



# CSCI-3403: Cyber Security

## Spring 2020

**Abigail Fernandes**

**Department of Computer Science**  
**University of Colorado Boulder**

# Week 11

- > NAT
- > VPN

# Network Address Translation

# Backstory!

## The backstory

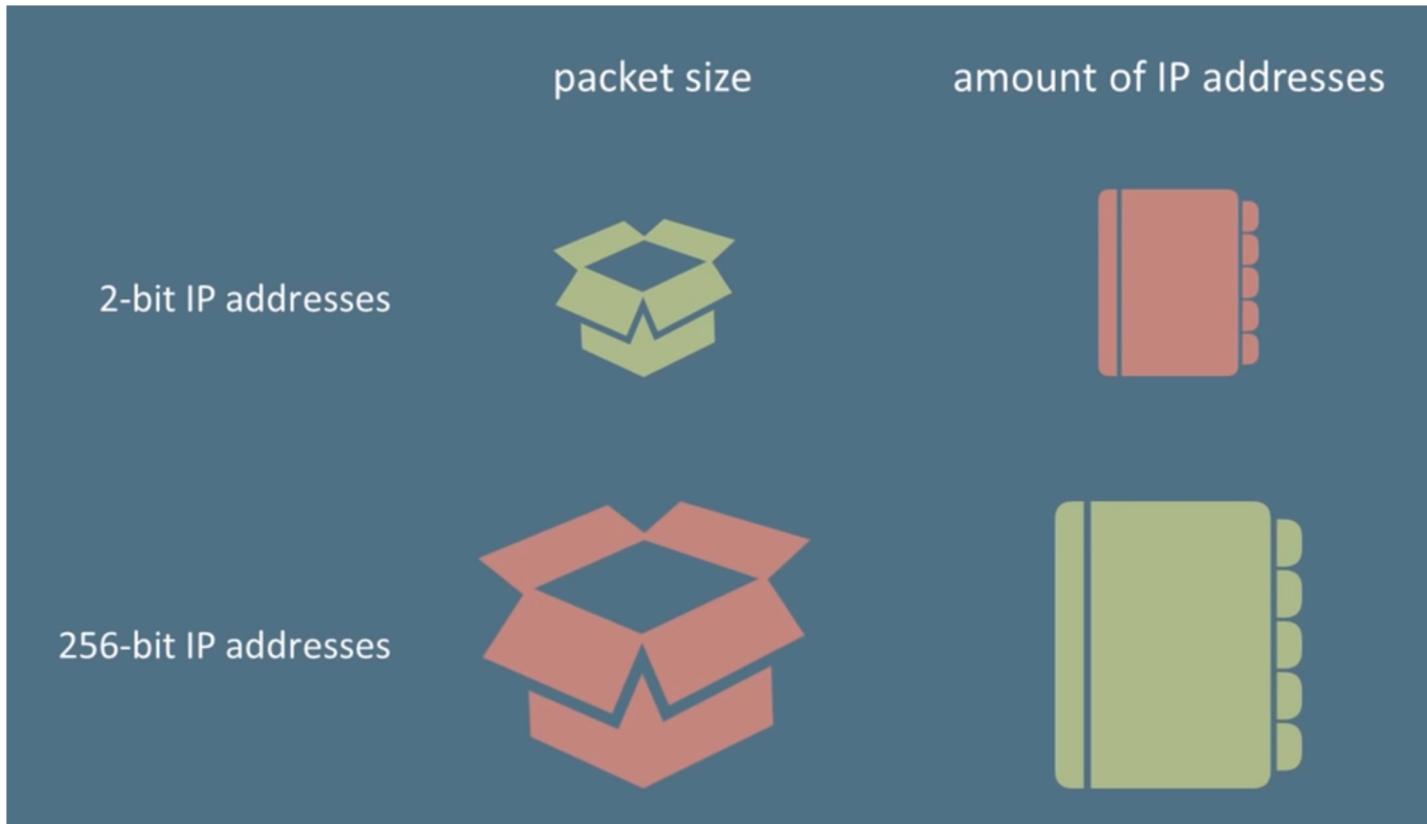
Where do IP addresses come from?



