GET YOUR DEVICES COMMUNICATING

PHONES, HOME PCS AND MOBILE COMPUTING: GET YOUR PHONE TALKING TO YOUR DESKTOP AND TALKING TO YOUR LAPTOP. THIS WAY, IF ONE OF THESE DEVICES GOES DOWN, YOU AREN'T DEAD IN THE WATER.

HOW TO MAKE DEVICES COMMUNICATE IN A WIRELESS WORLD

- The Ford Model T started rolling off the assembly line in 1908.
- If you'd purchased one you would have found yourself sharing the right of way with Stanley steam cars, battery-powered Baker coupes, horses and buggies, mule trains, ox carts, Indian motorcycles, bicycles and trolley cars.
- There was more than one way to get around and each one had unique advantages. The result, quite often, was sheer bedlam.

THE DIGITAL HIGHWAY

Modern digital communications may appear to be in a similar state of disarray. Newer protocols like USB and Wi-Fi haven't driven older protocols off the streets; they merely share the right of way.

There are still some things that serial communications do so well – connecting the pumps at your corner gas station to the cash register would be a good example -- that the total number of serial-equipped devices deployed around the planet is actually continuing to grow.

They'll be out there on the road for a long, long time.

SERIAL PORTS VS USB

Inconveniently, few computer manufacturers bother to support the serial protocol anymore, as its IT and desktop functions have largely been replaced by USB and wireless.

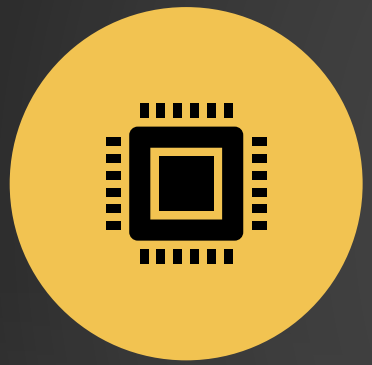
It's getting harder and harder to find a new computer with a serial port.

Tablets and smart phones are even worse.

Some don't even have a USB port; they largely depend upon wireless for their communications purposes.

They're useful tools, but what do you do if you need to connect to older devices and protocols?

THE CURRENT STATE OF AFFAIRS



ETHERNET AND SERIAL COMMUNICATIONS STARTED COOPERATING WITH ONE ANOTHER WHEN THE ETHERNET SERIAL SERVER CAME ALONG.

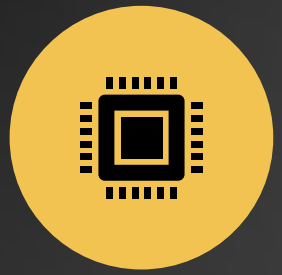
THE SERIAL SERVER TRANSLATED THE SERIAL DATA INTO TCP/IP FORMATS THAT COULD BE TRANSMITTED ACROSS A NETWORK.

THE SERIAL DEVICES COULD THEN BE NETWORK-ENABLED, AND THE DEVICE SERVERS COULD USE ORDINARY ETHERNET CABLE TO CONNECT TO A LOCAL AREA NETWORK (LAN).

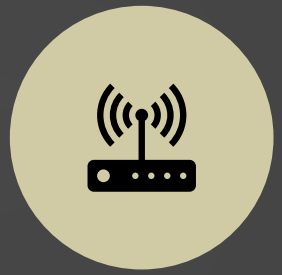
THE NEXT STEP WAS TO GO WIRELESS.

- A wireless device server contains a Wi-Fi client very much like the one in your laptop, usually 802.11b/g or 802.11b/g/n these days.

LOCAL AREA NETWORK



When a device server connects to a LAN it provides an IP address that is unique to the SDS.



The other network devices can then use that address to send and receive data.

