

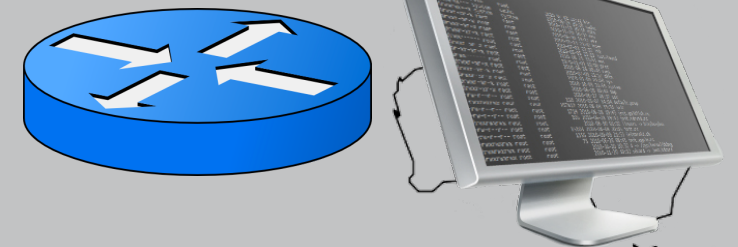
---

# SECURITY (COMP0141): NETWORK SECURITY, PART II



# STEP 2: REQUEST CONTENT

`http://me.bob.com/hi.html`  
`69.64.155.174`



`me.bob.com`

# LEASED LINES

---



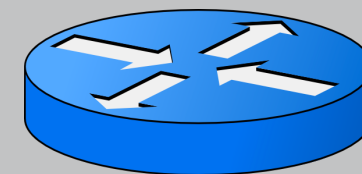
`http://me.bob.com/hi.html`  
`69.64.155.174`

Pros?

- incredibly fast
- reliable
- secure

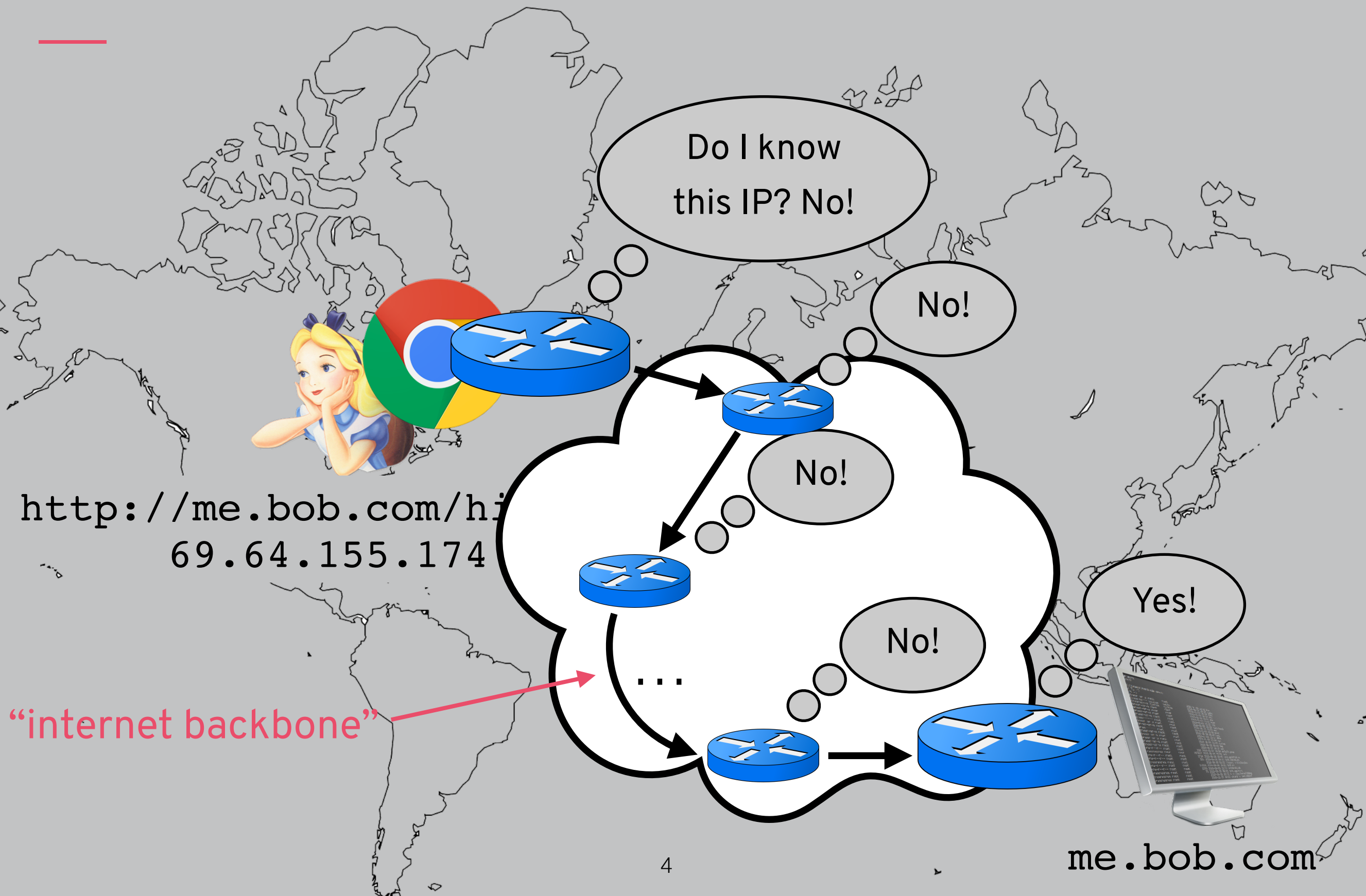
Cons?

