University of BRISTOL

Computer System- B Security

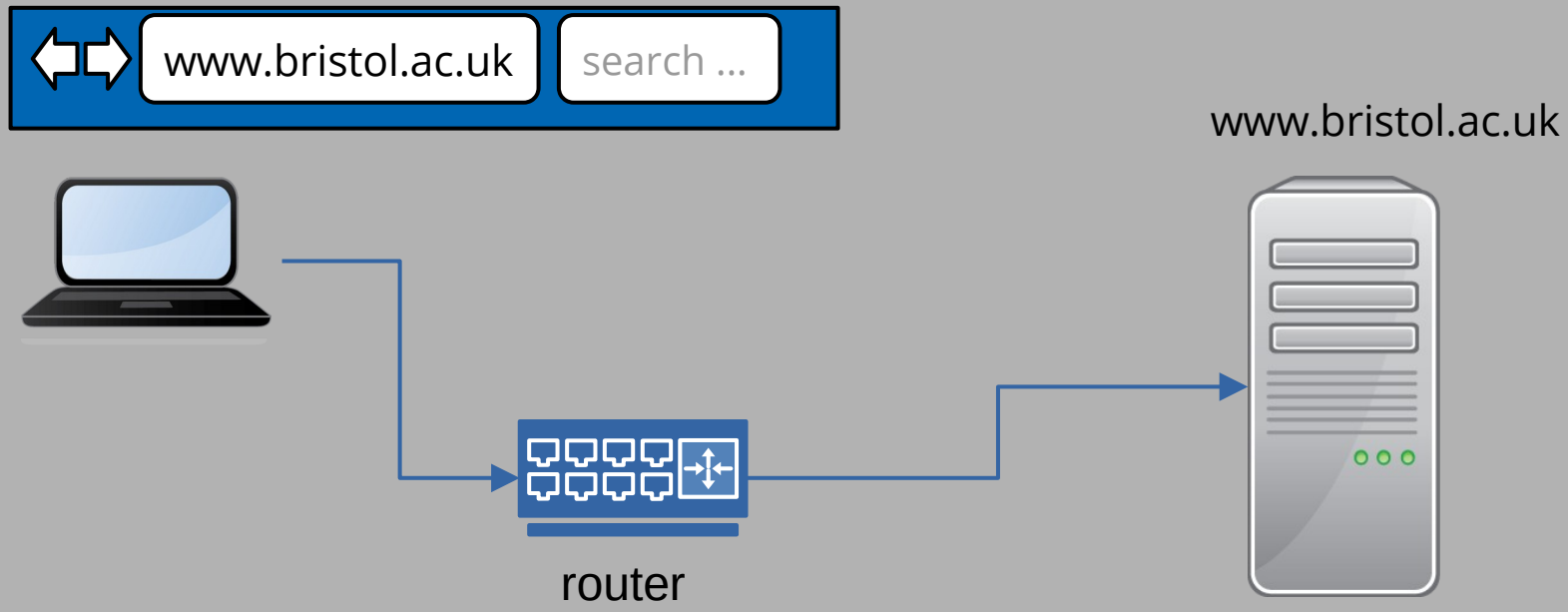
Introduction to Network Security

Networks 2

Sanjay Rawat

bristol.ac.uk

Networks-- Connecting to computers



IP: Routing. “How do you get there from here?”

- As mentioned before, you can only send ethernet packets out of your ethernet interface, and ethernet packets stay on your local network.
- You can put an IP (Network layer) packet inside of an ethernet (data layer) packet, but somebody’s got to pass it along, and that somebody’s a router.
- Every IP number not on your local network will “belong” to your router in your ARP table.
- If you want to talk to someone outside your local network, you’ll send that ethernet packet to your router’s ethernet address and trust that it will work afterwards. It’s out of your hands now. You know what’s “local” or “not” by the subnet mask.

More routing.

