Wireless Networks at Umass-Amherst

Scott Conti

Christopher Misra

UMASS-Amherst Network Vital Statistics

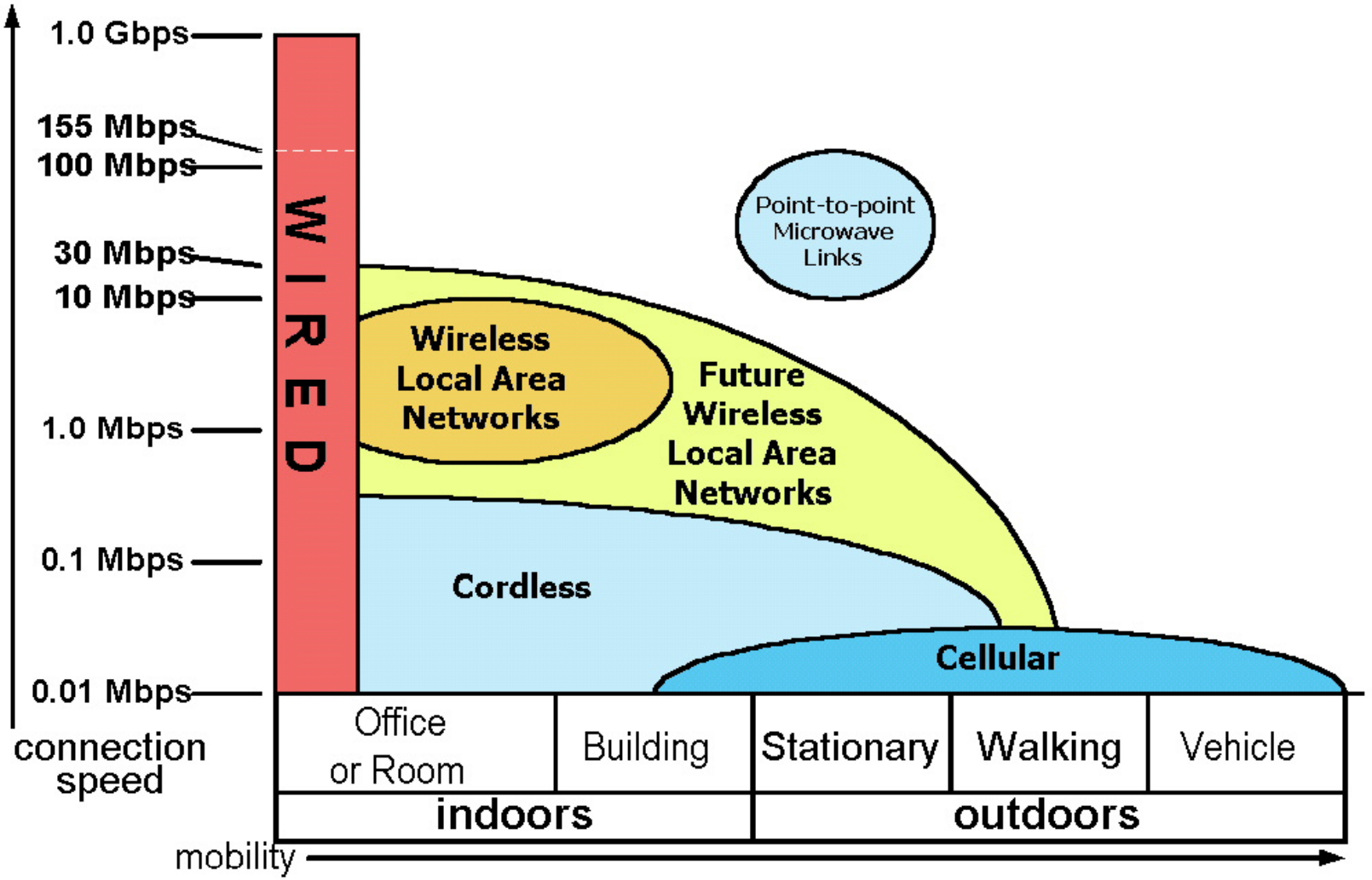
- Class B network (umass.edu - 128.119)
- 142 buildings
- All 42 Residential buildings networked
- 8800 Residence hall connections (port-per-pillow)
- 5500 Academic building connections
- 900- Cisco 24 port Switches (1900 and 2900 series)
- 5 Cisco 6509 core switches, 2 Cisco 5500 switches
- 600 Off-campus dial-in modem lines
- (2) DS-3 (45mb/s) commodity Internet connections
- DS-3 - Internet2 connection

Copyright 2002

UMASS at night

Copyright 2002

Wireless = Mobility



Copyright 2002

Equipment used

- 802.11b – 2.4ghz – 11mbps
- Cisco Aironet 350 series
- Cisco switches
- Aironet antennas