- incredibly expensive!



`me.bob.com`

# INTERNET BACKBONE



# ROUTING FAQs

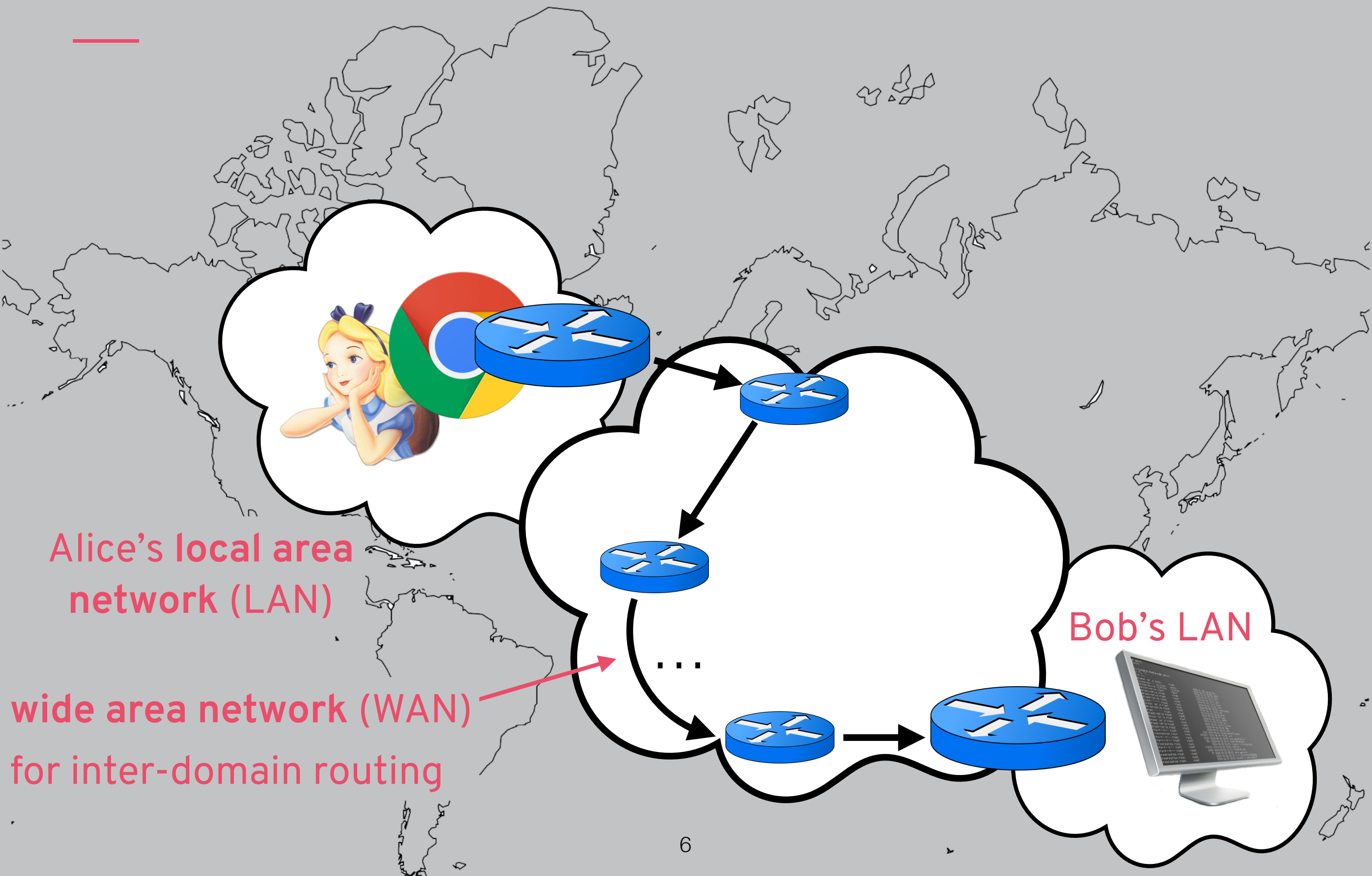
---

## FAQs

**q:** how does your router pick another router to ask?

**a:** we'll see later! autonomous systems (ASes), BGP, etc.

# LAN VS. WAN

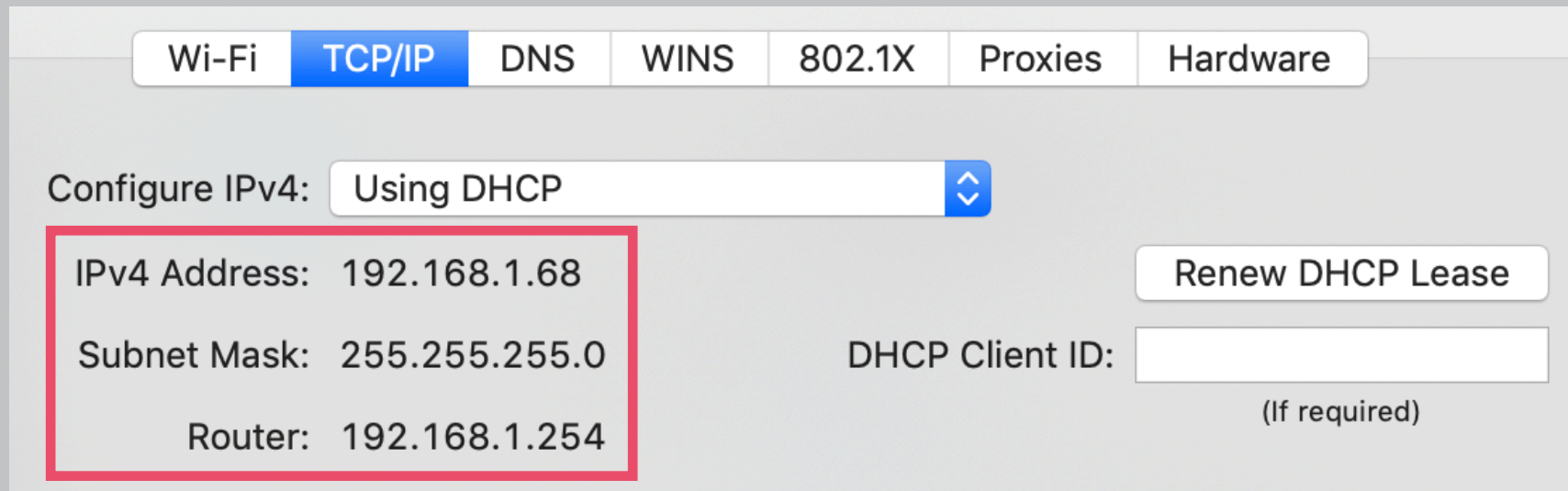




# ROUTING

To send a packet, Alice starts with:

- her IP address
- Bob's IP address
- **subnet mask** (255.255.255.0)
- **gateway/router** (192.168.1.254)



The screenshot shows a network configuration window with tabs for Wi-Fi, TCP/IP, DNS, WINS, 802.1X, Proxies, and Hardware. The TCP/IP tab is selected. Under 'Configure IPv4', the dropdown menu is set to 'Using DHCP'. A red rectangular box highlights the following information: IPv4 Address: 192.168.1.68, Subnet Mask: 255.255.255.0, and Router: 192.168.1.254. To the right of this box is a 'Renew DHCP Lease' button. Below the box, the 'DHCP Client ID' field is empty, with the text '(If required)' below it.

Tab	Configure IPv4	IPv4 Address	Subnet Mask	Router	DHCP Client ID	Action
Wi-Fi						
TCP/IP	Using DHCP	192.168.1.68	255.255.255.0	192.168.1.254		Renew DHCP Lease
DNS						
WINS						
802.1X						
Proxies						
Hardware						

# SUBNET

---

	Binary form	Dot-decimal notation
IP address	11000000.00000000.00000010.10000010	192.0.2.130
Subnet mask	11111111.11111111.11111111.00000000	255.255.255.0
Network prefix	11000000.00000000.00000010.00000000	192.0.2.0
Host identifier	00000000.00000000.00000000.10000010	0.0.0.130

IP address AND subnet mask = routing prefix (192.0.2.0/24 in **CIDR notation**)

