Location Management - I

Saurabh Srivastava
Department of Computer Sc. & Engg.
IIT Kanpur

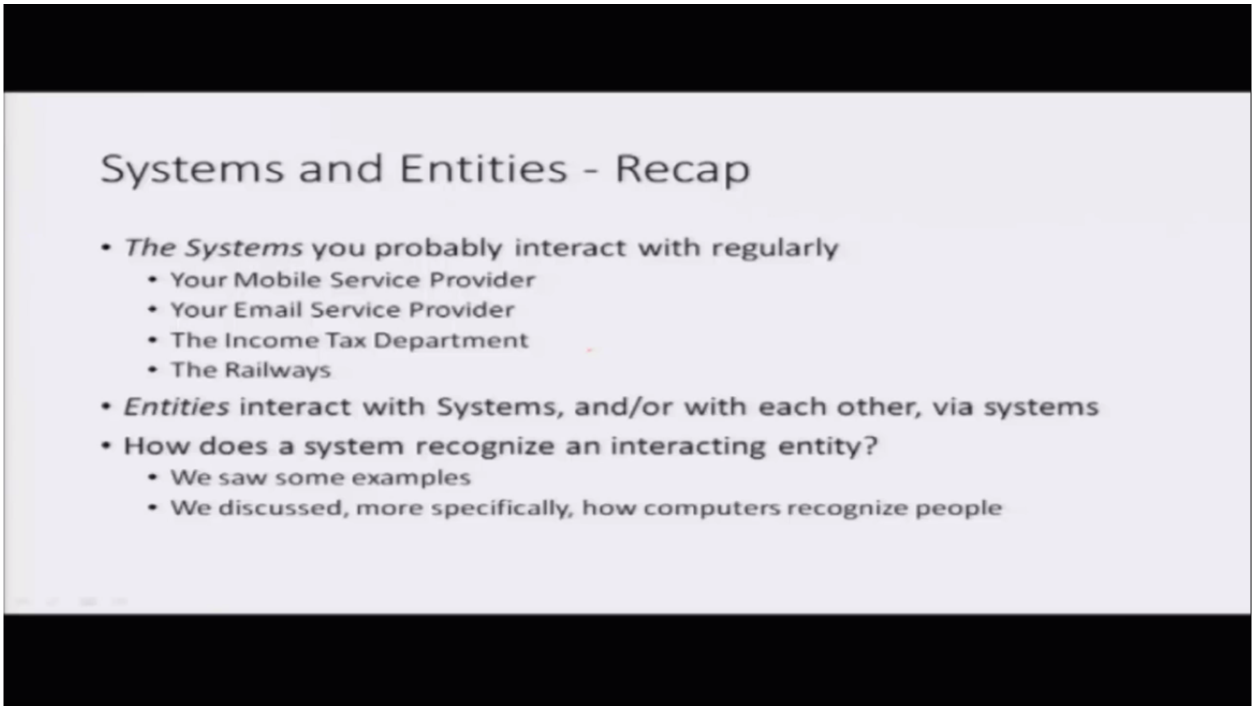
Location Management - I

Saurabh Srivastava

Department of Computer Sc. & Engg.

