

# Why Wi-Fi?

Al Prendergast  
IT Director  
LV-CCLD  
August 12, 2004



# What is Wi-Fi?

- Short for *wireless fidelity* and is meant to be used generically when referring to any type of 802.11 network, whether 802.11b, 802.11a, 802.11g, dual-band, etc
- Wi-fi is a wireless technology that uses radio frequency to transmit data through the air

# Brief History

- IEEE (Institute of Electrical and Electronics Engineers) established the 802.11 Group in 1990. Specifications for standard ratified in 1997
- Initial speeds were 1 and 2 Mbps
- IEEE modified the standard in 1999 to include 802.11 a and b
- 802.11g was added in 2003
- 802.11b equipment first available, then a, followed by g
- IEEE create standard but Wireless Ethernet Compatibility Alliance certifies products



# What can you do with it?

- Quick/easy temp network access
- Staff access to Corporate network
- Patron internet access (hotspot)
- Interconnecting two networks

# 802.11b

- Been around the longest, well-supported, stable, and cost effective, but runs in the 2.4 GHz range that makes it prone to interference from other devices (microwave ovens, cordless phones, etc) and also has security disadvantages
- Limits to the number of access points in range of each other, three
- Has 11 channels, with 3 non-overlapping, and supports rates from 1 to 11 Mbps, but realistically about 4-5 Mbps max
- Uses direct-sequence spread-spectrum technology

# 802.11g

- Extension of 802.11b, with the same disadvantages (security and interference)
- Has a shorter range than 802.11b
- Is backwards compatible with 802.11b so it allows for a smooth transition from 11b to 11g
- Flexible because multiple channels can be combined for faster throughput, but limited to one access point
- Runs at 54 Mbps, but realistically about 20-25 Mbps and about 14 Mbps when b associated
- Uses frequency division multiplexing technology

# 802.11a

- Completely different from 11b and 11g.
- Flexible because multiple channels can be combined for faster throughput and more access points can be co-located
- Shorter range than 11b and 11g
- Runs in the 5 GHz range, so less interference from other devices
- Has 12 channels, 8 non-overlapping, and supports rates from 6 to 54 Mbps, but realistically about 27 Mbps max
- Uses frequency division multiplexing technology

# 802.11b+

- Non-standard, runs in the 2.4 GHz range
- Is backwards compatible with 802.11b
- Supports rates from 1 to 22 Mbps, but realistically about 6 Mbps max
- Uses a totally different type of modulating technology

# What do you need to do Wi-fi?

- Existing wired network/services (Infrastructure Mode)
  - DHCP/DNS
- Access point
- Antennas and bridges
- Wireless adapter

# Why Wi-Fi?

- Setup Cost – Reduced cabling required
- Flexibility – Quick and easy to setup in temp or permanent space
- Scalable – Can be expanded with growth
- Freedom – You can work from any location that you can get a signal
- Lower total cost of ownership – Because of affordability and low install cost
- Additionally
  - Mobile Users – Can access the Corporate network from any public hotspot using VPN



# Disadvantages

- Planning – Depending on the goal
- Security – Greater exposure to risks
  - Access
  - Compromising Data
  - Denial of Service
- Speed – Slower than cable
- Range – Affected by various medium
  - Travels best through open space
  - Reduced by walls, glass, water, etc

# Security

- Data Security/Encryption
  - Third Party solution - Fortress
  - Wi-Fi Protected Access (WPA)
  - Wired Equivalent Privacy (WEP)-Shared key
- Access
  - WPA/WEP
  - Close System – No advertising
  - MAC Authentication – MAC address control
- Attack – Denial of Service
- Client Protection
  - Antivirus/Firewall

# Range and Performance

- Performance decreases as distance increases
  - 802.11a
    - Indoor 40-300 feet
    - Outdoor – 100 to 1000 feet
  - 802.11b
    - Indoor 100-300 feet
    - Outdoor 400 – 1500 feet
- Interference - doors, walls, furniture, ceiling
- 253 maximum number of client per AP, but 15-20 recommended

# Considerations

- Infrastructure/Design
- Other Patron Services
- Other Technical Services
- Cost
- Vendors
- Policy- End user/Corporate
- End User Experience