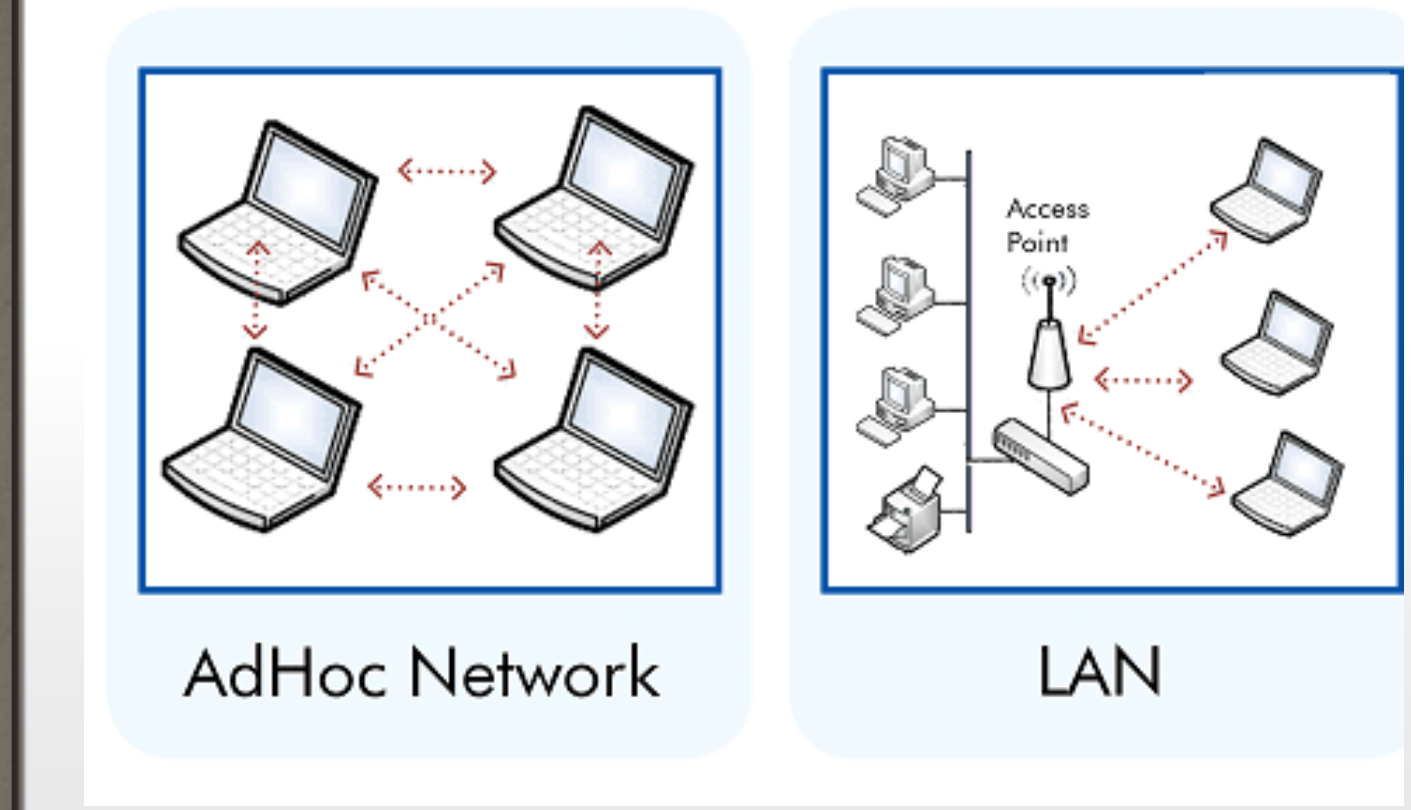
Since this IP address is the location for all interactions, a secondary reference is added to locate the information or resource required for the specific interaction.

The secondary reference is called the port number.

IP ADDRESS

- The IP address/port number combination makes it possible to uniquely locate any serial port on the network.
- Here's a typical scenario: A serial device server has a physical serial port connected to port 8023 on the network interface. The network interface connects to the network and gets an IP address of 192.168.2.100. After adding the second piece of information the full address of the serial port becomes 192.168.2.100:8023.
- Any network-connected device capable of accessing that address can establish two-way communication with the serial port. So far; so good.

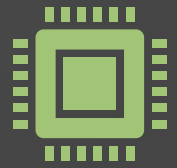
AD HOC NETWORK VS LAN



AD HOC NETWORK

An Adhoc network is a peer-to-peer based network that doesn't use a central resource (Access Point) to manage the network connections and structure.

AdHoc networks can be established when just two clients are within range of each other.



Groups of devices can also be connected, with each group being referred to as a "cell".

The AdHoc network uses the Internet Protocol Suite for data communication between the devices.

WHAT HAPPENS WHEN A DEVICE GOES OFF-ROAD?

- A serial device server needs a network connection to do its job.
- But some serial devices are placed in remote locations where they not only lack access to wired infrastructure; they're also outside the range of any potential wireless connection.
- Sometimes access is available, but it's restricted because of IT policy and security rules.
- The need to communicate with these devices still exists, but the connection isn't there.
- Where there's no available network infrastructure it's possible to set up an AdHoc network. (A wireless device server can connect to either an infrastructure network or to an AdHoc network.)

BUT AN ADHOC NETWORK HAS SOME DRAWBACKS:

You have to use Static IP Addresses. A service called DHCP, which larger networks often use to provide IP addresses to connected devices, is not normally available on an AdHoc network. That means you'll have to manually assign and distribute unique addresses to each device.

