CS 114: Network Security

Lecture 16 - Virtual Private Networks

Prof. Daniel Votipka
Spring 2023

(some slides courtesy of Prof. Micah Sherr)

Tufts UNIVERSITY

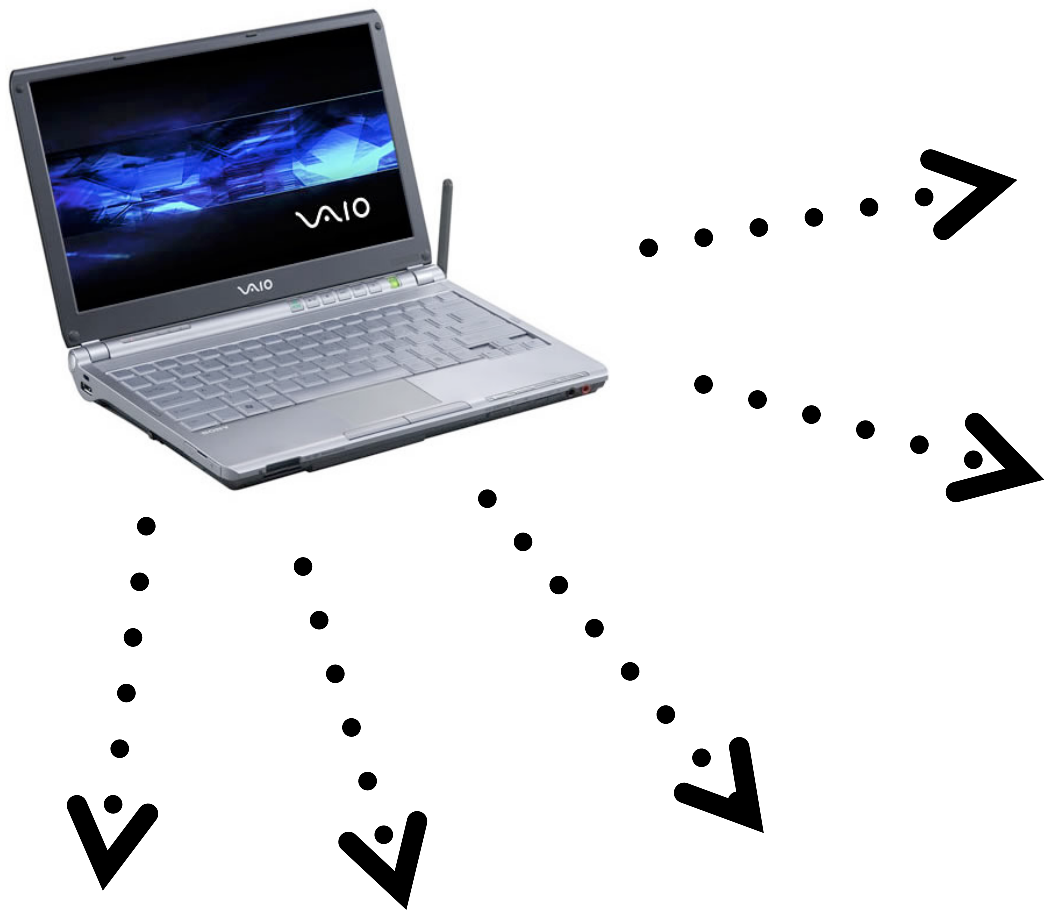
Plan for today

- Administrivia
- Wireless Review
- Virtual Private Networks
  - Overview
  - Protocol - IPsec
    - Key Management
    - Packet Processing
  - Alternatives

Administrivia

- Mid-semester course surveys (end of class)
- Homework 1, part 2 grades are available
- Homework 1, part 3 now due 3/30
- Homework 2 now due 4/27

Wireless Review

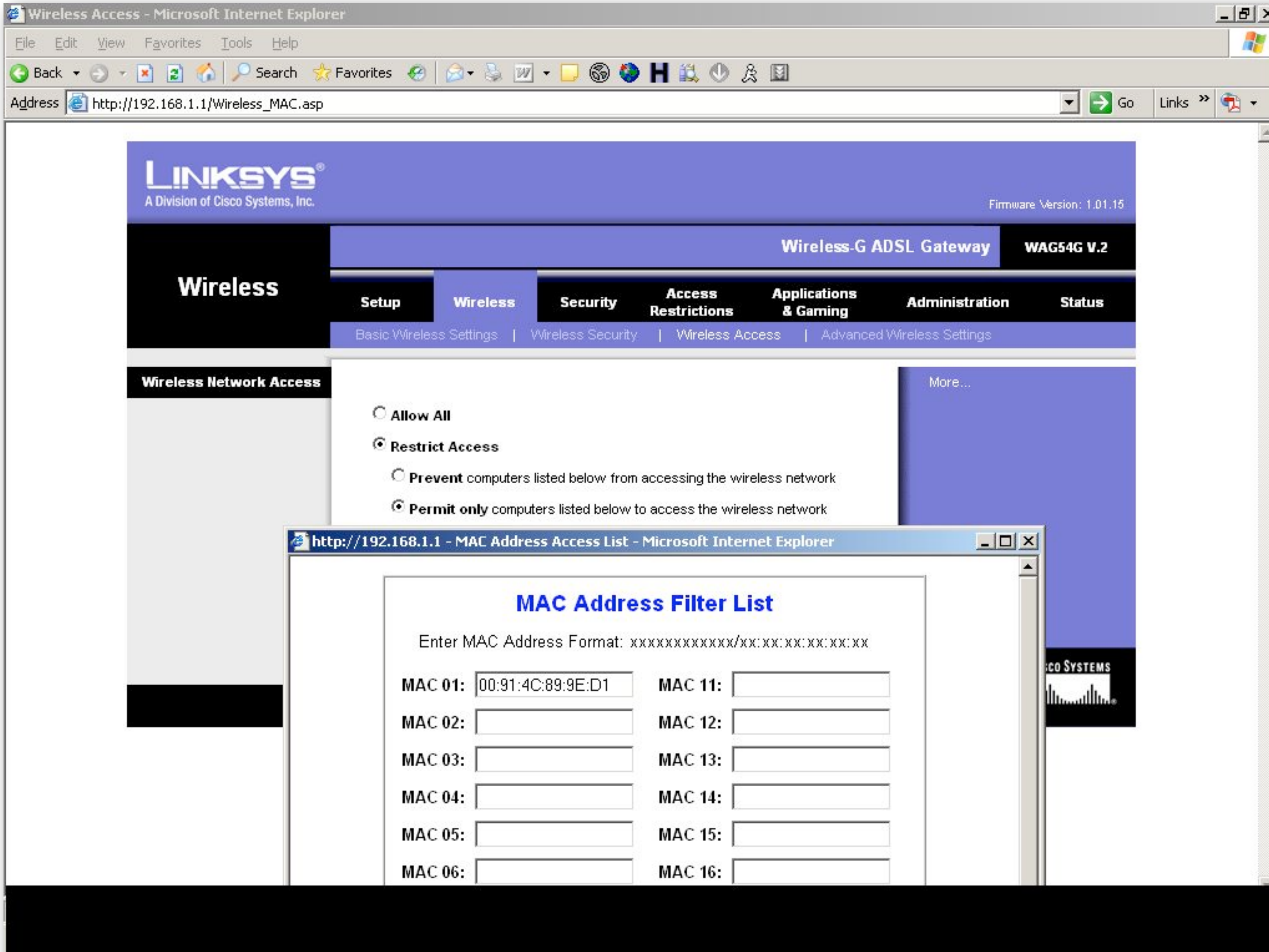


Unsecured wireless:

Problem #1:

Everybody is the receiver.