# History of IP Addresses



# IP Address Size



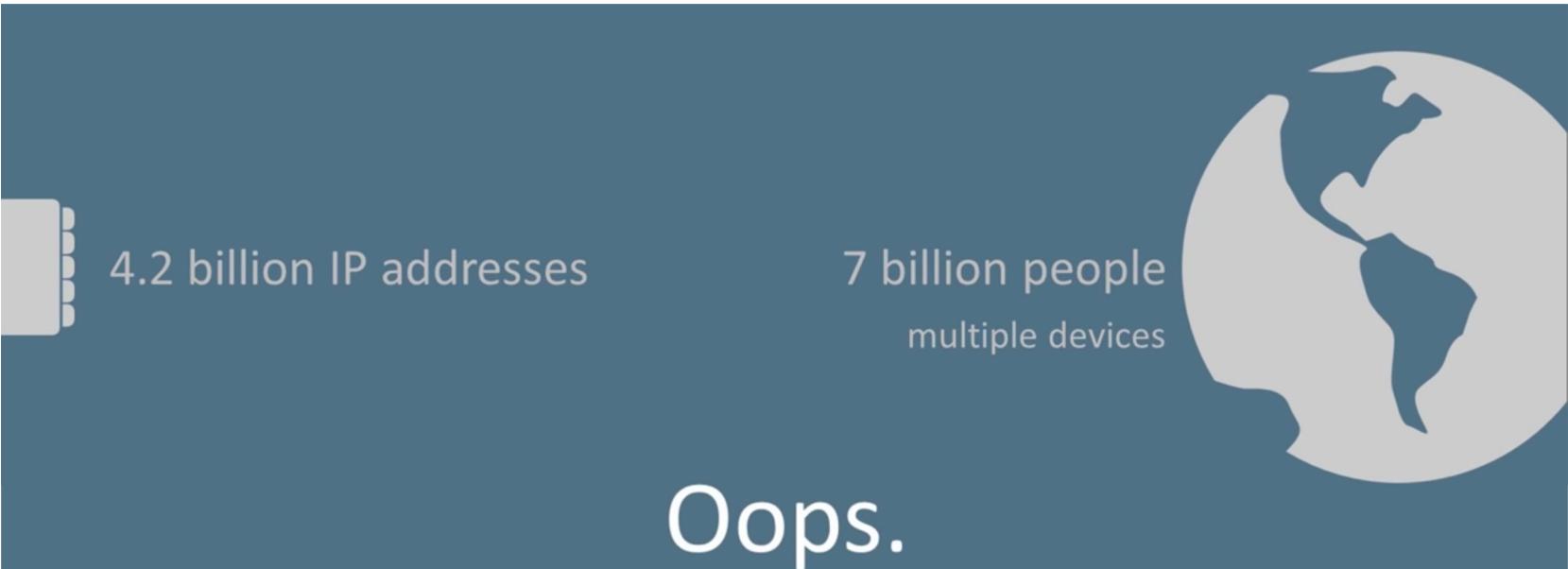
32-bit IP addresses

4,294,967,296 IP addresses

IP version 4



# Problem!



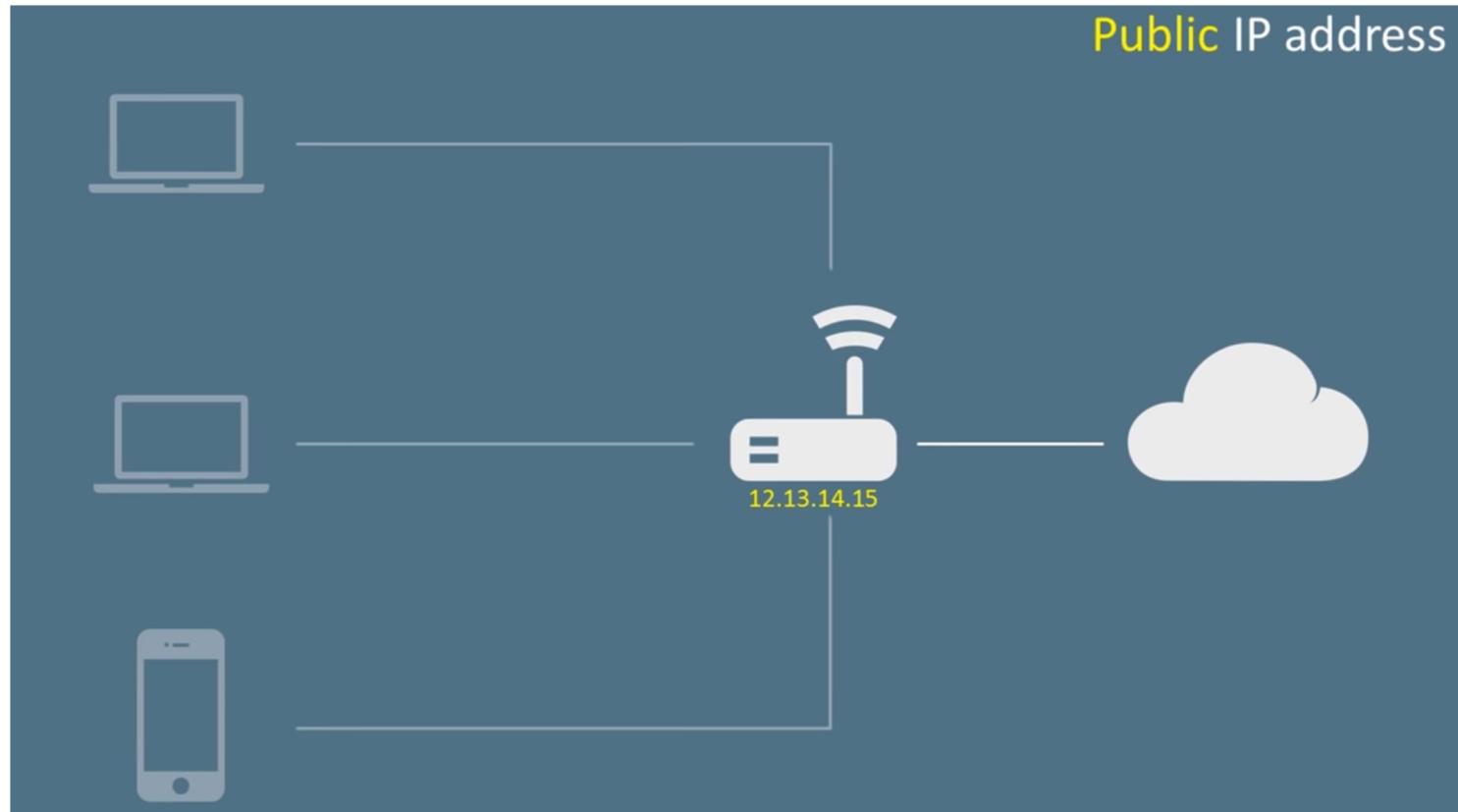
# The fix

The fix

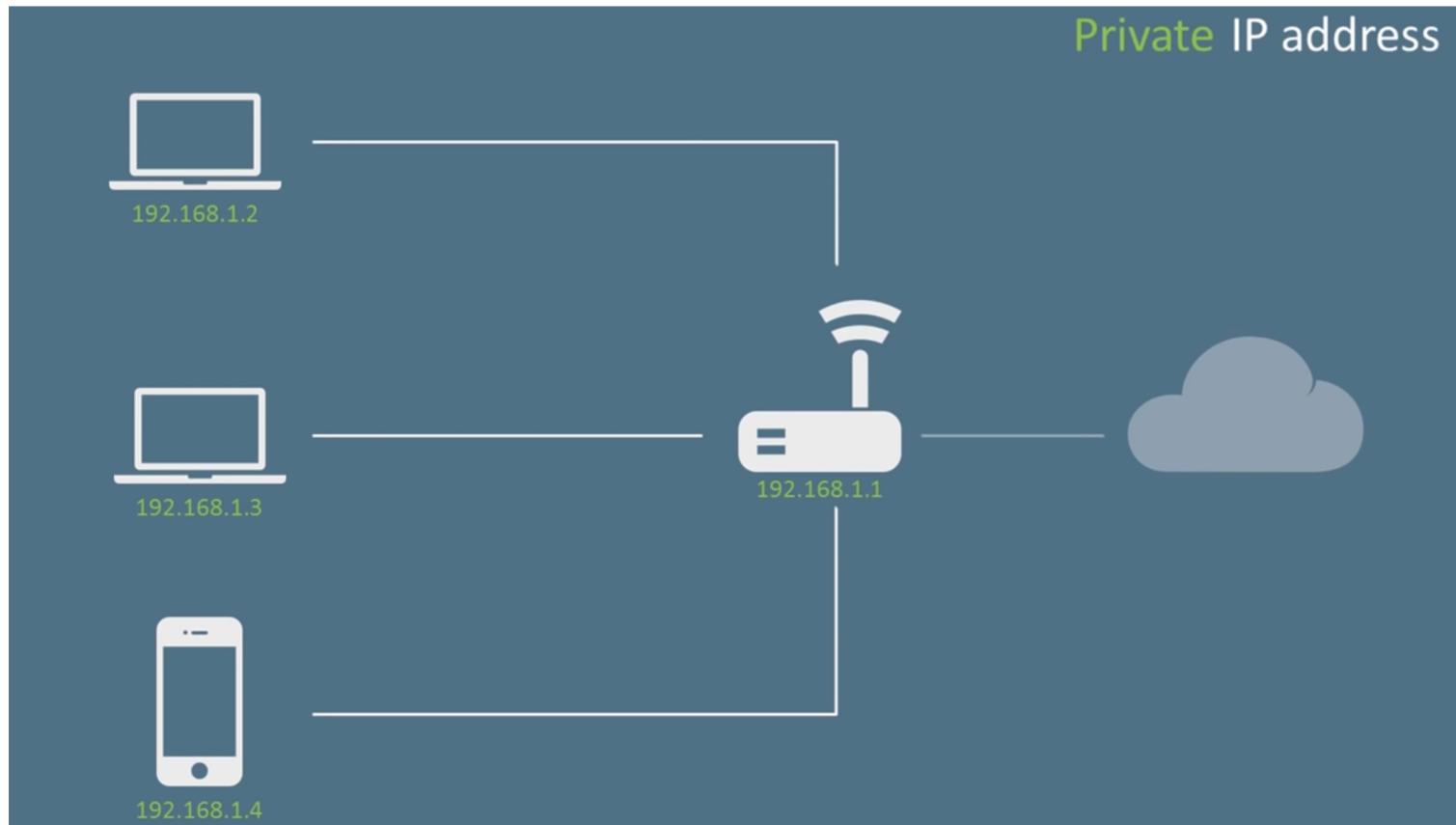
Network Address Translation



# Public IP



# Private IP

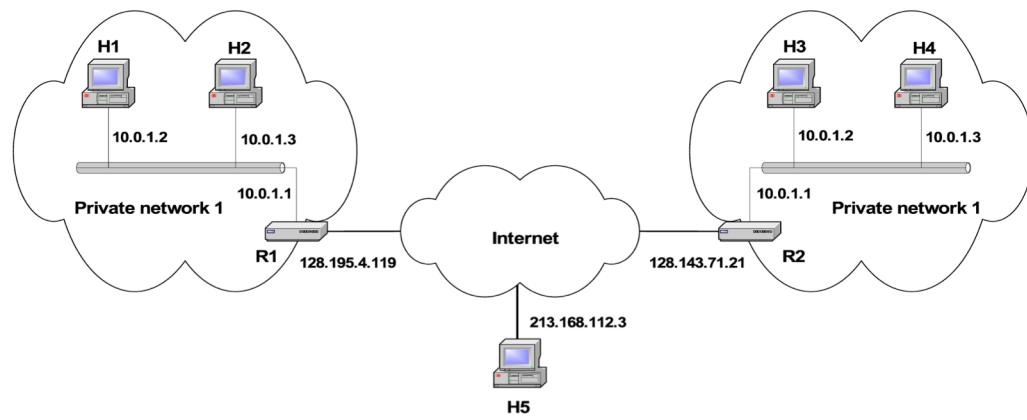


