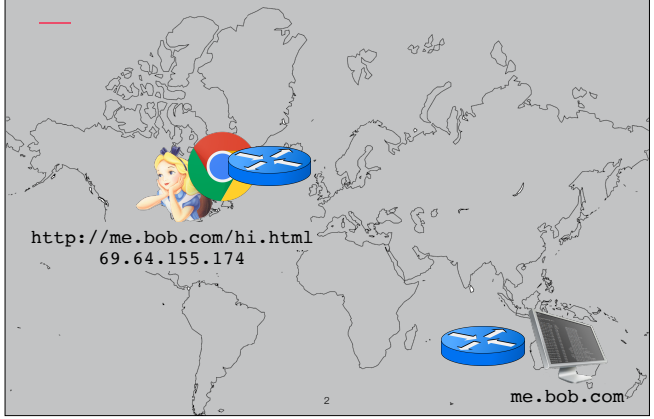
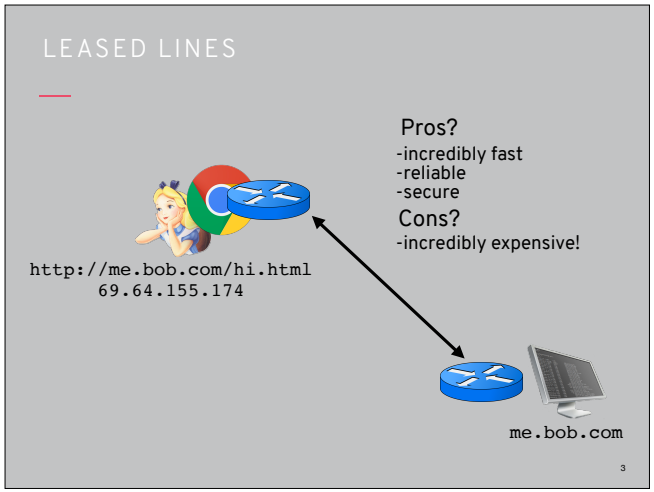
SECURITY (COMP0141): NETWORK SECURITY, PART II

UCL

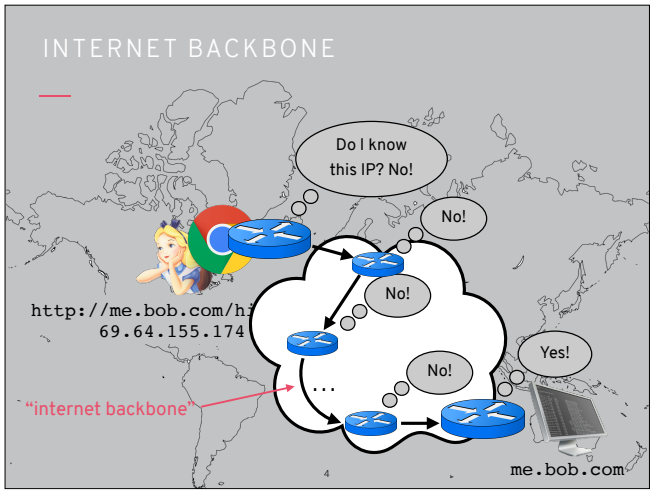
STEP 2: REQUEST CONTENT



So routing is really the IP layer



Remember from Week 2 that in terms of routing there were two approaches: leased lines (direct connection)…



…or what we called the “Internet backbone”

ROUTING FAQS

FAQs

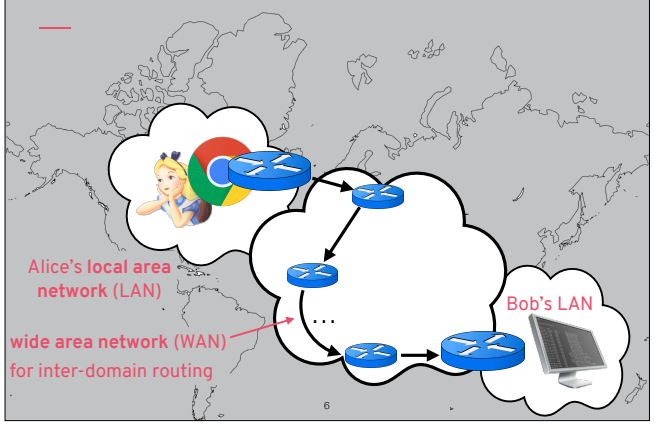
q: how does your router pick another router to ask?

