Securing Wireless Networks

Debunking the Myths

Chaffey College
Chino Information Technology Center
Steve Siedschlag, Associate Professor

What is a Wireless Network?

The wireless telegraph is not difficult to understand. The ordinary telegraph is like a very long cat. You pull the tail in New York, and it meows in Los Angeles. The wireless is the same way, only without the cat.

- Attributed to Albert Einstein

What is a Wireless Network? (really)

- It is a LAN
- Extension of Wired LAN
- Uses High Frequency Radio Waves (RF)
- Speed : 2Mbps to 54Mbps
- Distance 100 feet to 15 miles (with fancy antennas)
- Most importantly, It lets you sit on your deck and use your computer while sipping a cocktail of your choice

Is Wireless Secure?

- Not ‘Out of the Box’
- There are steps you can take
  - None are a total solution
  - In combination they may be sufficient
    - Defense in depth
    - Making the hackers ‘go next door’

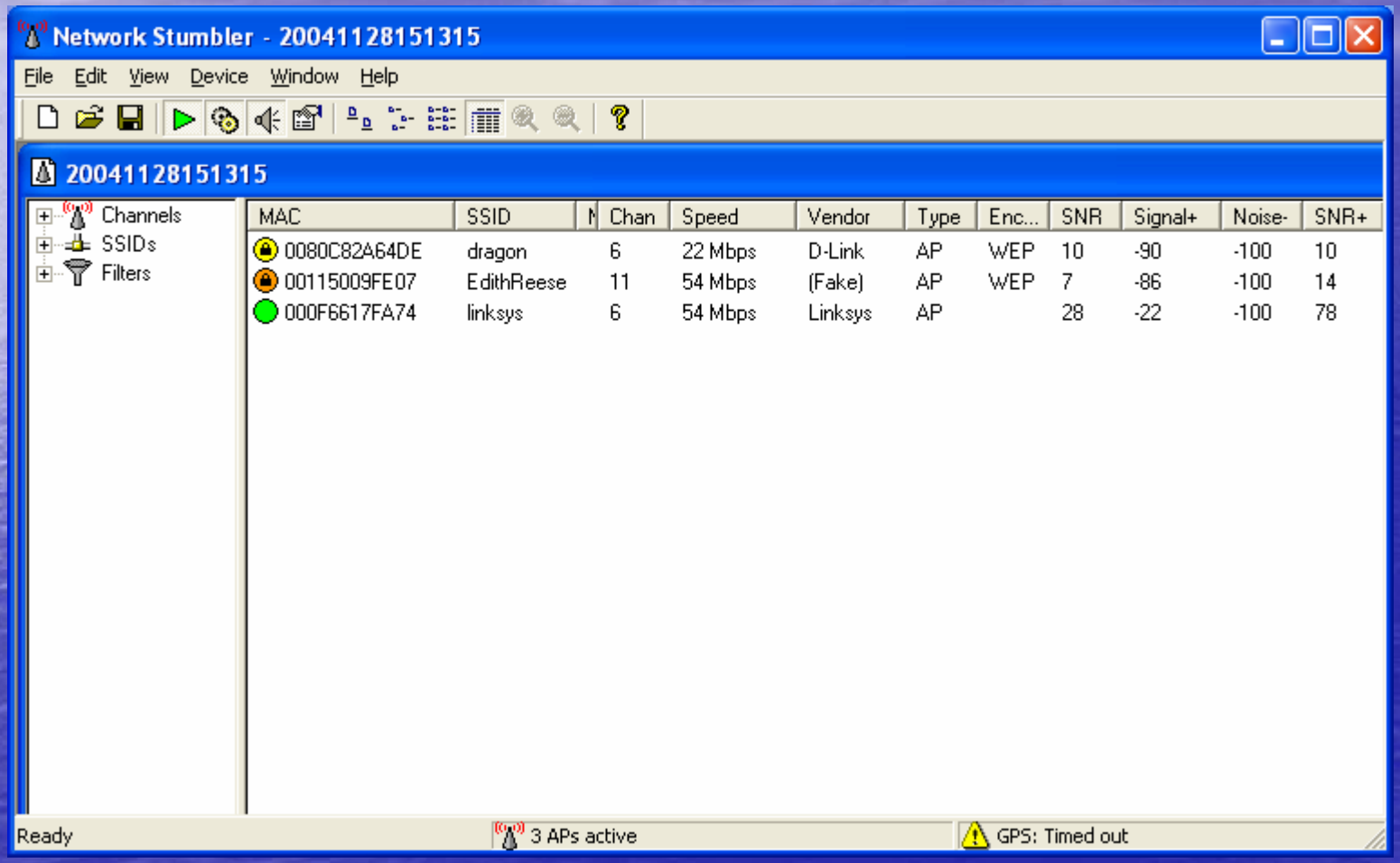
What Is This Phenomenon of Drive-by Hacking?