Copyright 2002

Typical Enclosure installation

Copyright 2002

Library Installation

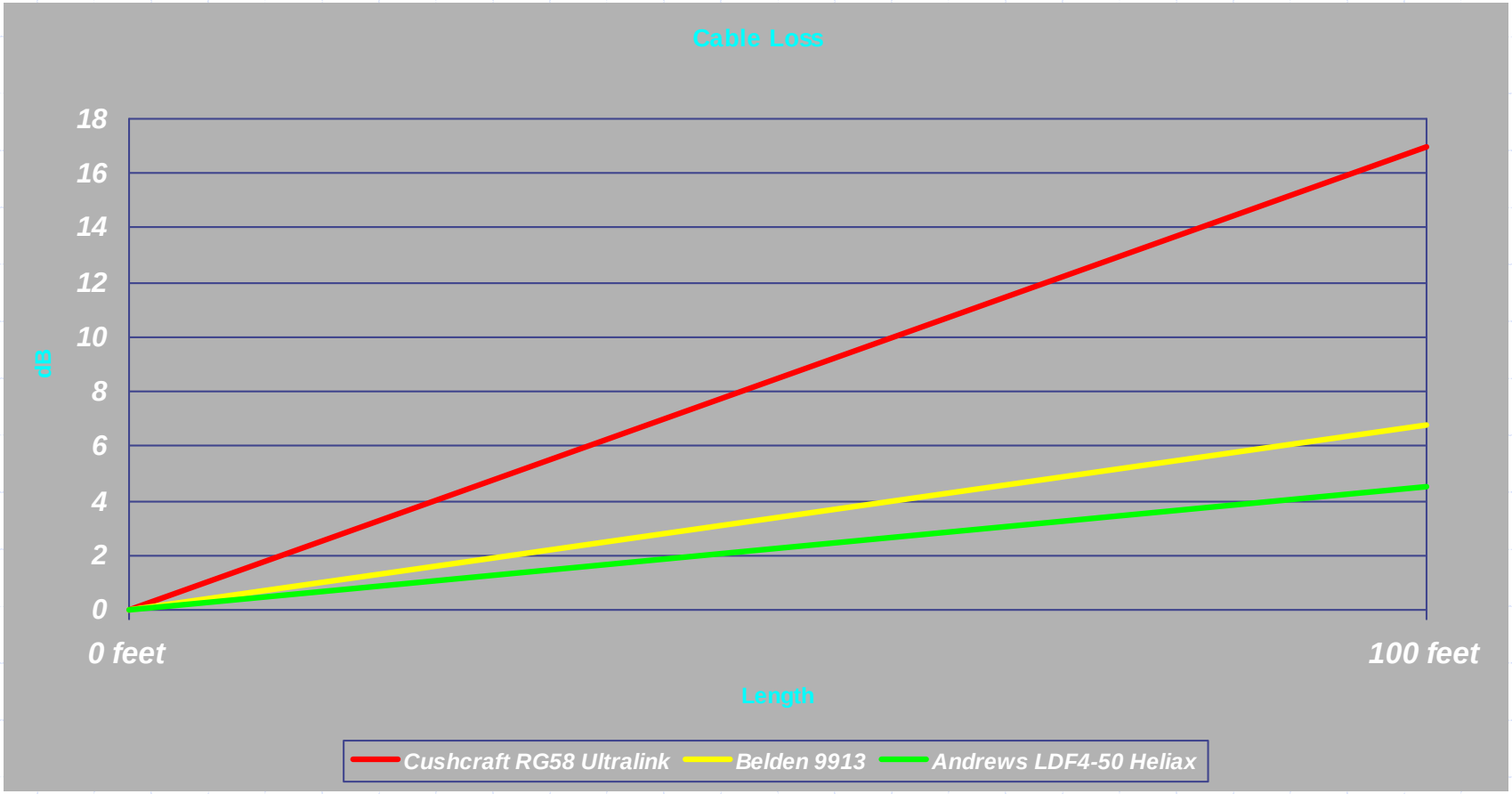
Copyright 2002

Inside of Enclosure

Ceiling Mount Antenna

Copyright 2002

Cable Losses



Copyright 2002

dB Factors

Increase	Factor	Decrease	Factor
0dB	1x	0db	1x
1dB	1.25x	-1dB	.8x
3dB	2x	-3dB	.5x
6dB	4x	-6dB	.25x
10dB	10x	-10dB	.1x
12dB	16x	-12dB	.06x
20dB	100x	-20dB	.01x
30dB	1000x	-30dB	.001x

Copyright 2002

Connectors

- Warning ! FCC Part 15 and rule 94 requires the use of RTNC Connectors !
- These are different from ordinary TNC connectors.
- RTNC connectors are “transsexual” – They use the male body and the female dielectric and pins.