IIT, Kanpur

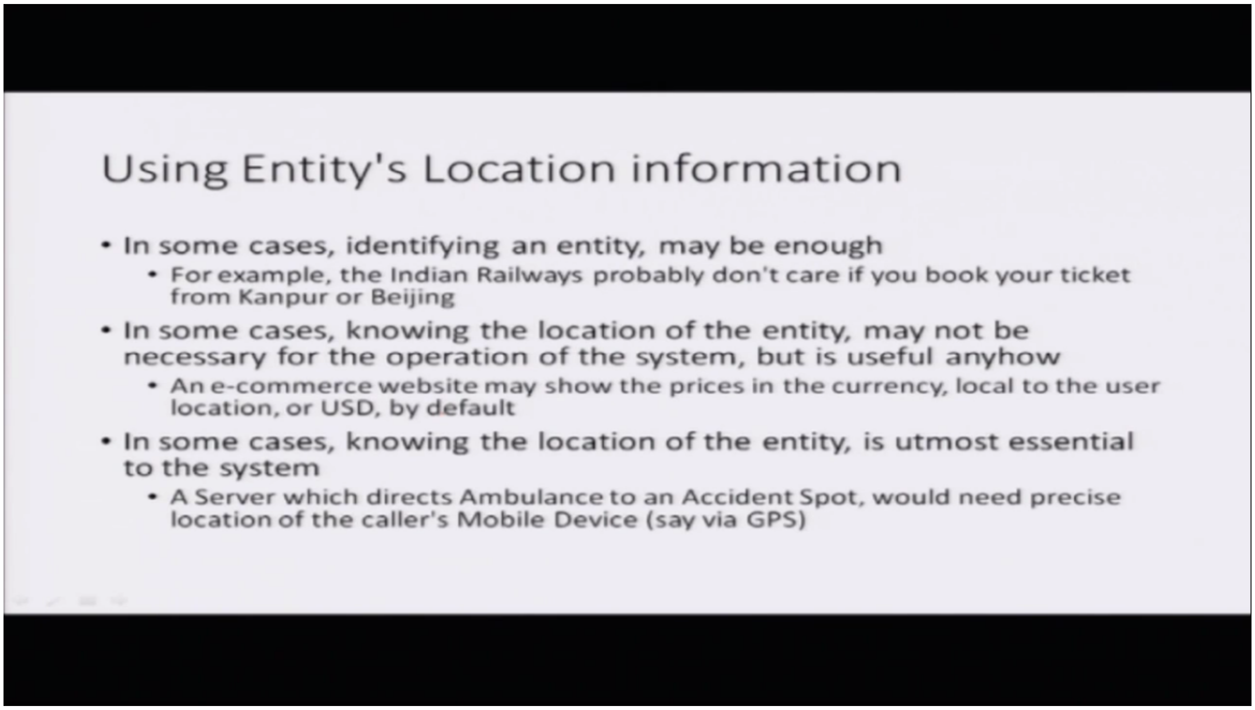
Hi, welcome back. I'm Saurabh Srivastava. I'm a PhD. scholar at IIT Kanpur. This is a lecture it is actually a two-part lecture on location management. We've already had a lecture on identity management. In this part we'll have a look at the devices and techniques that are used in location management. In the next part we'll have a look at how identity of an entity can actually be mapped in some cases to its location.



Systems and Entities - Recap

- *The Systems* you probably interact with regularly
  - Your Mobile Service Provider
  - Your Email Service Provider
  - The Income Tax Department
  - The Railways
- *Entities* interact with Systems, and/or with each other, via systems
- How does a system recognize an interacting entity?
  - We saw some examples
  - We discussed, more specifically, how computers recognize people

So let's start so we start with the brief recap of what we did in the identity management lecture. So in short consider systems to be computers we interact with in routine life and we gave examples of mobile service providers and we took examples of the email service provider. We took examples of Railways, the IRCTC. So entities are those which interacts with systems. So basically human beings, devices these are all entities and the systems are like servers and telephone exchanges; these are servers. We saw some examples. We discussed some very specific way in which systems recognize people. So this is what we did in the previous lecture.



Using Entity's Location information

- In some cases, identifying an entity, may be enough
  - For example, the Indian Railways probably don't care if you book your ticket from Kanpur or Beijing
- In some cases, knowing the location of the entity, may not be necessary for the operation of the system, but is useful anyhow
  - An e-commerce website may show the prices in the currency, local to the user location, or USD, by default
- In some cases, knowing the location of the entity, is utmost essential to the system
  - A Server which directs Ambulance to an Accident Spot, would need precise location of the caller's Mobile Device (say via GPS)

So now we come on entity's location information. So in some cases identifying an entity may be enough. So for example the IRCTC doesn't really care if you are booking your ticket from say Kanpur or Beijing because all they need to know is who's booking the ticket and as long as you are logged in they really don't care where from you are booking your ticket. In some cases knowing the location may not really be necessary for the operation of the system but it may actually be useful. For example an E-commerce website well they can show the currency of their items either in you know US dollars by default or they can choose to change the currency with respect to the location of the user. So for example if you are logging in from India they can probably show currencies in Rupees whereas you know US dollars otherwise.

