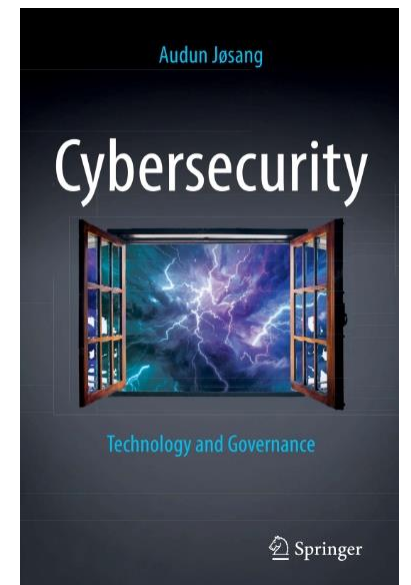


Chapter 6: Network Security

Cybersecurity: Technology and Governance

Audun Jøsang,

1st Edition, Springer Nature, 2024.

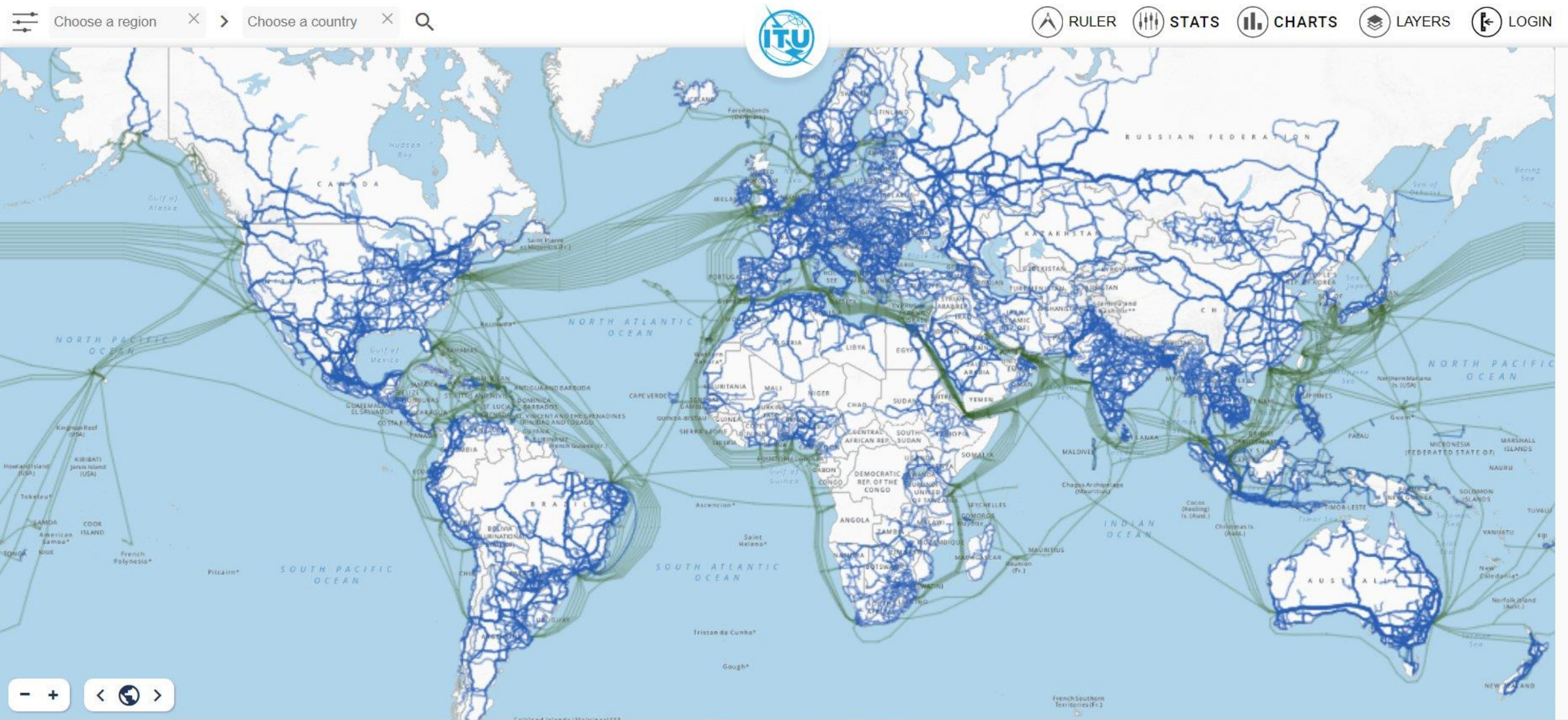


Overview

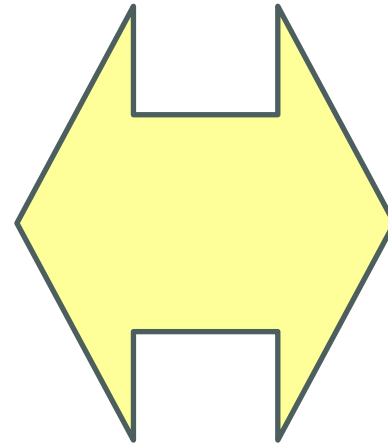
- Communication Security
 - The structure of the Internet
 - Network layer
 - Transport Layer Security (TLS)
 - IPSec (IP Layer Security)
- Computer network security
 - Firewalls
 - Intrusion Detection
 - TLS Inspection

The Physical Internet

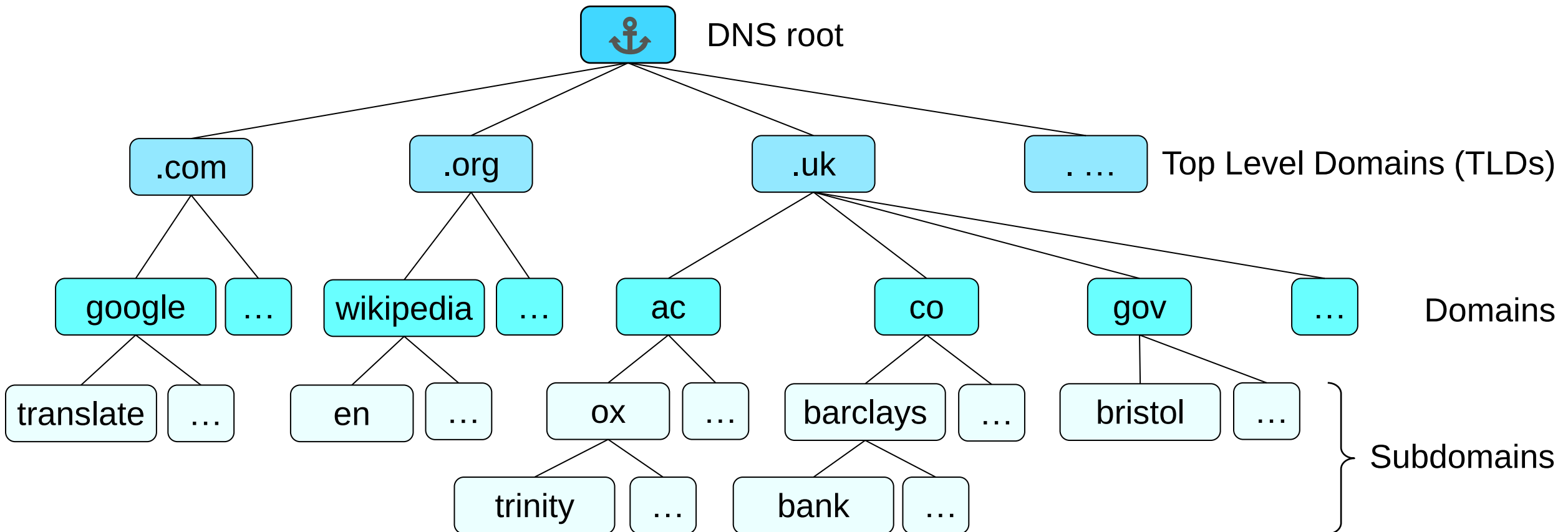
<https://bbmaps.itu.int/products>



Why not ITU?



DNS: The Domain Name System

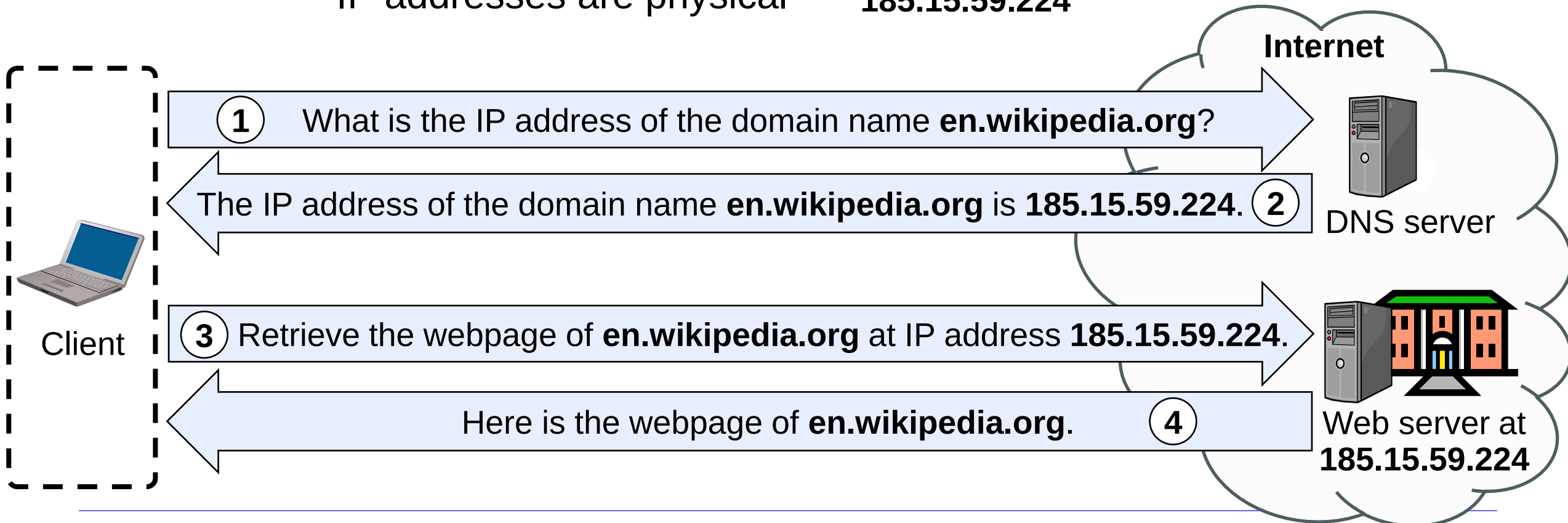


Domain names and IP addresses

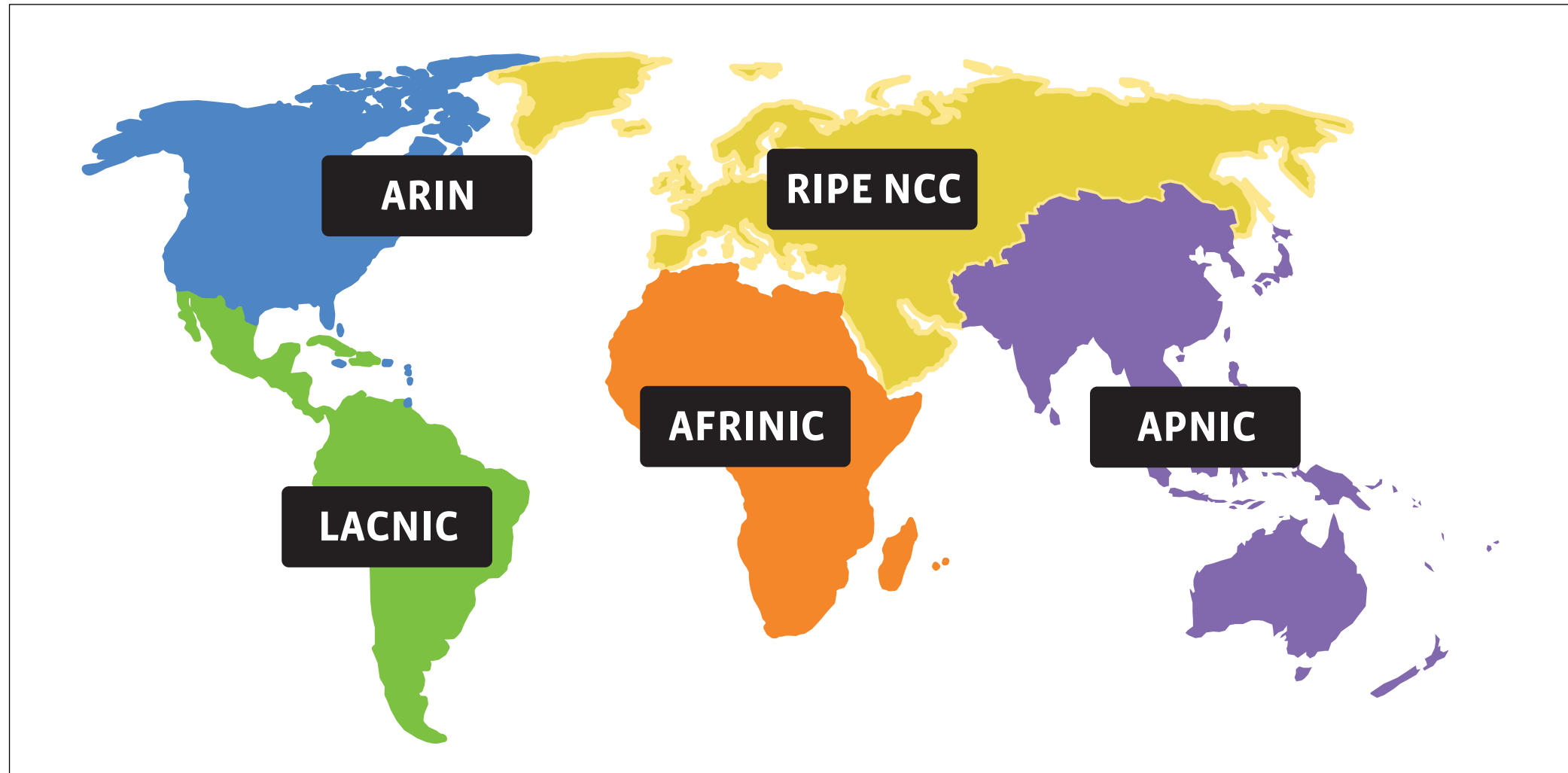
- Domain names are virtual **en.wikipedia.org**