Copyright 2002

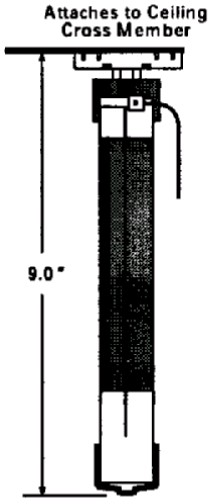
Omnidirectional Antennas

- Good choices where antenna is placed in the “middle” of the area to be covered.
- Tend to have low gain since signal is divided over 360 degrees.

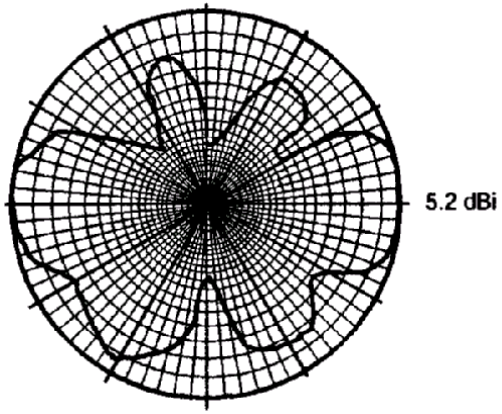
Copyright 2002

Omnidirectional Antennas

Dimensions and Mounting Specifications



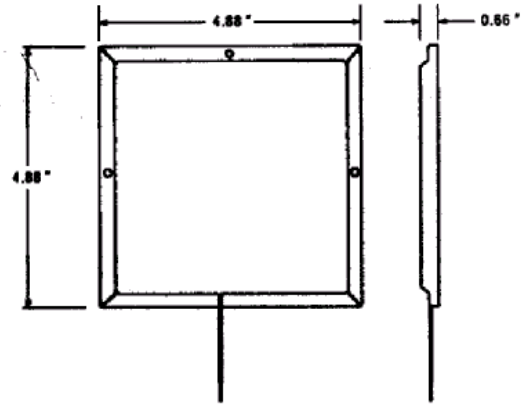
Vertical Radiation Pattern



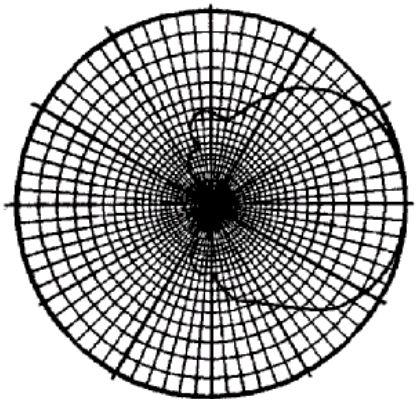
Copyright 2002

Directional Gain Antennas

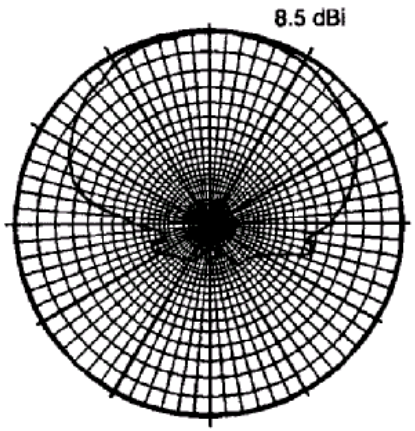
Dimensions and Mounting Specifications



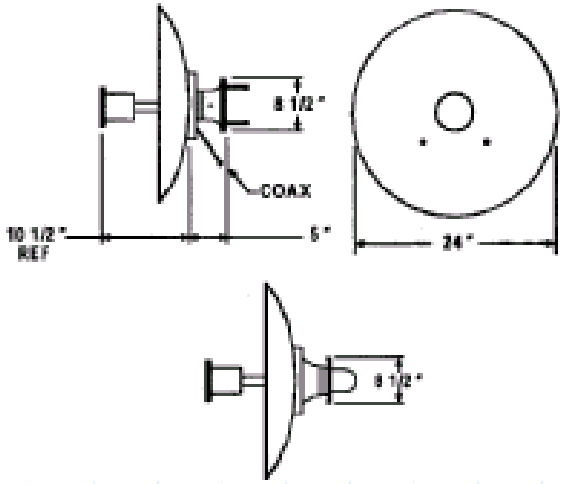
Vertical Radiation



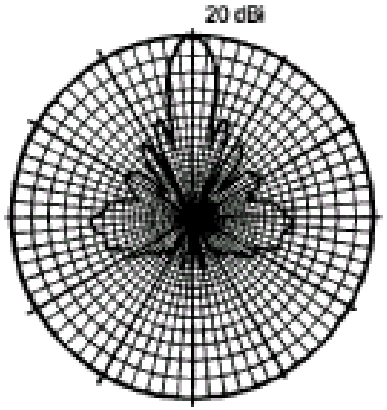
Horizontal Radiation



Dimensions and Mounting Specifications



Radiation Pattern



Copyright 2002

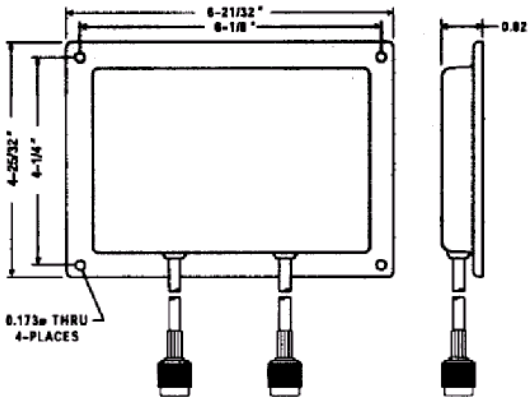
Diversity Antennas

- Diversity antennas have 2 antennas in a single enclosure.
- Diversity antennas are good choices where there will be signal reflections.
  - The Cisco Aironet 350 “votes” for the stronger signal by antenna at the start of receiving each packet, then transmits out the same antenna.

