ETH zürich

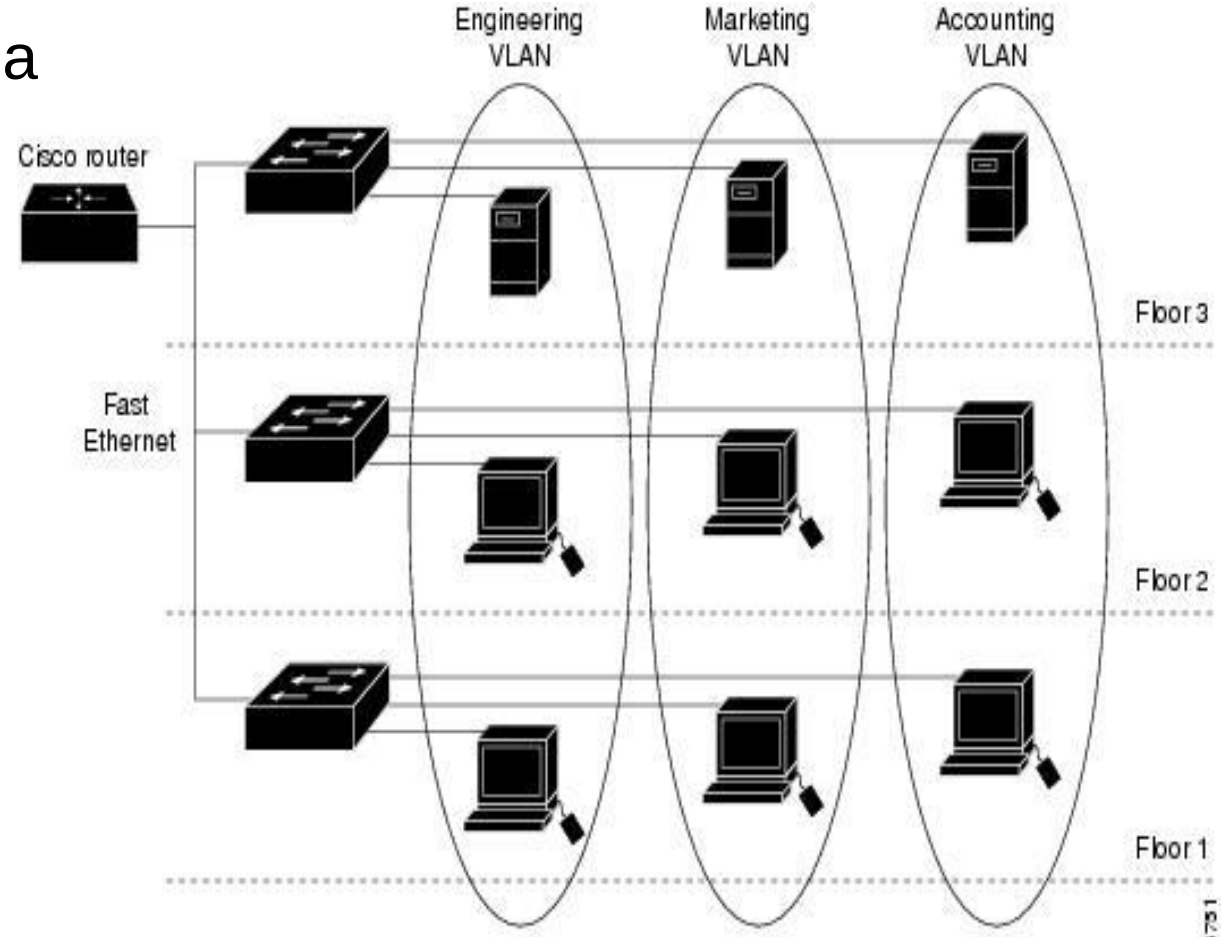
Discussion exercise sheet 5

Marc-Philippe Bartholomä
Student Assistant for Network Security 2020
22 October 2020, HG F1

Teaser of Video at the end. Removed for Download.

VLAN

- set up multiple isolated virtual networks on a single physical infrastructure
- Resides on L2



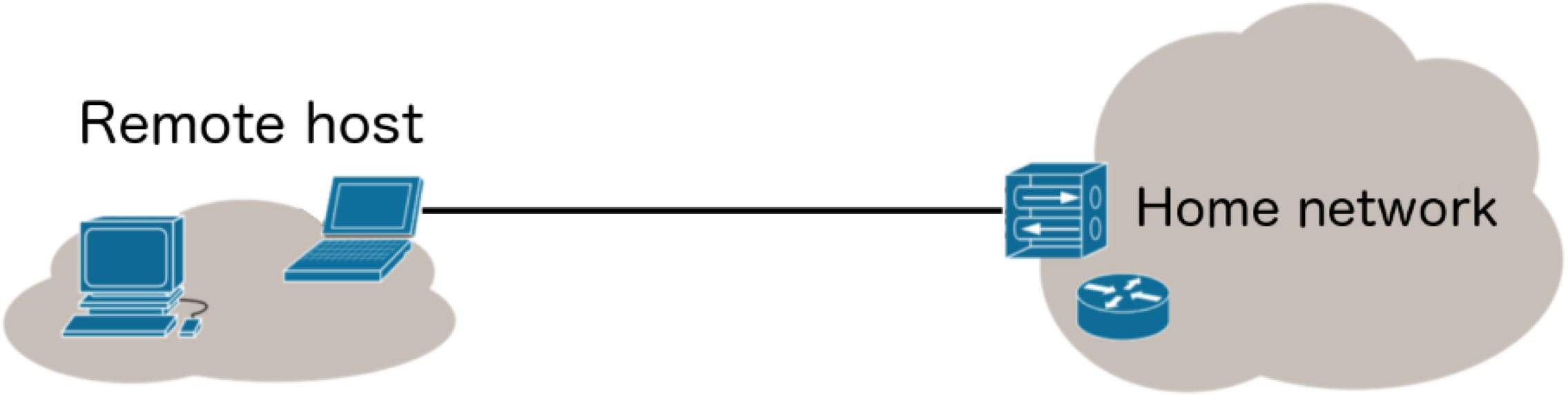
https://www.cisco.com

1.1: Avoid opening ports

You are hosting some service at **home**, how can you access it without exposing it to the internet?