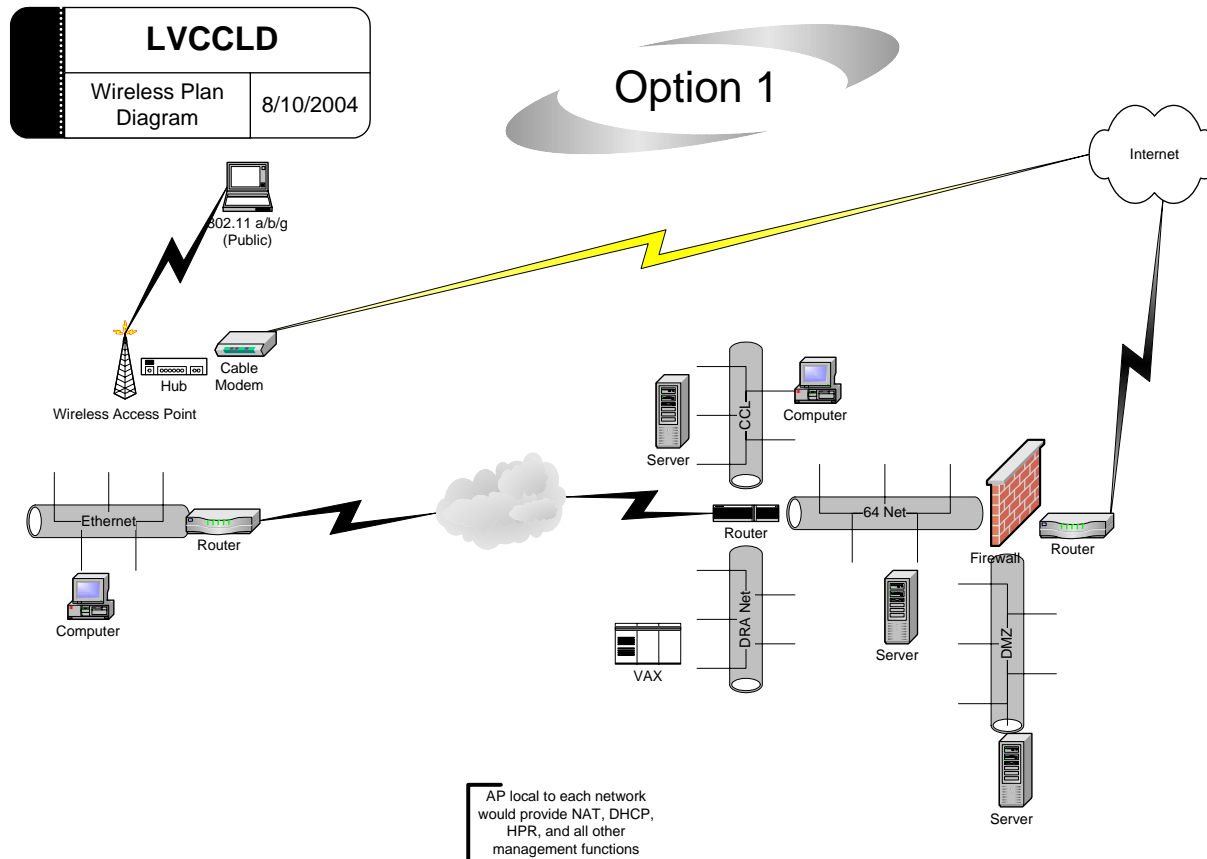
# Infrastructure/Design

- Option 1 – Provide patron access using a totally separate network Infrastructure
- Option 2 – Use the existing corporate network, with additional equipment to provide access to patrons while securing internal network
- Option 3 – Use the existing corporate network, with same equipment to provide access to patrons while securing internal network

# Separate Network-Option 1

- Provide patron access using a separate network from your corporate network
  - Advantages: Total internal network security, “a simple solution”, can provide redundancy for the existing internal network (however cost and complexity would increase)
  - Disadvantages: More administrative overhead, more expensive (recurring service charges)

