Introduction to Networking

Goal:

1. To understand the basic underpinnings of network security.

Roadmap

1. Recapitulation: the 4-layers model
2. Basics on security

Recap: the 4-layers model

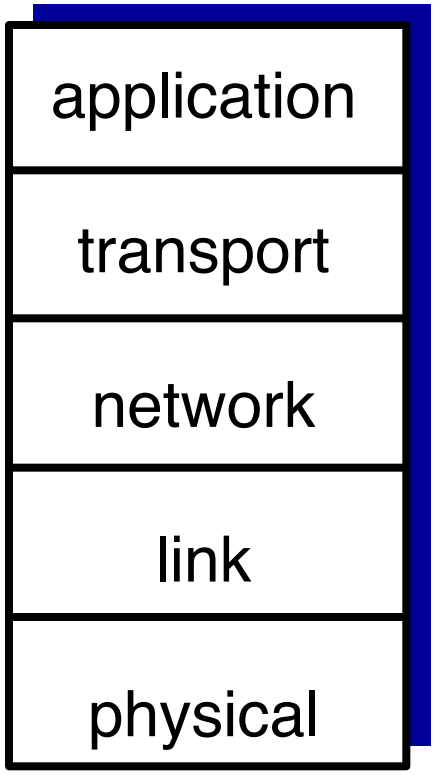
application: supporting network applications
- FTP, SMTP, HTTP, DNS

transport: process-process data transfer
- TCP, UDP

network: routing of datagrams from source to destination
- IP, routing protocols

link: data transfer between neighbouring network elements
- Ethernet, 802.111 (WiFi), PPP

physical: bits "on the wire"



Quiz - menti.com 5771249

1. A message from your friend arrives and your chat application displays a pop up notification

Select Network Layer...

2. A message arrives which states that your friend has closed the chat connection.

Select Network Layer...

3. A message gets sent from your computer to your router.

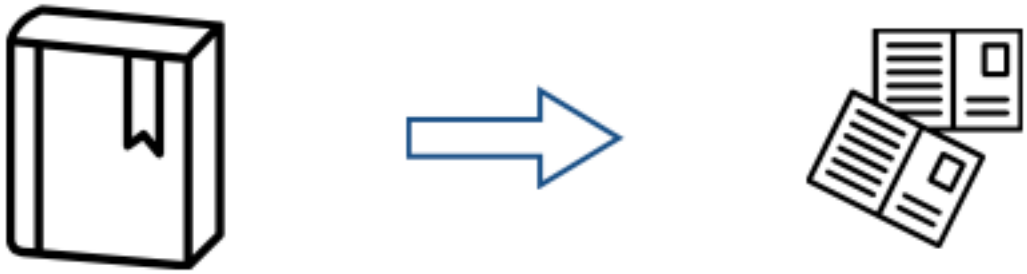
Select Network Layer...

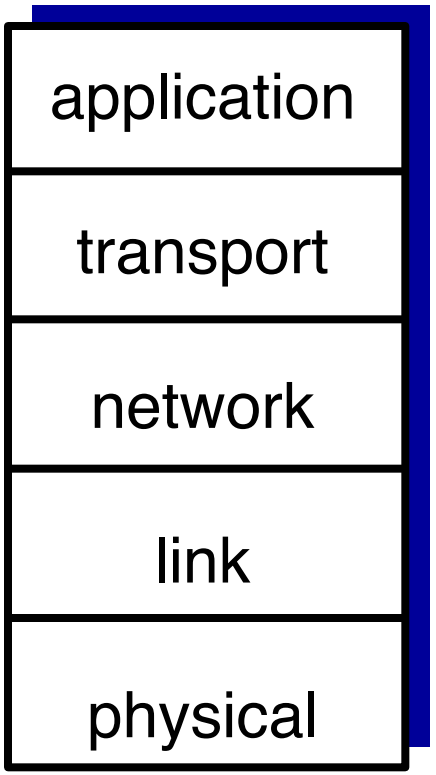
4. A message gets sent from your computer to your router to Google's server.

Select Network Layer...

How are packets sent/delivered?

