Types of Networks

Introduction

This section covers the reading material in Chapter 1 of Tanenbaum Sections 1.2 *Types of Computer Networks*, 1.3 *Network Technologies from Local to Global*, and 1.4 *Examples of Networks*, pages 7–47. Tanenbaum tends to concentrate on the differences, rather than the similarities, and often the differences that don't matter. In many cases, unless the term refers to the media, these are sometimes more marketing terms than ones of technical significance. It is important to be able to think clearly about these things. This lecture is more a commentary on the text, so the student should read the text noted above before starting.

Now that you have read the text. Let's get started (following the section numbers from the book).

Types of Networks

Tanenbaum starts off listing the types of networks:

1. Mobile and broadband access networks – Networks used to access the Internet. Lumping mobile and broadband together is a bit strange.
2. Data-center networks – Networks used within data centers. These should be organized as an MIMD supercomputer, but most aren't. Tanenbaum describes them as "networks that house data and applications." I have no idea how a network "houses" anything.
3. Transit networks – Networks that connect access networks to data centers. Tanenbaum is making a big error here in characterizing networking as only client/server, characterizing networking in much the same terms as those that would be used to characterize IBM's SNA 50 years ago, i.e., not distributed computing.
4. Enterprise networks – Networks used on campuses, in office buildings, or at other organizations. The only difference here is that there is generally single ownership. (But even in a corporate network that is not that large, single ownership is not likely to be the reality.) This category is basically the first three categories on a smaller scale.

A Reminder

Before we go any further, lets remind ourselves of what we said in the first lecture of Module 1: What *Really* Characterizes Networks?

The characteristics of the media create bounds:

- Point-to-point or multi-access
- Physical limits on distance
- Error characteristics – Single-bit or burst errors, affects on packet size, etc.
- Bandwidth/capacity
- If wireless, what are the propagation characteristics?
- Cost, cost, cost

Then it is a Resource Allocation Problem.

- To this, let us add:
    - Number of elements
    - Distance limitations

Why? These characteristics contribute to issues of scaling and the policies required for the time constants in the feedback mechanisms that the network will have to deal with.

What is *really* important?

Network technologies should not be built to support specific applications. Network technologies support a specific operating range. Applications require a particular operating range. Some applications require different ranges, and some may require the same range. The problem in designing a network or the equipment is to match the operating range of the equipment to the operating range of a collection of applications. Don’t believe what management tells you.

We talked about this before and it applies here too, but in a somewhat different way. Before we used it in the sense of management-proofing code. But it applies equally well in managing the operations of a network. The boundaries between these categories are not sharp, especially if the category is not based on the physical media and, even then, it may be market motivated. Although here, it is from the other side. Once the changes, including expansion, have been determined, circumstances can change.

Keep in mind, that the categories that Tanenbaum covers are not sharp or well-defined, and even the terms that may refer to physical media may turn out to reflect political or market preferences. Remember, these categories can also be blinders that keep one from seeing what is really going on. One has to see through the hype to what is really important. We will see examples of that.

Even though we have not yet gone through the details of protocol design, as we describe the various types of networks, consider how the differences might be manifested in a real network or how they might not be. Not is just as important.

Even though we have not yet gone through the details of protocol design. As we describe the various types of networks, consider how the differences might be manifested in a real network or not. Not is just as important.

Broadband Access Networks

Notice that Tanenbaum doesn't define what broadband is. If one googles, "What is the definition of broadband?" one gets the following from Oxford Languages: "a high-capacity transmission technique using a wide range of frequencies, which enables a large number of messages to be communicated simultaneously." When we cover the Physical Layer, broadband means that the modulation is across a wide range of frequencies. As an example, 56 Kbps over a phone line of 4 kHz is narrow band, but over coax or fiber, it would be broadband. If one digs more, one finds the odd distinction that, at least for some experts, wireless broadband does not include WiFi, even though the data rates are comparable. For them, the distinction seems to be more a question of what standards committee developed it.

The only category Tanenbaum notes here is home networks, and he really doesn't say much about broadband other than to cite Metcalfe's Law that the usefulness of a network is proportional to the square of the number of users and list some of the media types that will be found in home networks. (He leaves mobile to later.) Clearly, this is not based on precise definitions, but meant to capture the benefit of anyone being able to talk to anyone else and the ideas that can be exchanged that way.

One of the major issues now in the United States is getting broadband coverage for everyone. The use of the Internet has become so important as to be considered a necessity, like electricity and the telephone. There seems to be an attitude coming out of Silicon Valley that the norm there is the norm everywhere, both in terms of access and affordability. And not just access, but broadband access, which has become so integral to all aspects of society that not having broadband creates a real divide between the haves and the have-nots.

This isn't so much a problem of low income, although in some places that is definitely one aspect of it, but more rural vs "urban." Again, the concept of "rural" to many on the coasts means towns of several thousand. This is not rural, not even for towns of several hundred. Rural is when neighbors are a kilometer or more apart.

That said, there are towns that don't have broadband access because of their remoteness. Even in the lower 48 of the United States, there are places that can be very remote. (In the 1980s, I knew people who were associated with the National Rural Electrification Administration (NREA), formerly the New Deal REA, now the NRECA. "Cooperatives" were added to the name.) Even at that late date, they were announcing towns in the lower 48 that were getting electricity and telephone for the first time.) The problem is one of cost and distance and sometimes geography, e.g., mountains.

Mobile and Wireless Access

This is an odd title for this section. Do you think there are mobile networks that aren't wireless? Note that while wireless and mobile are related, they are not the same thing. We will discuss 802.11, or WiFi, in more

detail a bit later. For now, its advantage (as you are well aware) is avoiding the need for wires in a local environment. It is a wireless access technology that assumes that “hot spots” (wireless routers) are connected to a wired network. While it can support the movement of devices in a large WiFi network, it isn’t intended for mobility over large distances.

I generally contend that mobile computing or mobile applications is somewhat of a misnomer. There are very few applications that one only does when mobile. Most might very well be done at a desk as well. Even finding the nearest X. One might do that at one’s desk before going out. If there are real defining characteristics of “mobile computing,” they would be limited screen size and battery life. Tanenbaum does give some examples of truly mobile applications; I recommend reading about them.