In some other cases the location of the entity is actually utmost essential for the system to work. For example you built a system which alerts ambulances to go to the location of accidents. In that cases knowing the location of the entity is extremely important. How else will the ambulance be directed? Not just this basically you can also use the location of an entity to figure out what time you have to show. For example the server time maybe say in GMT but you want to show the time to the user in IST if the user is from India. You can also apply geographic restriction on content. You may have seen the message unavailable content on YouTube a number of times because that particular video is not available for your geographic location. So this kind of filtering can also be done if you actually are aware of the user's location.

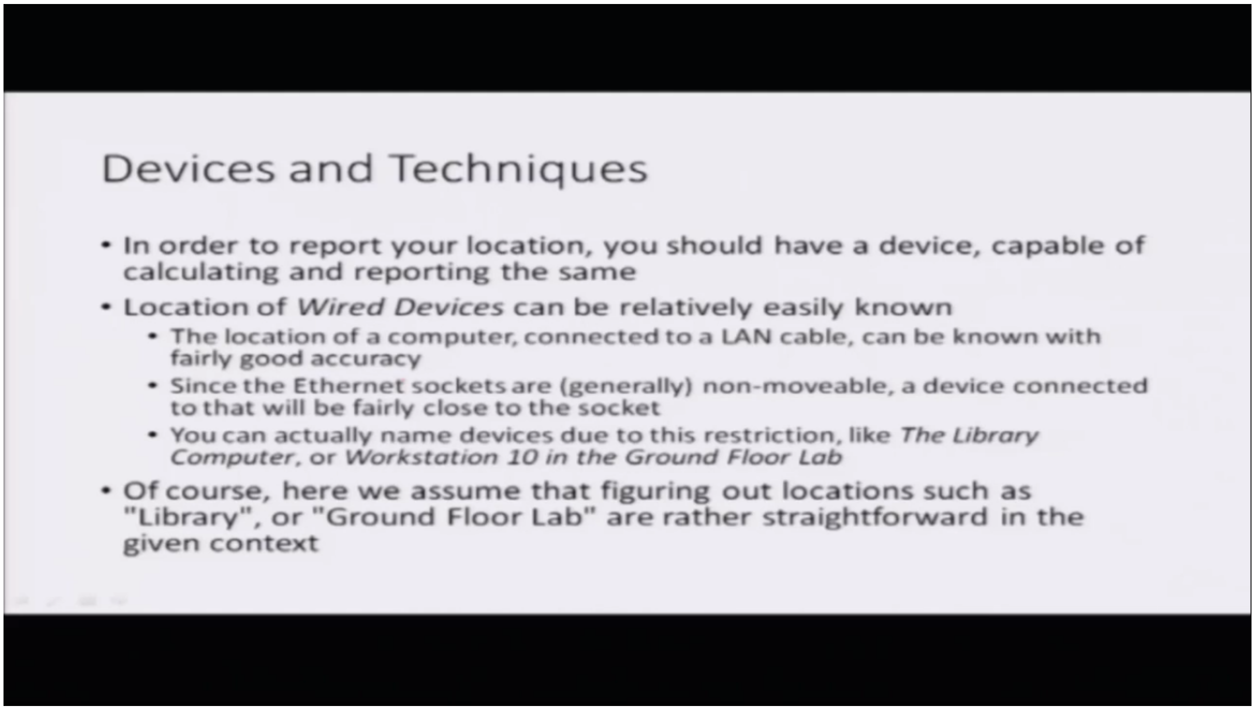
The location information we saw in the identity management lectures that this can actually be used for figuring out some kind of malicious activity. We talked about how if a person is logging in from Kanpur every day and then the same person logs in from Beijing all of a sudden then the system can get suspicious of this and you know they can probably take some further actions trying to figure out what is happening. Then there are some services which are actually based on location itself. For example the map services and the navigation apps these are services which actually require your location. They are actually built on the phenomena that your location is available to the system. Then there are apps which can give you alerts of traffic where traffic is there. You don't go via those routes where there is too much of traffic.

Then there can be other applications like finding hotels, shopping malls, that are just nearby your current location. So basically there are a number of ways in which the entity of a user can actually be used by a system.

