CSCI-3403: Cyber Security
Spring 2020

Abigail Fernandes

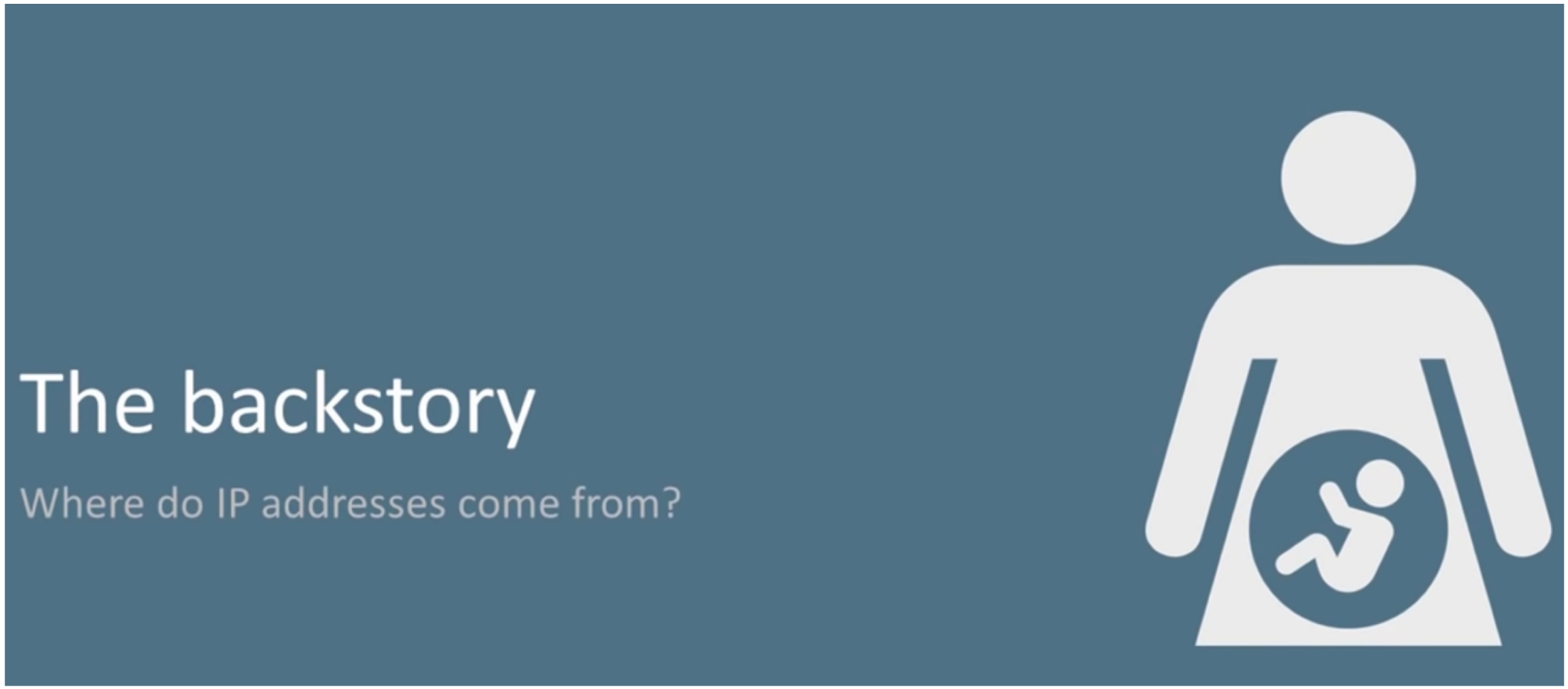
Department of Computer Science

University of Colorado Boulder

Week 11
> NAT
> VPN

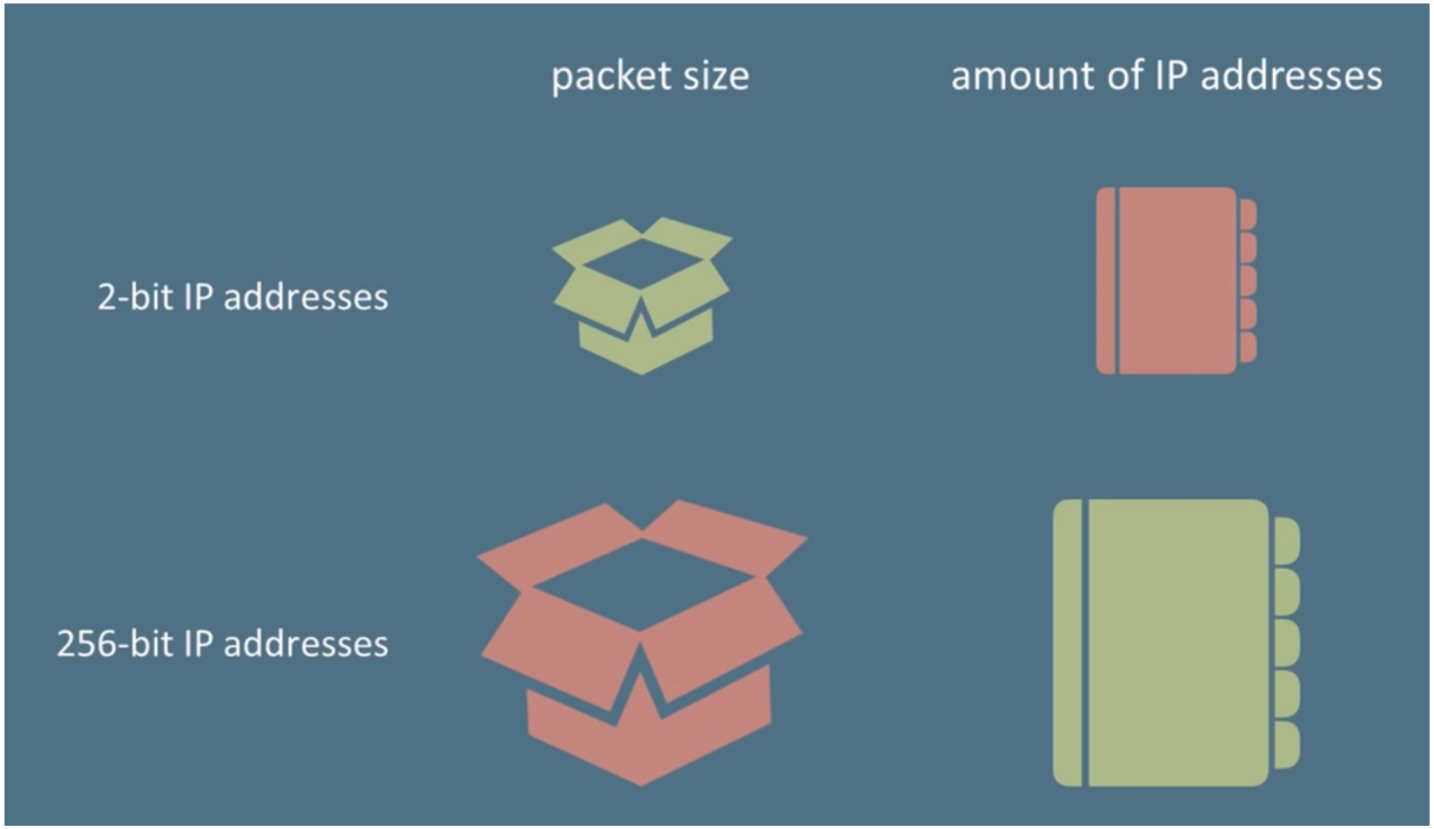
Network Address Translation

Backstory!



