Networks II: Local network attacks

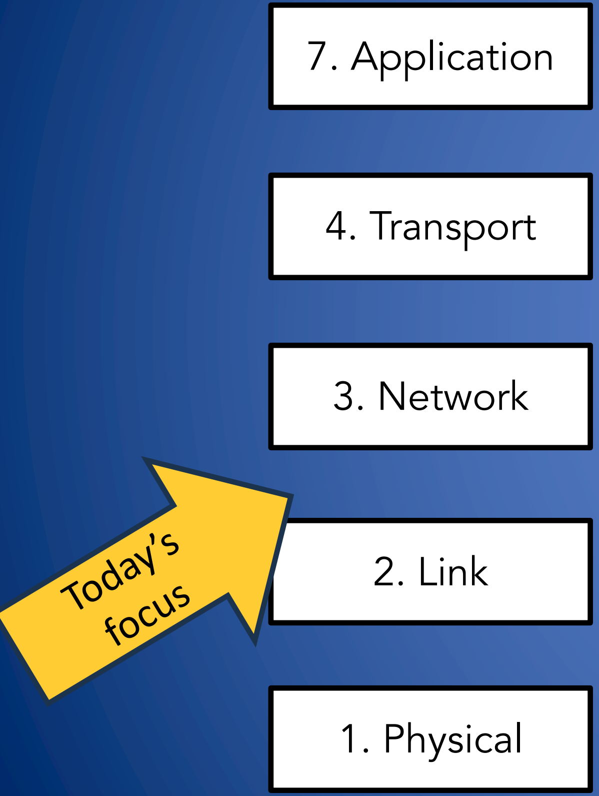
CS 1660: Introduction to Computer Systems Security

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

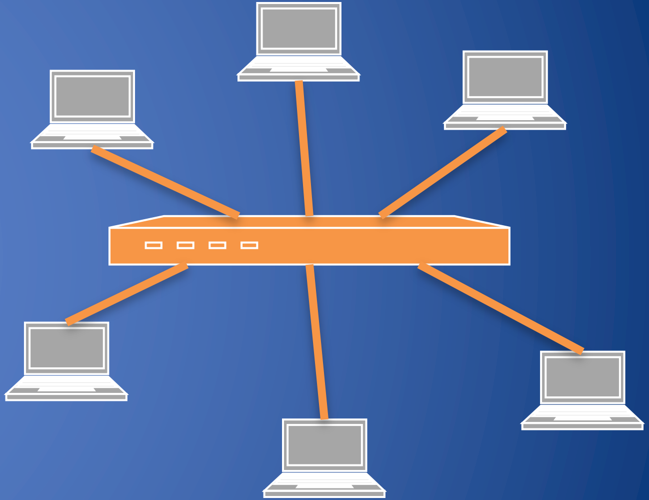
Protocols for sending data on individual links
Examples: Wifi, Ethernet, Bluetooth, …
Defines: MAC address *(more on this later)*

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)

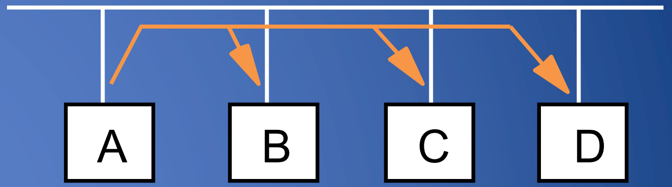
- Connects the network layer to the data link layer
- Maps IP addresses to MAC addresses
- Based on broadcast messages and local caching
- Does not support confidentiality, integrity, or authentication
- Defined as a part of RFC 826

