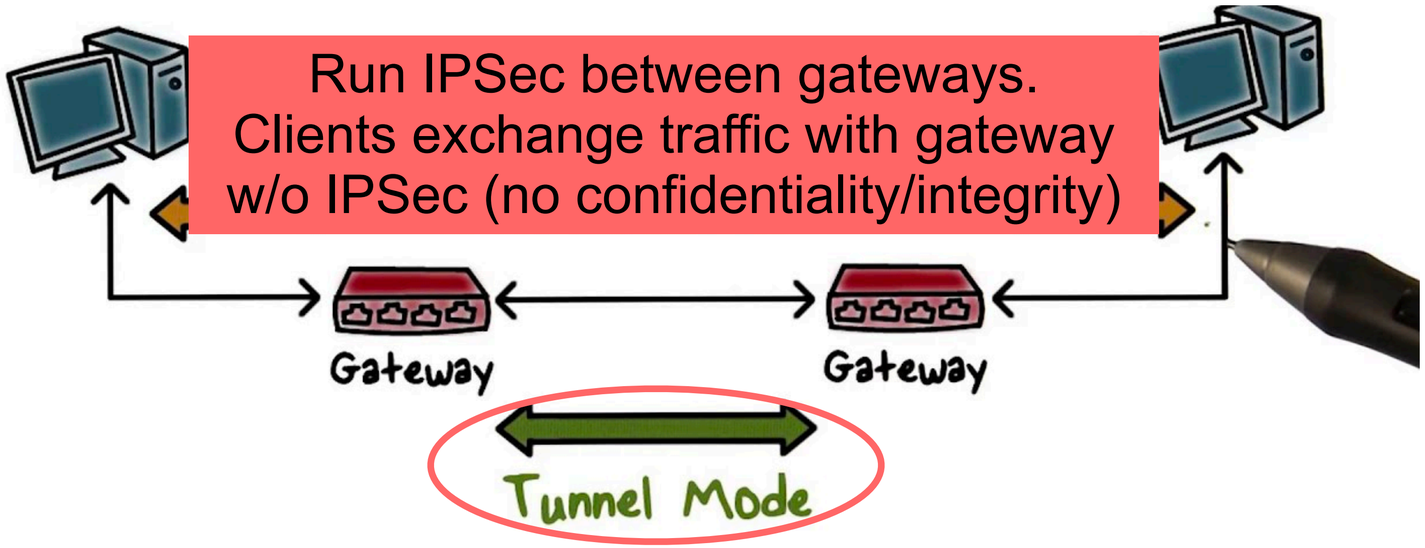
- Requires key exchange/establishment b/w IPSec endpoints
- Adopted in certain situations (e.g., b/w networks of the same company)
- Two IPSec modes:
  - Transport Mode (host <-> host)
  - Tunnel Mode (gateway <-> gateway, VPN-like)



IPSec

IPSec: Use encryption/MACs for confidentiality/integrity.

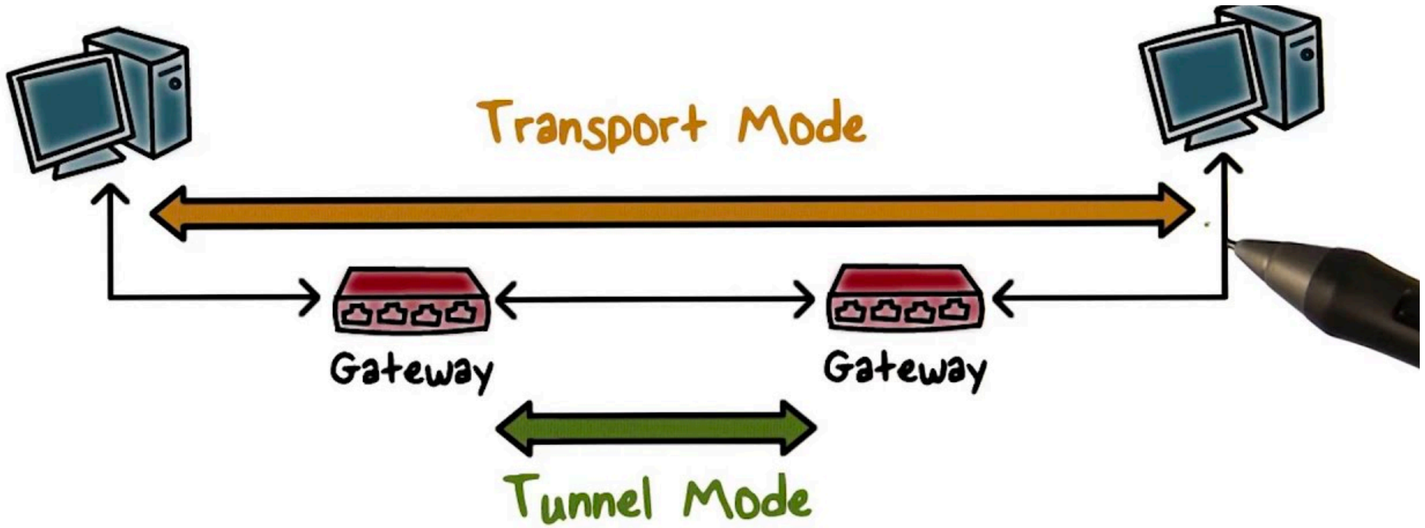
- Requires key exchange/establishment b/w IPSec endpoints
- Adopted in certain situations (e.g., b/w networks of the same company)
- Two IPSec modes:
  - Transport Mode (host <-> host)
  - Tunnel Mode (gateway <-> gateway, VPN-like)