History of IP Addresses

IP Address Size

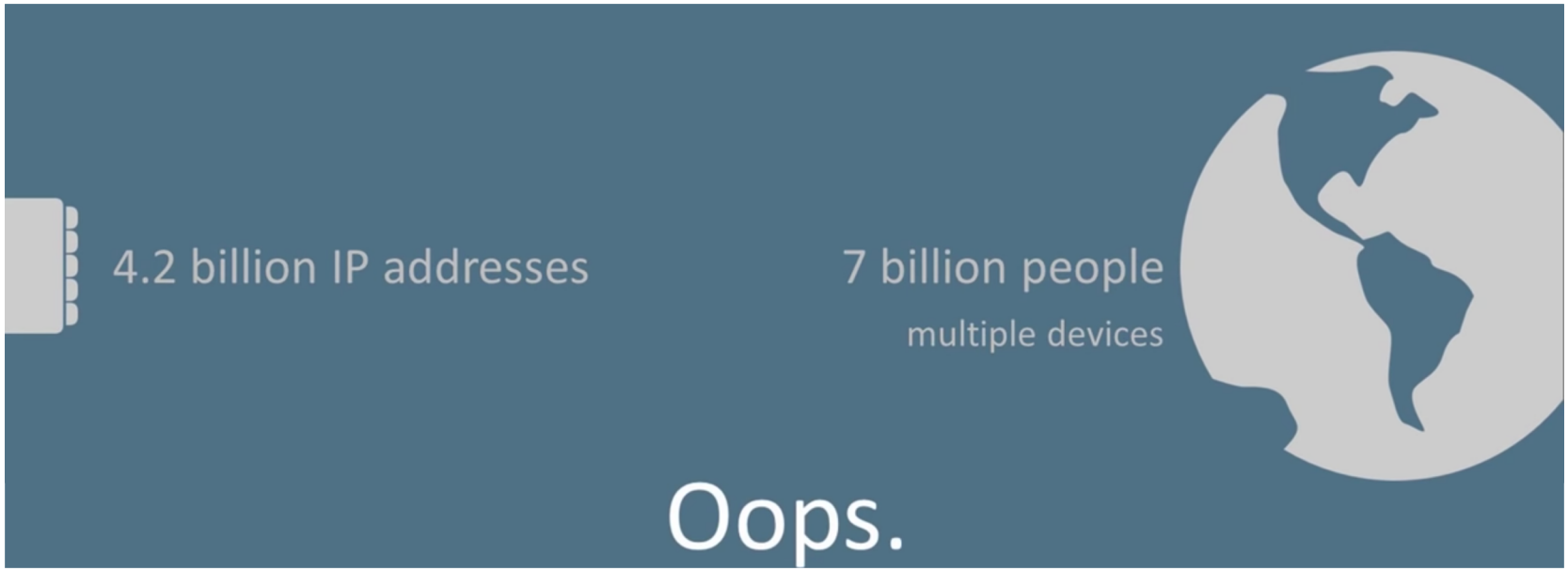


32-bit IP addresses

4,294,967,296 IP addresses

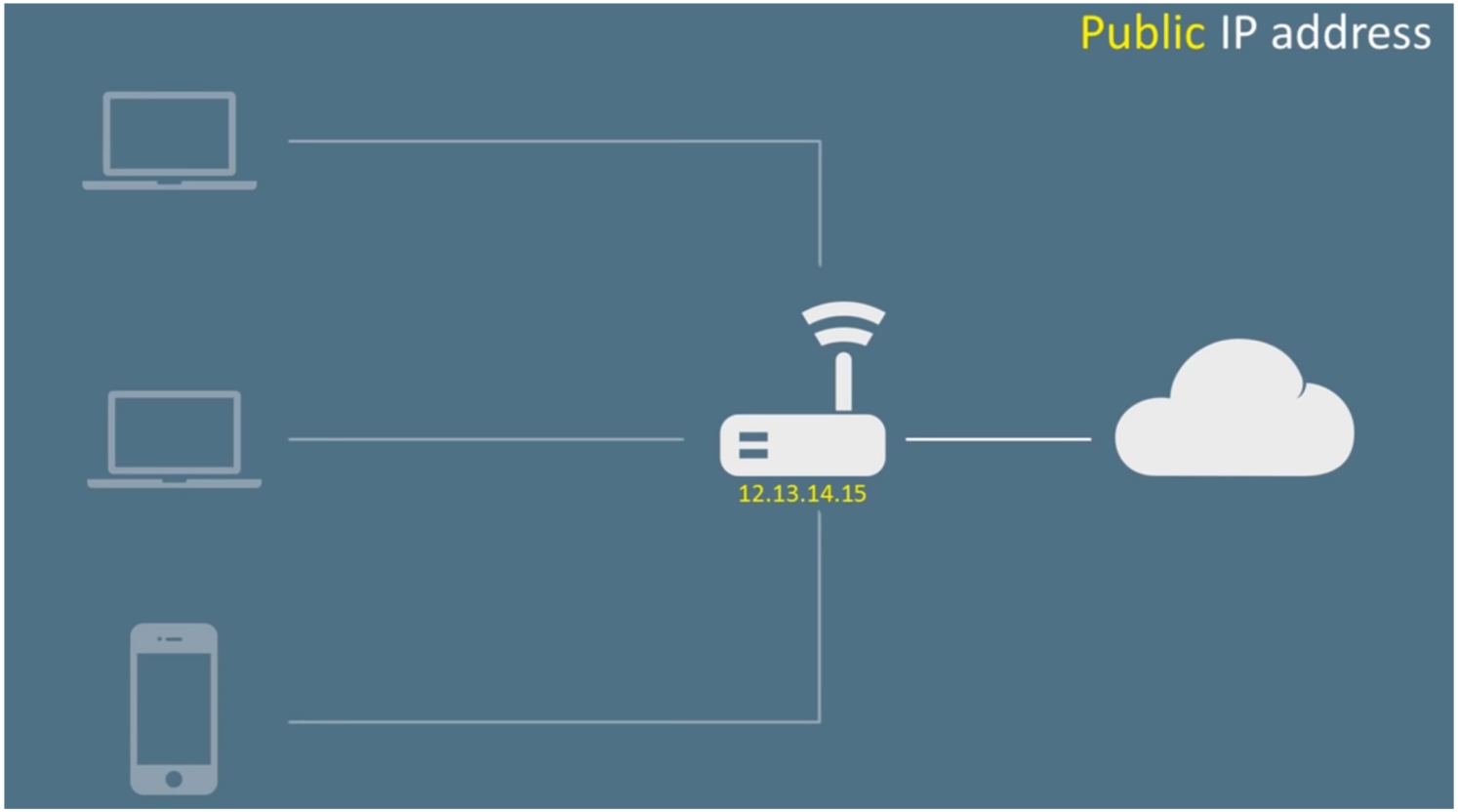
IP version 4

Problem!

