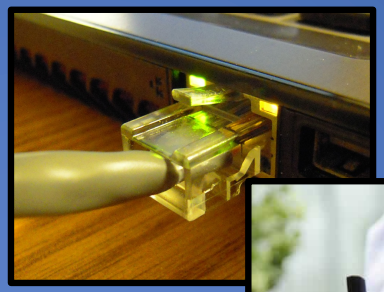
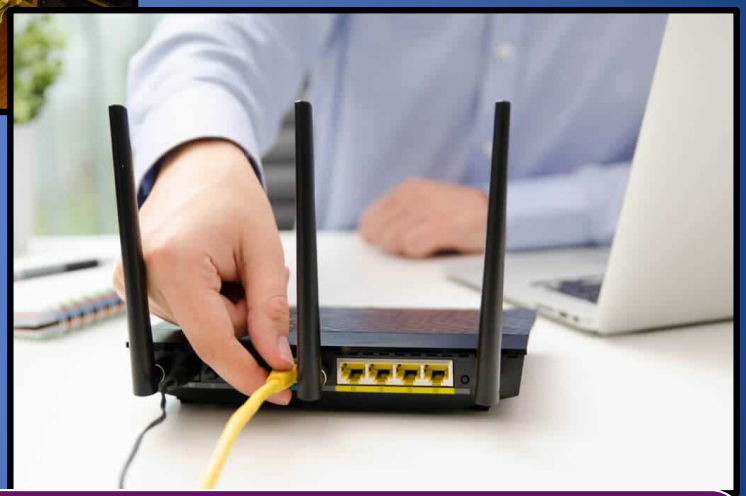
Networks II: Local network attacks

CS 1660: Introduction to Computer Systems Security

Where we are…





Local Area Network (LAN): "small" network: within a building, house, floor of office, etc.

=> Security concerns before we even start talking to the wider Internet!

Our high-level picture

7. Application

Provides applications to users (eg. HTTP, SSH, …)
Application-defined messages

4. Transport

Abstracts methods use to send data
Examples: TCP, UDP
Defines: port numbers;

3. Network

Provides way to get a packet to any other node on the Internet
Protocols: IP (IPv4, IPv6)
Defines: IP address (eg. 1.2.3.4)

2. Link

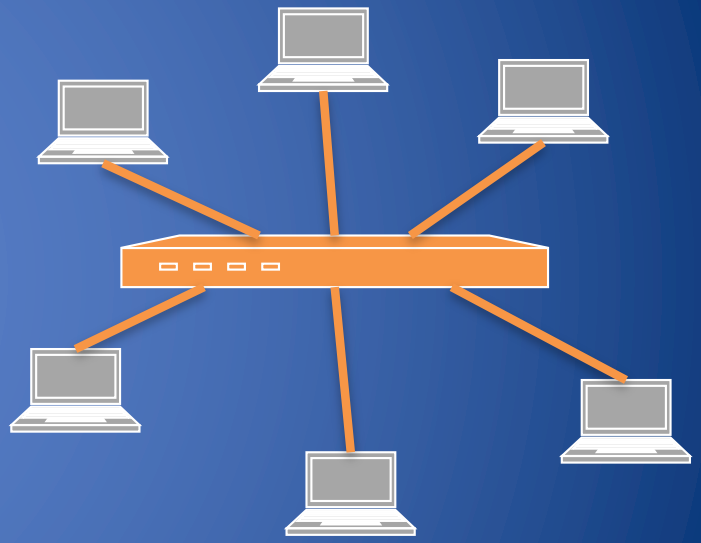
Protocols for sending data on individual links
Examples: Wifi, Ethernet, Bluetooth, ...
Defines: MAC address *(more on this later)*

1. Physical

Service: move bits to other node across link
(Electrical engineering problem)

Switching

- A switch connects devices on a local area network (LAN)
- Has multiple interfaces, or ports
- Operates on link-layer frames
- As devices connect, learns MAC addresses of some or all the devices on the network



Recap: MAC Addresses

- All interfaces have a MAC address
  - 48-bit number in hex (eg. 00-1A-92-D4-BF-86)
- Used to identify devices on a *local* network (eg. single house or building)

- First three bytes: assigned to manufacturers
  - E.g., 00-1A-A1 Cisco, 00-1B-11 D-Link , 00-0a-95 Apple
- Next three bytes: assigned per device, by manufacturer

  => Pre-programmed at factory, but can be changed by OS

MAC Address Authentication/Filtering

- Link-layer security which effectively allows network to grant and deny access to specific devices
- Administrator configures lists of allowed and blocked MAC addresses, which may change over time

- When is necessary a mac address authentication?
  - E.g. Systems without a user interface (a keyboard, a touch screen, etc.)
  - https://guestwifi.net.brown.edu/guest/mac_create.php

IP and MAC Addresses

- Devices on a local area network have
  - IP addresses (network layer)
  - MAC addresses (data link layer)
- IP addresses are used for high level protocols
- MAC addresses are used for low level protocol
- Network administrator configures IP address and subnet on each machine
- How to translate IP Addresses into MAC addresses?

ARP Protocol

Address Resolution Protocol (ARP)

- Connects the network layer to the data link layer
- Maps IP addresses to MAC addresses
- Based on broadcast messages and local caching
- Does not support confidentiality, integrity, or authentication
- Defined as a part of RFC 826

ARP Messages

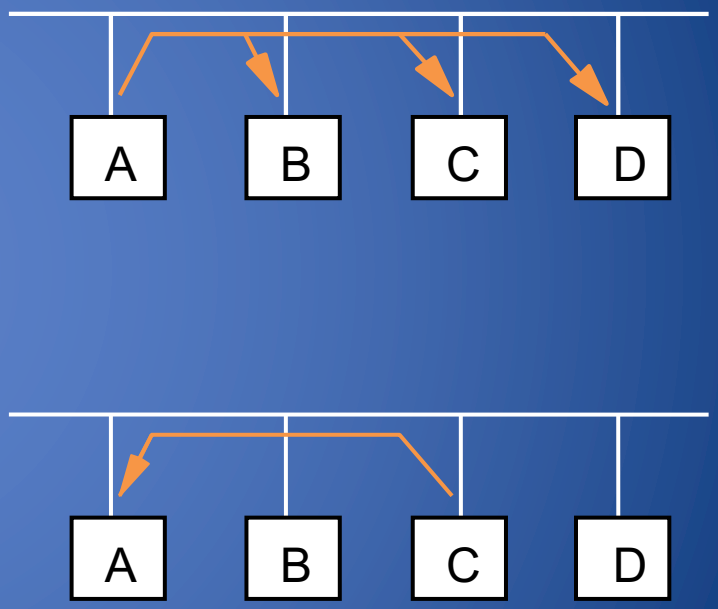
- ARP broadcasts in a frame a requests of type

  who has <IP addressC >
  tell <IP addressA >

- Machine with <IP addressC> responds to requesting machine message

  <IP addressC > is at <MAC address>

- Requesting machine caches response



ARP Cache

- The Linux, Windows and OSX command arp - a displays the ARP table

```
  Internet Address      Physical Address      Type
  128.148.31.1          00-00-0c-07-ac-00     dynamic
  128.148.31.15         00-0c-76-b2-d7-1d     dynamic
  128.148.31.71         00-0c-76-b2-d0-d2     dynamic
  128.148.31.75         00-0c-76-b2-d7-1d     dynamic
  128.148.31.102        00-22-0c-a3-e4-00     dynamic
```

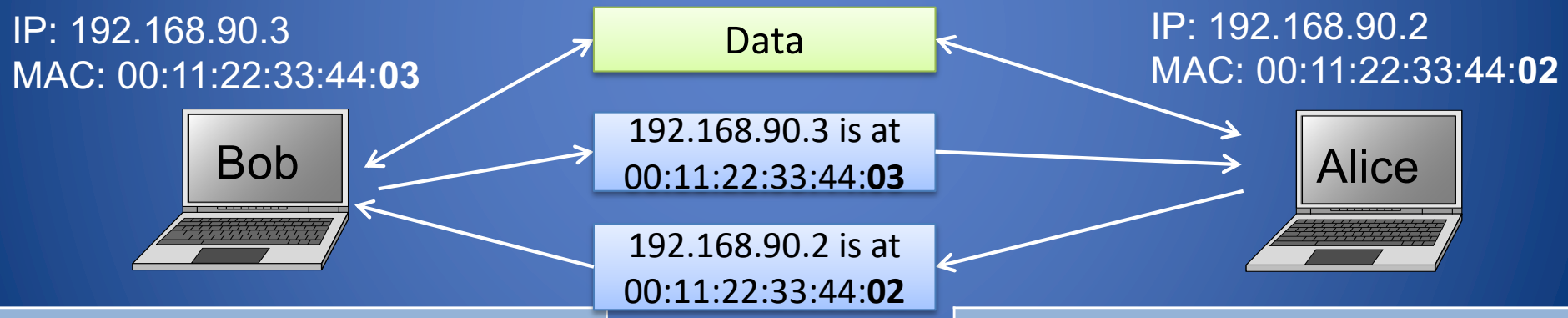
- Command arp –a –d flushes the ARP cache (with administrative privileges)
- ARP cache entries are stored for a configurable amount of time

ARP Security: Spoofing

- The ARP table is updated whenever an ARP response is received
- Requests are not tracked
- ARP announcements are not authenticated
- Machines trust each other
- A rogue machine can spoof other machines

ARP Normal Operation

- Normal operation
  - Alice communicates with Bob



ARP Cache	
192.168.90.2	00:11:22:33:44:**02**

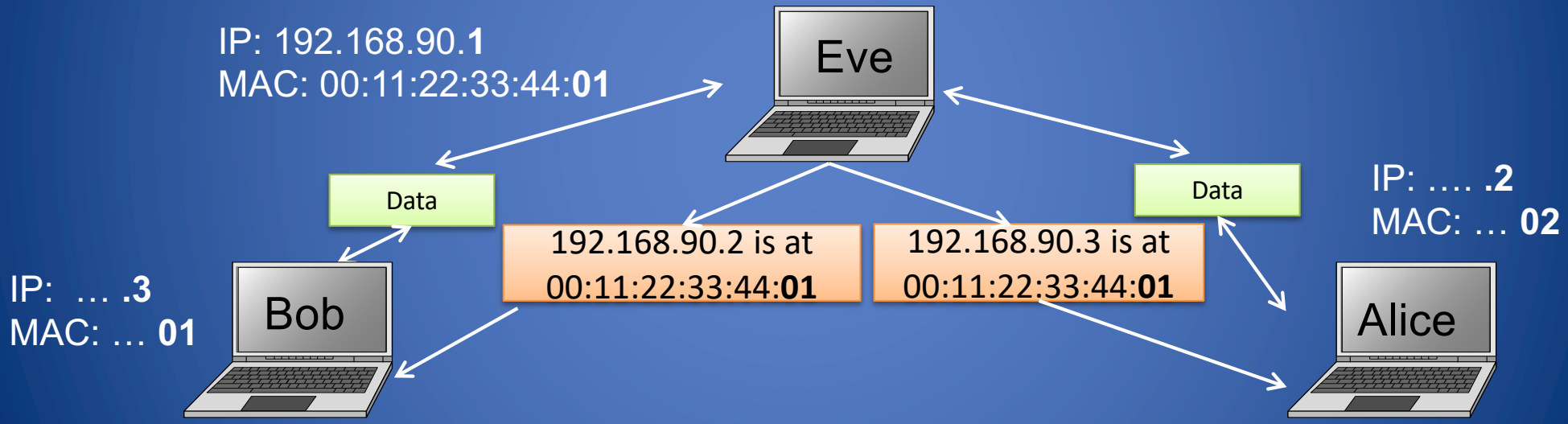
ARP Cache	
192.168.90.3	00:11:22:33:44:**03**

ARP Poisoning & ARP Spoofing

- Almost all ARP implementations are stateless
- An ARP cache updates every time that it receives an ARP reply
  - … even if it did not send any ARP request!
- Can "poison" ARP cache with gratuitous ARP replies
- Using static entries solves the problem but it is cumbersome to manage!

ARP Poisoning Attack

- Man-in-the-middle attack
  - ARP cache poisoning leads to eavesdropping

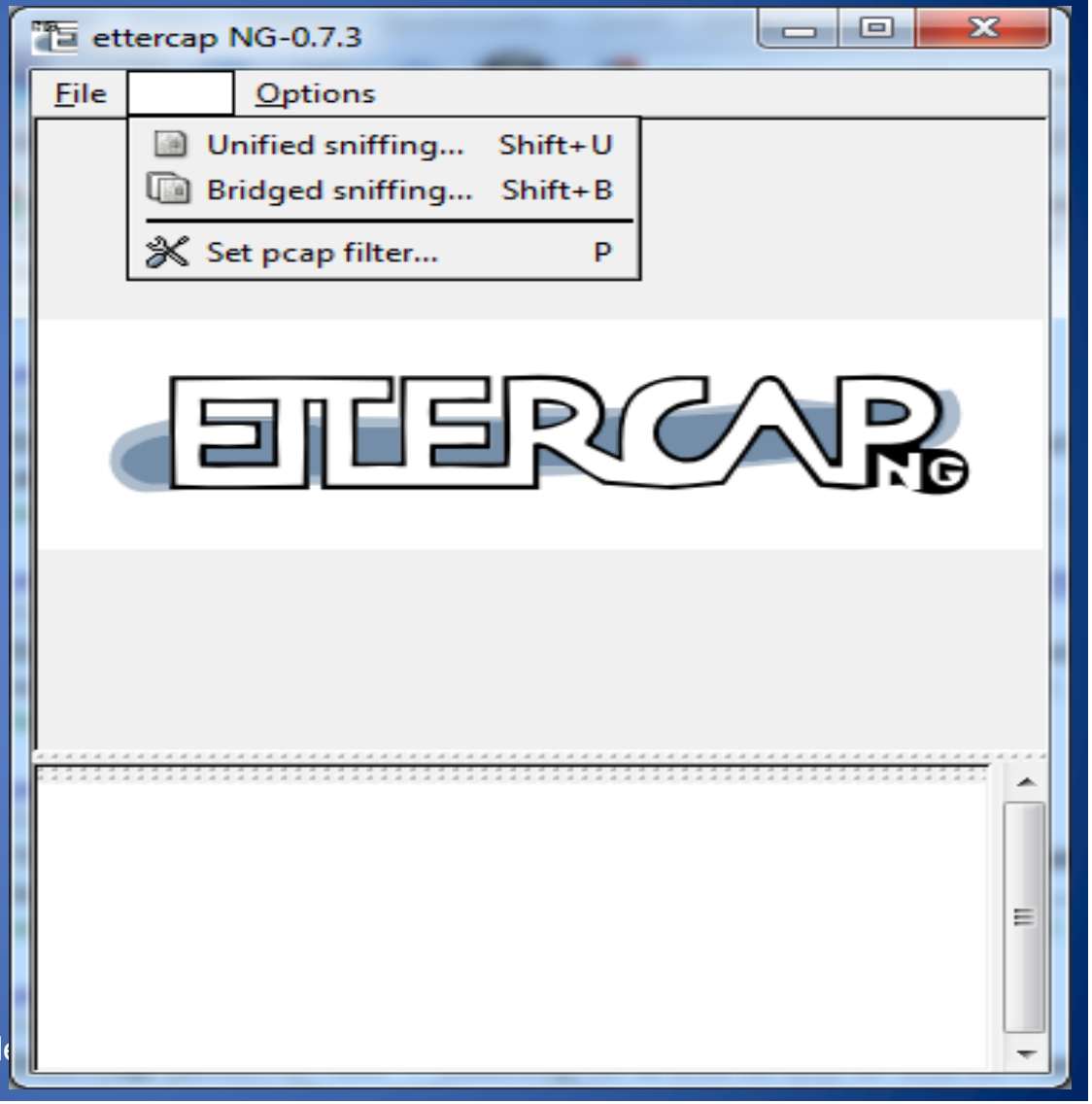


Poisoned ARP Cache	
192.168.90.2	00:11:22:33:44:**01**

Poisoned ARP Cache	
192.168.90.3	00:11:22:33:44:**01**

Ettercap

- Ettercap is a suite for man in the middle attacks on LAN
- In this demo we use:
  - Unified sniffing (promiscuous mode)
  - MiTM attack (arp poisoning)
  - Protocol dissection active and passive (telnet password retrieval)