VPN

Client to home network



1.2: Certificate Authority

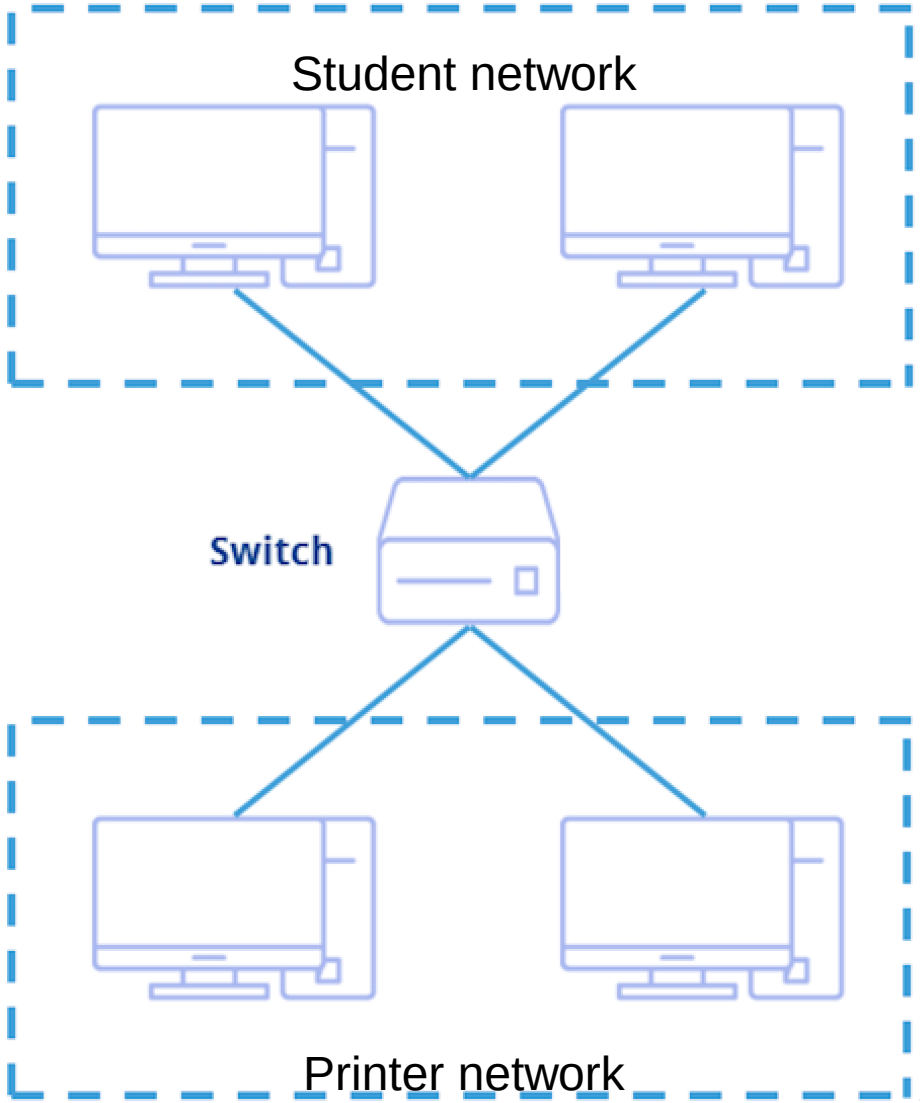
Accessing a **CA admin** panel from work

- VPN provides **client authentication**

VPN

as access control

1.3: University



Need to run **separate networks** for student access, staff and printers

- Classic case for **VLAN** configuration
- Guarantee isolation
- Can **share infrastructure**, no need to move printers close together