Most (if not all) cell phones now have GPS. This became a requirement, as more and more people no longer had a wired telephone. This made it more and more difficult to locate someone when there was an emergency (911) call. A 911 call from a wired phone gives the dispatcher the street address of the caller, regardless of whether the caller does. Triangulating a cellphone signal does not provide sufficient resolution to find someone quickly in an emergency.

This has also created a requirement that places that previously didn’t have addresses now have addresses. A few years ago, Hiawatha Bray of The Boston Globe, in his book, *You Are Here: From Compass to GPS, the History and Future of How We Find Ourselves*, explained how the response to the Ebola epidemic a few years ago was made more difficult because some city areas did not have street addresses. It is hard to send an ambulance to someone without an address. High-tech efforts were underway to bring street addressing to these areas. Bray noted how important something we all take for granted was, with the implication being that what was commonplace in developed countries was rare or non-existent in the developing world, and for the most part that is true.

However, we should not feel so superior. The house I grew up in (where my brother now lives) in a town of 900 in Southern Illinois did not have a house address until 1996, and only got one then because the county converted to E911. Out in the country (the land not in any town), roads that had never had official names had to be named. You can imagine how controversial it became when a consulting company created a name for a road, and the residents were irate, because they had local names that had been used for generations. “What are you talking about? That has always been Garrettville Rd. (Several Garretts lived on it.) But even this can be flawed. Often the GPS coordinates associated with the E911 address are at the mailbox, which may not be on the house but a kilometer down the road along with several other mailboxes at a corner with the “main” road.

Mobile and Wireless Access Networks (2 of 3)

Wireless	Mobile	Typical Applications
No	No	Desktop computers in offices
No	Yes	A laptop computer used in a hotel room

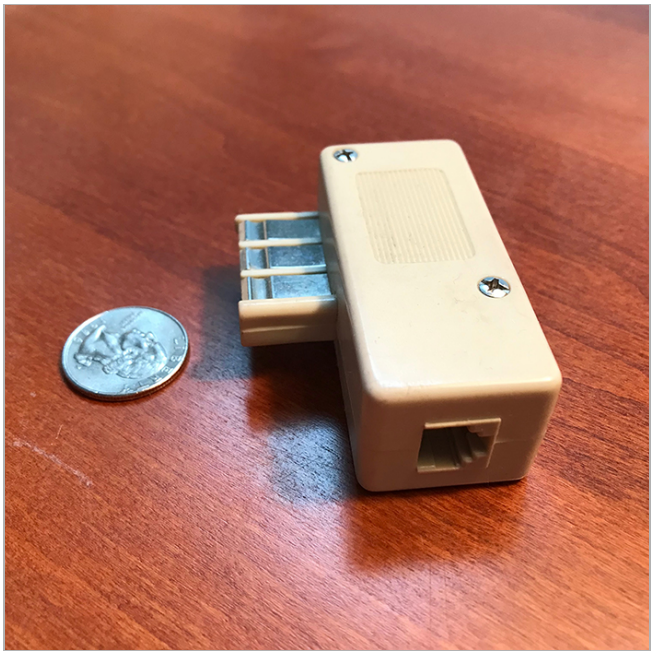
Yes	No	Networks in unwired buildings
Yes	Yes	Store inventory counted with a handheld computer

Although wireless networking and mobile computing are often related, they are not identical.

This table is woefully out of date. I would expect that most desktop computers in offices are connected by WiFi. I haven't been in a hotel in many years that didn't have WiFi.

Gone are the days when we carried a small bag of different national connectors for dial up, thank goodness. I remember one meeting we had overseas where the hotel didn't have a socket for a data connection. Some attendees actually disassembled the wall socket for the phone and re-wired it. The hotel was not happy. My favorite was the official French equivalent of an RS-232, which was huge and had contacts that looked like they could handle 100 amps!

RS-232 Socket



The French converter for access to dial-up over twisted pair to a US RS-232. For contrast, note the RS-232 socket on the end.

M-Commerce vs. E-commerce

M-commerce is the kind of distinction for the sake of distinction that I complain about, more for marketing hype than substance. Is there a difference between m-commerce and e-commerce? Not really. There is really no difference between buying something online from your phone, your tablet, your laptop, or what

have you. Is it “m-commerce” when you buy something on your phone sitting in your living room versus in a taxi on the way to a hotel in some other city? Other than the latter being more error-prone and less secure, not really. Interestingly, Tanenbaum contends that mobile users are more likely to pay for something than Internet users who expect things to be free. I am not sure I agree with this. Offering services for free is a calculated business decision. Or is this more sociological phenomena that people are more thoughtful sitting at a desk and more impulsive when not? M-commerce by its very definition implies paying for something. Again, this is the kind of off-the-cuff thinking that may obscure important implications.

Sensor Networks

Near-Field Communication (NFC) and other RFID technologies are very interesting. Previous editions of the book covered them in some detail, but that section is not in this edition. I have kept the slides so we can say a few words about the technology.

Sensor networks are being deployed for a myriad of applications. I have to say that the applications and what can be done with them, are more fascinating than the networks that support them.

As we will find later, the mobile communication industry does not understand mobility and has made the problem easily 100 times more complex than necessary. We will find that if the architecture is done correctly, nothing special is needed for mobility. The only difference between mobile and non-mobile is that the attachments to the network changes more frequently.

Content Provider Networks

As you will notice, there is not much to say about Content Provider Networks. This is a case where machines are very close together: tens of thousands of machines in a single building. This makes for short feedback loops, but it can make for truly topological routing and avoid the need for routing algorithms. The one thing I have found odd about data centers is that they seem to be organized like big web farms, rather than like MIMD (Multiple Instruction, Multiple Data) super-computers. For content delivery that probably makes sense, however for so-called cloud computing where one would expect a wider range of tasks, it doesn’t.

Transit Networks

There is not much to say about Transit Networks either. They are simply wide-area networks, as are most of the networks that make up the Internet. There is nothing technically different. What is unique is their business strategy and how they make money.