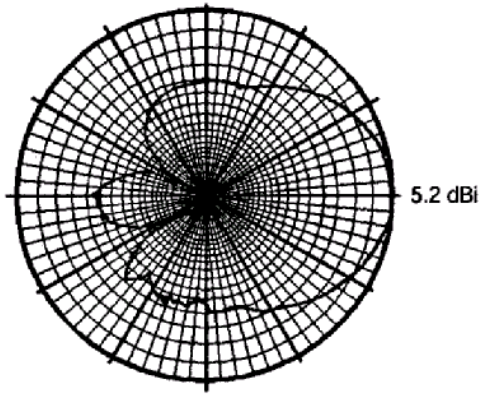
Copyright 2002

Diversity Antennas

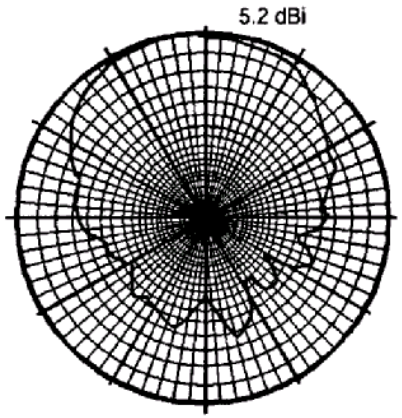
Dimensions and Mounting Specifications



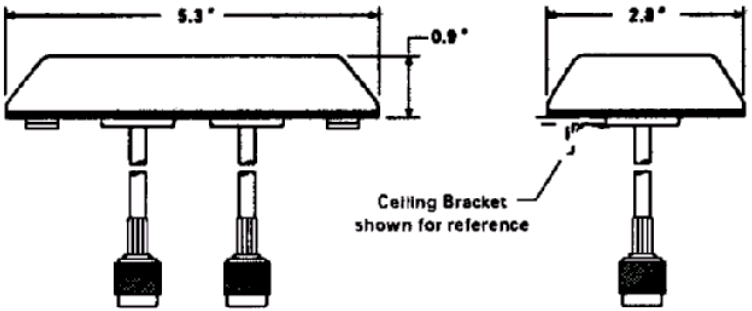
Vertical Radiation



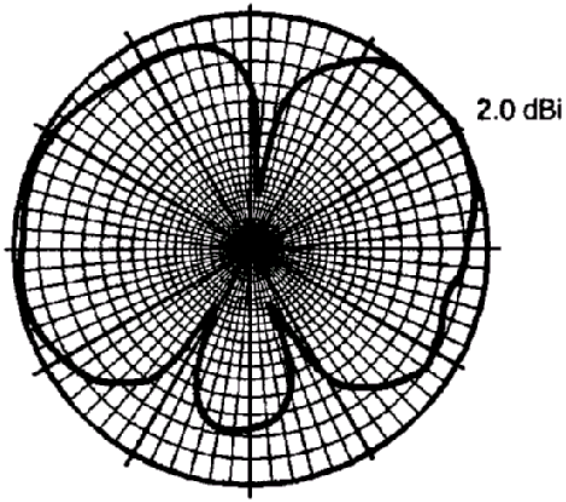
Horizontal Radiation



Dimensions and Mounting Specifications



