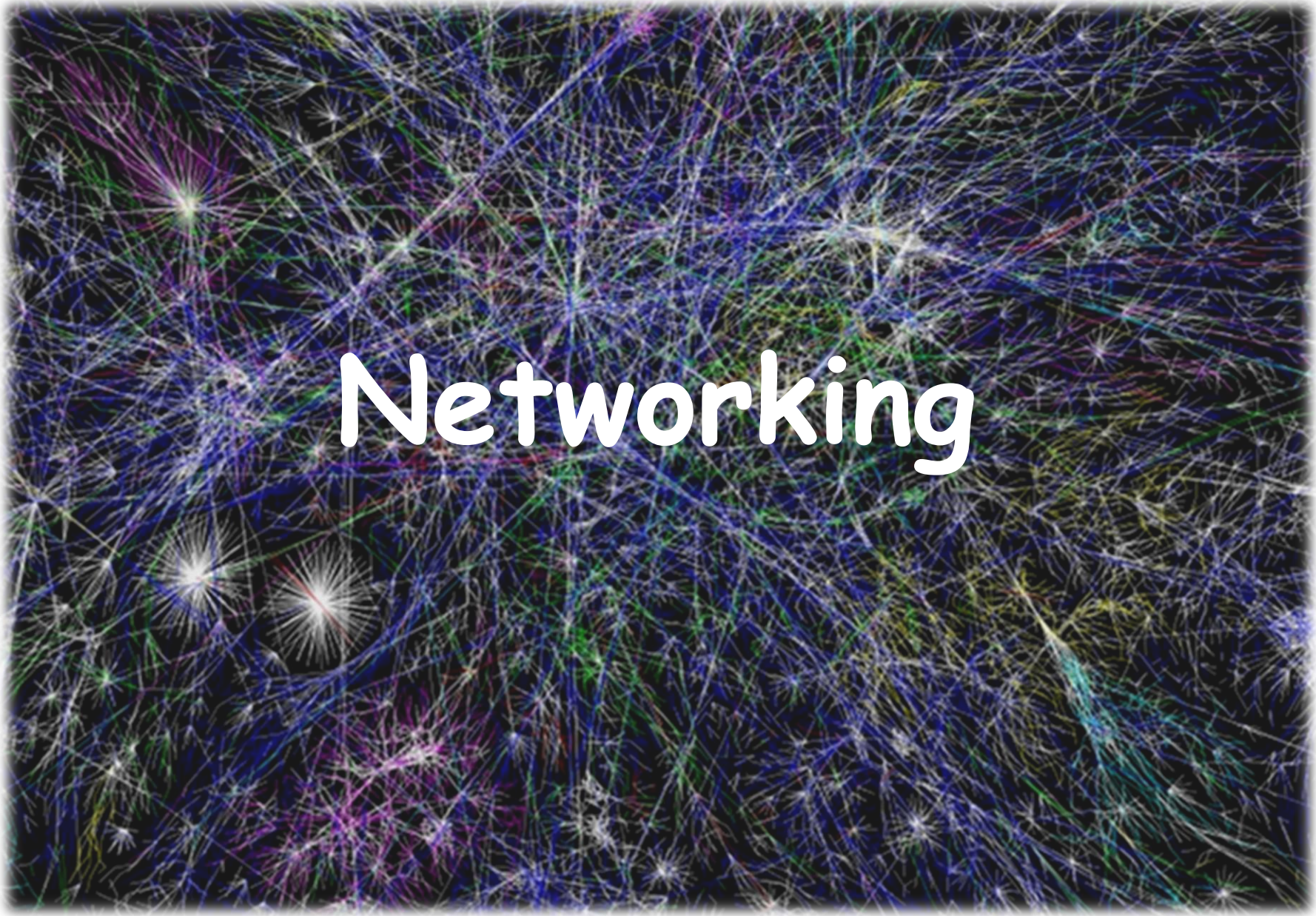

Networking

NIC

MAC

cat3, cat5, cat6

hub

switch

router

ISP

Static address

Dynamic address

DHCP

DNS

hosts table

IPV4 & IPV6

Private address space

LAN

NAT/IP masquerading

Server

Client

Daemon

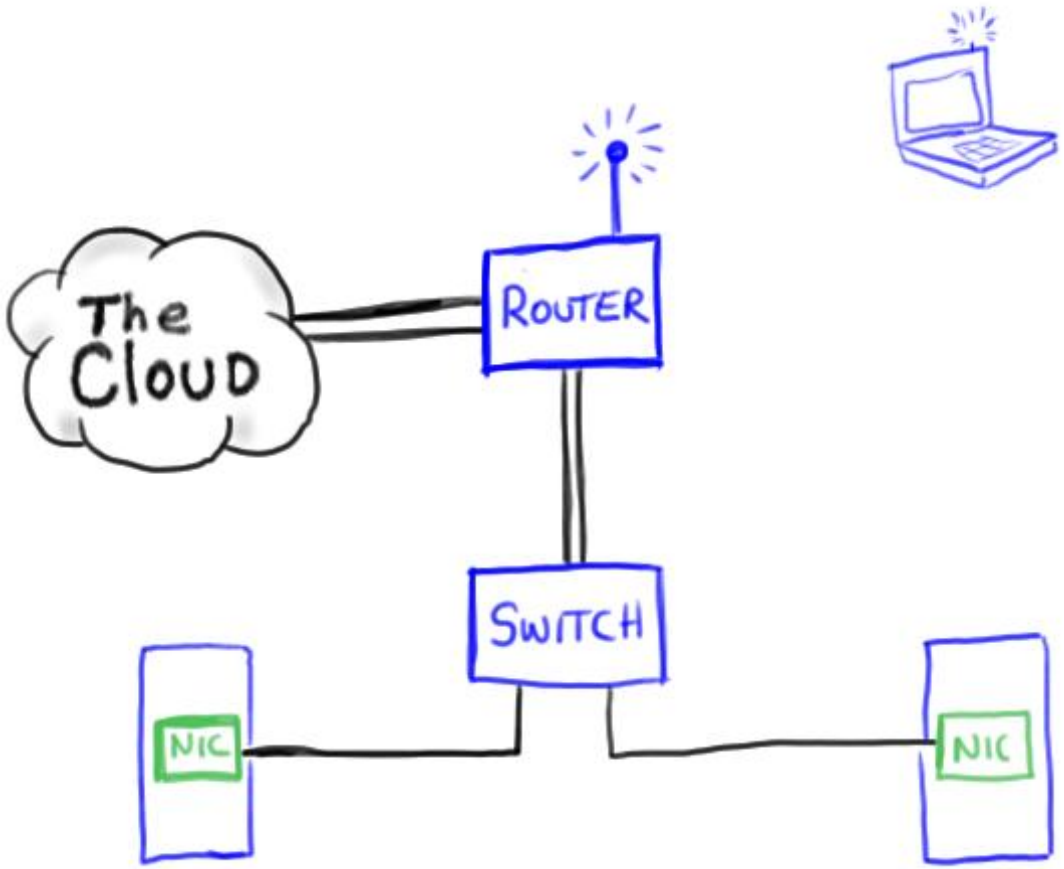
hosts.allow

perimeter/firewall

The Network involves:

1) Physical equipment (network cards, switches, cables, routers)

2) A set of communication rules or protocols.



The 7 layers of the OSI Model

The system of networking hardware and rules is divided into 7 layers, called the Open System Interconnection (OSI) Model.

The layers involve standards for: hardware, logic, starting and stopping communication, error handling, and programs.

Analogy: sending a letter depends on postal equipment (hardware), e.g., postal schedules, trucks, planes, post offices and rules for addressing the envelope & stamping it, mailboxes, etc.

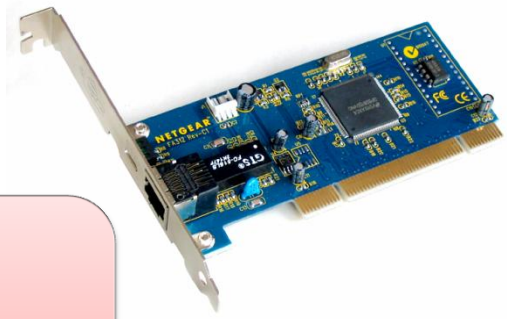
Networking Hardware

- Network card (**nic**),

- Cables (**cat3, cat 5, cat5e, cat6**)

- Hubs, Switches, and Routers

NICs and MACs



Network card: a.k.a. **Network Interface Controller (NIC)**, ethernet card

Each NIC has a Media Access Control Address (MAC, Hardware or physical address) e.g., 01:23:45:67:89:ab.