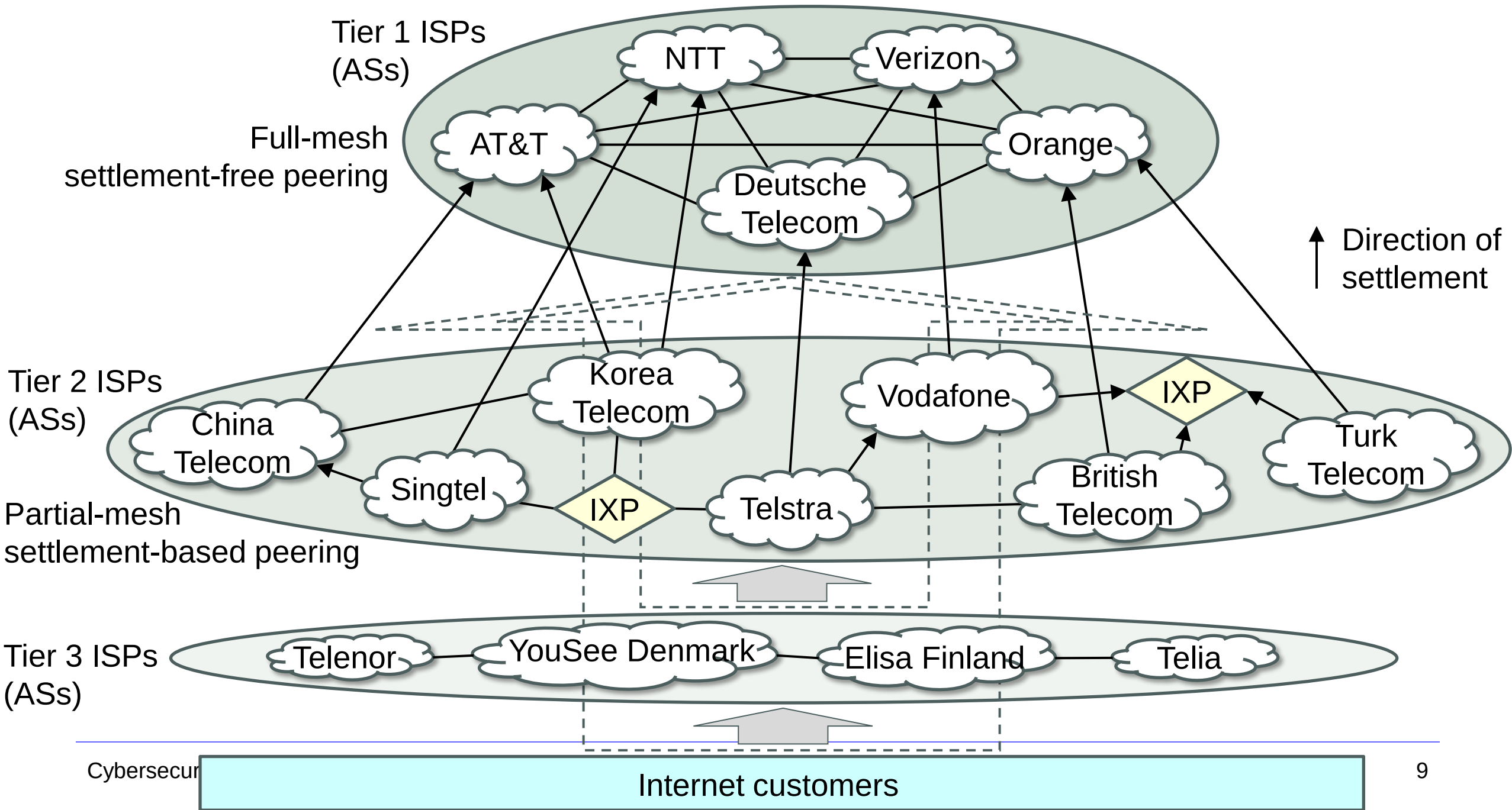


- IP addresses are physical **185.15.59.224**

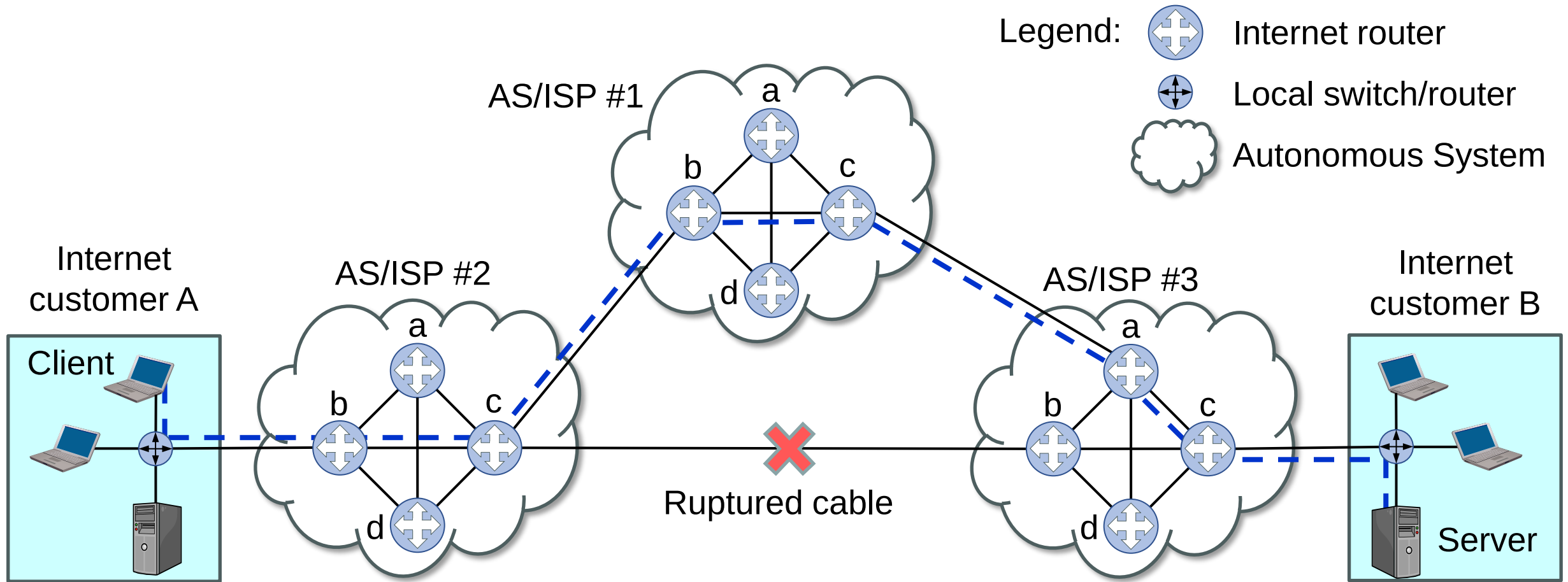


Assignment of IP address number ranges





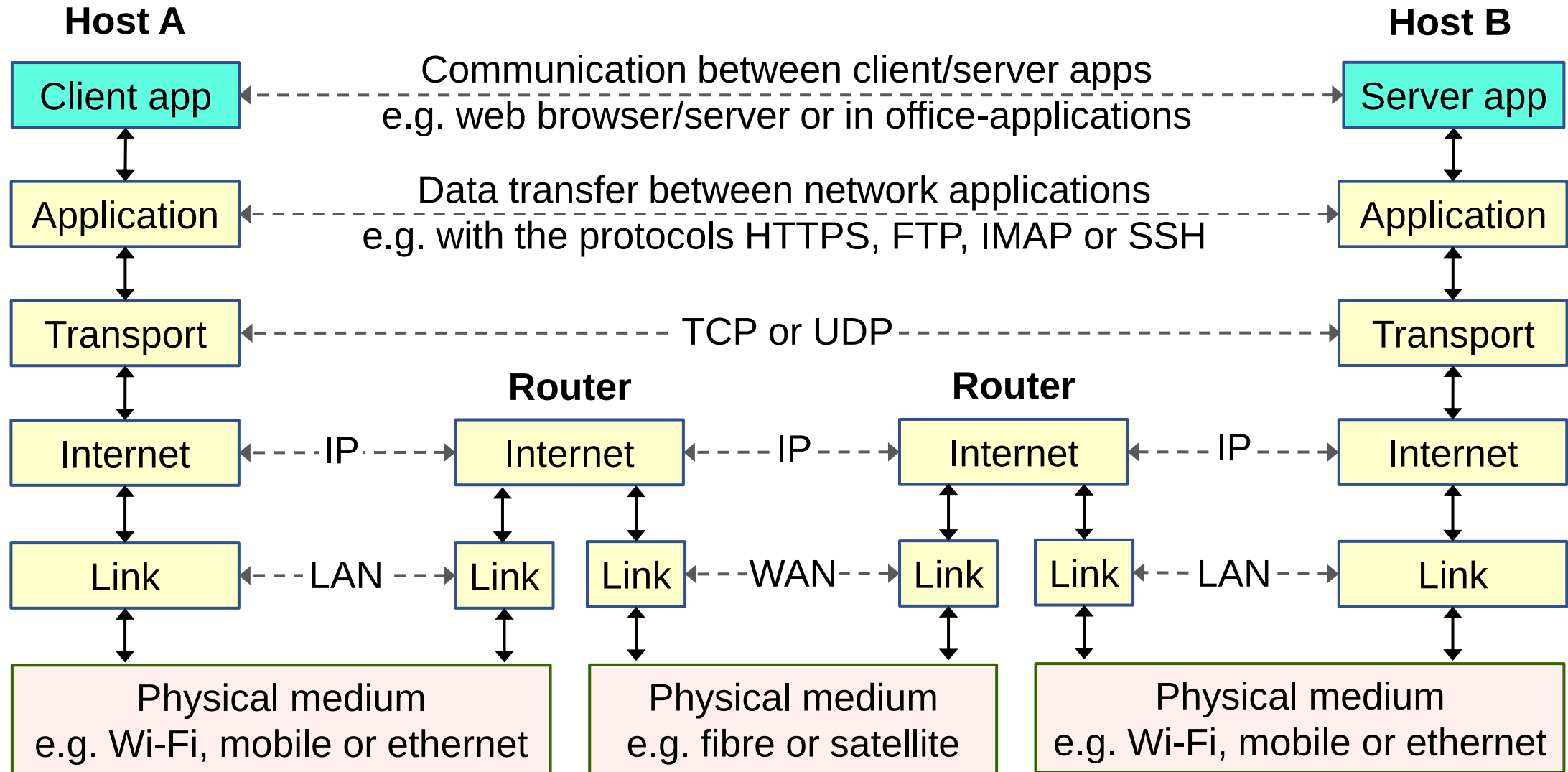
Internet routing



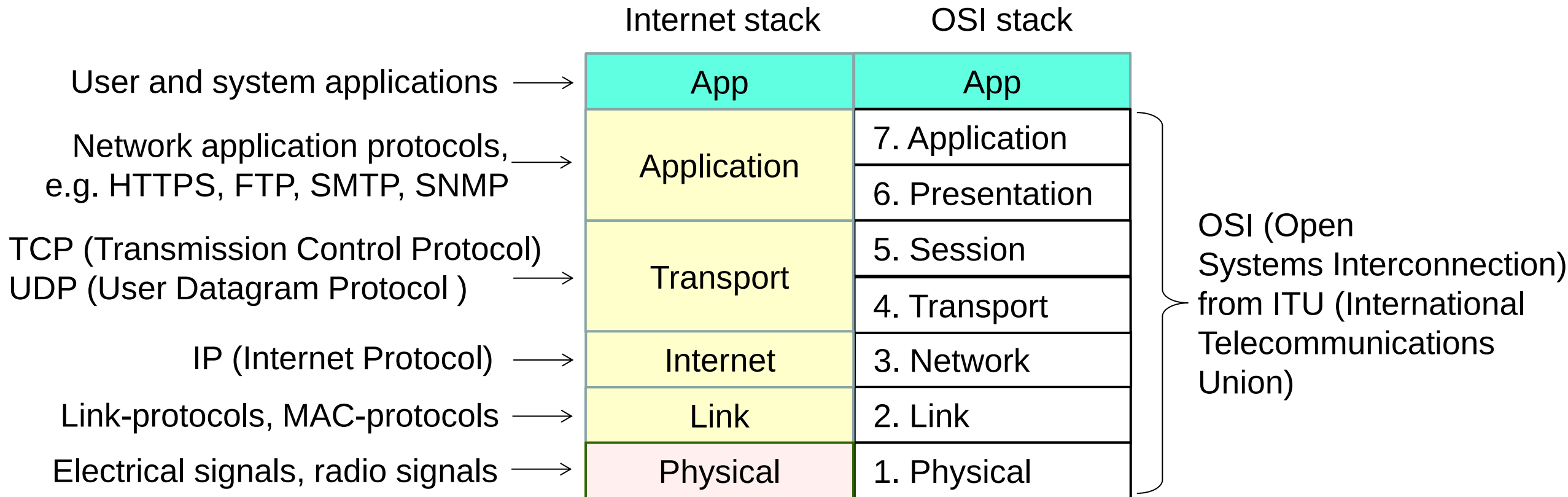
The Internet Stack

Legend

↕ Interface within the same node
←---→ Communication through network

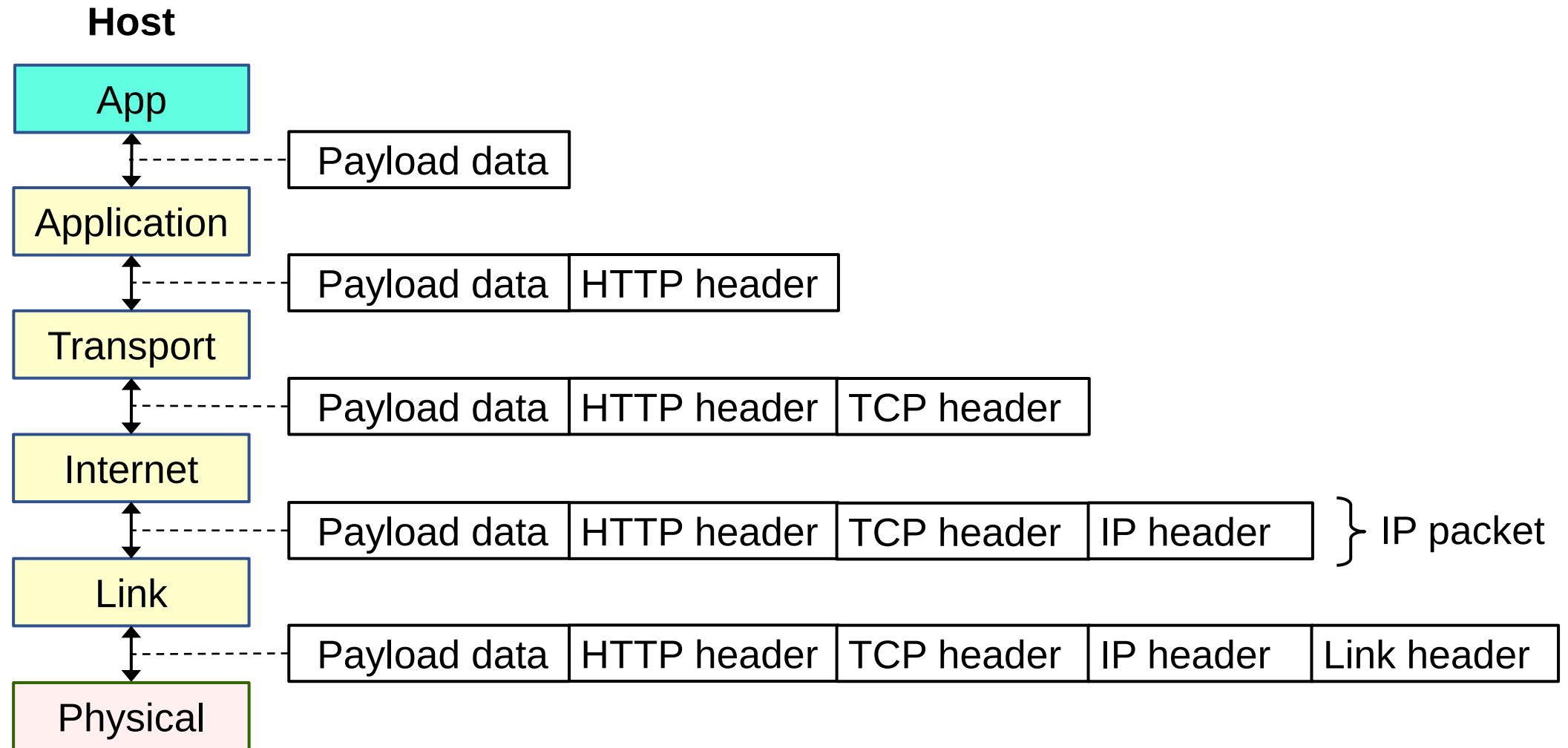


Protocol stack in the internet and the equivalent in OSI

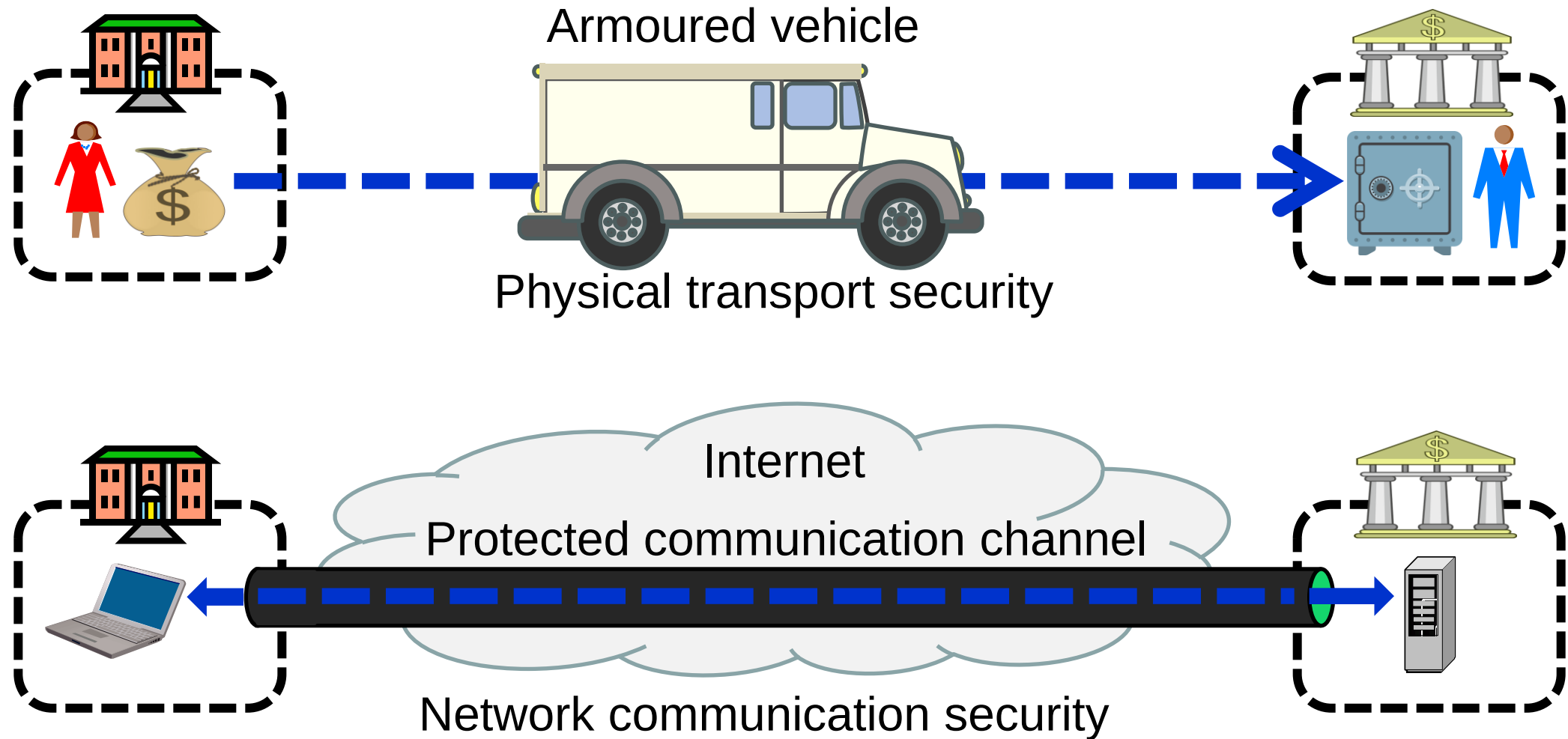


- OSI was a competitor to the internet in the period 1985-1995, but the internet eventually won