# Reserved for Private Networks



# 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



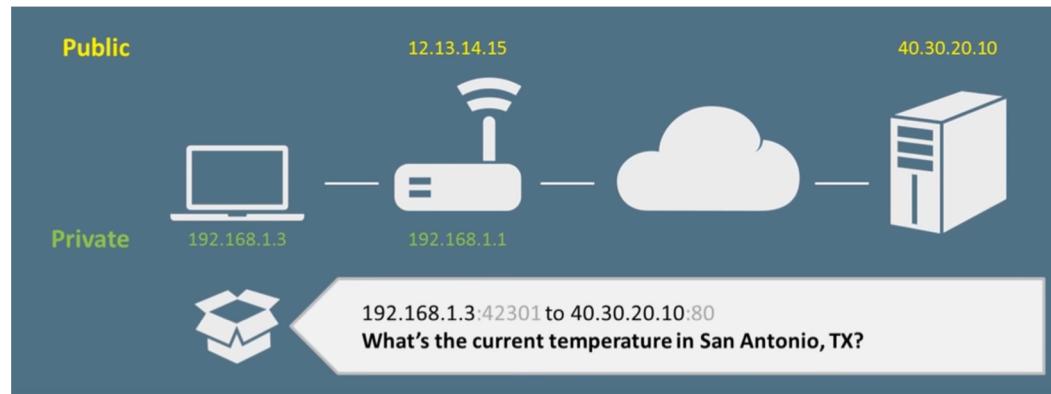
# Contact a public server



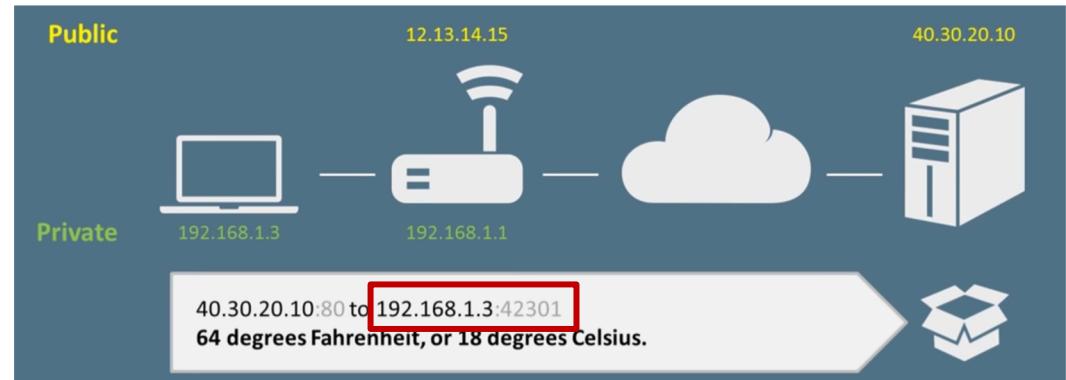
# Contact a public server



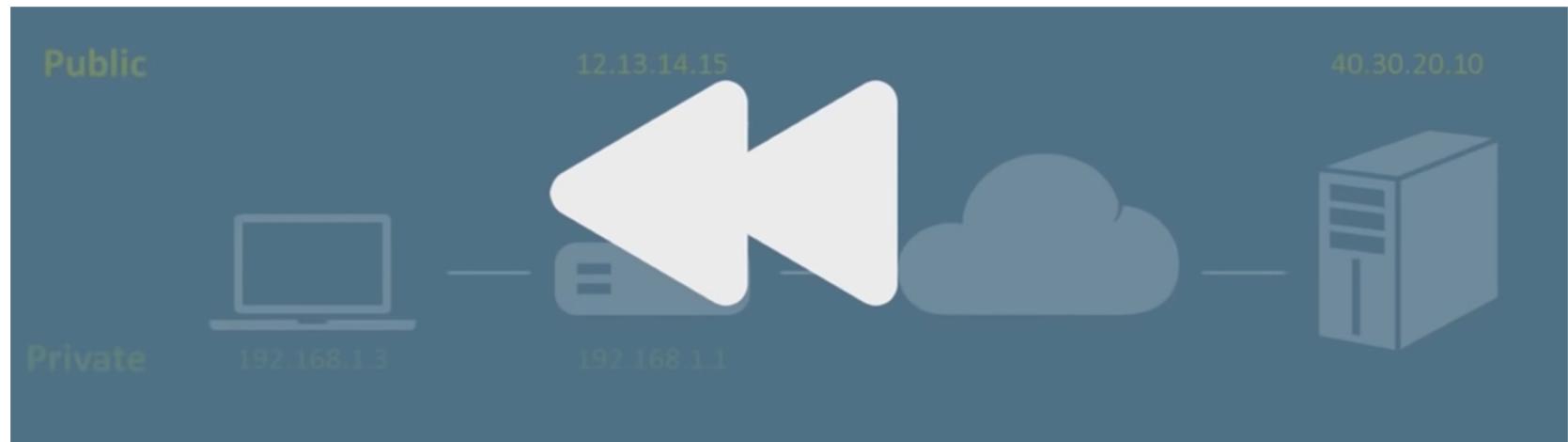
# What we expect to happen?