Enterprise Networks

In terms of networks (and the size of the enterprise), these networks are essentially Internets in the small to support the operation of the enterprise. For larger enterprises, which need to support multiple sites, the enterprise network may use the Internet to link different sites but require VPNs (Virtual Private Networks) to create a secure internal environment. A major part of an enterprise network support is resource sharing. There is a hodge-podge of applications to support this. It is unfortunate that USING was shut down in 1974, because it could have developed a rational approach to this requirement. A major requirement would be the support of Quality of Service (QoS) for the different applications. It is interesting how in less than 50 years, voice has gone from a high-bandwidth application to a minimal-bandwidth application while maintaining strong requirements for low jitter. In the limited environment of an Enterprise Network with limited traffic for multiplexing (not in volume but in kind), VoIP may require a separate network or dedicated resources to meet its required QoS.

Much more about these types of networks, Sensor, Content-Provider, Transit, Enterprise if they were characterized in terms of the ranges of QoS, they require. However, that work has never been done. It is better for sales to not be too specific.

Network Technologies from Local to Global

Personal Area Networks

This is primarily a category for short range (3–4 m), high data-rate wireless. Bluetooth is mentioned here and we will talk about it in more detail later. But it is a good example of how solving a problem turns into the problem disappearing. Initially, one of the main arguments for Bluetooth was to eliminate the rat's nest of wires around one's desk that connected various peripherals to the computer, e.g., printers, disks, etc. The solution was supported by the peripherals; it turned out that one didn't necessarily want them near your desk to begin with. Having them further away was much more desirable. In other words, WiFi was better for supporting those peripherals than Bluetooth. Bluetooth had to quickly find another market and switched to being used for headphones, keyboards, the mouse, or in a car where there are other constraints that keep the devices within range. WiFi could have supported these as well, but Bluetooth had attracted some heavy supporters and investors, and with pressure on WiFi for "compatibility," it survived.

Truth be known, there is no need for Bluetooth. WiFi can do everything it does and do it more simply with fewer restrictions, many fewer special cases, and a cleaner architecture. It can even replicate the short range by simply turning down the antenna gain. Bluetooth is an example of what can happen when a lot of important companies put a lot of money into developing a technology that turns out to be inferior and

unnecessary. Just by the weight of their presence in the industry, these supporters have created a market for it. We will look at Bluetooth in more detail later and its unnecessary complexity and poor design.

Local Area Networks

Tanenbaum discusses both wired and wireless Local Area Networks. Section 1.3.2 gives an early overview of the topic, which we will take up in more detail later. WiFi seems to be taking over from wired LANs. One advantage that wired LANs have developed recently is the Virtual LAN, which has some interesting security features. But these technologies are not as different as they may appear. We have shown how to unify VLANs and WiFi with the same protocols. We will find that VLANs and WiFi are architecturally the same thing.

Home Networks

Home networks are typically small WiFi networks for the home environment. Early on, their primary purpose was to provide a family's collection of smartphones, tablets, computer, etc. with access to the Internet, a local printer, and possibly a back-up disk. But that has begun to expand rapidly to access to the TV, doorbell, smart assistants (Alexa, etc.), control for lighting, thermostats, etc. Home automation has been around for decades, but it was too expensive and lacked a "killer app" that would bring the other things with it. WiFi provided that.

The only problem with a lot of these home IoT devices, doorbells, etc. is that they first talk to the cloud to be able to communicate with an app on the owner's phone. This brings up far too many privacy issues. Rudimentary attempts at a "home cloud" are starting to appear, but there needs to be a "home management system" that these IoT devices talk to totally within the home and that does not require talking to the manufacturer's cloud server.

Community Networks

These are not covered by Tanenbaum, but they are a very interesting development.

How many WiFi networks can you see from home?

Even in a low-density development in the suburbs, I can easily see more than 10.

Do you think the networks that you can see can also only see the same ones you do?

Not likely. They can see different ones that are beyond the range of your network access point, and those can see different ones beyond that, and so on.

How far do you think one could go relaying messages from WiFi network to WiFi network? Across a city? Across an entire metro area? How much excess

capacity is there?

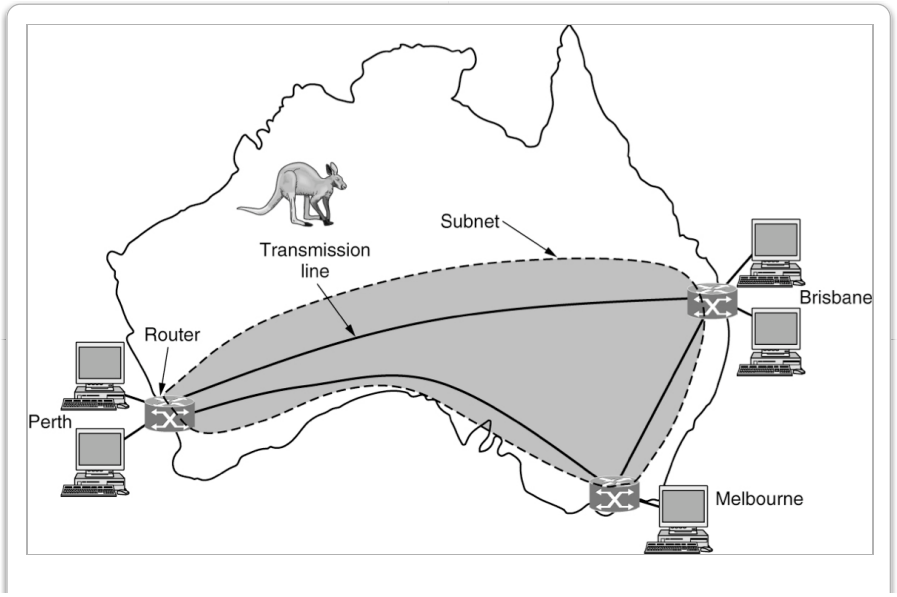
Depending on the area, it is likely pretty far. Around Boston, you can probably get from well into New Hampshire to well south of Providence, Rhode Island, perhaps as far west as Worcester? For New York, [you can get from?] perhaps New Haven, Connecticut, to Wilmington, Delaware, and maybe all the way to Washington, DC. If not, the gap isn't that large. For the West Coast, you can get from the Bay Area Richmond to Santa Cruz, perhaps to Carmel. What about the East Bay? There are areas west of Palo Alto and Mountainview where it is lost; for Los Angeles, you can go from Santa Barbara to San Clemente and, if not for Camp Pendleton, you could get to San Diego.