IPSec

IPSec: Requires key exchange/establishment b/w IPSec endpoints

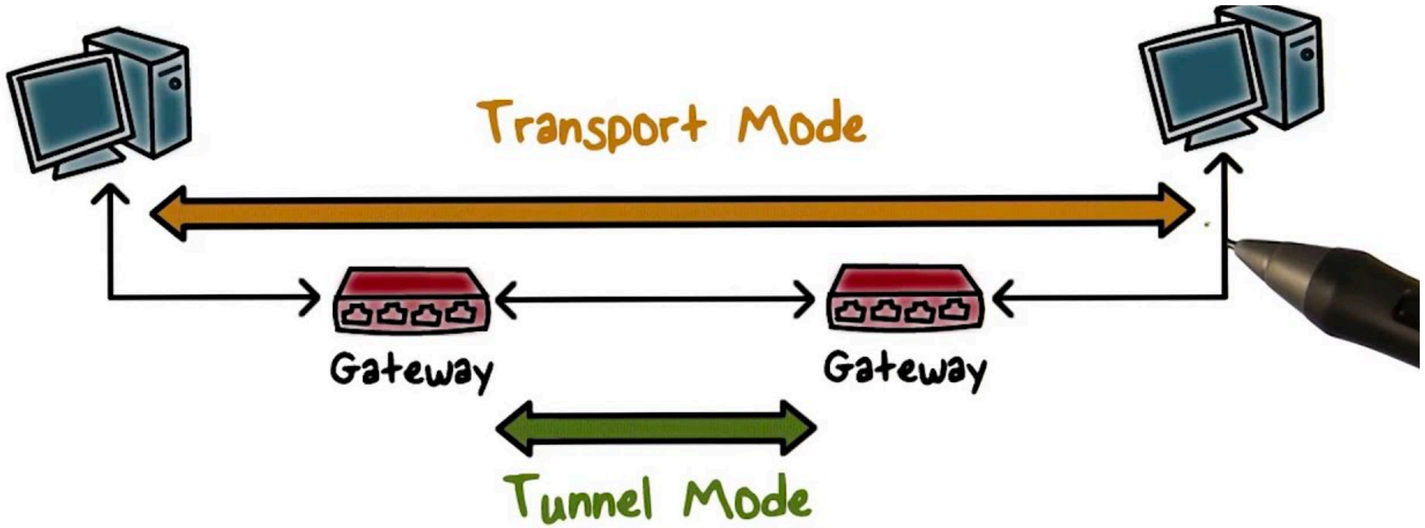
- Can be preconfigured symmetric keys
  - Bad: Everyone has same key! Compromised if only one client leaks key.
- PKI (public or internal to an organization): everyone has their own public/private key pair and a certificate, signed by a CA trusted by other clients
  - Good! Everyone has their own keys. CA must be properly secured!