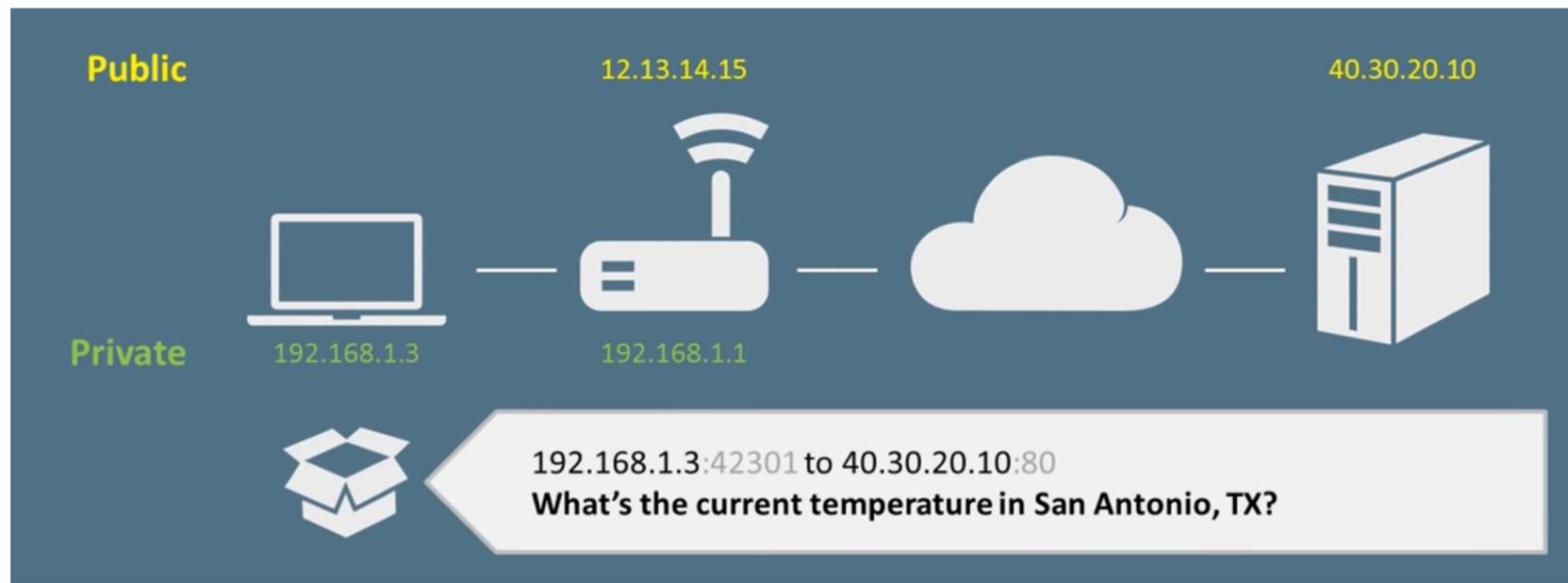
RESPONSE



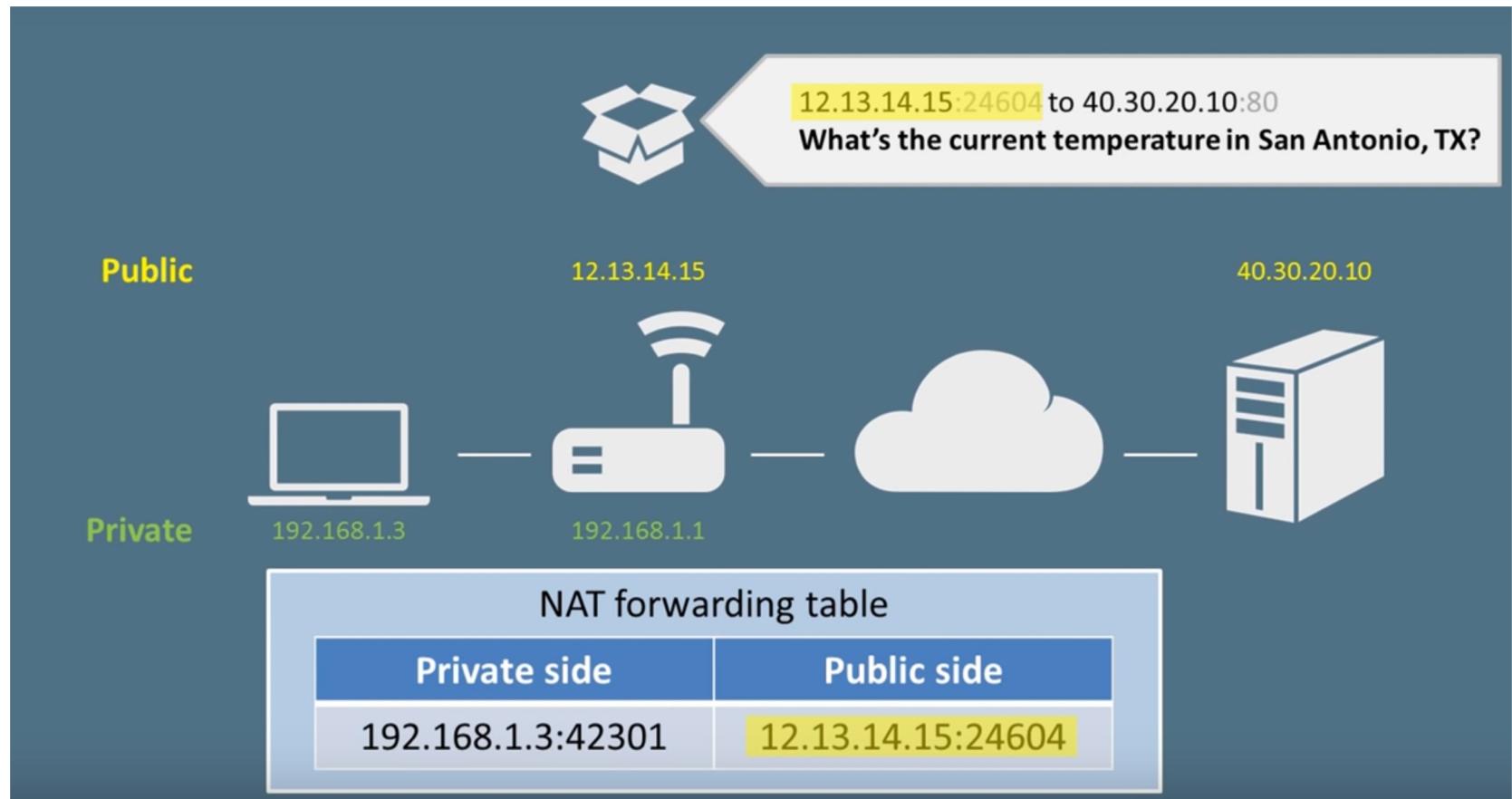
# Let's rewind!



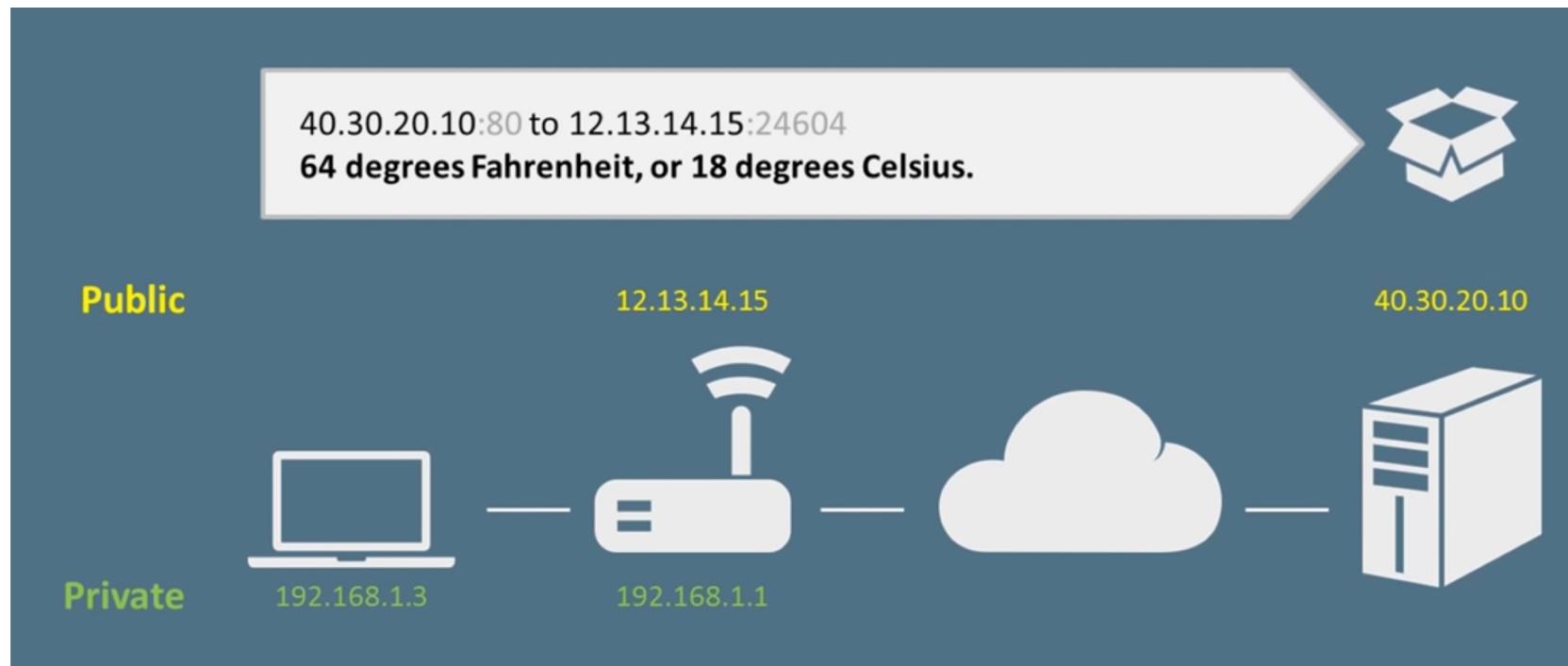
# What actually happens? (Part 1)