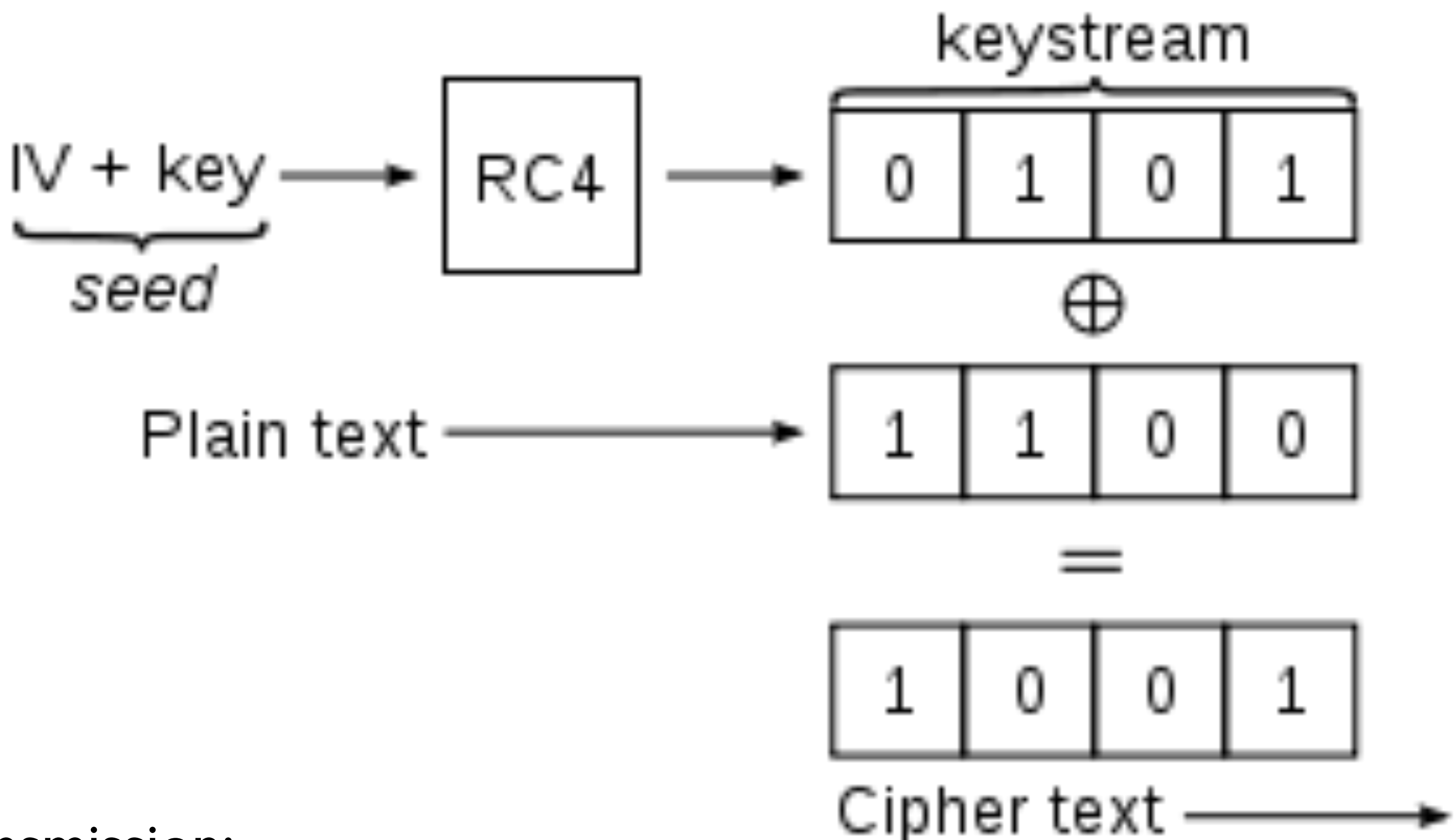
MAC Filtering



SSID hiding

- APs broadcast **Service Set Identifiers (SSIDs)** to announce their presence
- In theory, these should identify a particular wireless LAN
- In practice, SSID can be anything that's 2-32 octets long
- To join network, client must present SSID
- Crappy security mechanism for preventing interlopers:
  - Don't advertise SSID
  - Problem:
    - To join network, client must present SSID
    - This is not encrypted, even if network supports WEP or WPA

Wired Equivalent Privacy (WEP)

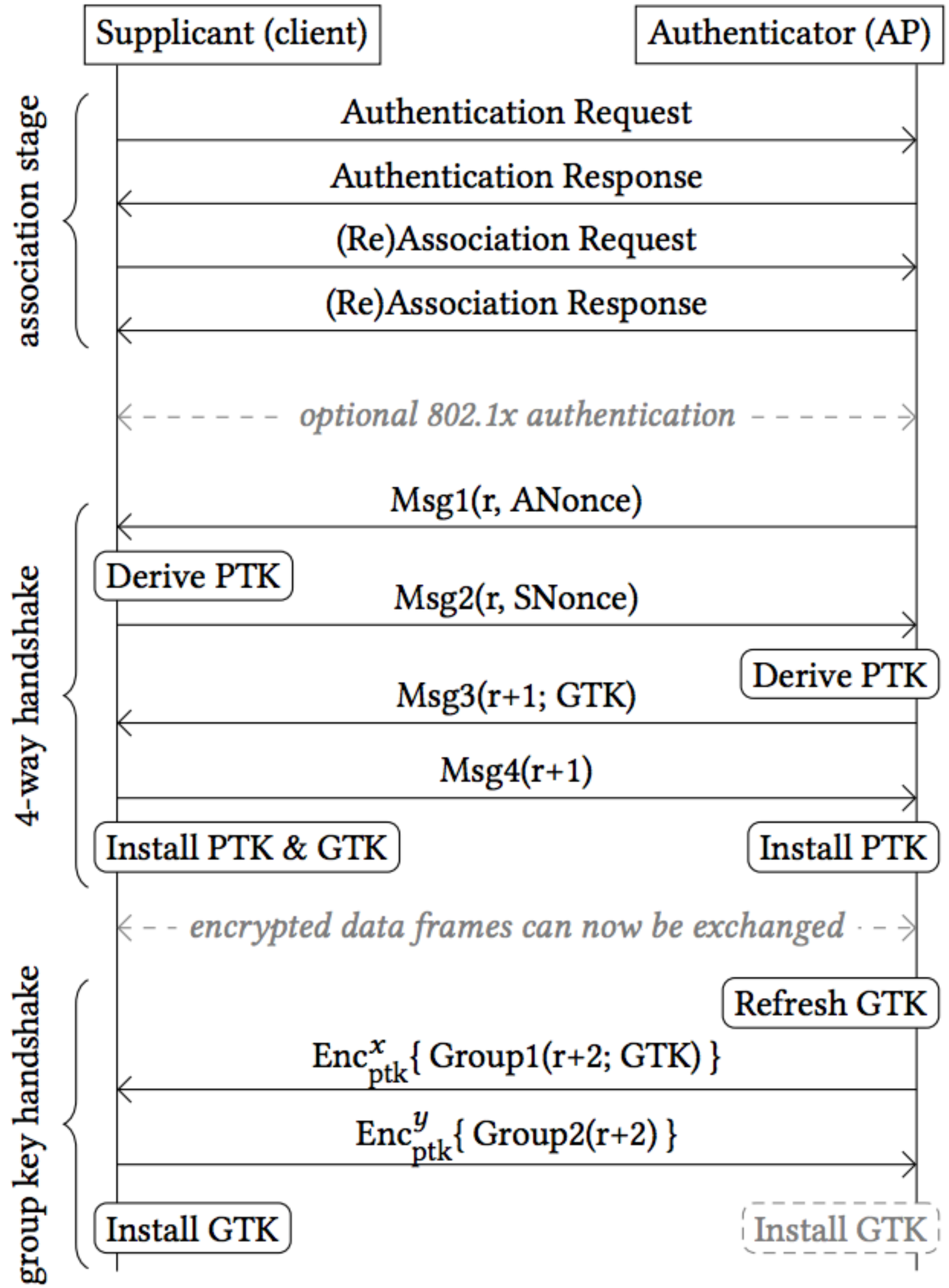


- Data transmission:
  - Produce keystream S using RC4 with seed function f(K,IV)
  - $C = M \oplus S$
  - send (IV, C) frames
  - knowledge of IV and K sufficient to decrypt C

WPA Authentication

Pairwise Transit Key (PTK) = f(PSK, ANonce, SNonce, AP MAC address, STA MAC address)