ARP Messages

- ARP broadcasts in a frame a requests of type

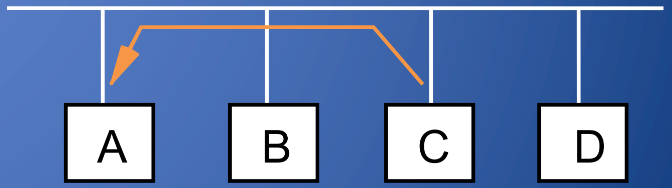
  who has <IP addressC >

  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
```

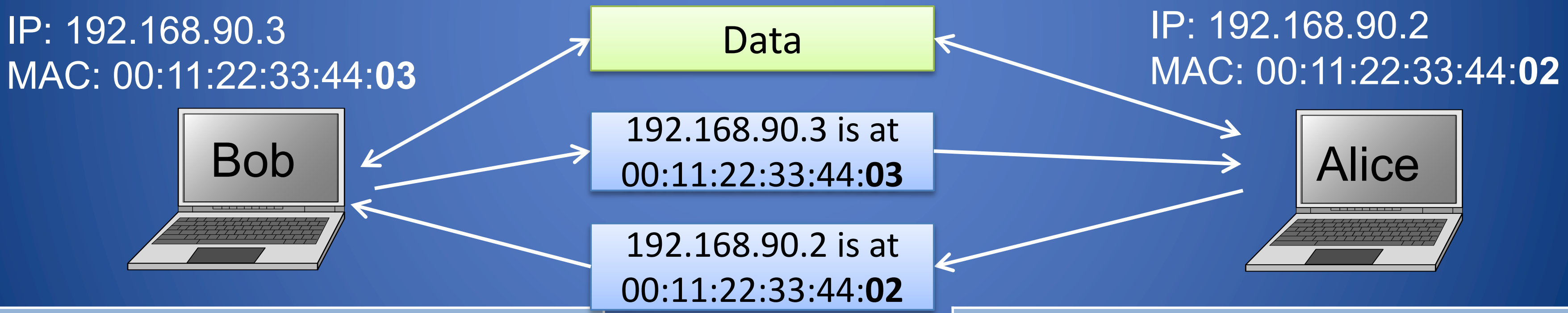
- Command arp –a –d flushes the ARP cache (with administrative privileges)
- ARP cache entries are stored for a configurable amount of time

ARP 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



IP: 192.168.90.3
MAC: 00:11:22:33:44:**03**

Data

192.168.90.3 is at 00:11:22:33:44:**03**

192.168.90.2 is at 00:11:22:33:44:**02**

IP: 192.168.90.2
MAC: 00:11:22:33:44:**02**

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

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

Clicker Question (1)

After a great experience at CS1660 TA hours, Bob decides to message Alice about how much he appreciates the CS1660 staff. Eve would like to trick Bob into sending this network traffic to her (instead of Alice). Assuming Eve has access to everyone’s MAC and IP, what ARP response could Eve send to Bob to accomplish this?

A. <Eve’s IP> is at <Eve’s MAC>

B. <Eve’s IP> is at <Alice’s MAC>

C. <Alice’s IP> is at <Eve’s MAC>

D. <Alice’s IP> is at <Alice’s MAC>

Clicker Question (1) Answer

After a great experience at CS1660 TA hours, Bob decides to message Alice about how much he appreciates the CS1660 staff. Eve would like to trick Bob into sending this network traffic to her (instead of Alice). Assuming Eve has access to everyone’s MAC and IP, what ARP response could Eve send to Bob to accomplish this?

A. <Eve’s IP> is at <Eve’s MAC>

B. <Eve’s IP> is at <Alice’s MAC>

C. <Alice’s IP> is at <Eve’s MAC>

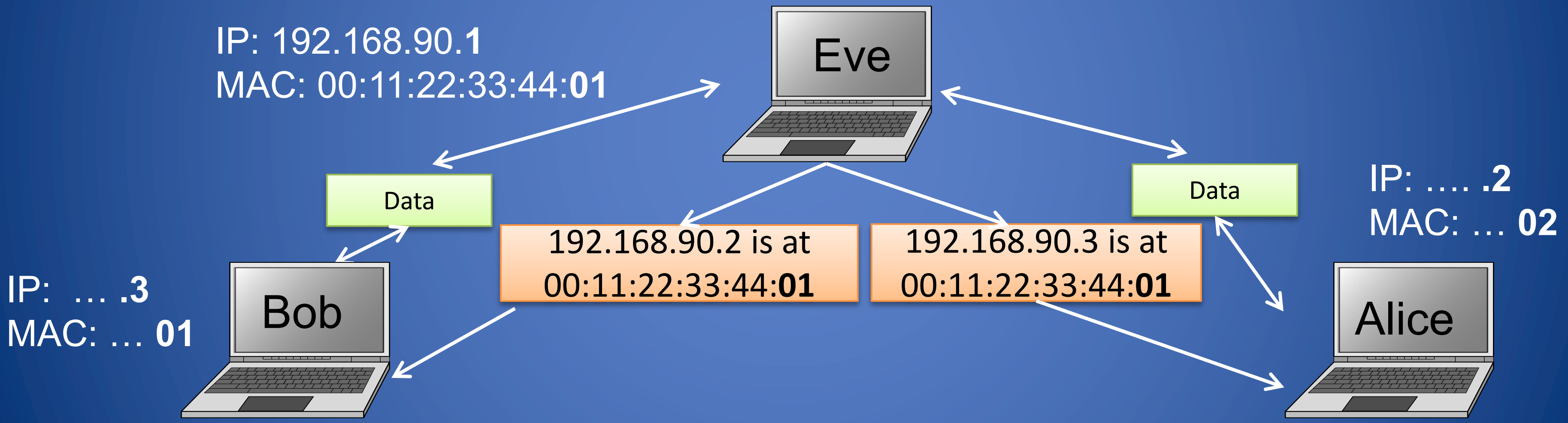
D. <Alice’s IP> is at <Alice’s MAC>

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



IP: 192.168.90.**1**
MAC: 00:11:22:33:44:**01**

Eve

IP: …. **.2**
MAC: … **02**

Data

Data

192.168.90.2 is at 00:11:22:33:44:**01**

192.168.90.3 is at 00:11:22:33:44:**01**

IP: … **.3**
MAC: … **01**

Bob

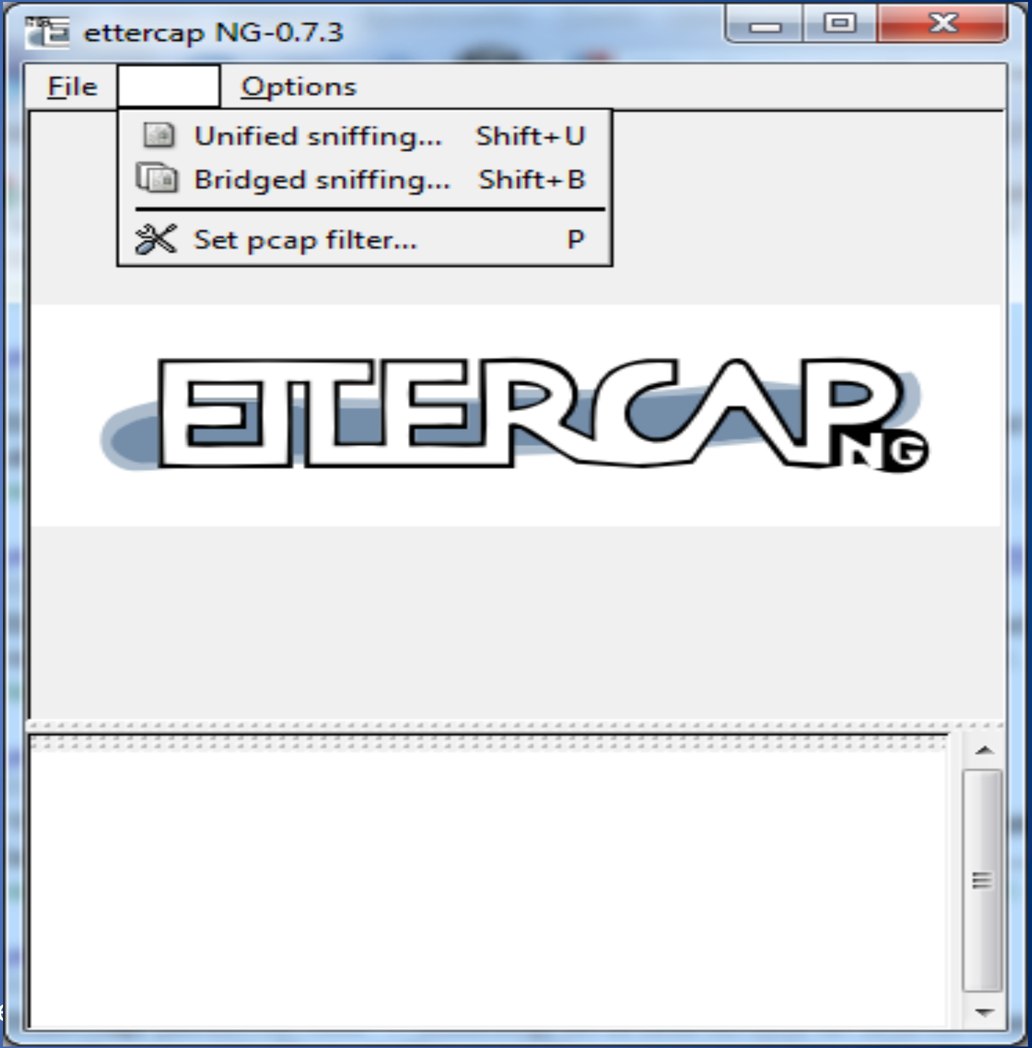
Alice

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)



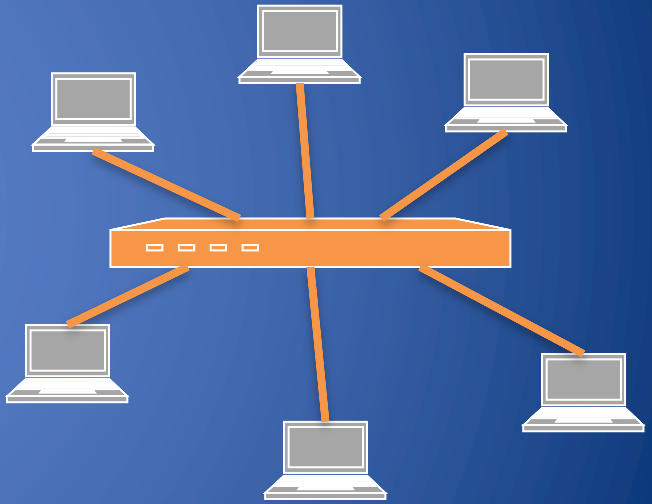
Another attack on switches…

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?

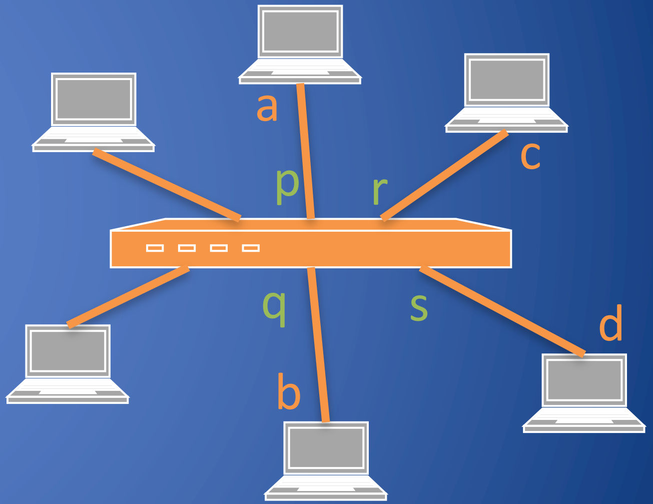


MAC learning: Example

- 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

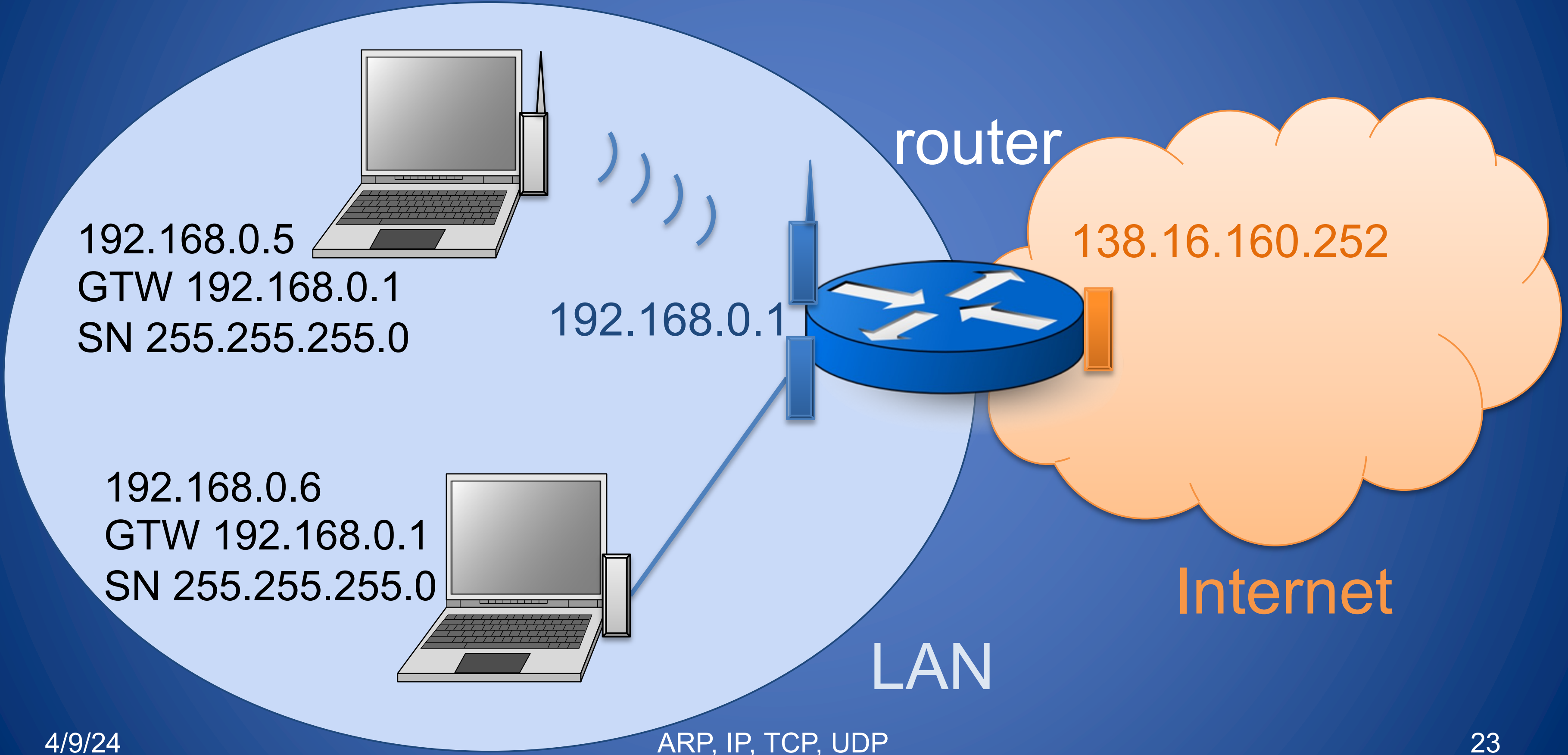


Attack on a learning switch

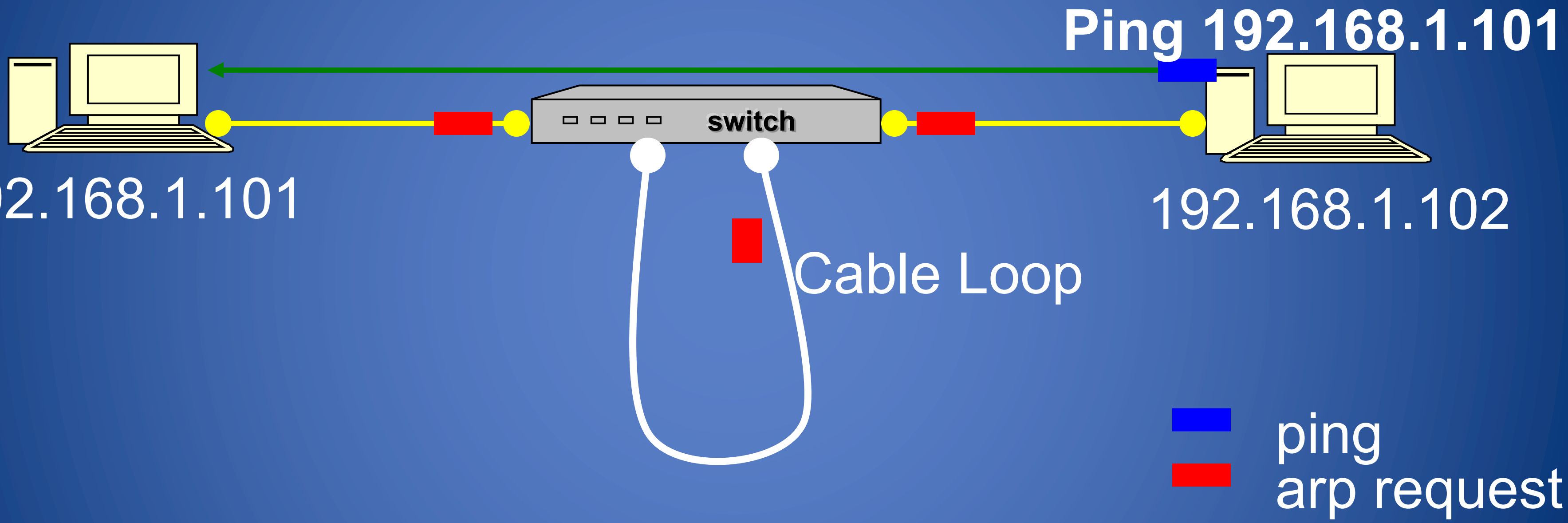
- Idea: flood the switch with many packets from different source MAC addresses

- If MAC table is full, switch just broadcasts all packets to all ports

From the LAN to the Internet



network DOS using ARP



Ping 192.168.1.101

switch

192.168.1.101

192.168.1.102

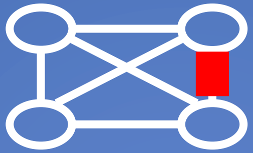
Cable Loop

🟦 ping

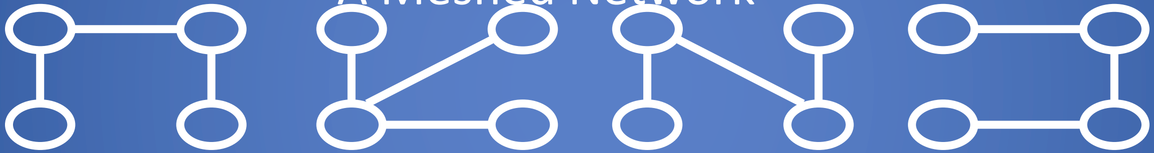
🟥 arp request

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

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?

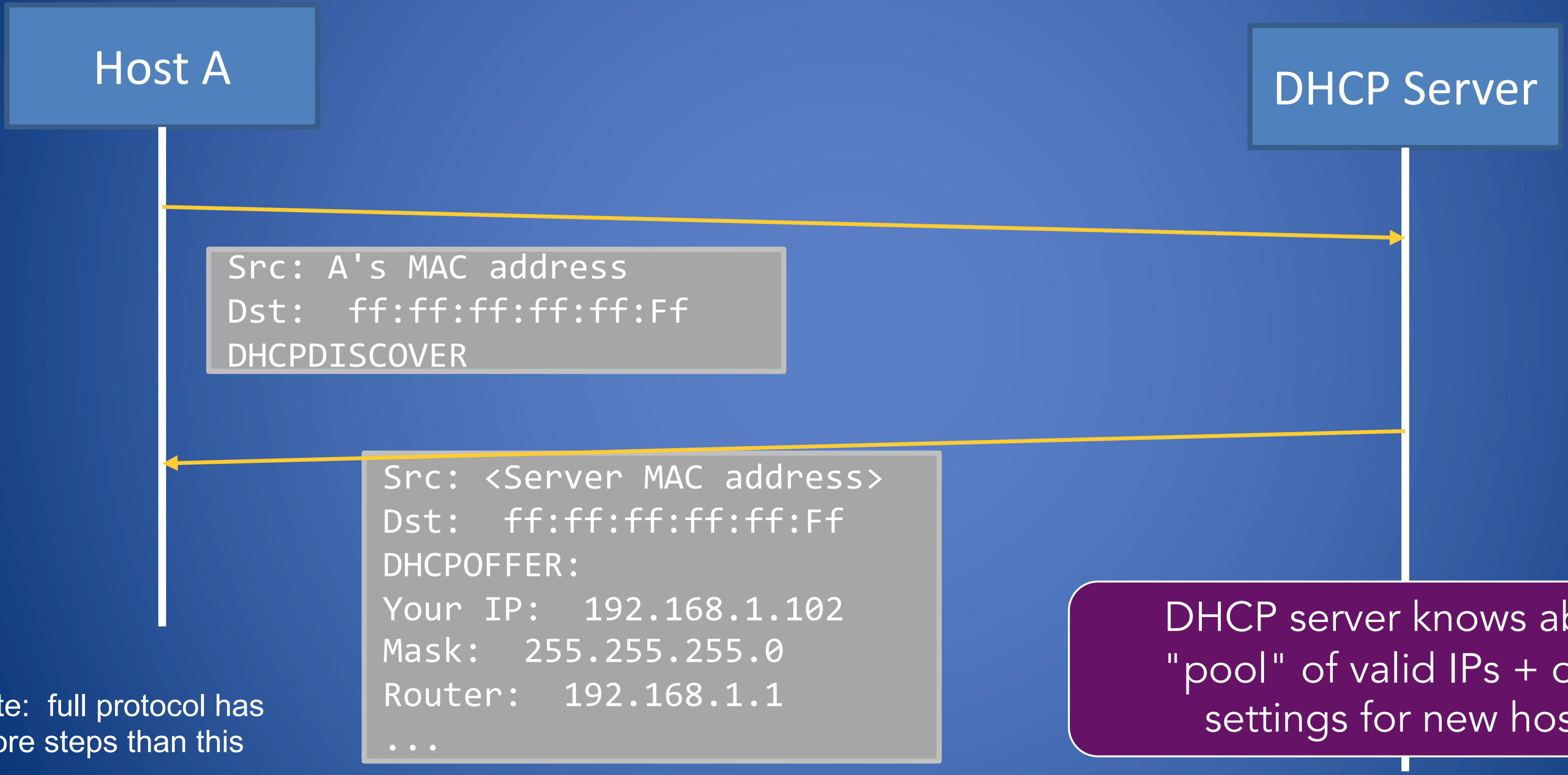
Broadcast traffic

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



