Today

What stands between you and your request?

- hubs and switches
- routers and gateways
- proxies
- firewalls
- TLS interception equipment

Hubs and switches

OSI layer?

Purpose?

Difference?

***Monitor* port**

#	Name	Example
7	Application	HTTP, DNS, NFS, SSH...
6	Presentation	TLS, SSH...
5	Session	SOCKS, SMB...
4	Transport	TCP, UDP, SCTP...
3	Network	IP
2	Data link	Ethernet MAC
1	Physical	Ethernet PHY

Historically, Ethernet hubs broadcast whatever they received on one port to all other ports, leading to quite a bit of contention, whereas switches could learn over time which MAC addresses were attached to which ports and thus be more selective in how they transmit traffic. These days, "managed" switches can do a lot more, too.

Since a switch doesn't repeat all traffic everywhere, many managed switches will allow you to configure a *monitor* port that _____ _____. This is very useful for network admins when they need to troubleshoot issues, but of course it could allow anyone plugged into it to become a very effective eavesdropper!

Routers

Purpose?

OSI layer?

#	Name	Example
7	Application	HTTP, DNS, NFS, SSH...
6	Presentation	TLS, SSH...
5	Session	SOCKS, SMB...
4	Transport	TCP, UDP, SCTP...
3	Network	IP
2	Data link	Ethernet MAC
1	Physical	Ethernet PHY

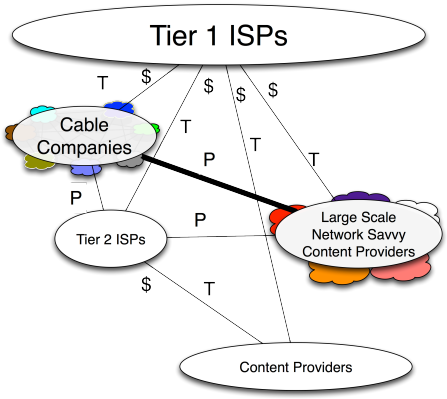
Local area network (LAN) names are only meaningful within the same LAN. So, my wireless Ethernet MAC address (`48:45:20:d3:16:f7`) isn't much good to you when you're trying to communicate with me from another network (on campus, at home, etc.). A router helps with this problem by routing packets from one local network (e.g., a wired Ethernet LAN) to another (e.g., a wireless Ethernet LAN). This is why you'll sometimes see a router labeled with LAN ports and a "WAN port": WAN stands for _____.

A router that routes between local networks exists at Layer 3: the Network layer. Your home "router" that you got from Bell, Rogers (hopefully not?), etc., may also contain things that aren't strictly a router, like a wired _____ (layer 2), a wireless _____ (layer 2) or a _____ (layer 2/3).

The Internet

What is the Internet?

- "a network of networks"
- connected at *Internet Exchanges*
- ... all over the world
- ... with *internet service providers* (ISPs) of varying "tiers"



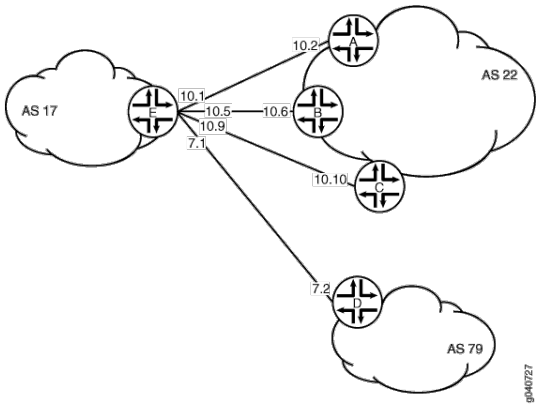
Source: Dr Peering

BGP: Border Gateway Protocol

Autonomous systems

- co-located in IXPs
- *peering* agreements reflected in *routing tables*
- routes advertised by BGP

Remember Dijkstra?



Source: Juniper Networks

Peering agreements can be considered confidential because they may contain _____. This can include _____ and _____, which could be valuable information for a competitor AS!