IPSec

IPSec: Requires key exchange/establishment b/w IPSec endpoints

- IKE (Internet Key Exchange): protocol that's part of IPSec for clients/gateways to set up the secure connection
  - Decide which cryptographic algorithms to use (ciphers, hash functions)
  - Use authenticated Diffie-Hellman to establish shared session keys (using PKI certificates for the authentication)



IPSec

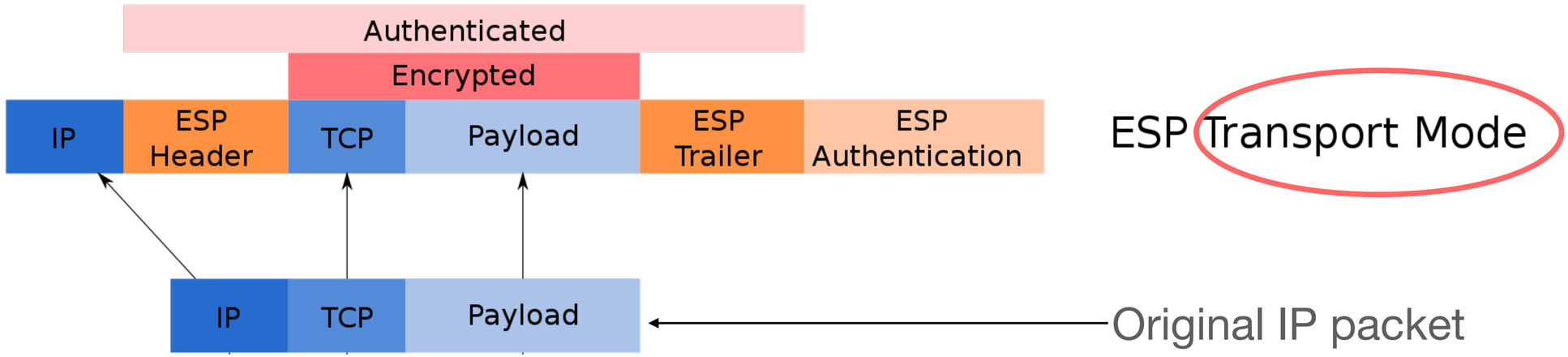
IPSec: Different security functionalities provided.

- **Encapsulating Security Payload (ESP)** functionality provides confidentiality + integrity
- **Authentication Headers (AH)** functionality provides only integrity (not often used)

IPSec

IPSec: Different security functionalities provided.

- **Encapsulating Security Payload (ESP)** functionality provides confidentiality + integrity

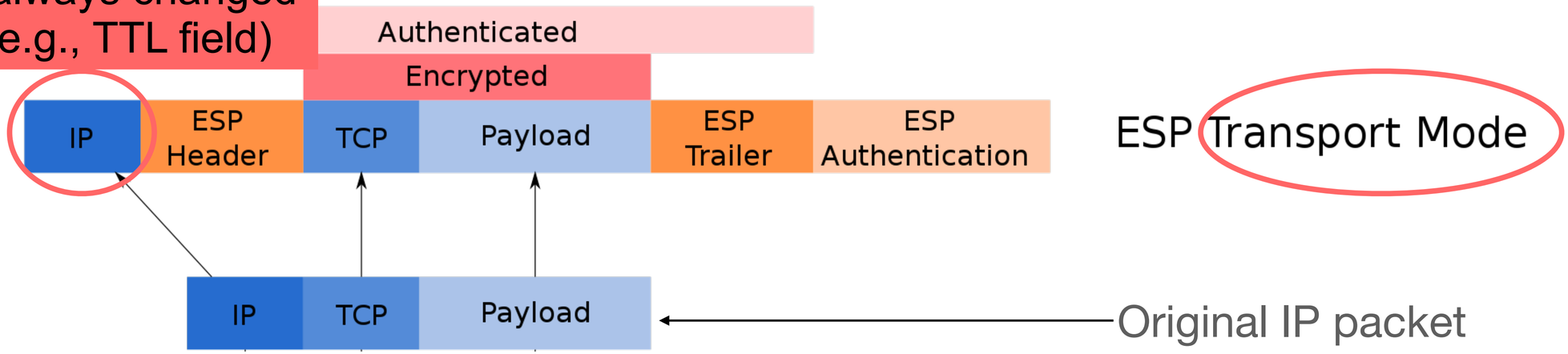


IPSec

IPSec: Different security functionalities provided.

