School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 171 T1 2023

Ngā whakapūtanga o Te Haumaru rorohiko
Cybersecurity Fundamentals

Networks and the Internet

Learning goals

- What is a network
- What is the internet
- Packet switching
- Addressing
- Ports
- Why is the internet insecure?

PART I:
What is a network?

We use *networks* all the time

- Allow **multiple** users to:
  - **Share** resources
  - **Communicate** electronically
  - **Exchange** files and access **storage**
  - Play **games**
- Historic milestones:
  - 1950s Semi-Automatic Ground Environment (**SAGE**) radar system
  - 1969 first four nodes of **ARPANET**
  - 1977 Xerox PC network
  - 1989 NZ connected to the Internet

Network elements

- **Computers** connected to network:
  - Clients or workstations (e.g. phones, laptops)
  - Servers (e.g. web server, zoom)
- Linked by **connection** medium.
  - **Digital** data is converted to **signals**.
    - Network card does translation
  - Follow communication ***protocols***.
    - Set of rules followed by sender and receiver.
  - Many types of communication medium
    - Copper wire, Optical fibre, radio, pigeons ….

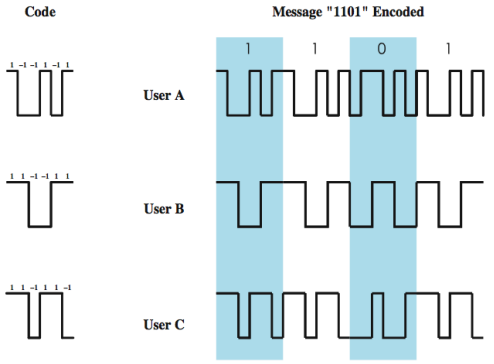
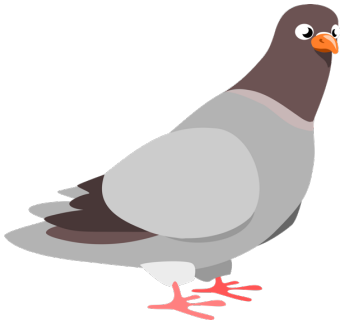


Figure 9.10 CDMA Example



https://tools.ietf.org/html/rfc1149

Main types of networks

- Local area network (**LAN**)
  - Small geographic area
    - E.g. room, ECS, building
  - Access is limited to organisation
- Wide area network (**WAN**)
  - Wider geographic area
  - Access limited to organisation or organisations
- Internet
  - Any computer with a public address
  - Also, a WAN and a Network of networks

