Wireless LANs: outline

- DNS (continued)
- wireless 802.11 and WiFi
- 802.11 security: WEP, 802.11i, WPA, WPA2

DNS Query

- a DNS client sends a query to any DNS server
- usually, every client is configured with the IP address of one or more DNS servers
- the servers authoritative for the zone know a given translation ("answer"), though other servers and clients may cache a translation
- since the DNS name space and the zones are arranged hierarchically, a DNS server always knows another server closer to the answer
- DNS names are encoded efficiently by replacing repeated strings with pointers: a.hawaii.edu and b.hawaii.edu become a.hawaii.edu and b.*pointer-to-previous-hawaii.edu*

DNS Query Response

- a server can respond to a query in one of three ways:
  - by returning the answer, if it is known or cached,
  - by returning the address of another server closer to the answer: this leads to the client performing an **iterative** query
  - by requesting the translation from a server closer to the answer, then returning the result to the client: this is a **recursive** query

ISM bands

- to operate most radios, a license is needed from a government body – in the U.S., from the FCC
- to operate a microwave oven, no license is needed
- microwave ovens work on a resonant frequency of water, around 2.4GHz
- the 2.4GHz-2.5GHz band has been designated an **Industrial**, **Scientific**, and **Medical** (ISM) band, free to use worldwide without a license
  - as long as transmission power is limited
  - and some countries restrict part of this band

Using ISM bands

- ISM equipment needs to tolerate interference (e.g., from microwave ovens!)
- there are many ISM bands, but most are limited to only some countries
  - e.g. 900MHz band only available in the Americas
- due to the unprecedented availability of the 2.4GHz ISM band, many applications for it exist
  - though even for the this band, details vary among countries
- The 5GHz band (~ 5470-5725 MHz) is also popular

Wireless 802.11/WiFi

- an early marketing term for 802.11 was WiFi
  - a pun on HiFi, High Fidelity audio equipment
- 802.11 works mostly in the 2.4GHz ISM band, though 802.11a works in the 5GHz band
- many successive standards:
  - 802.11 (1-2Mb/s)
  - 802.11a (54Mb/s)
  - 802.11b (11Mb/s)
  - 802.11g (54Mb/s)
  - foreseeably, future versions

802.11/WiFi Operation

- 802.11 has two modes: ad-hoc (point-to-point) and managed
- in managed mode, all communication is to or from a central access point (Wireless Access Point or WAP)
- in managed mode, end nodes (hosts) contend for the medium: this contention may result in collisions that require retransmissions

802.11 Security: WEP

- tapping a wired network requires access to the wires
- tapping a wireless network requires being near the transmitter (or specialized equipment)
- originally, WiFi was insecure
- later, cryptographic Wired Equivalent Privacy (WEP) was introduced to hide the contents of the messages
- the original design for WEP was not widely published – unfortunately, this resulted in a lack of serious examination of the protocol:
  - security by obscurity often does not work
  - especially if your design will be adopted widely!

802.11 Security: WPA and WPA2

- unfortunately, WEP is sufficiently weak that it can be cracked by listening to a few minutes of traffic
- 802.11i introduced:
  - WiFi Protected Access (WPA), a simple but much stronger encryption protocol, and
  - WPA2, stronger than WPA and requiring more resources for implementation (including, in some cases, newer equipment)