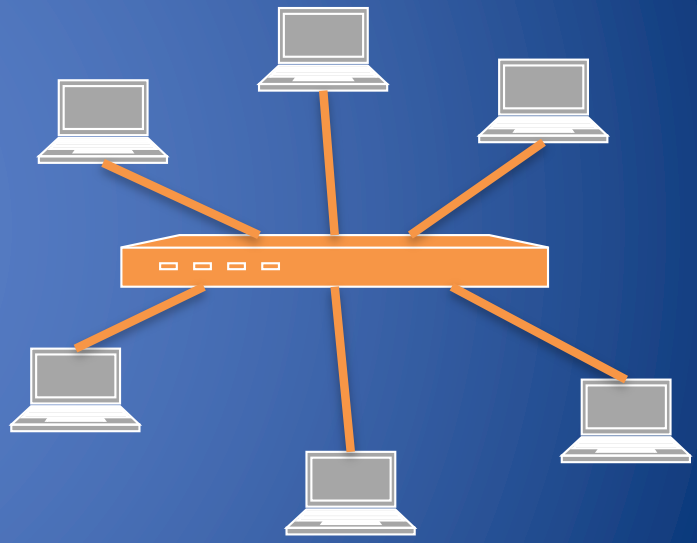
Another attack on switches…

Background: switch operation

- As switch sees packets, it *learns* which MAC address is on which port
  => MAC table: map of MAC address => Port

- When packet arrives: if destination MAC address is in table => send to that port
  - Otherwise, broadcast to all ports

Problems?

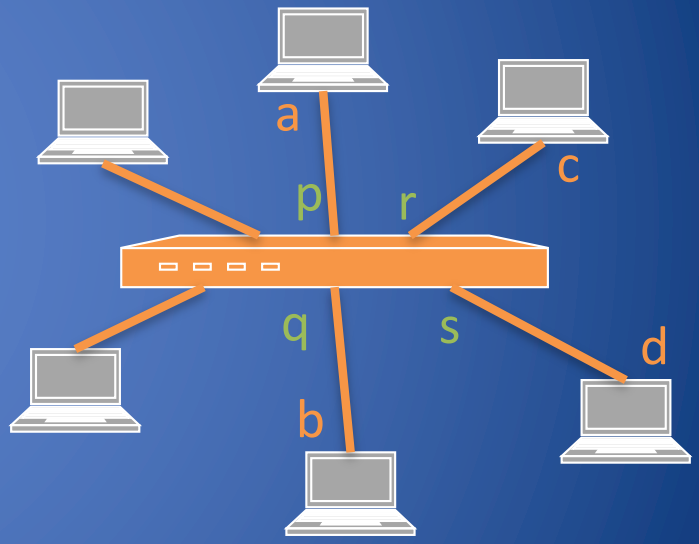


MAC learning: Example

- Table initially empty
- Frame (a, b) broadcast;
  - entry (a, p) added to table
- Frame (c, a) forwarded on p
  - entry (c, r) added to table
- Frame (a, c) forwarded on r
  - table unchanged
- Frame (a, d) broadcast
  - table unchanged

a	p

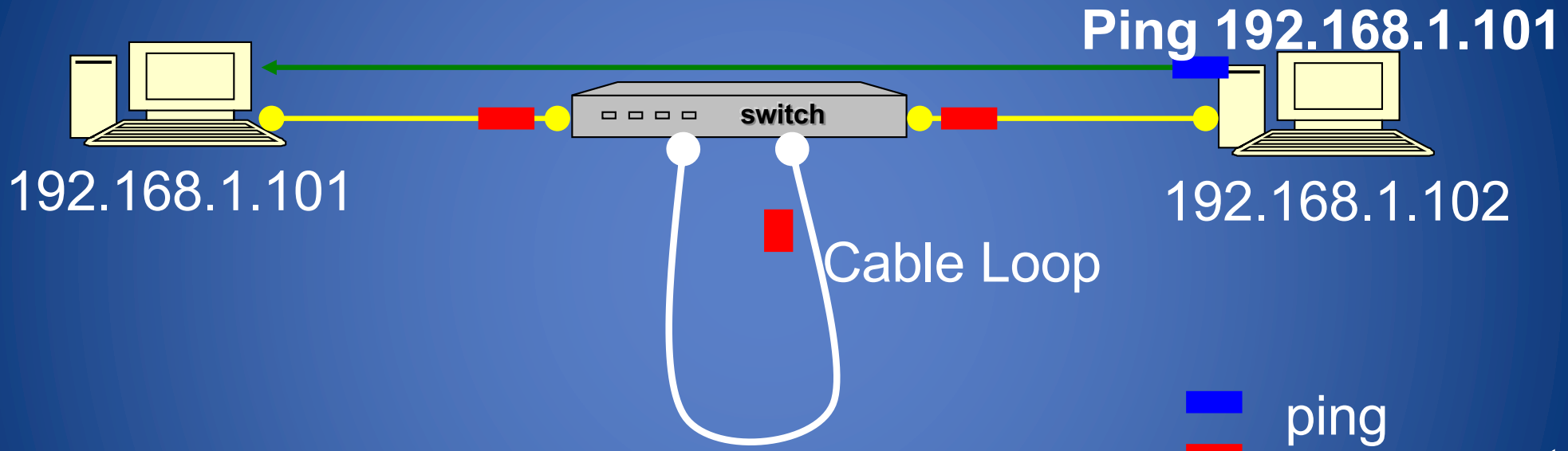
a	p
c	r



Attack on a learning switch

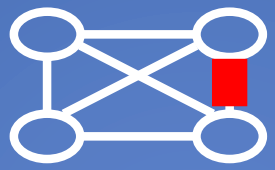
- Idea: flood the switch with many packets from different source MAC addresses
- If MAC table is full, switch just broadcasts all packets to all ports

network DOS using ARP



How can it be solved?

Spanning Tree Protocol (ISO 802.1D)

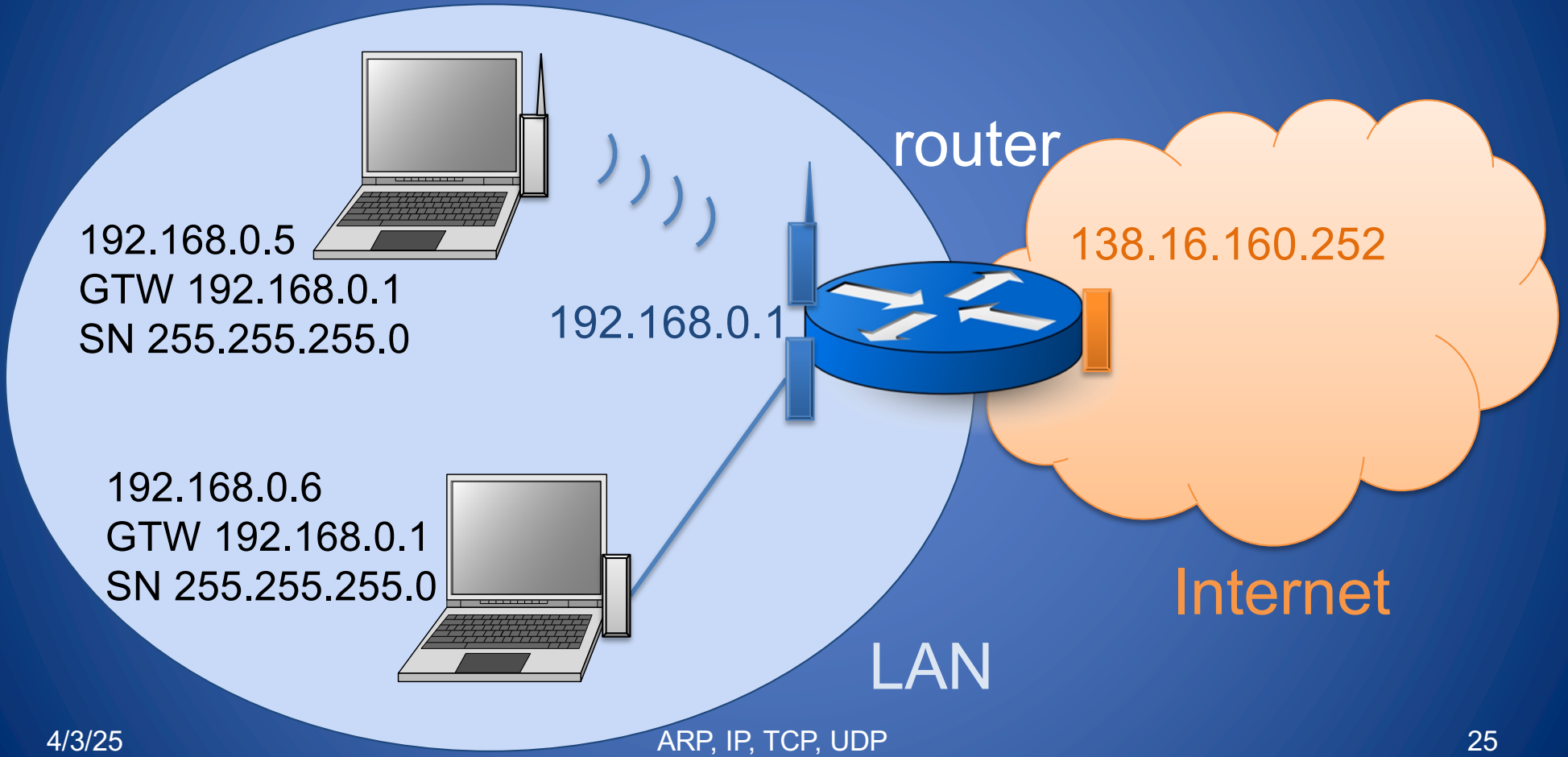


A Meshed Network

Four spanning trees of the Meshed Network

- Suppose you have a Meshed Network with bidirectional links that make loops/cycles…
- …then a spanning tree of the Meshed Network is the same network and no loops/cycles

From the LAN to the Internet



How do you get an IP address?

Obtaining Host IP Addresses - DHCP

- Networks are free to assign addresses within block to hosts
- Tedious and error-prone: e.g., laptop going from CIT to library to coffee shop
- Idea: client asks network for IP on connection

=> But how? How to send packets with no IP address?

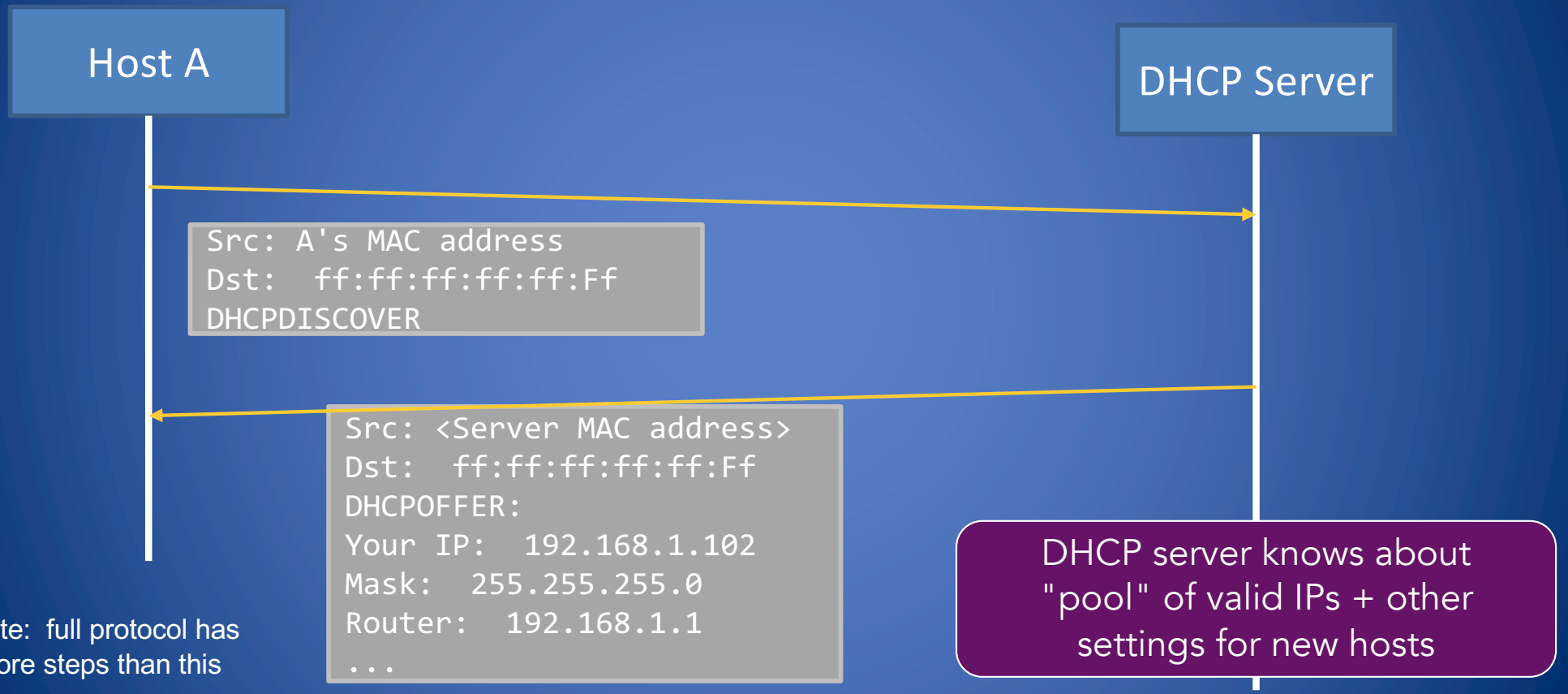
Broadcast traffic

Special MAC address: ff:ff:ff:ff:ff:ff

- Forwarded to all hosts on network!
- Used for link-layer protocols, particularly for finding IP addresses (DHCP, ARP)