IP address AND comp(subnet mask) = host identifier



# ROUTING

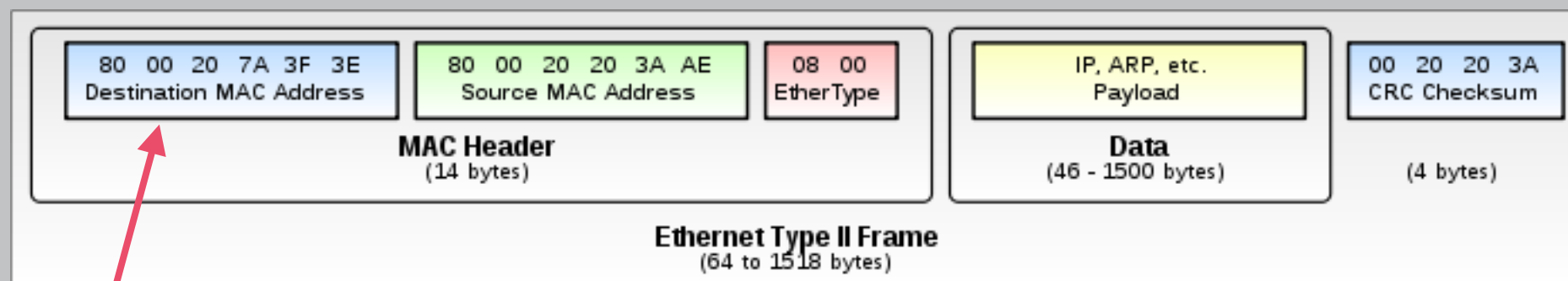
To send a packet, Alice starts with:

- her IP address
- Bob's IP address
- **subnet mask (255.255.255.0)**
- **gateway/router (192.168.1.254)**

If Bob is on the same subnet, route through **LAN**

If not, send to gateway (router) and route through **WAN**

Create IP packet and use **ARP** to create link-layer data frame

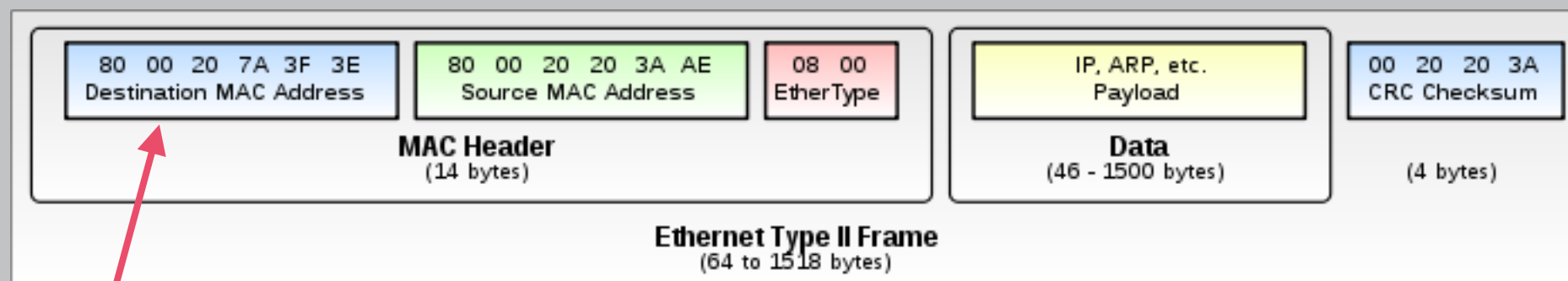


need Bob's MAC address, not IP address

# ADDRESS RESOLUTION PROTOCOL

Address resolution protocol (**ARP**) queries hosts on local network to get MAC address for an IP address

What guarantees the integrity of the MAC address? **Nothing!**



need Bob's MAC address, not IP address

# ARP SPOOFING/POISONING

---

ARP messages are broadcast and anyone can reply, so anyone can impersonate anyone else

Solutions:

- Fixed ARP tables (impractical)
- Port binding on switch
- Higher-level host authentication (e.g., TLS)

Same type of problem as with DNS! Address translation is always tricky

**That time change of address really worked: A Chicago man redirects all of UPS's mail to his one-bedroom apartment**

# ROUTING

---

To send a packet, Alice starts with:

- her IP address
- Bob's IP address
- **subnet mask (255.255.255.0)**
- **gateway/router (192.168.1.254)**