Determining Entity Location

Devices, Techniques, Addresses

So we now know that the entity of the user is actually something that a system may want, sometimes the system may actually rely on it but there has to be some ways by which these kind of information can actually be acquired by the system. So in this lecture what we will have look at is devices and techniques which can enable a system to figure out a particular identity's location.



Devices and Techniques

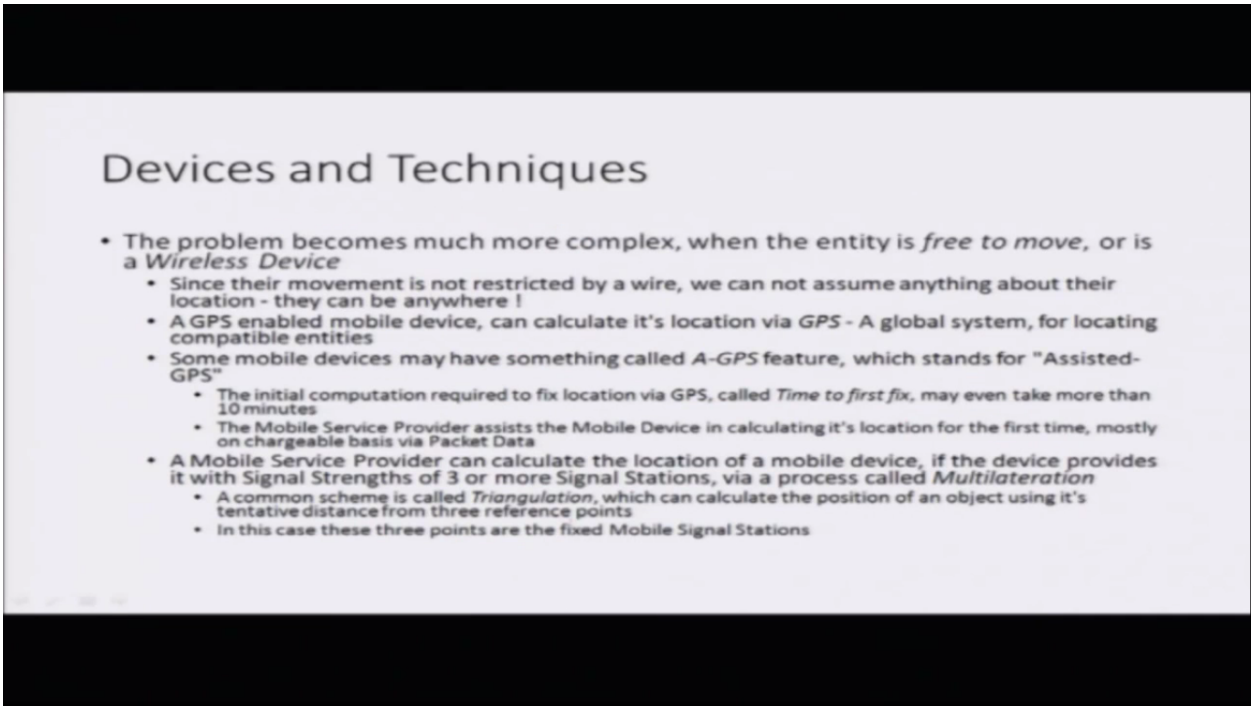
- In order to report your location, you should have a device, capable of calculating and reporting the same
- Location of *Wired Devices* can be relatively easily known
  - The location of a computer, connected to a LAN cable, can be known with fairly good accuracy
  - Since the Ethernet sockets are (generally) non-moveable, a device connected to that will be fairly close to the socket
  - You can actually name devices due to this restriction, like *The Library Computer*, or *Workstation 10 in the Ground Floor Lab*
- Of course, here we assume that figuring out locations such as "Library", or "Ground Floor Lab" are rather straightforward in the given context

So that in order to report your location a device must be capable of calculating and reporting its location. That's the fundamental thing. It must be able to report its location and there has to be some way by which the location can be computed locally on the device. Now location of wired devices is relatively easily known because the location of a computer for example connected to a LAN cable is relatively fixed with respect to the LAN socket to which the computer is connected. It is because wire devices cannot really be moved around beyond certain distances. So since the Ethernet sockets are generally non movable a device connected to that will be fairly close to the socket right. You can actually name devices on the basis of these restrictions. For example you can call a computer to be the library computer or or say workstation 10 in the ground floor lab. All these things are possible because the location of these systems are fairly restricted. They cannot really move beyond a certain level. So of course we are assuming that figuring out where that library is or where the ground floor lab is is significantly easier. So that is what we are assuming here. The problem becomes much more complex when the entity is free to move. So basically the entity is actually a wireless device because wireless devices can actually move well anywhere. They can be present anywhere. Figuring out their location is a little more tricky.