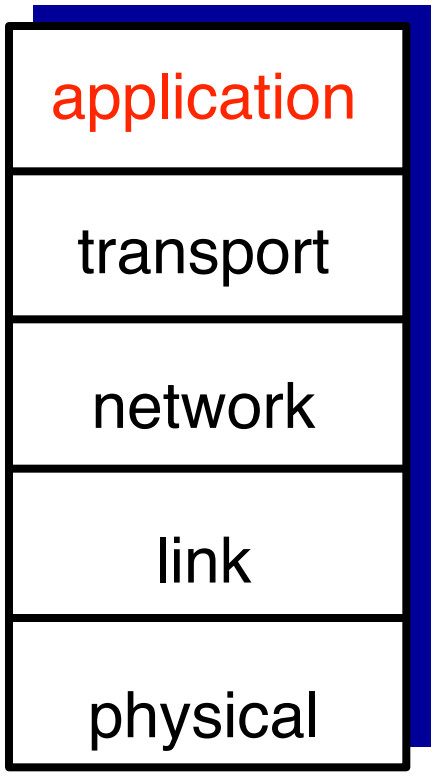
- messages are just packets: an array of bytes of data
- delivering a message is like sending a postcard
  - the message is split into multiple packets
  - in order to deliver a message you need to send many postcards/packets





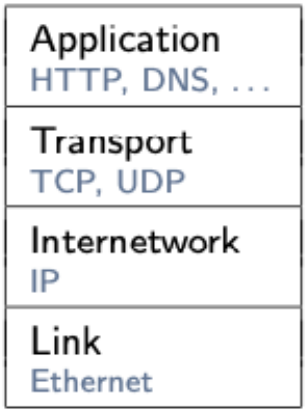
Postcard - application layer

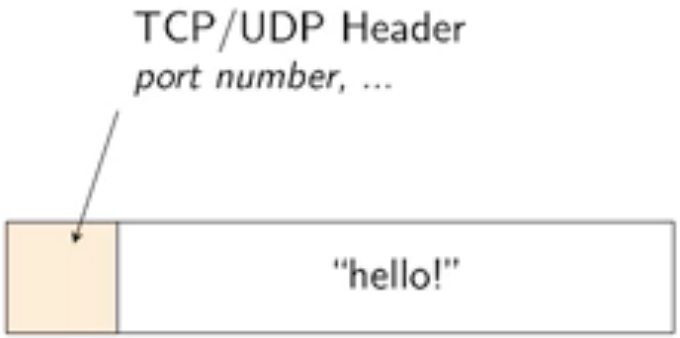
- Example:
  - putting a postcard into a bag and bringing it to the post office.
  - we want to send a "hello" message to a friend
    - application layer builds a hello packet, which is subsequently sent to transport —> network —> link layers

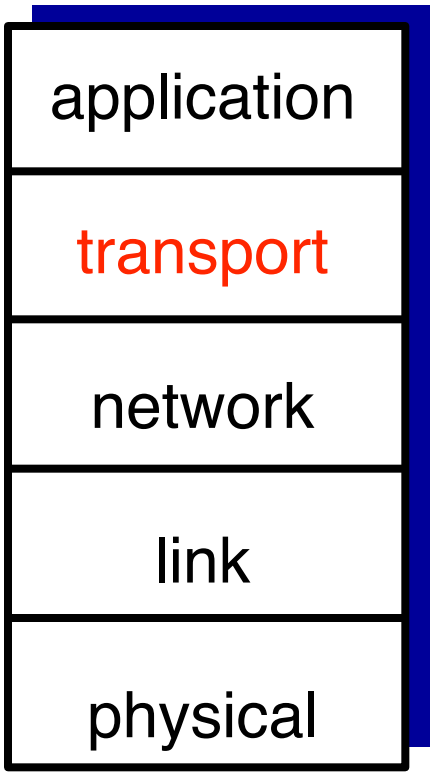


Postcard - transport layer

- the transport layer ensures the message is sent to the right application in the destination machine application
  - transport layer adds a **TCP** or **UDP** header to the message
  - i.e., websites usually listen on port 443; the recipient's name on the postcard.