If Bob is on the same subnet, route through LAN

If not, send to gateway (router) and route through WAN

Create IP packet and use **ARP** to create link-layer data frame

Gateway (router) forwards packet to **another router**

\_\_\_\_\_

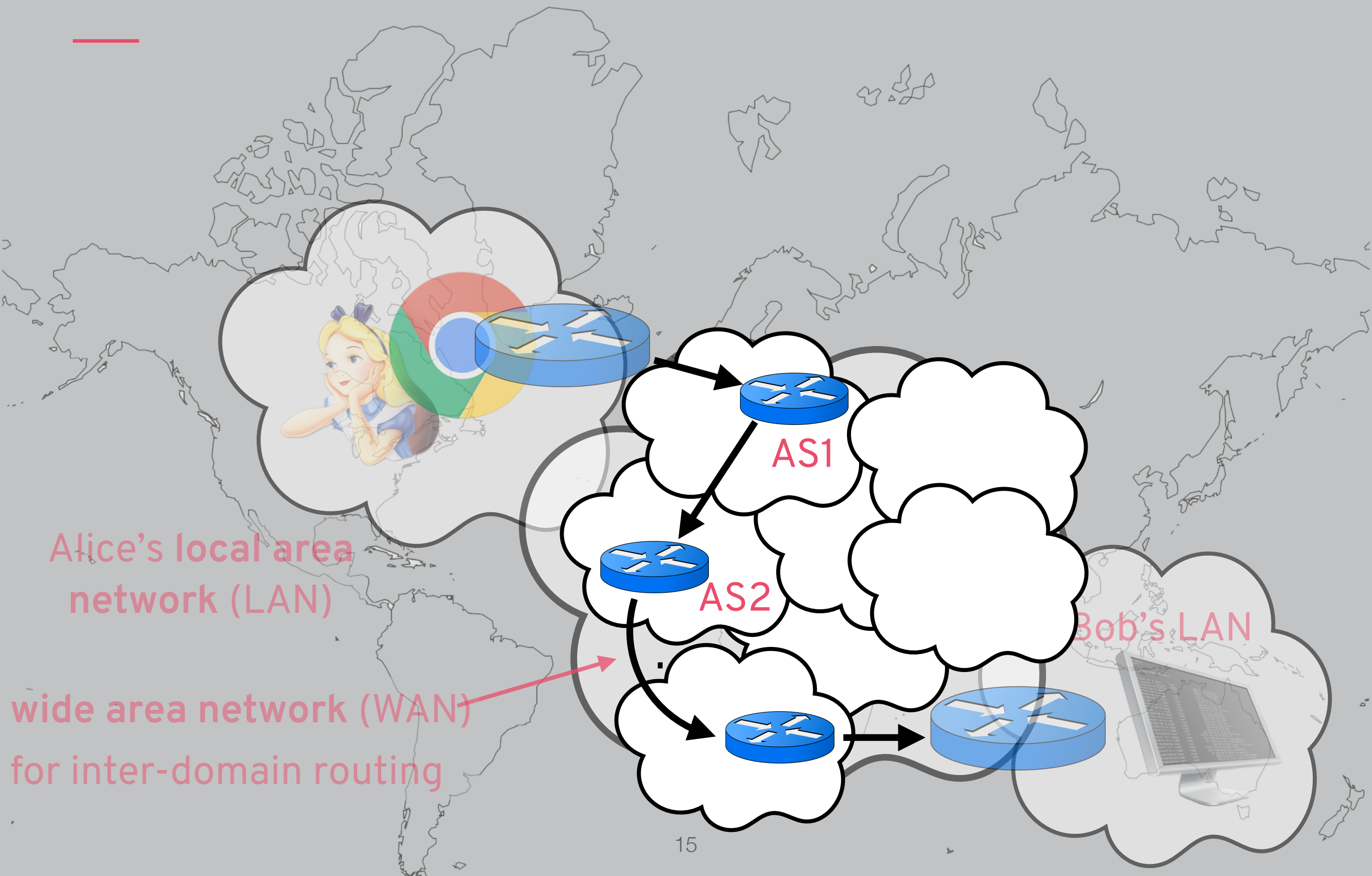


# AUTONOMOUS SYSTEMS

---

Every Internet domain connected to at least two others is an **Autonomous System (AS)** that controls some IP blocks/subnets

# INTERNET BACKBONE





# BORDER GATEWAY PROTOCOL

---

Every Internet domain connected to at least two others is an **Autonomous System (AS)** that controls some IP blocks/subnets

Border Gateway Protocol (**BGP**) is used to manage IP routing between different ASes

Neighbours share information according to **routing tables**

- destination subnet  $\mapsto$  (next IP, cost)

Routes change (due to faults, new cables, etc.) so BGP has to constantly and quickly update those routes

**Cost is important:** the routes with lowest cost are the ones that are chosen (save real money)

# BGP SECURITY

---

Authentication between routers:

- Shared secret (up to 80 bytes of ASCII)
- Ad-hoc MAC with each message, based on MD5
- This is very weak!