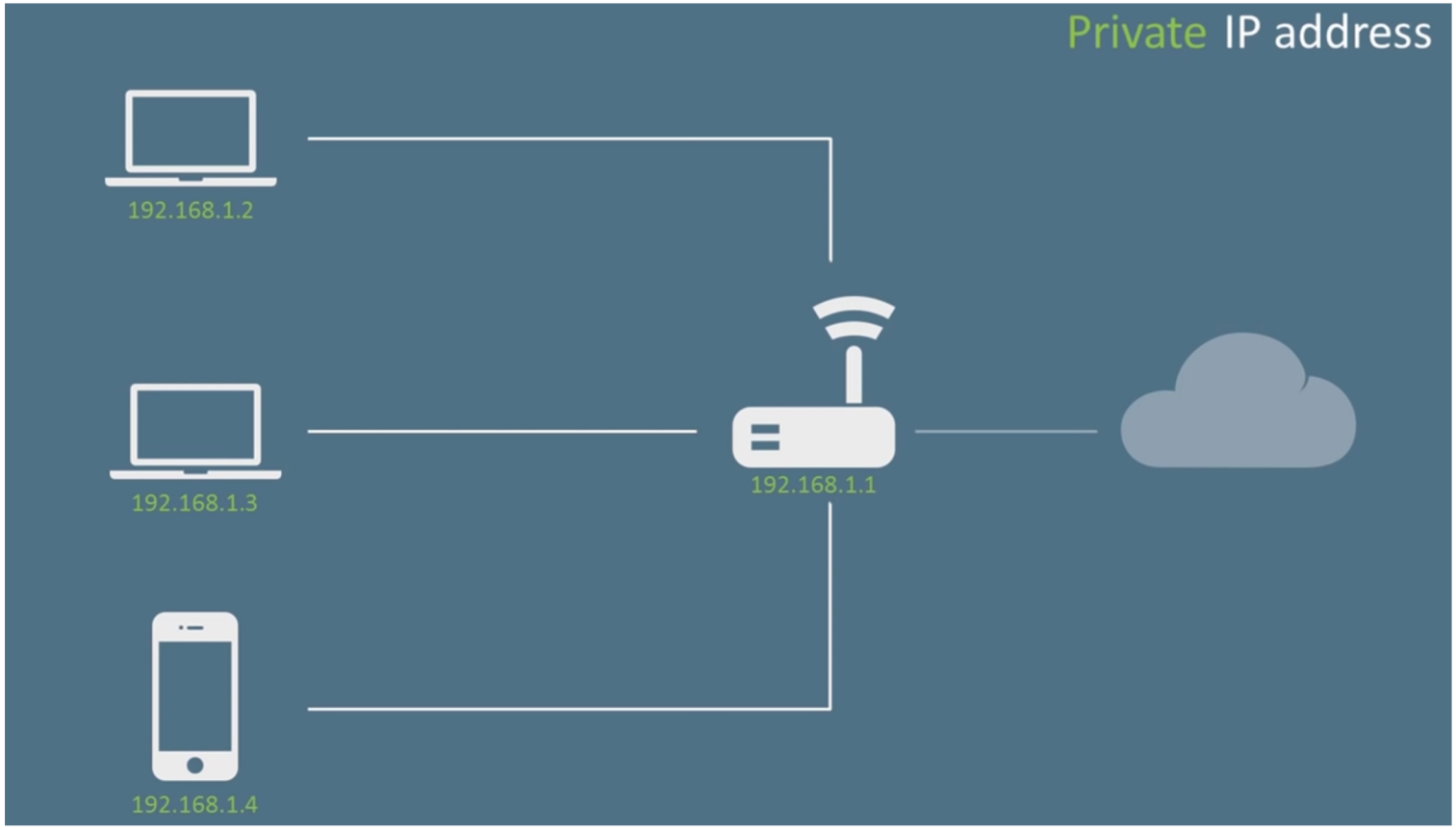

4.2 billion IP addresses
7 billion people
multiple devices
Oops.

The fix

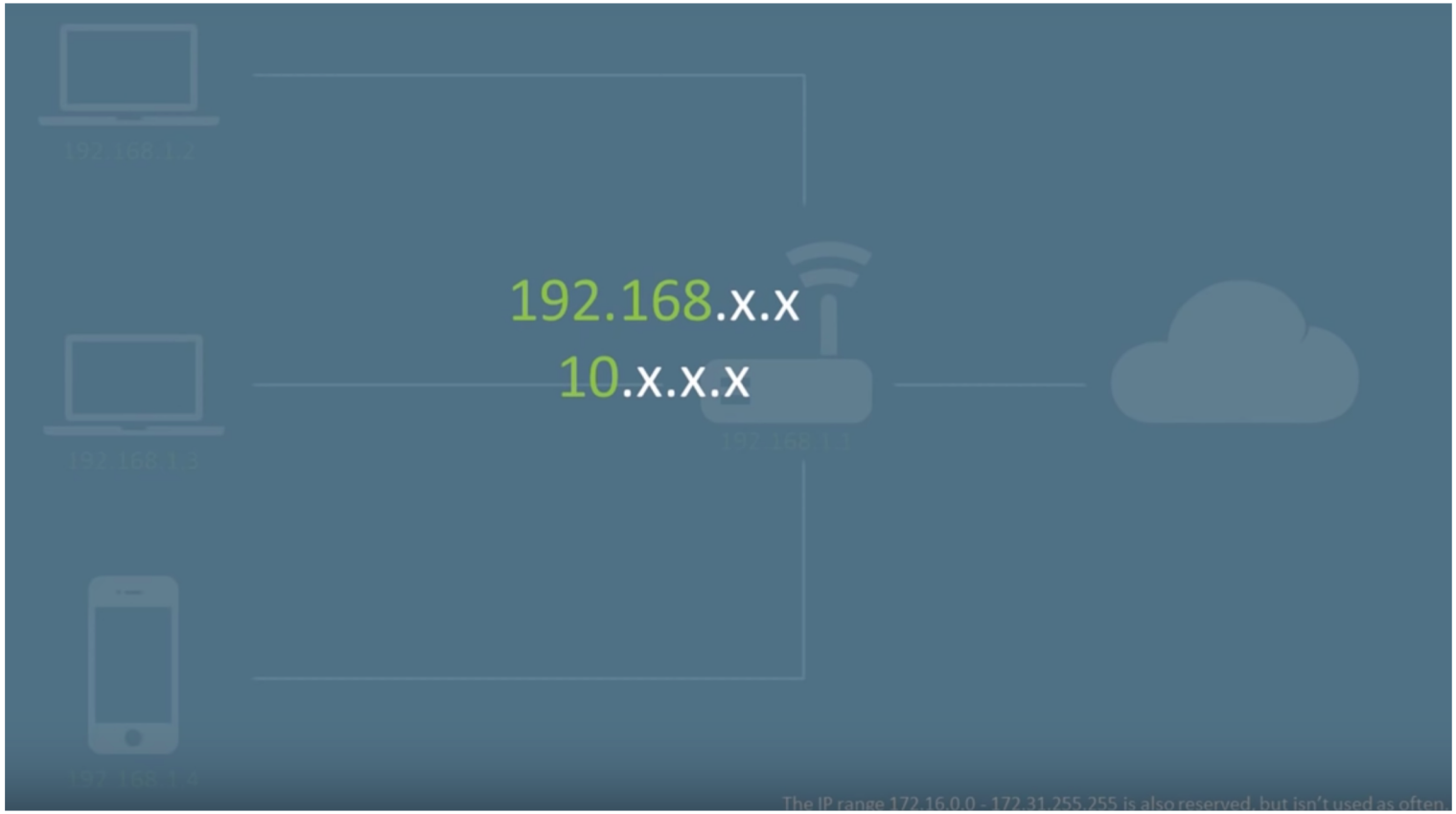
Public IP



Private IP

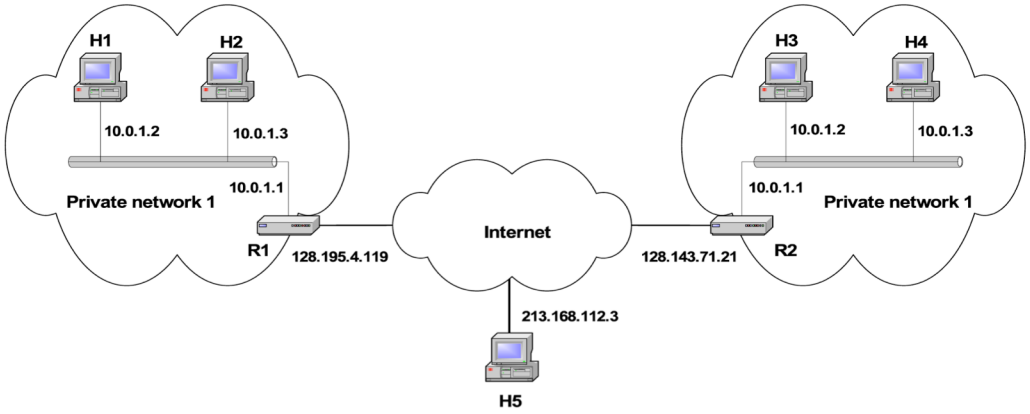


Reserved for Private Networks



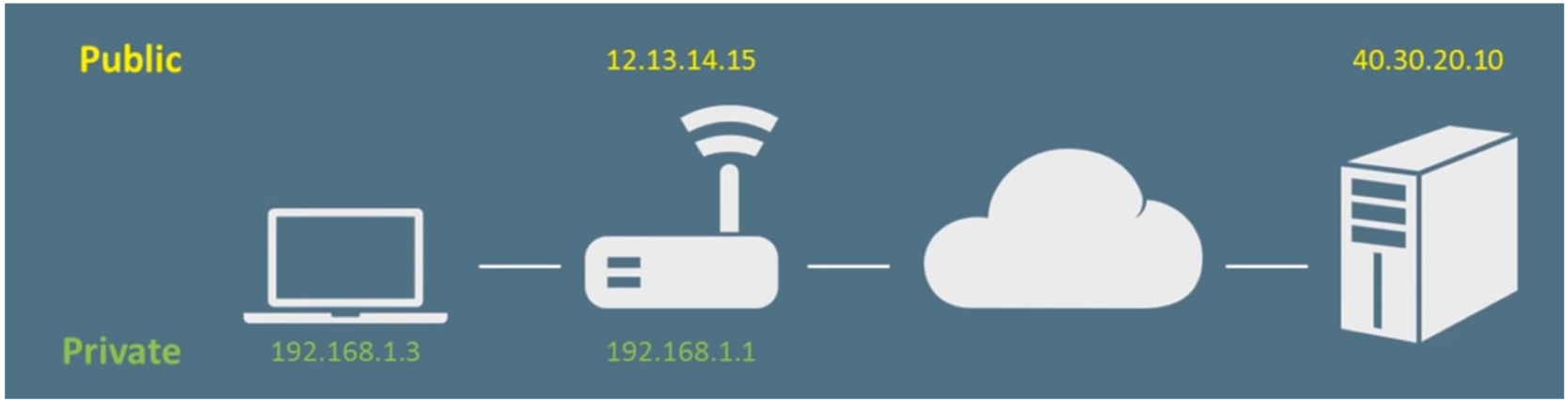
Private Network

- Private IP network is an IP network that is not directly connected to the Internet
- IP addresses in a private network can be assigned arbitrarily.
  - Not registered and not guaranteed to be globally unique
- Generally, private networks use addresses from the following experimental address ranges (non-routable addresses):
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255