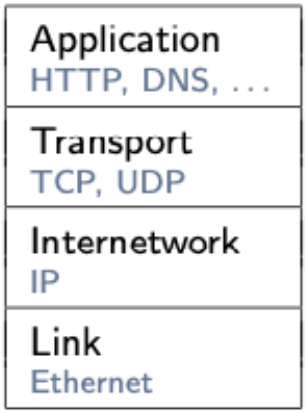


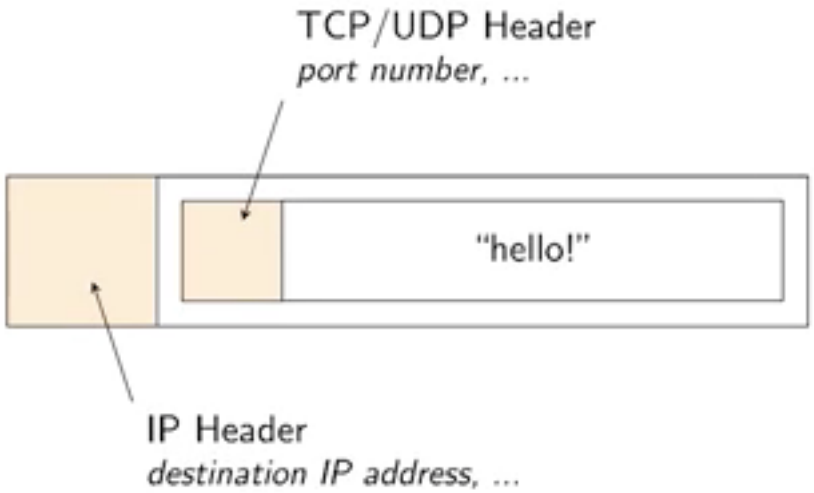


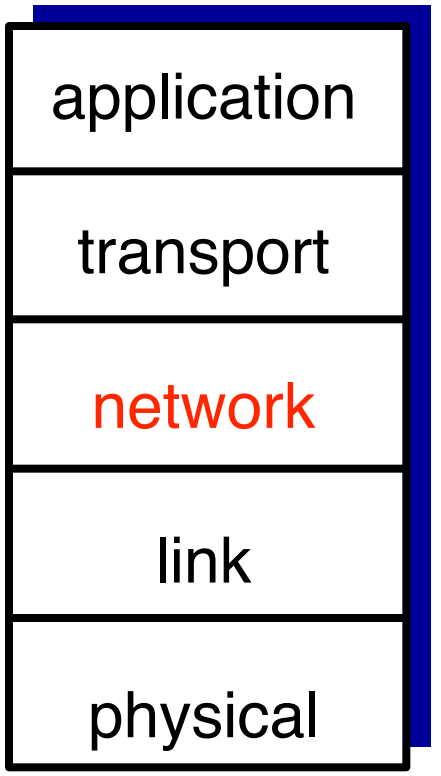


Postcard - network layer

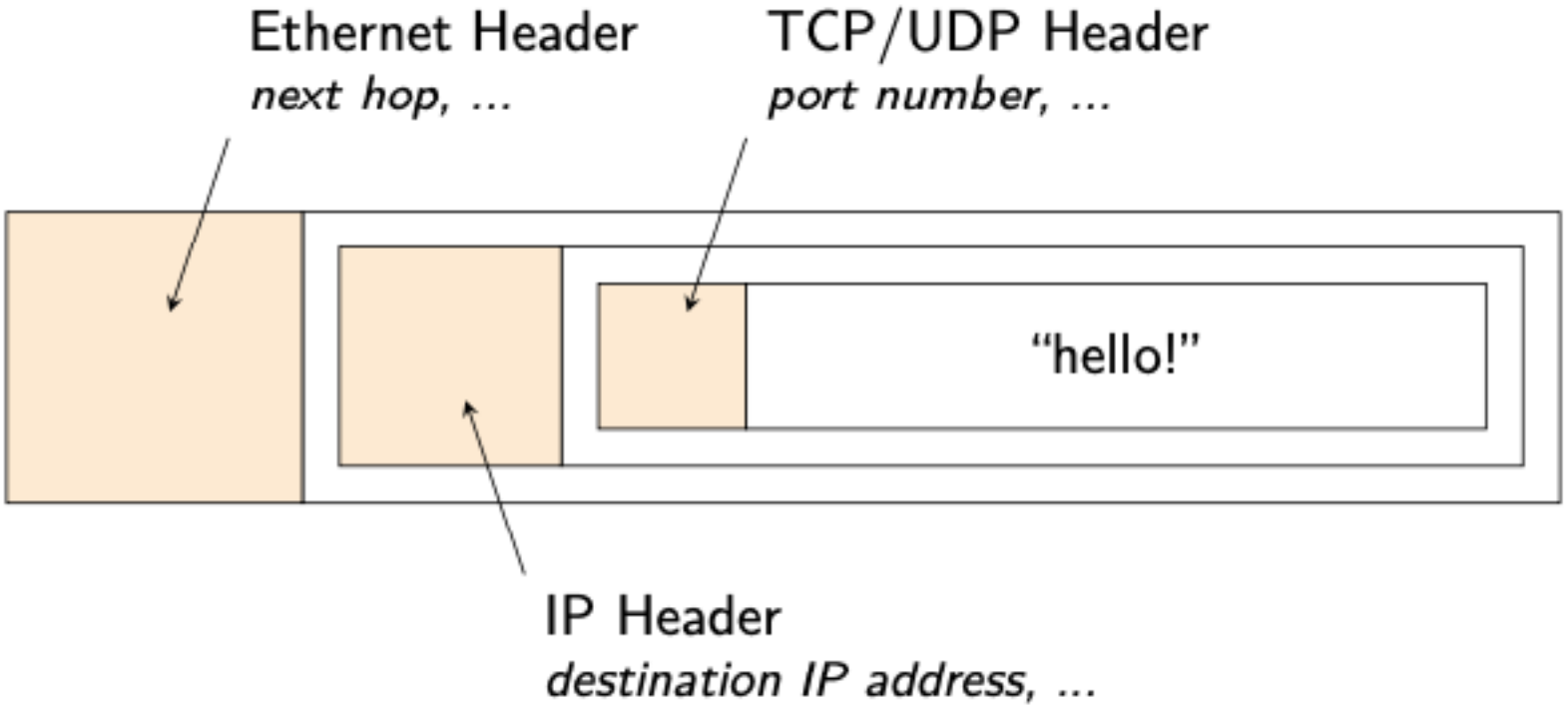
- the network layer adds an IP header
- for instance, the street address where the postcard will be sent