So we'll have a look at how these devices generally compute their location and then send it to the servers. So the most common way is via GPS. So GPS enabled mobile devices can calculate its location via GPS. GPS basically is a Global Positioning System. Any compatible entity can communicate with satellites and with the help of these satellites the entity can actually figure out where it is right now on the earth. Some mobile devices also have a feature called AGPS which is called actually Assisted GPS. So the reason that Assisted GPS is actually a technique which is very common is to the initial computation required to fix the location of the device for the first time it is not very easy. It requires locking of satellites and solving some very cryptic equations. So the initial time the first time when you try to get your location via GPS may actually increase even beyond 10 minutes. So some mobile service providers assist the mobile devices in calculating their locations for the first time and this is mostly done via these data packets. You may have used GPRS for this stuff. So some mobile service providers provide assistance to mobile devices in order to be able to calculate their location.

Now this was using satellites and with the help of a mobile service provider. The mobile service provider itself can calculate the location of a particular device by a technique called multilateration.

So multilateration is based on this phenomena. If a device is getting signals from more than three cell towers and it just records all the signals and send it to the mobile service provider, the mobile service provider can actually calculate the location of the mobile device based on the fact that the farther the cell tower is the weaker would be its signal at the mobile device. So if I have say three or more devices three by the way are minimum you won't be able to fix the location in less than three cell tower locations but yeah if you've got three or more then you can fix the position of a mobile device using something called triangulation. Basically this involves solving some trigonometric equations and all that stuff.