AdHoc creates a static subnet for the network and for all devices on the AdHoc network. This restricts interaction between different networks. You'll have to manually configure your IT (laptop) equipment when connecting, and enter a static IP address.

AdHoc networks are not self healing. Even if you have multiple AdHoc networks within the same geographical location, and they're all using the same network name, devices in one network still can't talk to devices in the other.

There's another problem with AdHoc networks, which is that the latest Android™ tablets and smart phones can't connect to them without advanced modification. And certain iOS devices can't connect to AdHoc networks that employ wireless SDS's.

SO HOW DO YOU GET THINGS MOVING AGAIN?

- Just as the Model T Ford eventually gave way to newer, sleeker vehicles, Wi-Fi technology keeps getting better and better.
- There is now technology that supports embedded Access Point functionality without changing the SDS functionality.
- The Stanley Steamer was only sold for about two decades.
- Serial ports have already been around a lot longer than that, with no end in sight.
- Embedded wireless AP ensures that you'll be able to keep yours running smoothly for as long as you need to.

WI-FI:

- This is a local area wireless technology that uses 2.4 GHz ultra-high-frequency or 5 GHz super-high-frequency radio waves.
- This tech is great for sending large amounts of data wirelessly between devices.
- But it also requires a lot of energy to operate and many devices in the Internet of the Things model only require a small level of data throughput.
- In other words, this is overkill for many applications and would require you to change batteries in all your devices on a regular basis.

BLUETOOTH:

- Introduced by Ericsson back in the 1990s, Bluetooth technology allows for personal data networks.
- It transmits data over the frequency band between 2.4 and 2.485 GHz.
- It operates over shorter distances than Wi-Fi and requires less power to operate.
- You can pair devices like phones, smartwatches, headsets, speakers, computers and more together.

BLUETOOTH CONTINUED

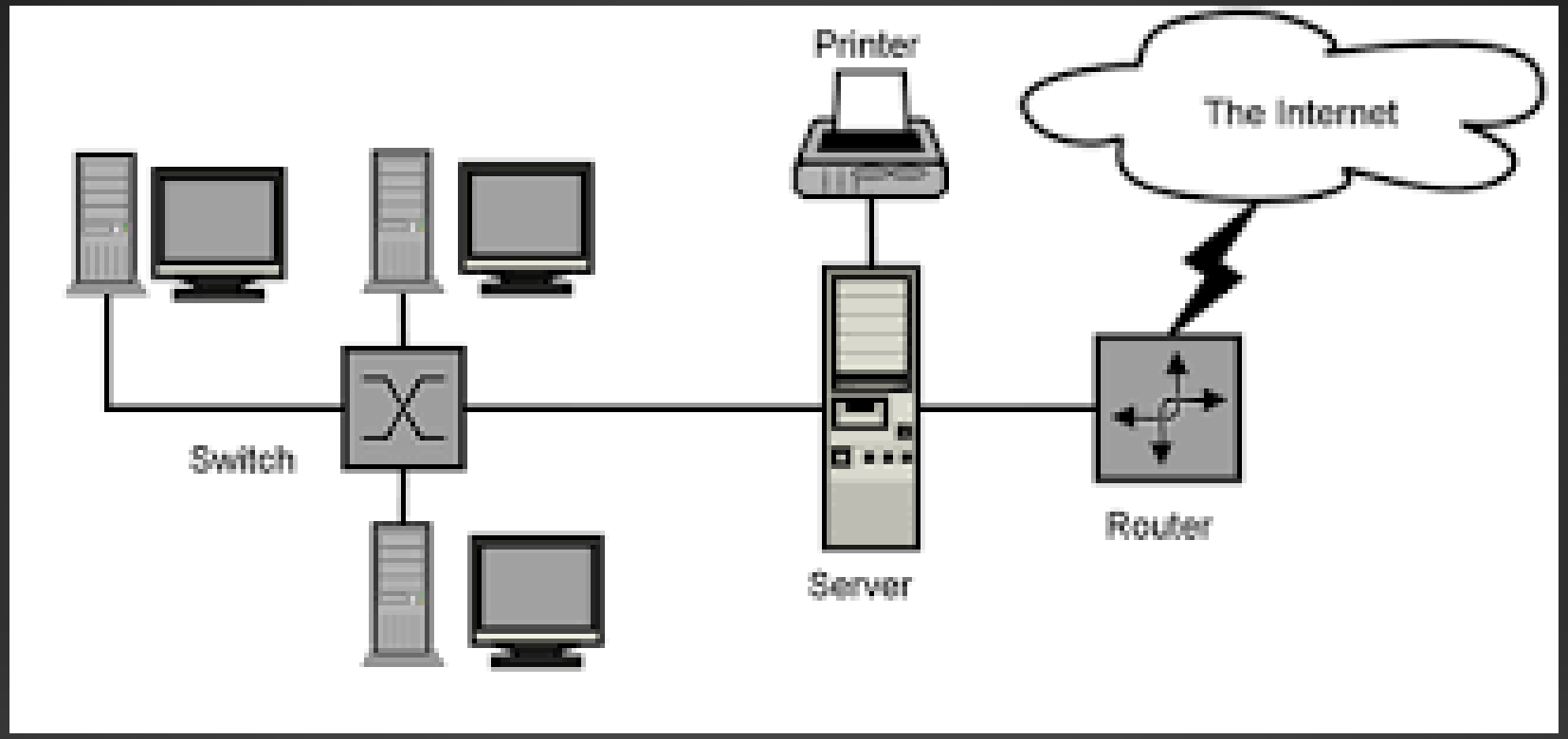
- Even with the limited range, early Bluetooth implementations were a big drain on battery life.
- With the development of Bluetooth v4.0 came the ability to implement low-energy features that conserve power more effectively.
- Typically, devices connect back to a centralized machine like a computer or smartphone -- they don't "talk" to each other so they aren't a candidate for mesh networks.
- One thing to note - this standard is still evolving, so perhaps in the future things could change.