Each IP subnet also has a broadcast address, usually last IP (eg. 192.168.1.255)

Start of DHCP



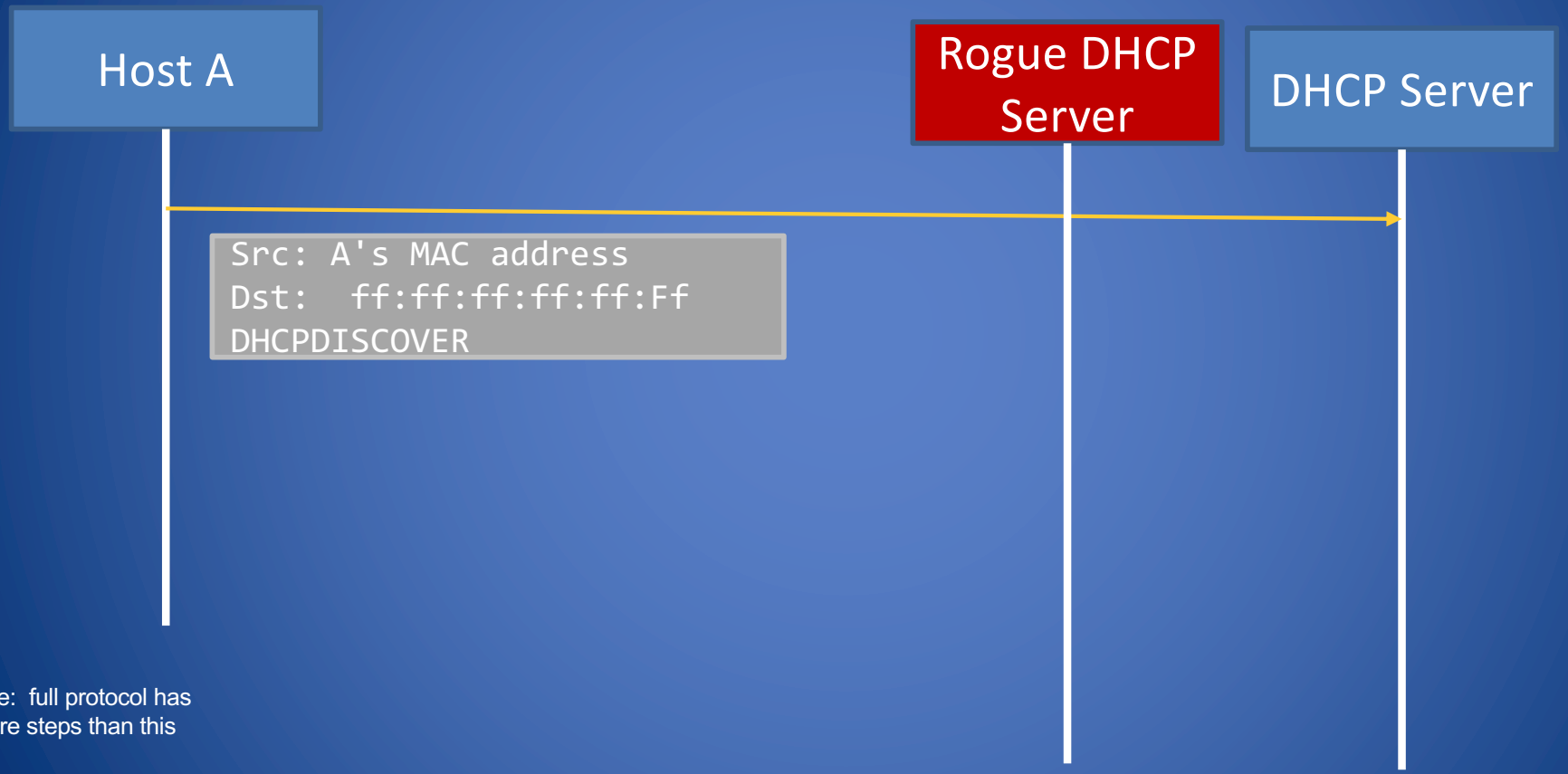
Note: full protocol has more steps than this

Problems with DHCP?

- What happens if a random host decides to be a DHCP server?

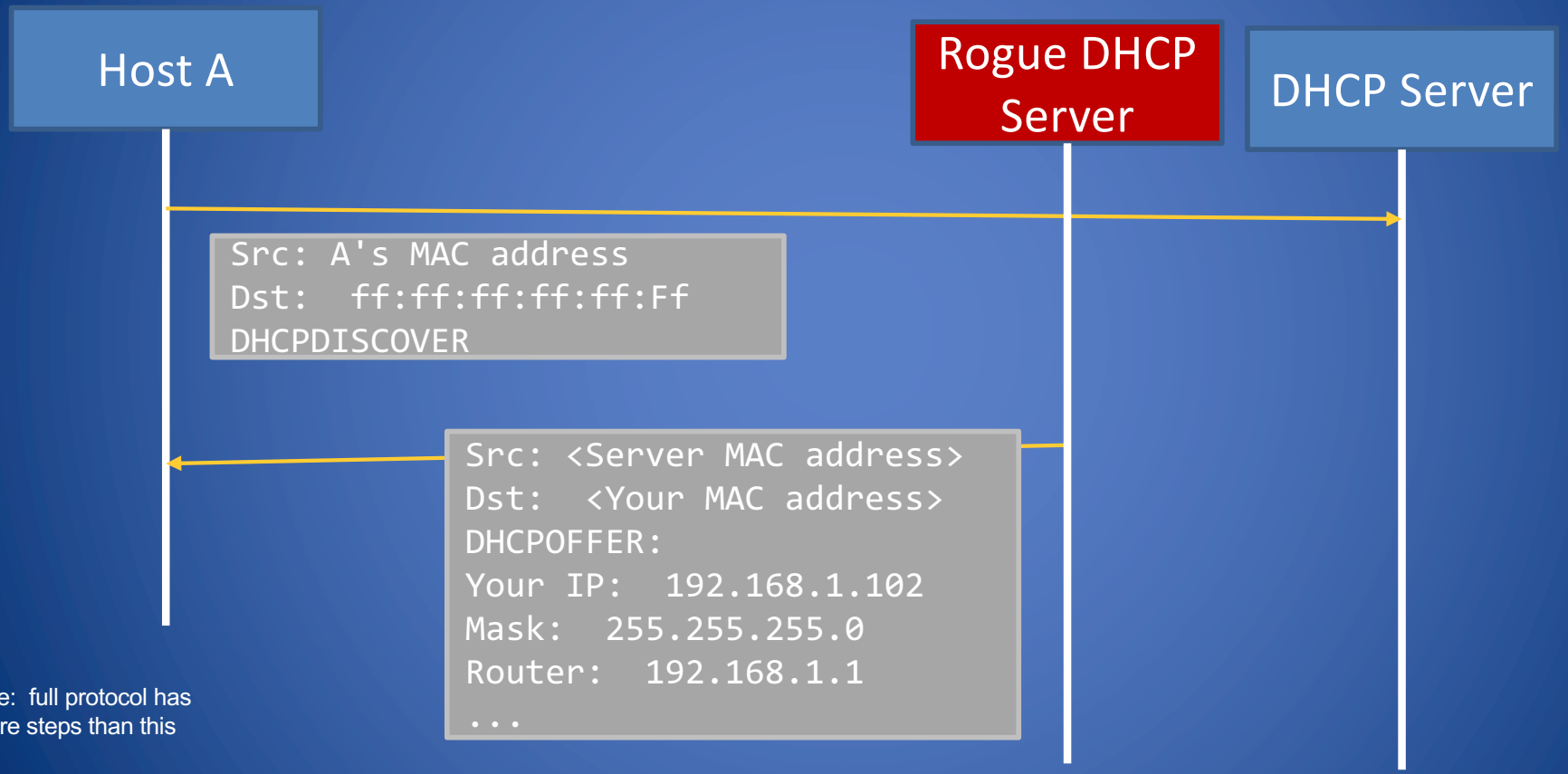
⇒Race condition! If an attacker can make an offer more quickly than the server, can assign a host's IP settings
  - Would be detected by the real DHCP server, though (why?)

DHCP Spoofing



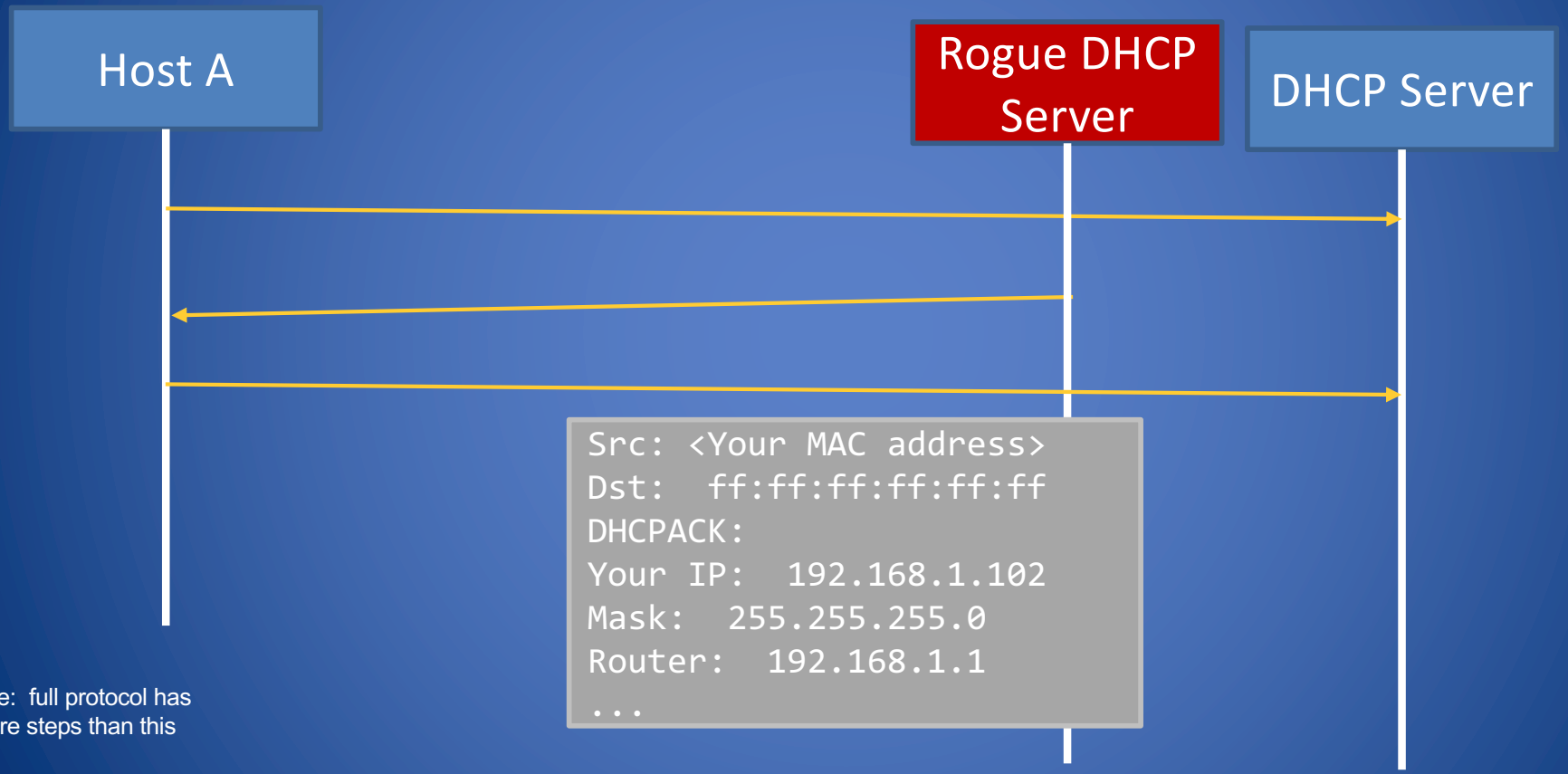
Note: full protocol has more steps than this

DHCP Spoofing



Note: full protocol has more steps than this

DHCP Spoofing



Note: full protocol has more steps than this

How to defend?

Initial DHCP messages are broadcast, so real server will see the rogue server's response

=> Can detect the attack!