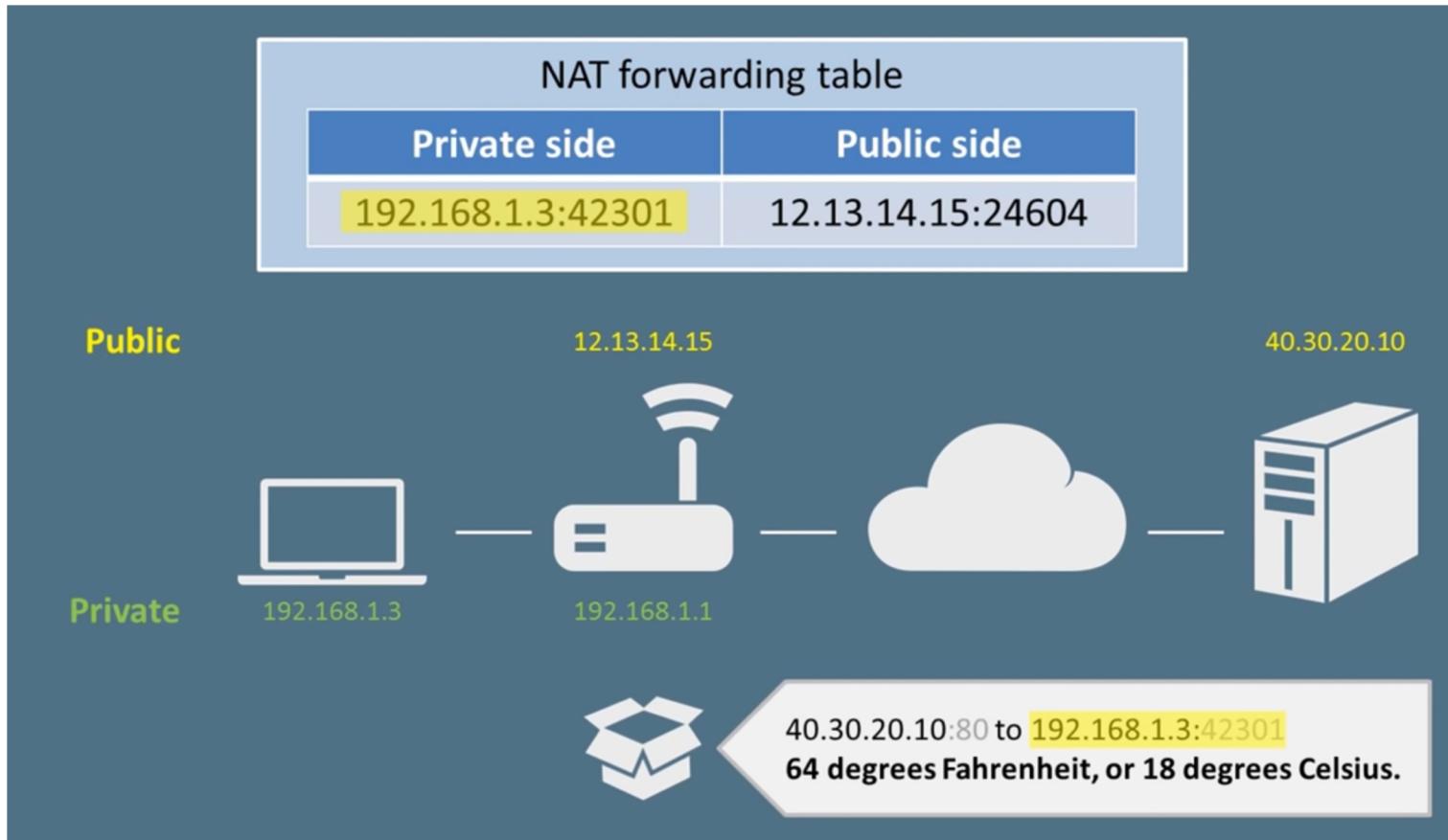
# What actually happens? (Part 2)



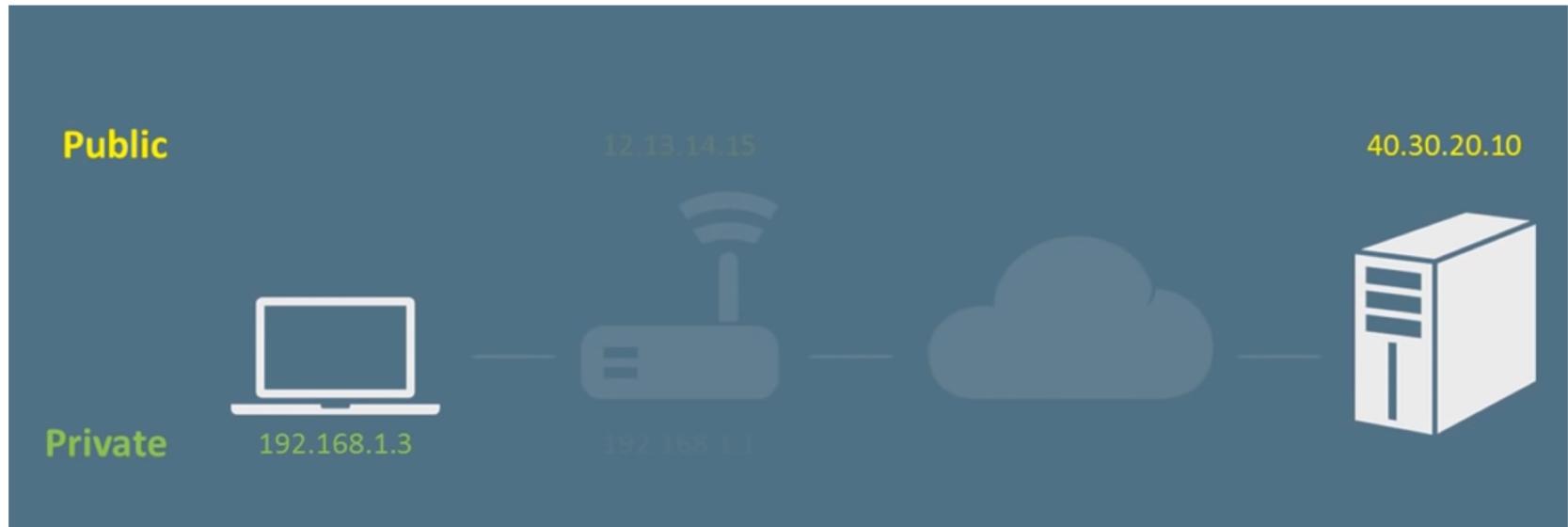
# What actually happens? (Part 3)