```
Src: A's MAC address
Dst:  ff:ff:ff:ff:ff:Ff
DHCPDISCOVER
```

```
Src: <Server MAC address>
Dst:  ff:ff:ff:ff:ff:Ff
DHCPOFFER:
Your IP:  192.168.1.102
Mask:  255.255.255.0
Router:  192.168.1.1
...
```

DHCP server knows about "pool" of valid IPs + other settings for new hosts

Note: full protocol has more steps than this

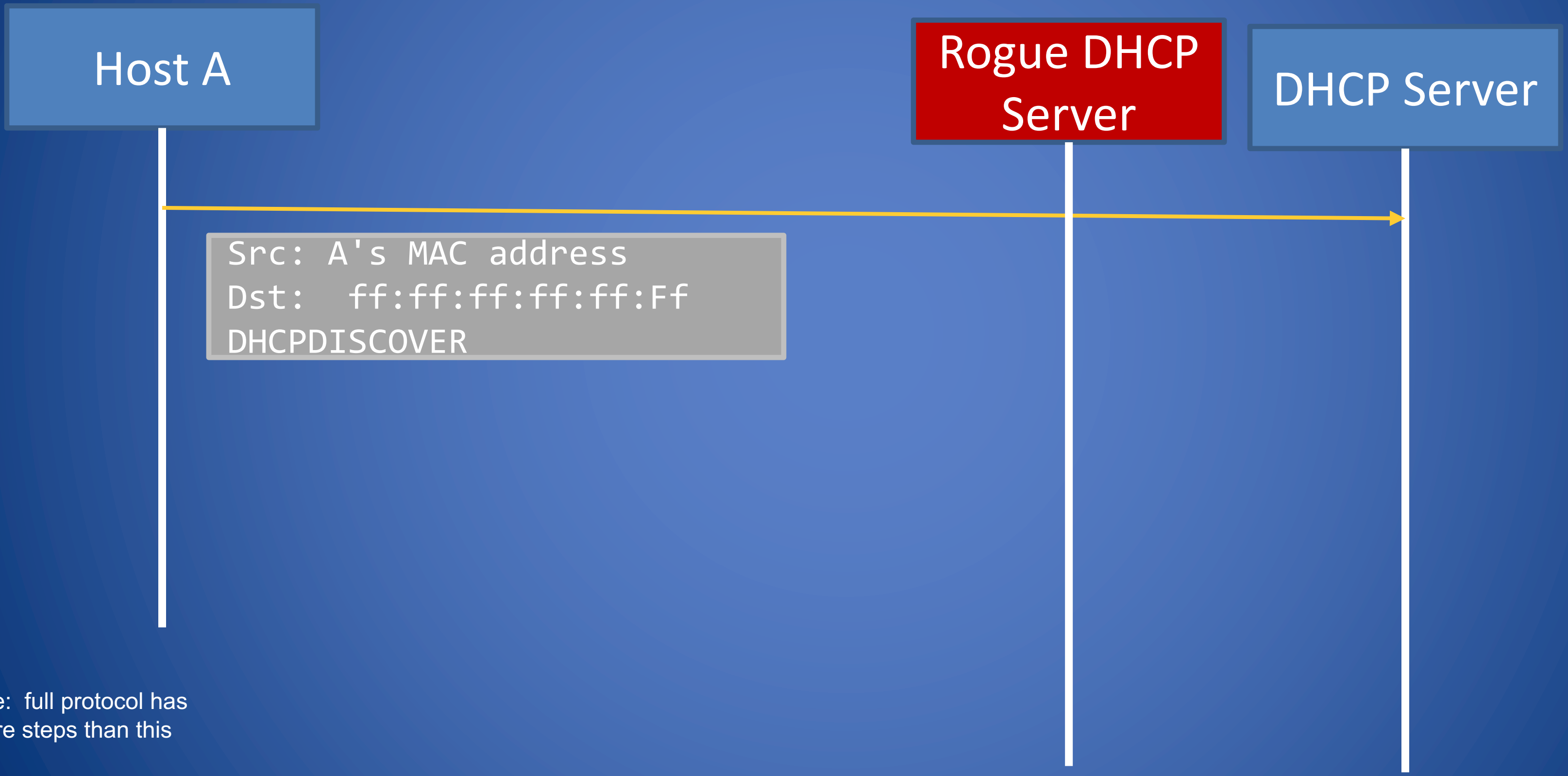
Problems with DHCP?

- 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



Host A

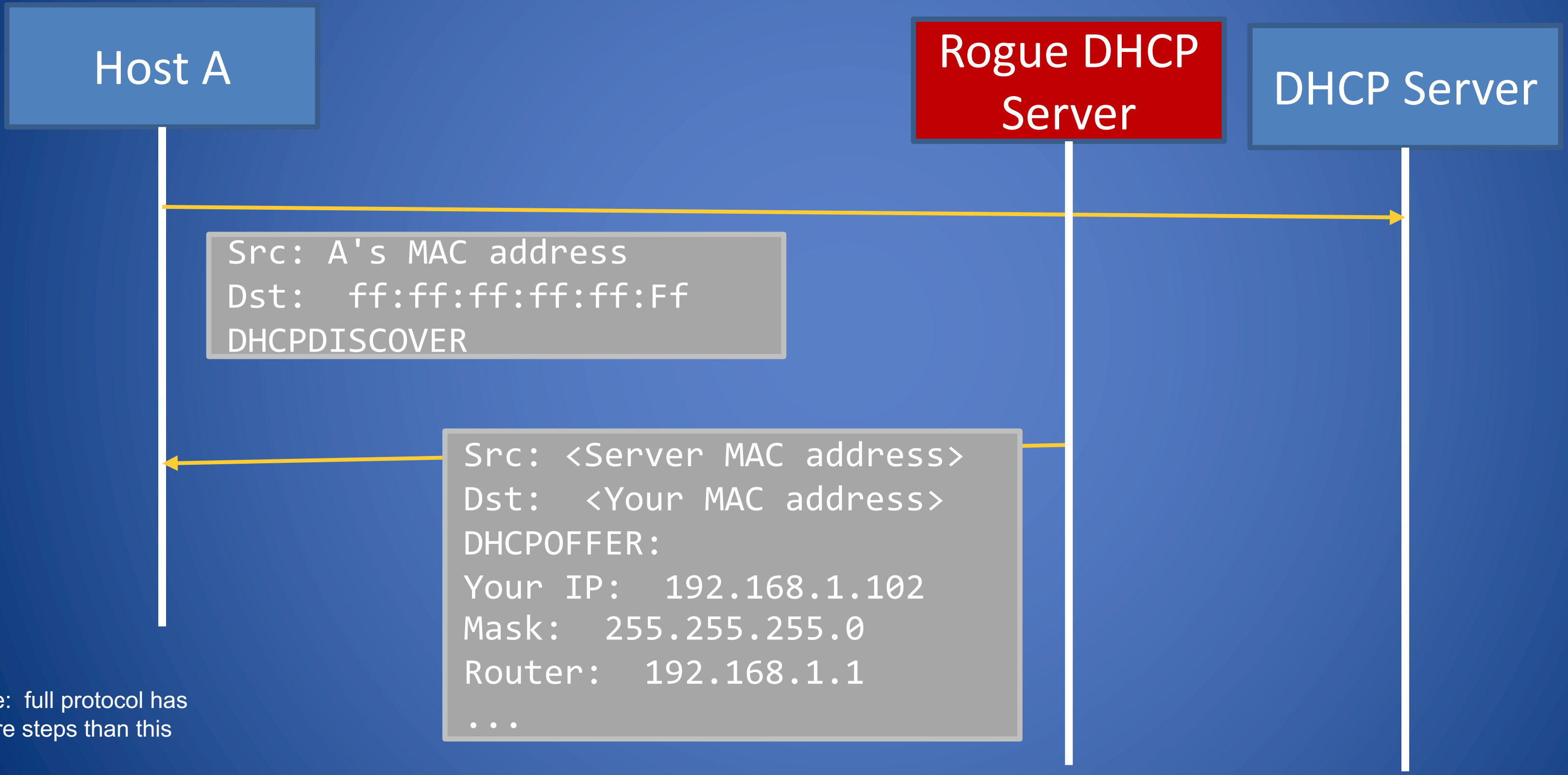
Rogue DHCP Server

DHCP Server