Why use broadcast? Allows multiple, redundant DHCP servers without extra coordination

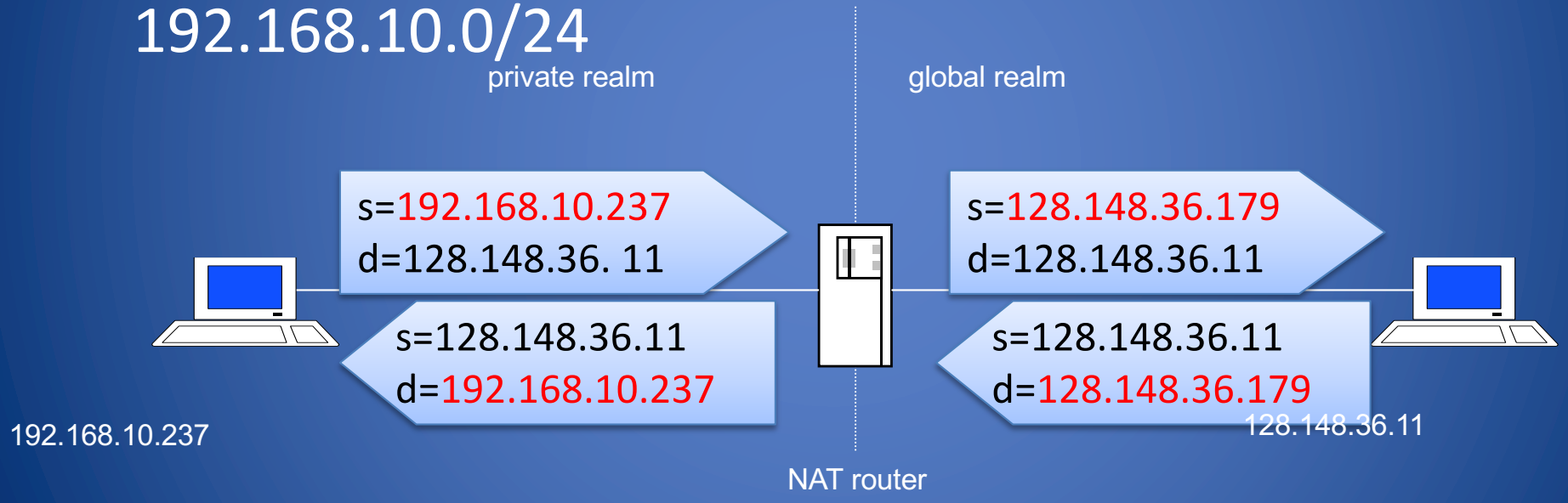
IP Address Space

Network Address Translation

- Introduced in the early 90s to alleviate IPv4 address space congestion
- Relies on translating addresses in an internal network, to an external address that is used for communication to and from the outside world
- NAT is usually implemented by placing a router in between the internal private network and the public network.
- Saves IP address space since not every terminal needs a globally unique IP address, only an organizationally unique one
- While NAT should really be transparent to all high level services, this is sadly not true because a lot of high level communication uses things on IP

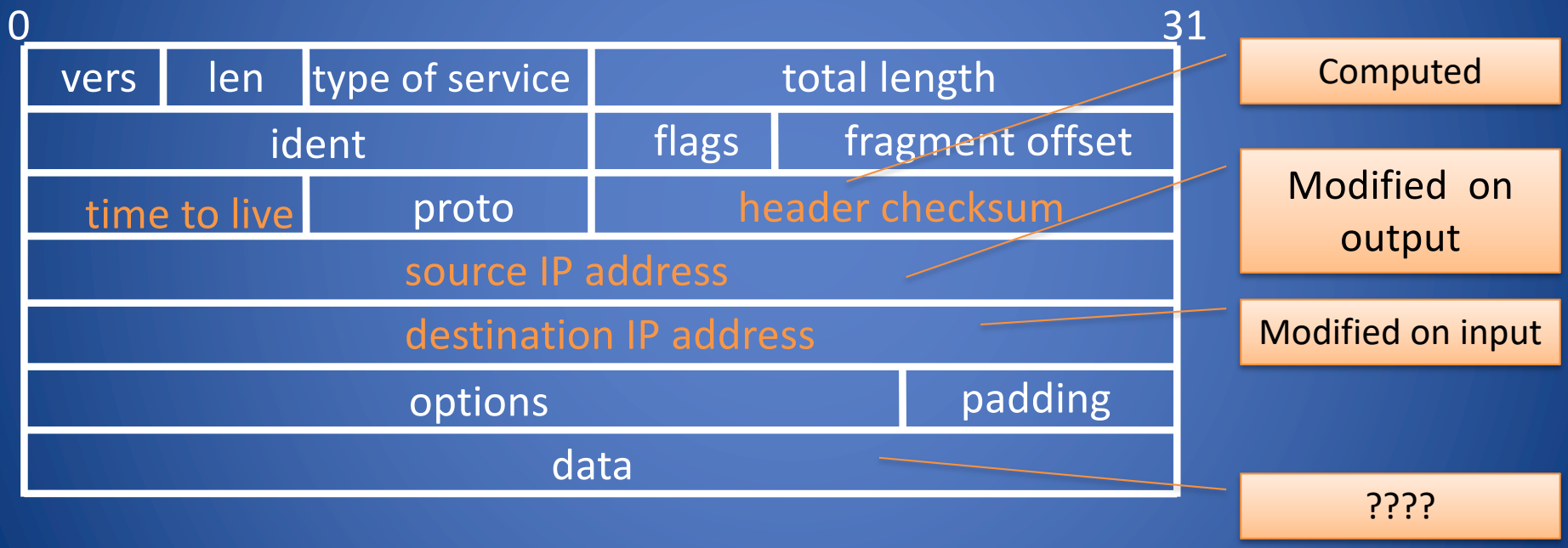
Translation

- Router has a pool of private addresses 192.168.10.0/24



To check external ip: e.g. https://whatismyipaddress.com/

IP Packet Modifications



Ping and Traceroute

A Simple Internet Protocol

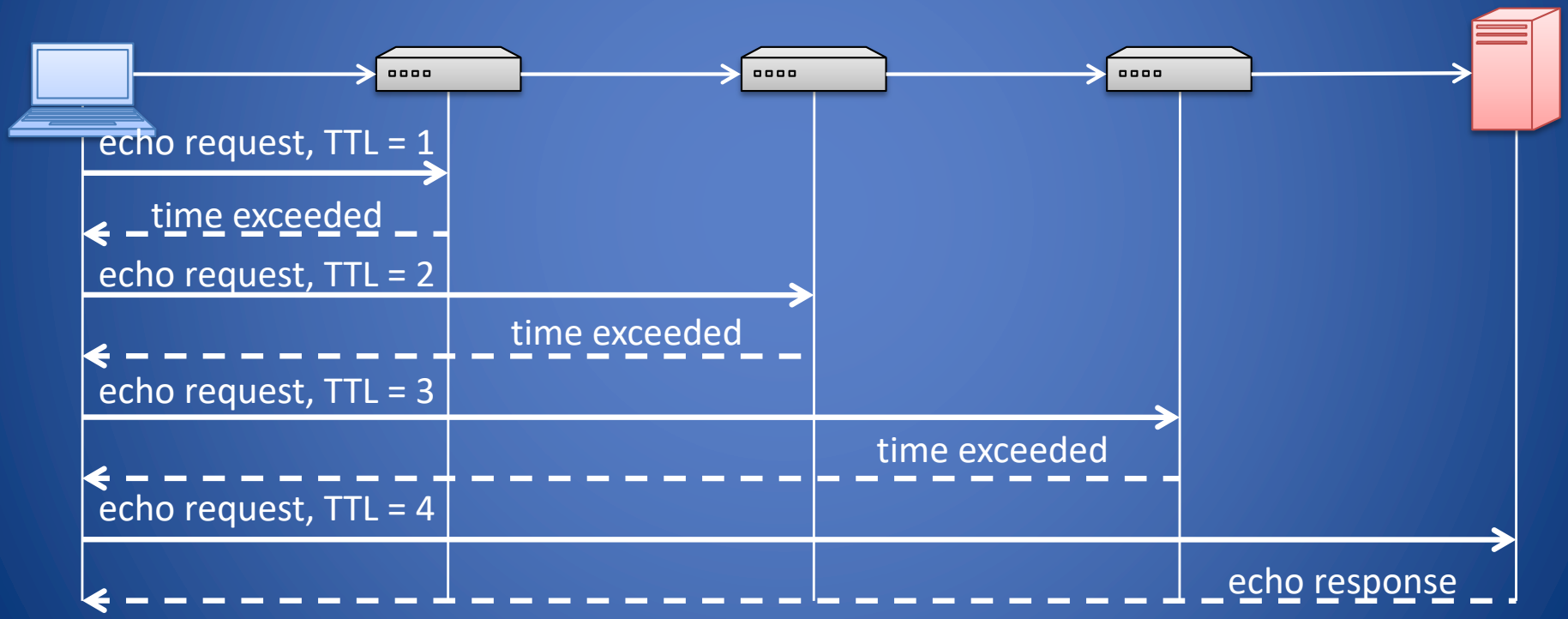
- Internet Control Message Protocol (ICMP)
  - Used for network testing and debugging
  - Network-layer protocol: simple messages about IP forwarding/routing
- Tools based on ICMP
  - Ping: send a message to an IP, get a response back
  - Traceroute: sends series ICMP packets with increasing TTL value to discover routes

TTL: Time to Live

- When TTL reaches 0, router may send back an error
  - "ICMP TTL exceeded" message
- If it does, we can identify a path used by a packet!

=> Traceroute takes advantage of this

Traceroute


echo request, TTL = 1
time exceeded
echo request, TTL = 2
time exceeded
echo request, TTL = 3
time exceeded
echo request, TTL = 4
echo response

Traceroute example

```
[deemer@Warsprite ~]$ traceroute -q 1 google.com
traceroute to google.com (142.251.40.174), 30 hops max, 60 byte packets
 1  router1-nac.linode.com (207.99.1.13)  0.621 ms
 2  if-0-1-0-0-0.gw1.cjj1.us.linode.com (173.255.239.26)  0.499 ms
 3  72.14.222.136 (72.14.222.136)  0.949 ms
 4  72.14.222.136 (72.14.222.136)  0.919 ms
 5  108.170.248.65 (108.170.248.65)  1.842 ms
 6  lga25s81-in-f14.1e100.net (142.251.40.174)  1.812 ms
```

Traceroute example

```
[deemer@Warsprite ~]$ traceroute -q 1 amazon.co.uk
traceroute to amazon.co.uk (178.236.7.220), 30 hops max, 60 byte packets
 1  router2-nac.linode.com (207.99.1.14)  0.577 ms
 2  if-11-1-0-1-0.gw2.cjj1.us.linode.com (173.255.239.16)  0.461 ms
 3  ix-et-2-0-2-0.tcore3.njy-newark.as6453.net (66.198.70.104)  1.025 ms
 4  be3294.ccr41.jfk02.atlas.cogentco.com (154.54.47.217)  2.938 ms
 5  be2317.ccr41.lon13.atlas.cogentco.com (154.54.30.186)  69.725 ms
 6  be2350.rcr21.b023101-0.lon13.atlas.cogentco.com (130.117.51.138)  69.947 ms
 7  a100-row.demarc.cogentco.com (149.11.173.122)  71.639 ms
 8  150.222.15.28 (150.222.15.28)  78.217 ms
 9  150.222.15.21 (150.222.15.21)  84.383 ms
10  *
11  150.222.15.4 (150.222.15.4)  74.529 ms
                                      . . .
30  178.236.14.162 (178.236.14.162)  83.659 ms
```

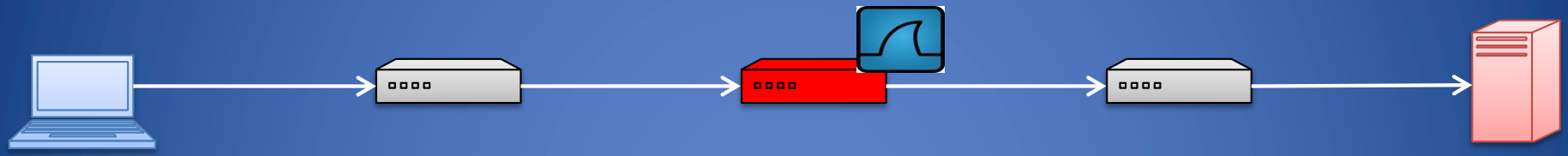
Practicing Ping and Traceroute

- Linux/Unix/Macos
  - ifconfig
  - ping www.brown.edu
  - traceroute www.brown.edu
- Windows
  - ipconfig
  - tracert www.brown.edu

Practice with Wireshark

- Checking a connection
  - Ping 127.0.0.1 (localhost)
  - Ping <your-ip-address> (ifconfig)
  - Ping www.brown.edu
- Traceroute www.brown.edu
- Let's see in Wireshark
- Let's see in geotraceroute.com

Sniffing: not just for hosts?



- Any network device that sees packets could be an eavesdropper
- This is why we encrypt traffic in transit!

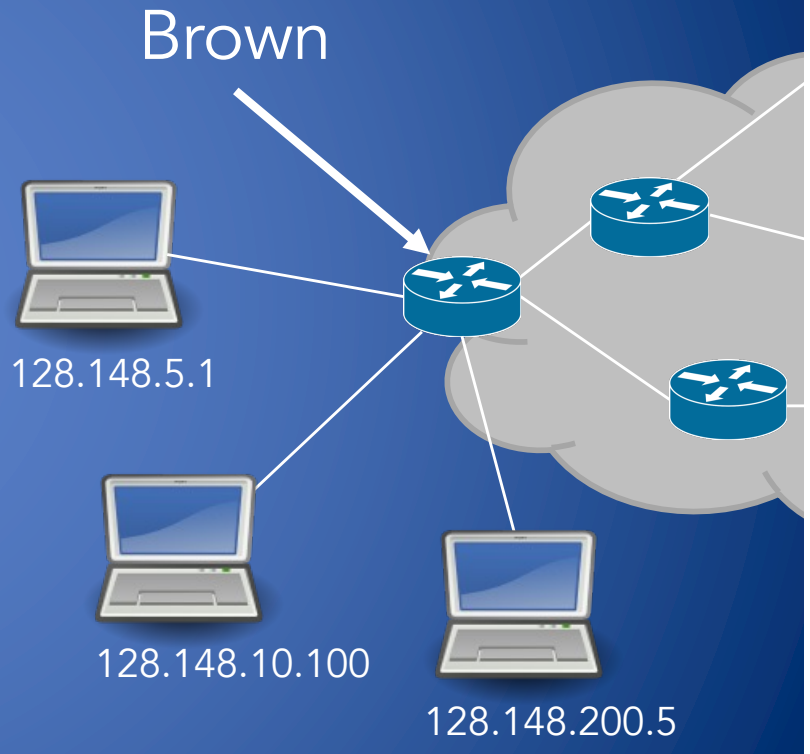
How do we move packets *between* networks?