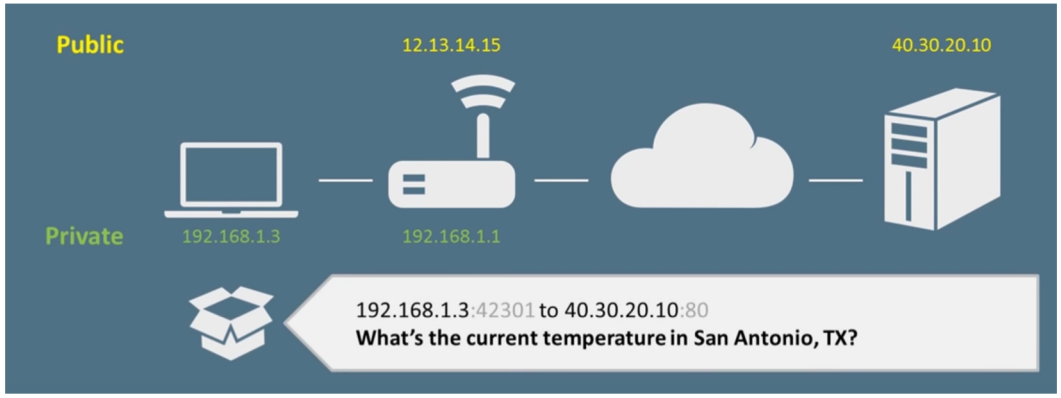


Contact a public server

Contact a public server

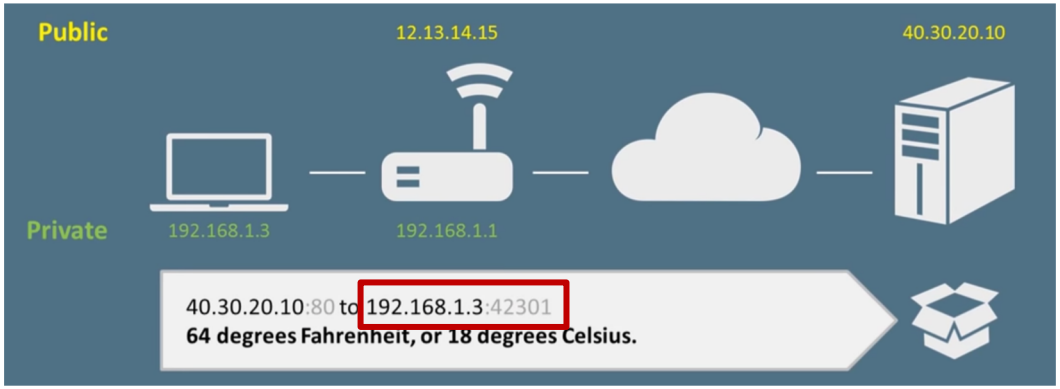


What we expect to happen?