ZIGBEE:

- This standard is well-suited for mesh networks.
- The ZigBee standard allows for low-powered devices to send data along a network, with each device capable of relaying the data toward its intended destination.
- This lets you set up a really effective network -- you don't have to worry as much about getting out of range as you would with a Bluetooth device.
- As long as your ZigBee gadget can chat with another gadget in the network, you're set.
- So what's the downside?
- The main problem is that there are lots of different flavors of ZigBee implementation -- in other words, the standard isn't as standard as it might need to be.

THREAD:

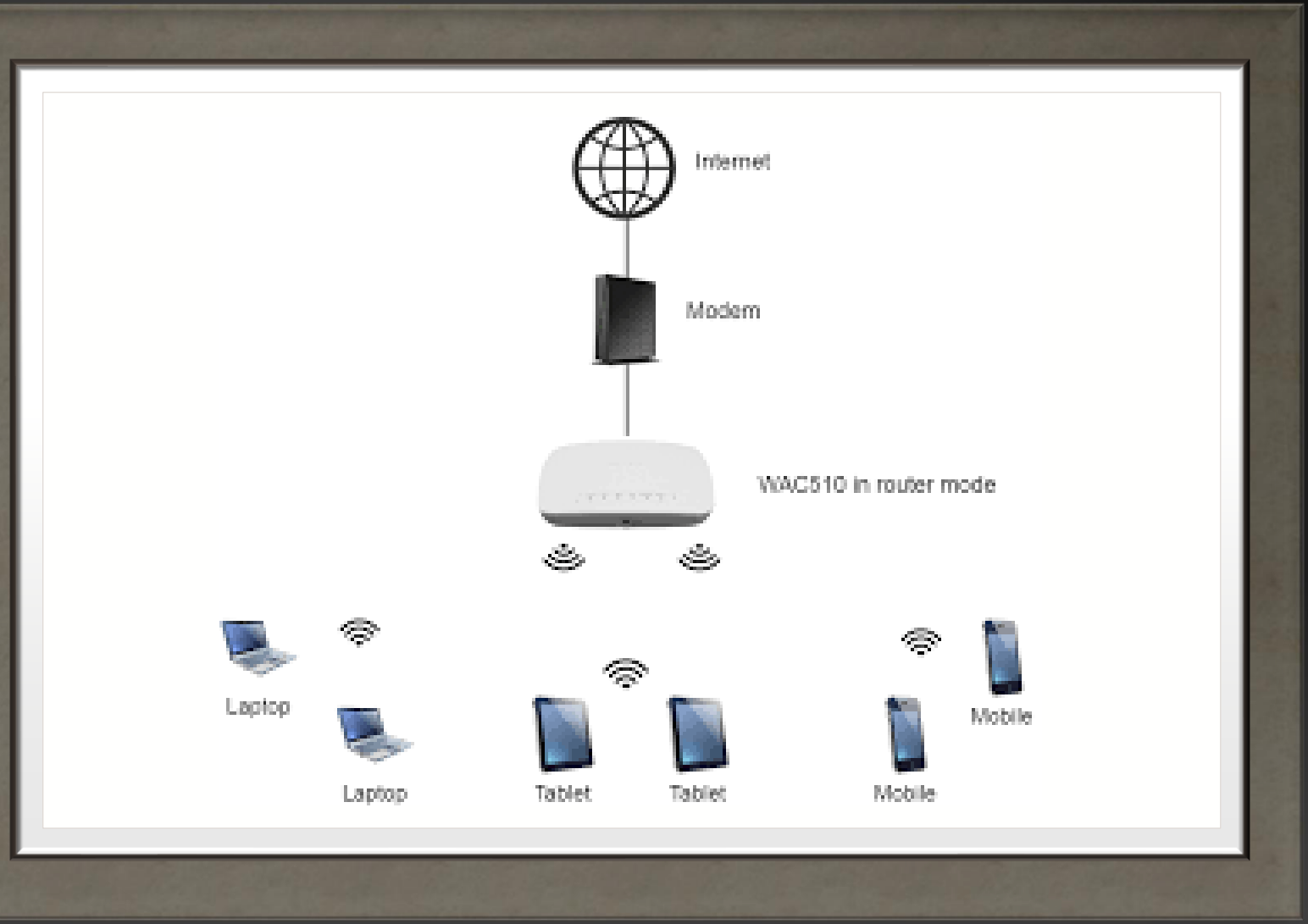
- The brainchild of an alliance between Nest, Samsung, ARM and a few other companies, Thread aims to anticipate the needs of the Internet of Things.
- Based on the current specifications, Thread would be able to support a network of up to 250 devices.
- Every house could be its own network, meaning your home could have up to 250 integrated devices interacting with you on a daily basis.
- Like ZigBee, Thread would allow for mesh networks -- all those devices would be capable of relaying data.
- Thread hopes to avoid the ZigBee problem of fractured standards by requiring a certification program for anyone wishing to incorporate the technology into a product.