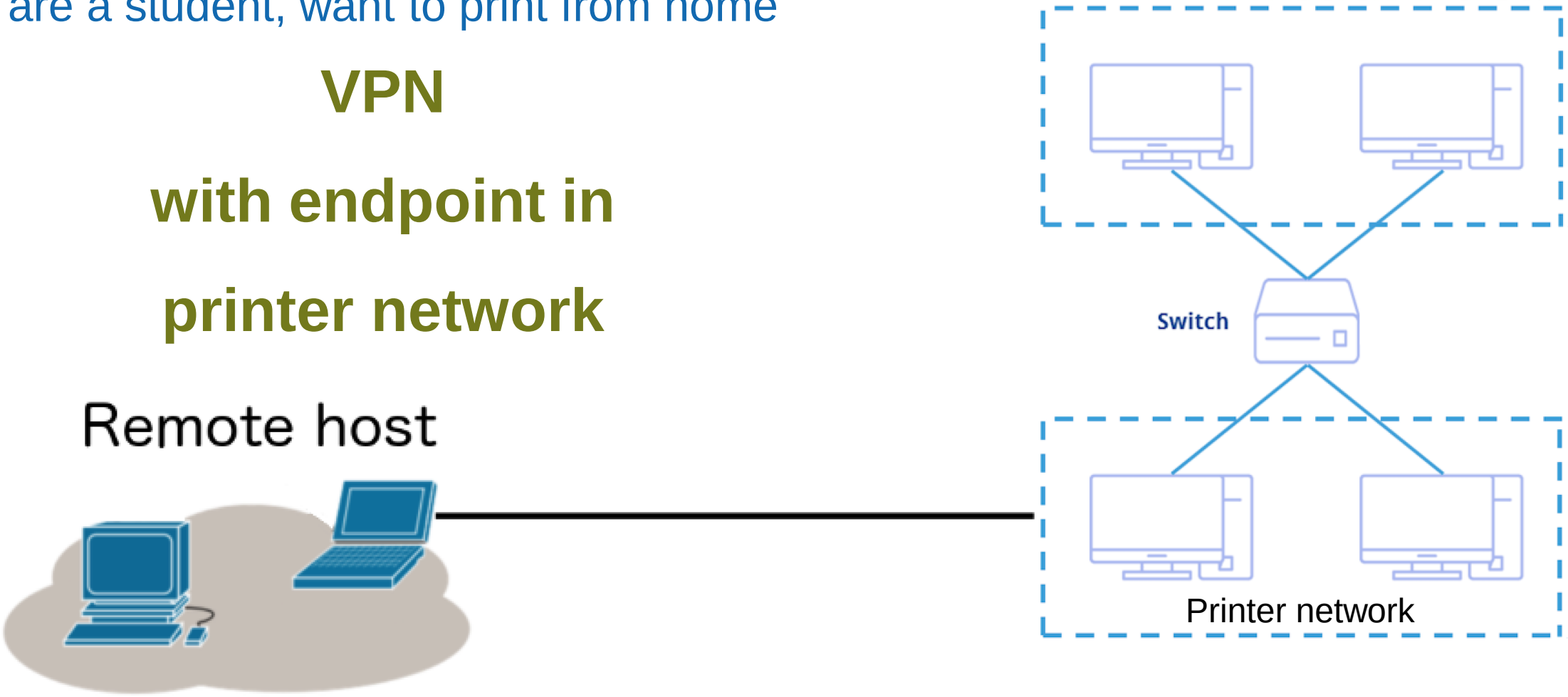
1.4: Print from home

You are a student, want to print from home

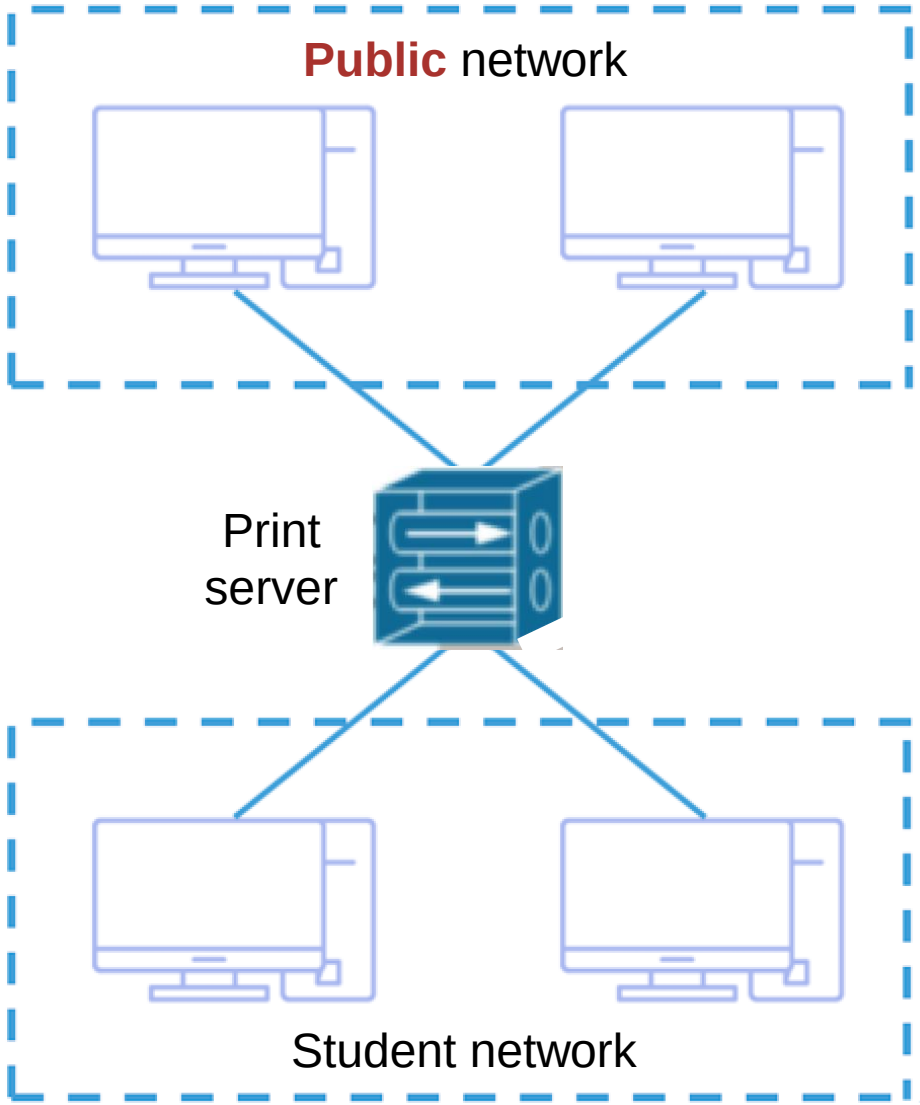
VPN

with endpoint in

printer network



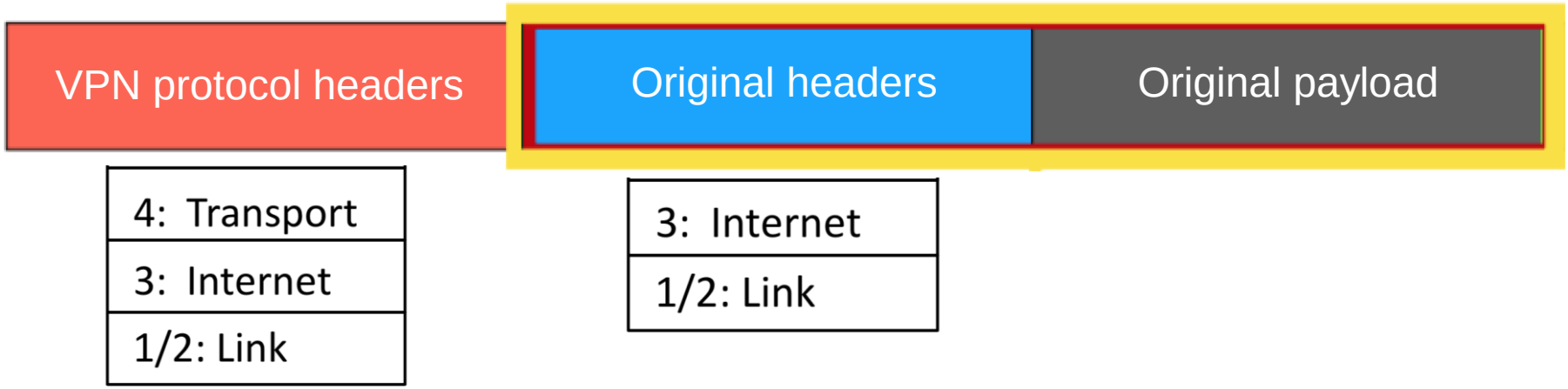
1.5: Print via email



How to enable print via email functionality?