Groups around the world have done just this by modifying the software of WiFi access points to support this kind of routing, while also providing security to the home network, but with possible access to the homeowner's cable Internet. Groups in Urbana, Illinois, Barcelona, Athens, and elsewhere have built these. There has also been "Internet in a suitcase," a network that governments can't (easily) shut down. There has also been some very interesting work done here, and there's more to be done. (Wikipedia is a good place to start if you are interested in more information.)

Metropolitan Networks

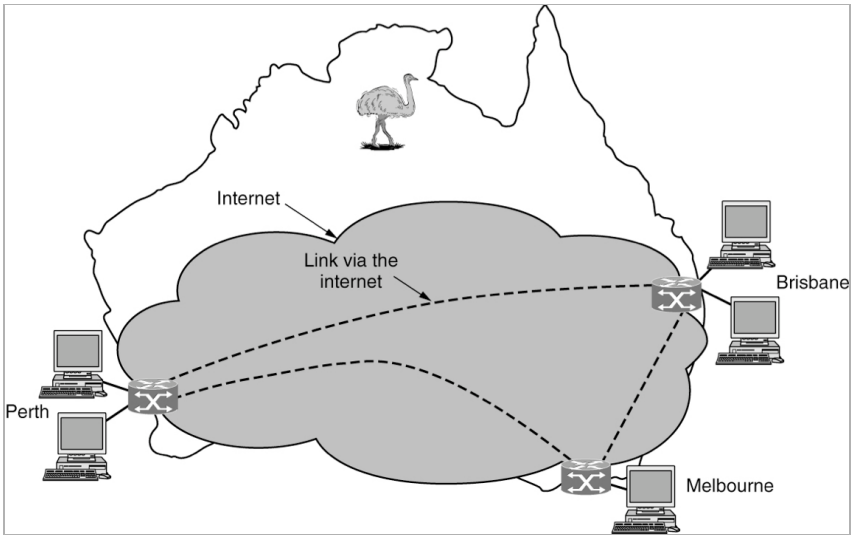
Metropolitan Networks are, if anything, a marketing term. What is depicted in the book is how early cable TV worked. This would be rare today. Major cable companies have their own distribution networks linking their area "head-ends." Satellites might be part of the network, but they don't play the central role they used to.

Wide Area Networks



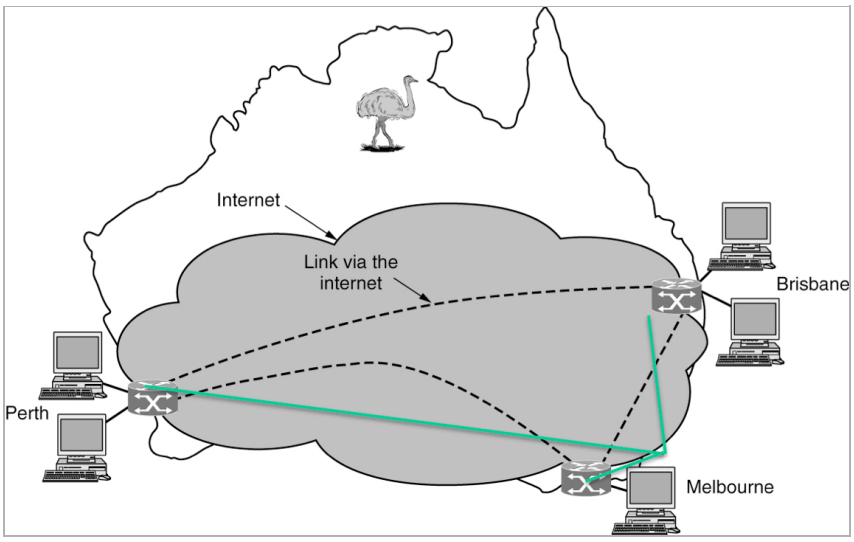
Source: Tanenbaum, A., Wetherall, D., & Feamster, N. (2020). *Computer Networks* (6th ed.).

Wide Area Networks are, for the most part, private networks possibly using Internet technology or perhaps older technologies, such as Frame Relay or ATM. What is illustrated here is a private company leasing lines to connect three metropolitan areas in Australia.



Source: Tanenbaum, A., Wetherall, D., & Feamster, N. (2020). *Computer Networks* (6th ed.).

In this figure, Tannebaum shows that the leased lines could be replaced by the Internet and probably save a lot of money. However, one must be careful. All may not be as it seems. Just because it appears as the Internet and the subnet is drawn as a cloud encompassing all three cities doesn't mean that that's whole story.



Source: Tanenbaum, A., Wetherall, D., & Feamster, N. (2020). *Computer Networks* (6th ed.).

The actual configuration of lines may be a star network with a single point of failure in Melbourne. No wonder it is cheaper!

This can actually happen. The reason that the New York Stock Exchange (NYSE) was shut down for a week after 9/11 was because of exactly this sort of situation. NYSE was up and able to be on the Internet. They had redundant lines. However, the major brokerage houses were not up on the Internet.

Did they not have redundant network connections? They did. They were paying for more than one line to their corporate networks. They had taken Verizon at its word that they were redundant. However, they had not gone the extra step and made Verizon show them the actual physical paths of the lines. As it turned out, they had been paying for redundant lines that all went through the same switching center at the base of the twin towers, which had been destroyed. NYSE, on the other hand, had made Verizon show them physically where their lines were and that there were no single points of failure.

It is important to make sure the ISP is redundant when buying service from an ISP. There isn't much between Brisbane and Perth. It would be expensive to run a line all that way to just get to Perth, when one already has a line to Perth through Melbourne. But this is back to the original configuration and the ISP is probably leasing the lines. The question becomes, can the ISP run that configuration for less money than the private company in the previous slide? They have more users to spread the cost over. But will those additional users degrade the performance of the network compared to the private configuration? And will the ISP pass that savings on to the users or pocket the extra profit? The choice is far from obvious.