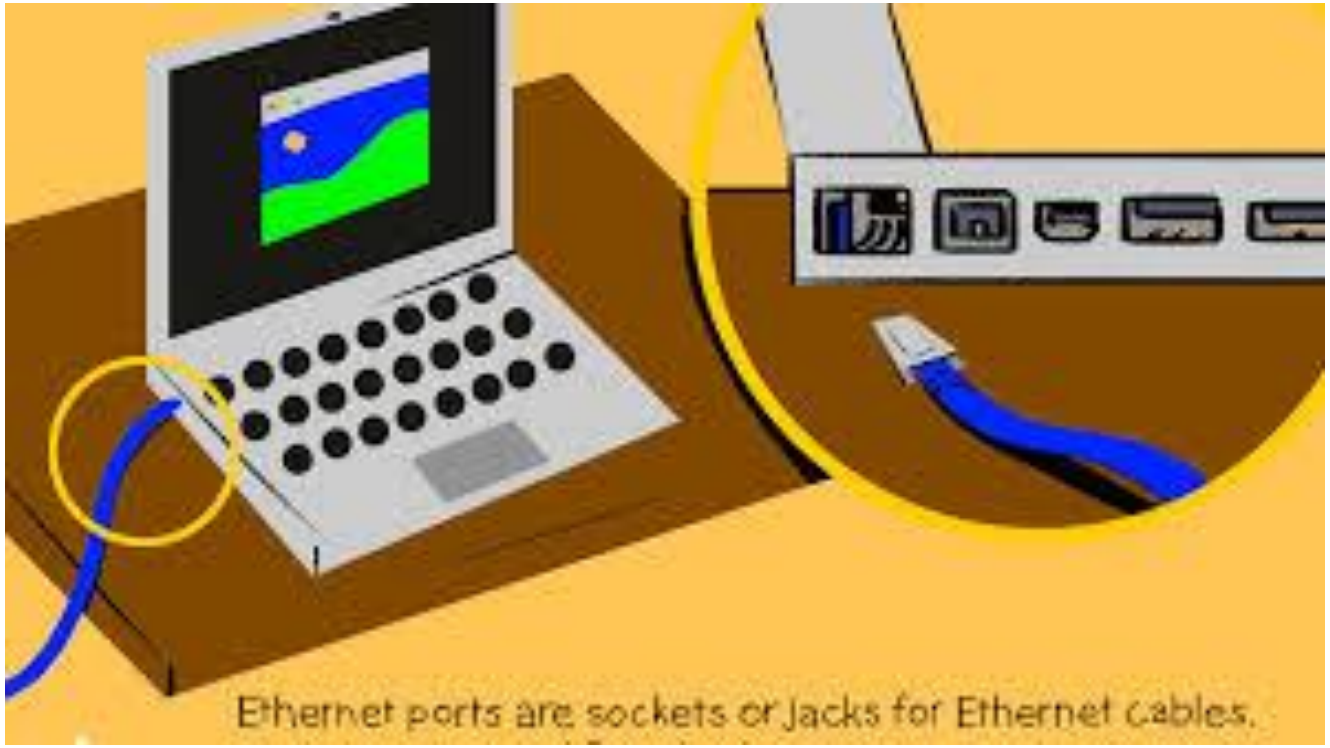
HOW DO NETWORKS COMMUNICATE

HOW WI-FI PRINTERS WORK

ACCESS POINT



ETHERNET PORTS



Smartphone applications do not transmit data in isolation

Apps depend on layers of technologies that can each generate identifiable digital traces

Application: Where users spend most of their time. Applications use "permissions" granted to them by the Operating System to access and interact with a device's lower-level data and functionality.