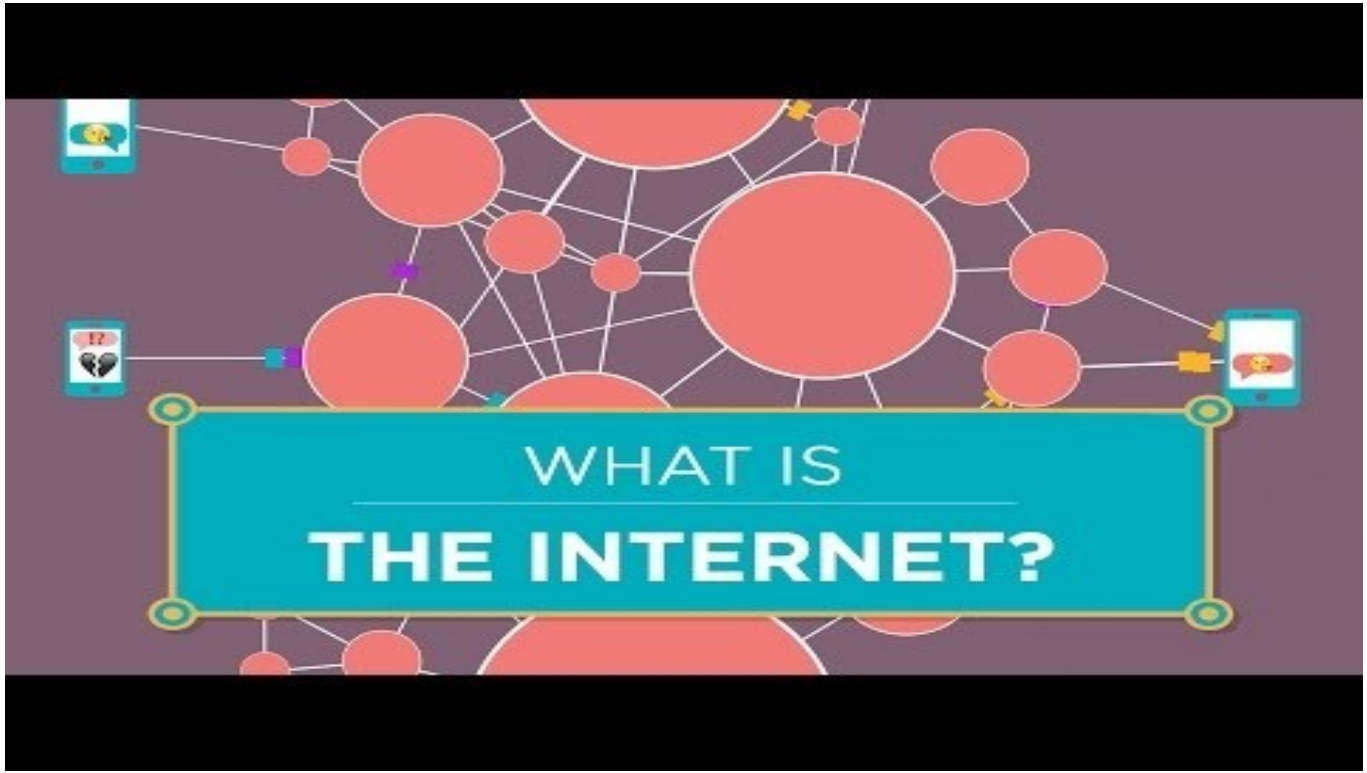
Common threats

- **Confidentiality**
  - Snooping on private communication
- **Integrity**
  - Changing communications
- **Availability**
  - Preventing access to clients and servers
- **Authentication**
  - Spoofing identity and communications
  - Accessing services as someone else

PART II:

So what is the *Internet*?

What is the Internet



https://www.youtube.com/watch?v=Dxcc6ycZ73M

Who develops the protocols?

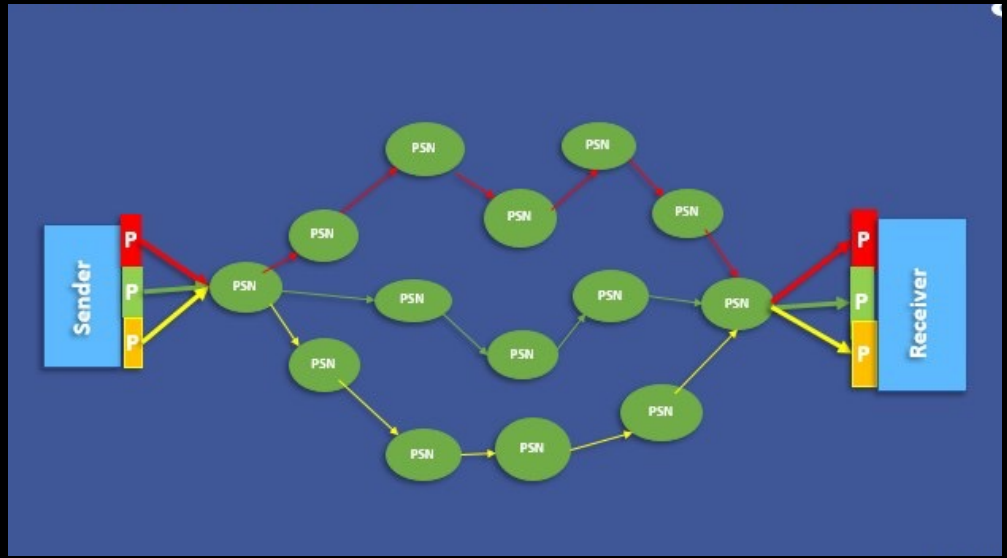
- Nobody is in charge of making it work.
- Everyone uses the same protocols.
- A **protocol** is a **set of rules**:
  - Formatting
  - Processing data

- Who develops these protocols?