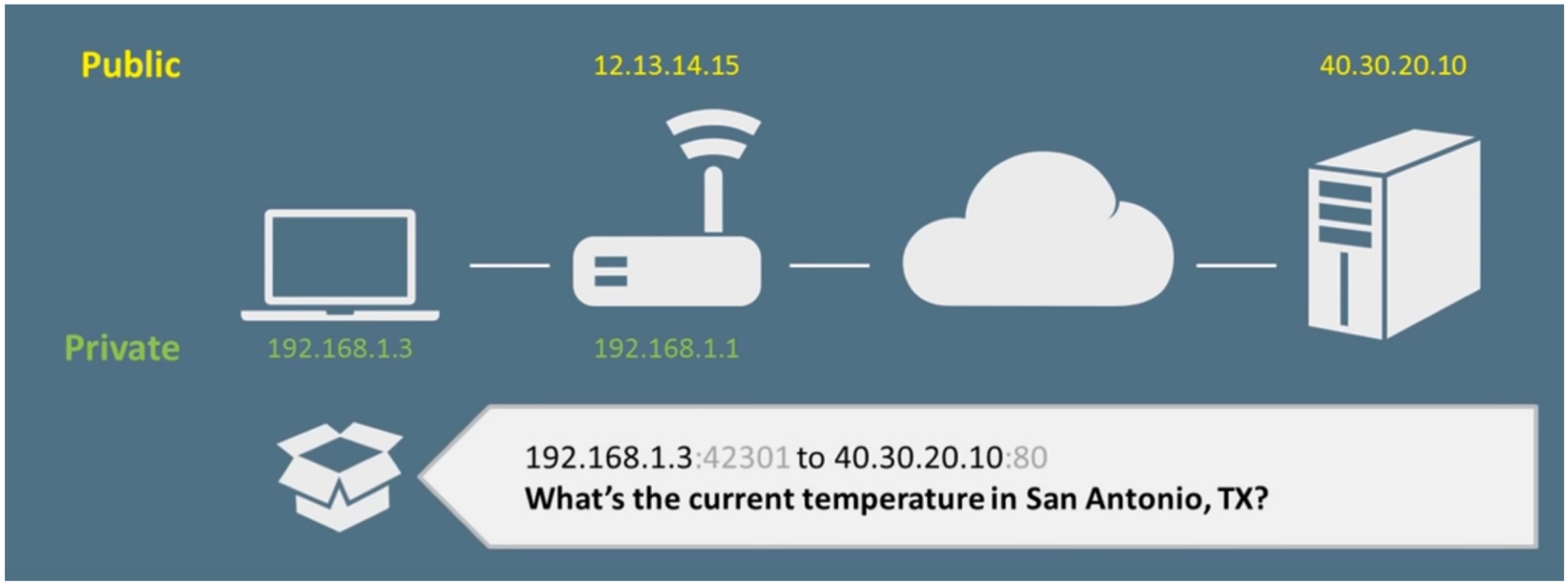
REQUEST

RESPONSE

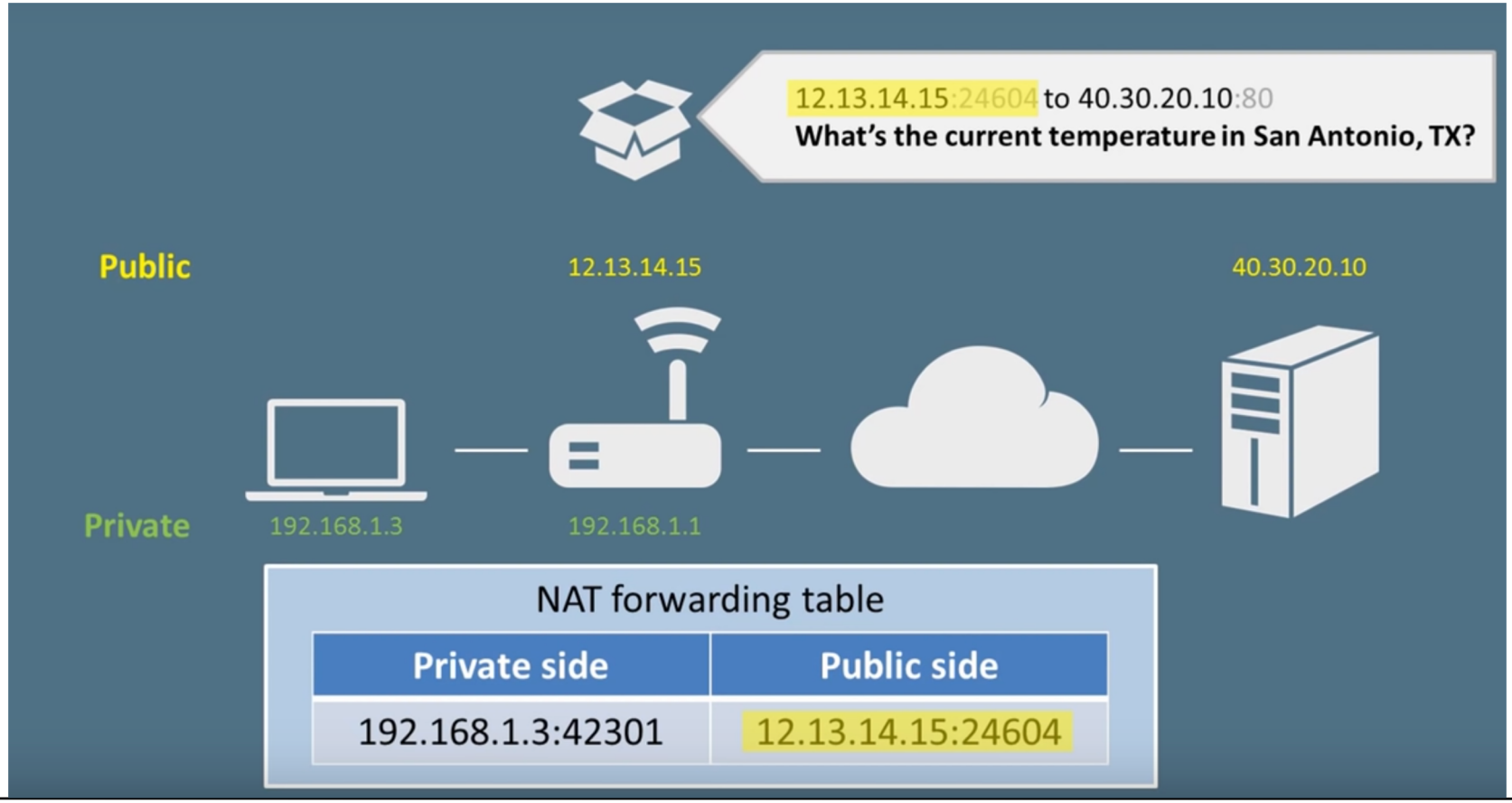


Let’s rewind!

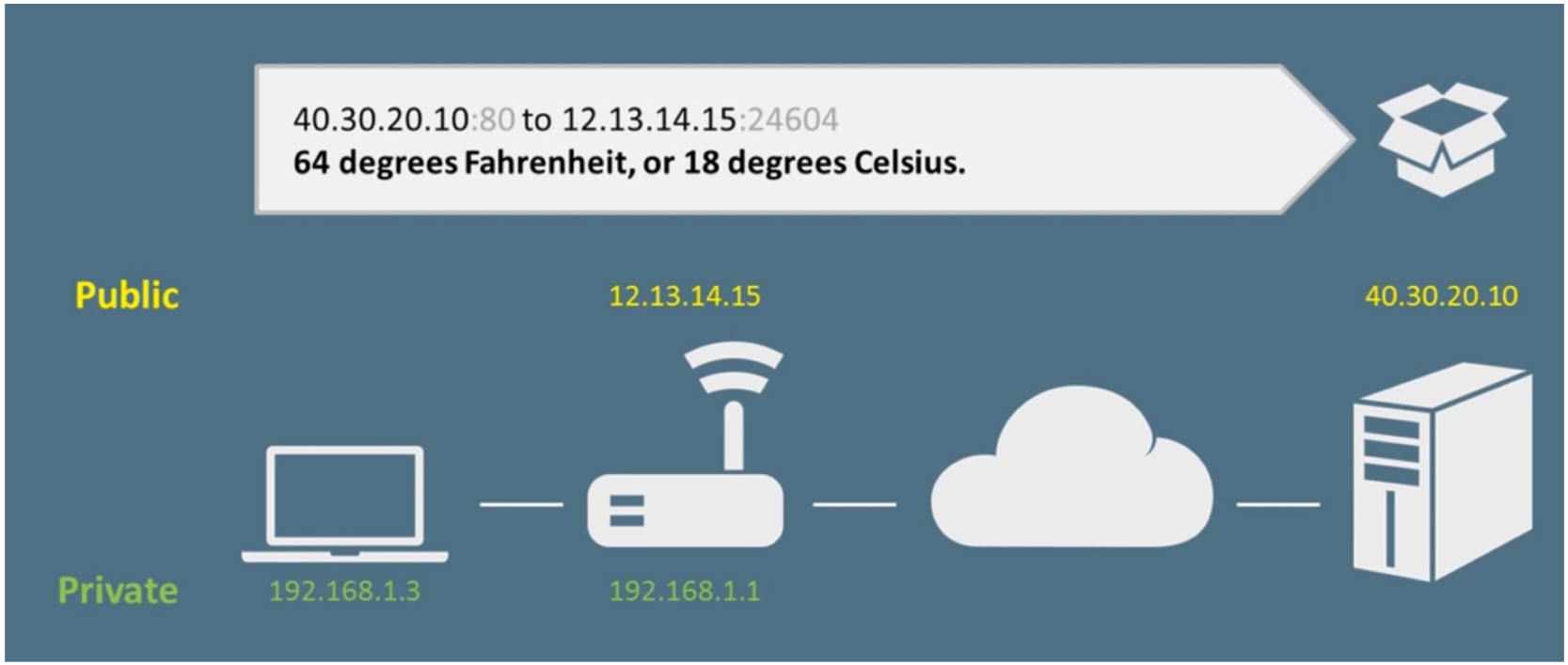
What actually happens? (Part 1)



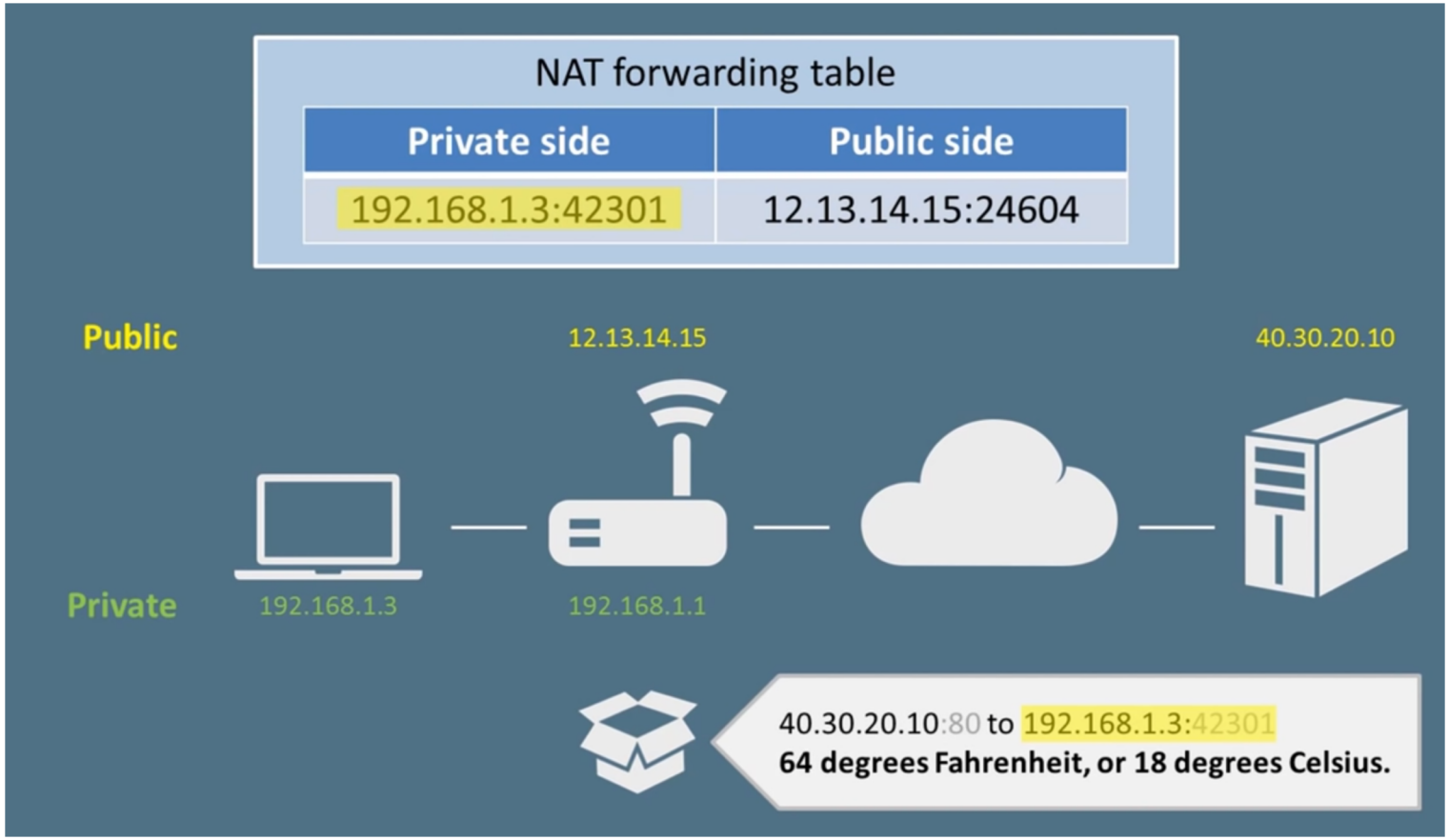
What actually happens? (Part 2)