Each MAC address (not each computer) gets assigned an IP address, e.g. 128.196.98.124.

Cables

- Cables are available in these categories: **cat3, cat5, cat5e, cat6**.
- Higher number→ better quality, fewer errors, higher speeds.
- Old cat3 in the walls in many UofA buildings limits network speed.
- UITS can tell you what kind of cable is in the wall.

Hubs/Switches/Routers

- All 3 of these devices connect network devices together.
- They vary in intelligence.
- Hubs are the least intelligent.
  - Information packets entering any port gets broadcast to all ports.
  - When packets collide (which is frequent), they have to be resent. This slows everything down.

Hubs/Switches/Routers

- A switch is more intelligent than a hub.
- A switch routes traffic to the intended port, greatly improving the flow of information.
- The more information the switch can keep track of, the better it is at moving information smoothly. Sophisticated switches are "smart switches".

Hubs/Switches/Routers

- A router is the smartest device.
- It is a gateway connecting your machine(s) to the internet.
- The router has its own IP address, so you can log on and change its settings.
- It can also assign IP addresses to connected computers.
- A good router is like a computer, and can do lots of clever things.

What Breaks?

Of all this hardware the most common problems are that a hub, switch, router or modem becomes "confused" and has to be unplugged and rebooted to regain its composure.

Cables also go bad fairly regularly.

Occasionally a physical port will go bad on a hub,switch or router.

Uncommonly a NIC will go bad.

Networking Service

- Like a telephone, networking hardware is useless without service.
- The **ISP** is the Internet Service Provider.
- They provide you with service and a modem (e.g., cable modem) to connect your computers to the internet. They may provide a router (or you could buy your own) if you want several machines to share the connection.
- The ISP will sell you a static or dynamic IP address.

Static vs Dynamic Address

A **static** ip address is like a phone number. If you have a predictable phone number, I can call you.

It is cheaper for ISPs to provide **dynamic** addresses. If you had a dynamic number for your phone, you could change your number at any time.

- You could call other people, but they would have a hard time calling you back if your phone number kept changing.
- A computer with a dynamic address can get to the internet, but people out there have a hard time contacting your computer.

Dynamic Host Configuration Protocol

- A DHCP Server manages a pool of ip addresses.
- When a client machine requests an address, the server provides one from its pool.
- A router can act as a DHCP server.

Names are easier than numbers

- For humans, it is easier to remember names than numbers (e.g., cellphone address book).
- google.com not 74.125.19.106
- So we have address books that match the name and IP address.
- The local one is called a hosts table.
- The big ones are called DNS servers.

Hosts Table

- Your computer has a tiny "phonebook" of its own called the **hosts table** where you can add name-address pairs of your own choosing. Your machine will try to resolve a name by looking first in the host table, then asking the DNS server.

Hosts Table Example

```
# Host Database
# Last Updated: $Date: 2008/12/20 20:51:02 $
# localhost is used to configure the loopback interface
# when the system is booting.  Do not change this entry.
##
127.0.0.1       localhost localhost.localdomain
255.255.255.255 broadcasthost #this local network (special address)
#
#private address of laptop at home
192.168.1.15    rasa rasa.tohono.com

#public address tommy at UMC
128.196.112.123   tommy
```

DNS

Domain Name Service is like a phonebook for computers.

DNS servers are separate machines that keep a list of static IP addresses (numbers) and the name associated with them (e.g., google, hagar)…

When you type in the name, your computer goes to the DNS server and consults the list to find out what IP address to go to.

IP Address Space

IPV4 (internet Protocol version 4; 1981): uses 32 bit addresses xxx.xxx.xxx.xxx (which defines only ~4.3 billion static addresses).

This is why static addresses cost more or require extra effort to get.

Blocks of addresses were allocated to companies and institutions.

The UofA owns a sizable block of addresses.

IPV6 is slowly replacing IPV4. IPV6 has 128 bit addresses which will vastly increase the number of available addresses (2^{128}).

Private Address Space

Private addresses:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Anyone can use these private addresses.

They are "private" (or internal) because they aren't accessible (routable) from the public internet/remote locations.

They can be static or dynamic

Private Address Space

- They are common in home and Office **LANs** (Local area networks).
  - Computers on the LAN can communicate with each other, because their addresses are static.
  - Remote computers can't get to LAN computers directly, making the LAN computers safer.