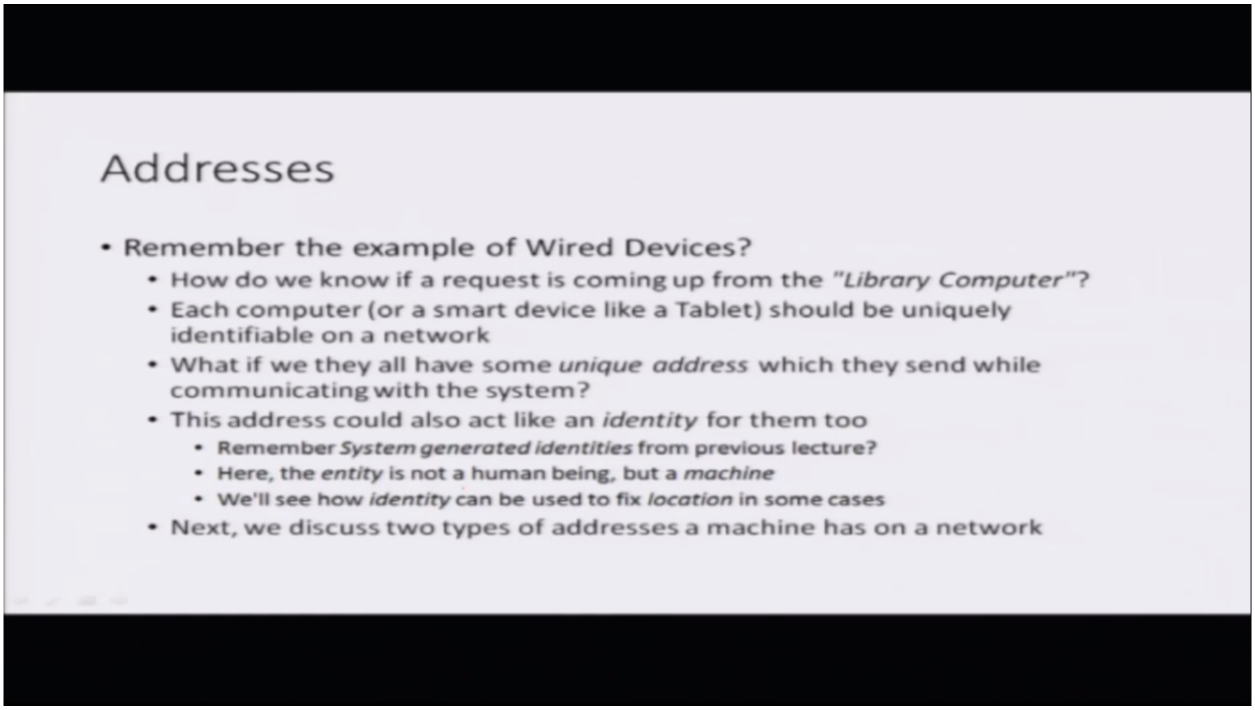
Devices and Techniques

- The problem becomes much more complex, when the entity is *free to move*, or is a *Wireless Device*
  - Since their movement is not restricted by a wire, we can not assume anything about their location - they can be anywhere !
  - A GPS enabled mobile device, can calculate it's location via *GPS* - A global system, for locating compatible entities
  - Some mobile devices may have something called *A-GPS* feature, which stands for "Assisted-GPS"
    - The initial computation required to fix location via GPS, called *Time to first fix*, may even take more than 10 minutes
    - The Mobile Service Provider assists the Mobile Device in calculating it's location for the first time, mostly on chargeable basis via Packet Data
  - A Mobile Service Provider can calculate the location of a mobile device, if the device provides it with Signal Strengths of 3 or more Signal Stations, via a process called *Multilateration*
    - A common scheme is called *Triangulation*, which can calculate the position of an object using it's tentative distance from three reference points
    - In this case these three points are the fixed Mobile Signal Stations

So the next thing we are going to have a look at some addresses. So we actually considered the example of wired devices. We said that if a computer is say connected to a socket in library we can tell its location with the help of that particular socket itself. So a device connected to the library socket is say library device but how do we know which socket is connecting to the network from the library. So there has to be some way to figure out what that particular socket is. So each computer or say in our case we are talking about sockets right now they should be uniquely identifiable on the network. So what if we all have some unique addresses with the help of which the system can actually identify a particular device. Again we are talking about wired devices right now. So when we are saying being able to identify a device we are basically saying being able to identify say LAN socket.

So the address should act in some ways which is similar to what we call identity in our previous lecture. So human beings have identities. With the help of the identity you can be recognized. So now what we are talking about is identity for systems. We now want to have identities for systems with the help of which devices can be identified on a network.

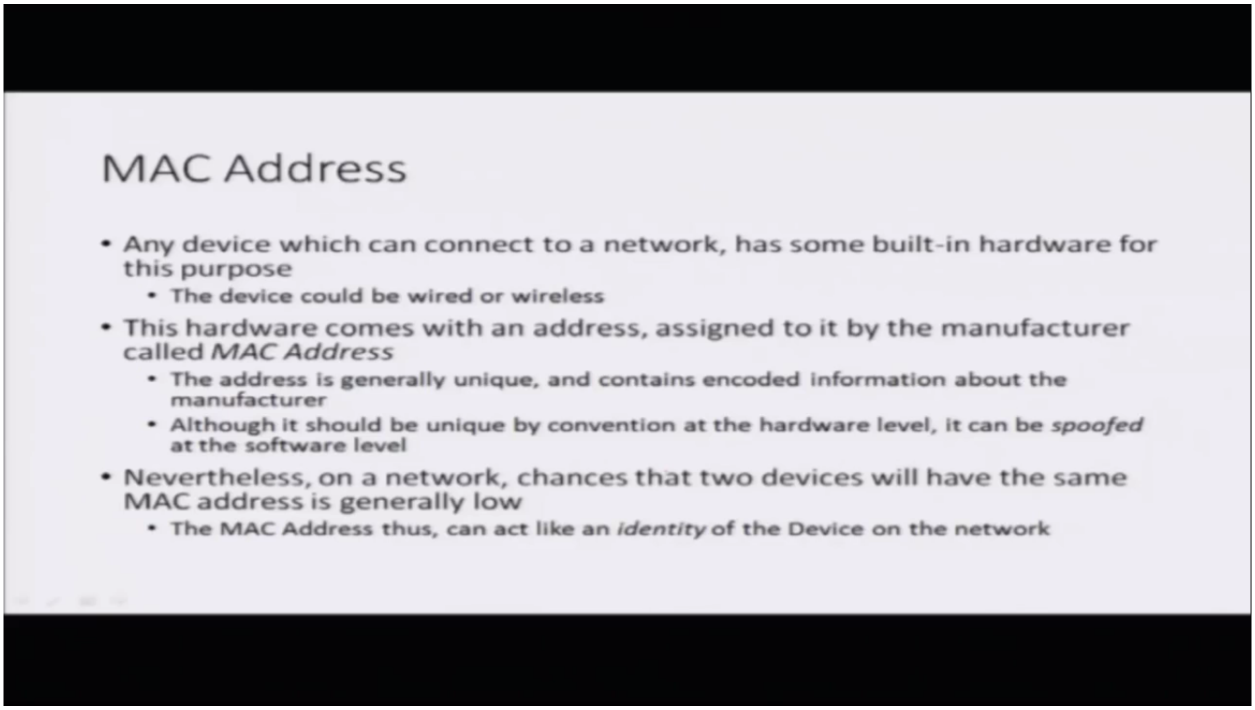
So we talked about system generated identities in the identity management lecture where we talked about a username and password and OTPs. So we now need to find out something like this for a machine. Earlier it was a human being now we won't need to find out identity for a machine. So we will just see how in some cases this identity can actually be mapped to device's location. Yes in some cases we can map the identity to location. So we will discuss these things next but before going doing that we will discuss two types of addresses. So these addresses are going to be the identities we are going to associate for the device and after discussing these addresses we'll have a look about how this can be mapped to a location.