Internet routing is the quintessential application of Dijkstra's algorithm, as it's about finding short paths from A to B.

BGP weaknesses

- "I, AS 1234, can route traffic to 134.153.0.0/16 in 1 hop"
- routers prefer short paths and long prefixes

BGP *hijacking*

- 2008 Youtube Hijack*
- post-Obama/Xi BGP advertisements by China Telecom†

---

* RIPE NCC, "YouTube Hijacking: A RIPE NCC RIS case study", *RIPE NCC News: Industry Developments*, 2008.

† Demchak and Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking," *Military Cyber Affairs* 3(1), 2018. DOI: 10.5038/2378-0789.3.1.1050

In 2008, the government of Pakistan decided to block its citizens from being able to access YouTube. However, the mechanism by which they chose to block YouTube caused some unindented side effects: their BGP hijacking of YouTube's address space caused the *entire world's YouTube traffic* to be directed through serverse of Pakistan Telecom. YouTube fixed the issue within 80 minutes of the problem starting via a BGP announcement of their own, but for those 80 minutes the world stood still...

In 2015, right after the Presidents of the US and China agreed that they really shouldn't hack each other's companies, China Telecom started advertising some Internet traffic routes that were... surprising. Apparently the new accord didn't cover Internet routing, because suddenly all of the traffic between Canada and South Korea, or between the US and Italy, or a bunch of other funny combinations, started to flow through China Telecom. Accident? Deliberate hijacking? I wouldn't care to speculate (in writing).

Securing routing

RPKI (Route PKI)

BGPsec*

Difficult to get everyone to move together!†

---

* Lychev, Goldberg and Schapira, "BGP Security in Partial Deployment: Is the Juice Worth the Squeeze?", in *SIGCOMM '13: Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, 2013. DOI: 10.1145/2534169.2486010

† Goldberg, "Why is it taking so long to secure Internet routing?", *ACM Queue* 12(8), 2014. DOI: 10.1145/2668152.2668966

RPKI and BGPsec work differently, with RPKI allowing signature-based validation of prefix announcements ("do you really own this prefix?") and BGPsec providing validation of entire routing paths. There are serious pros and cons to both, and as is often the case, the "right" answer (BGPsec) doesn't work well unless everybody starts using it. Collective action problems are hard.

Gateways

Boundaries between networks

Places for control, policy enforcement

```
sysctl net.inet.ip.forwarding=1      # FreeBSD
sysctl net.ipv4.ip_forward=1         # Linux
```


The term "gateway" is a bit looser than some of our other terms:

- routers typically act as gateways
- "gateway" can also be used to refer to a modem (a point-to-point device) + a router

Firewalls

In cars: a physical object

An automative firewall

In computing?

- logical "wall" between networks
- can be a physical device!

Firewall applicances

Software firewalls

Implemented in OS kernels

- sequence of *rules* that can be *matched*:

```
# Default rules: block incoming, allow outgoing
block in on em0
pass out all keep state

# Allow SSH
pass inet proto tcp from any to any port ssh

# TODO: disable this again AS SOON as the 8894/9875 lab is done!
#pass inet proto tcp from any to any port telnet
```

Linux firewalls

```
iptables -A OUTPUT -p tcp -d 31.0.0.0/8 -j DROP
iptables -A INPUT -p icmp -i eth0 -j DROP
iptables -L -n -v
```

```
Chain INPUT (policy DROP 544 packets, 87564 bytes)
 pkts bytes target     prot opt in     out     source               des
  101  8362 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0
   46  5733 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0

Chain OUTPUT (policy ACCEPT 535 packets, 46301 bytes)
 pkts bytes target     prot opt in     out     source               des
  203  174K DROP       tcp  --  *      *       0.0.0.0/0            31.
```

... and onward to nftables?