Packet layer hierarchy in the protocol stack



Analogy: Physical Transport and Communication Security



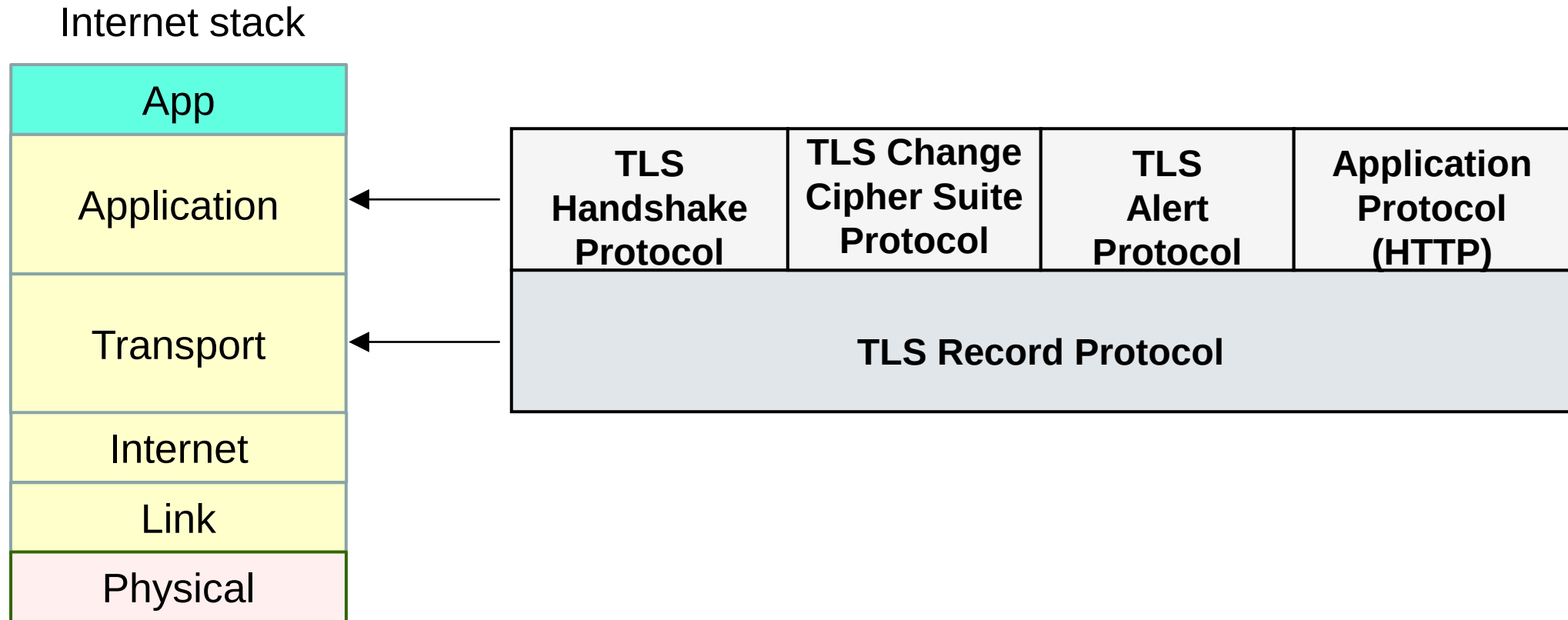
Security Protocols

- Many different security protocols for different purposes
 - Authentication, Integrity, Confidentiality
 - Key exchange
 - e-elections
- Examples: TLS and IPSEC
- Security protocols are surprisingly difficult to design without vulnerabilities!
 - Many vulnerabilities are discovered years later
 - ... some are never detected (or maybe only by threat actors)