- Hacker taps into a network using a wireless rig that allows him to park in front of a building and gain access to your network while sitting in the car.
- Unsecured wireless can be likened to installing a wired LAN jack in your front yard.
- Often referred to as “WarDriving”

WarDriving

- Term derived from War dialing, made popular in the movie War Games
- All that is required are a few readily available hardware and software components
  - A PC or PDA with a wireless network card
  - Optionally, a GPS and external antenna
  - Software such as Netstumbler, Kismet, etc.
    - Freely downloadable on the Internet
    - Easy for the average computer user to install

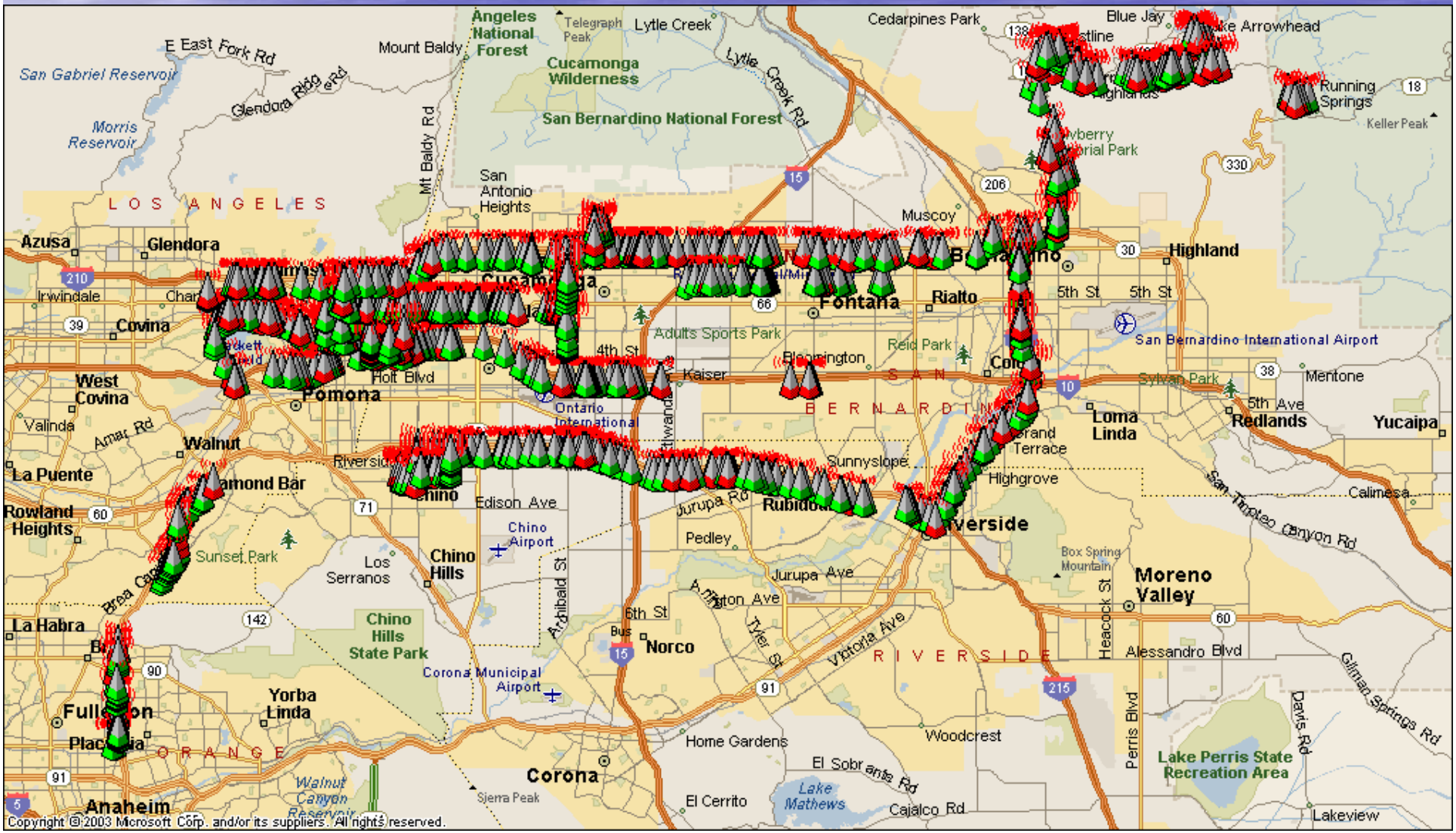
WarDriving


Network Stumbler - 20041128151315
File Edit View Device Window Help
20041128151315
Channels
SSIDs
Filters
MAC SSID Chan Speed Vendor Type Enc... SNR Signal+ Noise- SNR+
0080C82A64DE dragon 6 22 Mbps D-Link AP WEP 10 -90 -100 10
00115009FE07 EdithReese 11 54 Mbps (Fake) AP WEP 7 -86 -100 14
000F6617FA74 linksys 6 54 Mbps Linksys AP 28 -22 -100 78
Ready
3 APs active
GPS: Timed out

WarDriving (continued)

- The software logs configuration of detected WiFi devices, optionally including the map location
- Moving the WarDriving rig from place to place will eventually develop a large database of wireless networks and their locations

WarDriving


Angeles National Forest
Cucamonga Wilderness
San Bernardino National Forest
San Gabriel Reservoir
Morris Reservoir
Mount Baldy
Telegraph Peak
Lytle Creek
Cedarpines Park
Blue Jay
Running Springs
Keller Peak
Lake Arrowhead
LOS ANGELES
ORANGE
RIVERSIDE
SAN BERNARDINO
Azusa
Glendora
Irwindale
Covina
West Covina
Pomona
Walnut
La Puente
Rowland Heights
La Habra
Fullerton
Anaheim
Placentia
Yorba Linda
Chino Hills
Chino Hills State Park
Chino Airport
Corona Municipal Airport
Corona
Norco
Home Gardens
El Cerrito
Lake Mathews
Woodcrest
Lake Perris State Recreation Area
Moreno Valley
Perris
Riverside
Rubidoux