Operating System (OS): Bridge between apps and device hardware. Controls wireless radios, network connectivity, and grants permissions to applications. Each Android OS install has a unique System ID.

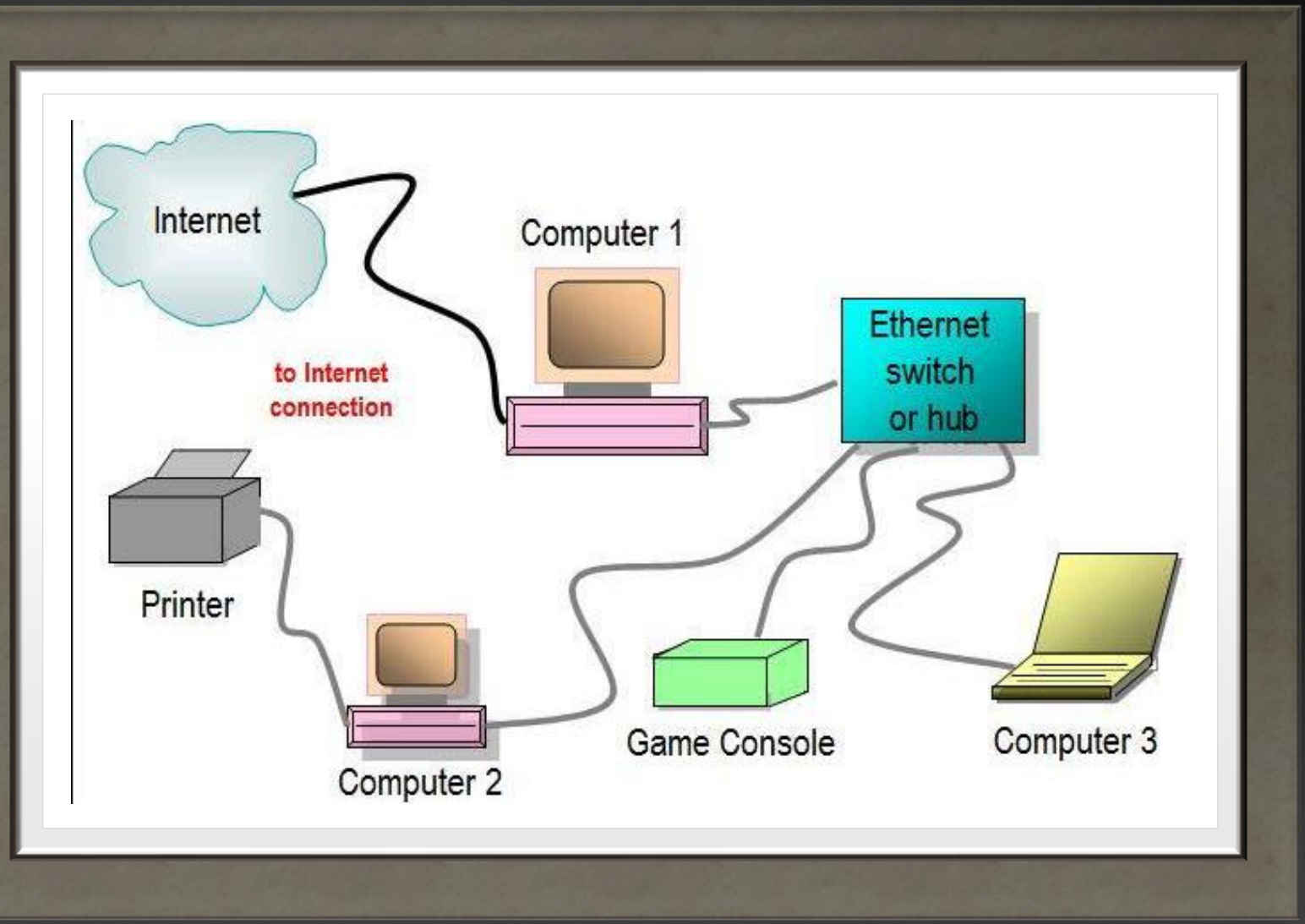
Hardware: The cellular, WiFi, and GPS radios, storage media, camera, processor, memory, display, etc. Device can be identified by IMEI, serial number, and MAC addresses.