TLS: Transport Layer Security

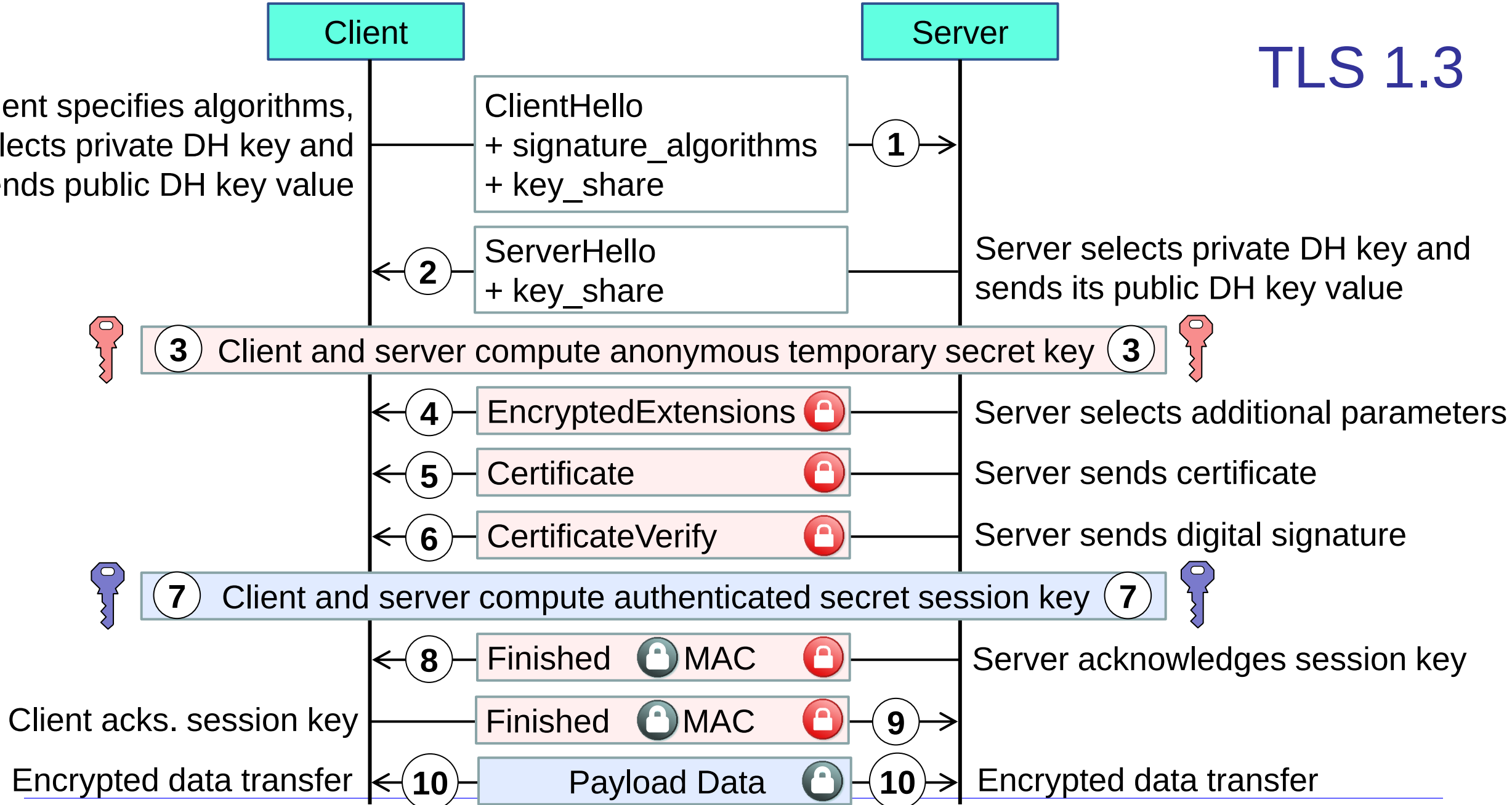
Formerly called SSL (Secure Sockets Layer)

TLS in the internet stack

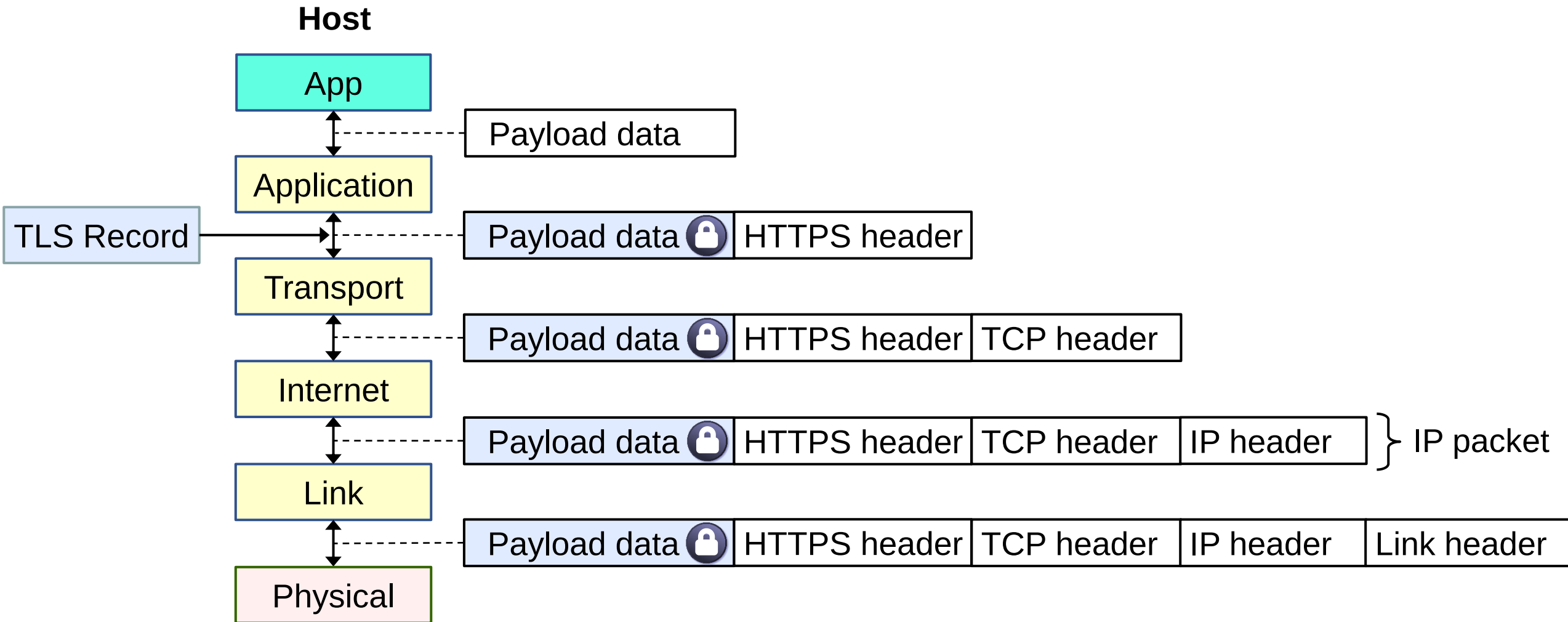


- TLS consists in reality of a set of protocols for different stages of a session

TLS 1.3



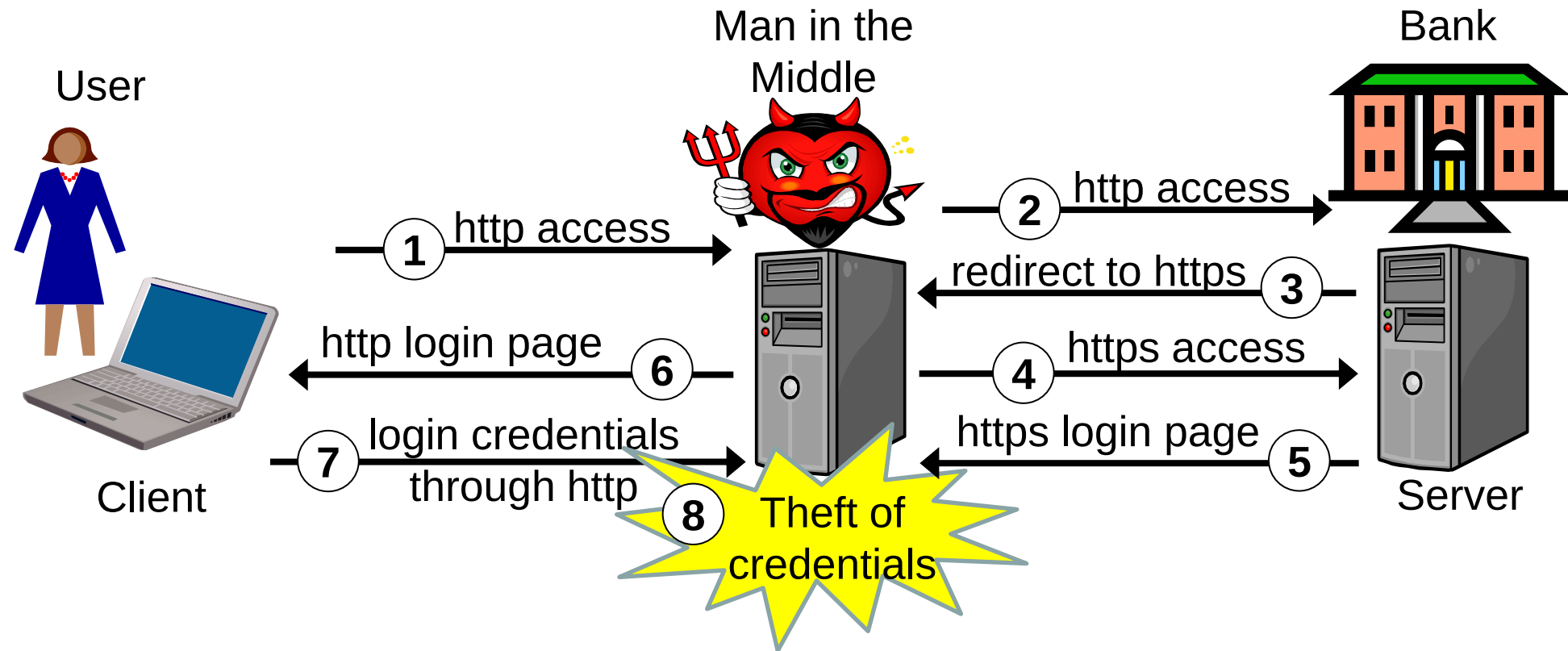
Encryption of payload data with TLS



TLS 1.3

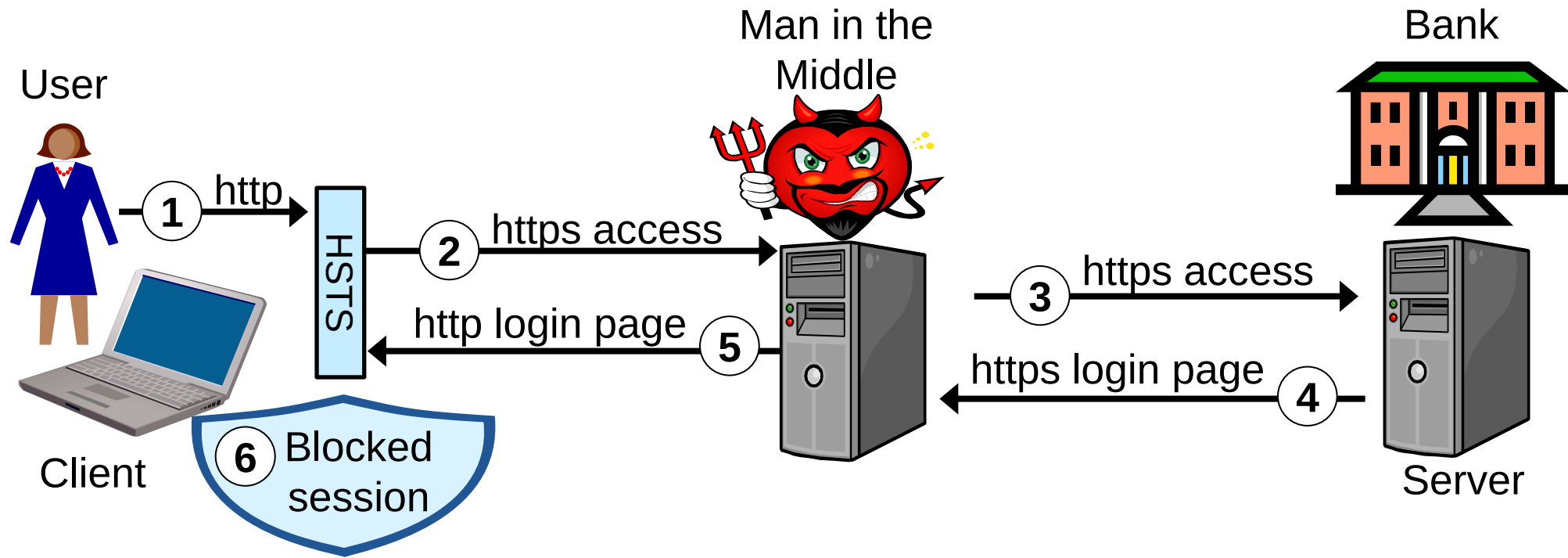
- Designed for speed in session key establishment
- Only needs one message round trip (back and forth) to establish session key
- Forward secrecy means that keys from previous sessions remain secret (not compromised) even if a long-term crypto key is compromised/leaked at some point in the future.
- In TLS, the server's private signing key is the long-term key.
- Compromise of the server's private key entails the violation of authenticity of the server from the time of the compromise, which is serious enough.
- Forward secrecy is achieved through the use of Diffie-Hellman.