- Routers keep tables of networks, often many and often large.
- Routers know: 1- Networks directly connected to them (sometimes one or two, sometimes a hundred or more), 2- Networks connected to their “friends and neighbors” and 3- The “default route” for everything else.
-

It really can’t be a networking class without ping and traceroute

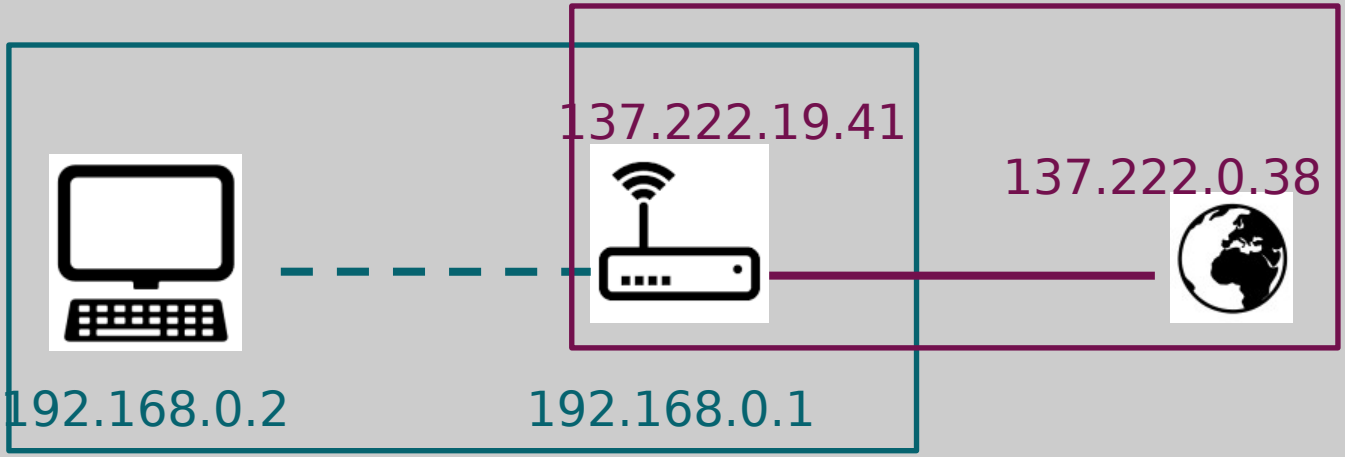
- Ping and Traceroute are two somewhat useful tools for looking at and learning about your network.
- Ping sends a small packet to a host which may or may not choose to reply to it, and times how long the packet takes to get back. Lack of a reply does (not) indicate a problem with the host or network.
- Traceroute asks all routers along the path between you and the destination host if they’d like to respond to you, and times how long each of 3 requests take to get back to you. Some routers may not respond, but may still pass the traceroute packet along, and many hosts will not reply to the traceroute inquiry at all.

IP and NAT

- Recall: computers communicate using **IP addresses** such as 137.222.0.38.
- However
- the world is running out of IPv4 addresses because the allocation system is stupid
- you don’t necessarily want the whole world to be able to reach your computer.