```
Src: A's MAC address
Dst:  ff:ff:ff:ff:ff:Ff
DHCPDISCOVER
```

Note: full protocol has more steps than this

DHCP Spoofing

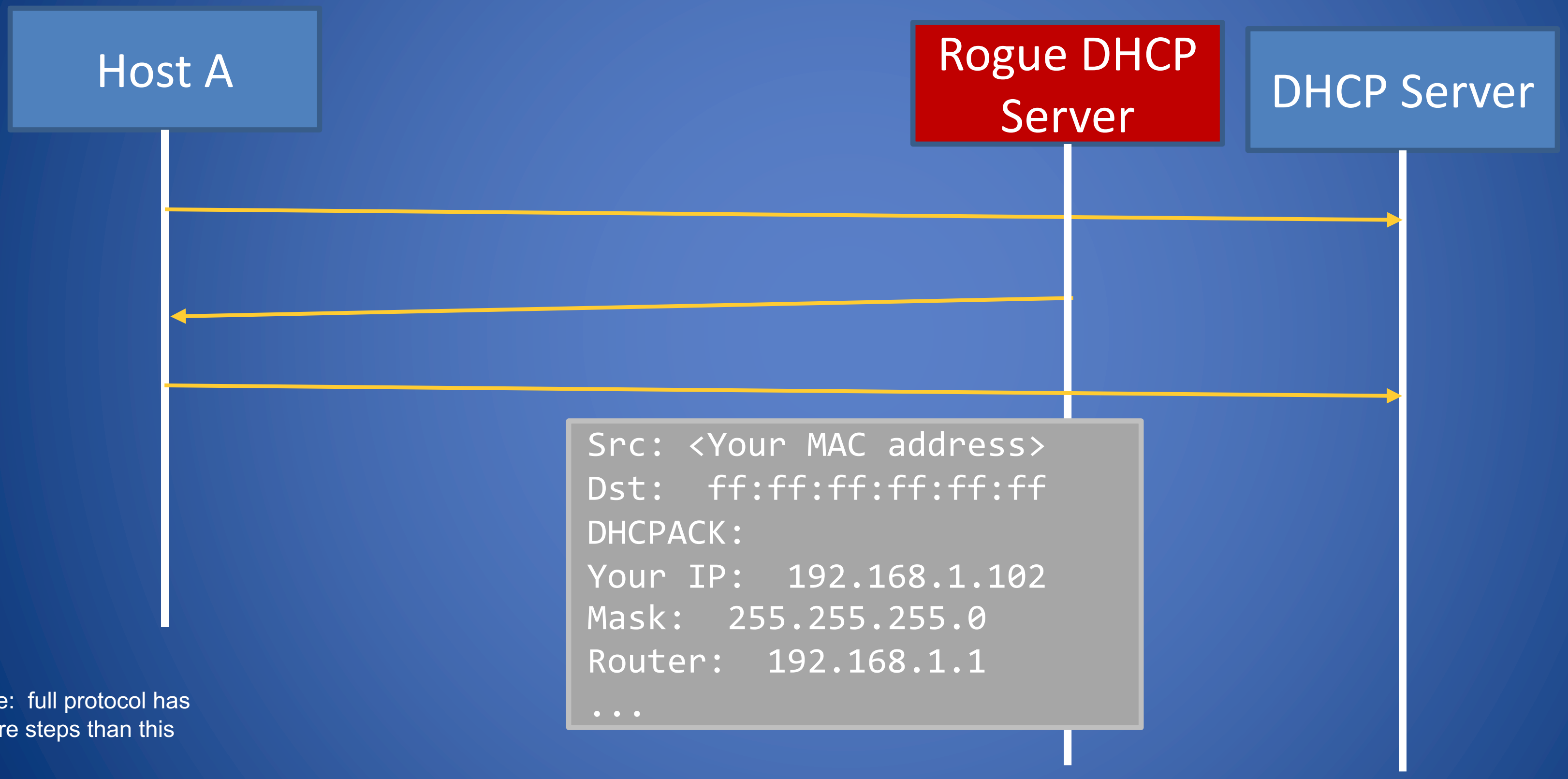


```
Src: A's MAC address
Dst:  ff:ff:ff:ff:ff:Ff
DHCPDISCOVER
```

```
Src: <Server MAC address>
Dst:  <Your MAC address>
DHCPOFFER:
Your IP:  192.168.1.102
Mask:  255.255.255.0
Router:  192.168.1.1
...
```

Note: full protocol has
more steps than this

DHCP Spoofing



