Exploration: Wireless Networking Introduction

Introduction

In this exploration we introduce the concept of wireless networking. Wireless is an enormous topic and is very complex, so as a disclaimer, in this course we will barely touch the surface of what is involved. We will take a look at some of the types of hardware, and some of the standards and protocols involved. We will also look at some of the issues that make wireless so challenging.

In this exploration we will examine:

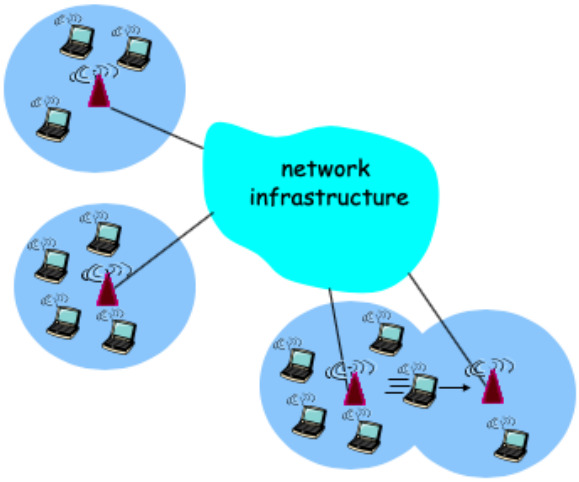
- The elements of wireless networking. The terms, types, and configurations.
- The characteristics and standards.
- The issues of multi-path, interference, and signal degradation.
- The 802.11 access protocol (CSMA/CA)

Wireless and Mobile Networks

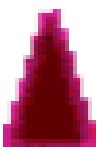
Wireless usage is pervasive in many parts of the world. In the United States in 2017, the percentage of wireless-only phone households surpassed that of homes that also had landlines. Consumers expect anytime/anywhere internet access. A popular debate in IT circles centers around the idea that wired Ethernet may have outlived its usefulness in the workplace.

With all of this growth, it is useful to remember that wireless is not without its challenges. These challenges divide naturally into two main groups:

- wireless: communication over wireless link
- mobility: changing the wireless link as the wireless device moves from one area to another



A typical wireless network, perhaps at a business or university.

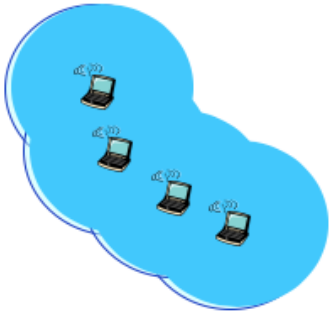


Consider what is required to have a wireless network. You first need an access point (AP), also sometimes called a base station. All of the wireless devices need to communicate with the access point. Typically the AP will be connected to the wired network, as it is with your home wifi device.

The next thing you need is wireless linking, and this is handled by radio broadcast medium.

This lets individual nodes (devices) connect to the AP. AP points will sometimes be connected to each other via wireless linking. The link access is controlled and coordinated by a type of MA protocol similar to that used in Ethernet. There can be various data rates, various transmission distances, many variables that determine how the wireless link works and how well it works.

Next of course are the hosts themselves, each of these will have a wireless adapter and will be communicating with the AP. These will run the end system applications which require communication. They may be stationary or mobile, and note that wireless does not always mean mobility (changing networks or subnets).



Four laptops connected together wirelessly in ad-hoc mode.

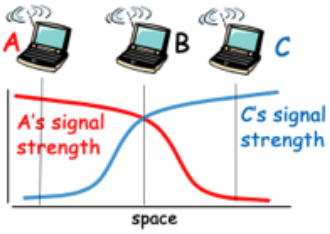
The other type is called ad-hoc mode. This is a group of friend devices that can communicate with each other is a peer-to-peer mode, but there is no central AP that wires them into a central network. Instead they can communicate amongst themselves, and will handle routing themselves.

The ad-hoc mode will be able to communicate with themselves and with the rest of the internet if at least one of the devices is connected to an AP. Each of these individual devices can relay messages from host to host similar to the way the ring network worked, where each host would pass on messages that had a different destination. If the destination was that one computer that was connected to the AP, then the message could reach the rest of the internet, and similarly, inbound messages would be passed along until they reach their destination host.

Characteristics of Wireless Networks

Several aspects of wireless communication are very different from wired communication, and in some ways make it very difficult to communicate…

Wireless takes place in undirected media, and while you don't have the chore of installing wires, this makes it more difficult to determine the destination. Hosts will need to check all incoming radio signals, even though those signals may never have been intended for them. Also radio signals fade out as they propagate through solid matter, piping, and so on. Radio signals will experience interference from a variety of sources, including electric motors, lighting, etc.



Finally there is the problem of multipath propagation. A receiver might receive the same signal at slightly different times due to signal reflection. This may even result in self-cancellation effects.