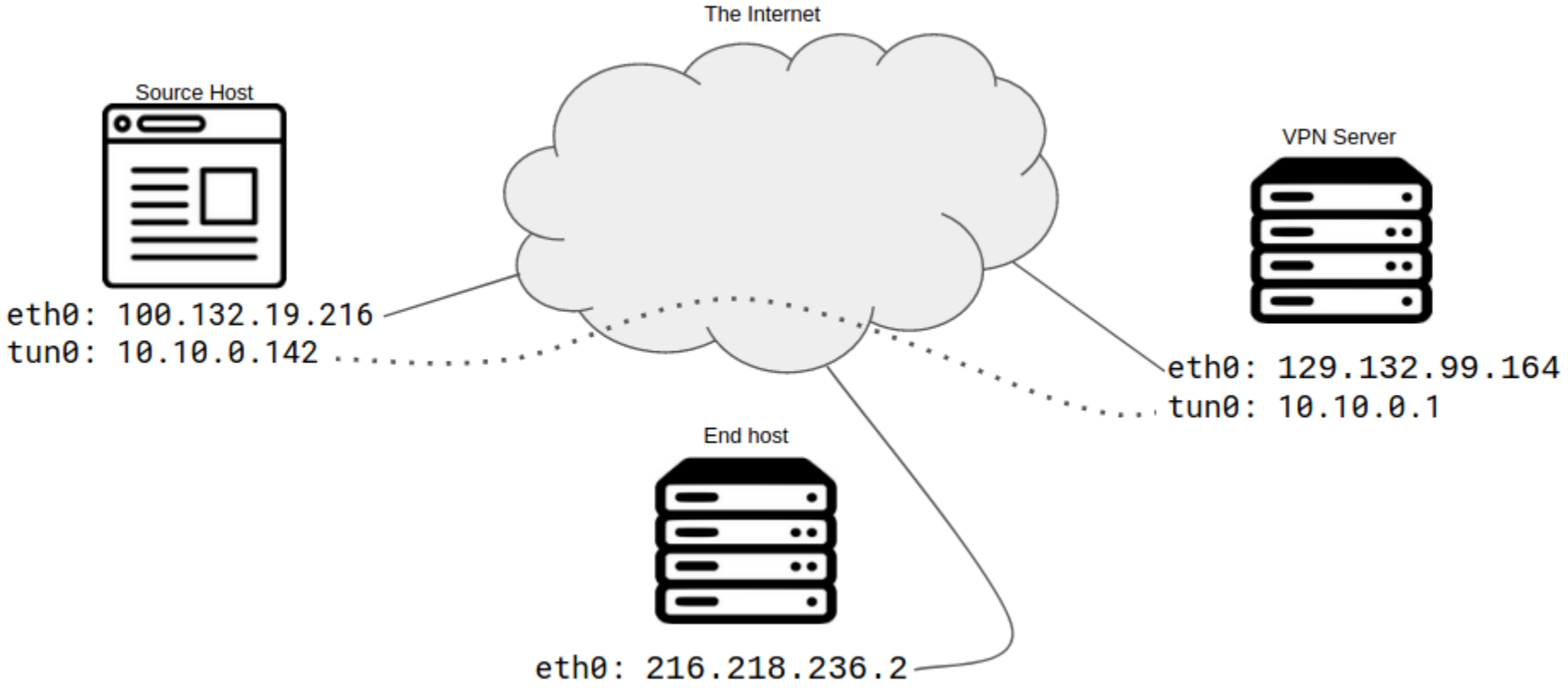
- Print + email server **connected to both VLANs**
- Receives emails from **public** network
- Sends them to the printer network
- **Isolation ensured via software**

2: Encapsulation of VPN packets



3: VPN Routing

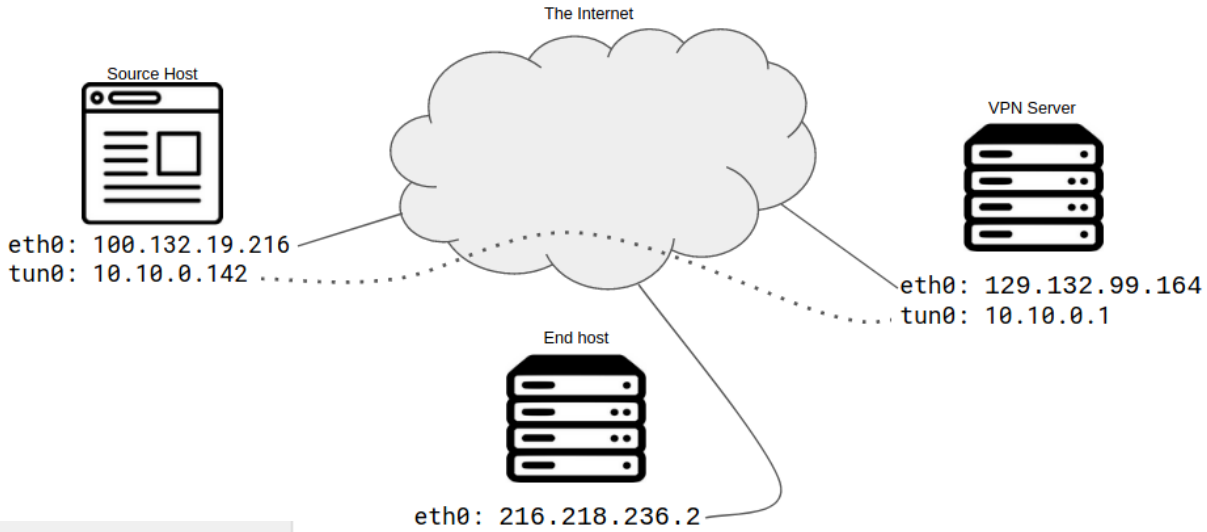
Fix routing table




```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         100.132.19.216  0.0.0.0         UG    0      0        0 eth0
100.132.19.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
10.10.0.0       0.0.0.0         255.255.0.0     U     0      0        0 tun0
```