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

I even said then that we'd learn more about routing later, and conveniently now it's later and that's what we're going to do

---

LAN VS. WAN

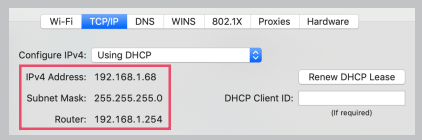


So really, what I described as a leased line can be thought of as a local area network, or LAN (be careful though, these two are actually different things), and this "internet backbone" is a wide area network, or WAN

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)



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

The subnet identifies which part of the broader network you're on, in terms of the prefix (whereas the host identifier is your position within that subnet)

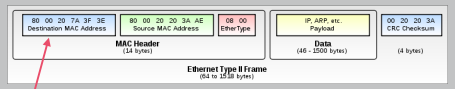
ROUTING

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

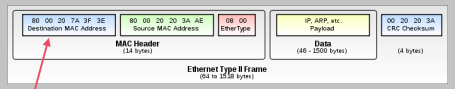
If the subnet is the same, you can use LAN, but otherwise need to use WAN. When Alice forms her packet, what she needs to send to the router is an Ethernet data frame, but this is at a lower level of abstraction so she needs Bob's MAC address (also known as a network address, see https://en.wikipedia.org/wiki/MAC_address) rather than just his 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

This is another type of translation service: Alice goes and asks people if they know the MAC address for this IP address (similar to asking for IP address for a domain name in DNS)

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

Just like in DNS, anyone can respond with any answer, so there is no integrity. There are some mitigations but ultimately this type of address translation is just a difficult problem

ROUTING

To send a packet, Alice starts with:

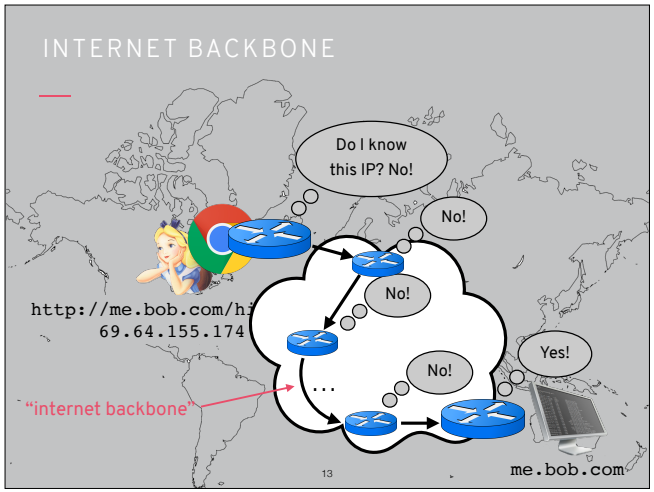
- her IP address
- Bob's IP address
- **subnet mask** (255.255.255.0)
- **gateway/router** (192.168.1.254)

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

Going back to routing, once the router has the necessary information they start talking to other routers to get the packet where it needs to go



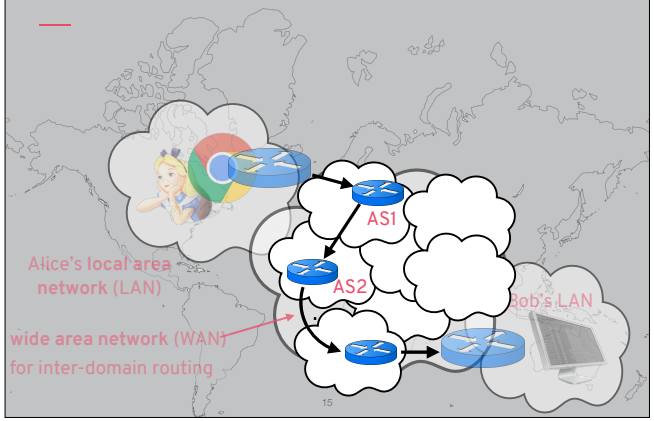
Before I said that routers do this by asking their “friends” but sadly routers don’t actually have friends. So how do they know who to ask?