What actually happens? (Part 3)



What actually happens? (Part 4)

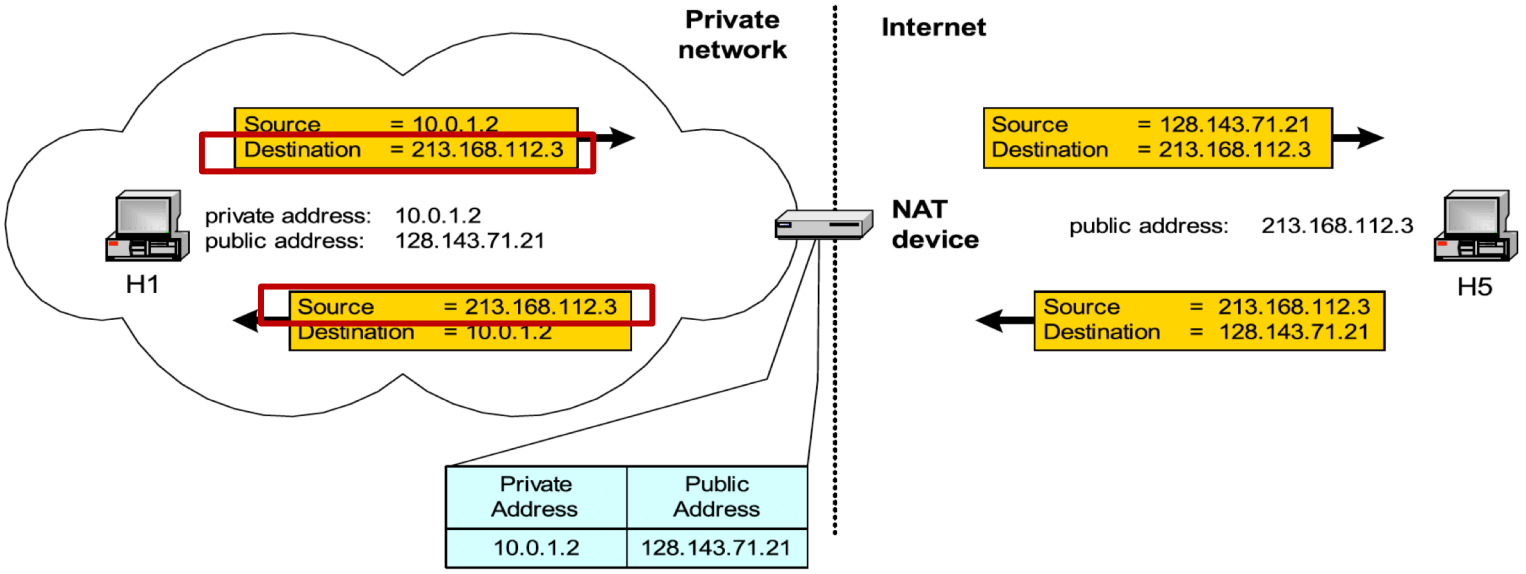


NAT is transparent

NAT

- NAT is a router function where IP addresses (and possibly port numbers) of IP datagrams are replaced at the boundary of a private network
- NAT is a method that enables hosts on private networks to communicate with hosts on the Internet
- NAT is run on routers that connect private networks to the public Internet, to replace the IP address-port pair of an IP packet with another IP address-port pair.

Basic NAT Operation



NAT device has address translation table

Pooling of IP Addresses

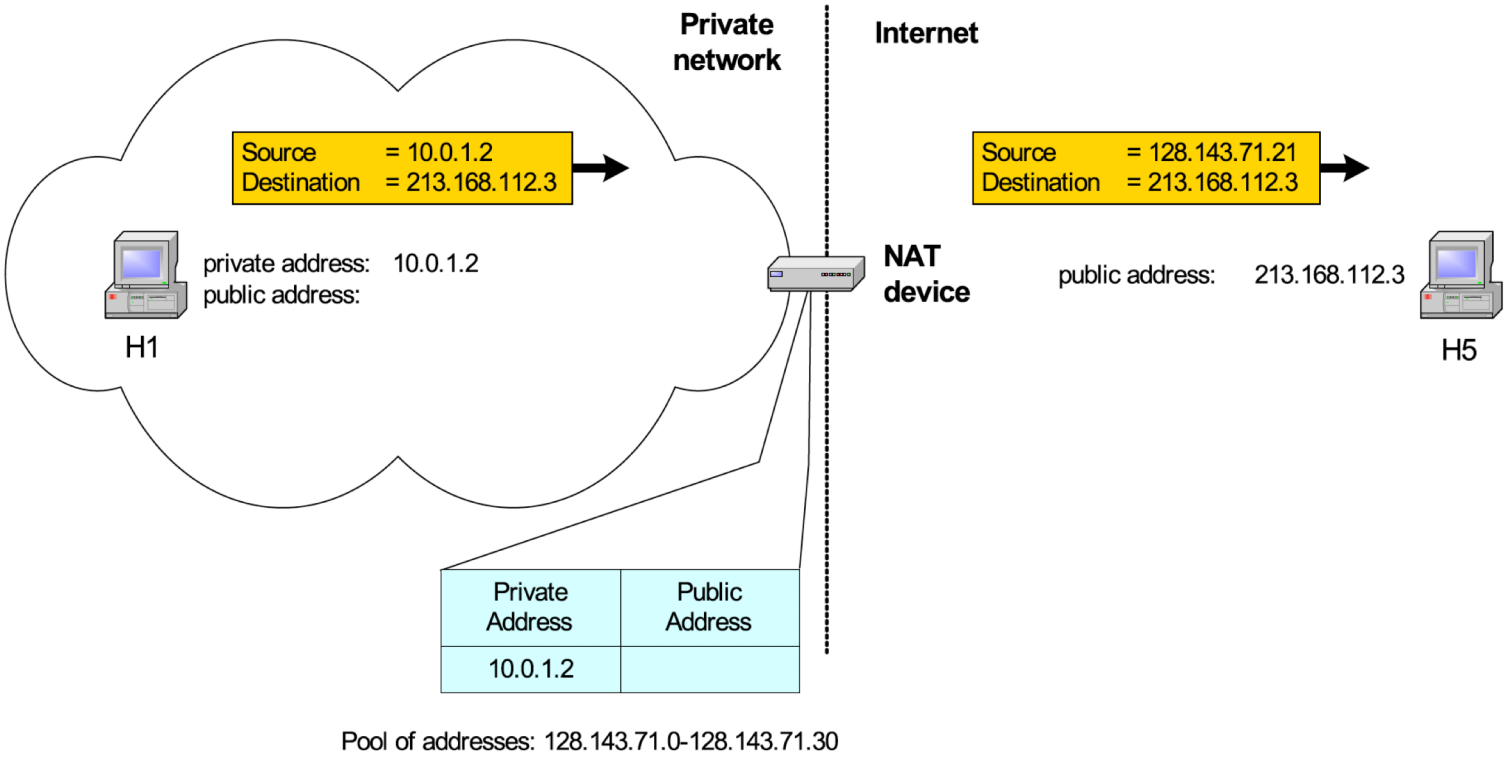
Scenario:

- Corporate network has many hosts but only a small number of public IP addresses

NAT Solution:

- Corporate network is managed with a private address space.
- NAT device, located at the boundary between the corporate network and the public Internet, manages a pool of public IP addresses.
- When a host from the corporate network sends an IP datagram to a host in the public Internet, the NAT device picks a public IP address from the address pool, and binds this address to the private address of the host