```
Src: <Your MAC address>
Dst:  ff:ff:ff:ff:ff:ff
DHCPACK:
Your IP:  192.168.1.102
Mask:  255.255.255.0
Router:  192.168.1.1
...
```

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

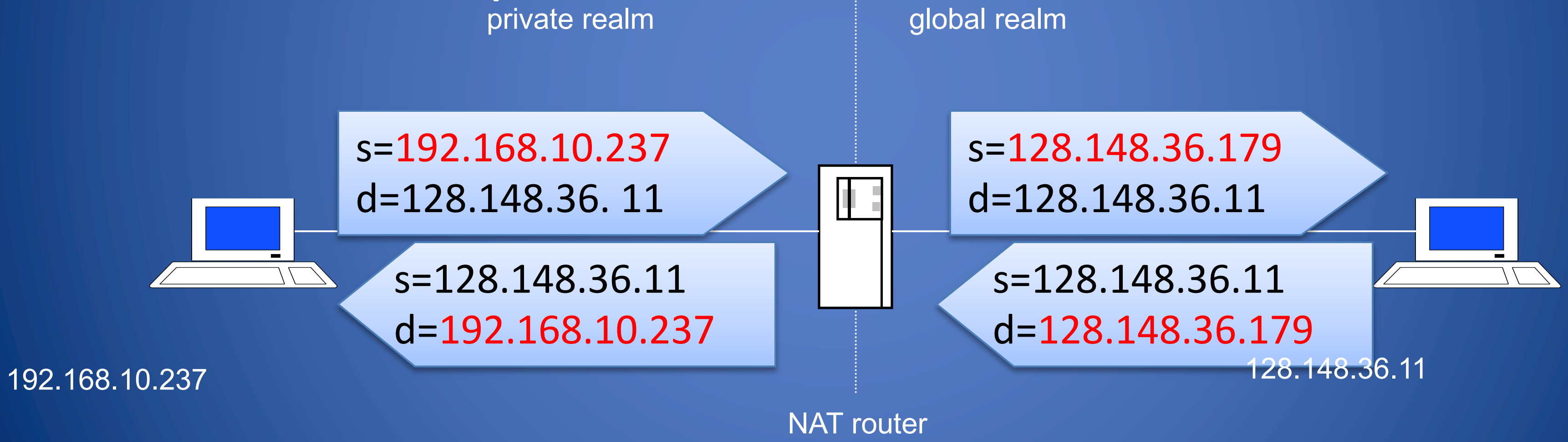
IP Address Space

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



private realm

global realm

s=192.168.10.237
d=128.148.36. 11

s=128.148.36.11
d=192.168.10.237

s=128.148.36.179
d=128.148.36.11

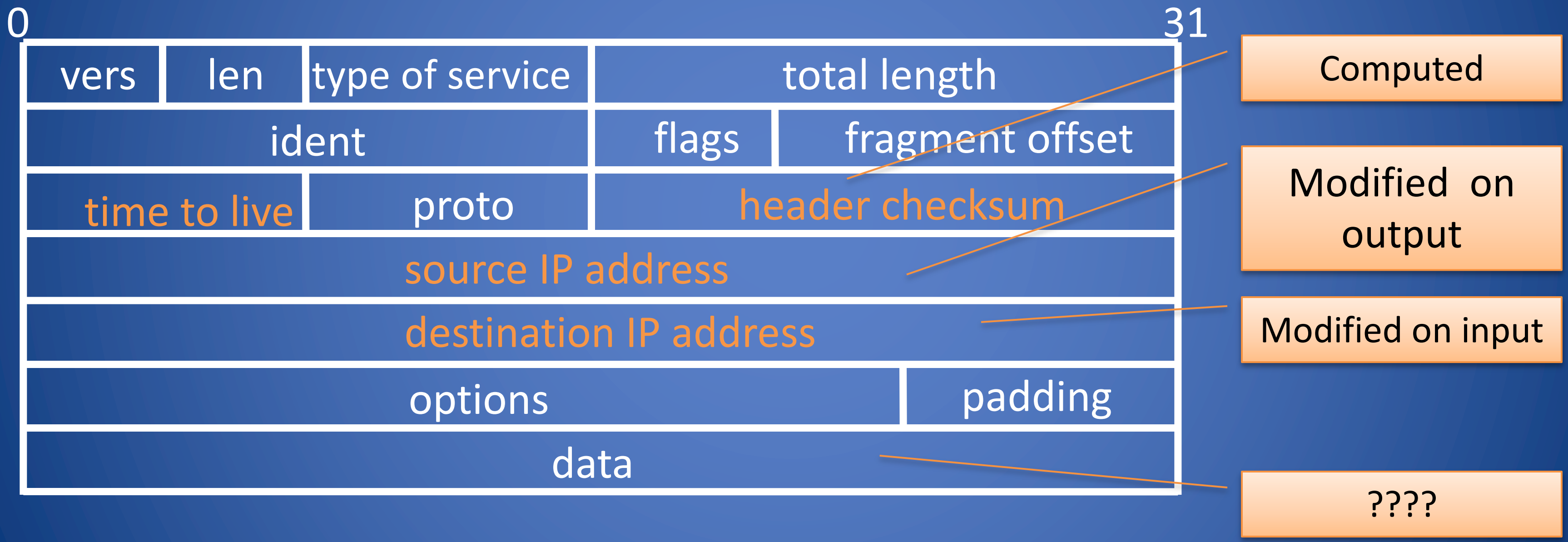
s=128.148.36.11
d=128.148.36.179

192.168.10.237

128.148.36.11

NAT router

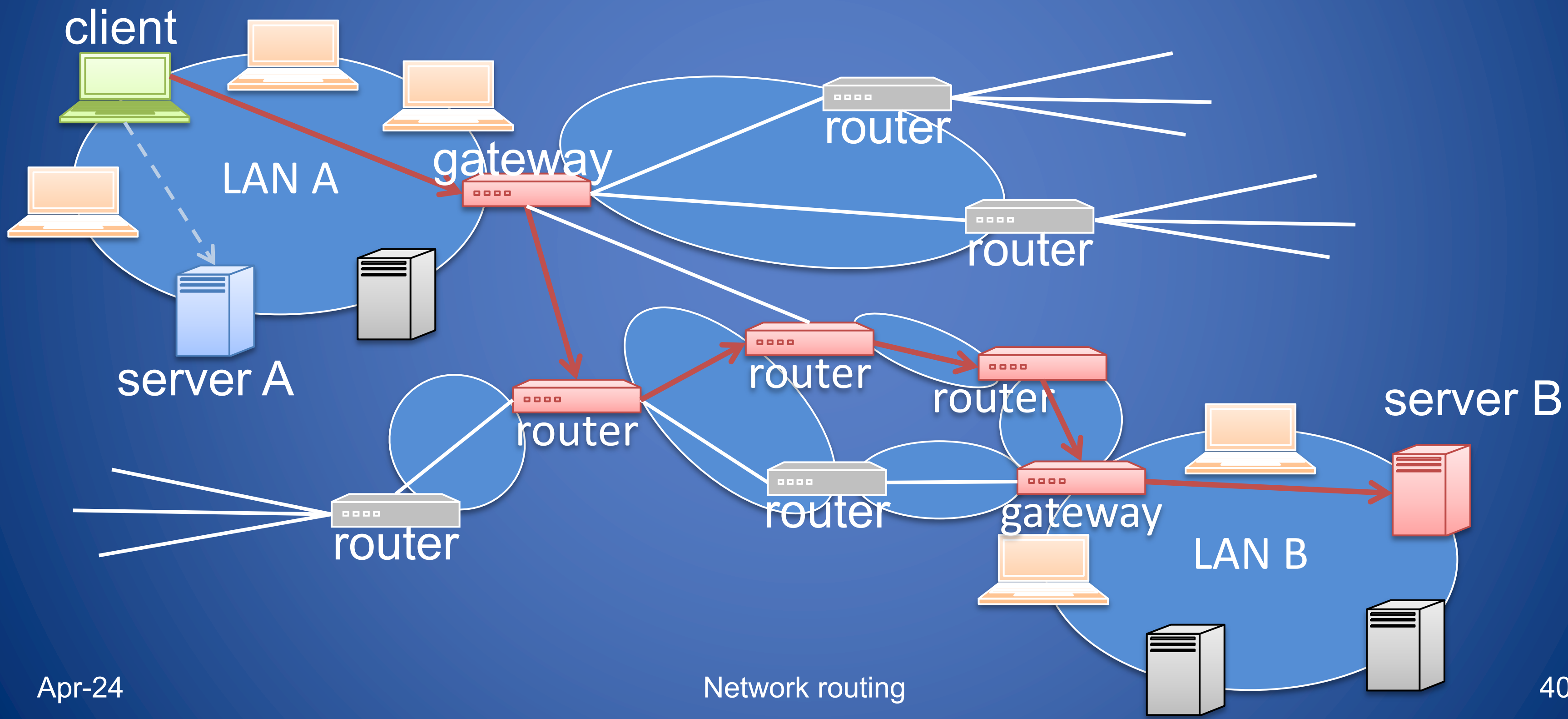
IP Packet Modifications



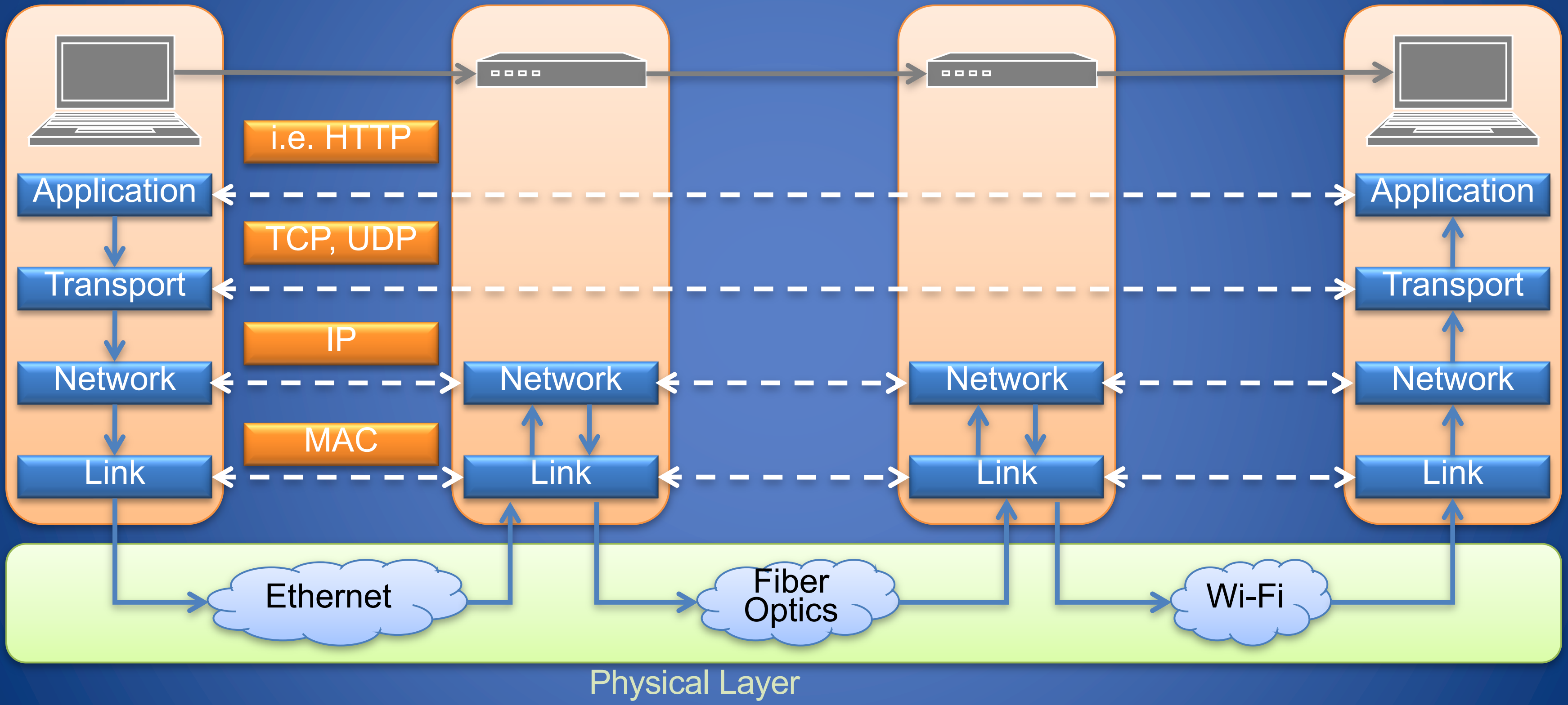
Routing
How does internet actually work?

Why Routing?

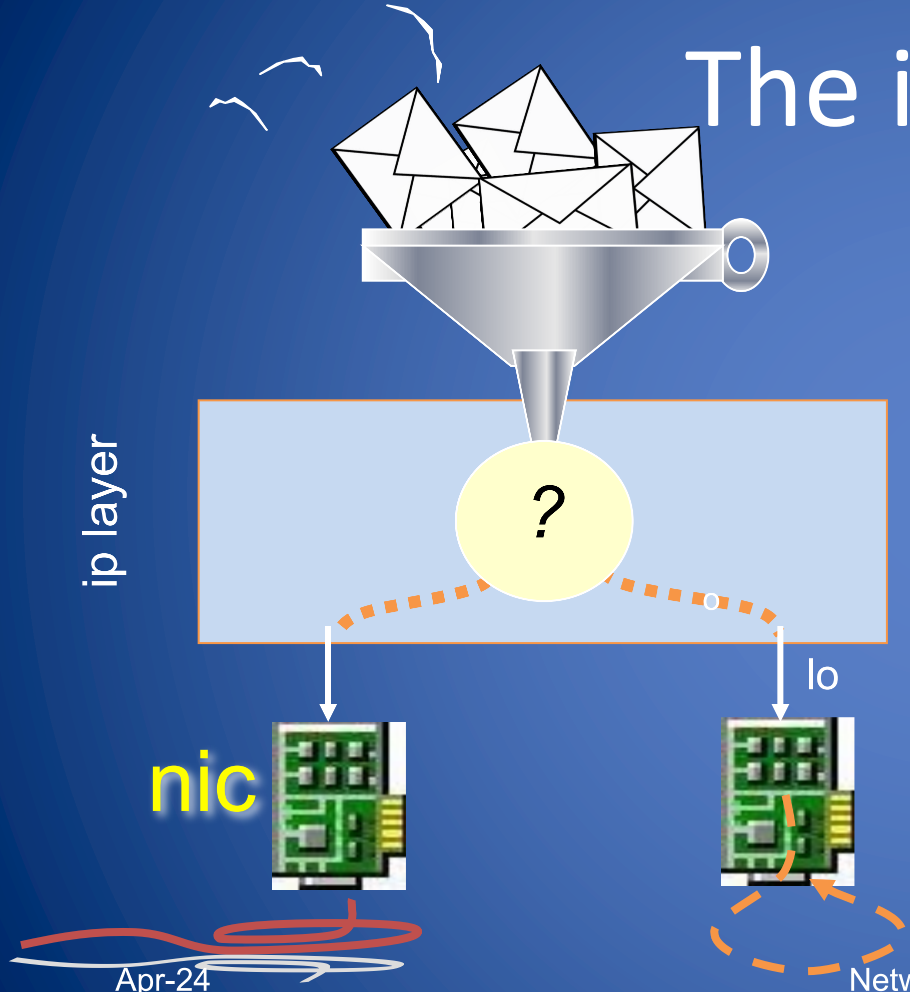
- Reaching a host within a network is a routing problem



Internet Layers

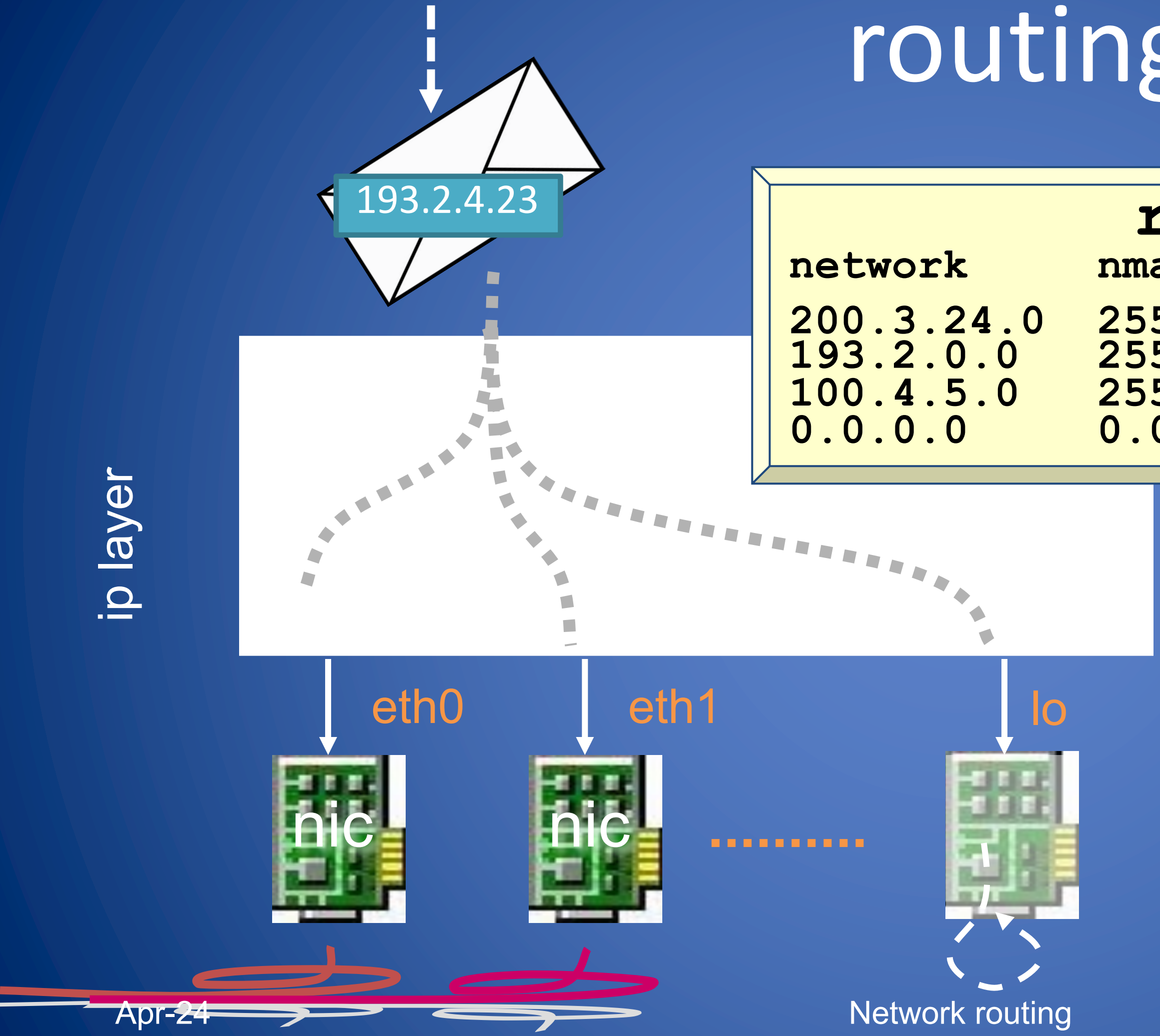


The ip layer



- 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