# Separate Network

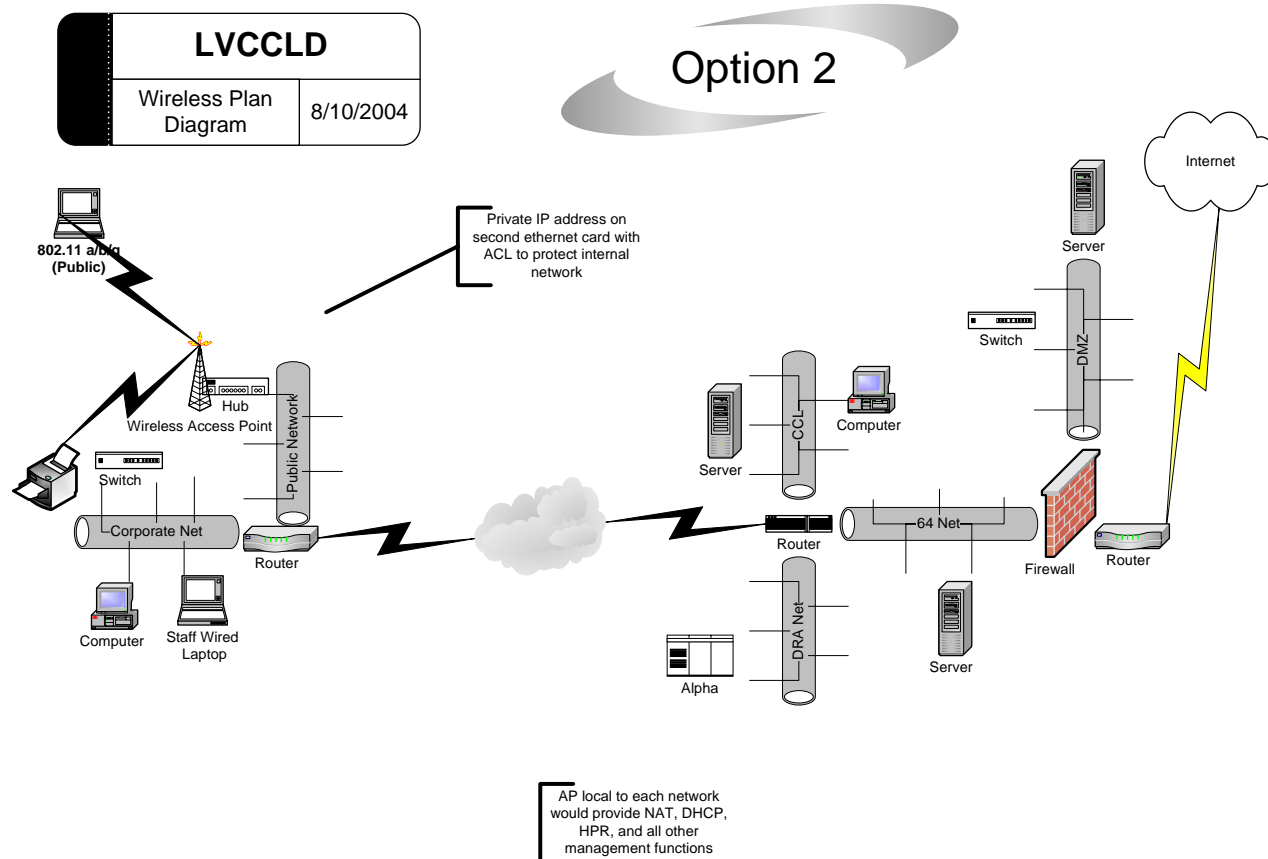


## Existing Network-Different Equipment- Option 2

- Use most of the existing infrastructure to provide access to patrons while securing internal network
  - Advantages: Easier administration, Less expensive (No recurring monthly service charges), but cost for more hardware
  - Disadvantages: Internal network down means no wireless access, “a more complex solution” (bandwidth, security, configuration implications)



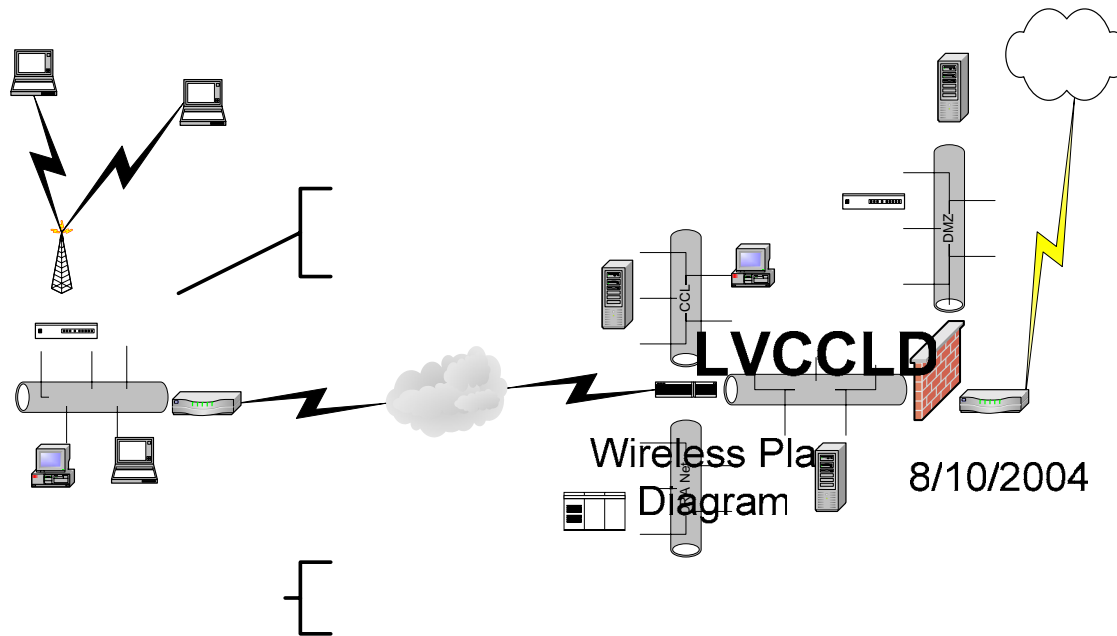
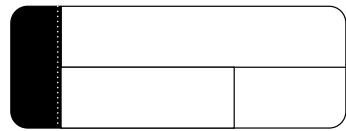
# Existing Network-Option 2