NAT

Network Address Translation (ip masquerading) allows all the private address machines on the LAN to browse the net using a single public address (either static or dynamic).

A router (a.k.a NAT box) keeps track of which private address is asking for which websites. The machines behind the NAT box browse the web anonymously…which is more secure (a hacker can't get to your machine directly)

U of A Networking Service

UITS (a.k.a CCIT) provides UA service.

Call UITS to find connection speed for wall outlets on campus. Many are old and slow.

Because the wall connection/building equipment is infrastructure, you can't (typically) use a grant to pay for upgrades.

Request a static address from your department IT staff (if you need one).

A static address is useful if you want to access your computer from elsewhere (e.g., UMC or home)

Servers and Clients

These terms are used to refer to hardware or software.

Think of a restaurant:

- Servers provide services
- Clients use services

For example, a DNS server provides a "phonebook" to any machine that cares to request information.

An SSH server allows clients to connect and request data.

Servers need static IP addresses.

Services

- A server is useful, but hackers want to take over servers, so servers require careful security.
- There are dozens of services a machine can provide. Each service has a "**daemon**". The daemon listens on a particular "**port**" number (a designated logical data connection) for requests from clients.
- Each daemon can be called a server. It listens only at its port for someone to ask to connect.

Mindbending logical constructs:
ports and daemons

I'm httpd, listening at port 80

Services

Some services are encrypted & secure (ssh; port 22).

- The service is provided by sshd (ssh daemon)

Other services (usually older) are very insecure (telnet; port 25) and (ftp; port 21).

- telnetd and ftpd are the daemons that provide the service

A web server usually uses port 80.

- httpd provides the web service

Hackers try repeatedly to connect to different ports on a server, hoping they'll find an overlooked unprotected way in to the computer.

Securing a Server

1) Turn off insecure and unnecessary services, patch the secure services, use good passwords.

2) Limit the machines that are allowed to connect to the server. (On linux, hosts.allow provides a list of machines that can connect, simple and powerful)

4) The university provides a perimeter (firewall) to protect machines in the university address space from attack. e.g., you can't use ping to see if a machine on the university network is present "alive".

IT managers are understandably reluctant to allow people to run servers, since any compromised server in the university's address space allows the attacker past the perimeter, and makes other university machines easier to attack.

Summary: Why you Care

Neuroimaging requires errorless transfer of large datasets.

You want high speed connections

You want high quality cables.

Sometimes you will need to run servers, or talk to servers.

e.g., Tommy at UMC runs an ssh server

To set up a server, you need some awareness of static vs dynamic addresses, and services.

Summary: Hardware

You want switches, not hubs.

You want very fast NICs and switches (1000 not 10 or 100)

You want high quality cables that won't get errors (cat5 or cat5e or cat6).

SWS Electronics is a fantastic source for cables…you can even get different colors to help you keep track.

Summary: Addresses

Static addresses are more expensive.

Servers need static addresses (well, you need to know the address of a server, so if it is static, that really helps)

Static addresses are more dangerous, because hackers can go to them too.

Dynamic addresses are cheaper. They are typically what you get on a public wireless network.

Dynamic addresses are handed out by DHCP.

Summary: Addresses

Private addresses are unroutable and must come from a particular subset of possible addresses.

They are used behind a router to keep things secure and share a single public address.

This is called Network Address translation or IP Masquerading.

Summary: Names

Names are helpful to humans

The "Hosts table" is an editable list on your computer of IP addresses and associated names.

A DNS server has a giant list of IP addresses and names. The University has its own DNS servers, and so does Comcast, Cox etc.)

Summary: Services

The Transport layer of the OSI model specifies which ports (logical, not physical) go with which services.

Sometimes a program like matlab will have its own associated port and service.

You need to turn off unnecessary or insecure services on your server, to help keep it safe. This is called **hardening** or **securing** the server. Advice abounds on the internet.