TLS stripping attack



- There are different variations of the TLS stripping attack

HSTS to prevent TLS stripping (Hypertext Strict Transport Security)



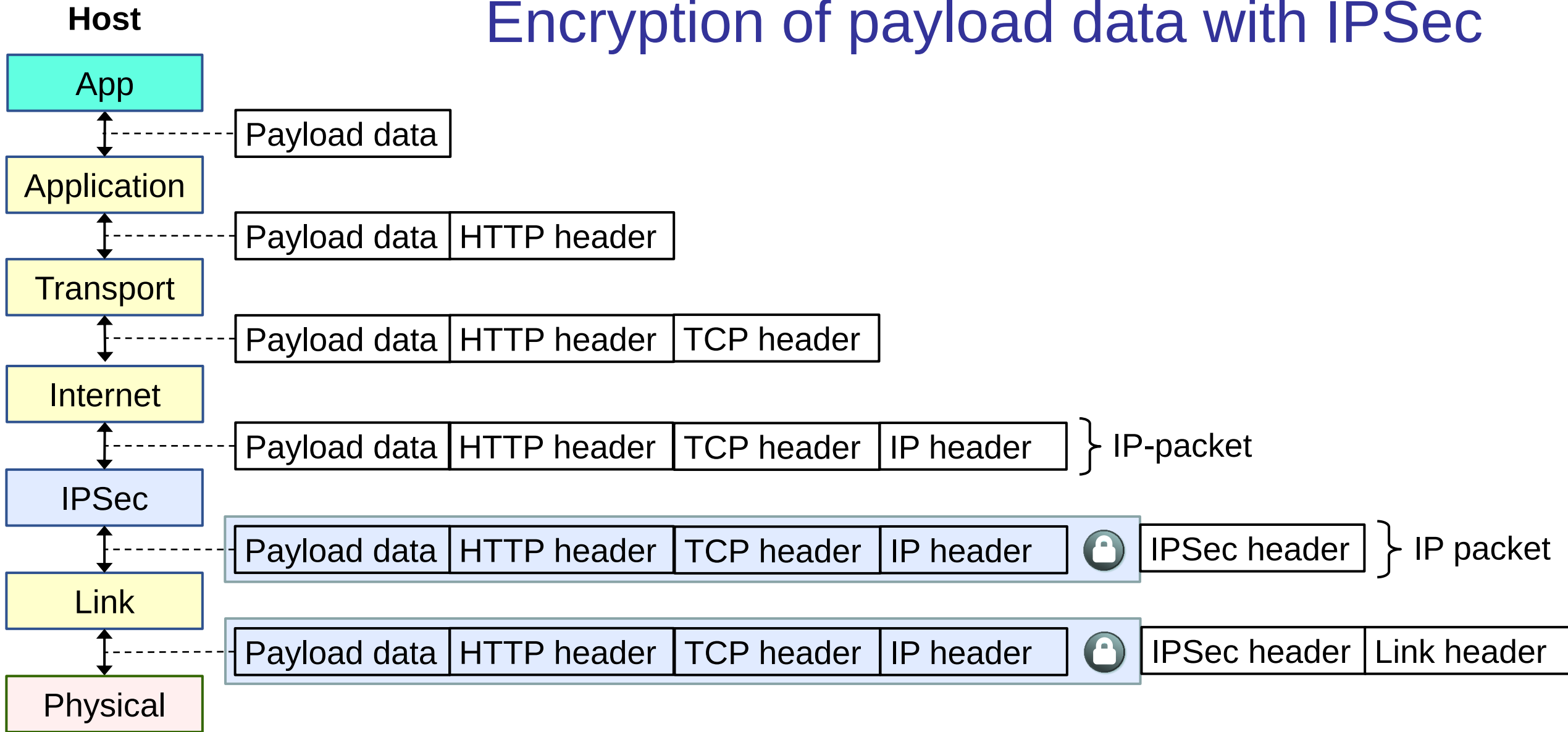
- Browser refuses to establish session with http only (without TLS)
- Browser requires https (with TLS)

IP Security

IPSec

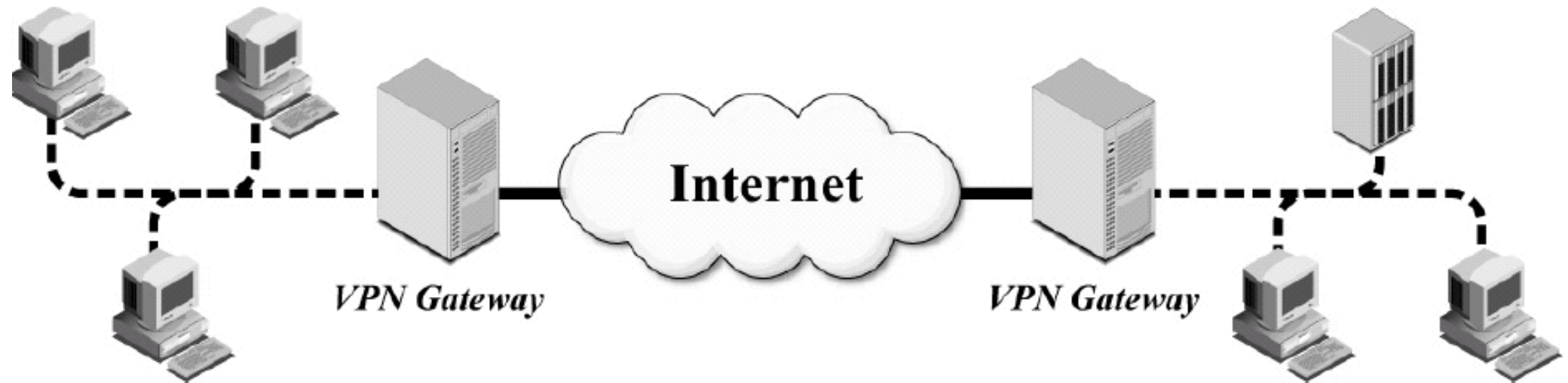
- Internet Protocol Security (IPSec) is the standard for secure communication over the Internet Protocol (IP layer)
 - using cryptographic security services.
- Uses encryption, authentication, and key exchange protocols
- Based on end-to-end security at the IP layer
- Configured at the OS level, not in applications.

Encryption of payload data with IPSec



IPSec:

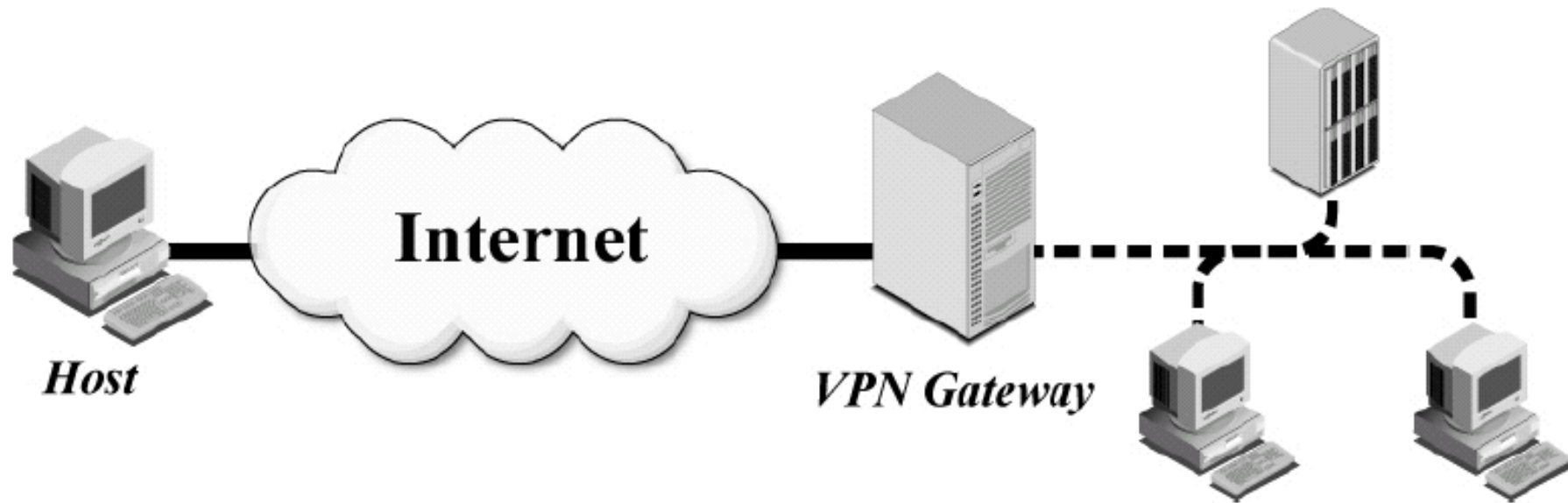
Gateway-to-Gateway Architecture



Source: NIST Special Publication 800-77

IPSec:

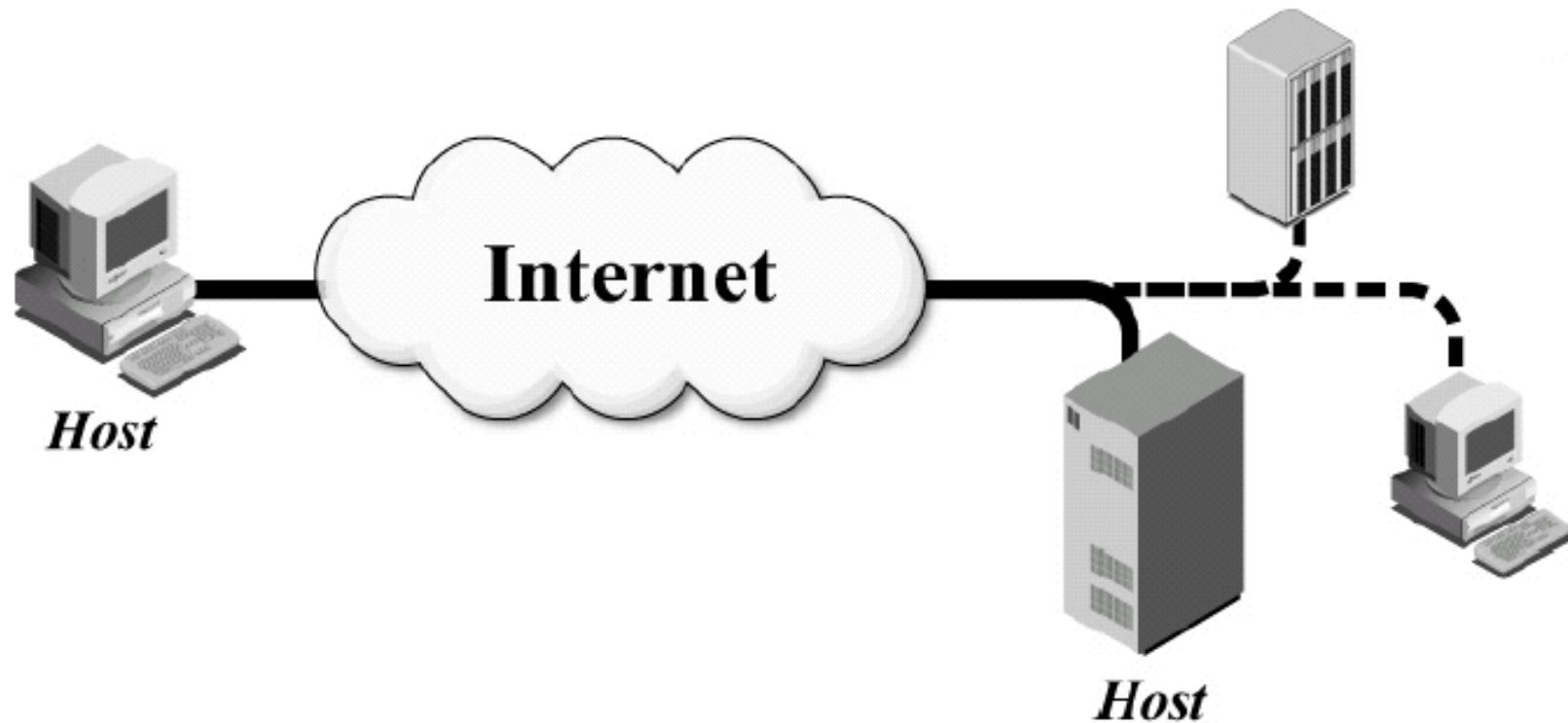
Host-to-Gateway Architecture



Source: NIST Special Publication 800-77

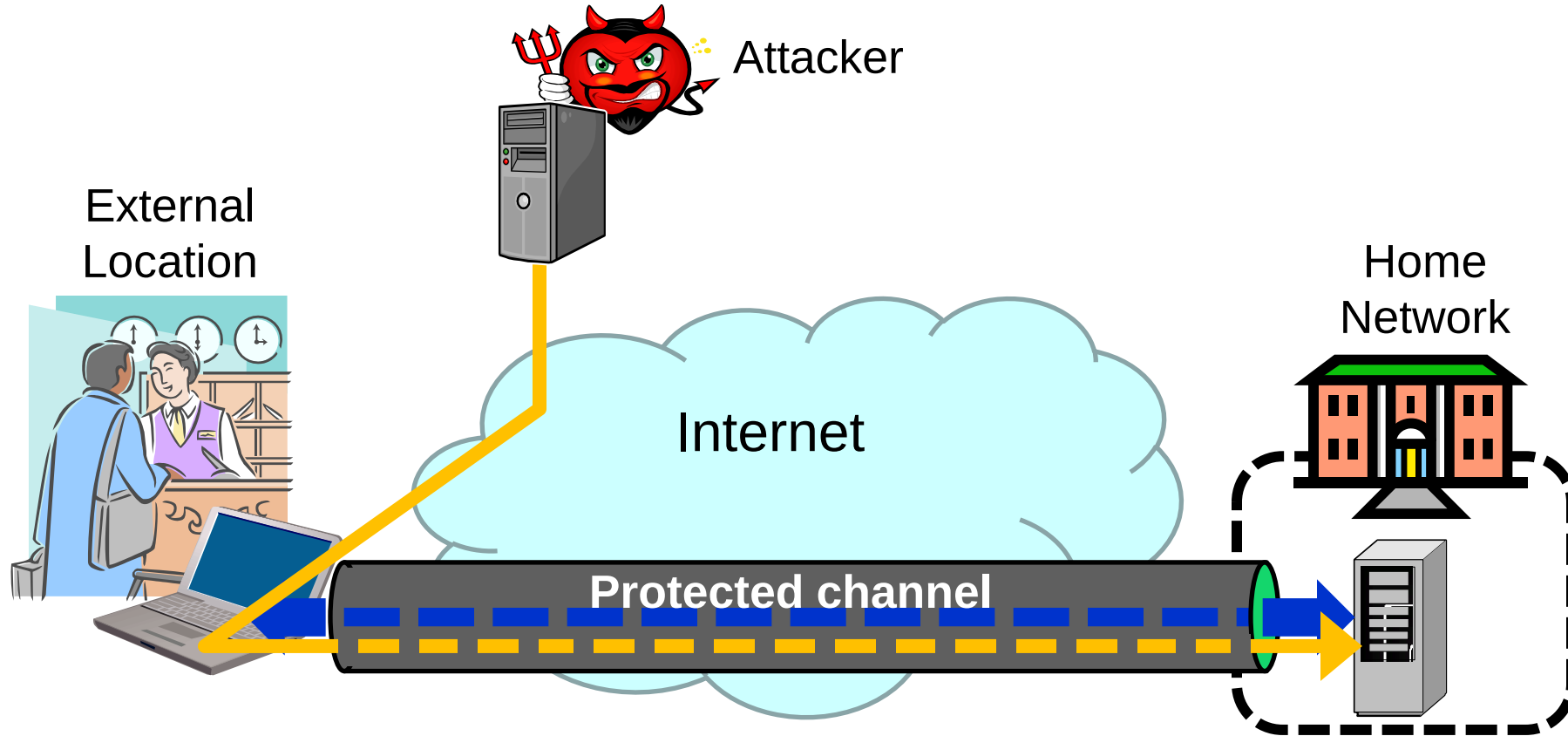
IPSec:

Host-to-Host Architecture



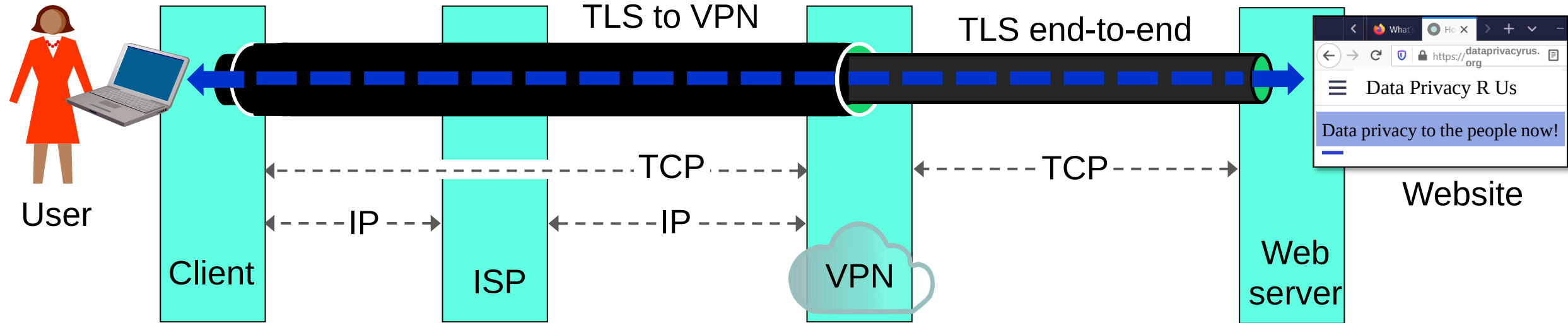
Source: NIST Special Publication 800-77

VPN for tilgang til hjemme-datanett



Possible attack vector through portable device

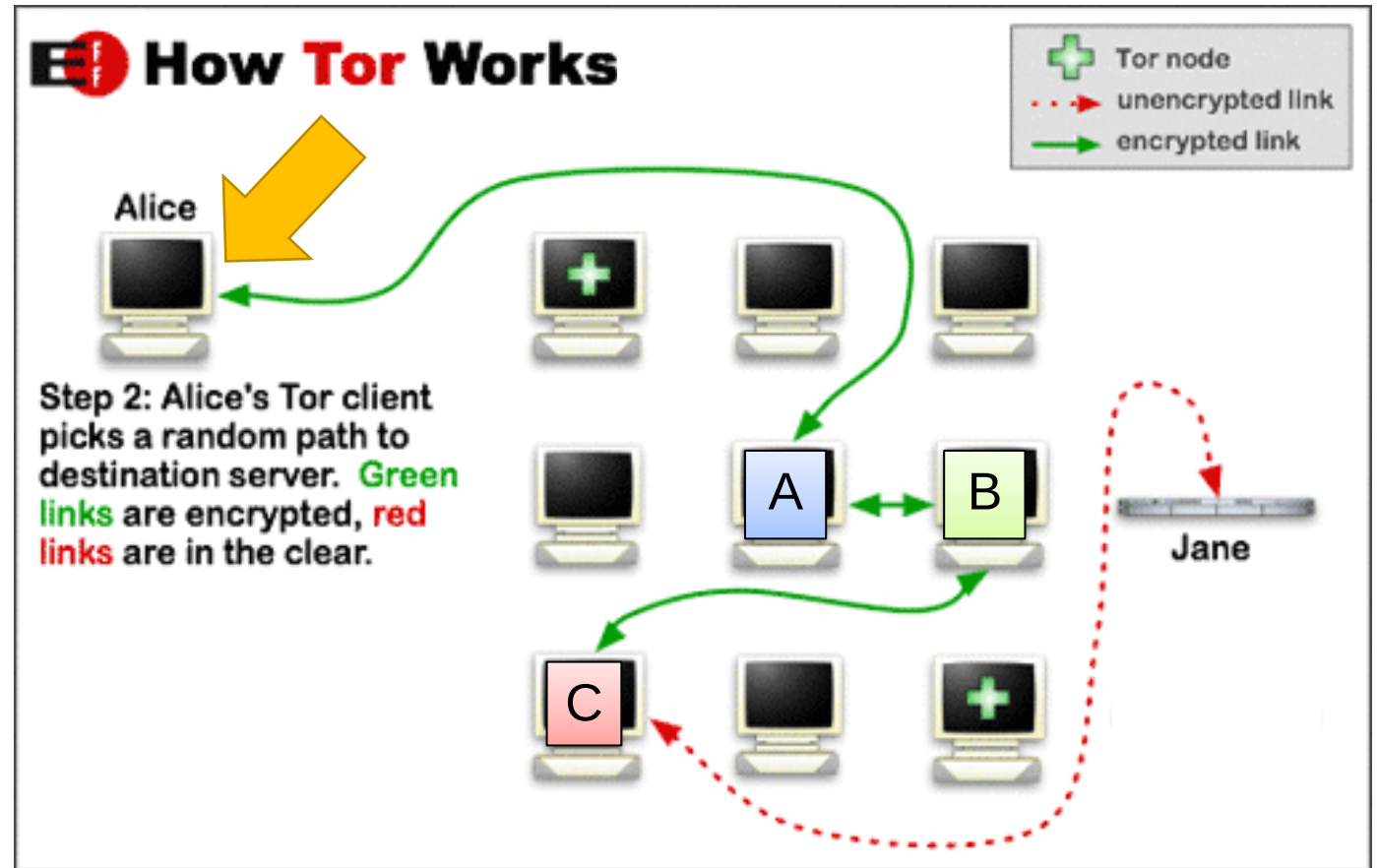
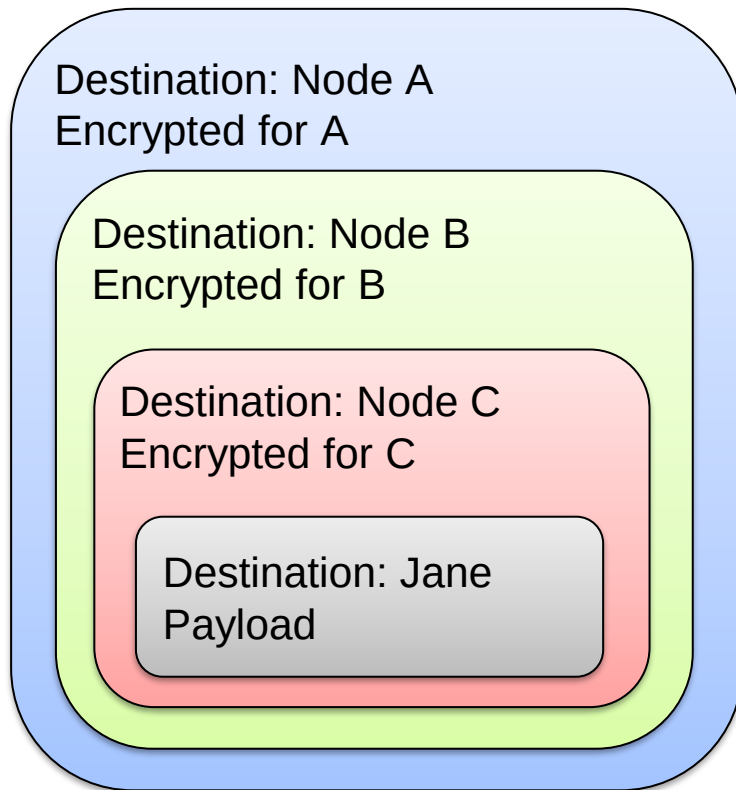
Cloud VPN



Tor (The onion router)