What guarantees the integrity of the advertised routes? **Nothing!**

# BGP SPOOFING

---

Adversary controls or compromises router somewhere

- Inject false low-cost routes to redirect traffic to themselves
- The routing information propagates and stays in routing tables until it expires

This means traffic in targeted networks is redirected to malicious networks, so adversary can carry out surveillance, injection, censorship, etc.

Worse than address translation (DNS and ARP spoofing) because there is no authority on the optimality of routes

# EXAMPLES OF BGP SPOOFING

In February 2013, global traffic was redirected to Belarusian ISP GlobalOneBel (report by Renesys)



Set of victim networks changed daily and include major financial institutions, governments, and network service providers in US, South Korea, Germany, Czech Republic, Lithuania, Libya, Iran

# EXAMPLES OF BGP SPOOFING

---

In February 2008, Pakistan hijacked global YouTube traffic in an attempt to block YouTube within the country [1]

- Pakistan Telecom used BGP hijacking to claim IP block belonging to YouTube
- BGP nodes forwarded this routing information

In April 2018, attackers stole \$100K+ worth of Ethereum [2]

- Used BGP hijacking to claim chunk of Amazon DNS addresses
- Used hijacked DNS traffic to direct people looking for `MyEtherWallet.com` to malicious servers in Russia
- Used login/key data to steal cryptocurrency from users