Subscription: A SIM card, identified by an IMSI number, is typically used to authenticate a device to connect to a wireless carrier's network.

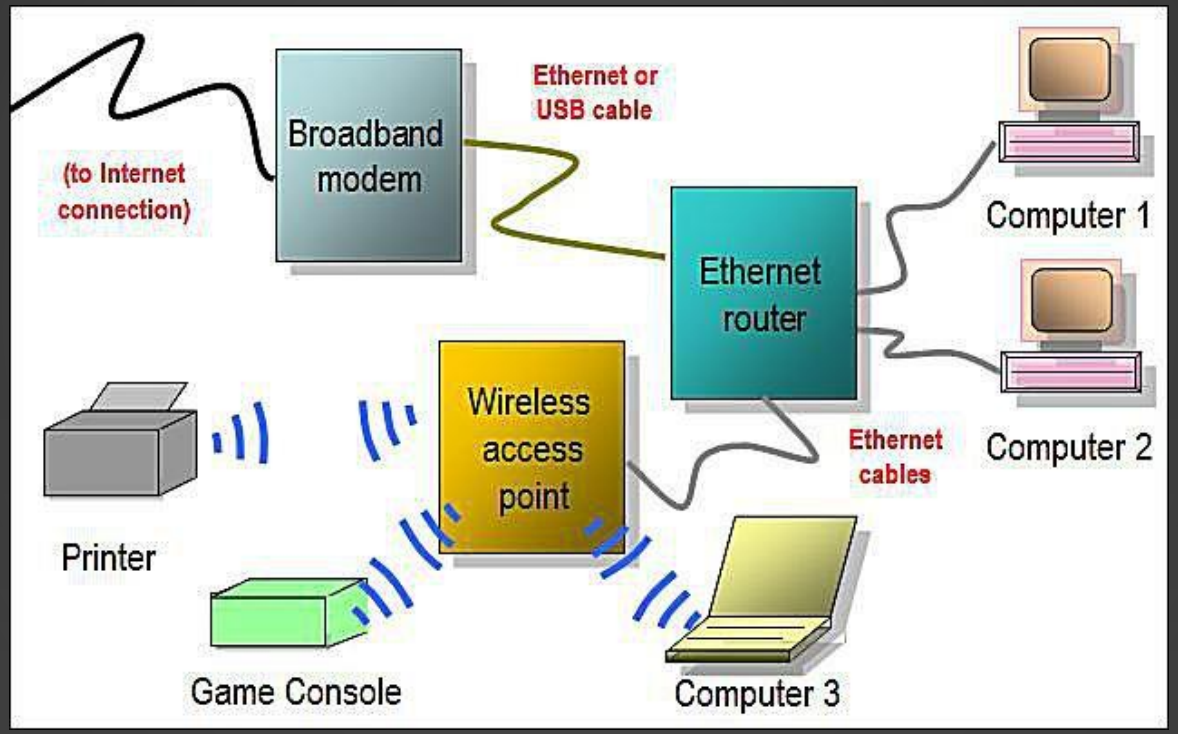
Connectivity: Cell phones use a variety of technologies to wirelessly connect to external networks or services. Cellular, WiFi, Bluetooth, GPS, and NFC technologies all use types of radios to search for, connect to, and communicate with connectivity points.

Unique identifiers associated with each of these radios can be transmitted without encryption and, when that occurs, users are left vulnerable to passive tracking of their devices' identifiers and correlated physical locations.