Pooling of IP Addresses



Load Balancing of Servers

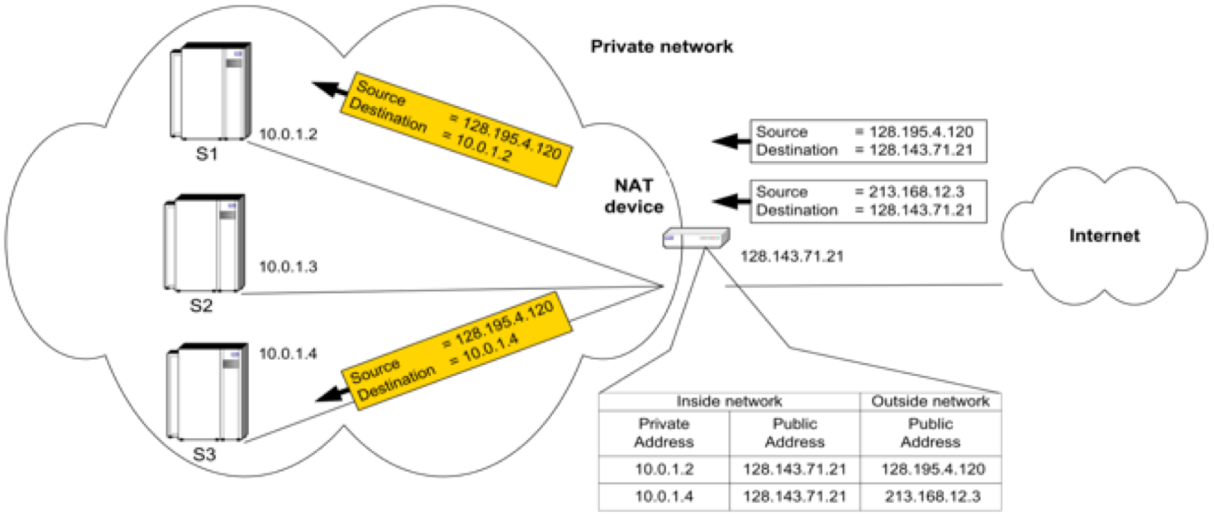
Scenario:

- Balance the load on a set of identical servers, which are accessible from a single IP address

NAT Solution:

- Here, the servers are assigned private addresses.
- NAT device acts as a proxy for requests to the server from the public network.
- The NAT device changes the destination IP address of arriving packets to one of the private addresses for a server.
- A sensible strategy for balancing the load of the servers is to assign the addresses of the servers in a round-robin fashion.

Load Balancing of Servers



Concerns about NAT

- Performance
  - Modifying the IP header by changing the IP address requires that NAT boxes recalculate the IP header checksum.
  - Modifying port number requires that NAT boxes recalculate TCP checksum
- Fragmentation
  - Care must be taken that a datagram that is fragmented before it reaches the NAT device, is not assigned a different IP address or different port numbers for each of the fragments
- End to end connectivity
  - NAT destroys universal end-to-end reachability of hosts on the Internet.
  - A host in the public Internet often cannot initiate communication to a host in a private network.
  - The problem is worse, when two hosts that are in a private network need to communicate with each other.

Week 11

> NAT

> VPN

Virtual Private Networks

Why a VPN


The Deathly Hallows, Part 2
I was wrong about Downton errors
The Daily Telegraph
Hackers 'snooped on Soham families'
Police contact parents of murdered Holly Wells and Jessica Chapman
Relations of 7/7 bomb victims were also targeted by News of the World
More pay in public sector and the gap is growing
vodafone


newspaper of the year
theguardian
News of the World hacked Milly Dowler's phone during police hunt
Exclusive Paper deleted missing schoolgirl's voicemails, giving family false hope
'It is distress heaped on tragedy to learn that the News of the World had no humanity at such a terrible time'
Rebekah Brooks
CEO of News International was editor of the News of the World when Milly Dowler's phone was hacked
Andy Coulson
Former head of communications at No 10 was Brooks's deputy in 2002 and became News of the World editor in 2003
Glenn Mulcaire
Investigator hacked into Milly Dowler's phone for News of the World, allowing paper to listen to friends' messages

Staying safe online!

1. Updating your Application security settings
2. Creating long, secure passwords
3. Start using a VPN

What is Network Layer Confidentiality

Between two network entities:

- Sending entity encrypts datagram payload, payload could be:
  - TCP or UDP segment, ICMP message, OSPF message ….
- All data sent from one entity to other would be hidden:
  - web pages, e-mail, P2P file transfers, TCP SYN packets …

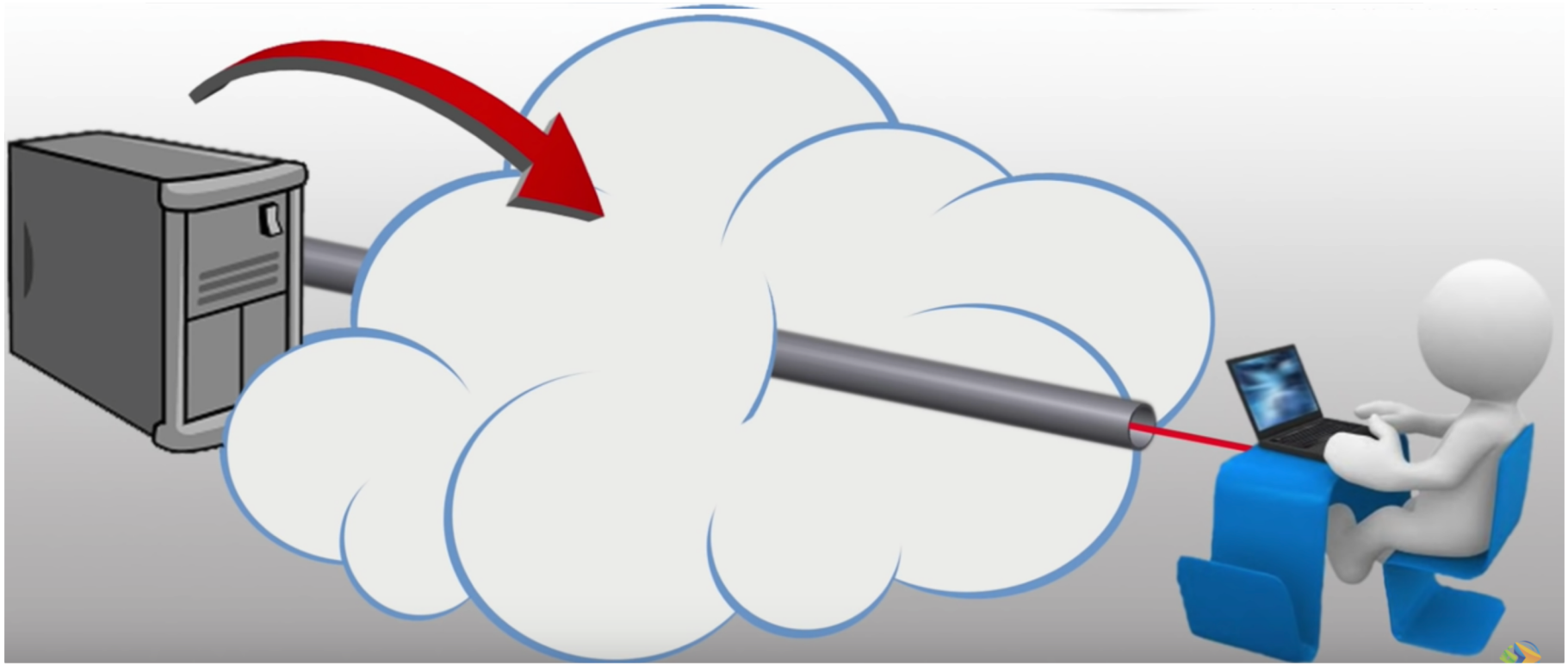
"Blanket Coverage"