Addresses

- Remember the example of Wired Devices?
  - How do we know if a request is coming up from the *"Library Computer"*?
  - Each computer (or a smart device like a Tablet) should be uniquely identifiable on a network
  - What if we they all have some *unique address* which they send while communicating with the system?
  - This address could also act like an *identity* for them too
    - Remember *System generated identities* from previous lecture?
    - Here, the *entity* is not a human being, but a *machine*
    - We'll see how *identity* can be used to fix *location* in some cases
  - Next, we discuss two types of addresses a machine has on a network

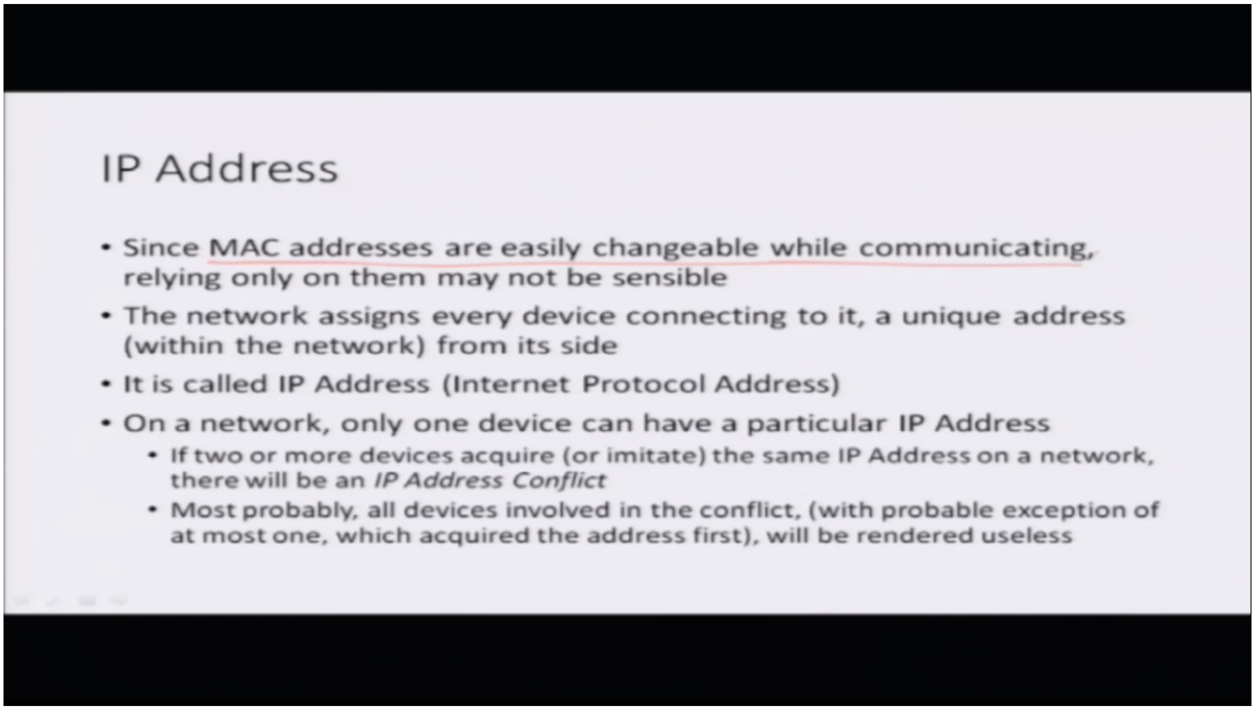
So the first thing is we will talk about MAC addresses. So MAC addresses are something that are built in a particular device. They are built in by the manufacturer of the device. So for example if you are having a laptop it may have a network interface card and that network interface card was built by some manufacturer. That particular manufacturer encoded some information in the hardware itself. That particular information is the MAC address. So the hardware comes with an address assigned to it by the manufacturer. This is called Mac address. The address is generally unique. Let me just point out that I don't think so there are any legal issues with it. So if a manufacturer actually sends out devices with duplicate MAC addresses there isn't I don't think so there is any kind of legal obligations but yeah in general you'll find all the MAC addresses to be unique the problem though is that even though by convention at the hardware level it is unique it can be easily spoofed at the software level. This is the problem. So even if the manufacturer is good even if the manufacturer is actually producing devices which are having unique MAC addresses it can actually be spoofed at the software level. So well anyhow nevertheless on a network the chances that two devices will have the same MAC address is generally low and thus we can actually consider the MAC address to be an identity of a device.