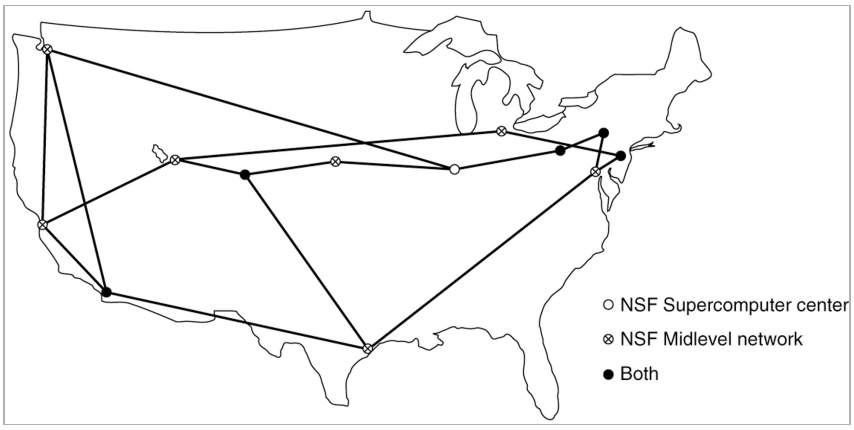
Internetworks

This is pretty much self-explanatory as to at least part of the definition of what an internet is. The only thing that is missing is that the point of an internet is to have an overlay layer over the different network layers. An overlay internet layer resolves the technology differences and differences in addressing conventions of different kinds of networks, to provide a network-technology independent service to the applications. As we will learn later in the course, the Internet lost the internet layer and is merely a network. Perhaps more clearly, the Internet is an internet in the same way that the international telephone system is an internet for telephones.

Examples of Networks

The ARPANET and the Internet

We have already covered the ARPANET and CYCLADES, so we will skip them here.

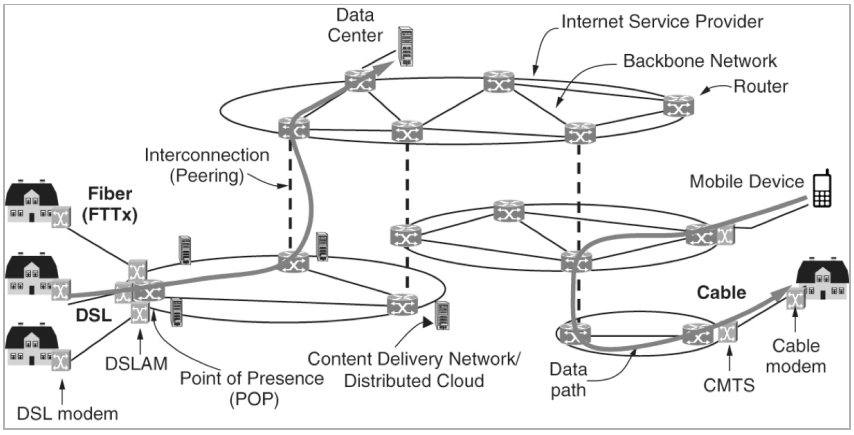


Source: Tanenbaum, A., Wetherall, D., & Feamster, N. (2020). *Computer Networks* (6th ed.).

NSFNET was primarily created to redress an inequality created by the Internet. The Internet was created by the U.S. Department of Defense (DoD), one had to have a DoD contract to be on it. The contract did not limit access to the project but allowed the entire organization to be on the Internet. If the ECE Department at Boston University had a small DoD contract, then all of BU was on the Internet, e.g., the English or Anthropology departments and their students. All of the members of the university were able to collaborate and work with their colleagues in other universities that had DoD contracts. This left those schools without DoD contracts at a disadvantage. As the move began to commercialize the Internet, the universities without DoD funding would still have no access, so the National Science Foundation (NSF) created NSFNET to redress this inequality. Tanenbaum goes on to describe the process by which the early Internet was moved into the public sphere. Unfortunately, this process did not include productizing it, so what we have is basically an escaped demo.

In the book, the term “cable modem” is a bit of a misnomer. Generally, a modem is strictly a physical layer device that converts analog signals to digital signals. We will talk about this in more detail when we cover the Physical Layer itself. This was true of cable modems when cable infrastructure only carried TV channels. Today, a cable modem does this function but also acts as a router.

Examples of Networks

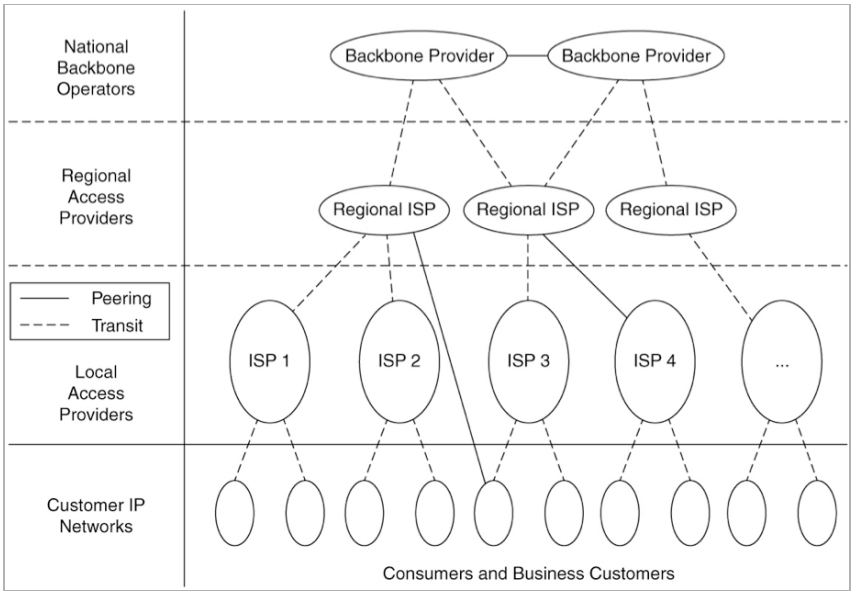


A common method for connecting to the Internet from your home is to send signals over the cable television infrastructure.

Source: Tanenbaum, A., Wetherall, D., & Feamster, N. (2020). *Computer Networks* (6th ed.).