IP Addressing

A network can designate IP addresses for its own hosts within its address range

How? Every address has two parts:

- Network part: identifies the network (eg. "Brown") to the Internet
- Host part: identifies individual hosts within Brown

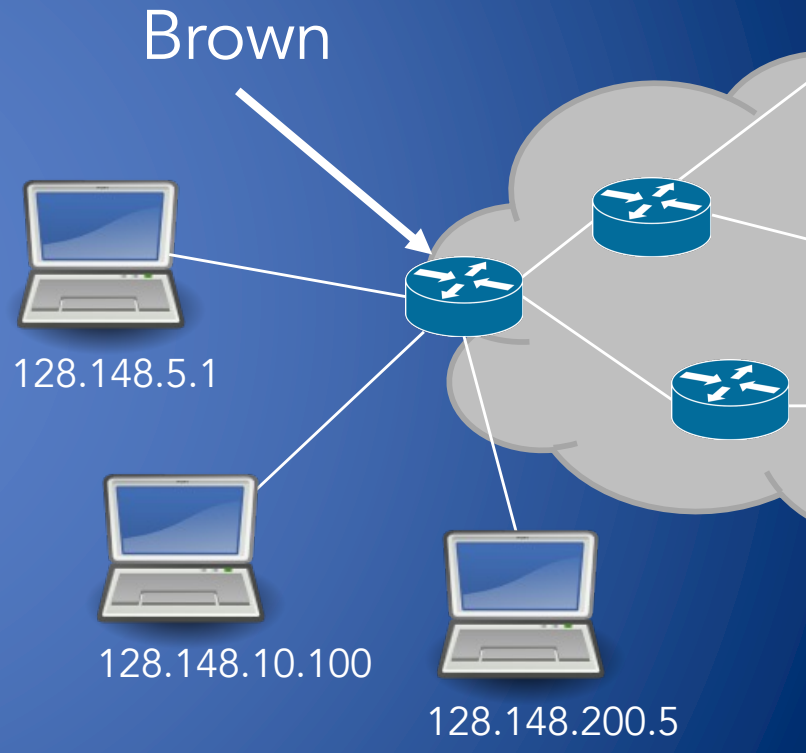


IP Addressing

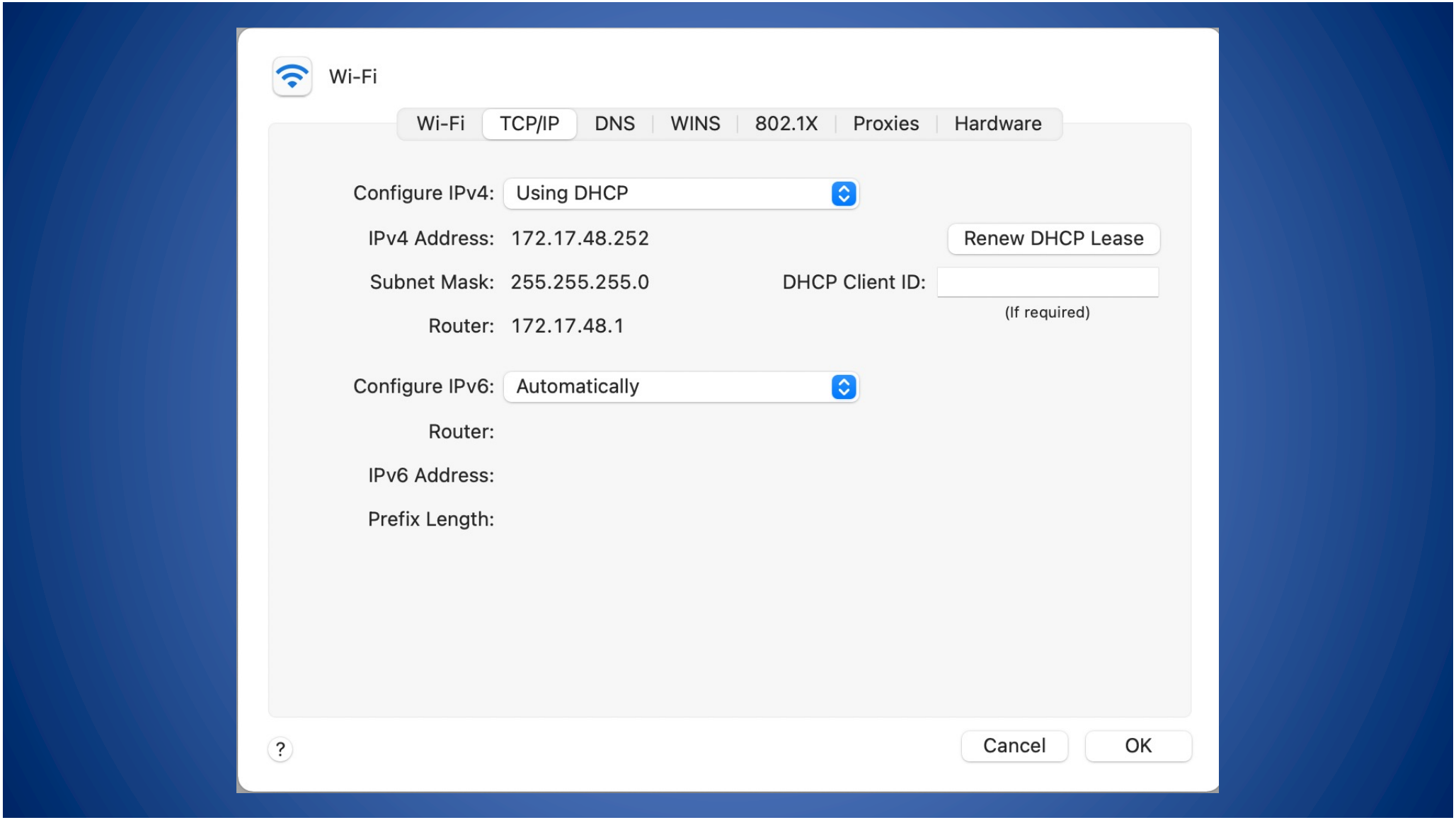
A network can designate IP addresses for its own hosts within its address range

How? Every address has two parts:

- Network part: identifies the network (eg. "Brown") to the Internet
- Host part: identifies individual hosts within Brown



Why? Routers need to check which *network* an address belongs to


Wi-Fi
Wi-Fi
TCP/IP
DNS
WINS
802.1X
Proxies
Hardware
Configure IPv4:
Using DHCP
IPv4 Address:
172.17.48.252
Renew DHCP Lease
Subnet Mask:
255.255.255.0
DHCP Client ID:
(If required)
Router:
172.17.48.1
Configure IPv6:
Automatically
Router:
IPv6 Address:
Prefix Length:
?
Cancel
OK

Components of an IP

IPv4 Address:	172.17.48.252
Subnet Mask:	255.255.255.0
Router:	172.17.48.1

172.17.48.252

```
Addr: 172.17.48.252   10101100 00010001 00110000 11111100

Mask: 255.255.255.0   11111111 11111111 11111111 00000000
```

Key point: networks can be of different sizes!
=>The "subnet mask" defines what part of is the network part

Common Prefix Sizes

Prefix	IPs	Number of hosts	Note
1.2.3.0/24	1.2.3.*	2^8 = 256	Common for local networks (LANs) Old term: "Class C"
1.2.0.0/16	1.2.*.*	2^16 = 65536	Old term: "Class B" Large (or older) organizations
1.0.0.0/8	1.*.*.*	2^24 = ~16M	Old term: "Class A"
1.2.3.100/30	1.2.3.1-1.2.3.3	4	A smaller prefix

Special/private IP ranges

Prefix	Note
127.0.0.0/8	Localhost (for networks on same system), usually 127.0.0.1
192.168.0.0/16	Private: often used for home networks
10.0.0.0/8	Private: often used for larger organizations (eg. Brown)
172.16.0.0/12	Private: larger space for organizations, systems (eg. Docker)

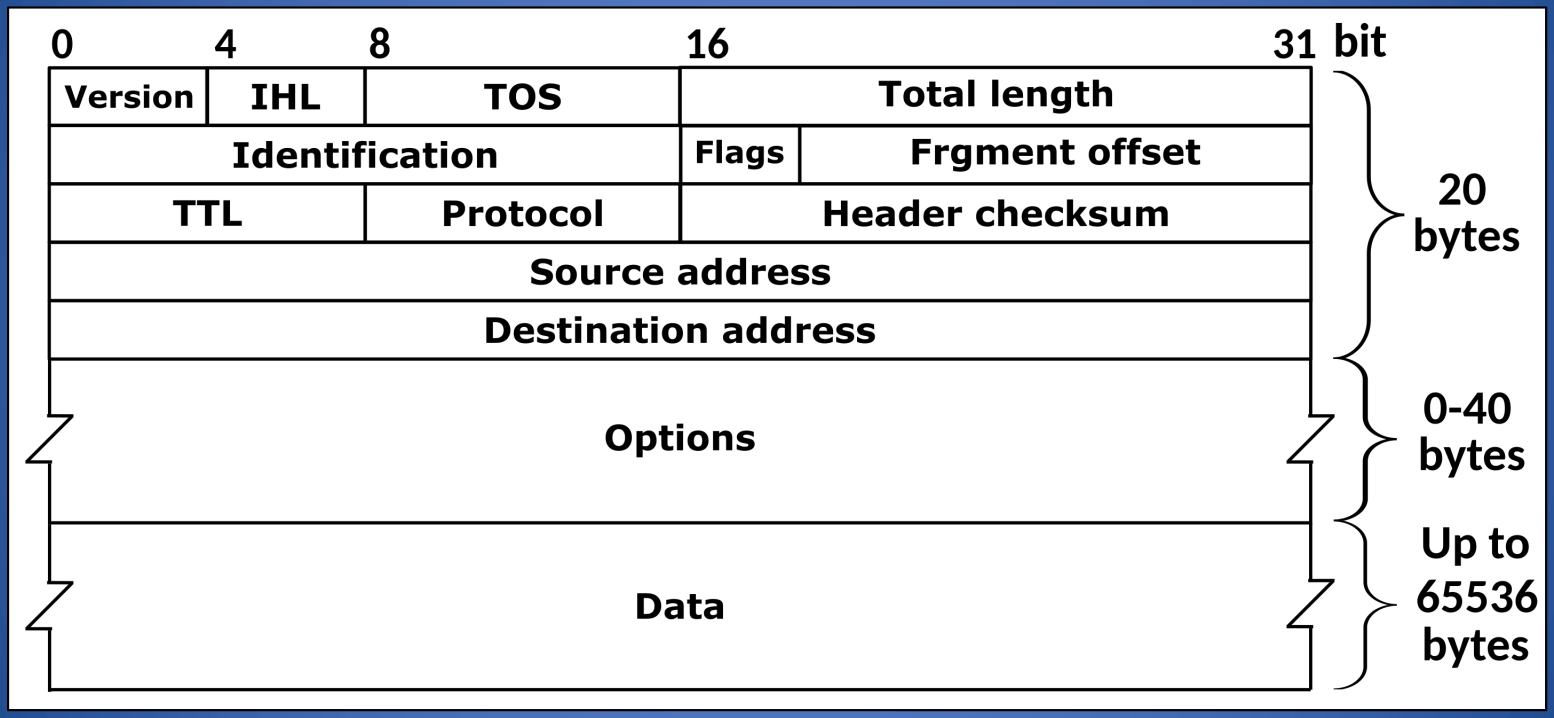
- Used for LANs, private networks *not* publicly routable on the global internet RFC 1918
- More on this later

IP Address Space and ICANN

- Hosts on the internet must have unique IP addresses
- Internet Corporation for Assigned Names and Numbers
  - International nonprofit organization
  - Incorporated in the US
  - Allocates IP address space
  - Manages top-level domains
- Historical bias in favor of US corporations and nonprofit organizations

```
003/8   May 94   General Electric
009/8   Aug 92   IBM
012/8   Jun 95   AT&T Bell Labs
013/8   Sep 91  Xerox Corporation
015/8   Jul 94   Hewlett-Packard
017/8   Jul 92   Apple Computer
018/8   Jan 94   MIT
019/8   May 95   Ford Motor
040/8   Jun 94   Eli Lily
043/8   Jan 91   Japan Inet
044/8   Jul 92   Amateur Radio Digital
047/8   Jan 91   Bell-Northern Res.
048/8   May 95   Prudential Securities
054/8   Mar 92   Merck
055/8   Apr 95   Boeing
056/8   Jun 94   U.S. Postal Service
```

The IPv4 Header

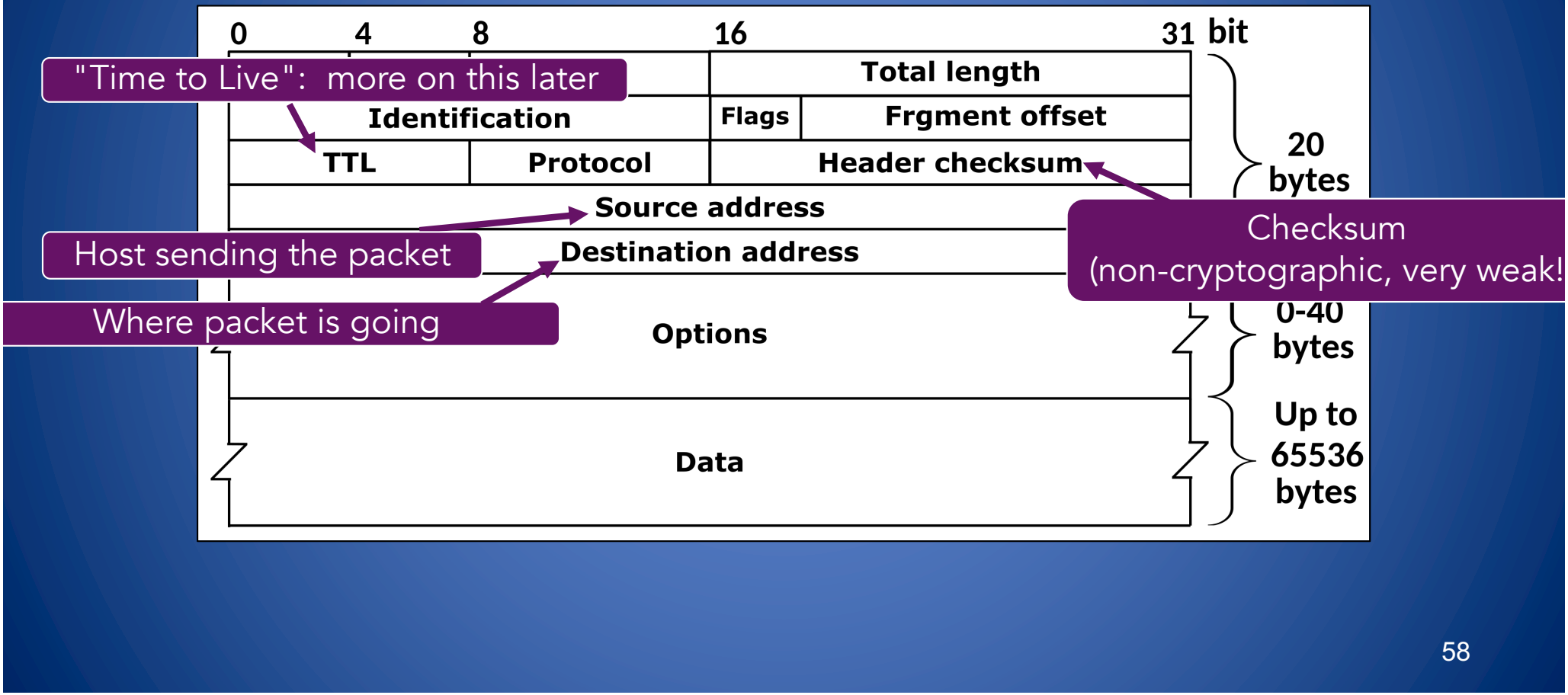


Defined by RFC 791
RFC (Request for Comment): defines network standard

IP Routing

- A router connects two or more networks
  - Maintains tables to forward packets to the appropriate network
  - Forwarding decisions based solely on the destination address
  - Hosts (regular systems) can be routers too!
- Routing table
  - Maps ranges of addresses to LANs or other gateway routers