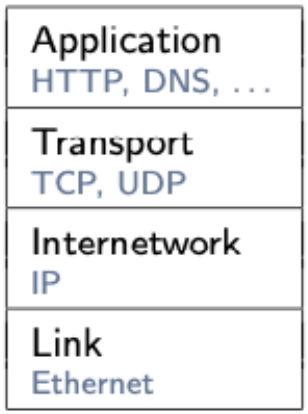
packets

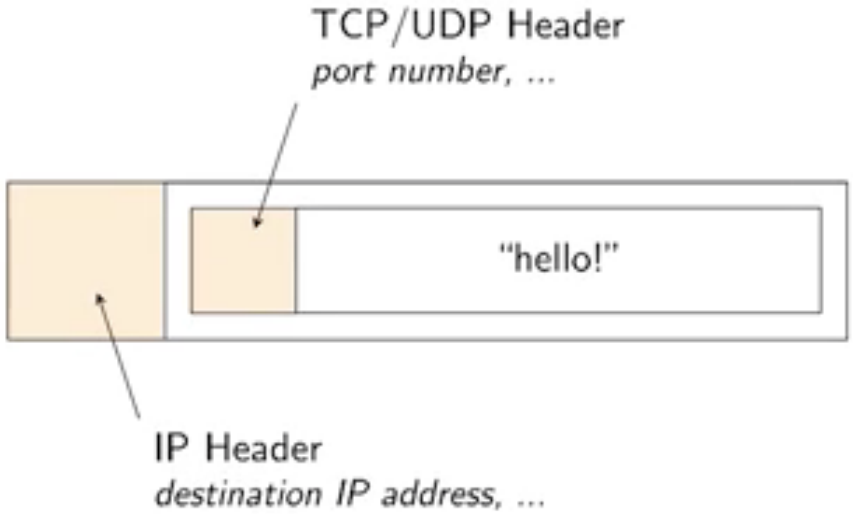


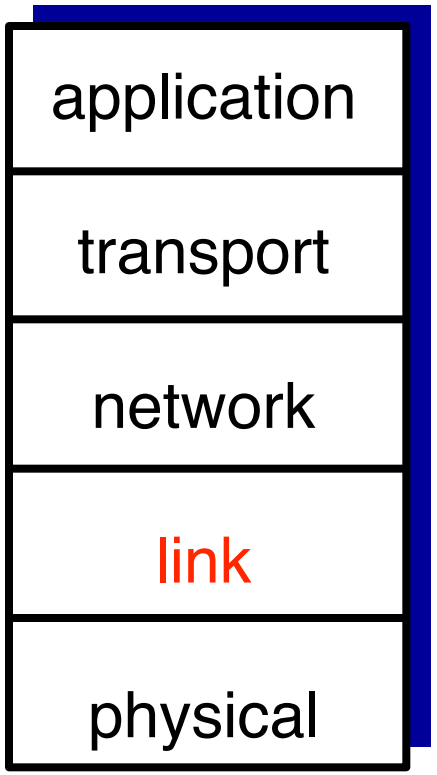
Application HTTP, DNS, ...
Transport TCP, UDP
Internetwork IP
Link Ethernet

Postcard - link layer

- link-layer adds an ethernet header: information on the next hop (router/ machine) to which the packet will be sent







Question

Question

Which of the following statements are true?