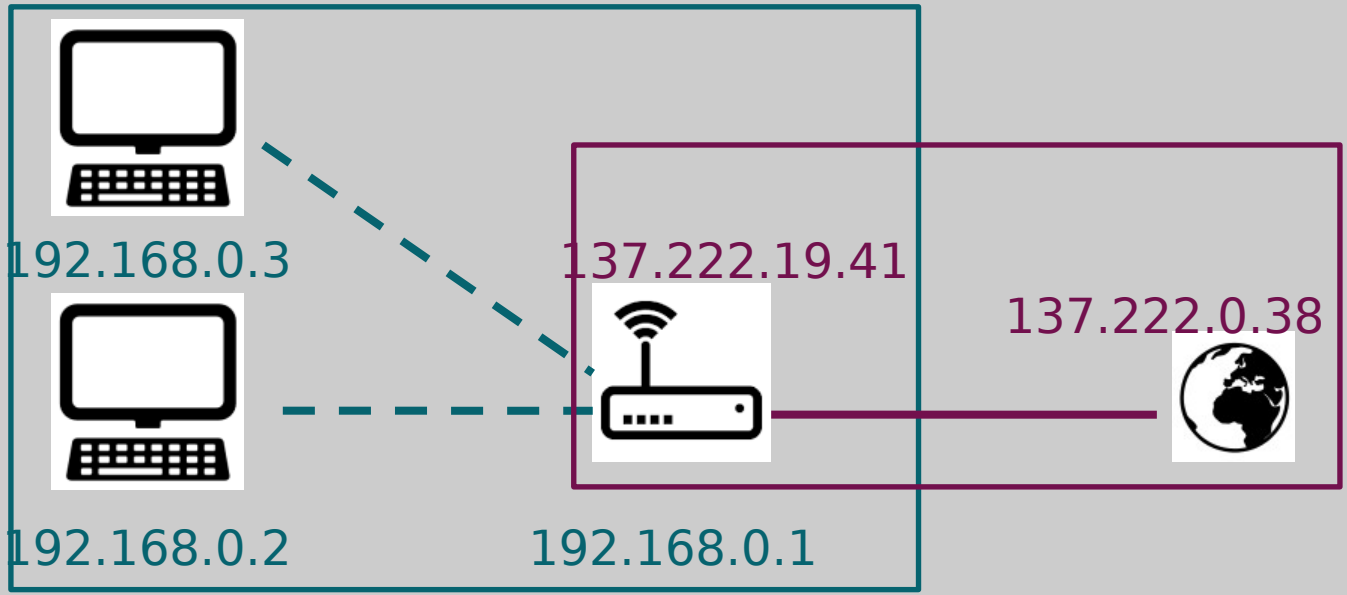
IP and NAT

- Routers (whether wireless or not) can split the network into two components and perform **Network Address Translation (NAT)**.



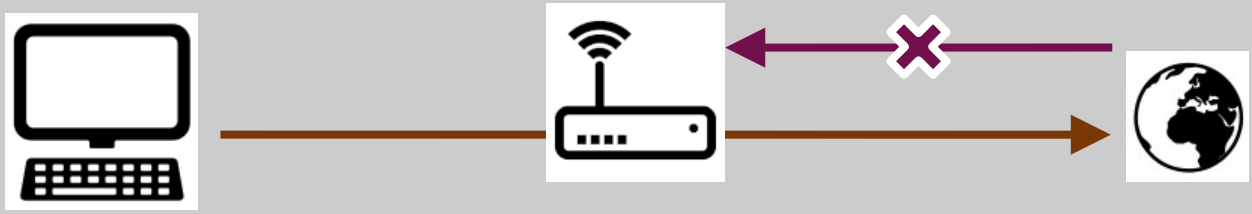
IP and NAT

- Consequence #1 of NAT: you can have several devices behind one NAT with only one external IP address.



IP and NAT

- Consequence #2: although you can initiate connections outbound, the world cannot initiate connections to you – the router wouldn't know which device to forward to.
- (You cannot, without extra set-up, host a server behind a NAT.)



IP and NAT

- Consequence #3: if your router is secure, you are protected from a lot of incoming attacks because they can’t reach your PC in the first place.

- **A NAT automatically does some of the work of a firewall.**

PAT and Port forwarding

Ports

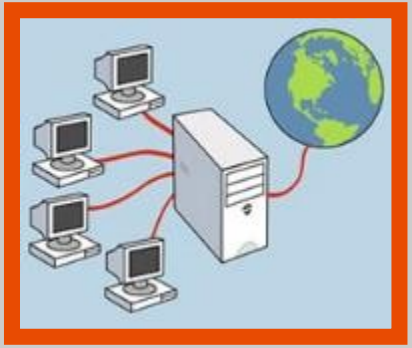
- On the TCP / UDP layer, applications use **ports** to distinguish several applications running on the same machine.
- For example, HTTP (web) is port 80 or 443 (with TLS).

- To connect to another machine, you need an IP address and a port number.
- Port address translation (PAT) is like Nat, but at port level.
  - Same IP but different port numbers to distinguish computers.