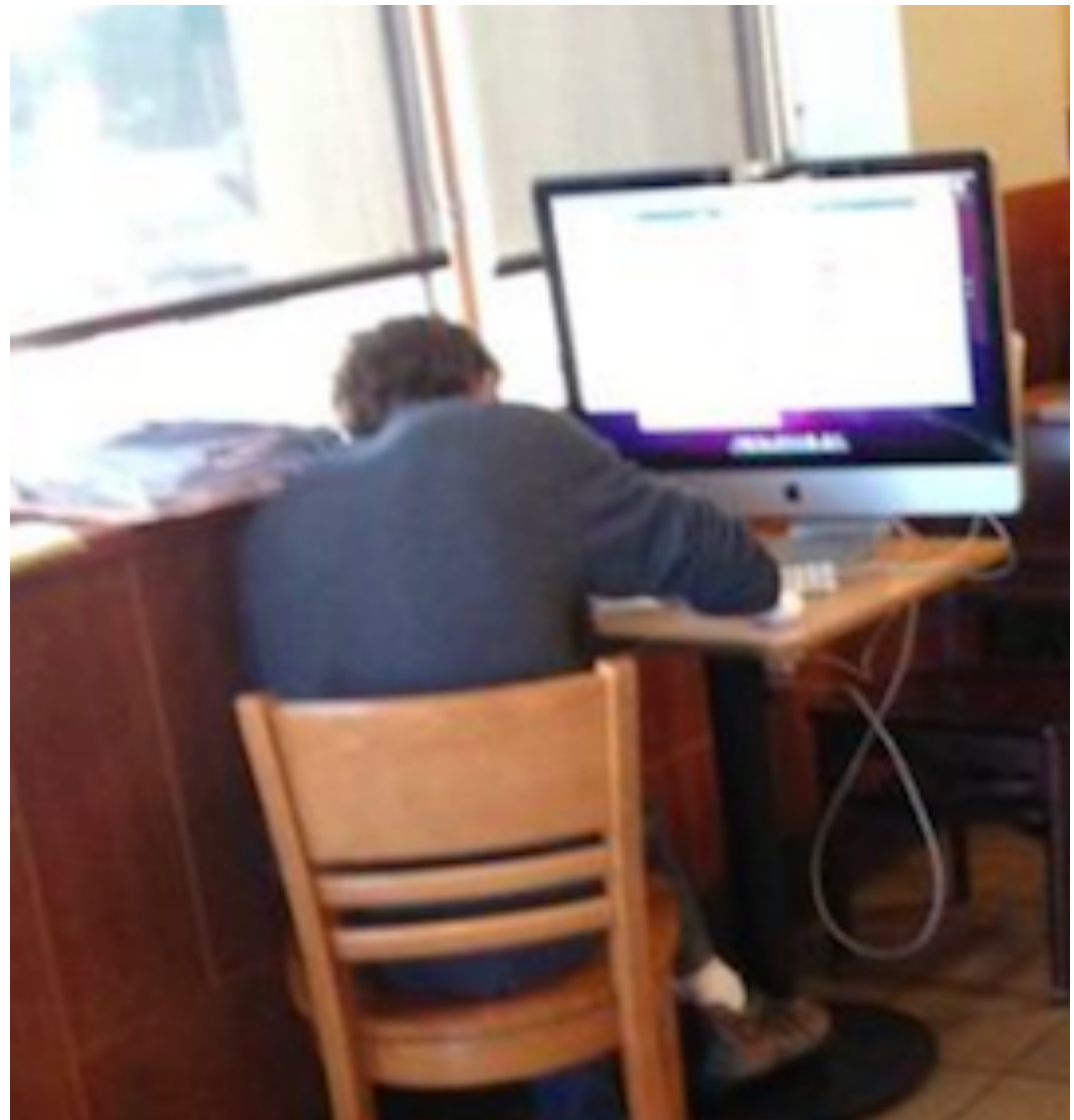
Pre-Shared Key (PSK)



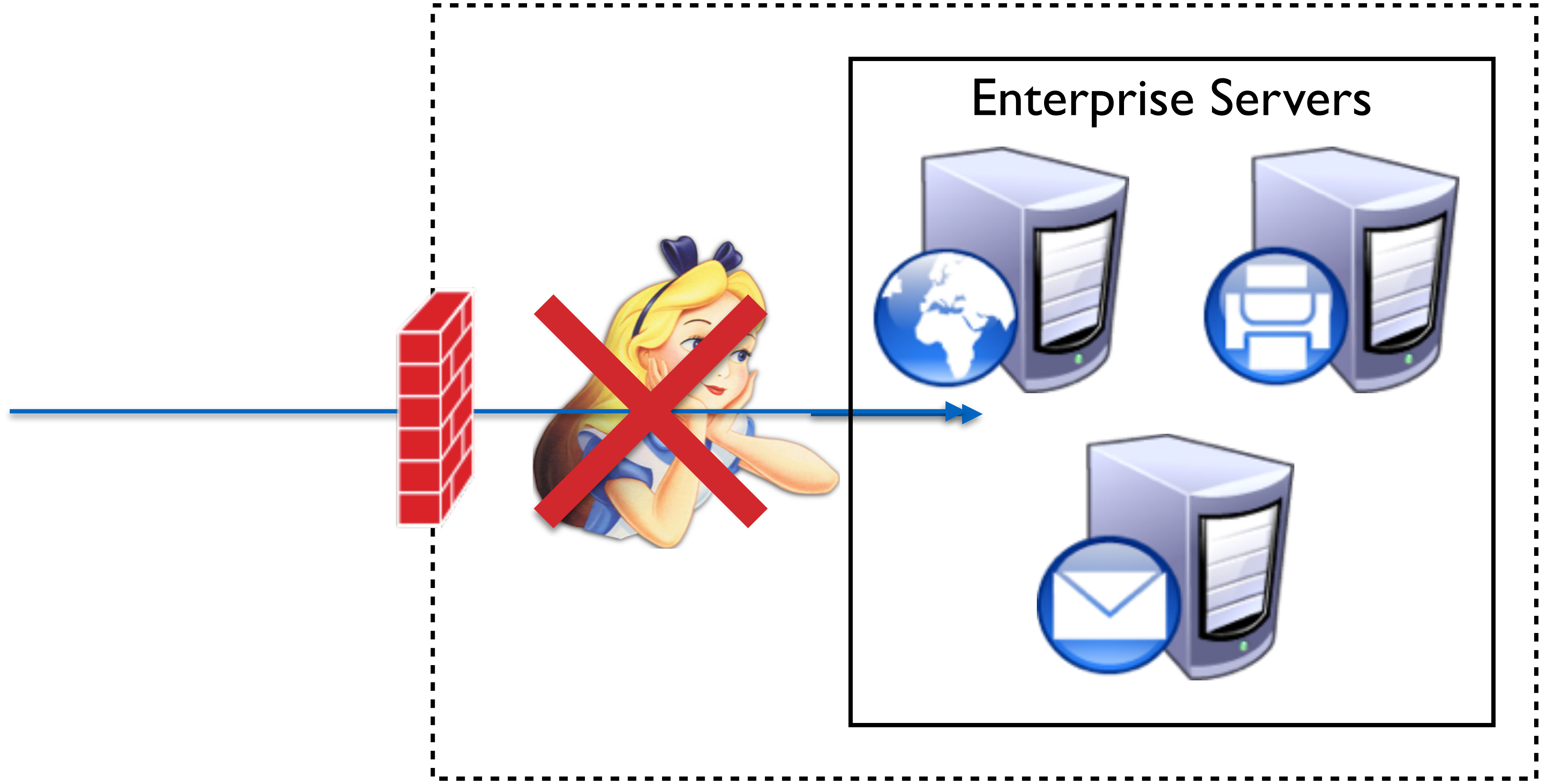
Plan for today

- Wireless Review
- Virtual Private Networks
  - Overview
  - Protocol - IPsec
    - Key Management
    - Packet Processing
  - Alternatives

Problem:



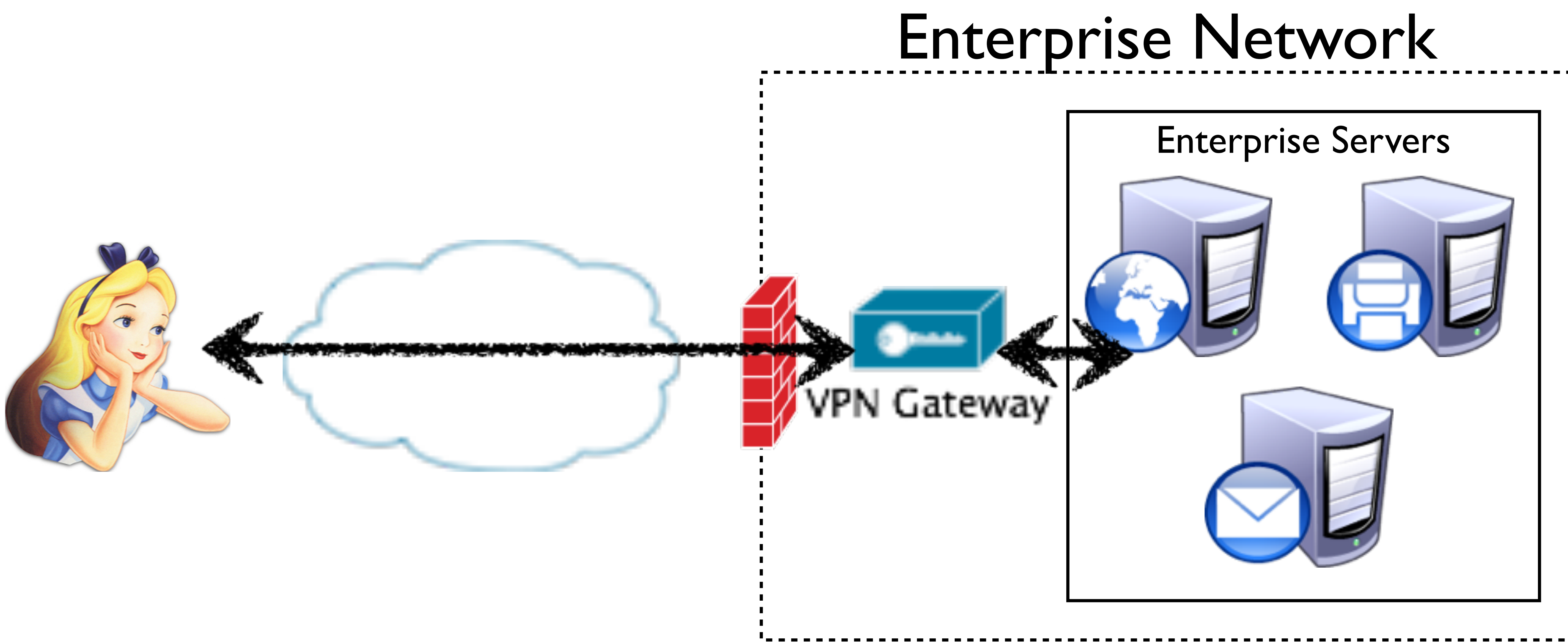
Work from home



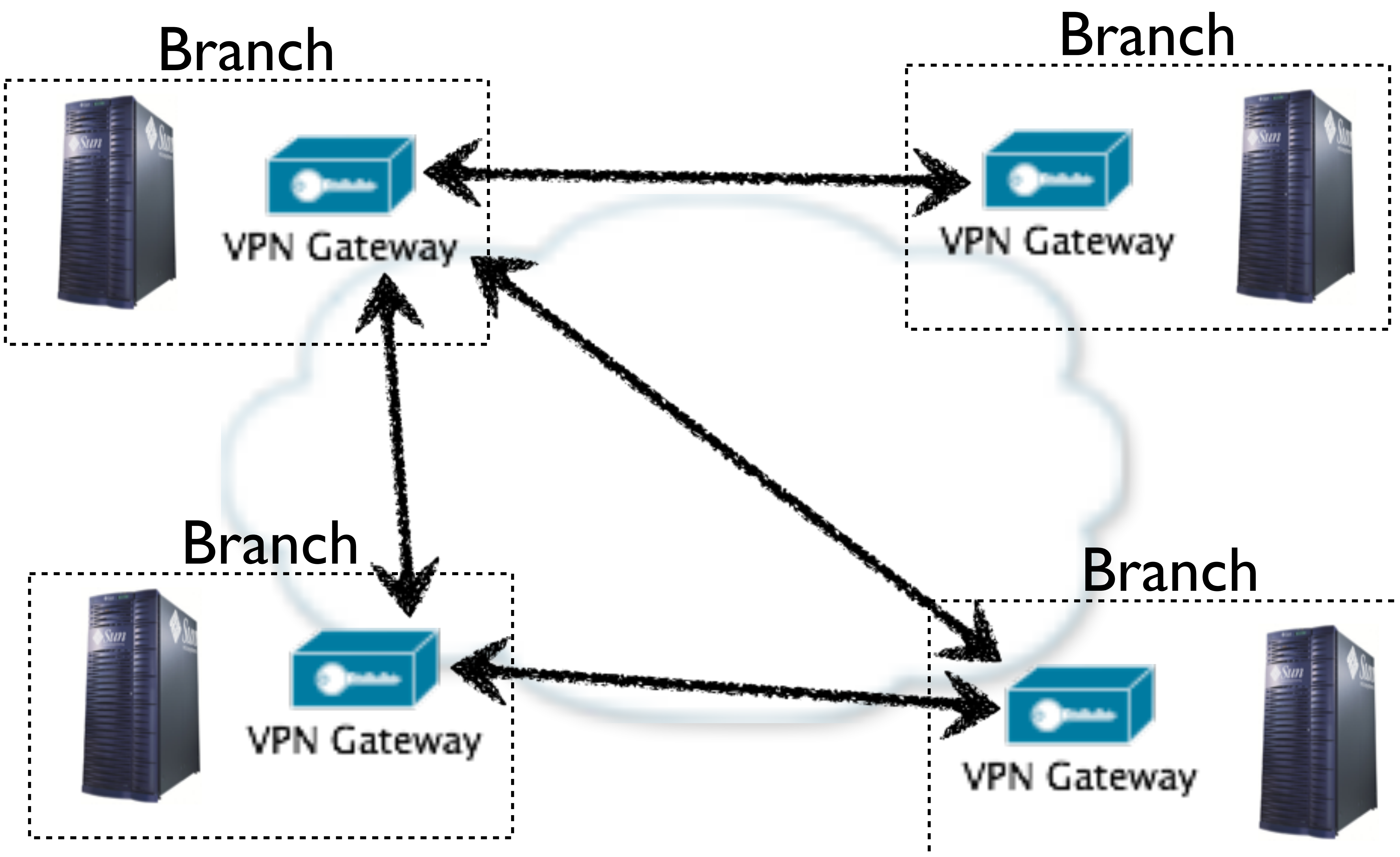
Virtual Private Networks (VPNs)

- Provides secure access to private network over public links
  - Often, goal is to provide access to corporate network (intranet) from outside (Internet)
  - Or, logically join physically separated networks
- Achieves some combination of:
  - Confidentiality
  - Integrity
  - Mutual authentication