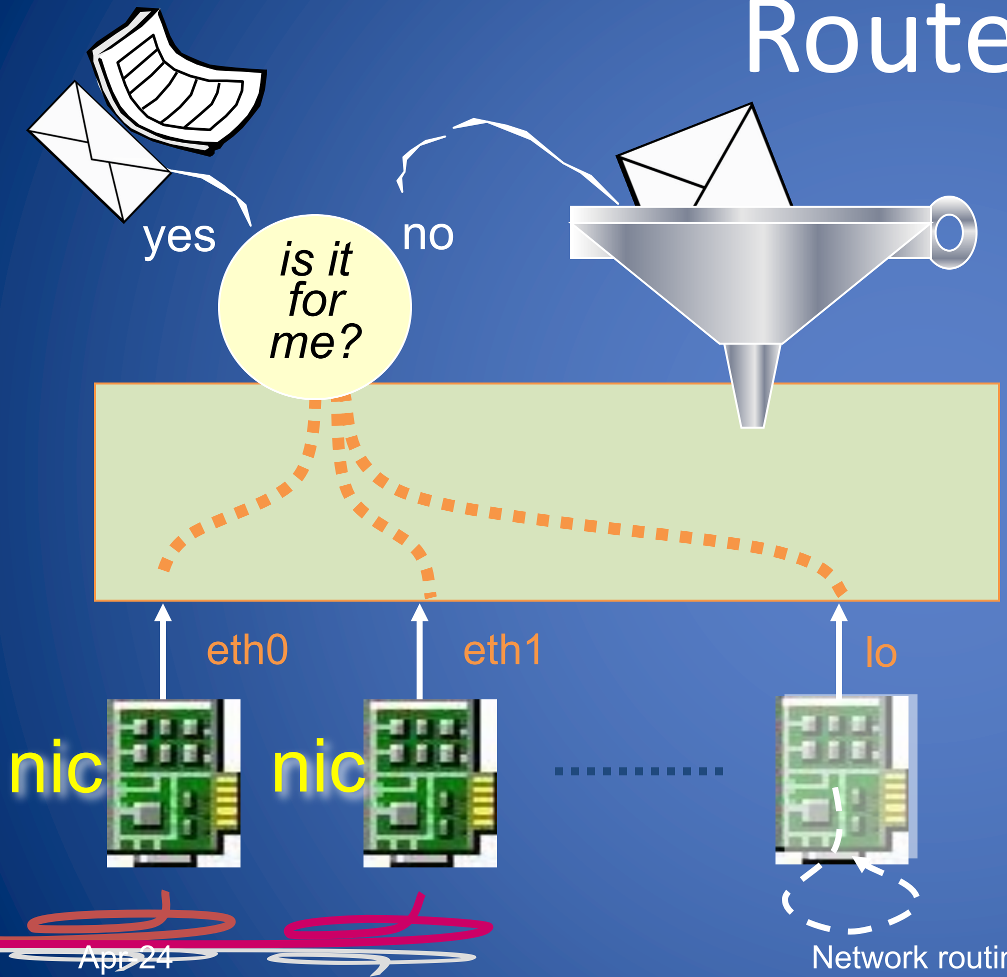
```
1100 0001.0000 0010.0000 0100.0001 0111
```

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*

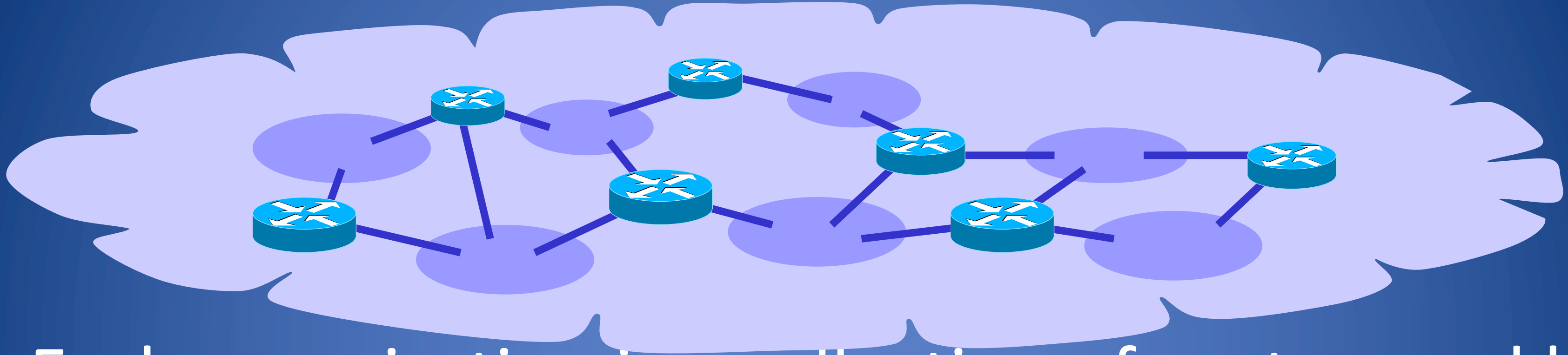
how to update the routing tables?

- 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

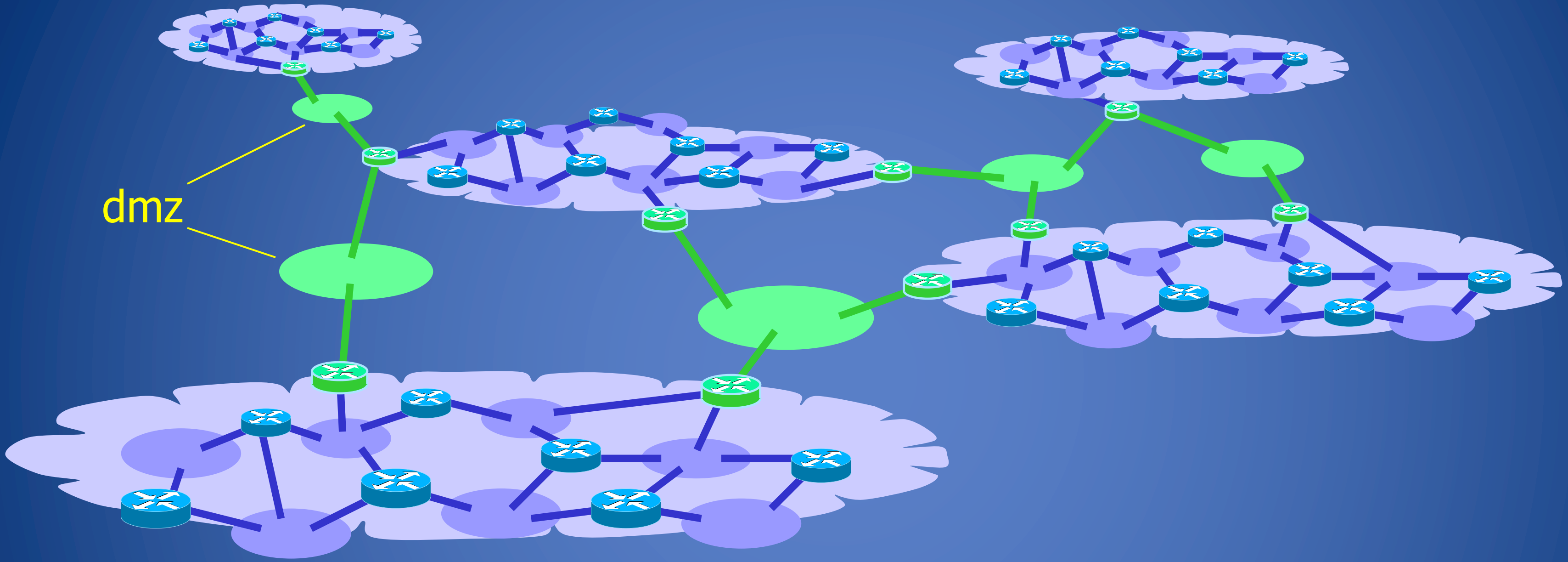
- They fall into two main cathegories:
  - link-state routing protocols
    - approach: talk about your neighbors to everyone
    - each router reconstructs the whole network graph and computes a shortest path tree to all destinations
    - examples: IS-IS, OSPF
  - distance-vector routing protocols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

Why interdomain routing?



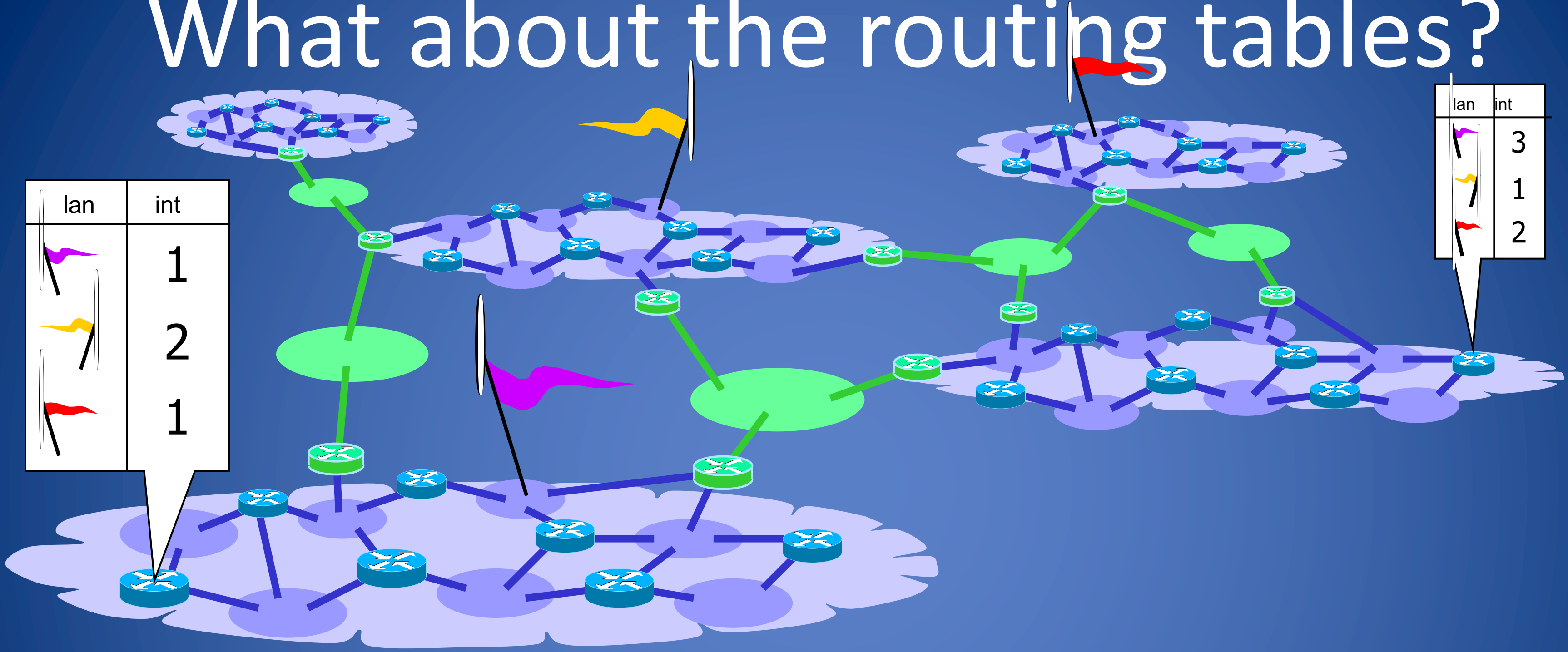
- Each organization is a collection of routers and lan under a single administration
- A routing algorithm may be chosen to automatically update the routing tables

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