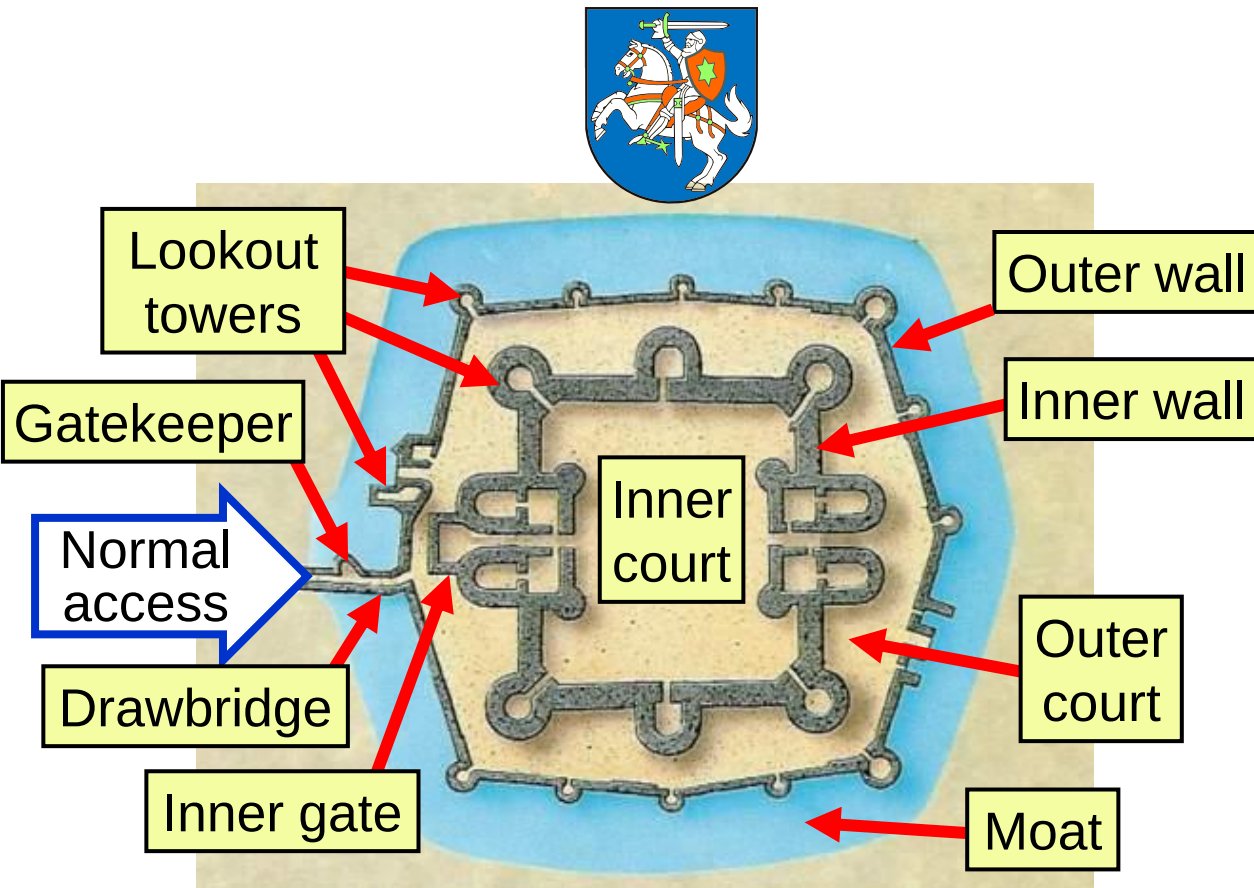


- VPN that uses 3 individual VPN connections that are on top of each other

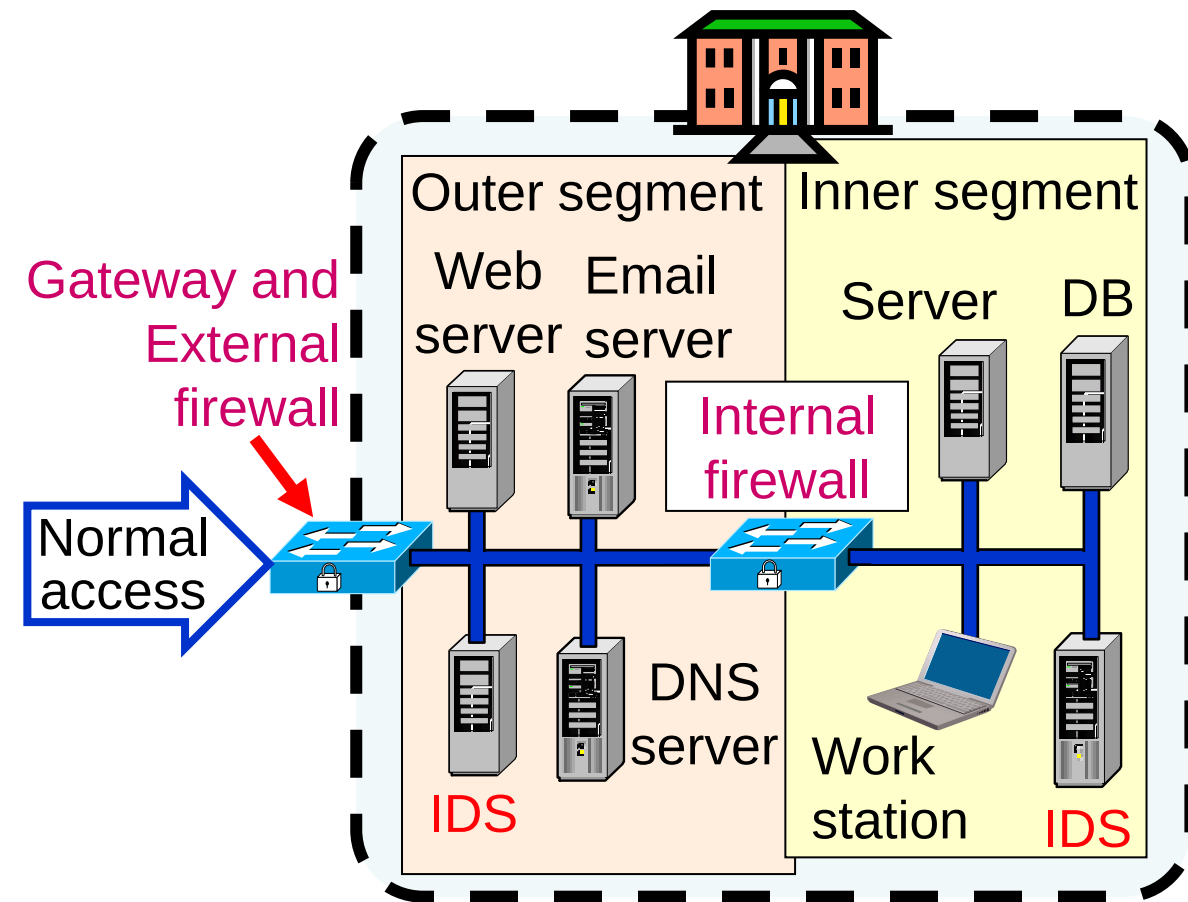


Computer network security

Analogy: Medieval castle and computer network



Medieval castle

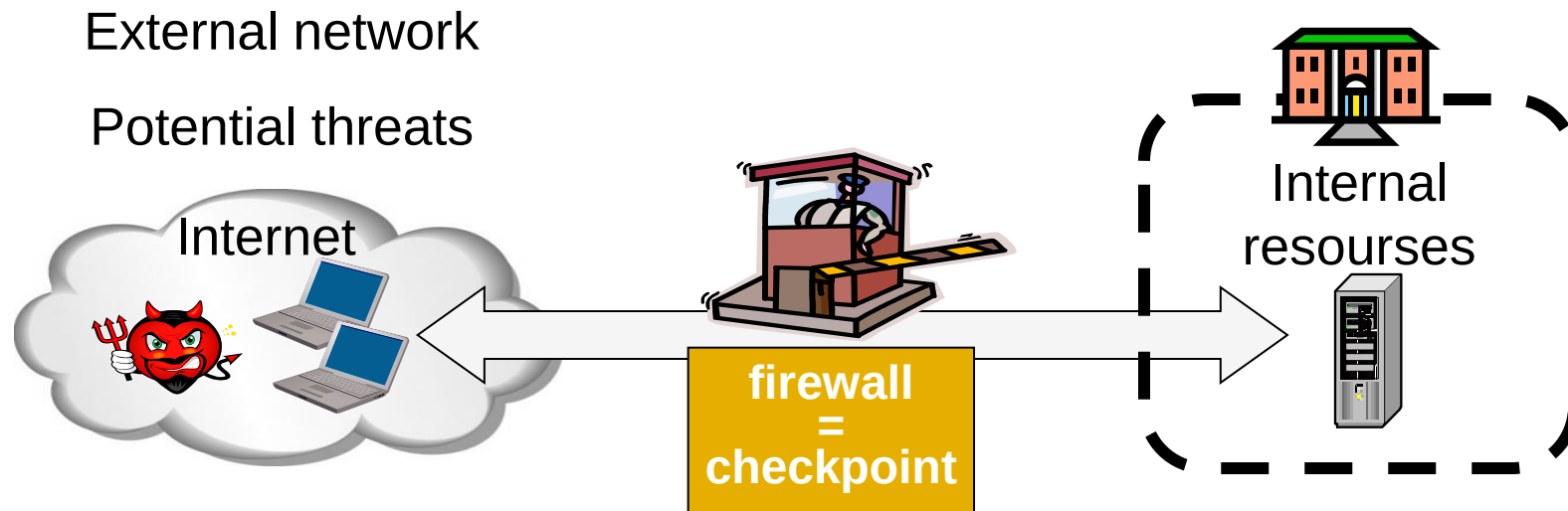


Computer network

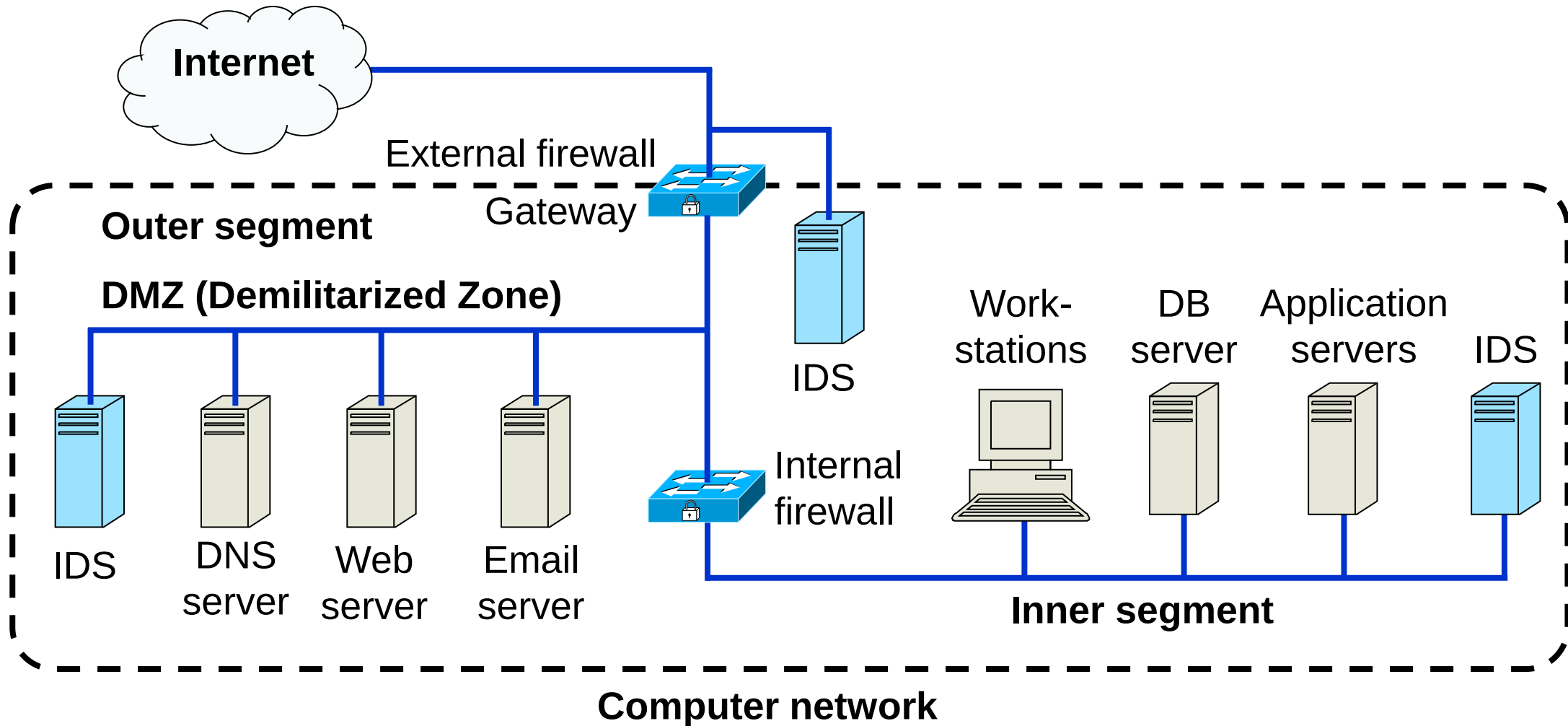
Firewalls

Computer network security with firewalls

- A firewall is a checkpoint that protects your internal networks from attacks from external networks (internet)
- The checkpoint determines which traffic can pass in and out based on rules



Simple computer network architecture with firewalls



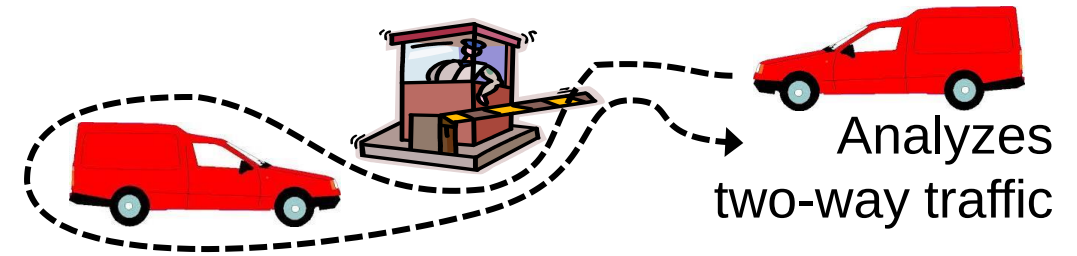
Stateless firewalls



Only inspects
packet headers

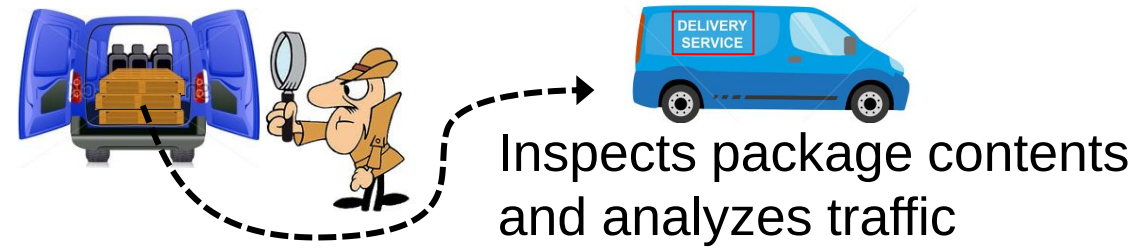
- Simplest type of firewall that inspects packet headers at the transport and web layer and based on this decides whether packet should be accepted or rejected
- For example, uses IP address, port number, type of transport protocol
- `iptables` is a widely used package filter for Linux
 - `iptables -A FORWARD -s 131.234.142.33 -j ACCEPT`
 - All packets from (source) IP address 131.234.142.33 are accepted
 - `iptables -A FORWARD -p tcp -d 10.0.0.56 --dport 22 -j ACCEPT`
 - All TCP packets to (destination) IP address 10.0.0.56 and port 22 are accepted

State-based firewalls



- Has an overview of the state of each connection/session between client and server
- Can create temporary rules for specific session
- More flexibility and high performance but requires memory to remember state
- **Example:** `iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT`
 - Accepts all packets that belong to an established TCP connection or are related to existing UDP communications

Application Firewall



- An application firewall can inspect user data in addition to packet headers
- Supports specific application protocols (HTTP,FTP,...)
- Can be configured for filtering specific user applications (Youtube, Facebook,...)
- Can filter in end-to-end connection between client and server
 - ... or in 2 parts where the firewall plays the role of proxy
 - Proxy server for the client and proxy client for the server
 - A proxy firewall is often called a gateway and is used in VPN as we have seen
- High-performance application firewalls are often referred to as Next Generation Firewalls

Advanced firewalls

Next Generation Firewalls (NGF)
Web Application Firewall (WAF)



Top Model: PA-7080

Capacity: 200 Gbps

Price from: US\$ 200,000



Top Modelo:

Maestro Hyperscale Orchestrator 175

Capacity from 17,6 Gbps to 850 Gbps

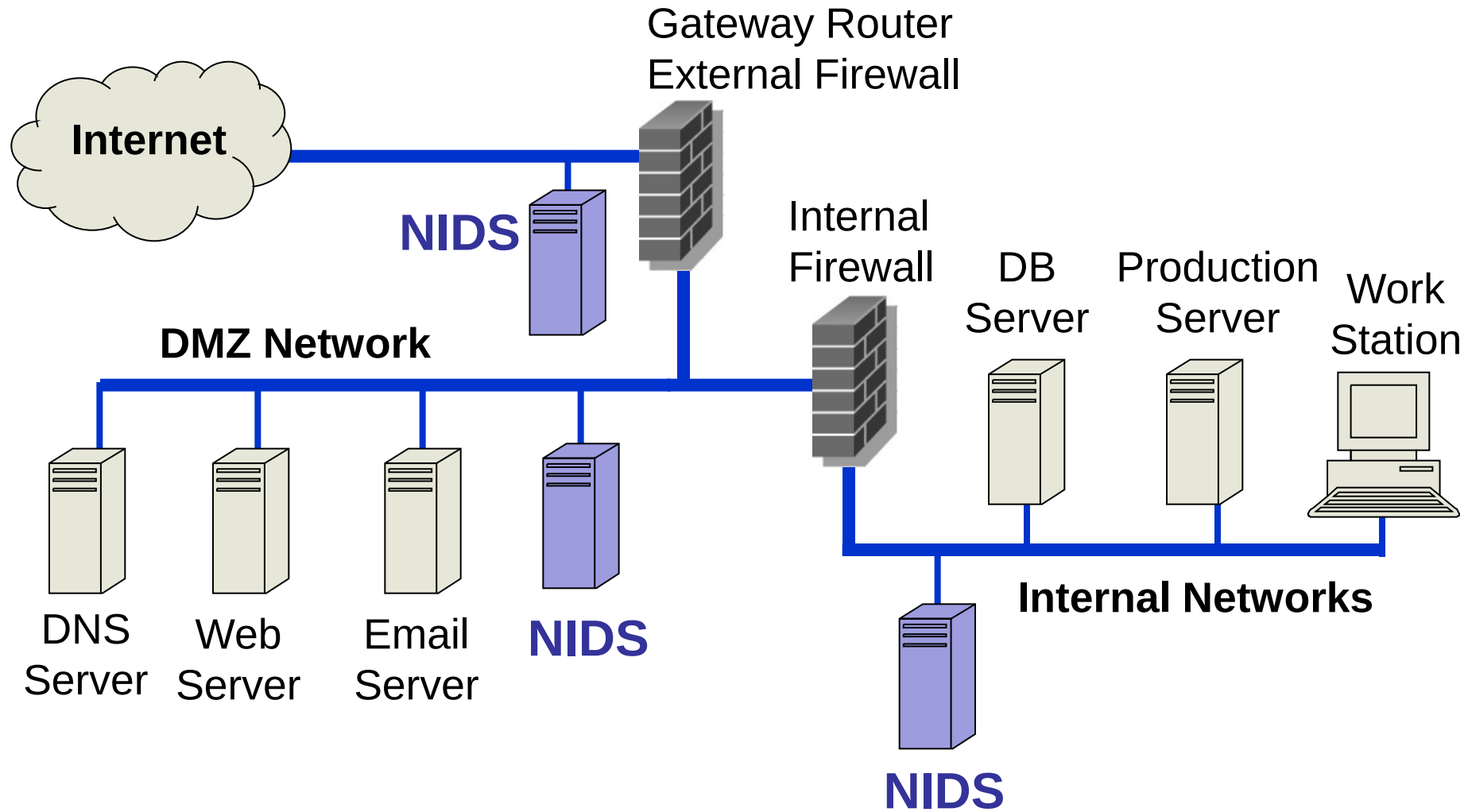
Price from: US\$ 100,000

Intrusion Detection

Intrusion detection

- Intrusion detection systems (IDS) are systems that attempt to detect suspicious activity
- HIDS (Host-based IDS) attempts to detect the activity on the host/system it is installed
 - Monitors processes, file modification, ...
- NIDS (Network-based IDS) attempts to detect activity on one or more network segments
 - Monitors network traffic
 - We focus on NIDS here
- Two main categories: signature-based and anomaly-based

Network intrusion detection



Signature-based intrusion detection

- Signature-based detection
 - Known attack signatures (description of known attacks)
 - Sequences of system calls, patterns of network traffic, etc.
 - Can only detect known attacks
- Snort is a widely used signature-based NIDS
 - Example signature:

```
alert tcp $HOME_NET any -> 10.0.0.56 22
      (msg "SSH til IP-adresse 10.0.0.56")
```

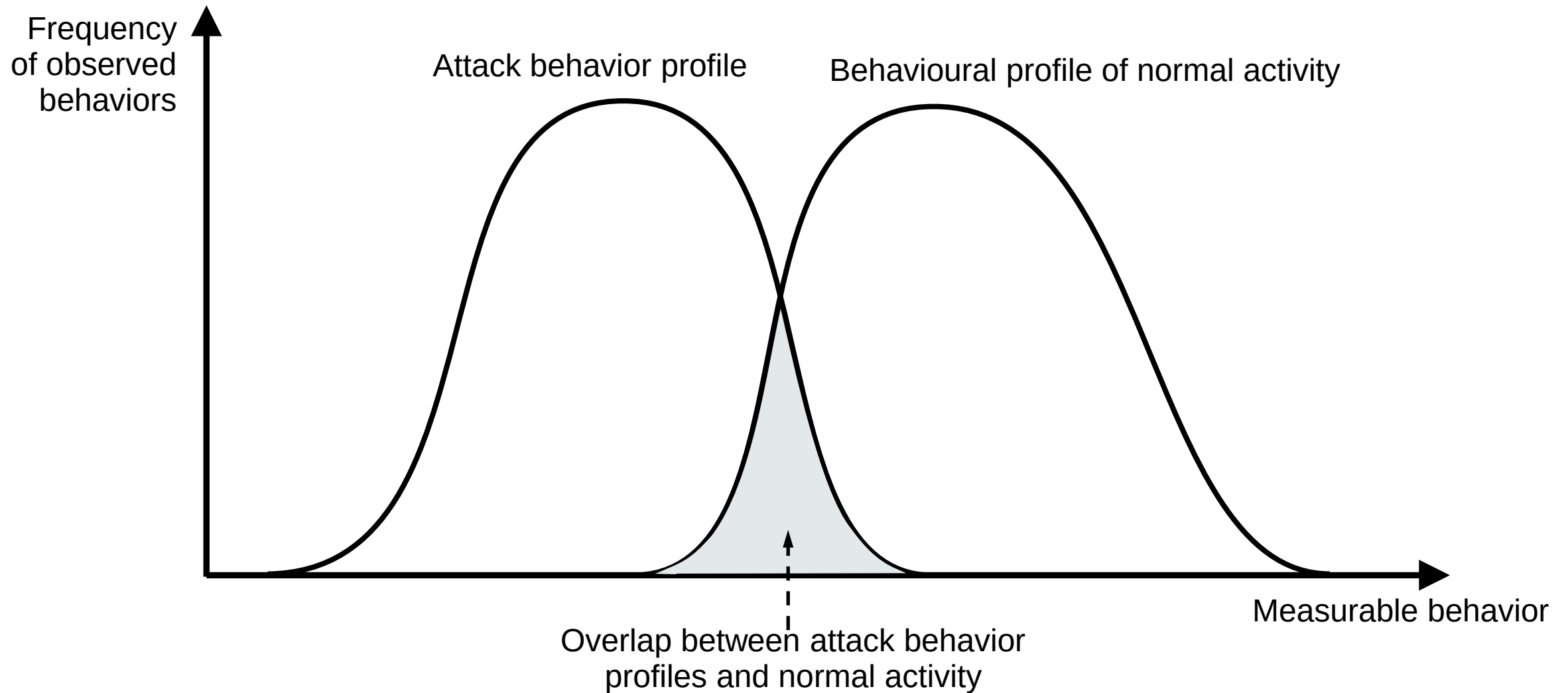
 - Gives alarm if own network (\$HOME_NET) if TCP packet of 22 to IP address 10.0.0.56 (Port 22 is the default port for SSH)



Anomaly-based intrusion detection

- Signature-based detection
 - Can only detect known attacks
 - You have to (manually) prepare signatures
 - Often requires deep packet inspection
 - Encryption (through TLS) makes them less effective
- Anomalibasert deteksjon
 - Use a model of normal system behavior to detect anomalous behavior
 - For example, sound an alarm when a statistically rare event occurs
 - Often based on machine learning
 - Can detect unknown attacks
 - Higher rate of false alarms (false positives) than signature-based

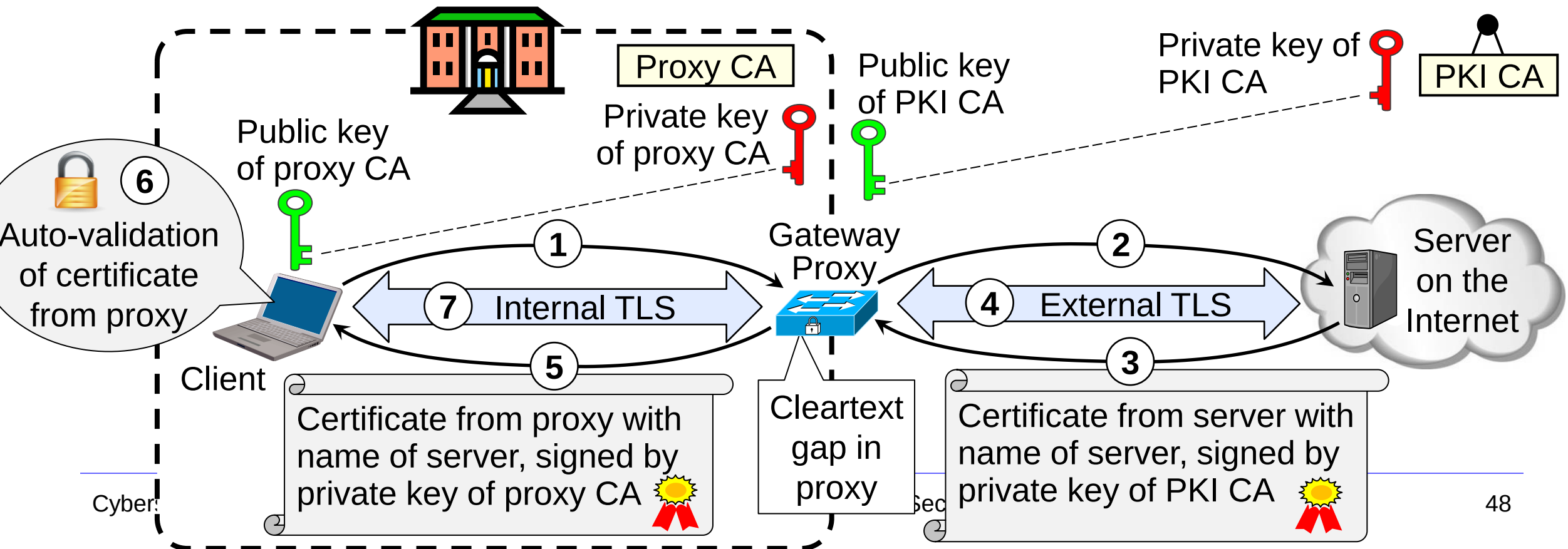
Challenge in distinguishing between attack and normal activity



TLS Inspection

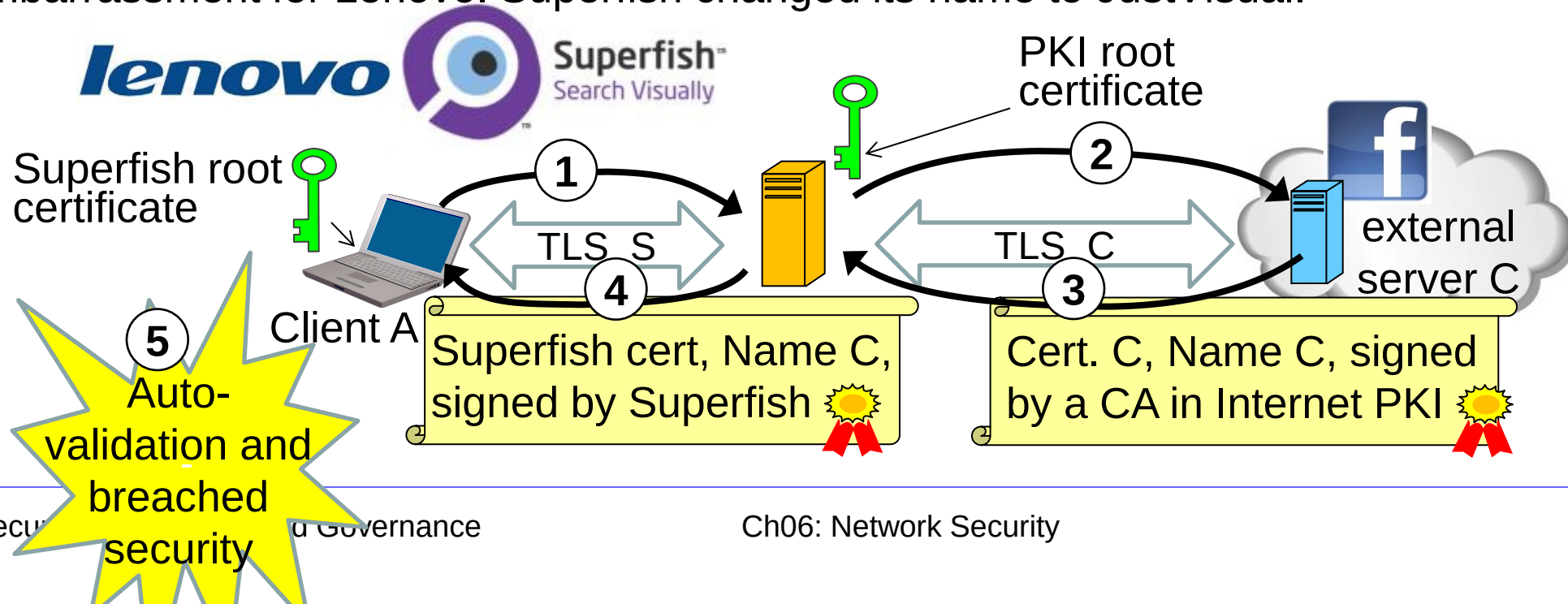
TLS Inspection

- Some organizations want to be able to read encrypted https traffic from employees
- To break TLS encryption, the gateway firewall (proxy) must pretend to be a remote server
- The proxy server certificate is automatically validated by the local client, so the user may mistakenly believe that he/she has encrypted end-to-end TLS connection to the remote server



Infection with Lenovo and Superfish

- Superfish root certificate and redirect in Lenovo models shipped during 2014
- All HTTPS connections were diverted to the Superfish server to inject ads.
- Superfish created fake server certificates with the names of web servers (e.g. Facebook.com), signed by Superfish root private key.
- Fake server certificates were automatically validated, so users believed that he/she had a secure end-to-end HTTPS connection to the web server.
- Scam discovered in 2015, Superfish cert. deleted and redirect removed.
- Embarrassment for Lenovo. Superfish changed its name to JustVisual.



End of presentation