Vertical Radiation



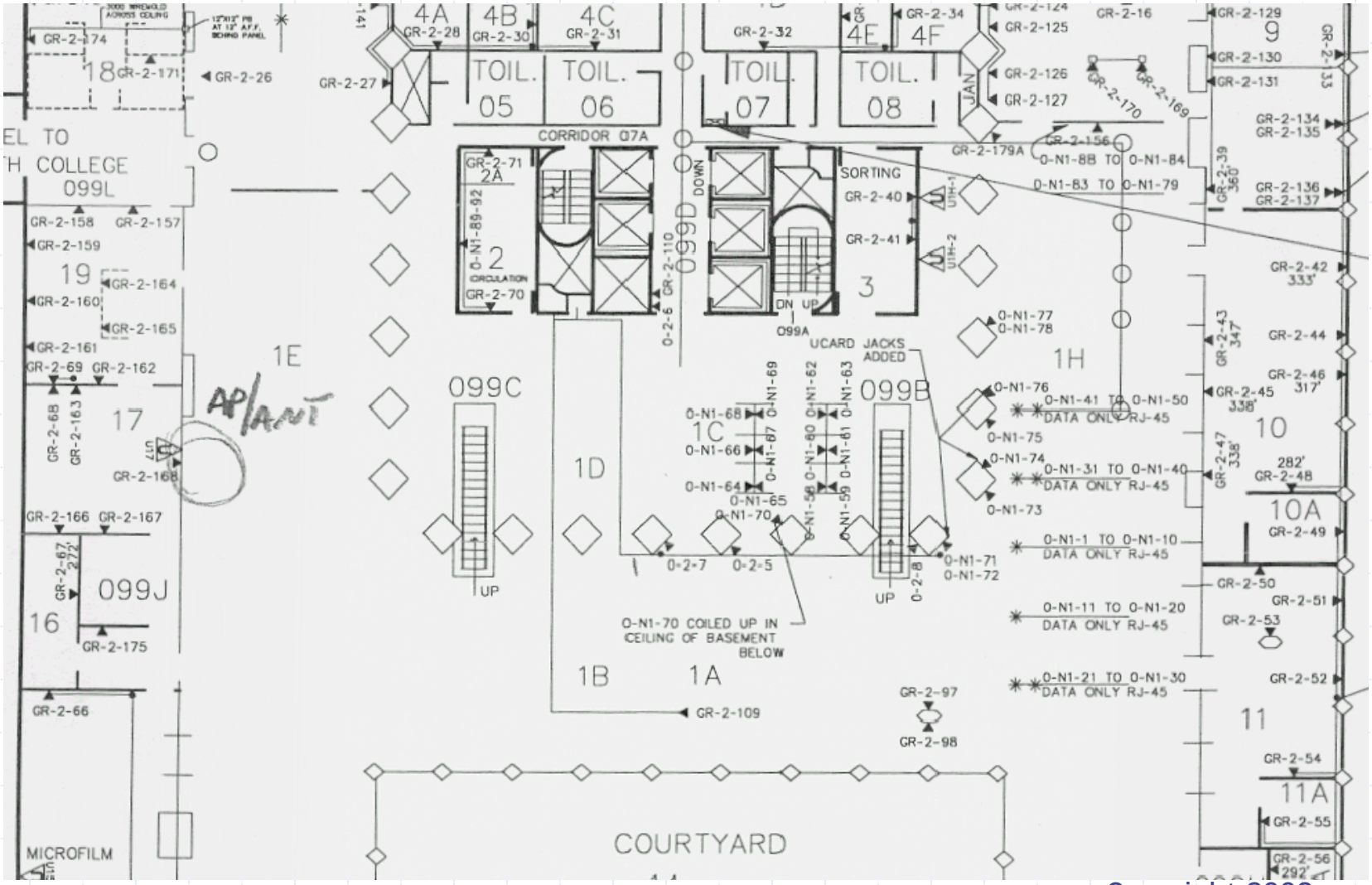
Copyright 2002

Site Surveys

- Start with Blueprints
  - Never believe the prints !
  - Walls move...
  - Construction materials not shown
- Walk-around
  - Select antenna/enclosure locations
  - Pay attention to wall materials !

Copyright 2002

Never Believe Prints...