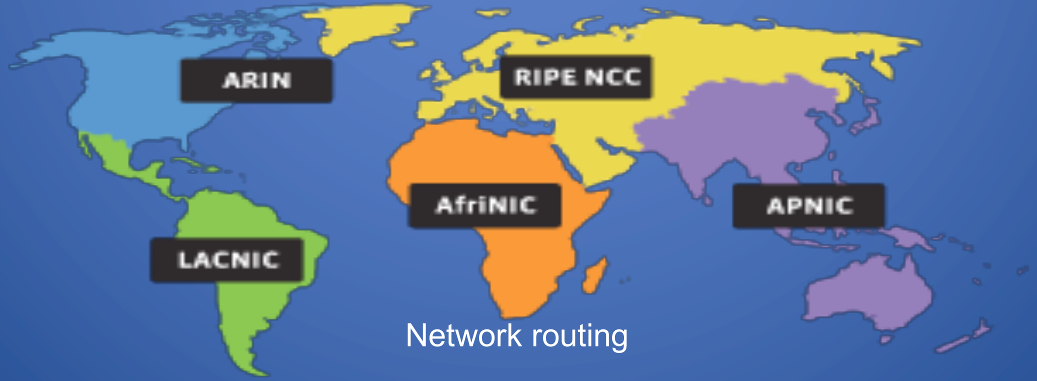
Autonomous System

- 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

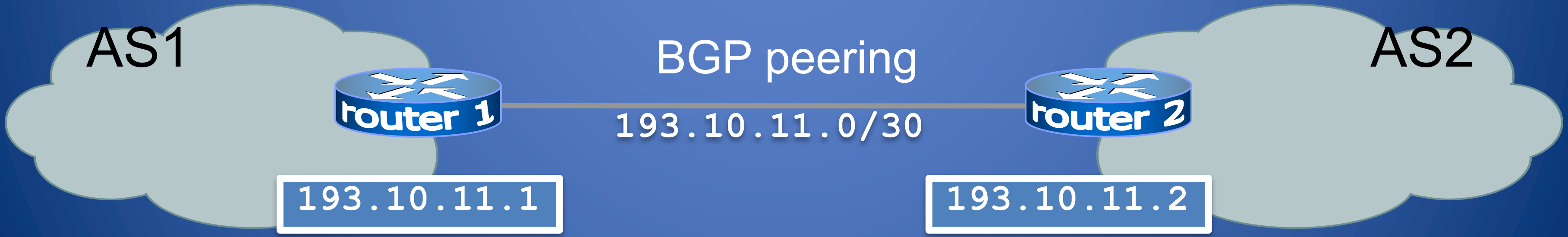
- you may ask an asn to:
  - global asn - to your *regional internet registry* (rir): ripe, arin, apnic, etc.
  - private asn - to your upstream isp
- see also:

  www.iana.org/assignments/as-numbers



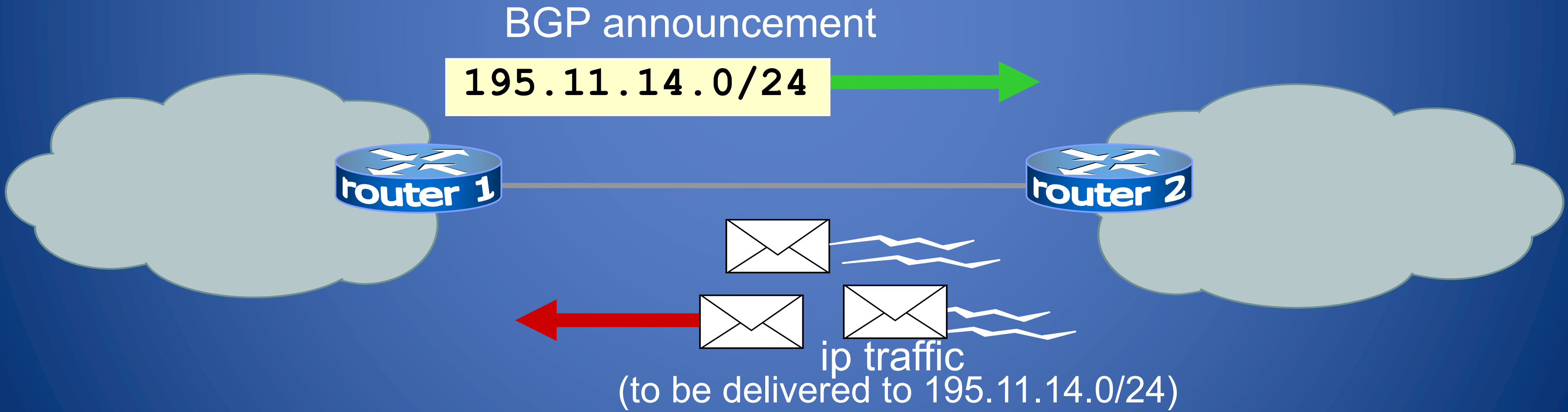
BGP peering

- 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

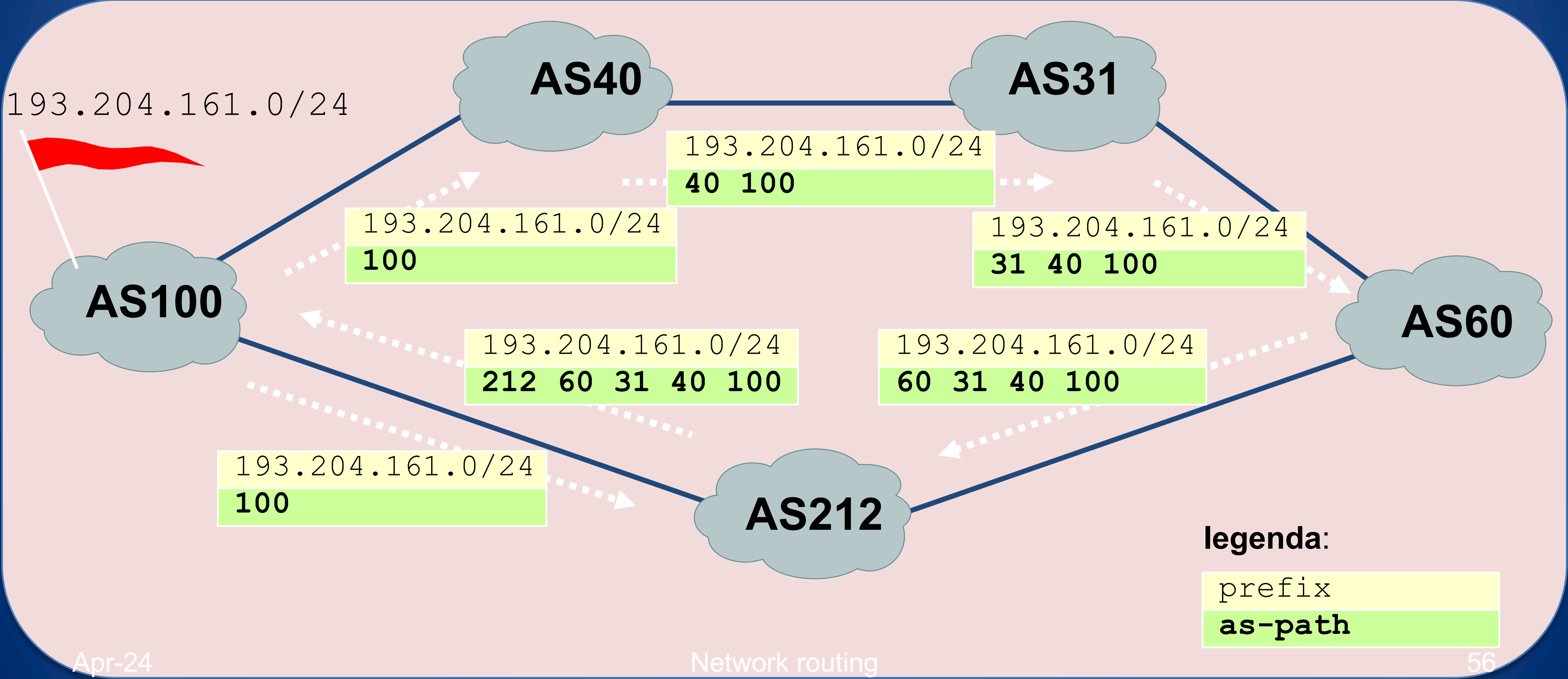
- BGP allows a router to offer connectivity to another router
- “offering connectivity” means “promising the delivery to a specific destination”


BGP announcement

195.11.14.0/24

ip traffic
(to be delivered to 195.11.14.0/24)

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/

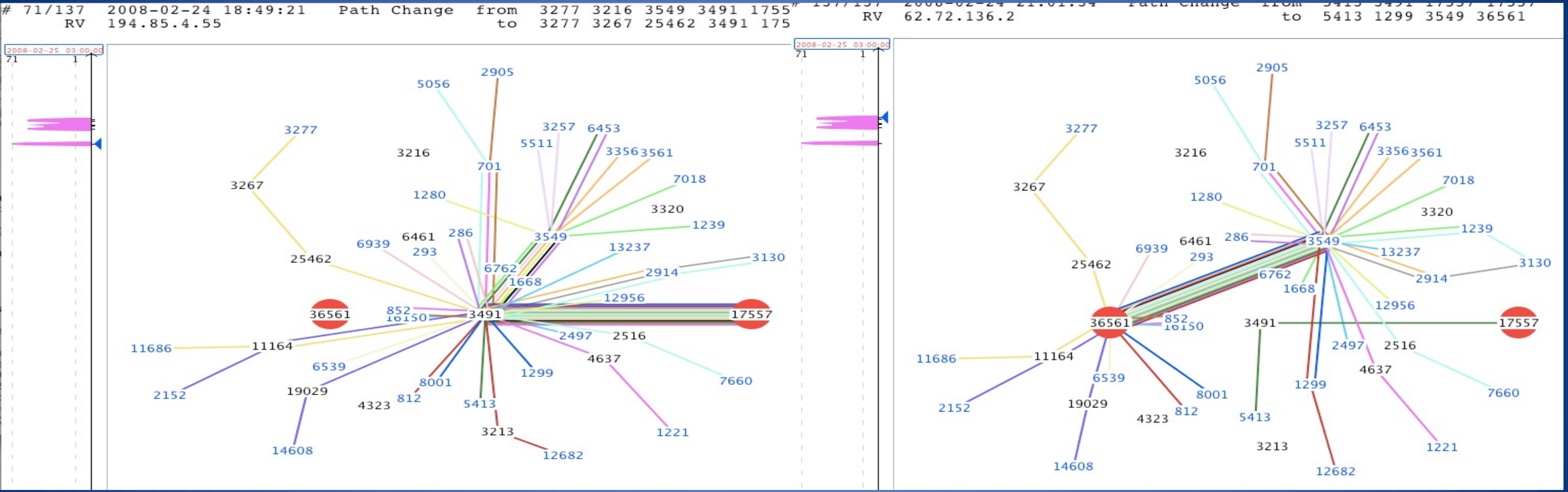
BGP Vulnerabilities

- 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