Internet Engineering Task Force

- Established 1986
- Membership of Citizens and Volunteers
- Cardinal principles:
  - Open process
  - Sound network engineering principles
  - Rough consensus and running code
  - Volunteer core
  - Protocol ownership

PART III:
Packet switching

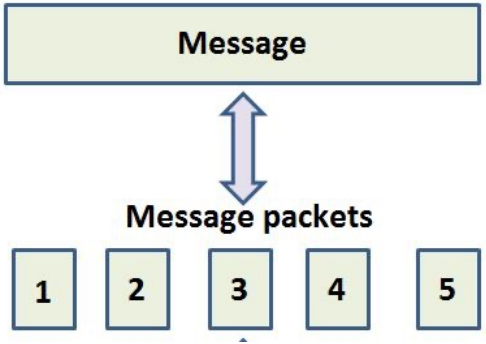


Packet switching concept

- Concept developed during Cold War (1960s)
- Paul Barran from RAND
- Network of nodes and connections
- Deliver messages between any two nodes
- Must be able survive nuclear strike on a node

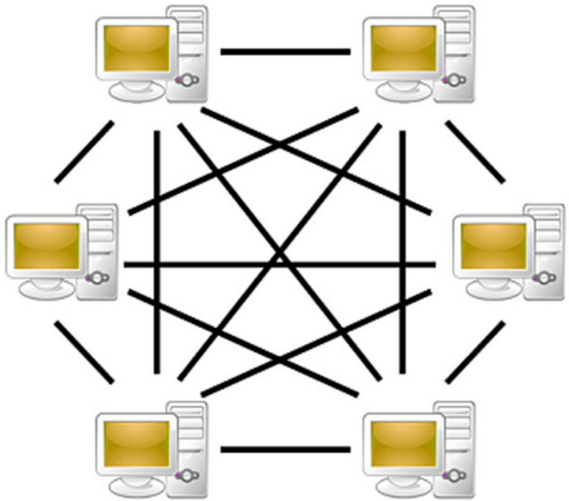
What is a *packet*?

- Messages are **divided** into equally sized blocks called packets.
- Packets have ***headers*** and a ***payload***.
- Headers:
  - Source address
  - Destination address
  - Port number
- The packet reassembled into a message at the destination.