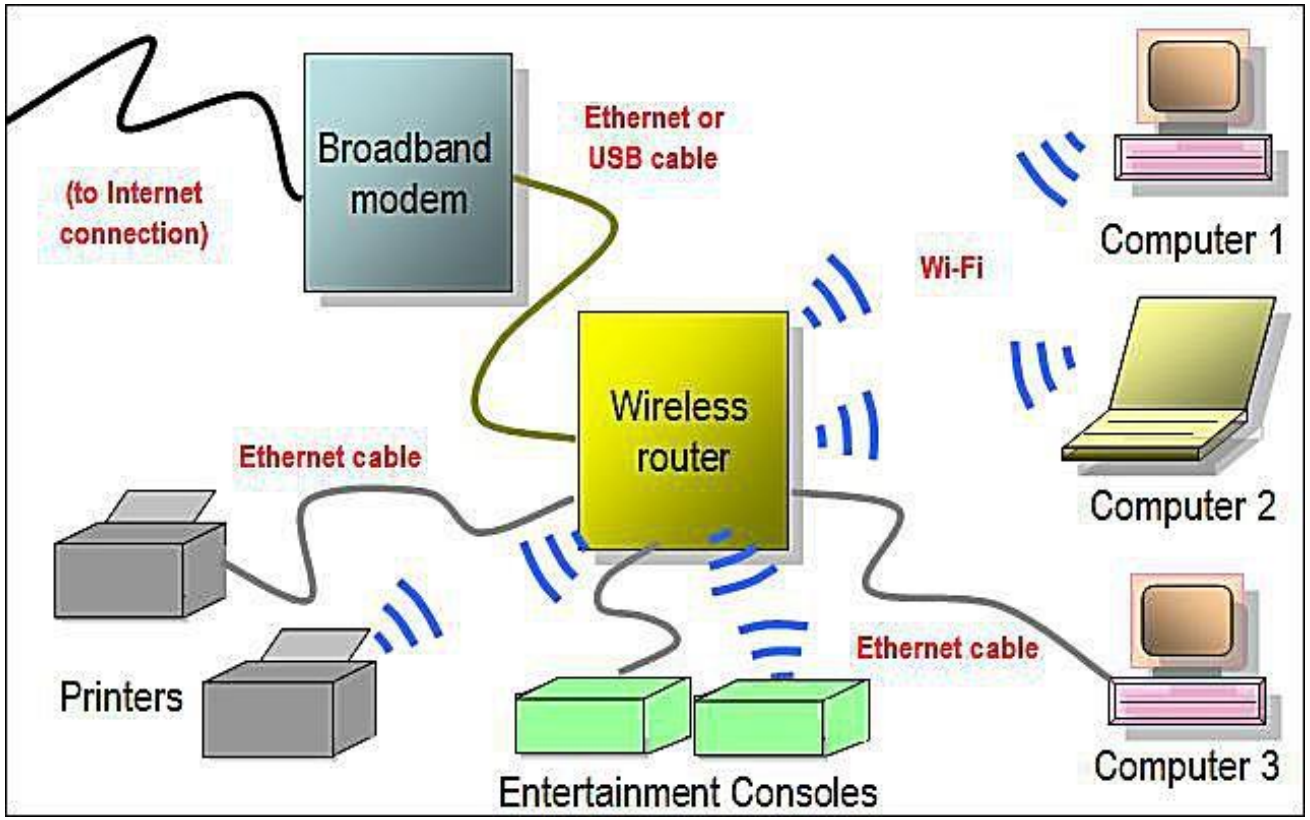
ETHERNET NETWORKING



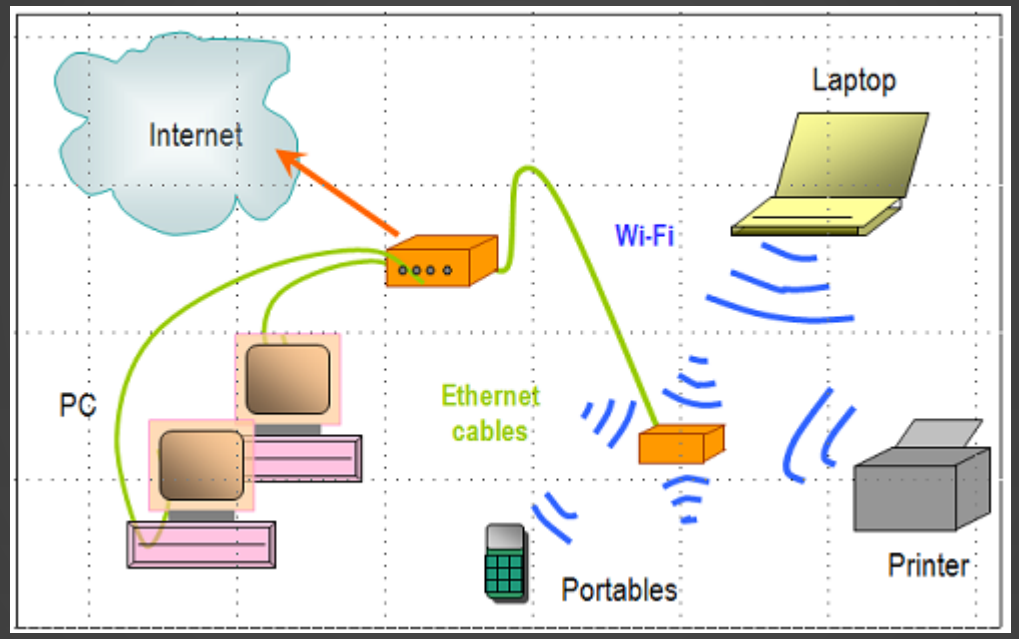
WIRED NETWORK



HOME NETWORK SWITCH AND ROUTER



HOME NETWORK



TYPICAL WI-FI NETWORK