Copyright 2002

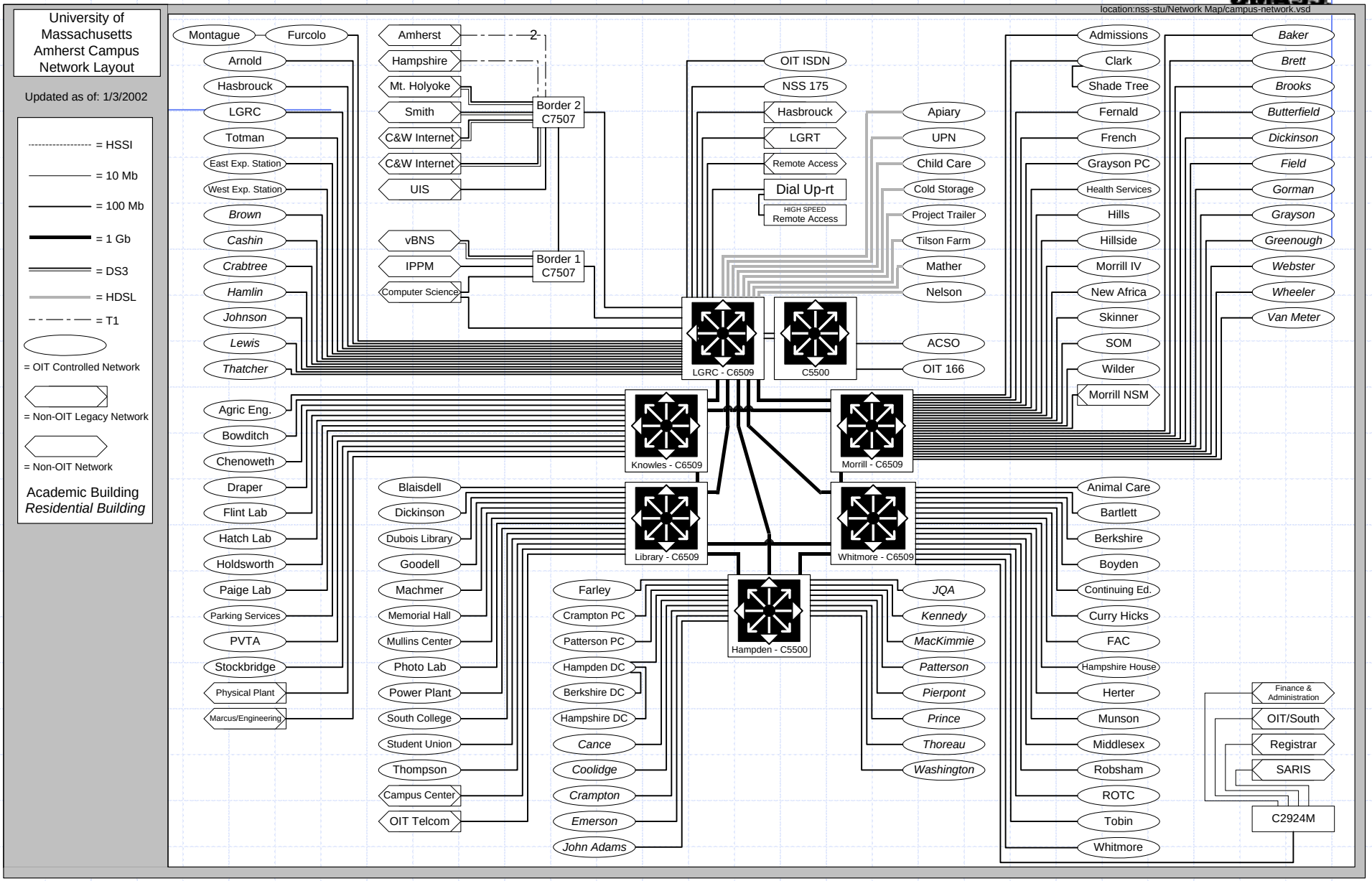
Library Structure

Copyright 2002

RF-Hell...

Copyright 2002

UMASS-Amherst Network Map



Copyright 2002

Initial Design Goals

- Virtual Classroom
  - We closed some labs due to budget constraints
  - Wireless network is meant to reproduce similar function
- Focused at public areas where students gather
  - Not initially a ‘campus-wide’ rollout
- Scalable
  - Although initial rollout is targeted, design must fit campus-wide

Copyright 2002

Initial Design Requirements

- Identification & Authentication
  - We register all MAC addresses in Residence Halls
  - Accountability
- Encryption
  - Too many plaintext protocols still in use
- Card heterogeneity
  - We don’t enforce a single vendor for wired network cards...
  - This limited our set of solutions

Copyright 2002

Initial Constraints

- Short time to implement
  - First pilot discussed in late November 2001
  - First pilot went live late January 2002
  - Phase 1 production rollout March 2002
- Didn't want a campus wide VLAN
  - VLANs are local to our 6 major nodesites
  - We don't switch VLANs across our backbone
  - This meant a parallel rfc1918 network
- Management driven

Copyright 2002

Initial Assumptions

- No pre-existing campus wireless implementation
  - Some local deployments
  - Netstumbler is your friend
- MAC address filtering doesn't scale
  - Based half on fact
  - Didn't feel 'right'
- WEP alone is likely insufficient

Copyright 2002

WEP Weaknesses

In case we haven't all seen this already...

- WEP uses RC4 encryption
- Fluhrer, Mantin, and Shamir described a passive, ciphertext-only attack against RC4
  - Specifically targeting the key scheduling algorithm of RC4

http://www.cryptonomicon.net/papers/rc4_ksaproc.pdf

Copyright 2002

WEP Weaknesses

- Stubblefield, Ioannidis, and Rubin implemented the attack against the RC4 weakness (6 Aug 2001)
  - Using only off-the-shelf hardware, and some custom software
  - Large amounts of data are needed for the attack
    - *"We conclude that 802.11 WEP is totally insecure, and we provide some recommendations. "*
  - http://www.cs.rice.edu/~astubble/wep/

Copyright 2002

WEP Weaknesses

- Nikita Borisov, Ian Goldberg, and David Wagner did an an analysis 30 Jan 2001
  - “Wired Equivalent Privacy (WEP) isn't”
  - http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- We felt justified in saying WEP is insufficient for our implementation
  - We are network security guys. We try do design secure systems...