This diagram, Figure 1-16 in the textbook, shows what the typical cable system looks like and illustrates some uses of it. I have my doubts about the example on the right, showing data going from a home directly to a mobile device. It is highly unlikely that this is possible today. It is more likely that the data from the home, perhaps an Internet-enabled doorbell with a camera, delivers data to a server application in a data center and an app on the owner's phone can access that data on the same server. There are several reasons for this, not least of which is that the cable network allocates more capacity "downstream" to the host than "upstream" from the host. In addition, the constraints of security in today's Internet would prevent this from happening. Either the mobile device or something in the home would have to be able to act as a server for this to be possible, something that is generally not allowed. It is made more difficult by the fact that the home (and the mobile device) would be in private address space. It is important to note here that none of this is technically difficult, in fact it is easy, but represents artificial barriers created on purpose or out of habit. For example, the typical smartphone has interfaces for cellular phone Physical Layer, WiFi, and Bluetooth. But within their characteristics of QoS, including cost, they are not treated the same. (It is getting more common that if a phone transitions from using cellular to being in range of a WiFi network that it knows, it will switch over automatically.)

Examples of Networks

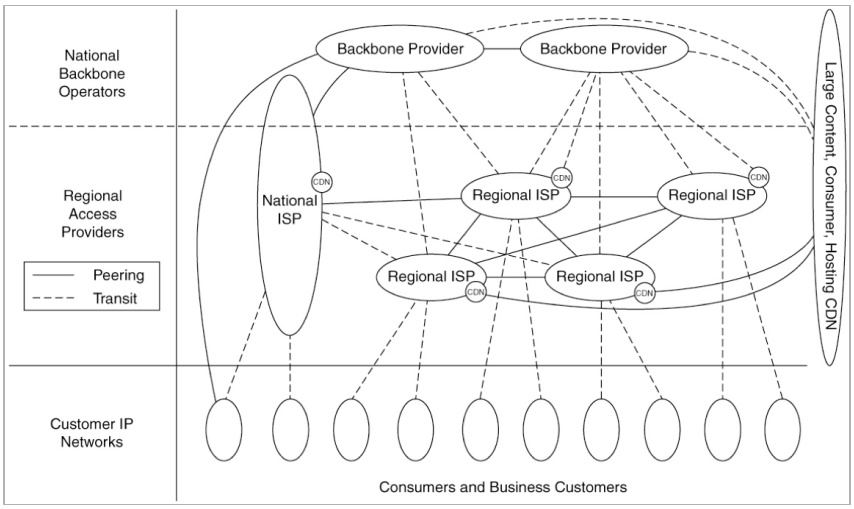


Source: Tanenbaum, A., Wetherall, D., & Feamster, N. (2020). *Computer Networks* (6th ed.).

The Internet is generally viewed (Figure 1-17 in the textbook) as a hierarchy of networks. As we will see later in the course, this view makes it difficult to see what is going on and makes it more complex than it needs to

be. It is much simpler (and much more secure) if it is recognized that the levels of this hierarchy are seen as layers of different scope rather than as networks.

Examples of Networks

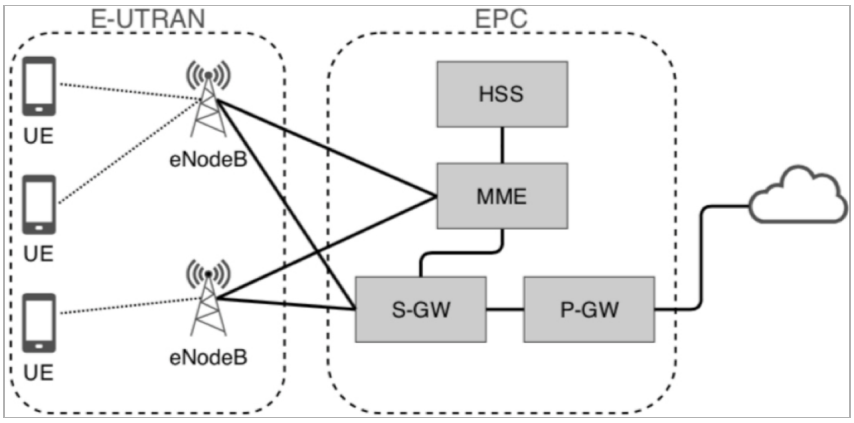


Source: Tanenbaum, A., Wetherall, D., & Feamster, N. (2020). *Computer Networks* (6th ed.).

Later, we will see that this picture (Figure 1-18 in the textbook) can be more clearly viewed as simply multiple hierarchies, with overlay layers as appropriate. In fact, one configuration of this yields an internet with excellent security properties that either keeps the malware controllers out or, if not, ensures they are in a domain where they can be eliminated and prosecuted. Read the textbook on this to be better prepared for the solution. But we have a lot to work through before that.

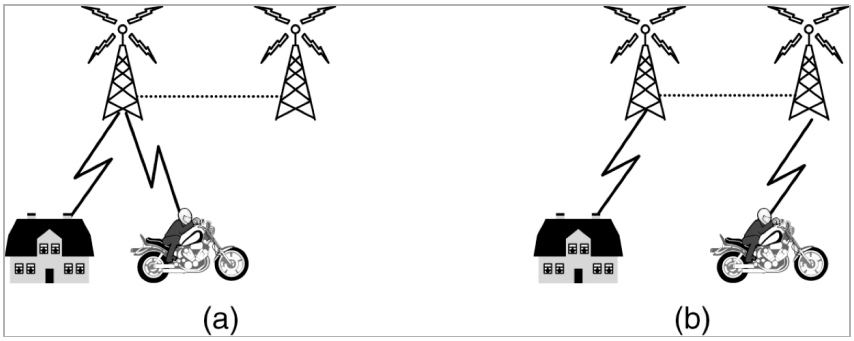
Mobile Networks

Mobile Networks



Source: Tanenbaum, A., Wetherall, D., & Feamster, N. (2020). *Computer Networks* (6th ed.).

Tanenbaum now launches into a brief overview of how current mobile communications works. The reader will quickly notice that Tanenbaum doesn't really explain what all of these elements do. That is explained (to some degree) later in the book. The basic idea is that a mobile network is a fixed wired network where the "last mile" to the customer's device is wireless. The customer is going to move from one wireless base station to another, requiring a notorious hand-off that often fails. Just to briefly describe what all of these boxes do: Clearly, the eNodes are the wireless base stations that connect the User's UE+ User Element to the network. The eNodes connect to the MME (Mobility Management Entity) that tracks the device and manages the hand-off, choosing the appropriate S-GW. From the description, you are probably wondering what the difference is between an S-GW and a P-GW. They are basically "gateways" to the Internet. The S-GW tries to make sure no data is lost during a hand-off, and the P-GW handles normal data transfer when a hand-off is not in progress. The HSS is the Home Subscriber Server that knows who the valid users are of the mobile phone network. There is a HSS for an area and the customer device resides in the HSS database where it is "most of the time."