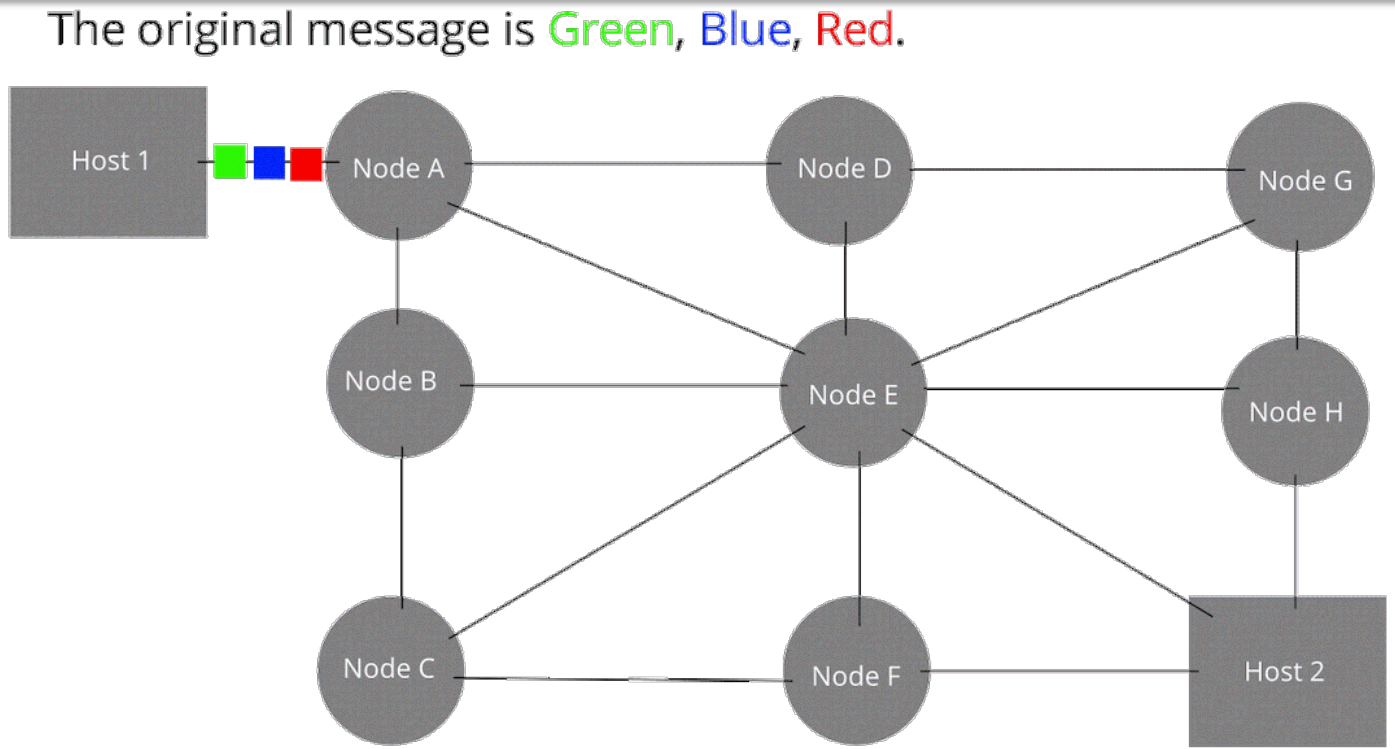


What is *switching*?

- **Redundant** connections between the same nodes.
- Packets associated with the message can take **different routes**.
- Switches and routers use the **header** to direct the packets towards the **destination**.
- Doesn't have to take the most direct route as long as delivered.



Packet switching example



By Oddbodz - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=29033823

PART IV:
Addressing

What are *addresses*?

- An address **uniquely identifies** within a network.
- You typically use ***two*** types of addresses:
  - Internet protocol (**IP**) address
    - Private – only used on LAN or WAN
    - Public – used for publicly accessible network hardware
  - Media access control (**MAC**)
    - Tied to network interface controller (**NIC**)
    - Issued by manufacturers
    - 12-digit hexadecimal number
      - `2C:54:91:88:C9:E3` or `2c-54-91-88-c9-e3`

IPv4 addresses

- IPv4 addresses
  - 32 bit address
  - Four bytes separated by periods
- **Private** IPv4 addresses
  - **10.0.0.0** to **10.255.255.255**
  - **172.16.0.0** to **172.31.255.255**
  - **192.168.0.0** to **192.168.255.255**
- **Public** anything else (close enough)
- Maximum of **4,294,967,296** addresses