The IPv4 Header

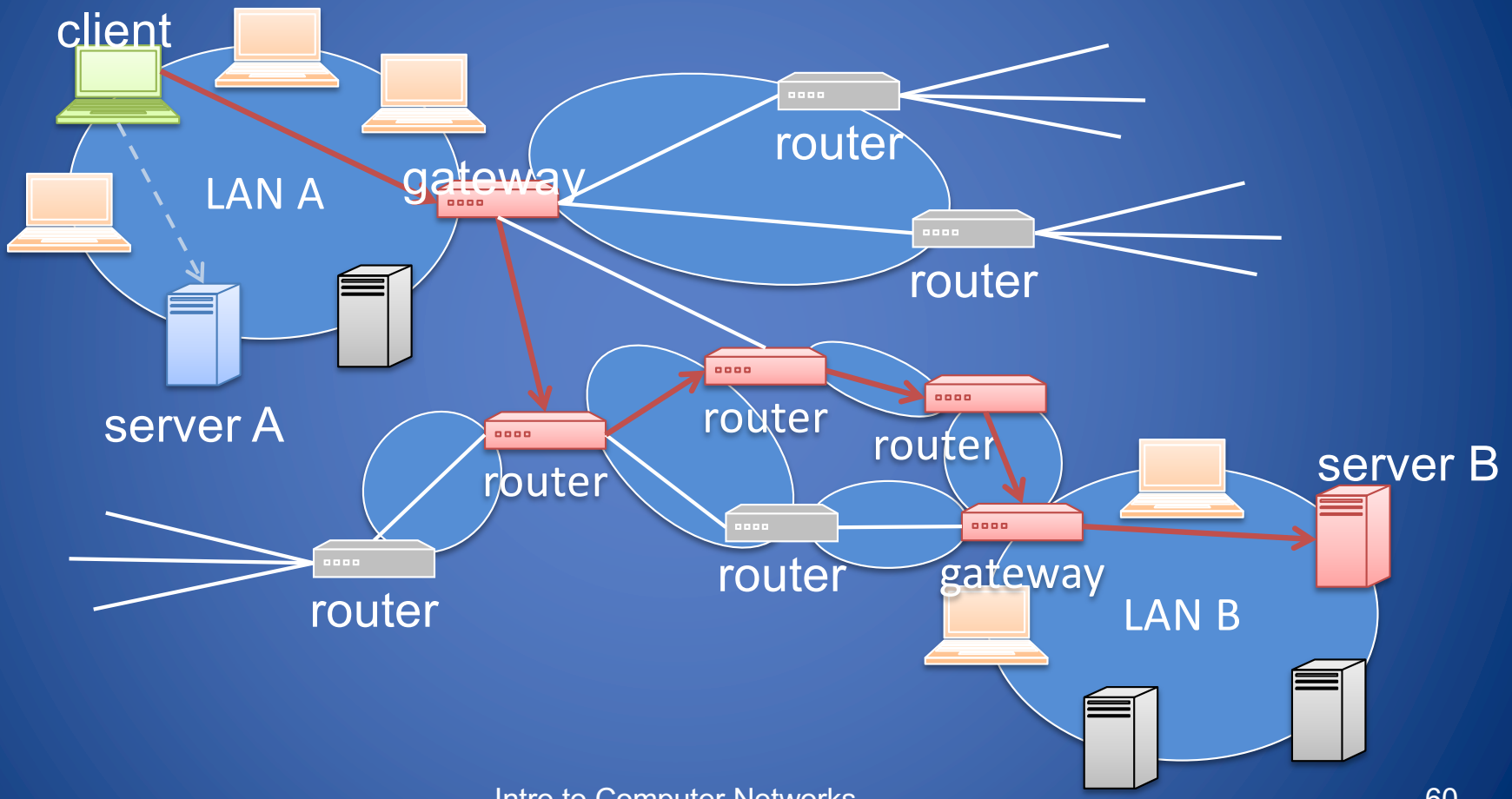


Example routing table

```
deemer@ceres ~ % ip route
127.0.0.0/8 via 127.0.0.1 dev lo
172.17.48.0/24 dev enp7s0  proto kernel
default via 172.17.48.1 dev eth0 src 172.17.44.22
```

- "Default": where to send packets when they go to a network you don't know about
- Also known as "next hop"

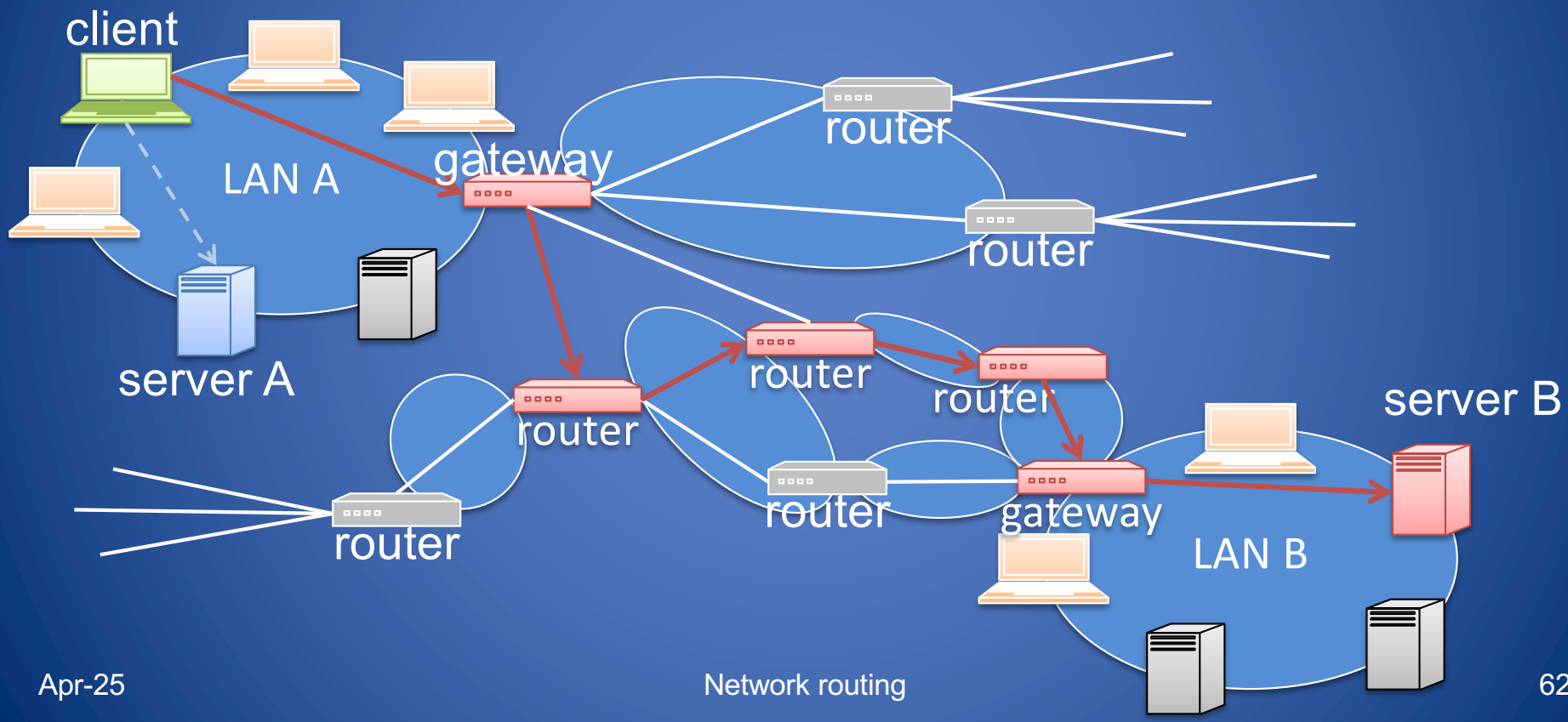
Routing Examples



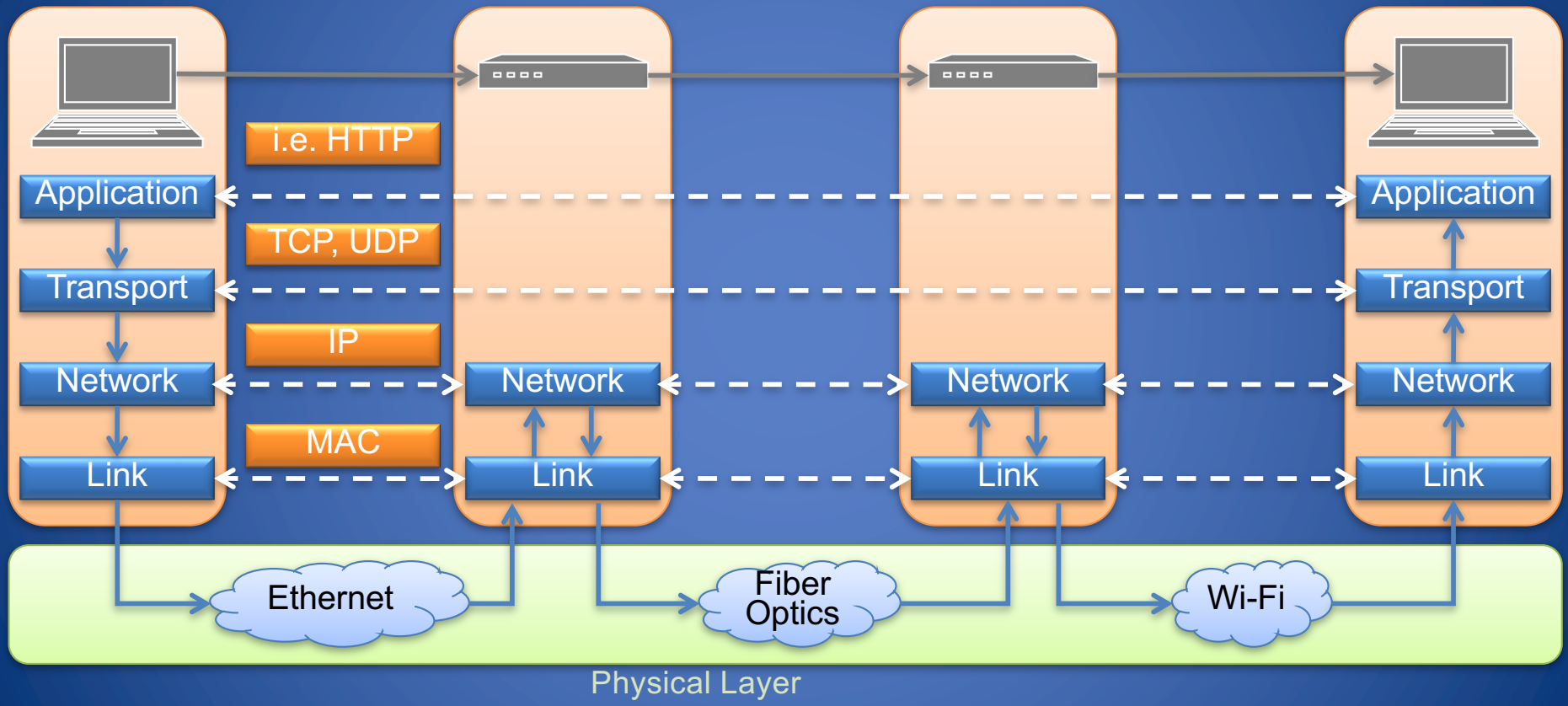
Routing
How does internet actually work?

Why Routing?