## Existing Network-Same Equipment-Option 3

- Use the existing infrastructure to provide access to patrons while securing internal network
  - Advantages: Easier administration, Least expensive (No recurring monthly service charges and no hardware)
  - Disadvantages: Internal network down means no wireless access, most complex solution (bandwidth, security, configuration implications), using VLAN

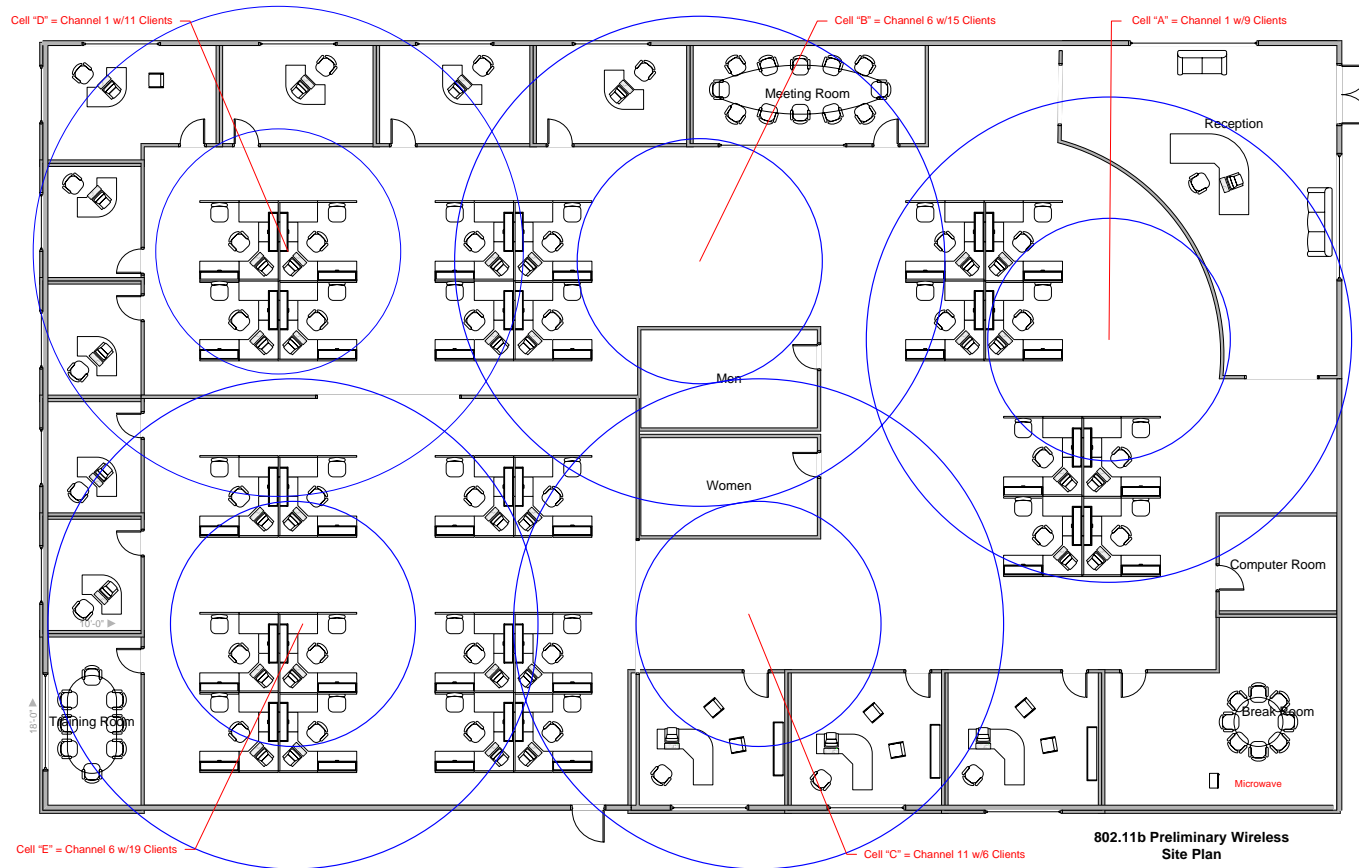
# Existing Network-Option 3



# Physical Placement and AE

- Active Ethernet powers access points over the ethernet connection
- Access Points should be mounted in an open space to optimize the signal strength, so no closets. Larger locations may require multiple access points to provide “good” coverage

# Placement Site Plan



# Other Patron Services

- Do you provide printing capability?
- Do you provide filtering for younger kids?
- Do you provide assistance with connectivity?
- Do you provide laptops for checkout?
- Do you provide PDA Support?
- Others
  - Do you limit access to valid patrons only?
  - Do you charge patrons for access?



# Other Technical Services

- Required Services
  - DHCP – Automatic IP assignment
  - DNS – Website resolution
- Access Point Features
  - HRP – Home Page Redirection
  - Bandwidth Management
  - SNMP Management
- Authentication – Free access for everyone?
- Accounting – Do you charge?

# Cost

- Access Point - \$20 to \$1000
- Extended Range Antenna-\$20 to \$100
- 802.11a/b/g Kit - \$40 to \$100
- Active Ethernet - \$100-\$200
- Wireless Adapter - \$20 to 100
- The average cost of adding a wired connection is about \$400, more if conduit is needed

# Vendors

- Netgear
- D-Link
- Linksys
- Proxim
- Cisco
- Enterasys
- Avaya
- Aruba Networks

# Selection criteria to consider

- Standards – 802.11a, b, or g?
- Features – Does it have all of the services that you need?
- Upgradeability – Support for firmware upgrades?
- Aesthetics – Looks good?
- Security – Has WEP for encrypting data and controlling access?
- Range – How strong is the signal, does it accommodate an antenna?
- Installation and Support Tools – Company reputation?
- Price – Does it fit in your budget?
- Availability – Can you buy it now?
- Manageable – Can you manage it remotely?
- Certified – Is it “Wi-Fi Certified”?