Copyright 2002

Authentication and Access Control

- We considered four options
- Wireless with WEP
  - Insufficient...
- Wireless with dynamic WEP
  - Dynamic WEP is better, but...
  - Basically a race condition
  - Most implementations require card homogeneity

Copyright 2002

Authentication and Access Control

- We considered four options
- Wireless with WEP and VPN
  - WEP didn't improve the situation in this model
  - Added management overhead
- Wireless with VPN, no WEP
  - What we ended up going with
  - Maybe not the best solution, but the best for us given our environment

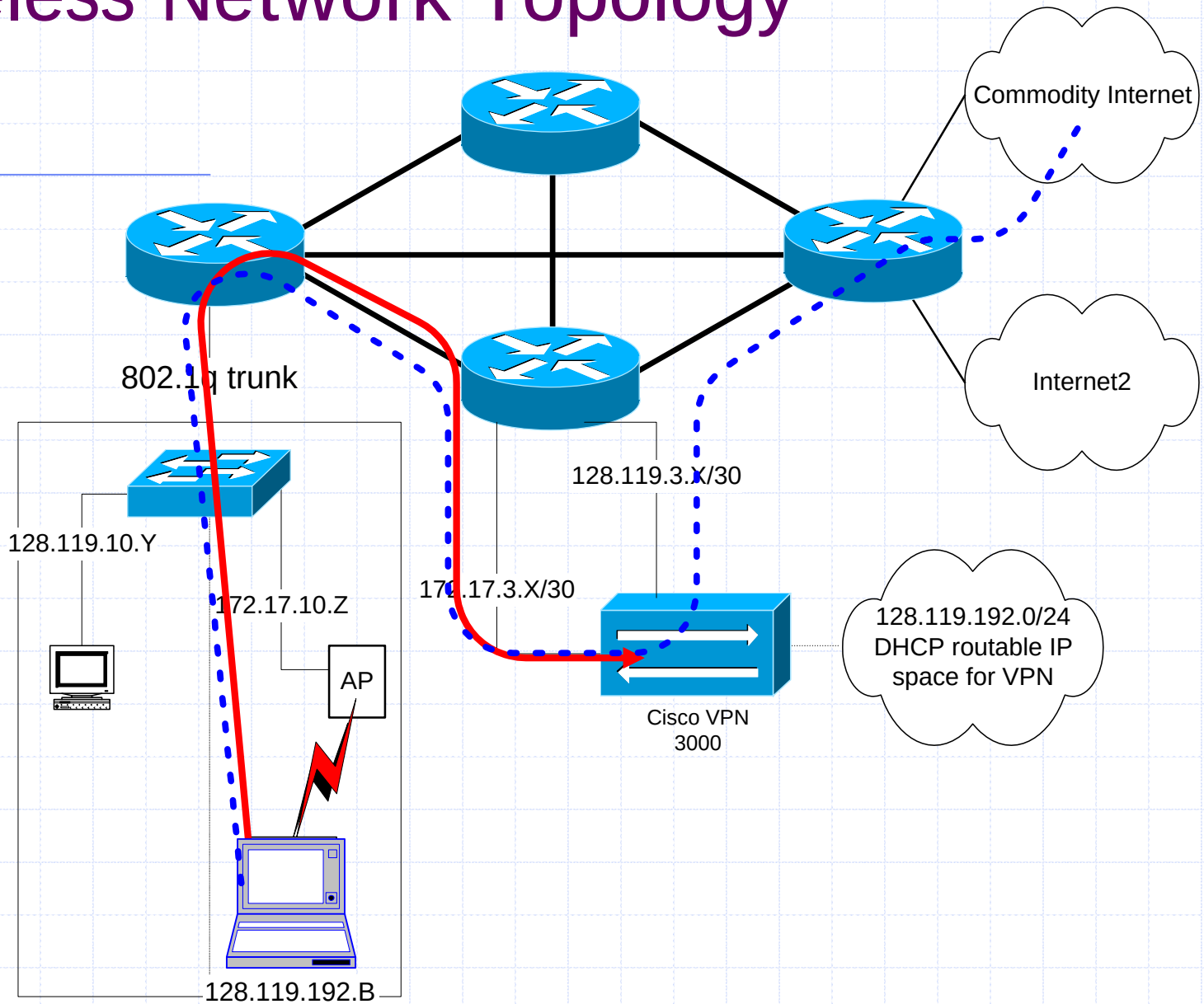
Copyright 2002

Wireless Network Topology

- Private DHCP/DNS for wireless network
- Same hostname for VPN from wireless and wired
  - To minimize client configuration changes
  - Really just DNS spoofing
- Runs over campus network backbone
- Using rfc1918 address space
- Parallel mapping to routable IP space
  - If bldg is 128.119.10.0/24, wireless is 172.17.10.0/24