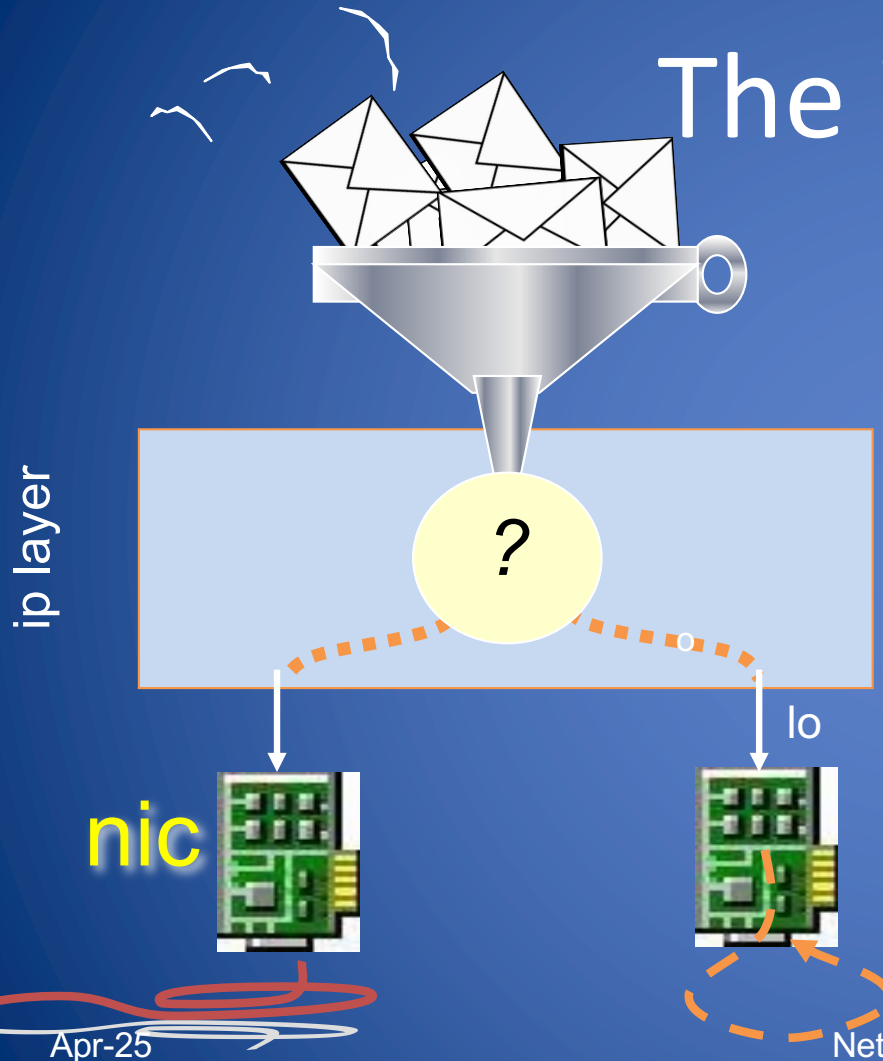
- Reaching a host within a network is a routing problem



Internet Layers



The ip layer

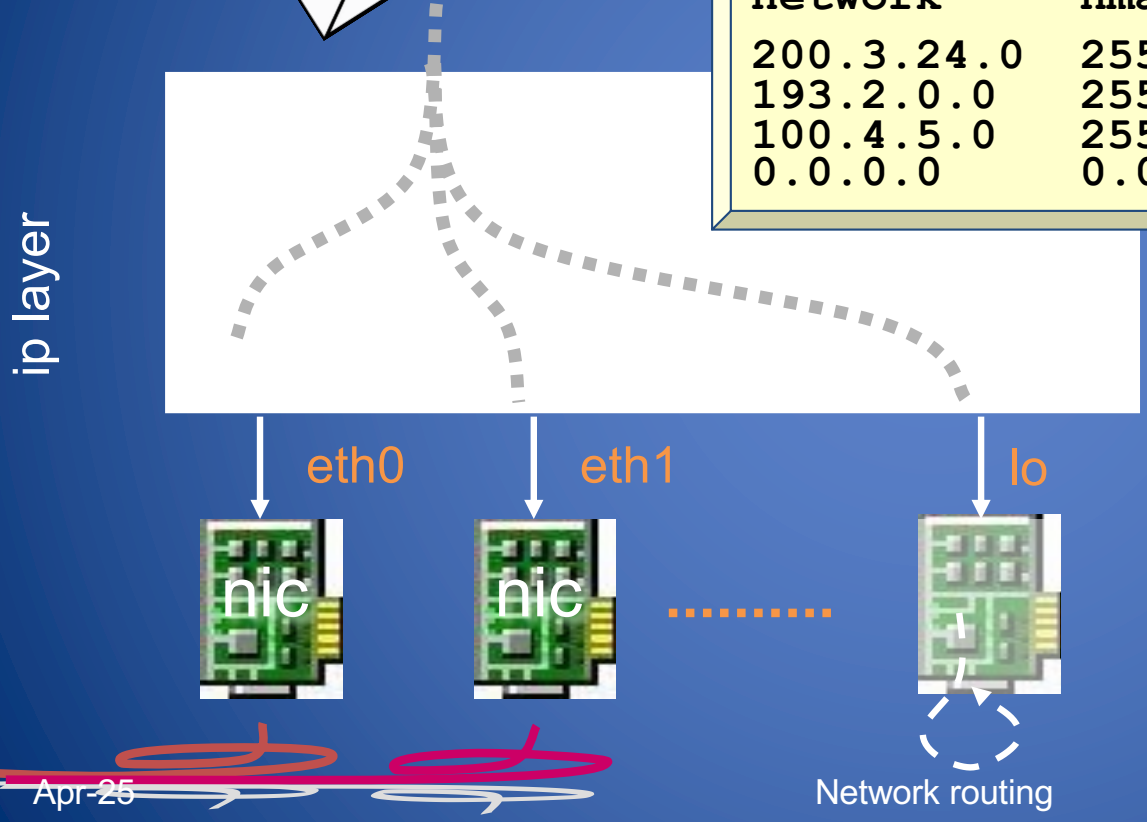


- the ip layer decides which interface an outgoing packet has to be forwarded to
  - regular hosts have at least two interfaces, nic and loopback

routing table

routing table

network	nmask	nexthop	int
200.3.24.0	255.255.255.0	12.0.0.4	eth1
193.2.0.0	255.255.248.0	11.0.0.2	eth0
100.4.5.0	255.240.0.0	11.0.0.3	eth0
0.0.0.0	0.0.0.0	11.0.0.2	eth0



routing table usage

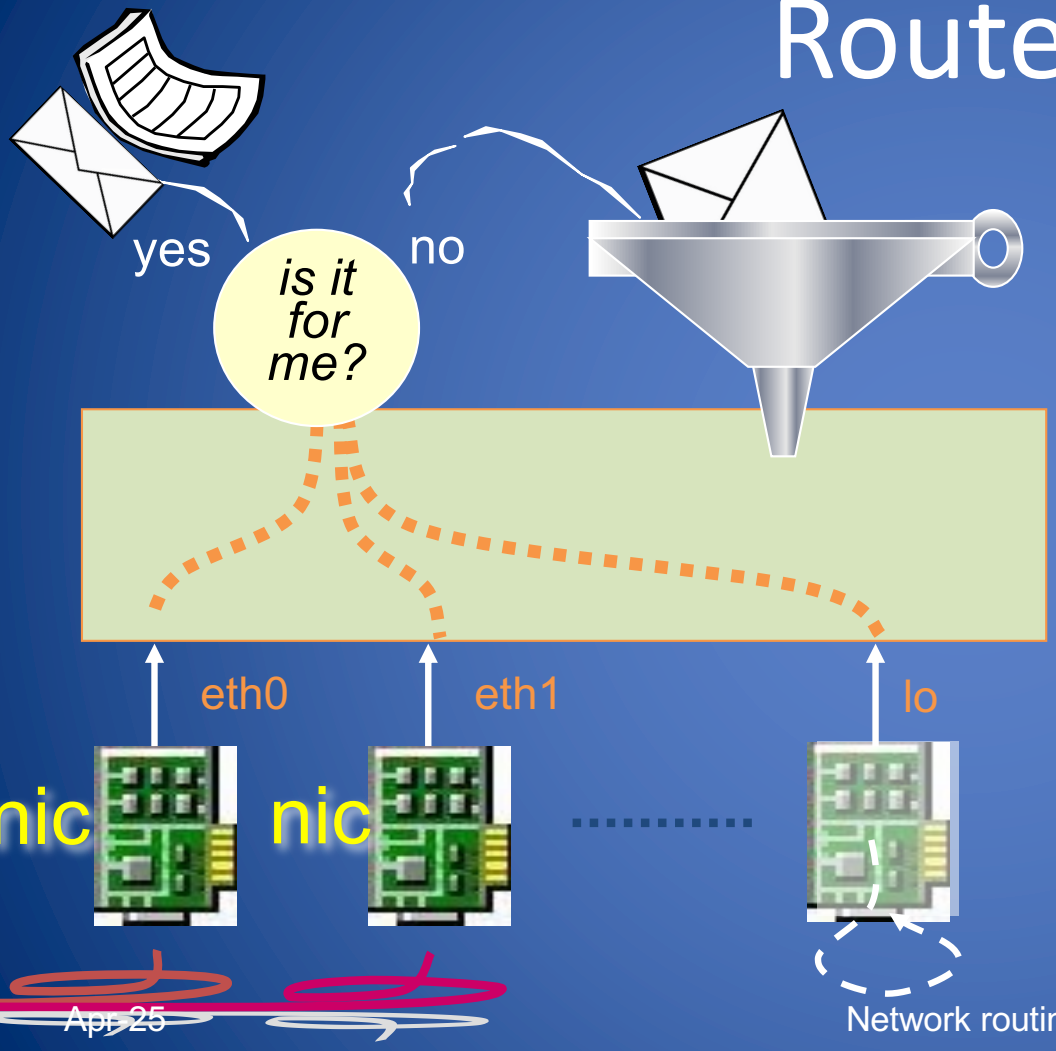
1100 0001.0000 0010.0000 0100.0001 0111

routing table

network	nmask	nexthop	int
200.3.24.0	255.255.255.0	12.0.0.4	eth1
193.2.0.0	255.255.248.0	11.0.0.2	eth0
100.16.0.0	255.240.0.0	11.0.0.3	eth0
0.0.0.0	0.0.0.0	11.0.0.2	eth0

network	nmask
1100 1000.0000 0011.0001 1000.0000 0000	1111 1111.1111 1111.1111 1111.0000 0000
1100 0001.0000 0010.0000 0000.0000 0000	1111 1111.1111 1111.1111 1000.0000 0000
0110 0100.0001 0000.0000 0000.0000 0000	1111 1111.1111 0000.0000 0000.0000 0000
0000 0000.0000 0000.0000 0000.0000 0000	0000 0000.0000 0000.0000 0000.0000 0000

Routers



- a router:
  - has more than one network interface card
  - feeds incoming ip packets (that are not for the router itself) back in the routing process
    - this operation is called *relaying* or *forwarding*
  - also called: *gateway*, *intermediate-system*

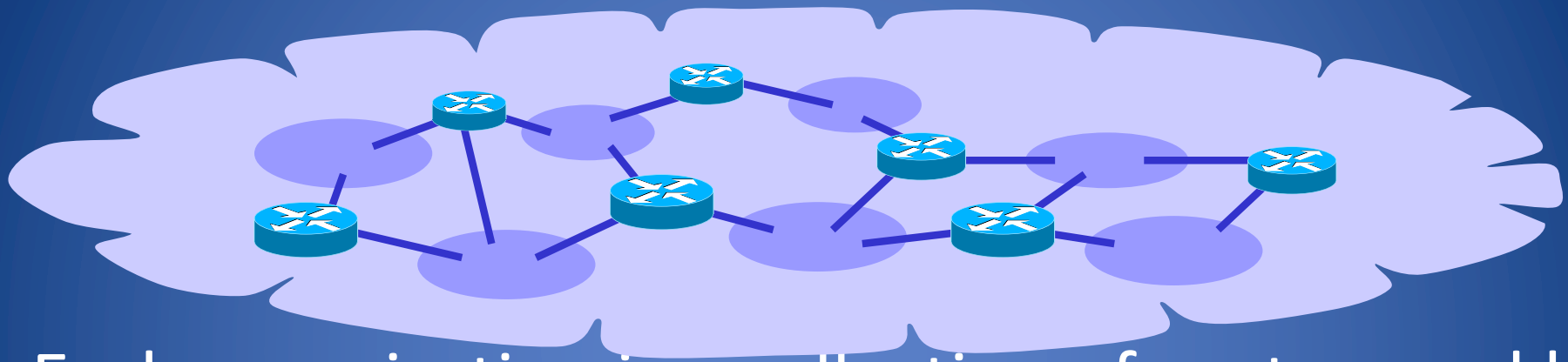
how to update the routing tables?

- Which are the main features that we need?
  1. Global reachability
  2. Dynamic & Automatic update
  3. Fast convergence time
- Different Routing protocols are available
  - Static and manual routing table update is possible but usually not practical

Routing protocols

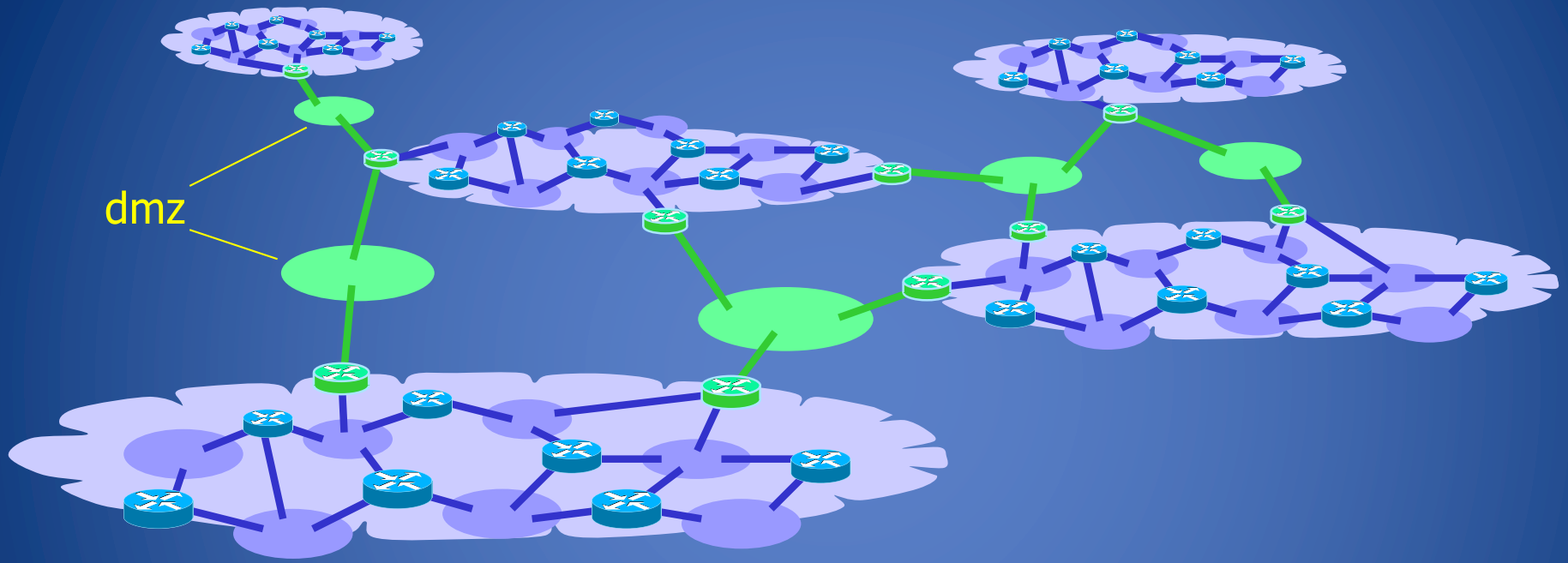
- They fall into two main cathegories:
  - link-state routing protocols
    - approach: talk about your neighbors to everyone
    - each router reconstructs the whole network graph and computes a shortest path tree to all destinations
    - examples: IS-IS, OSPF
  - distance-vector routing protocols
    - approach: talk about everyone with your neighbors
    - update your routing information based on what you hear
    - examples: RIP, BGP

Why interdomain routing?