Source: Tanenbaum, A., Wetherall, D., & Feamster, N. (2020). *Computer Networks* (6th ed.).

Clearly, as a mobile user moves, it will move out of the range of the current base station. Hence its connection must be "handed off" (and its traffic re-routed) to a base station that it is range of. This tries to illustrate the hand-off process. For historical reasons (the lack of resources on early mobile devices), the hand-off is controlled from the fixed network, the base station. There is currently talk of controlling it from the mobile device, which makes more sense. Currently, a mobile device cannot have wireless connections to two base stations at the same time. (A major contributor to dropped hand-offs.) This also needs to change.

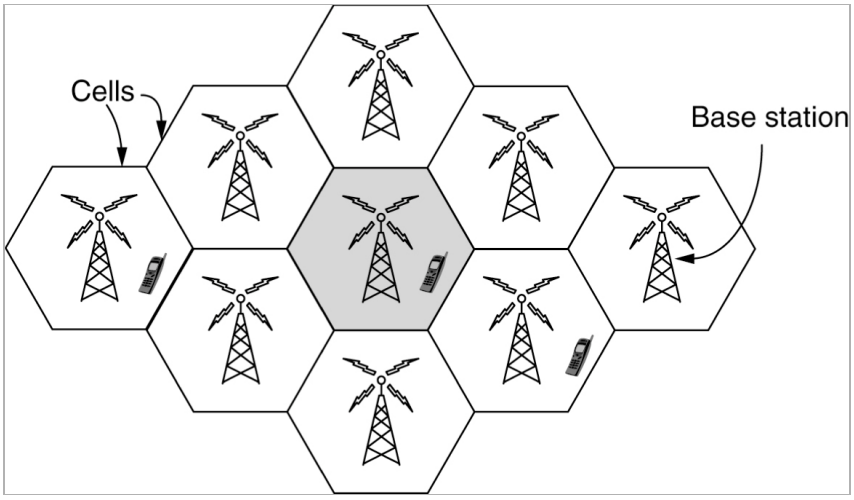
If all of this sounds very complicated, it is. If you are thinking, there must be an easier way, there is. In fact, if the mobile phone industry understood mobility, none of this would be required. The fact is that there is nothing special about mobility. A moving mobile device is simply a device whose connection to the network changes more frequently than most mobile devices.

This is a pretty strange topic to take up in this overview. We will take up the so-called connection/connectionless debate later. It would be better to refer to it as the virtual-circuit/connectionless debate. Virtual circuit was the traditional beads-on-a-string model of networking that the phone companies have tried to move to networking, as opposed to the more distributed computing model adopted by the

computer industry. The former is very inefficient in its tendency toward static allocation of resources. It appears that the only reason for mentioning it here is that early mobile phone architectures were more virtual circuit and only later became more connectionless. The depressing aspect of this (which is not uncommon) is that the transition did not occur because they finally understood the advantages of connectionless, but because the old guys retired.

The first-generation mobile phones used analog rather than digital technology. With analog mobile phones, two frequencies were required for each phone conversation. Mobile phones were much more popular earlier in Europe than in the United States. The primary reason for this was that wired phone service was so bad I Europe that mobile phones were an improvement. The opposite was the case in the United States. The first attempt to break up the AT&T monopoly was finally settled by AT&T agreeing to be regulated (the creation of the FCC), and in return they would deploy a first-rate phone system and provide good service, which they actually did. In Europe, it could take months to turn on a new phone in a home and the quality of the calls was terrible. In the United States, a new phone could be activated in a matter of hours and the voice quality was quite good.

To pick up on the last point, the first-generation (AMPS) was analog. The United States was slow to move to digital. A major contributing factor to the delay was that the market was dominated by Motorola. (Motorola was the IBM of wireless at the time.) The mobile phone guru at Motorola was convinced that only analog signals could provide high quality voice and fought the adoption of digital methods. Of course, this is crazy. (Did he use his phones?!) Not only did digital allow as many as 10 conversations on a single frequency, but digital processing techniques could be used to clean up the quality of the voice call!



Source: Tanenbaum, A., Wetherall, D., & Feamster, N. (2020). *Computer Networks* (6th ed.).

Before going on to discuss the later generations, Tanenbaum takes a diversion into how mobile phone cells are laid out. Generally, the antennas are constructed to provide more or less hexagonal cells. (No single antenna would generate that sort of coverage.) Greater denisity of users can be achieved by limiting the range of each base station, creating a “cell.” Hence, each cell only serves the users within that range. As a

user moves, it is handed-off from cell to cell. A group of frequencies are assigned to each cell with none of the same frequencies used in adjacent cells. Consequently, this comes down to solving a famous math conjecture called the Four-Color Problem. For over 150 years it had been conjectured that any planar map could be colored with four colors without the same colors touching. Assigning frequencies to mobile phone cells is the same problem. (The conjecture was confirmed in 1976 by Appel and Haken at the University of Illinois. I had Real Analysis with Haken while they were working on the proof. He seemed to be a stereotypical stern German professor who lectured with a strong accent in a monotone that never varied. However, it turned out that he had a great sense of humor and would drop little jokes in class without breaking his monotone. It took us awhile to be sure they were on purpose! Then we looked for them! This was one of the first math proofs done by computer. The problem came down to a couple of hundred configurations. Appel and Haken wrote a program to 'color' all of them. Just to confirm the program was correct. They printed them out and the two families got together and colored them!)

Doing frequency allocation for mobile phone cells is art, engineering, geography and even botany. Hills and buildings can affect the layout of the cells. Cells may be expanded or contracted to accommodate the load on the cell. One of my favorite frequency allocation problems occurred when Motorola was deploying cells in northwest Houston, Texas. The reception was terrible. Whatever adjustments they made didn't seem to help. Measurements showed that signal strength dropped off precipitously. There was no apparent reason why it should. It was all very puzzling. They tried everything. They had specially equipped trucks covering the area taking measurements. Then someone noticed the Big Piney Forest came down into northwest Houston, and the pine needles were exactly a half-wavelength long! The trees were perfect absorbers of the radio waves! The moved the frequencies being used to a different part of the band with a different wavelength.