NIC

MAC

cat3, cat5, cat6

hub

switch

router

ISP

Static address

Dynamic address

DHCP

DNS

hosts table

IPV4 & IPV6

Private address space

LAN

NAT/IP masquerading

Server

Client

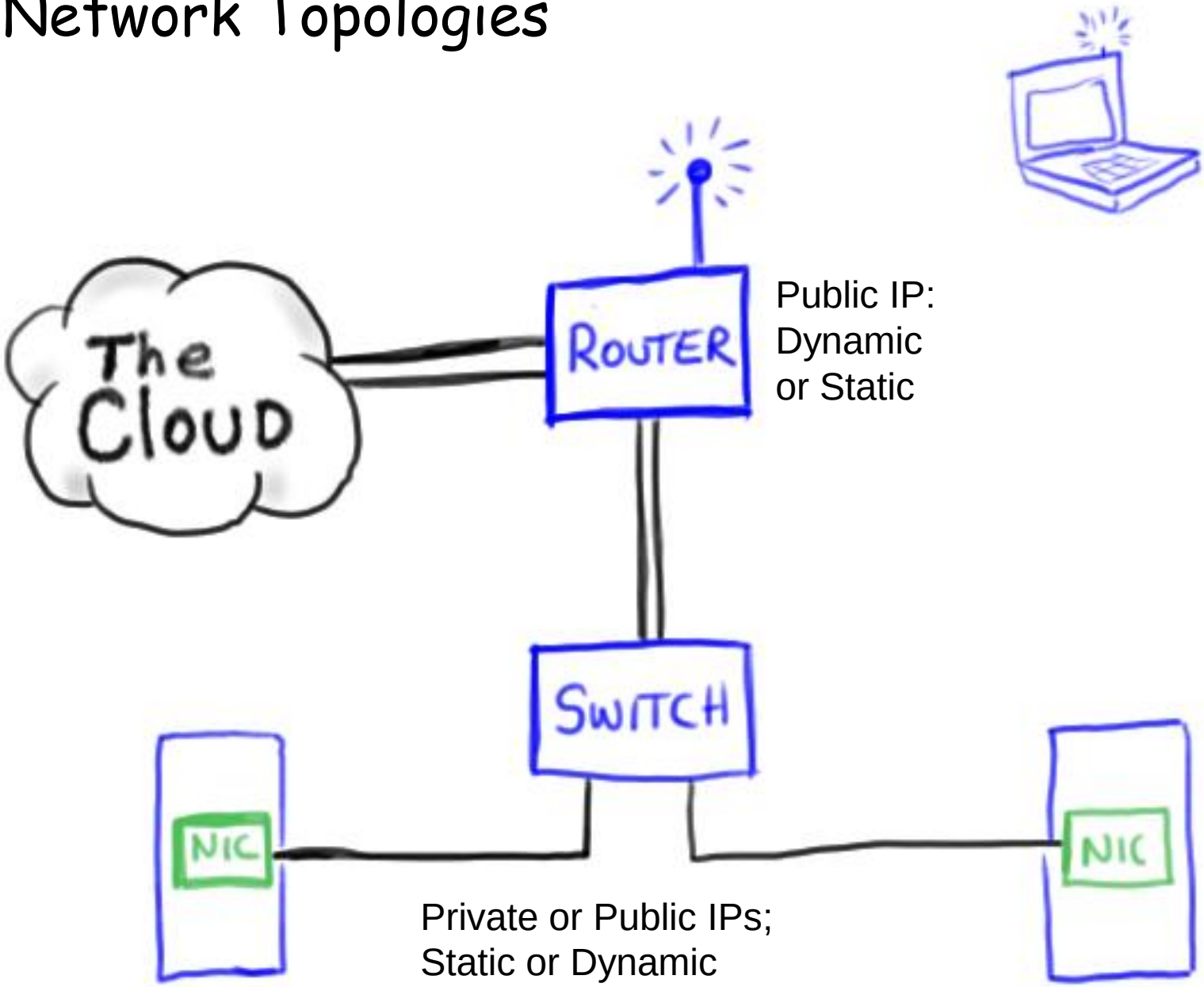
Daemon

hosts.allow

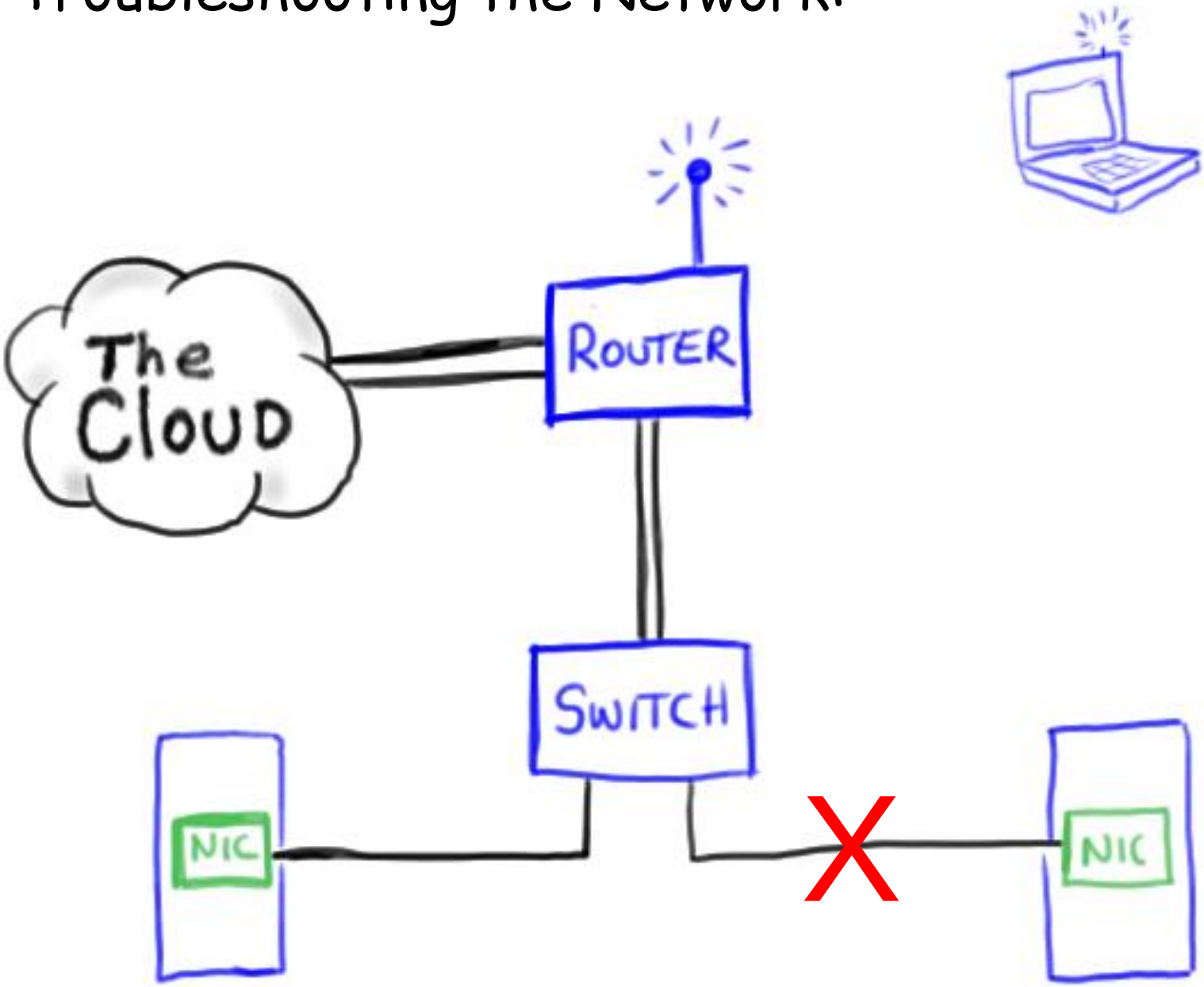
perimeter/firewall

- To get to the network, your computer needs to know:
  - its own IP address (IPV4 & IPV6),
  - the IP address of the router or gateway that handles connections to the internet
  - addresses for some DNS servers (a.k.a "name servers") to consult for information about web addresses.
- Each piece of information may reside on the DHCP server/router or on your machine.

Network Topologies



Troubleshooting the Network:



Tools

- Network settings on your machine will allow you to display or set IP address, gateway and DNS servers addresses.
- ipconfig (windows); or ifconfig (mac/unix) at the commandline will display: mac address, IP address, gateway address.
- ping at the commandline will allow you to see if a computer is "alive".

Troubleshooting

- ipconfig or ifconfig gives you a 169.xxx.xxx.xxx IP address or no address.
- The machine has failed to get a "real" IP address. Why?
- How might you fix it?

Troubleshooting

- DNS server information has been lost, but the LAN is up and running.
- What happens:
  - You can ping other machines in your lab (if they know their ip addresses).
  - You can ping the building gateway.
  - You cannot browse to google.com.