Wide Area Network

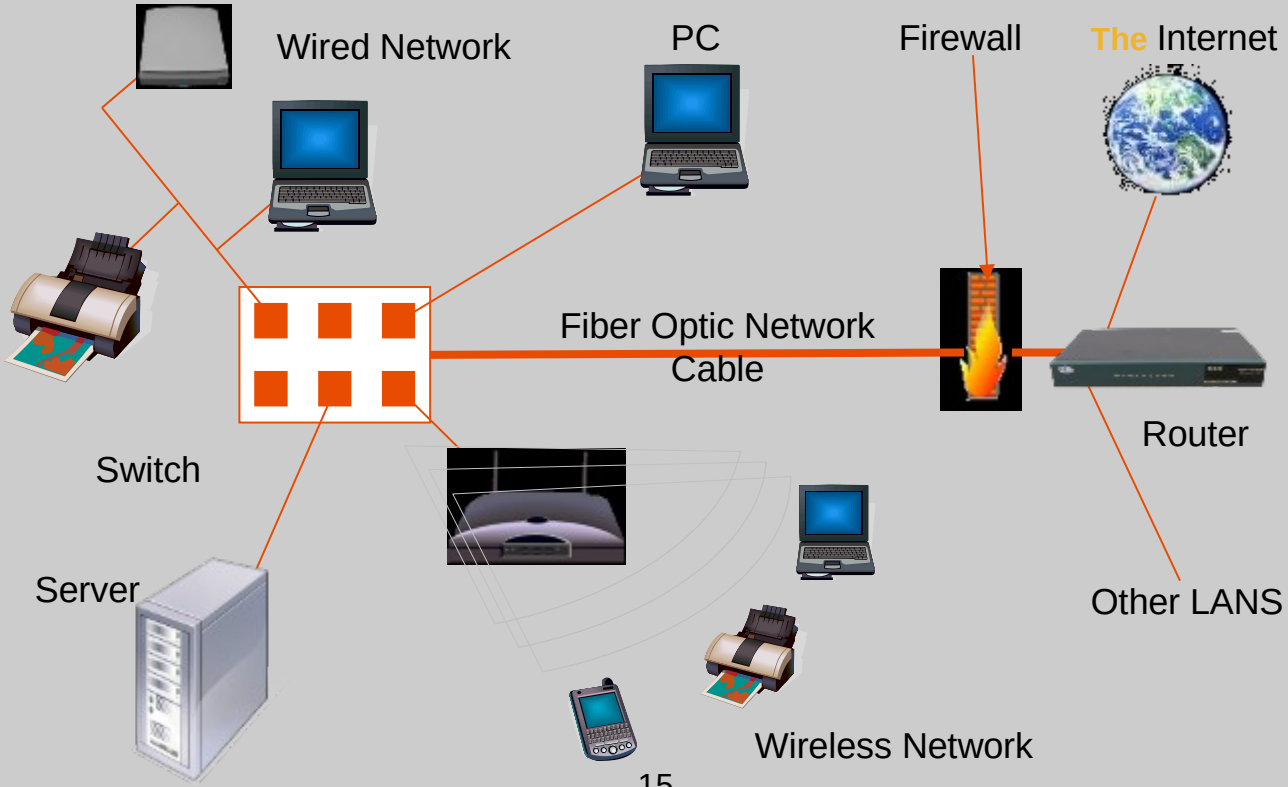
- **A Wide Area Network exist over a large area**
- **Data travels through telephone or cable lines**
- **Usually requires a Modem**
- **The world’s largest Wide Area Network in the Internet**

Local Area Network



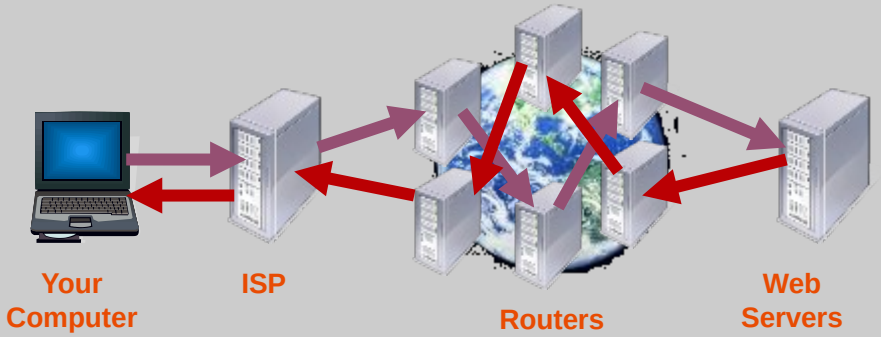
- **A Local Area Network spans a relatively small area**
- **LAN are usually confined to one building or a group of buildings**
- **Data travel between network devices via network cables.**
- **The most common type of Local Area Network is called Ethernet**