AUTONOMOUS SYSTEMS

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

14

INTERNET BACKBONE



15

Really this whole internet backbone can be thought of as a collection of large ASes, which are mostly run by large telecoms and other companies

---

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 ↦ (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)

16

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!

Routers can prove that they're the router they claim to be, meaning no MitM – although crypto here is very weak since 80 bits is small and MD5 is fairly broken

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

The story is the same as for DNS and ARP: nothing prevents an adversary from lying about routes. Because the internet is distributed/decentralised though, there is no authority on which routes are best (unlike in address translation where there is a globally correct answer), so this is even harder to deal with

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/

This is a very real and common problem

SOLUTIONS TO BGP SPOOFING

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

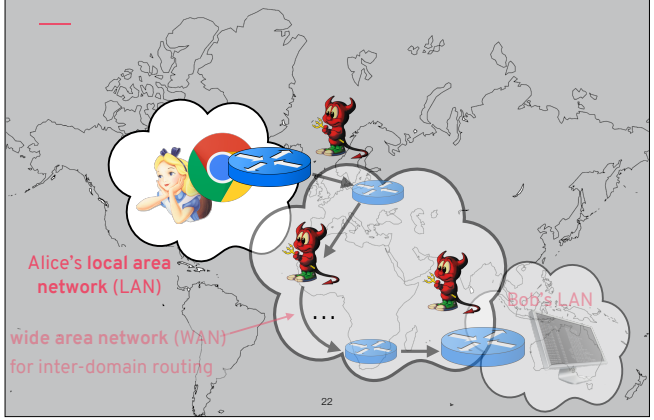
BGPSec:

- 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

BGPSec is similar (or worse) story to DNSSEC, need people to deploy it and that hasn't happened yet

---

NETWORK PERIMETERS



The final thing we'll talk about is: the Internet is clearly full of many adversaries, lying about all sorts of things and trying to infect you with malware and whatever else. What does Alice do to protect her local network from these adversaries lurking in the broader Internet?

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

We'll talk briefly about firewalls, NAT, and NIDS

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)

Firewalls are likely familiar to you, and involve filtering packets from "bad" places (e.g., if the firewall is configured to blacklist a certain site/country/subnet than it filters out packets from that site/country/subnet)

DESIGN PRINCIPLES

Least privilege
Separation of responsibilities
Complete mediation
Fail-safe default
Defence in depth
Open design
Psychological acceptability
Economy of mechanisms

25

Firewalls exhibit a lot of the security principles

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

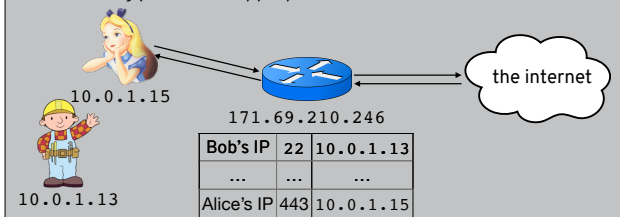
26

On the other hand they may provide a false sense of security because they don't actually prevent many threats

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



Bob's IP	22	10.0.1.13
...	...	...
Alice's IP	443	10.0.1.15

External users only see IP address and port of the NAT

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

NAT is good at protecting people inside network, can't connect to them directly unless they talk to you first

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

NIDS varies a lot depending on the goal, what are you trying to achieve for your network?

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

NIDS can be very powerful but is difficult to do

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 ⇒ SYN flood

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

- TCP hijacking

This was a very fast overview of this topic and ultimately if you want to know more you should take Networked Systems next year!

QUIZ!

Please go to

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

to take this week's quiz!