Jurupa Valley
Fontana
Rialto
Bloomington
Muscoy
San Antonio Heights
Highland
San Bernardino
Loma Linda
Redlands
Yucaipa
Calimesa
Mentone
Grand Terrace
Colton
Ontario International
San Bernardino International Airport
Adults Sports Park
Reid Park
Sylvan Park
Sunnyslope
Highgrove
Pedley
Sunset Park
Los Serranos
Edison Ave
Jurupa Rd
Jurupa Ave
Victoria Ave
Alessandro Blvd
Cajalco Rd
El Sobrante Rd
Lakeview
Copyright © 2003 Microsoft Corp. and/or its suppliers. All rights reserved.

WarDriving (continued)

- IS THIS LEGAL?
  - Probably, if that is all the farther it goes
  - Accessing a network is another matter entirely
    - Definitely NOT legal if you do not have the owner's permission
    - Even if you ONLY use it to access the Internet
    - Most Wardrivers do NOT access the networks that they detect
      - Surprised?

Why Is It Easy to Get Into a Wireless Network?

- The most common wireless local area networks are built based on a standard known as 802.11
- The security of this technology has been demonstrated to be inadequate when challenged by simple hacking attempts
- In addition, products sold with this technology are usually delivered with security functionality disabled.

What if I Change My Network's Name?

- That is more than most do, but it doesn't make you much more secure
  - Your SSID (Service Set ID) is beaconed by your AP
  - You can turn off beaconing, but your SSID is still sent each time a computer connects and is easily captured
    - At least your neighbor will not accidentally connect!

I Also Changed My Channel

- Once again, that is more than most do, but it does nothing for security
  - Windows xp will automatically scan all the available channels for an active access point
- It is helpful to select a channel that does not overlap your neighbor!
  - This will improve the function of your WLAN
  - Most Access Points are set to channel 6 by default
    - Pick 1 or 11 for your AP

Does the Built-in WEP Encryption Option Make Me Secure?