3: VPN Routing

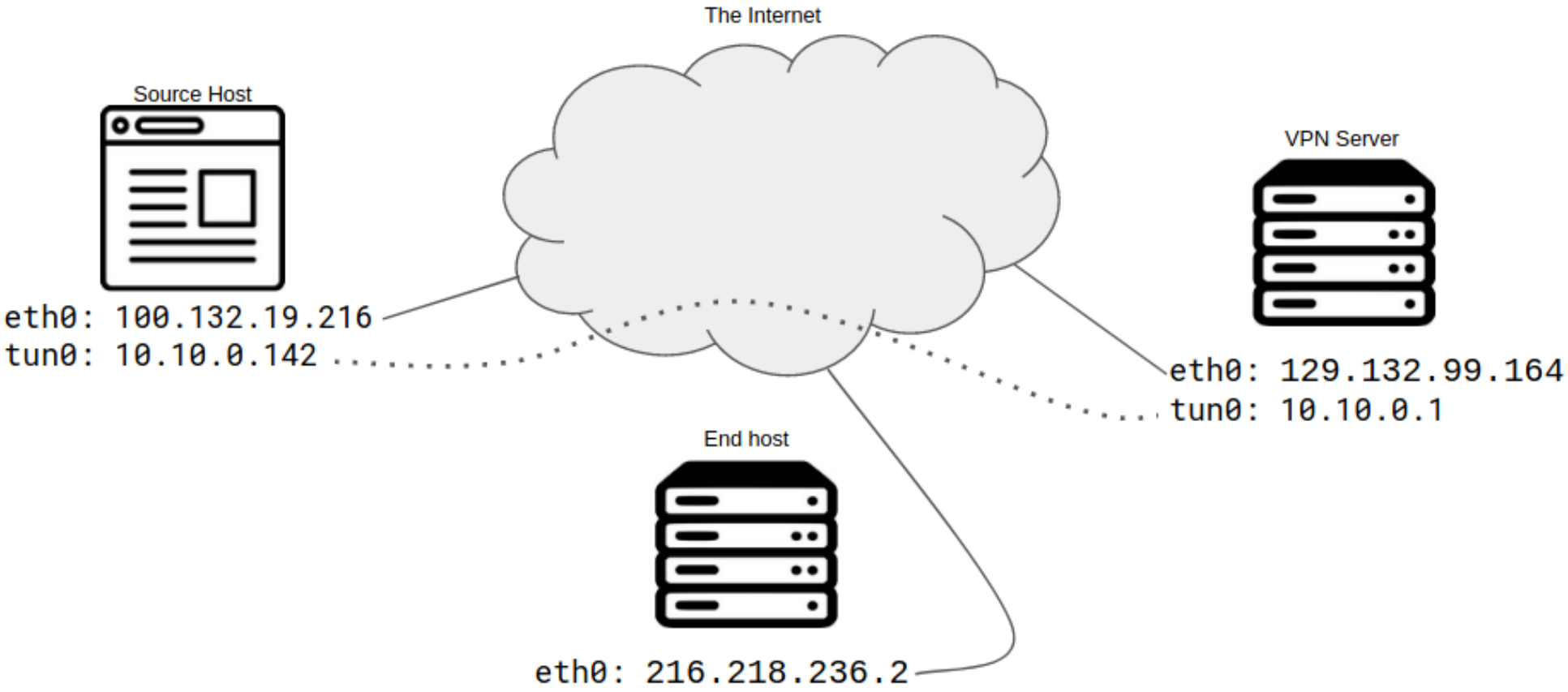
Track source and destination



packet	source IP	destination IP
original packet at source host (client)	`not set`	`216.218.236.2`
packet after routing decision	.....	.....
headers of the outer protocol	.....	.....
packet after decapsulation at VPN server	.....	.....
packet after NATing at VPN server	.....	.....

3: VPN Routing

Return route



4.1 Client certificate authentication

IPSec

- Supposed to be a **private network**
- VPN **access must be restricted** by definition
- Identifying both clients and servers is important
- Client certificates are exchanged

TLS

- Usually **no client certificate**
- Websites are **publicly accessible**
- Client identity not important*
- Server identity critical
- MitM risk otherwise!

*or achieved with different mechanisms

4.2: Client Cert leaks identity

IPSec

- **Encrypt using Anonymous Diffie Hellman!**
- Passive MitM can’t see certs
- Active MitM can still hijack the session (Remember: ANON DH)

TLS 1.3

- Also protects client identity
- (TLS 1.2 didn’t)
- **Error in exercise sheet: just replaced TLS 1.2 with TLS 1.3**

4.3: Sequence numbers in IPSec (vs TLS)

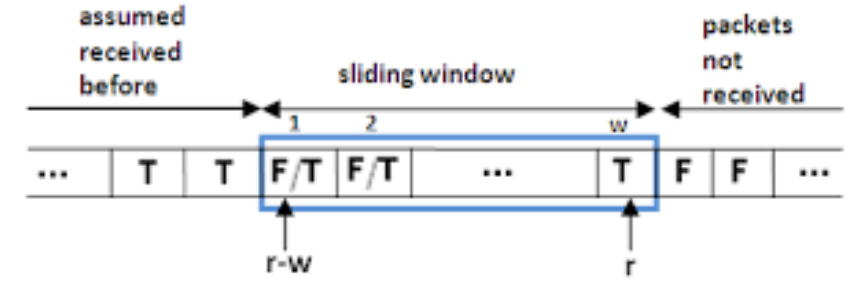


Figure 1: The anti-replay window

- Sequence numbers used to **prevent replay attacks**
- Every party has a sliding window to avoid repeated packets