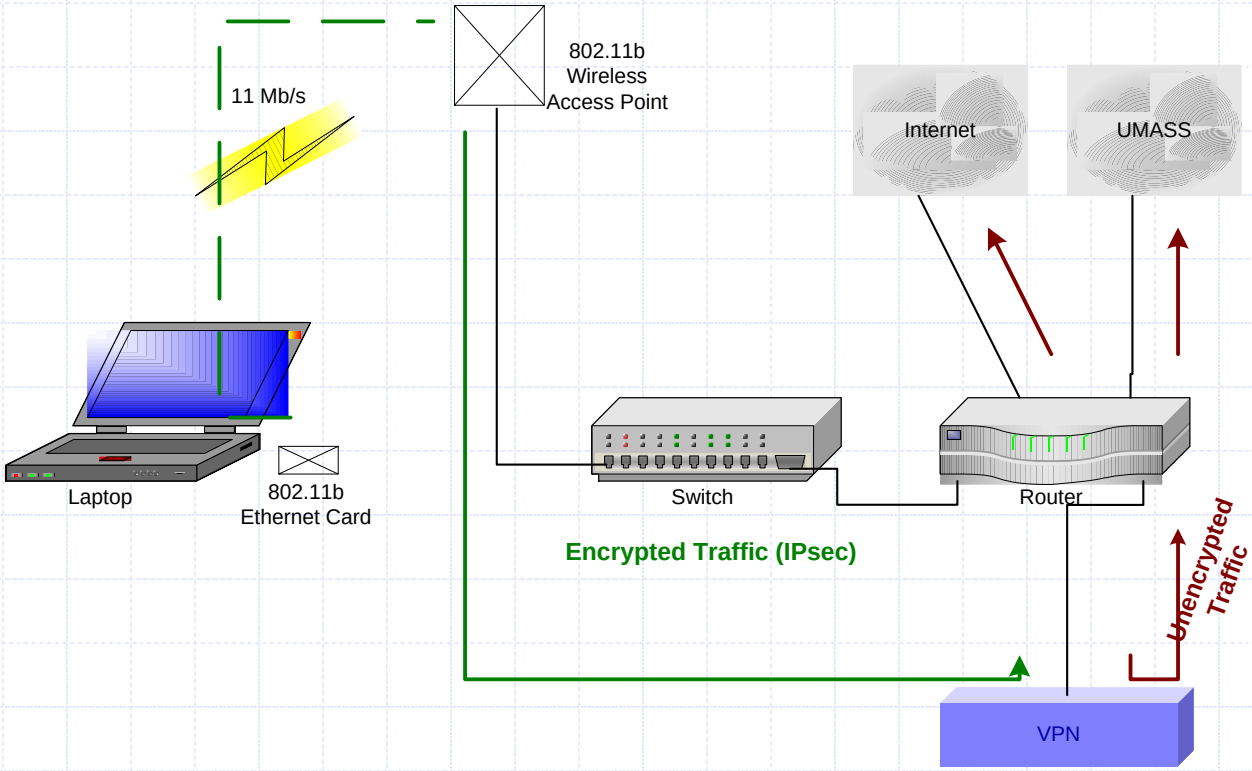
Copyright 2002

Wireless Network Topology



Copyright 2002

Basic Diagram for our Users



Copyright 2002

Enforcing the use of VPN

- Rules without consequences are merely suggestions
- Enforced with Cisco ACLs

```
access-list 120 permit esp 172.17.78.192 0.0.0.63 host
    172.17.3.190
access-list 120 permit udp 172.17.78.192 0.0.0.63 host
    172.17.3.190 eq isakmp
access-list 120 permit udp 172.17.78.192 0.0.0.63 host
    172.17.175.14 eq domain
access-list 120 permit udp 172.17.78.192 0.0.0.63 host
    172.17.166.14 eq domain
access-list 120 permit tcp 172.17.78.192 0.0.0.63 host
    172.17.175.14 eq domain
access-list 120 deny   ip any any log
```

Copyright 2002

Benefits and Drawbacks

- Benefits
  - VPN provides encryption and authentication
  - Use of VPN is required for any access outside of wireless network
  - Not necessary to track/filter MAC address
  - Limited to authorized users
- Drawbacks
  - Client software install required
  - No free Mac client for Cisco VPN 3000
  - Increased overhead
  - No easy access for visitors

Copyright 2002

Where are we going next?

- Looking at some gateway software
  - VPN without the client?
  - 802.1x
- Scalability of VPN
  - VPN concentrators at major nodesites?
- Roaming Access
- Easier access for authorized visitors
- 802.11a or 802.11g?

Copyright 2002

Summary

- Maybe not the best solution
  - But the right one for us at this time
  - Only time will tell...
- Questions?

Copyright 2002