- **Encapsulating Security Payload (ESP)** functionality provides confidentiality + integrity

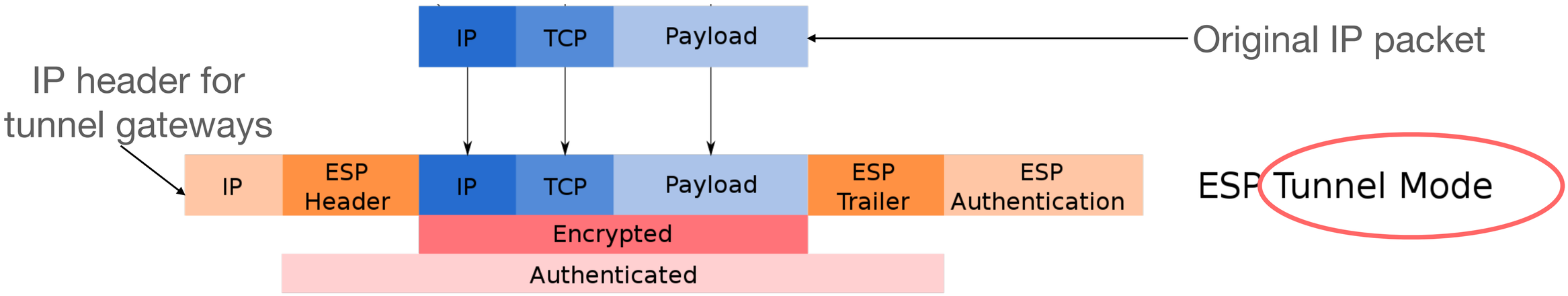
Why no integrity for IP header?
B/c header always changed each hop (e.g., TTL field)



IPSec

IPSec: Different security functionalities provided.

- **Encapsulating Security Payload (ESP)** functionality provides confidentiality + integrity



IPSec

Recap:

- Provides confidentiality/integrity for IP packet
- Transport mode gives end-to-end benefits, but no IP header encryption/ integrity
- Tunnel mode provides full IP confidentiality/integrity in transit across the Internet, but unencrypted between host and gateway (also requires gateways to be configured)
- In practice, requires host pre-configuration (e.g., public/private keys + certificates + PKI), so most apt for use within an organization/company (e.g., supported by cloud providers like Amazon and Cloudflare)

IPSec in IPv6

- In theory, IPv6 standard says to use **"opportunistic"** IPSec by default
  - Opportunistic: even w/o a global PKI (where we can verify someone else's public key), we can just use the other person's key. As long as there's not active MITM attack, this provides confidentiality/integrity.
  - Hasn't been deployed much in practice though

IP Packet Vulnerability #2

IP source address can be forged/spoofed.

Defenses:

- **Ingress filtering:** A network should not accept/forward incoming packets where the source IP address is not within the origin network's IP range.
- **Egress filtering:** A network should not send outbound packets where the source IP address is not within the network's IP range.

If all networks did this filtering, spoofing will be largely infeasible. Many do! But not all :(

IP Packet Vulnerability #2

Why isn't ingress/egress filtering universal?

- Filtering may require some work (e.g., implementation, administrative, policy) by a network that doesn't directly benefit it
- Filtering's benefits really arise only if most/all networks implement. This can lead to a lack of incentivies for early adoption
- **But** there's hope. Today ~80% of networks disallow spoofing.

IPv6-Specific Security Issues

IPv6 is a separate protocol + software stack

- IPv6 doesn't need NAT (b/c plenty of addresses for every device). But NAT used to hide IPv4 end hosts. IPv6 networks with NATs may lose this property.
- Instead, a network firewall should be used to protect a network. **But** many networks forget to deploy their IPv4 firewall for IPv6. So IPv6 remains open/unprotected.

IPv6-Specific Security Issues

IPv6 address space is huge

- Some networks rely on security through obscurity, assuming that IPv6 is too large for attackers to find their host's IPs. Not true! IPs in various dataset, plus active research on ways to predict where active IPv6 addresses are.

- Data structures (e.g., tables) tracking all IP addresses can get overly large, leading to resource exhaustion vulnerabilities. For example, most IPv4 LANs are /24s, with only 2^8=256 addresses. An IPv6 LAN may be a /64, with 2^64 = HUGE number of addresses!