Telecommuter VPNs: Client-to-Gateway

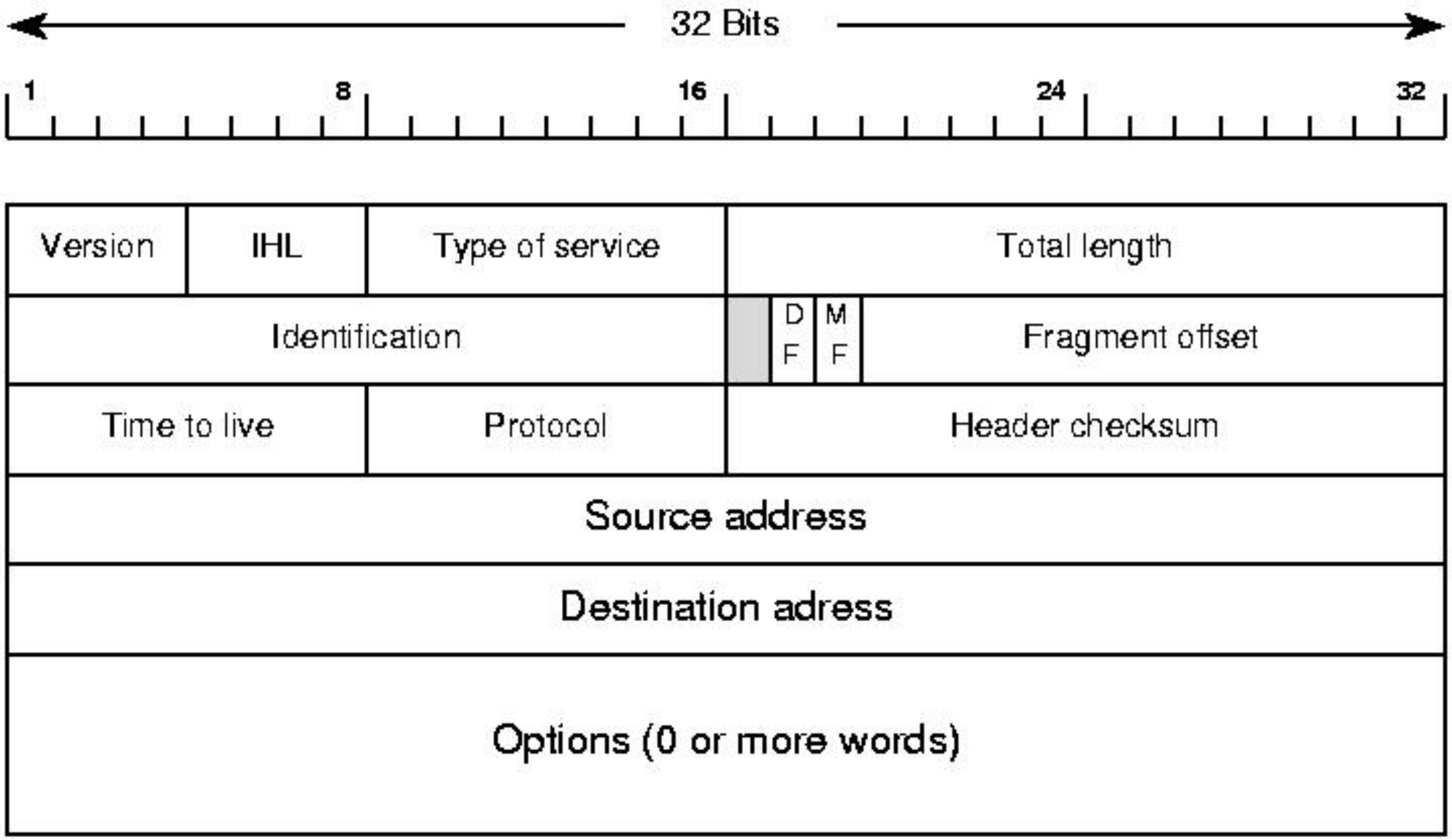


Gateway-to-Gateway VPNs

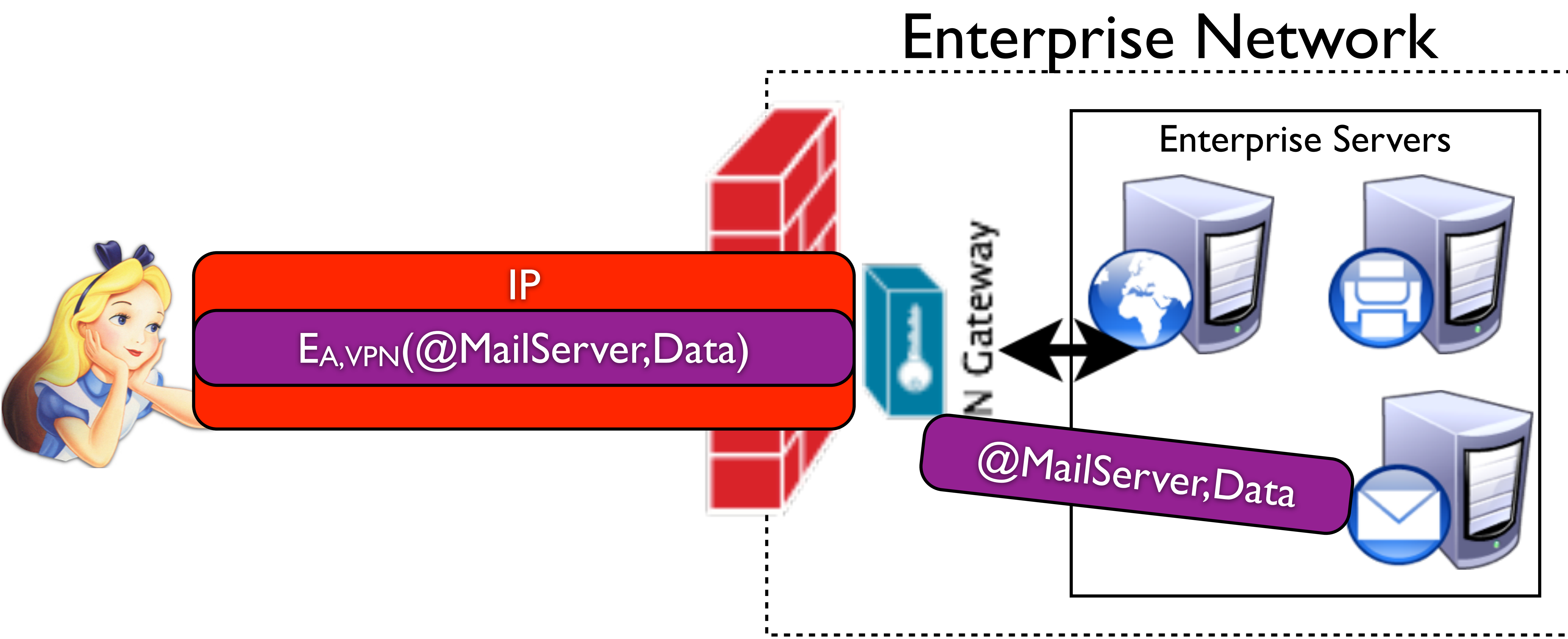


How do we build VPNs?

We can't rebuild the Internet



VPN Tunneling



Plan for today

- Wireless Review
- Virtual Private Networks
  - Overview
  - Protocol - IPsec
    - Key Management
    - Packet Processing

IPsec (not IPSec!)

- Host level protection service
  - IP-layer security (below TCP/UDP)
  - De-facto standard for host level security
  - Developed by the IETF (over many years)
  - Available in most operating systems/devices
    - E.g., Windows, OS X, Linux, BSD*, …
  - Not a single protocol; IPsec is a protocol suite
    - Implements a wide range of protocols and cryptographic algorithms
- ***Selectively*** provides ….
  - Confidentiality, integrity, authenticity, replay protection, DoS protection

"The spelling **IPsec** is preferred and used throughout this and all related IPsec standards. **All other capitalizations of IPsec (e.g., IPSEC, IPSec, ipsec) are deprecated.**"

Source: RFC 4301 **Security Architecture for the Internet Protocol** (December 2005)
https://datatracker.ietf.org/doc/html/rfc4301

IPsec (not IPSec!)

- Host level protection service
  - IP-layer security (below TCP/UDP)
  - De-facto standard for host level security
  - Developed by the IETF (over many years)
  - Available in most operating systems/devices
    - E.g., Windows, OS X, Linux, BSD*, …
  - Not a single protocol; IPsec is a protocol suite
    - Implements a wide range of protocols and cryptographic algorithms
- ***Selectively*** provides ….
  - Confidentiality, integrity, authenticity, replay protection, DoS protection

IPsec Protocol Suite

Policy/ Configuration Management	Key Management	Packet Processing
(SPS) Security Policy System	Manual	(ESP) Encapsulating Security Payload
	(IKE) Internet Key Exchange	(AH) Authentication Header