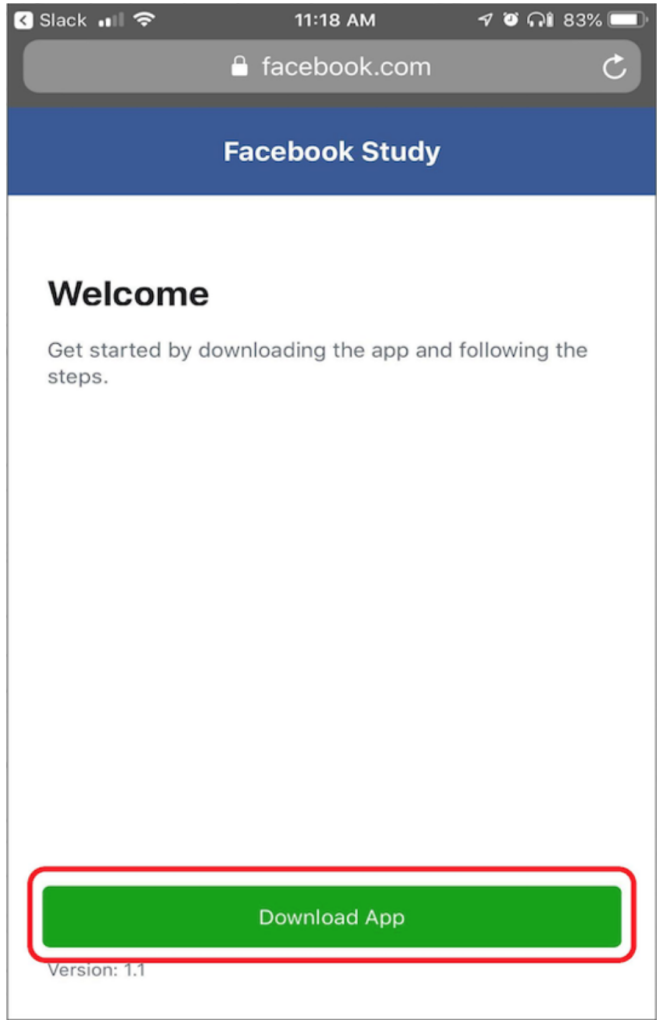
- **IP is best effort**, packets could be lost and order disrupted
- Need to transmit the numbers in IPSec header

Facebook Research app

- Dear Facebook user, why don't you participate in a study?
- Join Facebook research program and get **20$/month** for your collaboration!

What's the catch?

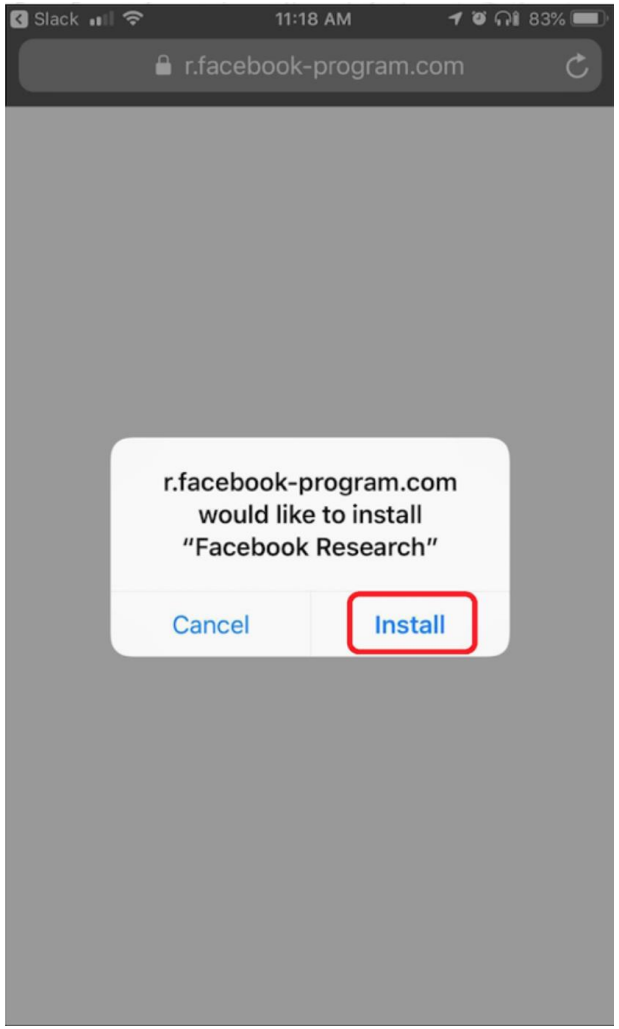
What is actually happening



Phase 1:

Unsuspecting users download the app

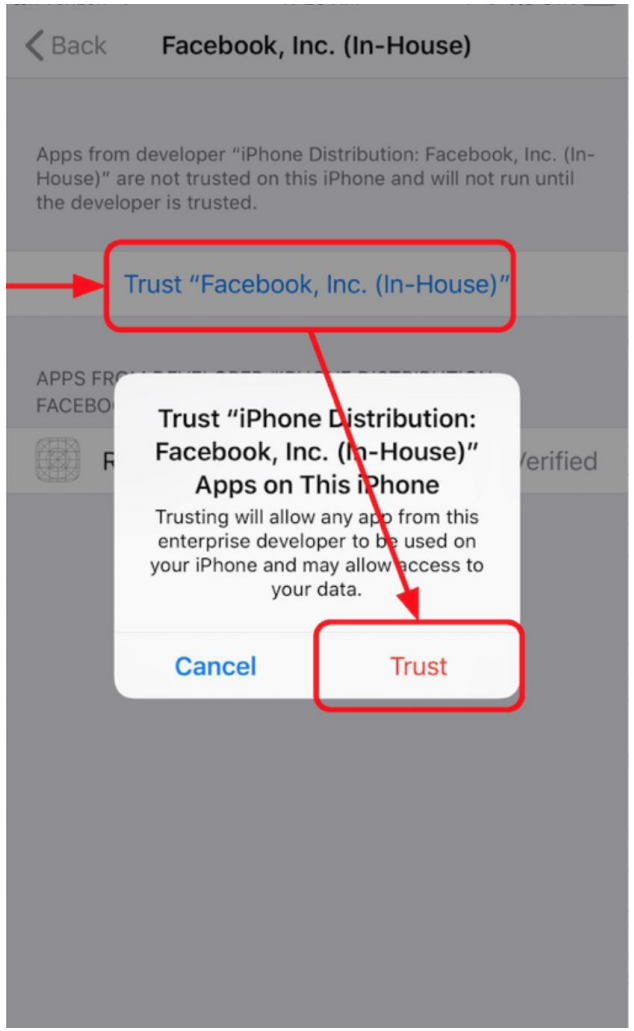
What is actually happening



Phase 2:

The app installs and activates a VPN pointing to Facebook

What is actually happening



Phase 3:

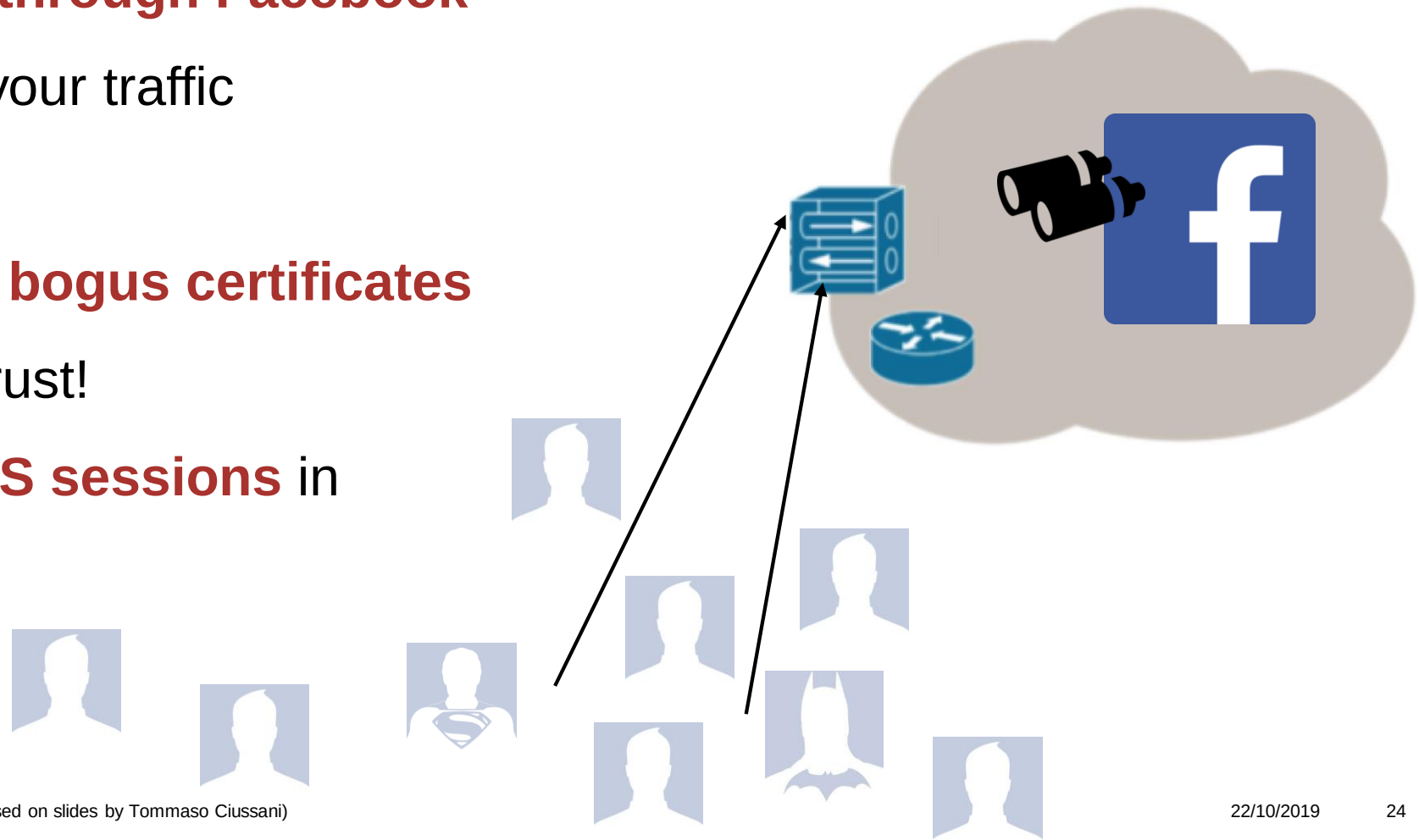
The app installs and activates a root certificate

Most users have no idea they just sold their privacy for 20$

5: Facebook in the Middle

- Your traffic is **routed through Facebook**
  - **No effort** to sniff your traffic

- Facebook can create **bogus certificates** that your phone will trust!
  - Can **read** your **TLS sessions** in plain text!