- Each organization is a collection of routers and lan under a single administration
- A routing algorithm may be chosen to automatically update the routing tables

Why interdomain routing?



- when several organizations join to form the internet they have to set up links between them
  - the added lan are called “demarcation zones”

What about the routing tables?

- in order to have global connectivity:
  - each router must have a routing entry (possibly the default one) that matches the destination address of the packet
  - this should be true for packets to be delivered locally as well as for packets to be delivered to remote lans

Border Gateway Protocol (BGP)

- The routing protocol that makes the Internet work
  - A path vector protocol (similar to a distance vector)
- Used by:
  - customers connected to an Internet Service Provider (ISP) or several ISPs
  - transit providers
  - ISPs that exchange traffic at an Internet eXchange Point (IXP) or Neutral Access Point (NAP)
  - customers with very large networks

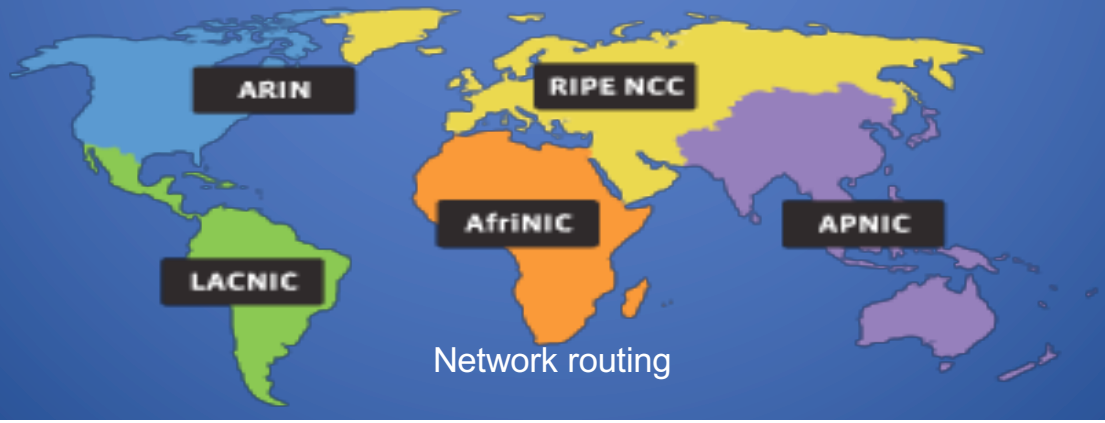
Autonomous System

- autonomous systems (ASes) are the cornerstones of BGP
  - used to uniquely identify networks with a common routing policy
  - usually under single ownership, trust and administrative control
- each AS is identified by an *autonomous system number* (asn): 32 bit integer
- two ranges
  - 0-65535 (original 16-bit range)
  - 65536-4294967295 (32-bit range - RFC4893)

Autonomous System Number

- you may ask an asn to:
  - global asn - to your *regional internet registry* (rir): ripe, arin, apnic, etc.
  - private asn - to your upstream isp
- see also:

  www.iana.org/assignments/as-numbers



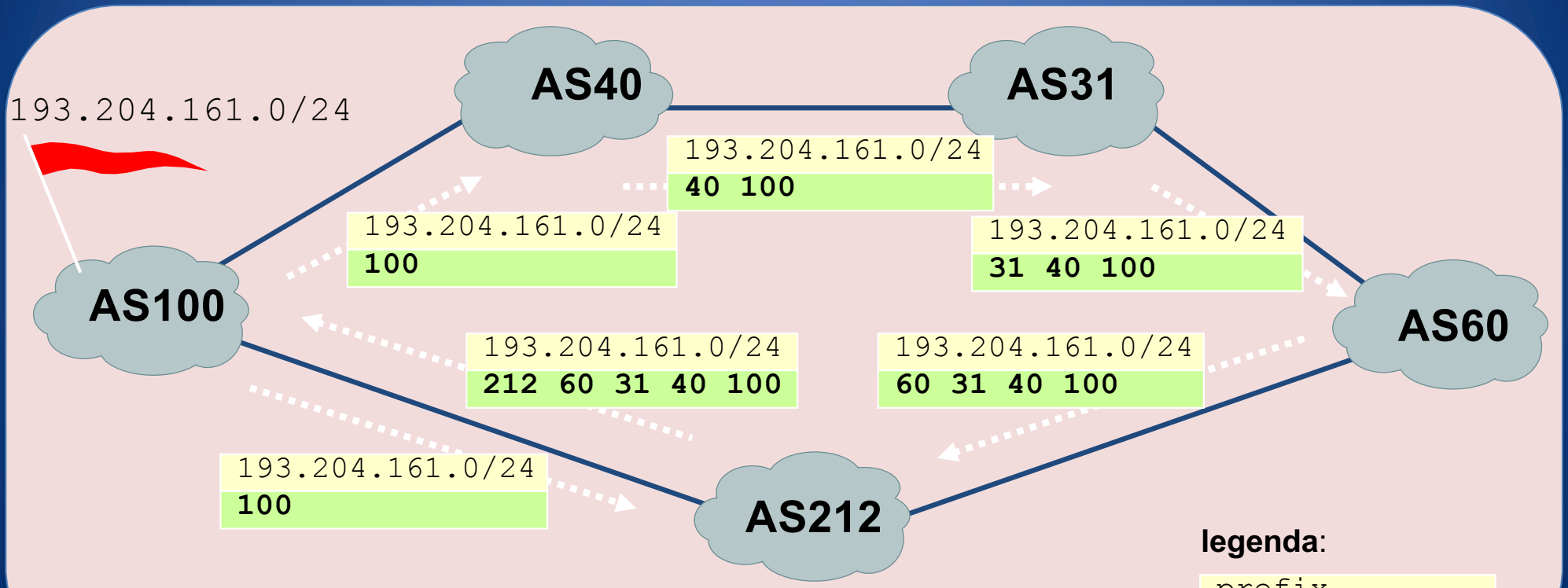
BGP peering

- BGP allows routers to exchange information only if a *peering* session is up
- a BGP peering is the tcp connection (port 179) over which routing information will be exchanged

Announcements and traffic flows

- BGP allows a router to offer connectivity to another router
- “offering connectivity” means “promising the delivery to a specific destination”

attributes: AS-path



Looking Glass Server (Demo)

- Provides backbone routing and network efficiency information
  - BGP, Traceroute, and Ping
    - tools that are possible to use with the same transparency that users on ISP network receive directly
- Demo: Hurricane Electric
  - http://bgp.he.net - http://lg.he.net/
  - https://bgp.he.net/super-lg/#128.148.0.0/21

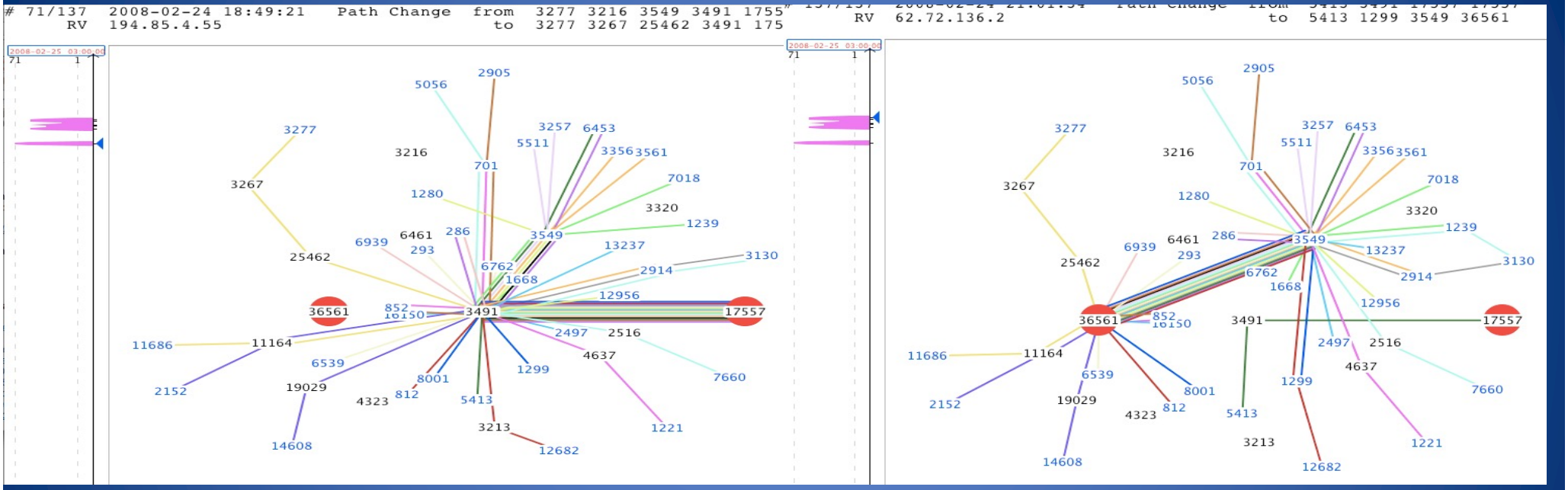
BGP Vulnerabilities

- In the original version BGP has no security mechanisms:
  - No encryption: Eavesdropping
  - No timestamp: Replaying
  - No signature: Hijacking
  - Selective dropping
- Possible attacks:
  - Injecting false information into the global routing database
  - Reroute traffic to perform a Man-in-the-Middle (MITM) attack
  - Trying to create a Denial of Service (DoS) like a black hole in the network

A big incident

- February 2008 Pakistan Telecom (PT) would like to block Youtube access from Pakistan
  - PT falsely informed that through this company there was the most directed way to reach Youtube
- Soon over 2/3 of the Internet was not able to reach Youtube for a couple of hours
- A Routing problem…

YouTube Internet Hijacking In Pakistan



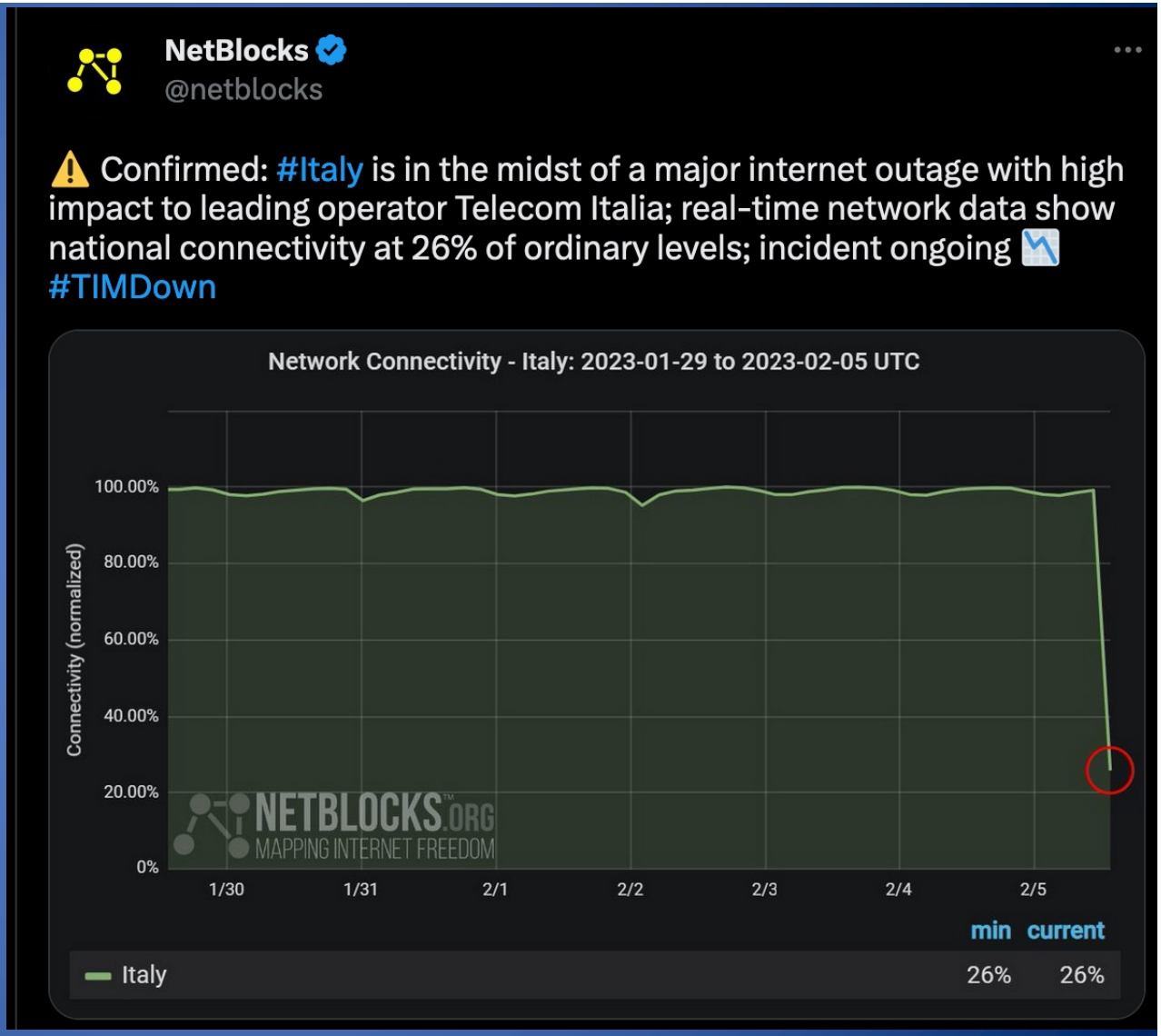
AS 17557 Pakistan, AS 36561 Youtube

[Ripe description using bgplay tool developed at Roma Tre University: https://www.youtube.com/watch?v=IzLPKuAOe50]

TIMDown

Stopped the communication for 6 hours on 2/5/23

Probably a human error due to a bad DDOS configuration



What We Have Learned

- IP address space allocation
- ARP protocol
- ARP poisoning attack
- Transport layer protocols
  - TCP for reliable transmission
  - UDP when packet loss/corruption is tolerated
- Lack of built-in security for link, network, and transport layer protocols
  - Security enhanced protocols have been developed for these layers
  - Alternate solution is to provide security at application layer