Tanenbaum covers the current 4G and the much-hyped 5G mobile phone systems, which actually take what we saw before and make it even more complex. To some extent, most providers (and their customers) were happy with 4G. It had sufficient capability for what most users were doing. However, with 4G fully deployed, the vendors had nothing to sell. So 5G was invented.

The physical layer of 5G is a step up in the sophistication of the use of the media and, if you are an electrical engineer, quite interesting. The other big capability 5G pushes is low latency. This is sometimes referred to by the buzzword *Edge Computing*, which is a misnomer that says nothing. As we have seen, all computing is at the edge. There is no other place for it to be. The transport layer ensures that.

What is really going on here is that the mobile phone providers have dreams of co-locating "data center-like" resources along with their network equipment near (or at) the base stations and taking business away from cloud providers. This is a repeat of the strategy they were pursuing in the mid-1970s of locating services "in the network" and were beat out by the cloud providers. One aspect they don't seem to have addressed is the much larger number of data-center sites this will require and the amount of energy (and heat) it will generate. To get the low latency they claim could require a density of data centers that could affect the weather. (Without 5G, there are already 275 mammoth data centers in the suburbs of Washington, DC.) It has also been predicted that, given the amount of hardware 5G implies, it could bankrupt the providers. Of

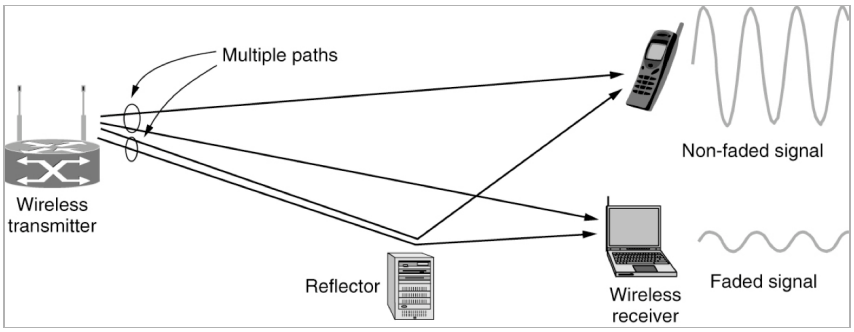
course, what will happen after all this hype is that at some point well-short of the hype, carriers will declare they have 5G and assume the public and the industry will have conveniently forgotten what was promised. 6G is already being discussed.

Wireless Networks (really, WiFi)

Tanenbaum now shifts his focus primarily to WiFi developed by IEEE 802. As all of you will know, WiFi has become ubiquitous. Read about what Tanenbaum says. In general, IEEE 802.11 has done some good engineering. This primarily covers the technologies for the physical layer. We will talk more about this when we cover WiFi later in Module 2. But even that will be at a high level. To get down in the details of this requires more of an electrical engineering background.

Tanenbaum remarks that WiFi mobility is limited. This is less a limitation of the architecture and more a limitation of the unlicensed bands in which it operates. The unlicensed bands require such low power signal strength, so that range is very limited. WiFi is organized like the mobile phone network, i.e., a fixed wired network where the last 100-300 meters is wireless. The fixed part of a WiFi network is not intended to cover a whole city or state. Generally, WiFi is deployed within buildings or for a campus of buildings. Actually, its procedures for mobility are simpler than for mobile phones. However, see the section on Community Networks above.

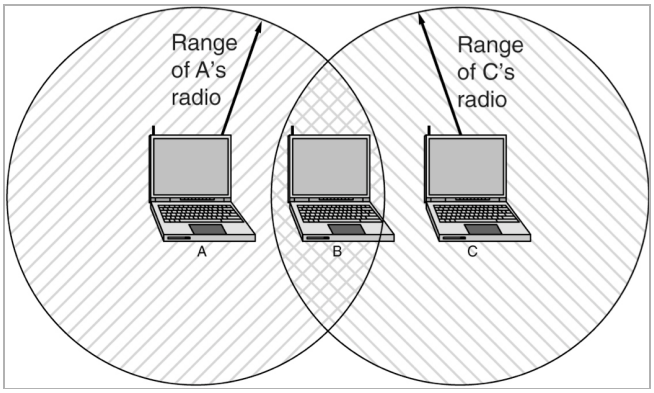
Initially, WiFi had trouble getting security right. The first attempt was compromised fairly easily. But they were finally able to get an effective security standard in place. As we will learn later in the semester, a well-designed architecture security at this level can be quite simple and mainly involve authenticating users of the network. First of all, WiFi can only provide protection between the wireless device to the fixed wireless base station. In a typical Internet environment, this is only 1/15th to 1/20th of the problem. We will go into this in more detail later, where we will find that security requirements at this level are minimal to non-existent.



Source: Tanenbaum, A., Wetherall, D., & Feamster, N. (2020). *Computer Networks* (6th ed.).

This figure illustrates the problems caused by WiFi signals bouncing off objects and causing the signal to be received multiple times with different delay. This can result in the signals re-enforcing and being stronger or canceling and creating “dead spots.” Read about it, but this is another topic that requires more of an

electrical engineering treatment to fully understand.



Source: Tanenbaum, A., Wetherall, D., & Feamster, N. (2020). *Computer Networks* (6th ed.).

This figure illustrates the heart of almost all wireless networks, the so-called hidden terminal problem. With wireless, if two (or more) transmitters transmit on the same frequency at the same time, both signals are unintelligible, both will be garbage. The best solution would be for each station to listen before sending; if it hears another transmitter, it will back off and try again later. However, this isn't good enough. There can be situations where not all of the transmitters can hear each other. Consequently, it is hard to avoid collisions. This can happen as illustrated here where B can hear A and B can hear C, but A and C are too far apart to hear each other. If both A and C transmit at the same time on the same frequency, B will hear trash. This can also happen if A and C are on opposite sides of a building or hill, but B can hear both. Later we will look at methods for avoiding this problem.

And that wraps up this overview of the types of networks. We will be going into these topics in more detail in the rest of the course. But there were some important points made here, especially about the interaction of business and technology.