# What actually happens? (Part 4)



# NAT is transparent

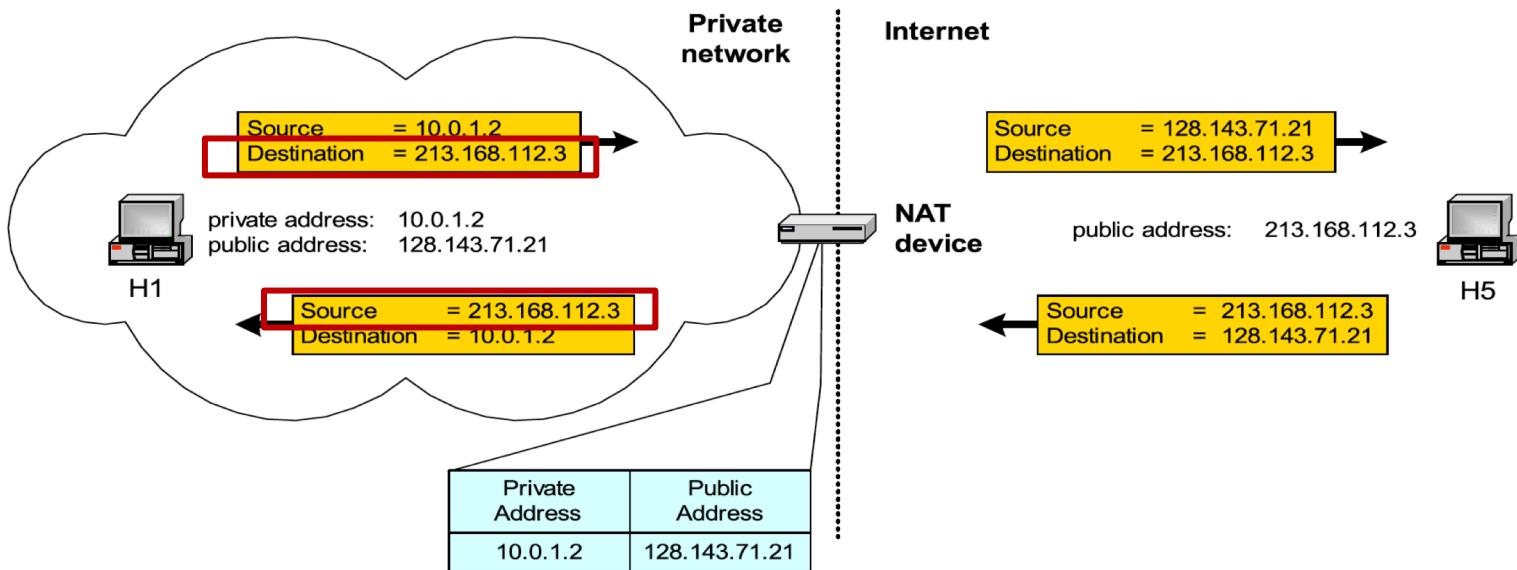


# NAT

- 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:

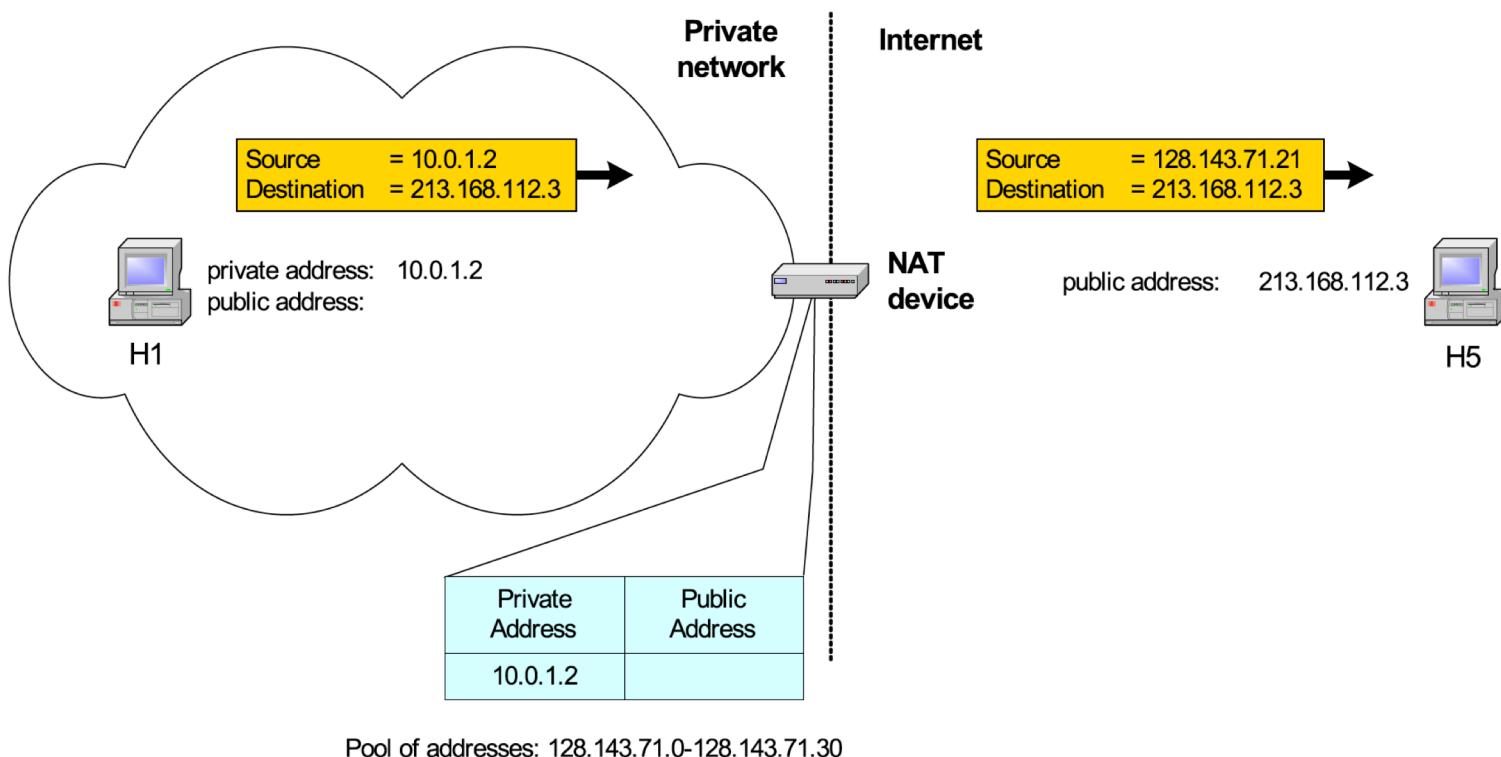
- Corporate network has many hosts but only a small number of public IP addresses

## 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:

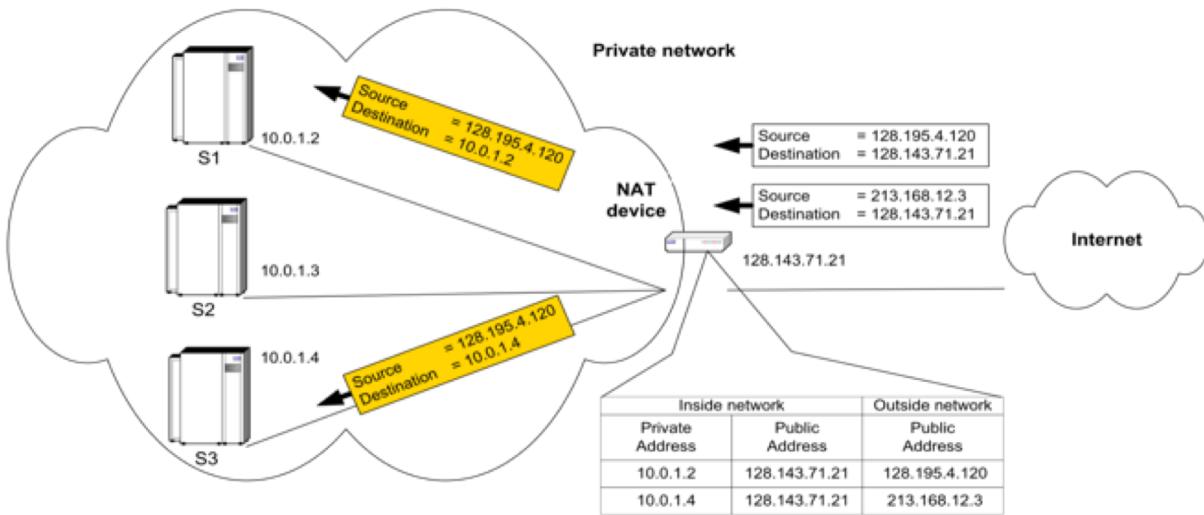
- Balance the load on a set of identical servers, which are accessible from a single IP address