Wireguard basics

- **Lightweight** codebase, just 4K lines
- **Limited** set of **cipher suites**
- Every party has a static **key pair**
- Public key is not supposed to be available to everyone

Cryptokey routing

- Every interface has **private key** and a **list of peers** (public keys)
- List associates public keys with allowed IPs
- IPs used for **routing**
- IPs used for **access control**

```
[Interface]
PrivateKey = yAnz5TF+lXXJte14tji3zlMNq+hd2rYUIgJBgB3fBmk=
ListenPort = 51820

[Peer]
PublicKey = xTIBA5rboUvnH4htodjb6e697QjLERt1NAB4mZqp8Dg=
AllowedIPs = 10.192.122.3/32, 10.192.124.1/24

[Peer]
PublicKey = TrMvSoP4jYQlY6RIzBgbssQqY3vxI2Pi+y71lOWWXX0=
AllowedIPs = 10.192.122.4/32, 192.168.0.0/16

[Peer]
PublicKey = gN65BkIKy1eCE9pP1wdc8ROUtkHLF2PfAqYdyYBz6EA=
AllowedIPs = 10.10.10.230/32
```

6.1: PFS in WireGuard

- Tunnel_ephemeral keys derived from pubkeys and ephemeral keys
- Via DH and MAC computation

- PFS:
  - **REKEY_AFTER_MESSAGES**
  - **REKEY_AFTER_TIME**

PFS or weaker form?

Why is this different from Signal?

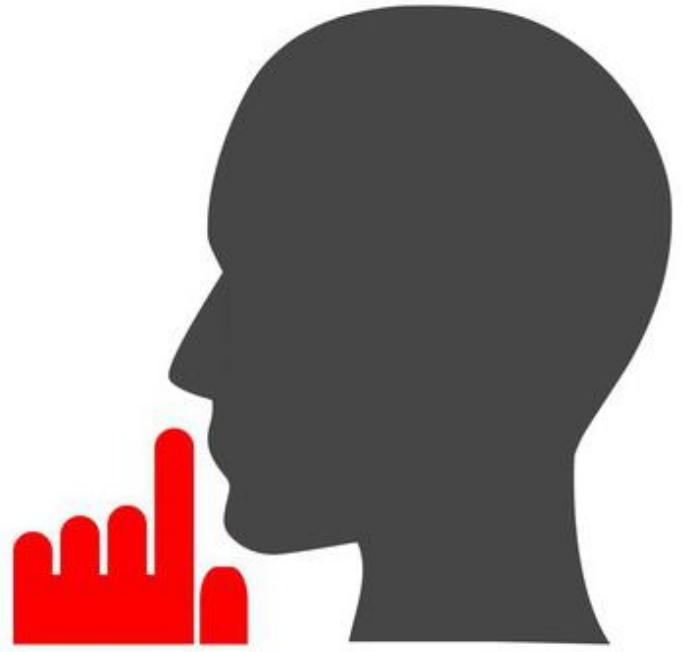
More details: https://www.wireguard.com/protocol/

6.2: DoS attack mitigation

1. Silence is virtue

No reply in these situations:

- Sender doesn’t know receiver public key
- Unauthorized originating IP



Attackers **not able to flood**, no state kept

- Think about SYN flood…

6.2: DoS attack mitigation

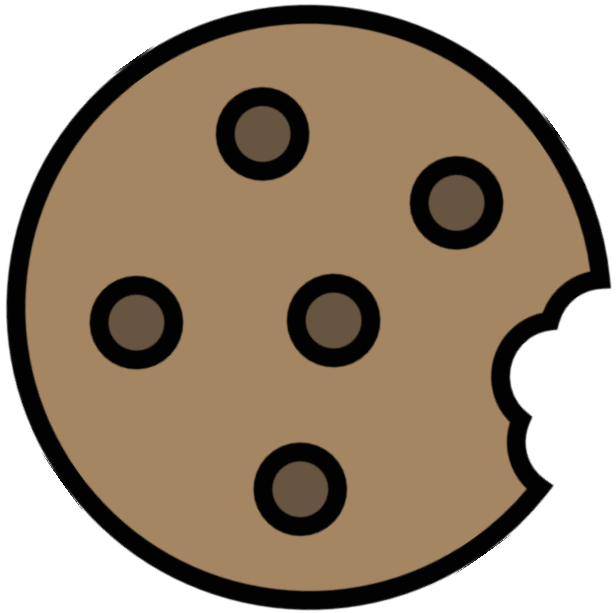
2. Timestamp

Sent with **every packet**:

- **Prevents replay attacks**
- Same function as seqnum in IPSec

3. Cookie: server already under load, needs to avoid crypto

1. S replies with **cookie**:
   - S has periodically changing random value R
   - Cookie **encrypted** with client public key as symmetric key
   - Content: MAC_R(IP of client C)



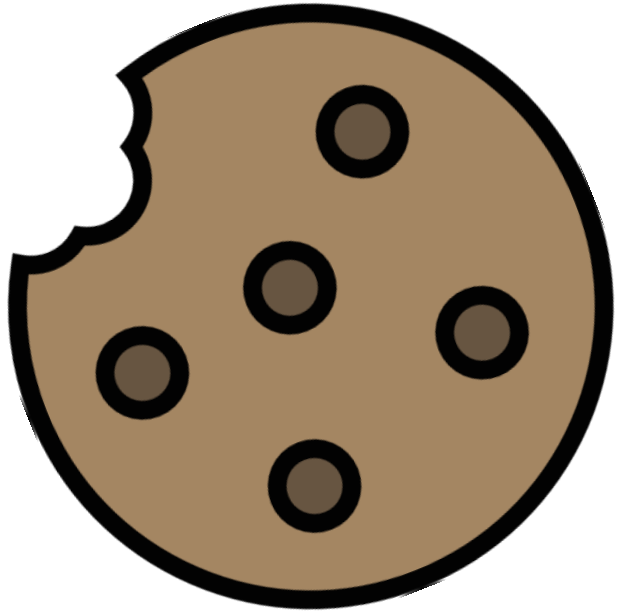
https://www.flaticon.com/authors/freepik

3. Cookie: server already under load, needs to avoid crypto

2. Client resends message, msg.mac2=**MAC_{cookie}**(msg)
   - Server checks a **symm** encryption

     and matches the IP
   - Proof of **IP ownership**

3. Server can apply **rate limiting** to IPs



Difference with IKEv2

Very similar cookie mechanism, but:

- IPSec **maintains state**
- Max num of open connections
- No msg.mac1 verification -> **no silence**
- Cookie transmitted in **plaintext**

5.4 VPNs and logging

Tom Scott, https://www.youtube.com/watch?v=WVDQEoe6ZWY

Your Questions