- ☐ The router will replace/modify the existing Ethernet header before forwarding a packet.
- ☐ The TCP header contains the packet's destination IP address.
- ☐ To forward a packet, the router needs to parse and understand the packet's TCP header.
- ☐ Your internet service provider can read the contents of your packets when they pass through their network.

Roadmap

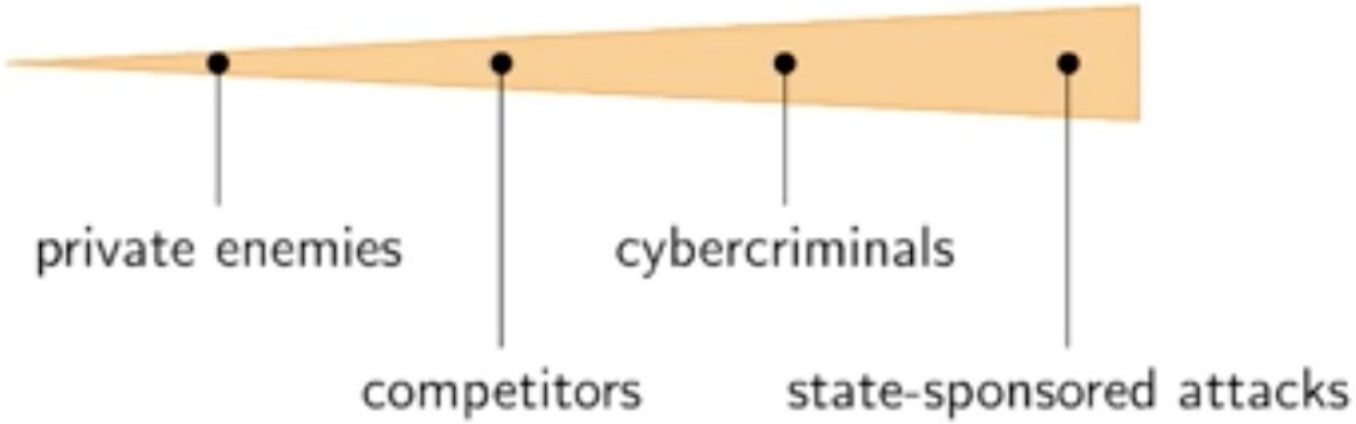
1. Recapitulation: the 4-layers model
2. Basics on security

Security: CIA protection goals

- (C) Confidentiality - messages remain private - you don't want anyone to know the messages you wrote on your postcard
- (I) Integrity - messages remain unmodified - no one tampered with your messages, e.g., no one changed the address on your postcard.
- (A) Availability - messages can always be transmitted - you need a communication channel to be always available.

Threat model

- Who are my adversaries?
- What are my assets?
- Who will attack us?
- What are my protection goals?
- What are my capabilities?
- What are the attacker's capabilities?



Security of network protocols - Dolev-Yao

Adversary's capabilities:

- Observe, modify, drop, delay, forge, or replay messages.
- Falsify circumstances (e.g. redirect messages, use fake identities).
- Concurrent protocol executions

Security of network protocols - Dolev-Yao

Adversary's constraints:

- Trusted areas are secure.
- Cryptographic primitives have no vulnerabilities.
- Unable to guess keys.

Dolev-Yao model

You listen to a presentation about a new network protocol for online banking. After the talk, there is a lot of discussion going on. Check all remarks that are relevant under the Dolev-Yao model.

- ☐ The bank runs Windows on their servers. This will be insecure!
- ☐ Looks nice, but the NSA will break the encryption function and use this to spy on us.
- ☐ What happens if someone breaks into the bank's data center? They should use a blockchain instead!
- ☐ I don't think they properly protect against transaction replay.

CIA model

For each network capability, which protection goal is *directly* violated?

Only check one goal – the most directly violated one – per capability.

	Protection Goals		
Attacker Capability	Confidentiality	Integrity	Availability
Observe Packets	☐	☐	☐
Modify Packets	☐	☐	☐
Drop Packets	☐	☐	☐
Delay Packets	☐	☐	☐
Forge Packets	☐	☐	☐
Replay Packets	☐	☐	☐

Summary

- The 4-layer model
- The Dolev-Yao model