IPv6 addresses

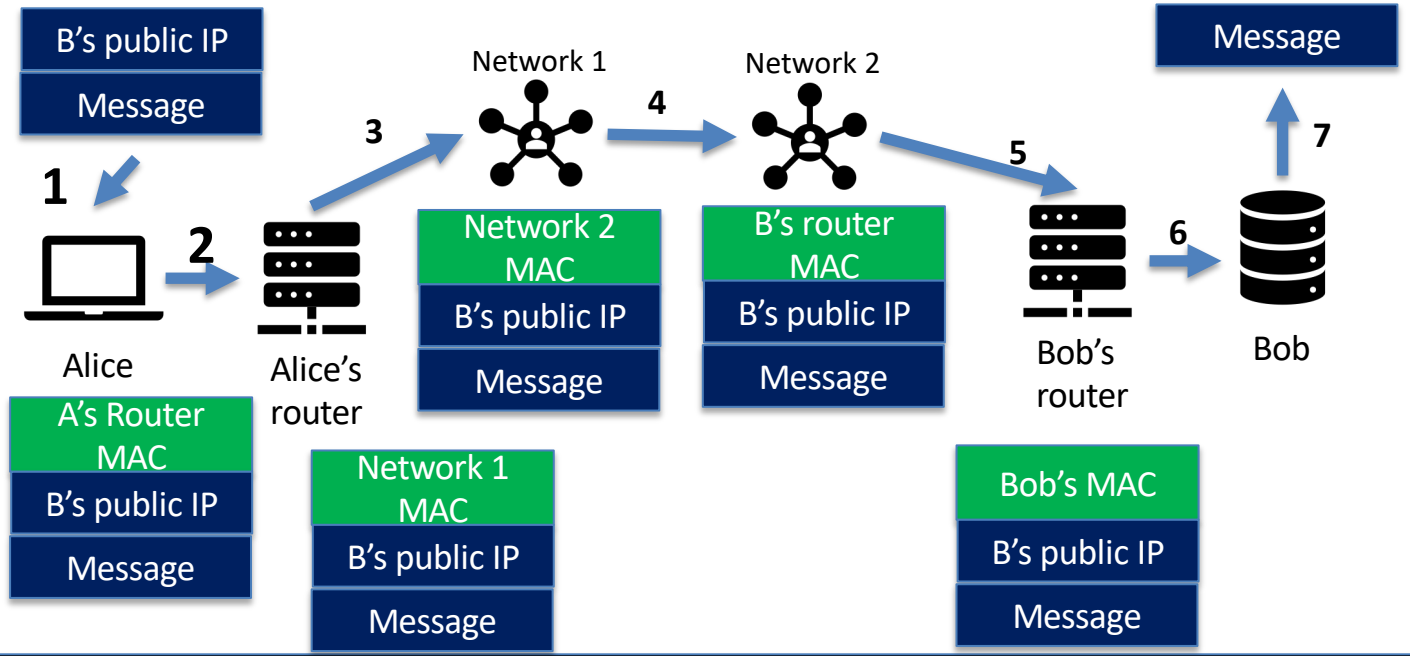
- IPv6 addresses
  - Since 2017
  - 128 bits
  - **3.4×10^{38}** possible addresses
- Example address formats
  - Initial address:
    `2001:0db8:0000:0000:0000:ff00:0042:8329`
  - After removing all leading zeros in each group:
    `2001:db8:0:0:0:ff00:42:8329`
  - After omitting consecutive sections of zeros:
    `2001:db8::ff00:42:8329`

Domain name system (DNS)

- Translates **domain names** to **IP addresses**
- DNS servers maintain a **database**
- DNS resolution process
  - Convert **hostname** (e.g. `ecs.vuw.ac.nz`)
  - To **IP address** (`130.195.5.18`)
- The operating system runs the resolution process
  - Contact the **local** DNS server
  - Ask it to do the translation
  - Should it ***not know***, contact the **next DNS** server
  - Continue until resolved