MAC Address

- Any device which can connect to a network, has some built-in hardware for this purpose
  - The device could be wired or wireless
- This hardware comes with an address, assigned to it by the manufacturer called *MAC Address*
  - The address is generally unique, and contains encoded information about the manufacturer
  - Although it should be unique by convention at the hardware level, it can be *spoofed* at the software level
- Nevertheless, on a network, chances that two devices will have the same MAC address is generally low
  - The MAC Address thus, can act like an *identity* of the Device on the network

Another more interesting address that we will talk about are the IP addresses. So since MAC addresses are easily changeable while communicating relying only on them may not really be a sensible idea. We are trying to identify a device and if it is possible that two devices can have the same identity then well it may not be a good idea to just rely on them. So the network assigns every device that is connecting to it a unique address. Now this address is assigned by the system. So currently we are assuming that our system is the whole network; all the software, all the hardware, the service everything we are calling it as a system. So a particular device is connecting itself to the network means that it is now connecting itself to the system.



IP Address

- Since MAC addresses are easily changeable while communicating, relying only on them may not be sensible
- The network assigns every device connecting to it, a unique address (within the network) from its side
- It is called IP Address (Internet Protocol Address)
- On a network, only one device can have a particular IP Address
  - If two or more devices acquire (or imitate) the same IP Address on a network, there will be an *IP Address Conflict*
  - Most probably, all devices involved in the conflict, (with probable exception of at most one, which acquired the address first), will be rendered useless

This address is called IP address. Basically it is called Internet Protocol address. We will not go in detail of what Internet Protocol is but just for the understanding IP addresses are unique. So if two or more devices acquire the same IP address on a network well there will be an IP address conflict.

Now we saw that it is possible that two devices can have the same MAC address. So similarly it is possible that you know add software level someone spoofed someone else's IP address but the problem is that in such a case most probably all devices involved in the conflict well sometimes the system may actually leave the first device to acquire that IP address but it is possible that it actually punishes all of them who are trying to portray the same IP address and so the system will actually kick them out and they'll be rendered useless on the network.

So this is a uniqueness about IP addresses that the system takes care of the fact that no two devices with the same IP address would be present on the network simultaneously.

So this is the end to our first part. We will have a look at the second part of the lecture now. In that part what we have a look at is how these identities can actually be mapped to locations.

Thanks.