What is a Virtual Private Networks

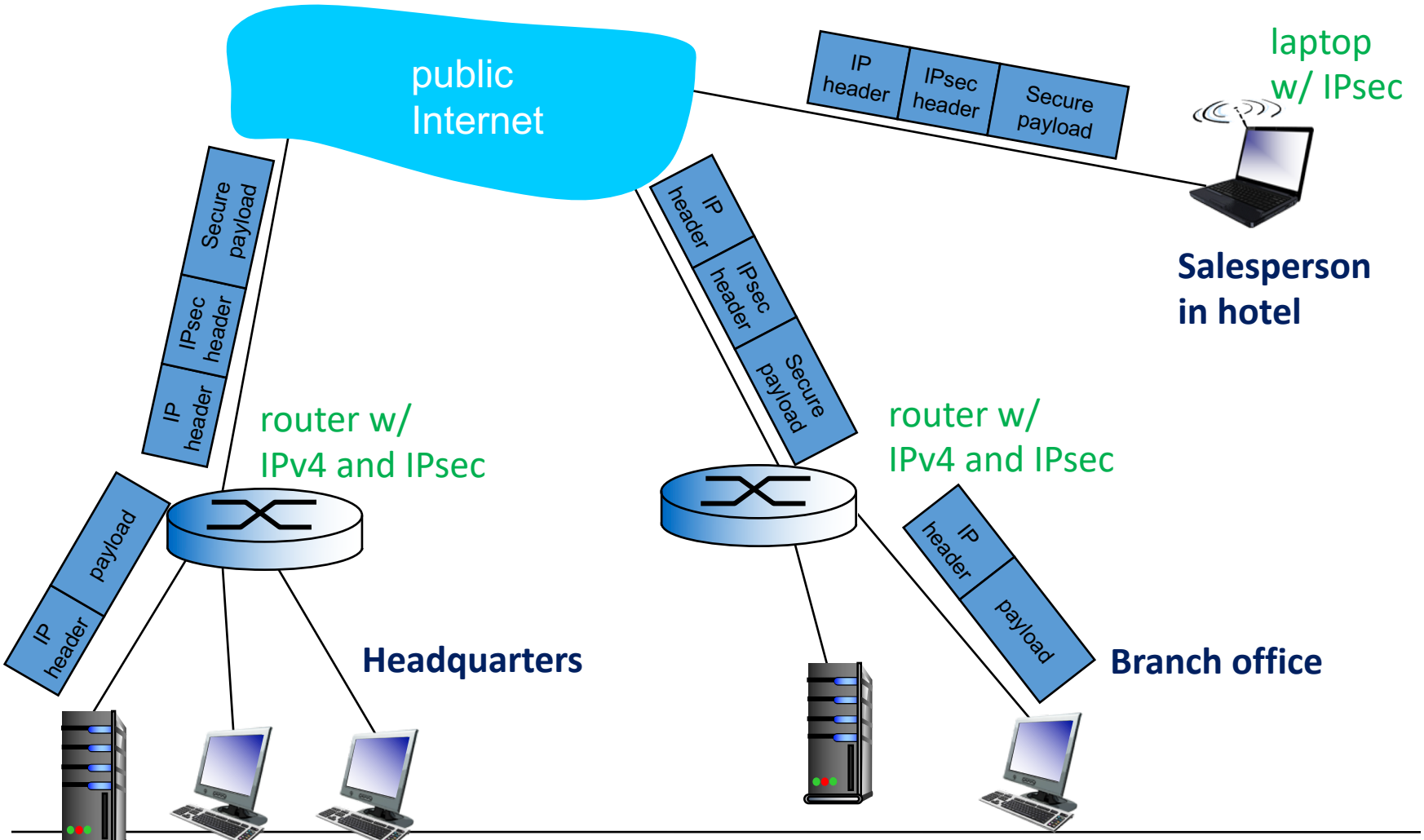
A technology that allows for the extension of a private or local network to hosts that might not be on that local network.

VPN is used to encrypt your data and to add a layer of privacy to protect your identity

What is a VPN



VPN Example


public
Internet
IP header
IPsec header
Secure payload
laptop
w/ IPsec
Salesperson
in hotel
router w/
IPv4 and IPsec
router w/
IPv4 and IPsec
IP header
payload
Headquarters
Branch office

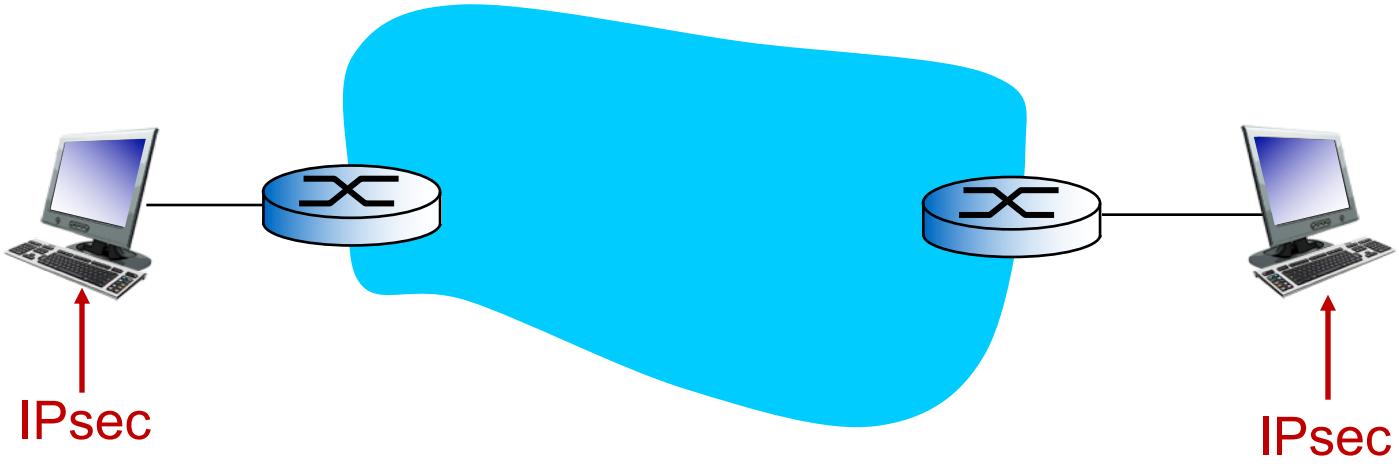
IPSec Services

- Data integrity
- Origin authentication
- Replay attack prevention
- Confidentiality

Two protocols providing different service models:

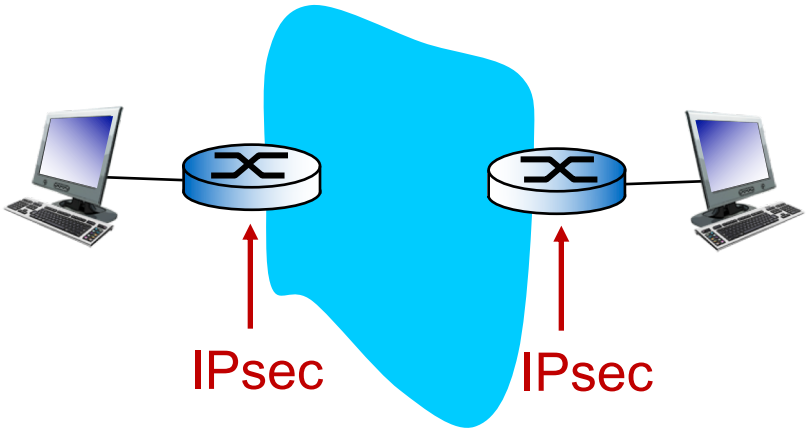
- AH
- ESP

IPSec Transport Mode

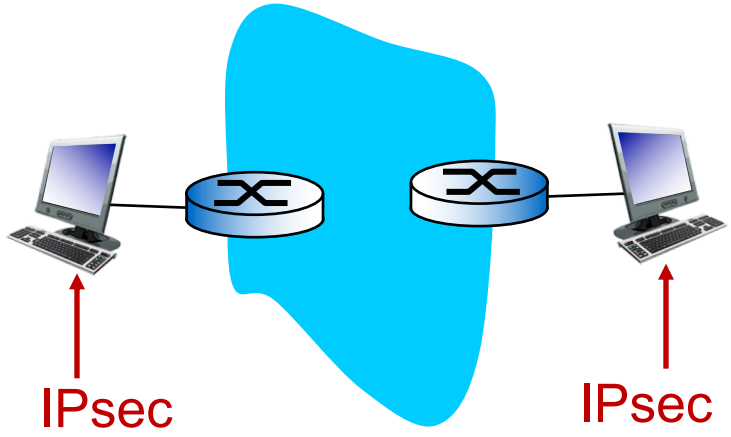


- IPsec datagram emitted and received by end-system
- protects upper level protocols

IPSec Tunneling mode



edge routers IPsec-aware



hosts IPsec-aware

IPSec Protocols

- Authentication Header (AH) protocol
  - provides source authentication & data integrity but *not* confidentiality
- Encapsulation Security Protocol (ESP)
  - provides source authentication, data integrity, *and* *confidentiality*
  - more widely used than AH

Using a VPN

Spoofing your location

Why not use a VPN

1. Most people don’t understand the security risk
2. VPNs cause a natural loss in internet speeds
3. Personal VPNs cost $$$$

Final Thoughts!