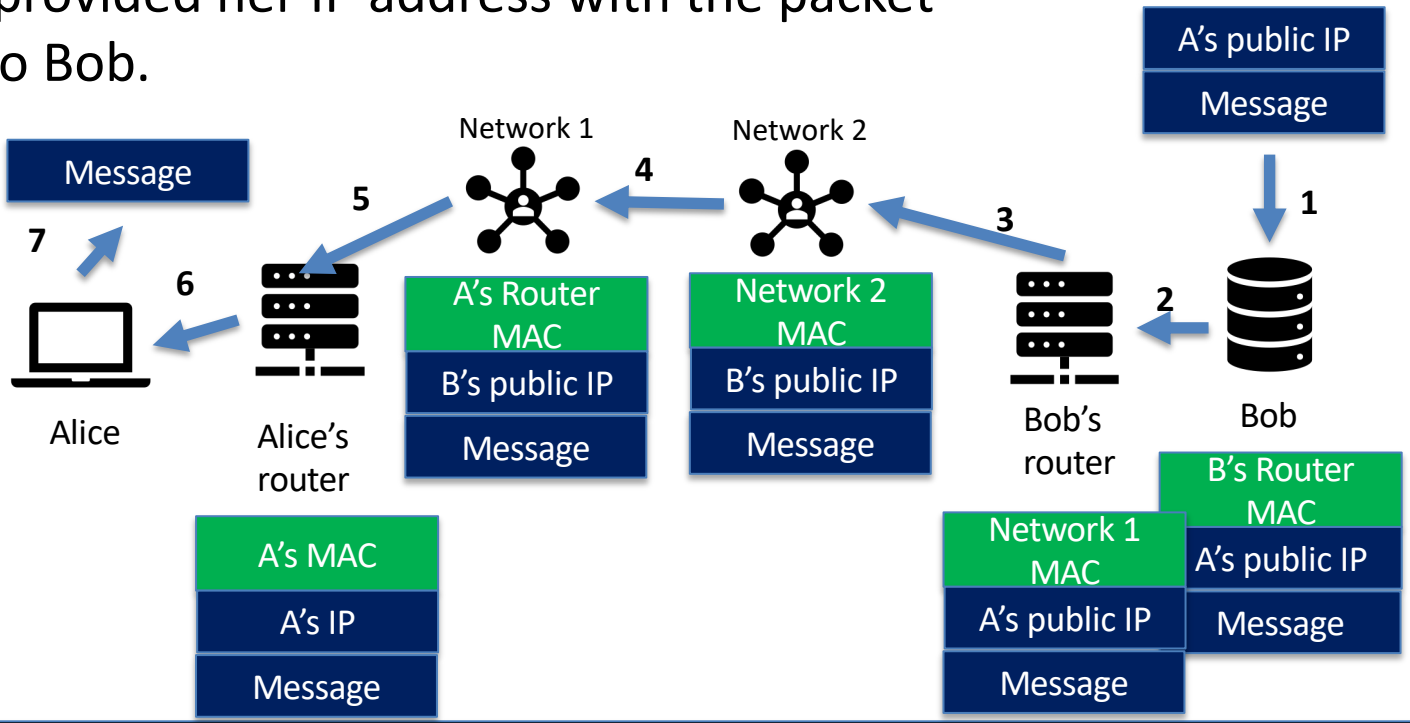
Routing from Alice to Bob

- IP address is used to select next hop that will get the message to the destination.
- Each router adds the address to the next router at the top of the packet.
- Alice's IP address travels along with the packet (not shown in diagram)



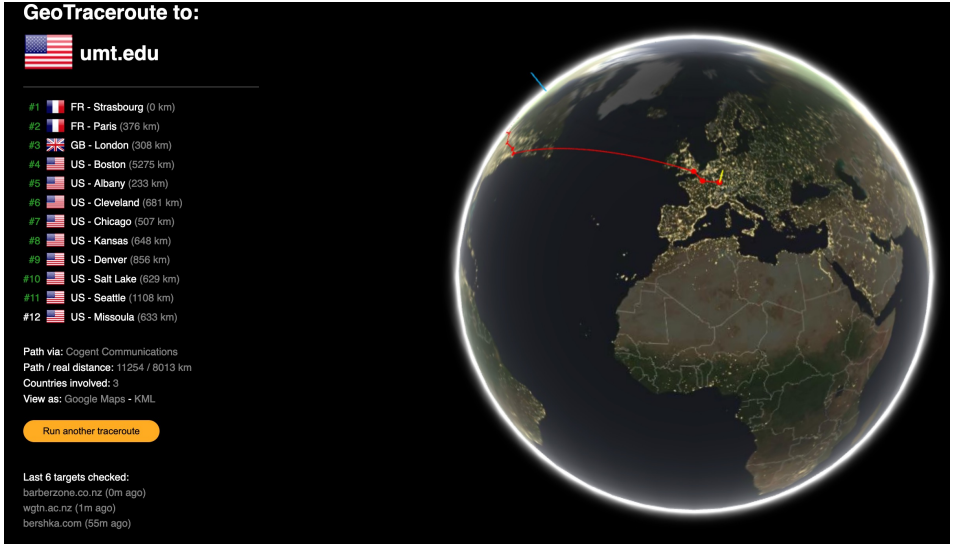
Routing the return message

- Same process on the return path from the server.
- Alice provided her IP address with the packet sent to Bob.