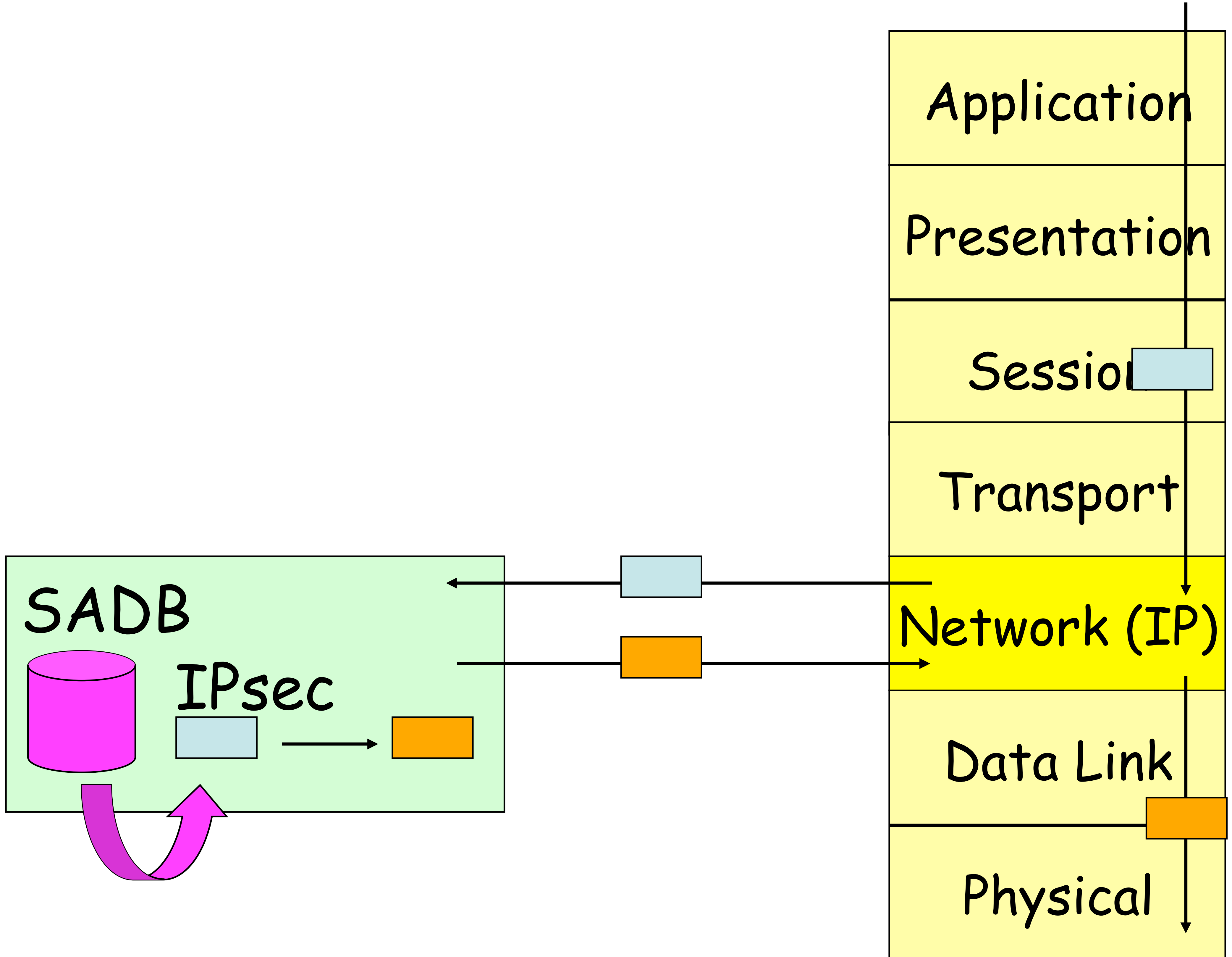
Key Management

- Two options:
  - Manual: use pre-shared secrets; or
  - Internet Key Exchange (IKE)

Internet Key Exchange (IKE)

- Two phase protocol used to establish parameters and keys for session
  - **Phase 1**: authenticate peers, establish secure channel via Diffie-Hellman key exchange
  - **Phase 2:** negotiate parameters, establish a **security association (SA)**
- The SA defines algorithms, keys, and policy used to secure the session for a unidirectional traffic flow
  - Pairing requires two SAs -- one for each direction
  - SAs stored in host's Security Association Database (SADB)
    - Each gateway may define policies for each SA
    - Policies stored in the SADB

IPsec: Packet Handling



Internet Key Exchange
Harkins and Carrel, RFC2409, Nov. 1998

- Phase 1: Key Exchange (Simplified)
  1. Initiator sends list of supported crypto algos to responder
  2. Responder chooses crypto algo from sender's list
  3. Initiator sends first half of DH exchange and a $nonce_I$ to responder
  4. Responder sends second half of DH exchange, and a $nonce_R$ to initiator
  5. Initiator sends its id, its cert, and a sig, all encrypted using key derived from previously exchanged messages
  6. Responder sends its id, its cert, and a sig, all encrypted using key derived from previously exchanged messages

Internet Key Exchange

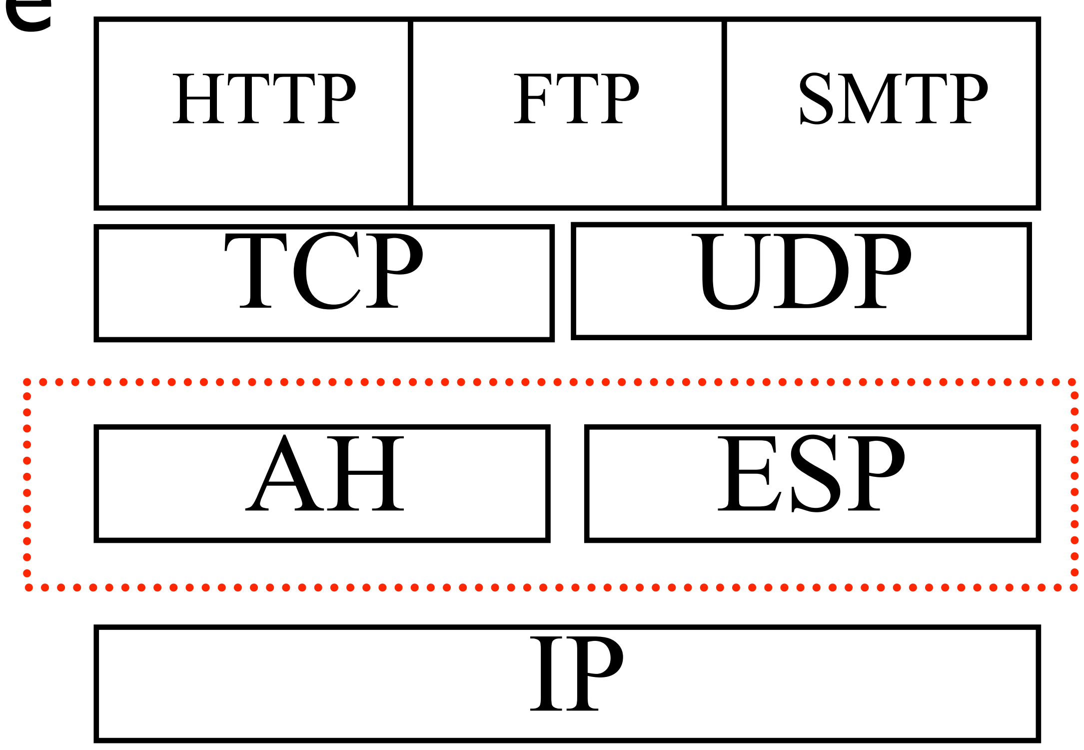
- Phase II: Security Associations
  - Using secure channel, establish at least 2 security associations:
    - inbound
    - outbound

IPsec Protocol Suite

Policy/ Configuration Management	Key Management	Packet Processing
(SPS) Security Policy System	Manual	(ESP) Encapsulating Security Payload
	(IKE) Internet Key Exchange	(AH) Authentication Header

IPsec and the IP protocol stack

- IPsec puts the two main protocols in between IP and the other protocols
  - **AH: Authentication Header**
  - **ESP: Encapsulating Security Payload**
- Other functions provided by external protocols and architectures



Authentication Header

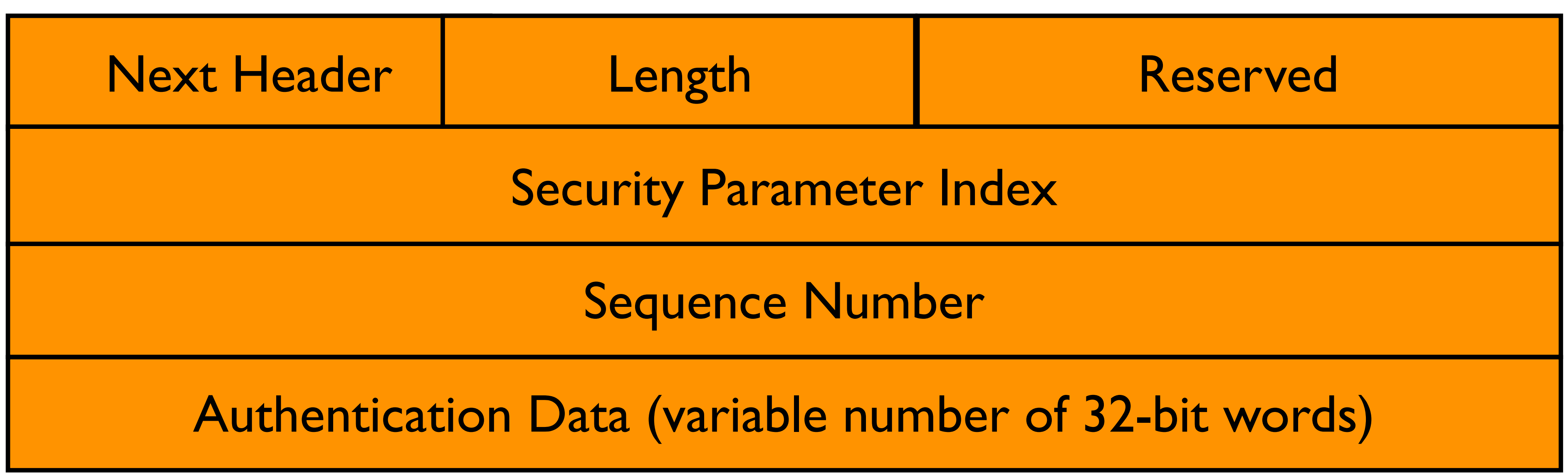
Authentication Header (AH)