[1] <https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>

[2] <https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/>

# SOLUTIONS TO BGP SPOOFING

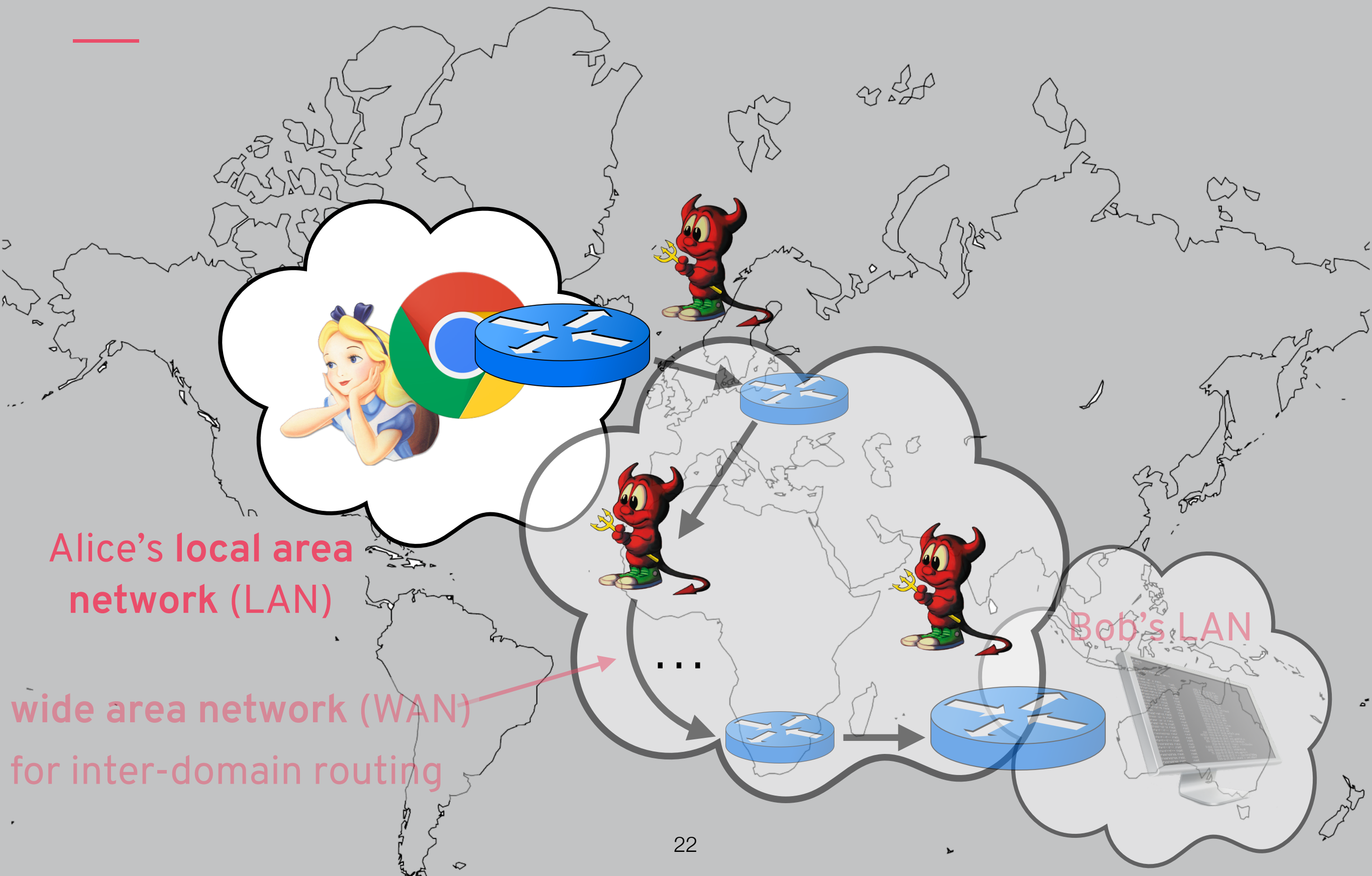
---

Filtering helps (some routes should not come from some routers)

## BGPSec:

- Each AS has a certificate that links signing keys to IP blocks
- Updates accepted as genuine only if they are signed by the authority for the AS/IP block
- AS can delegate authority to advertise routes to other ASes
- Nice idea but... effort started in 2003 and still not deployed

# NETWORK PERIMETERS





# NETWORK DEFENSES

---

**Firewalls** filter or limit network traffic from outside

**Network address translation (NAT)** shares IP addresses

**Network intrusion detection (NIDS)** looks at network traffic

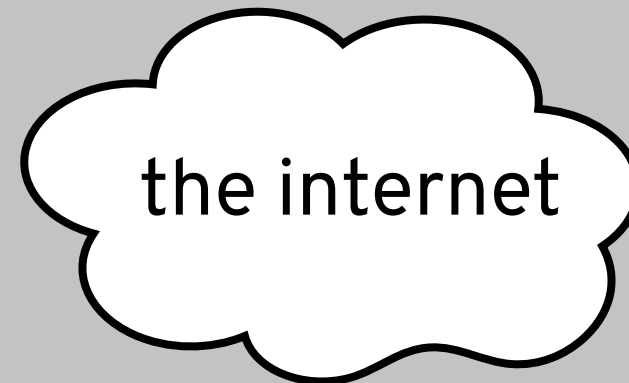
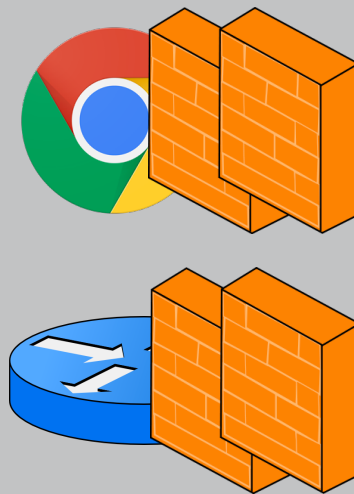
# FIREWALLS

---

**Firewalls** filter or limit network traffic from outside

This can be done by providing **filtering** at the level of:

- individual user applications
- the network



Filtering can be applied based on packets, ports, etc.

There are also **proxy-based** firewalls in which local server connects to a web proxy (proxy can provide other services too)

# DESIGN PRINCIPLES

---

**Least privilege**

Separation of responsibilities

**Complete mediation**

**Fail-safe default**

Defence in depth

**Open design**

**Psychological acceptability**

**Economy of mechanisms**

# NETWORK DEFENSES

---

**Firewalls** filter or limit network traffic from outside

- **Pros:** satisfy many security principles, filter out “noise”
- **Cons:** costly, false sense of security (doesn't help with malware or many other threats)