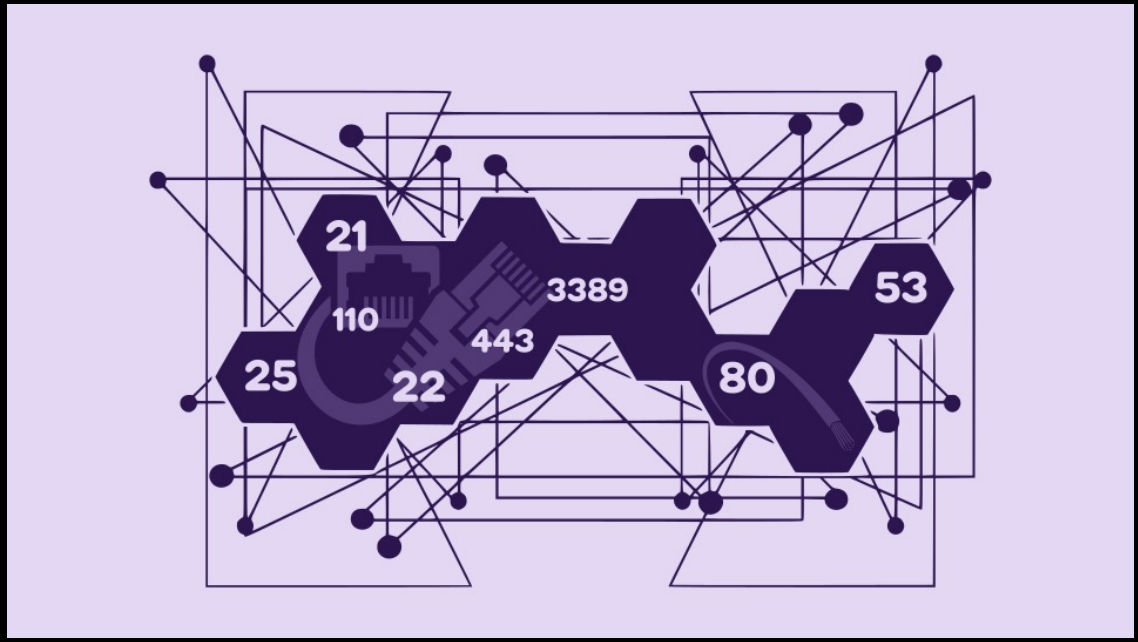


Visual traceroute

- Process of selecting a path across one or more networks.
- A visual traceroute is a tool showing the path to a given computer on the Internet
  - https://geotraceroute.com/