```
# 71/137    2008-02-24 18:49:21    Path Change   from   3277 3216 3549 3491 1755
       RV   194.85.4.55                            to   3277 3267 25462 3491 175
```

```
137/137   2008-02-24 21:01:34    Path Change   from   5413 3491 17557 17557
     RV   62.72.136.2                            to   5413 1299 3549 36561
```

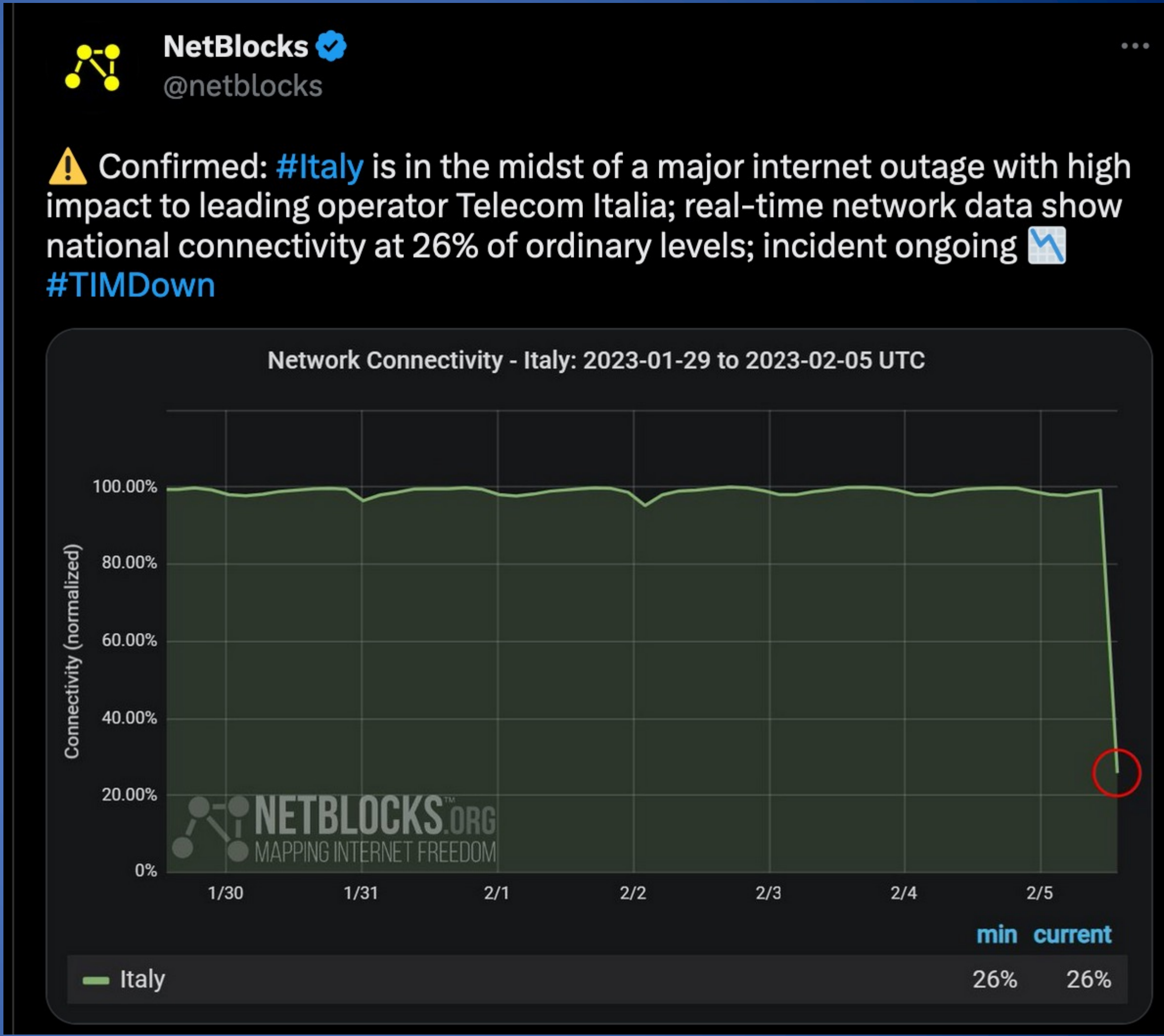
AS 17557 Pakistan, AS 36561 Youtube

[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



NetBlocks ✓
@netblocks

⚠ Confirmed: #Italy is in the midst of a major internet outage with high impact to leading operator Telecom Italia; real-time network data show national connectivity at 26% of ordinary levels; incident ongoing 📉
#TIMDown

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