# Acceptable Use Policy

## Sample

- *1. Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret ...*
- *2. Sending unsolicited mail messages, including the sending of "junk mail" ...*
- *3. Unauthorized use, or forging, of mail header information (e.g. "spoofing").*
- *4. Unauthorized attempts by a user to gain access to any account or computer resource not belonging to that user (e.g., "cracking").*
- *5. Obtaining or attempting to obtain service by any means or device with intent to avoid payment.*
- *6. Unauthorized access, alteration, destruction, or any attempt thereof, of any information of any Las Vegas- Clark County Library District patrons by any means or device.*
- *7. Knowingly engage in any activities that will cause a denial-of-service ...*
- *8. Advertising, transmitting, or otherwise making available any software, program, product ...*
- *9. Using the District's Services to interfere with the use of the District's network by other customers or authorized users.*
  
- *Complaints about customers/representatives or end-users of a District IP customer will be forwarded to the District's postmaster for action. If violations of the Acceptable Use Policy occur, the District reserves the right to terminate services with or take action to stop the offending customer from violating the AUP as deems appropriate, without notice.*



# End User Experience

- Customer enters the hotspot and turns on WiFi computer
- Customer connects to the access point
- Customer launches their browser
- Customer attempts to connect to their homepage to browse the web
- Customer is redirected to the “walled garden”, at this point customer can browse anything on our web site
- The customer wants to access other sites on the web, so customer clicks on access the web and is redirected the District’s Acceptable Use Policy
- Customer reads the District’s Acceptable Use Policy and then clicks “I Agree”
- Customer is then presented with a “Free Access” billing plan
- Customer enters the number of days of free access they would like and clicks “Submit” ... customer is now logged in
- Customer can now browse any web site on the internet



# Summary

- Understand it
- Plan it
- Implement it
- Use it
- Refine it
- Support it

- Discussion and Questions