PART V:
Ports

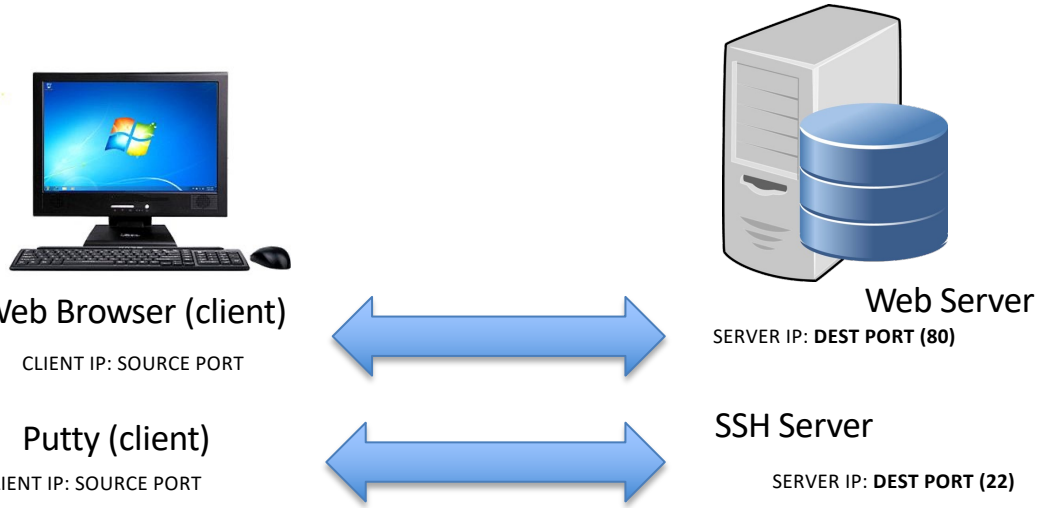


Ports

- A **virtual point** where connections **start** and **end**.
- Software-based and managed by the operating system.
- Each port is associated with a **specific** running **program** or **service**.
- Traffic between services travels over the same internet connection.
- Allows **differentiation** between kinds of traffic.

Port numbers

- The **destination port** indicates **service** to **process** the packet
  - For example, a web page to load
- The **source port** indicates the **client program** to **send a reply** packet
  - For example, the content of the web page
- Port identifies which **program** on the **client PC** is connecting to which **application** on the **server PC**



Port number assignment

- Clients use **dynamic ports** for source port:
  - Also known as ***private ports***.
  - Randomly chosen.
  - Always from the range of **49152** to **65535**.
  - *Changes each time the client program runs.*
- Servers use **fixed well-known ports** for destination port:
  - The convention followed by agreement.
  - Defined in RFC 1700 (https://tools.ietf.org/html/rfc1700)
  - Always from the range of **0** to **1023**.

PART VI:

Why is the internet insecure?

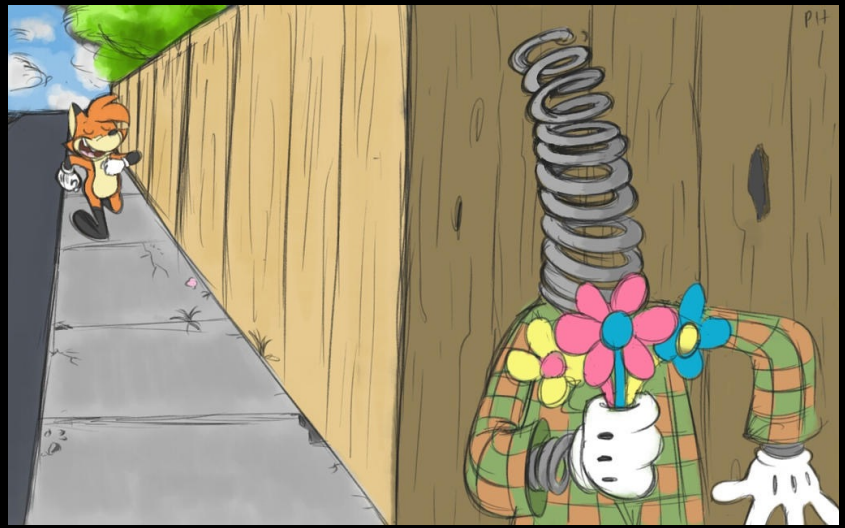
Why is Internet insecure

- Lack of **authentication**
  - Based upon a **domain name**, **IP address** and **port number**
  - Anyone send packet claiming any of these
- Lack of **confidentiality** and **integrity**
  - Protocols don't use encryption
- Open design for routing
  - No single authority directing traffic
  - Anyone can offer to carry your traffic

Bad things can happen

- Routing depends upon cooperation between networks using border gateway protocol (**BGP**)
- Pakistan's state-owned telecommunication company received a censorship order.
- Accidentally broadcast to the world that Pakistan Telecom was the actual address of **YouTube** servers.
- https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/
- Attack on **availability** - YouTube taken offline globally for two hours in 2008.

PART VII:
What’s next



What's up next

- Next lecture we look at some historical attacks that affect authentication, confidentiality, integrity and availability.