## 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 Daily Telegraph

Wednesday, June 15, 2011

**The first review**  
The Deathly Hallows, Part 2 [more](#)

**JULIAN FELLOWES**  
I was wrong about Downton errors [more](#)

# The Daily Telegraph

Hackers 'snooped on Soham families'

Police contact parents of murdered Holly Wells and Jessica Chapman

Relations of 27 bomb victims were also targeted by News of the World

More pay in public sector and the gap is growing

News of the World

It is distress heaped on tragedy to learn that the News of the World had no humanity at such a terrible time

Mark Lewis, Bowes family lawyer

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' deputy in 2002 and became News of the World editor in 2003

Glen Mulcaire  
Investigator hacked into Milly Dowler's phone for News of the World, allowing paper to receive messages

**the guardian**

newspaper of the year

# News of the World hacked Milly Dowler's phone during police hunt

Exclusive Paper deleted missing schoolgirl's voicemails, giving family false hope

Ick Davies and Amelia Hill

In News of the World illegally targeted the Bowes family, who had been targeted earlier in March 2011, interfering with police inquiries into her disappearance, and investigating the Guardian's coverage.

Scotland Yard is investigating the hacking, which is likely to put new pressure on the then editor of the paper, Rebekah Brooks, and her chief executive, Andy Coulson, who was deputy editor at the prime minister's office.

The Dowler family lawyers, Mark Lewis, issued a statement yesterday morning detailing the News of the World's actions. In an open letter to the paper, he said the Dowler Family was now pursuing damages against the News of the World.

Milly Dowler disappeared at the age of ten on her way home to St Ives-on-the-Thames, Surrey, on 23 March 2002. Detectives believe Scotland Yard's new investigation into the phone hacking, Operation Willow, are believed to have found evidence of the hacking of the Dowlers' mobile phones in London and Essex. Last week, Glenn Mulcaire, the private investigator, claimed he had been paid £10,000 to hack into Milly Dowler's phone for News of the World.

He has now given a letter to the Met officers. He has also issued formal police and legal statements from some of those referred to in the inquiry, whereupon they will be interviewed under caution. Mr Lewis said: "We are awaiting the results of the investigation and the outcome will remain unreported – and delayed – until formal charges of Milly Dowler."

The messages were deleted by journalists and hacked into the mobile phones of the directory's phone contacts for many families called Dowler in the Wiltshire area. The three addresses Whittamore found could be traced back to the Wiltshire town of Trowbridge. The three ex-directory numbers, however, were "tagged" illegally from British Telecom's confidential records by one of Whittamore's confidential sources. John Smith, who was still alive in Wiltshire. One of the ex-directory numbers was attributed to Whittamore to Milly's family home.

Then, with the help of a computer programme he had built himself, he recorded the messages that had been left in the first

going to Milly's phone messages, Scotland Yard and the investigating police force had to search through thousands of messages and discovered that her voicemail had been hacked. They concluded that no more housebreakers by Milly herself and that the messages were sent by someone else who was not. The investigation created false hope and extra agony for those whose loved ones had died.

The Dowler family then granted an exclusive interview to the News of the World in which they talked about their hope, quite accurately, that Milly would be found.