BSD firewalls

IPFW

PF (packet filter)

PF example

```
# Redirect jailed DNS requests to local (caching) resolver.
rdr log (all) inet proto udp to $jail_ifs port domain -> lo0

# NAT jails and machines on the internal network.
nat pass log (all) on $ext_if from $jail_ifs to any -> $ext_if
nat pass on $ext_if from $internal_net to any -> $ext_if


# Default rules: block incoming traffic, allow outgoing and internal ne
pass in log (all) on $jail_ifs
pass in on $internal_if
pass out all keep state

pass proto udp from $local port domain
pass inet proto tcp from any to any port ssh
pass in on $ext_if proto tcp from any to any port {http,https}
```

NAT

Network address translation

```
nat pass on $ext_if from $internal_net to any -> $ext_if
```

```
iptables -t nat -A POSTROUTING -o $external -j MASQUERADE
```

Helps with IP scarcity

Hides internal IPs ... does that help security?

In most networks you connect to, you'll see that your computer has an address like 192.168.1.1 or 10.0.0.1. These are example of _____ _____ that have been designated by IANA as only usable on local networks, *not* for routing over the Internet (see RFC 1918). So what's the good of an IP address that you can't route to?

Answer: _____. For one thing, nothing says that a NAT has to restrict incoming traffic. NAT shouldn't be thought of primarily as a security mechanism, but then again, nobody said that you *have* to give your network topology information to your adversaries!

Proxies

Can be pure data caching

- Squid, vagrant
- Netflix!

Integrity questions

```
<script src="...min.js" integrity="sha384-vtXRMe3mGCbOeY7l30aIg8H9
```


How can we know whether the content that we received from a proxy is the same as the original content? For some content, we may not be able to. For things like software packages and software updates, we should rely on techniques like _____ rather than trusting the proxy.

For things like proxied JavaScript libraries, we have the ability to specify in an HTML `script` tag that a fetched JS file ought to hash to a specific value.

DMZ

For *demilitarized zone*

- not really in, not really out
- computers reachable from both inside and outside your network
- mail servers, Web servers, SSH jump hosts, VPN concentrators...

Source: Rishabh Tatiraju via Wikipedia

DPI: *deep packet inspection*

- what URL are you visiting?
- what keywords are you using?

Dual-use technology:

- protecting corporate network from known malware vectors
- surveilling a population for unapproved/"unpatriotic" sentiment
    - "Great Firewall" may employ as many as 50,000 people*

* "The Great Firewall of China" , *Bloomberg News*, 5 Nov 2018.

"Going dark"

Who talks on the phone any more?

- Harder to do lawful interception / exceptional access
- "Going dark" phrase popularized in US discourse*
- Continuing debate†‡

---

* Savage, "U.S. Tries to Make It Easier to Wiretap the Internet", *The New York Times*, 27 Sep 2010.

† Schneier, "Attorney General William Barr on Encryption Policy", in *Lawfare*, 23 Jul 2019.

‡ Marks and Schaffer, "The Cybersecurity 202: The Justic Department is racking up wins despite encryption concerns", *The Washington Post*, 16 Jun 2021.

Quietly into that goodnight?

> *Rage, rage against the dying of the light*

TLS interception

- Proxy with "trusted" certificate(s)
- Current estimates: 5-10% of all Web requests!*

---

* Durumeric, Ma, Springall et al., "The Security Impact of HTTPS Interception", in *NDSS 2017: Proceedings of the 2017 Network and Distributed System Security Symposium*, 2017. DOI: 10.14722/ndss.2017.23456.

More TLS workarounds

Compelled backdoors

- deliberate insertion of backdoors (e.g., SP800-90 Dual EC PRNG)
- extra protocol participants (e.g., Ghost Protocol)

Compelled key disclosure

- this kind of thing has happened *at least* once*

---

* Poulsen, "Edward Snowden's E-Mail Provider Defied FBI Demands to Turn Over Crypto Keys, Documents Show", *Wired*, 2 Oct 2013.

Summary

What stands between you and your request?

- hubs and switches
- routers and gateways
- proxies
- firewalls
- TLS interception equipment