The Network Diagram



The Internet

- **How Information Travel Through the Internet**
  - **When you connect to a Web site through an ISP and start exchanging information, there isn't a fixed connection between your computer and the Web server computer hosting the Web site. Instead, information is exchanged using the best possible path at that particular time. Special computers called routers determine these paths, avoiding slow links and favoring fast ones.**

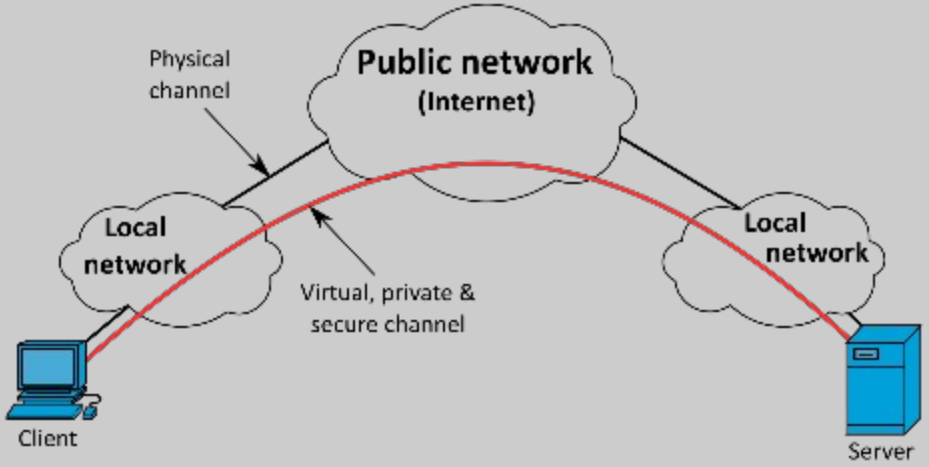


Virtual Private Network (VPN)

- IPv4 is designed without keeping security in mind.
  - Data is sent over public network.
- A **virtual private network** (**VPN**) extends a private network across a public network, by using of cryptographic protocols.

Virtual Private Network (VPN)

- IPv4 is designed without keeping security in mind.
  - Data is sent over public network.
- A **virtual private network** (**VPN**) extends a private network across a public network, by using of cryptographic protocols.



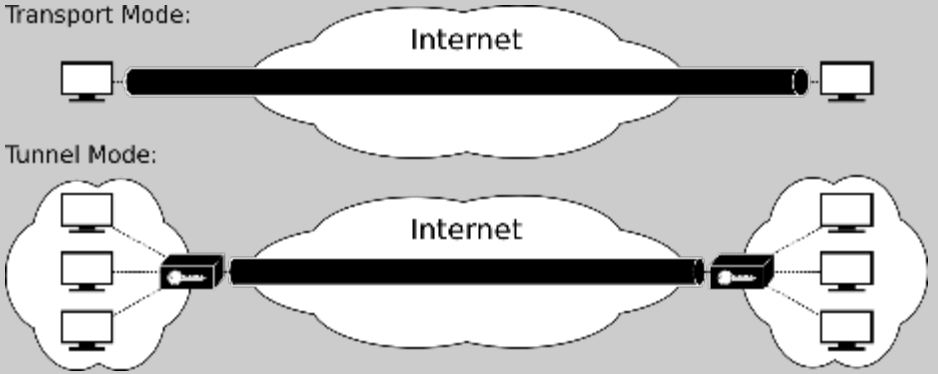
**Taken from https://en.wikipedia.org/wiki/Virtual_private_network

VPN across layers

- Network Layer (2/3)
  - IPSec
    - Transport mode: only the payload of the IP packet is usually encrypted or authenticated.
    - Tunnel mode: the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header.

VPN across layers

- Network Layer (2/3)
  - IPSec
    - Transport mode: only the payload of the IP packet is usually encrypted or authenticated.
    - Tunnel mode: the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header.



** https://en.wikipedia.org/wiki/IPsec

VPN across layers

- Transport layer
  - SSL/TSL
    - Provides encryption and authentication at application layer, which is the most common way to provide CIA security properties over the internet.