IEEE 802.11: multiple access protocol

The IEEE maintains the standards for various wireless communications, including for cell phone wireless and 802.11n which is the familiar wifi. There are many others, but all of them use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) for the multiple access protocol. In addition, all have both infrastructure and ad-hoc network versions.

802.11 does not provide any collision detection. The reasons are:

- It is difficult to sense collisions (due to signal strength, multipath, etc.)
- It is impossible to sense all collisions anyway (hidden terminal, etc.)
- A collision will cause a garbled message (drop message due to error)

So instead of using collision detection, 802.11 uses collision avoidance (CSMA/CA).

Instead of simply testing the transmission medium and waiting until no other transmission is present before sending a packet, the protocol will allow the sender to reserve a channel to send.

1. The sender first transmits request-to-send (RTS) packets to access point using CSMA
2. The access point broadcasts a clear-to-send (CTS) reservation response to RTS
3. The CTS (designating sender) is received by all nodes
4. When the sender gets CTS, it can send the packet.
5. When the packet is received, or after a timeout, the access point will broadcast channel-open, so that any other node can try to reserve the channel.

With CSMA/CA, in theory other stations will defer transmissions, and longer data packets should not collide. In actuality, however:

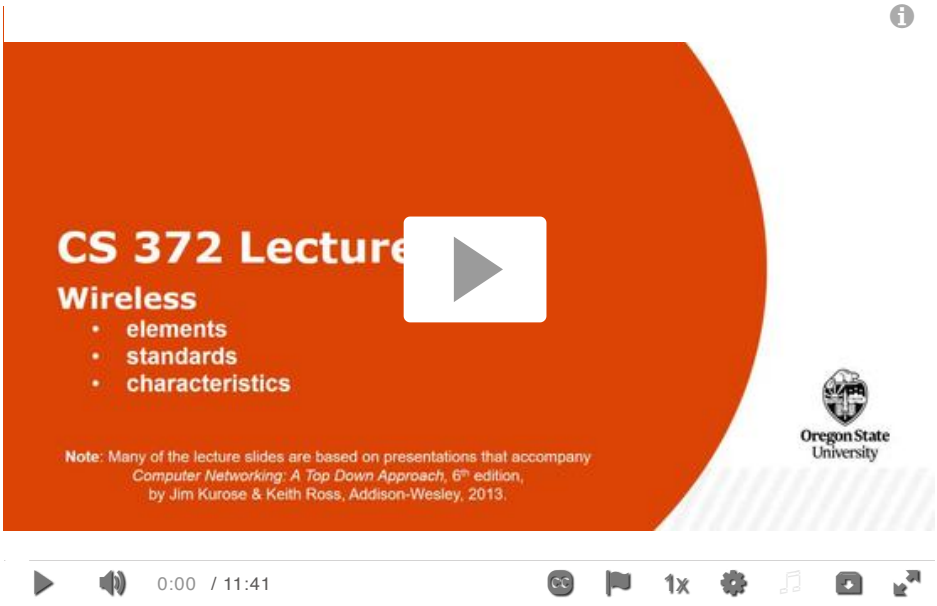
- RTS’s may collide with each other (but they’re very small).
- RTS’s might collide with a data packet.
- A new node might join after CTS and send RTS

There are other scenarios which can cause problems. But hopefully you now have a feel for some of the challenges.

That concludes our discussion of 802.11 standards. The next exploration will address the problem of wireless mobility. For more on wireless networking, be sure to watch the video lecture, then test your knowledge with the Self-Check exercises below.

Video Lecture

Wireless



(PDF (https://oregonstate.instructure.com/courses/1798856/files/83165109/download?wrap=1) (https://oregonstate.instructure.com/courses/1798856/files/83165109/download?wrap=1) |PPT (https://oregonstate.instructure.com/courses/1798856/files/83165077/download?wrap=1) (https://oregonstate.instructure.com/courses/1798856/files/83165077/download?wrap=1))

Self-Check Exercises

What is the difference between “wireless “and “mobility” in terms of networking?

Turn

Card 1 of 4

What multiple access control scheme does 802.11g Wifi use?

- CSMA/CA
- CSMA/CD
- ARP
- TDMA

Reuse <> Embed

Resources

- **Wireless Phones Surpass Landlines in the United States (https://apps.prsa.org/Intelligence/Tactics/Articles/view/11913/1143/Wireless_Phones_Surpass_Landlines_in_the_United_St#.XjyKQRNKiS4)**
  Beaubien. “Wireless Phones Surpass Landlines in the United States.” PRSA. Accessed March 11, 2020.
- **Animation: CSMA/CA (https://www.ccs-labs.org/teaching/rn/animations/csma/)**
  “CSMA/CA” ccs-labs.org, coded by Johannes Kessler 2012
- **IEEE Standards Index (https://standards.ieee.org/standard/index.html)**

IEEE 802.11 Wireless LAN standards