- Provides **authenticity** and **integrity**
  - via HMAC
  - over immutable IP headers and data
- Advantage: the authenticity of data and IP header information is protected

IPsec AH Packet Format

IPv4 AH Packet Format

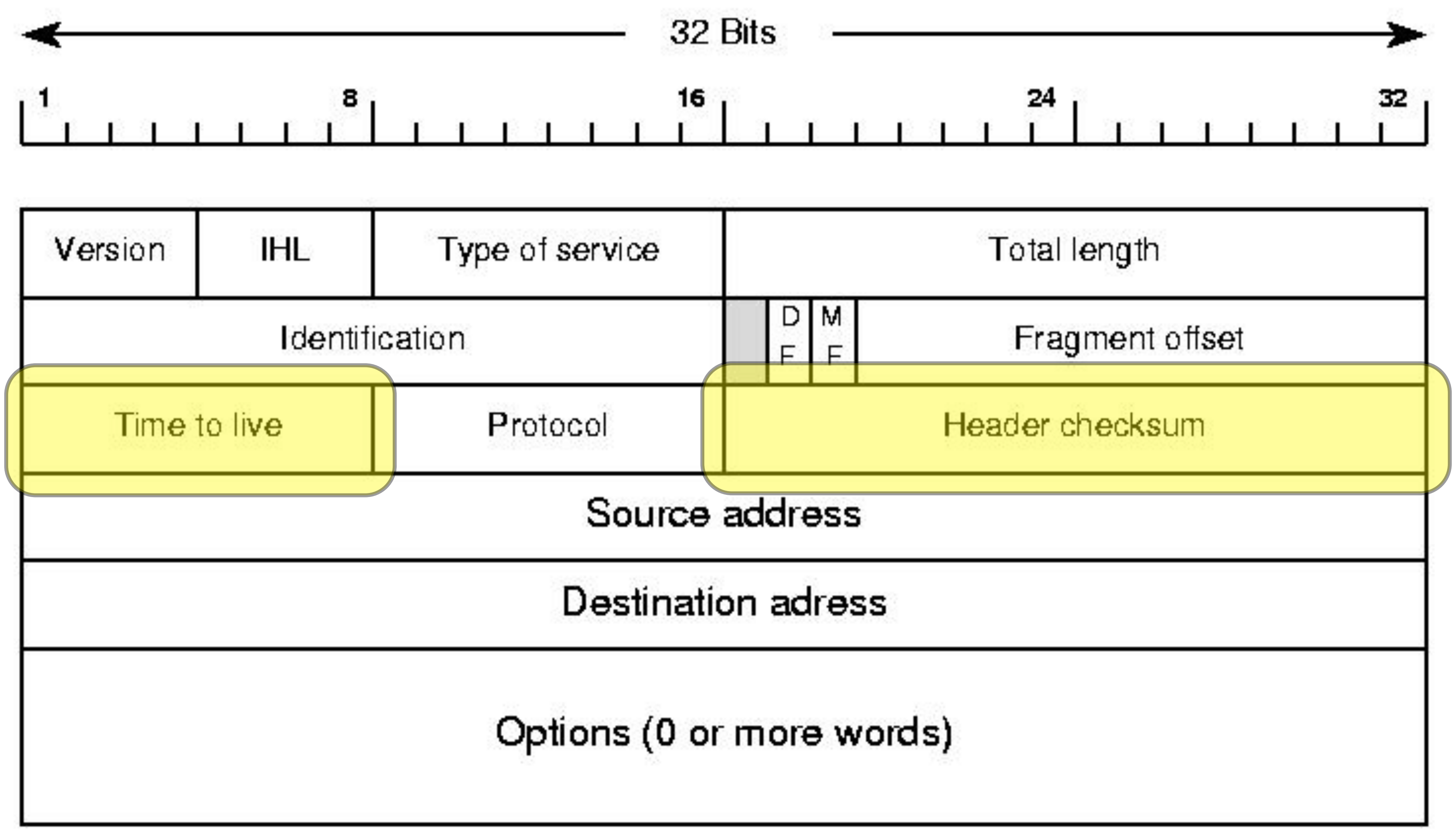
AH Header Format



Authentication Header (AH)

- Provides **authenticity** and **integrity**
  - via HMAC
  - over immutable IP headers and data
- Advantage: the authenticity of data and IP header information is protected
- Replay protection via AH sequence numbers
  - note that this replicates some features of TCP
- Disadvantage: the set of immutable IP headers isn't necessarily fixed
  - **For example?**

Mutable fields



IPsec Authentication

- **SPI:** (spy) identifies the SA for this packet
  - Type of crypto checksum, how large it is, and how it is computed
- Authentication data
  - Hash of packet contents include IP header as specified by SPI
  - Treat mutable fields (TTL, header checksum) as zero
  - Keyed MD5 Hash is default

Authentication Header (AH)

- Provides **authenticity** and **integrity**
  - via HMAC
  - over immutable IP headers and data
- Advantage: the authenticity of data and IP header information is protected
- Replay protection via AH sequence numbers
  - note that this replicates some features of TCP
- Disadvantage: the set of immutable IP headers isn't necessarily fixed
  - **For example?**
- Confidentiality of data is *not* preserved

Encapsulating Security Payload

Encapsulating Security Payload (ESP)

- Confidentiality, authenticity, and integrity
  - via encryption and HMAC
  - over IP payload (data)

ESP Packet Format

IPv4 ESP Packet Format

← Unencrypted →			← Encrypted →
IP Header	Other IP Headers	ESP Header	Encrypted Data

ESP Header Format

Security Parameter Identifier (SPI)
Opaque Transform Data, variable length

ESP Format

Security Parameters Index (SPI)
Initialization Vector (optional)
Replay Prevention Field (incrementing count)
Payload Data (with padding)
Authentication checksum

Encapsulating Security Payload (ESP)