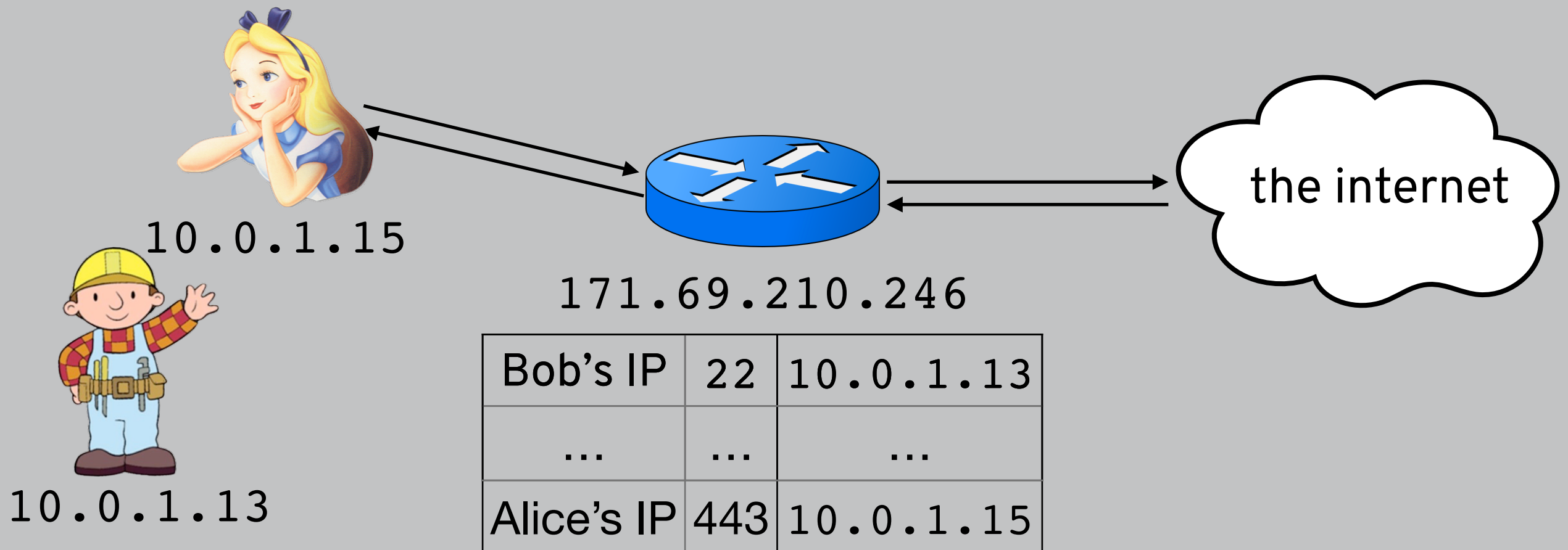
**Network address translation (NAT)** shares IP addresses

**Network intrusion detection (NIDS)** looks at network traffic

# NETWORK ADDRESS TRANSLATION

**Network address translation (NAT)** shares IP addresses

This can be done by providing a single IP address to the outside world that represents many clients on the local network, then forwarding packets as appropriate



# NETWORK DEFENSES

---

**Firewalls** filter or limit network traffic from outside

- **Pros:** satisfy many security principles, filter out “noise”
- **Cons:** costly, false sense of security (doesn’t help with malware or many other threats)

**Network address translation (NAT)** shares IP addresses

- **Pros:** allow only connections established from inside
- **Cons:** rewriting IP addresses isn’t that easy (what if they appear in protocol data?)

**Network intrusion detection (NIDS)** looks at network traffic

# NETWORK DEFENSES

---

**Network intrusion detection (NIDS)** looks at network traffic

Many reasons to try to do this:

- Find signatures of malware or other attacks
- Perform spam filtering
- Data leakage (prevent sensitive information from leaving)
- Filter out or slow down BitTorrent traffic



# NETWORK DEFENSES

---

**Firewalls** filter or limit network traffic from outside

- **Pros:** satisfy many security principles, filter out “noise”
- **Cons:** costly, false sense of security (doesn’t help with malware or many other threats)

**Network address translation (NAT)** shares IP addresses

- **Pros:** allow only connections established from inside
- **Cons:** rewriting IP addresses isn’t that easy (what if they appear in protocol data?)

**Network intrusion detection (NIDS)** looks at network traffic

- **Pros:** can address a wide variety of misbehaviour
- **Cons:** tricky to get right, expensive, doesn’t work for HTTPS

# SUMMARY OF SECURITY ISSUES

---

**Naming security:** the association between lower-level names and higher-level names should not be influenced by the adversary

- DNS (cache) poisoning
- ARP spoofing/poisoning

**Routing security:** the route over the network and the delivery of messages should not be influenced by the adversary

- BGP spoofing
- IP spoofing  $\Rightarrow$  SYN flood

**Session security:** the association between messages and sessions should not be tampered with

- TCP hijacking

# QUIZ!

---

Please go to

`https://moodle.ucl.ac.uk/mod/quiz/view.php?id=2867680`

to take this week's quiz!