# 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”**



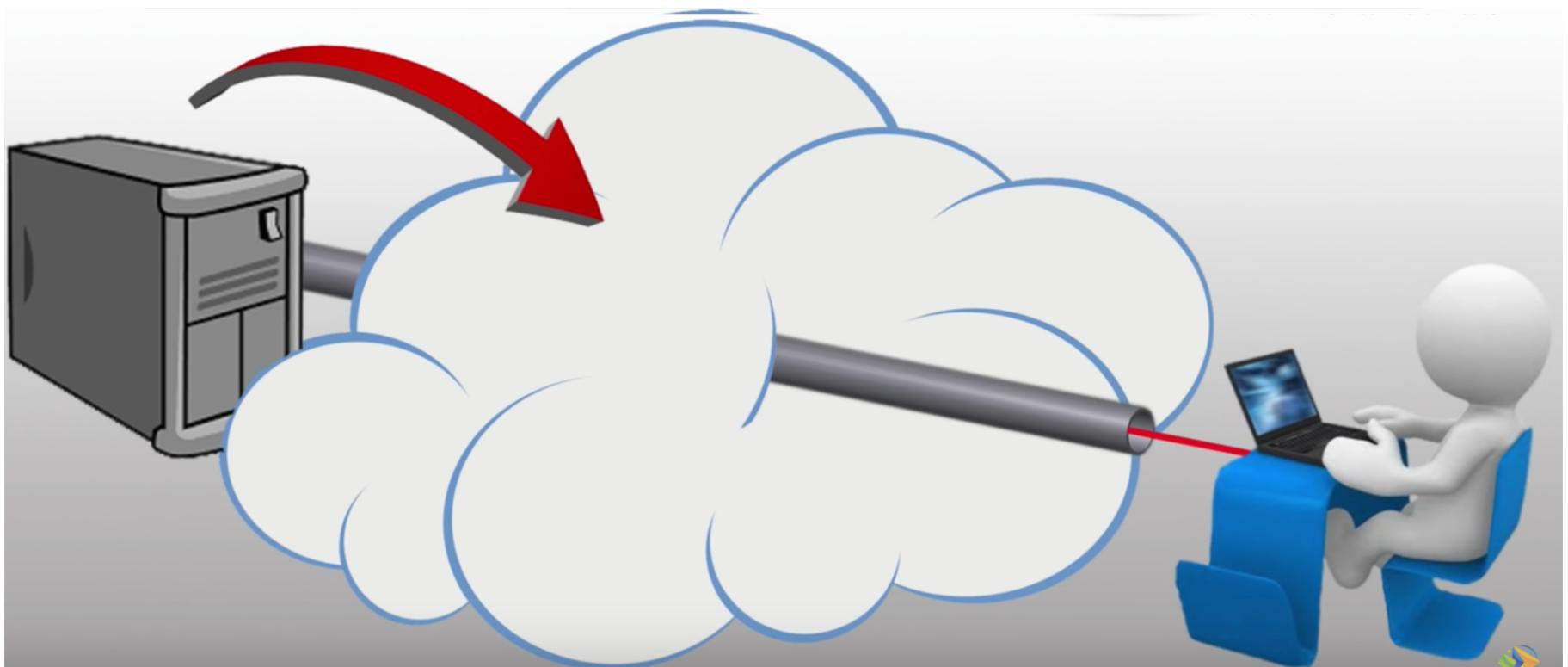
# What is a Virtual Private Networks

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

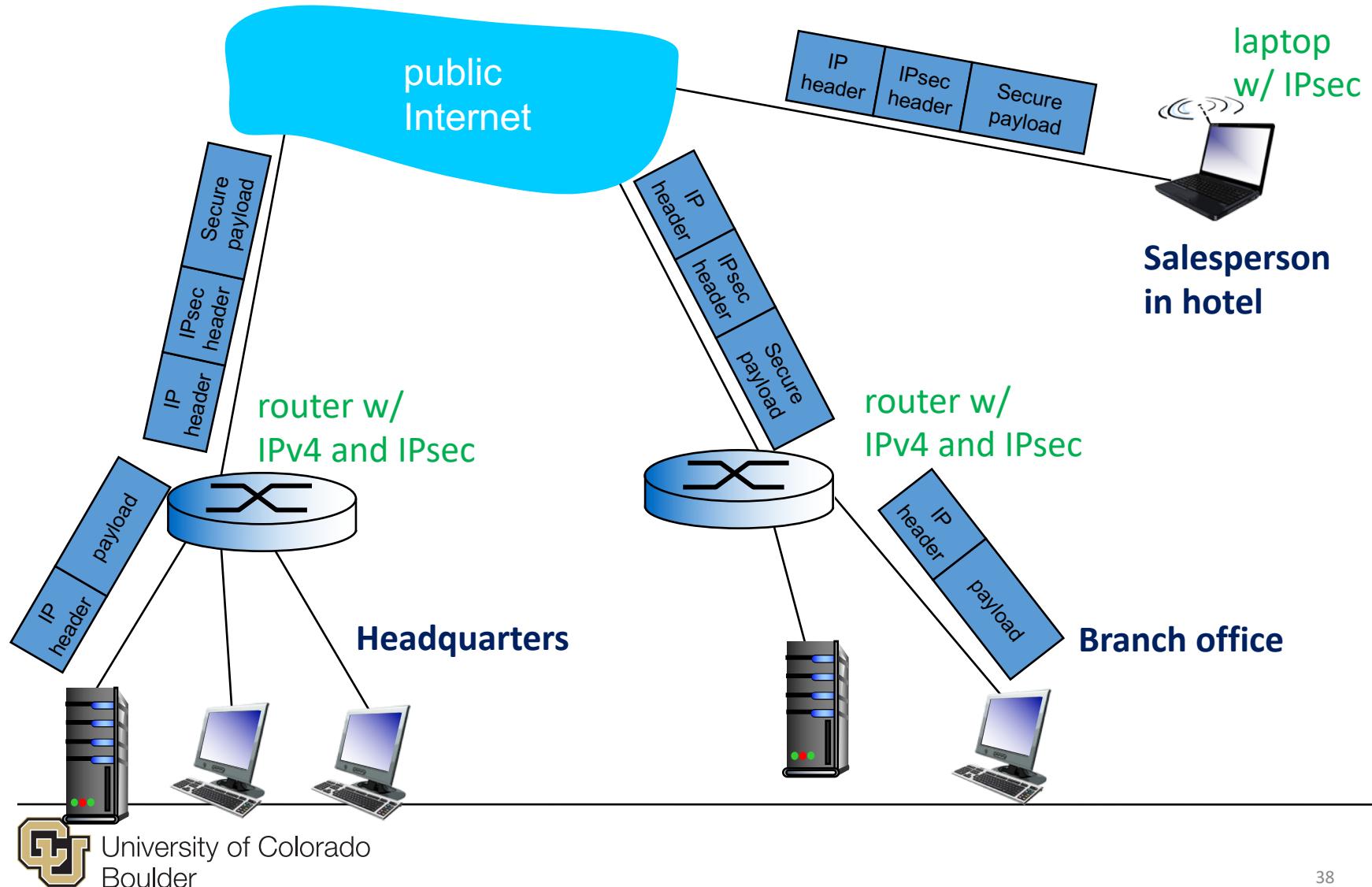
VPN is used to encrypt your data and to add a layer of privacy to protect your identity



# What is a VPN



# VPN Example



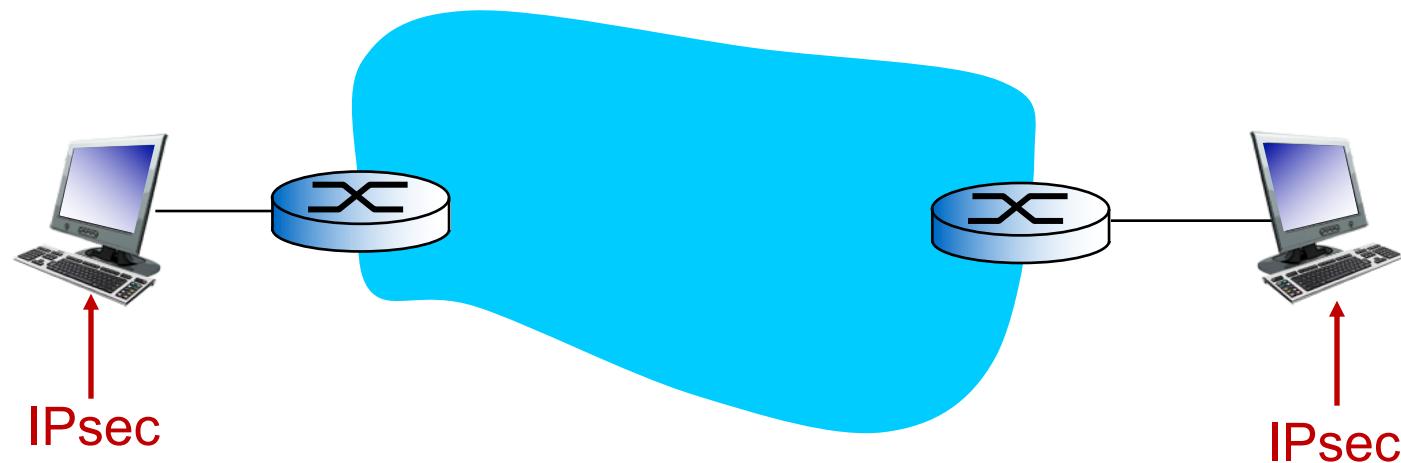
# IPSec Services

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

Two protocols providing different service models:

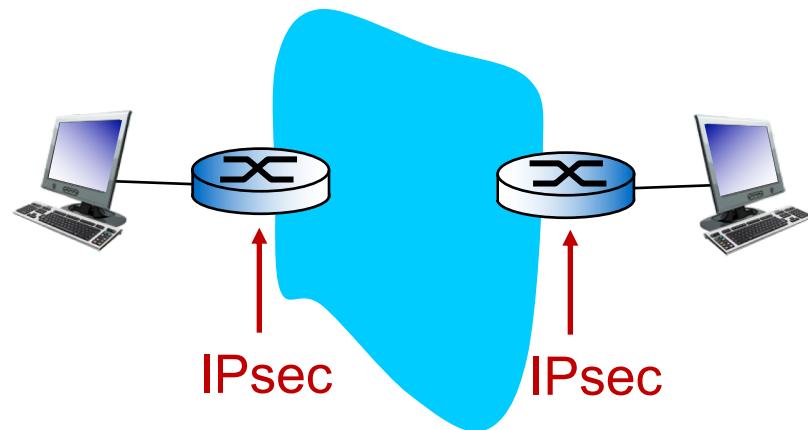
- AH
- ESP

# IPSec Transport Mode

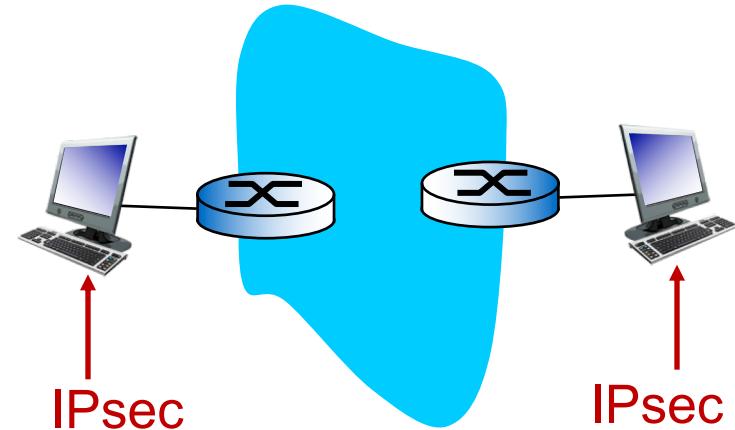


- IPsec datagram emitted and received by end-system
- protects upper level protocols

# 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!

1

A VPN is NOT an internet connection. It is a secure way to access the internet.

2

A VPN is really easy to use, even if you don't consider yourself "tech-savvy".

3

If you use any public Wifi, you should seriously consider a VPN.





University of Colorado  
Boulder