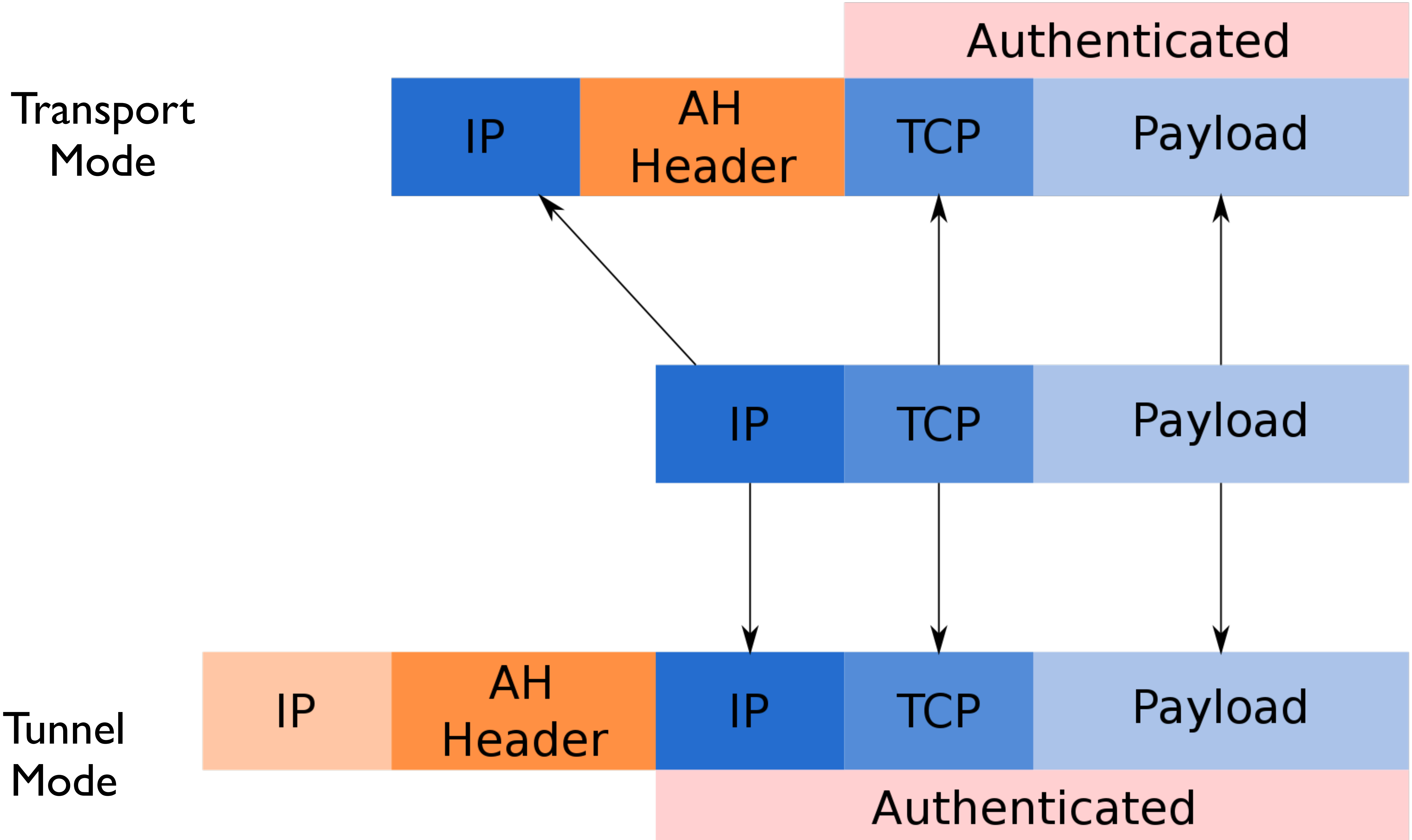
- Confidentiality, authenticity, and integrity
  - via encryption and HMAC
  - over IP payload (data)
- Advantage: encapsulated packet is fully secured
- Use "null" encryption to get authenticity/integrity only
- Note that the TCP/UDP ports are hidden when encrypted
  - good: better security, less is known about traffic
  - bad: impossible for FW to filter/traffic based on port
- Cost: can require many more resources than AH

Modes of Operation

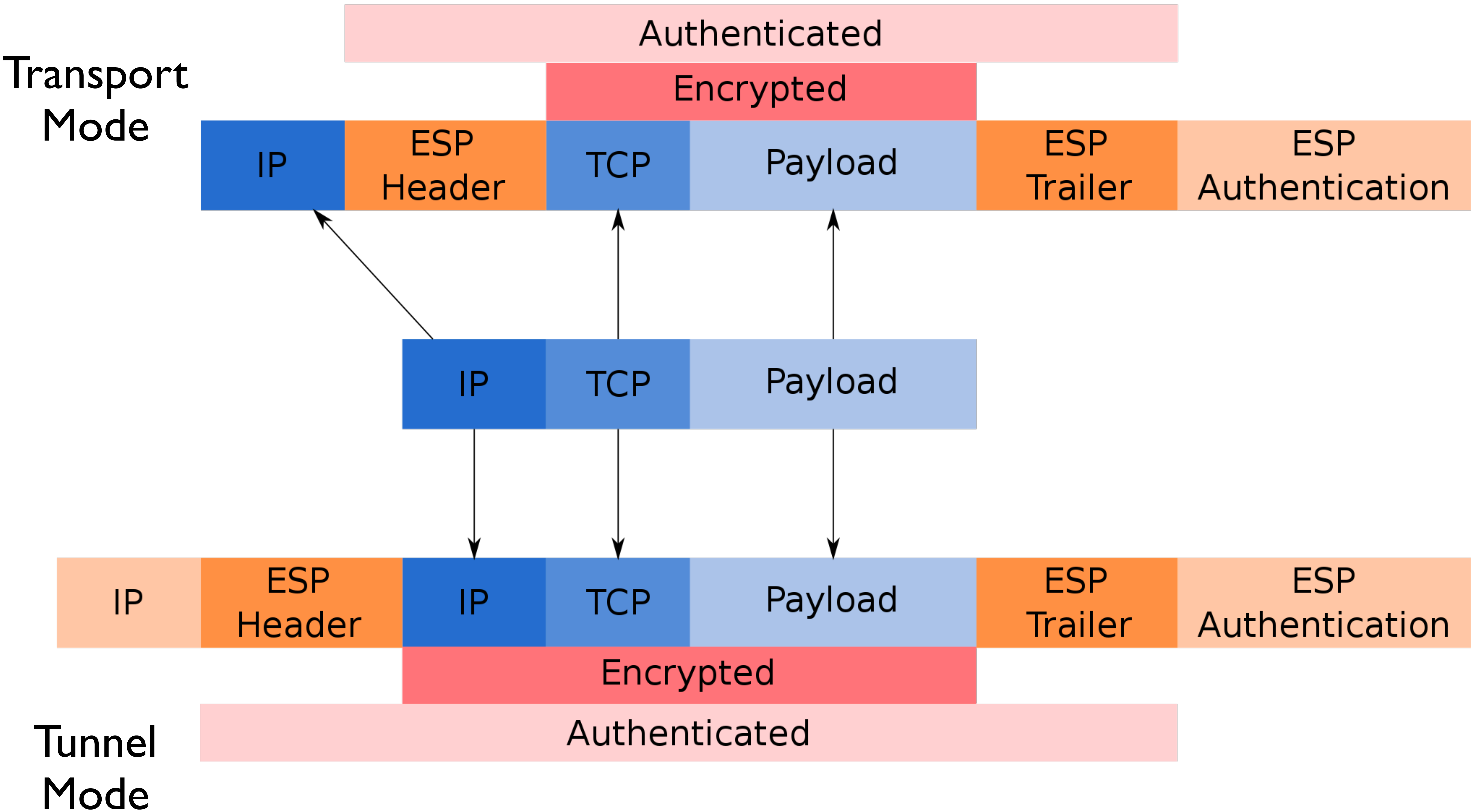
Modes of Operation

- **Transport**: the payload is (optionally) encrypted and the *non-mutable* fields are integrity verified (via MAC)
- **Tunnel**: each packet is completely encapsulated (and optionally encrypted) in an outer IP packet
  - Hides/protects not only data, but some routing information

Authenticated Header



Encapsulating Security Payload



Practical Issues and Limitations

- IPsec implementations
  - Large footprint
    - resource poor devices are in trouble
    - New standards to simplify (e.g, JFK, IKE2)
  - Slow to adopt new technologies
  - Configuration is extremely complicated/ obscure

Practical Issues and Limitations

- Issues
  - IPsec tries to be “everything for everybody at all times”
    - Massive, complicated, and unwieldy
  - Large-scale management tools are limited (e.g., CISCO)
  - Often not used securely (common pre-shared keys)

Plan for today

- Wireless Review
- Virtual Private Networks
  - Overview
  - Protocol - IPsec
    - Key Management
    - Packet Processing
  - Alternatives

Alternatives to IPsec

- **SSH Tunneling**: Tunnel packets over SSH connection
- **OpenVPN**: Tunnel traffic via SSL/TLS connections
- **Point-to-Point Tunneling Protocol (PPTP)**: Tunnel using Control (TCP) and Data (GRE) channels; mostly a Microsoft thing

SSH Tunneling

- Alice has an account on linux.cs.tufts.edu
- Alice wants to access page that is is only available to Tufts IP addresses
  - ... and Alice lives off campus
- `ssh -D9999 -NfCx linux.cs.tufts.edu`
  - run SOCKS server locally on port 9999, forwarding all traffic to linux.cs
  - If we tell our browser to use use localhost:9999 as our SOCKS proxy, everything from the browser goes through the tunnel

Summary

- Wireless Review
- Virtual Private Networks
  - Overview
  - Protocol - IPsec
    - Key Management
    - Packet Processing
  - Alternatives