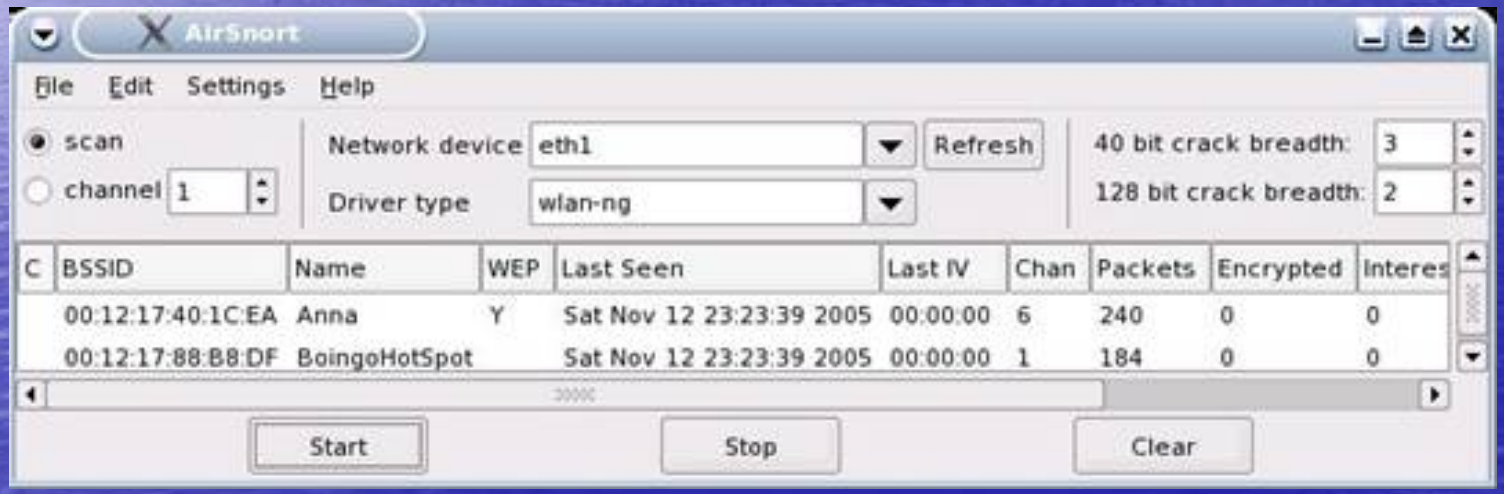
- Not if you don't use it!
  - Less than 50% of detected WLANs have WEP enabled
  - Many that do, have 64bit rather than 128bit encryption
- Even if you use it...
  - The algorithms used are well understood and not considered weak, but the way in which they are used has resulted in a number of easily exploitable weaknesses

Does the Built-in WEP Encryption Option Make Me Secure? (continued)

- WEP weakness
  - WEP security flaws were documented in a 2001 UC Berkley study
    - Weak encryption (never intended for repeated use)
    - Short keys (64bits – 24bit Init Vector = 40 bits)
    - Static Keys
    - No distribution method (shared key)

Does the Built-in WEP Encryption Option Make Me Secure? (continued)

- There are freely distributed programs that can crack WEP keys (but it takes a while)



What about WPA?

- WPA is MUCH more secure
  - Encryption keys are frequently rotated
    - Before they can be cracked
  - WPA uses a passphrase as the starting point for the key exchange
    - Much more secure if a complex passphrase is used
      - Several upper & lower case letters, numbers, symbols
  - Can also be used with enterprise systems (RADIUS) for more security
    - Not practical in a home or small office

So WPA Makes Me Secure?

- Not if you don't use it!
  - Are you seeing a trend here?
- IF you don't use too simple a passphrase
  - There are tools that will crack passphrases, but it could take many years on a COMPLEX passphrase

What is MAC Address Filtering?

- Every network card ever produced has a unique address that can be used to limit access to your wireless network
- This feature is disabled by default

So...MAC Address Filtering Makes Me Secure?

- Not if you don't use it!
  - OK, so this is getting old
- Authorized computers send their MAC address when they attempt to connect
  - This can be logged
- In spite of what some people believe, MAC addresses can be changed on most network cards (at least temporarily)

Are You Telling Me It's Hopeless?

- NO
  - Most of the security measures we have already described work well when used correctly
  - When several are used in conjunction, they are a formidable barrier to attack
  - Just being better than the status quo is often enough to get the hacker to 'go next door'

Why Do I Care?

- Why do I care if somebody uses my connection to check their mail?
  - If that was all they did, you probably wouldn't care
  - Those engaged in illegal activity on the Internet frequently steal network connections to 'conduct business'
    - Try explaining to the FBI or the NSA that you are 'not a crook'
  - Many Viruses, Worms and Denial of Service attacks are launched using stolen network connections in order to hide the true source

Then What Should I Do?

- Most modern access points support WEP or WPA
  - Use the highest level of security that your Access Point and computer network card supports (they must be the same).
- MAC filtering and disabling beaconing are good added measures
  - This will make it difficult for visitors to connect to your network
- Change the channel, password and address of your AP

HOW...?

- You will need to spend a little time in the manual or website for your access point
- Some examples follow, but every AP works slightly differently

Wireless LAN Protection Strategies

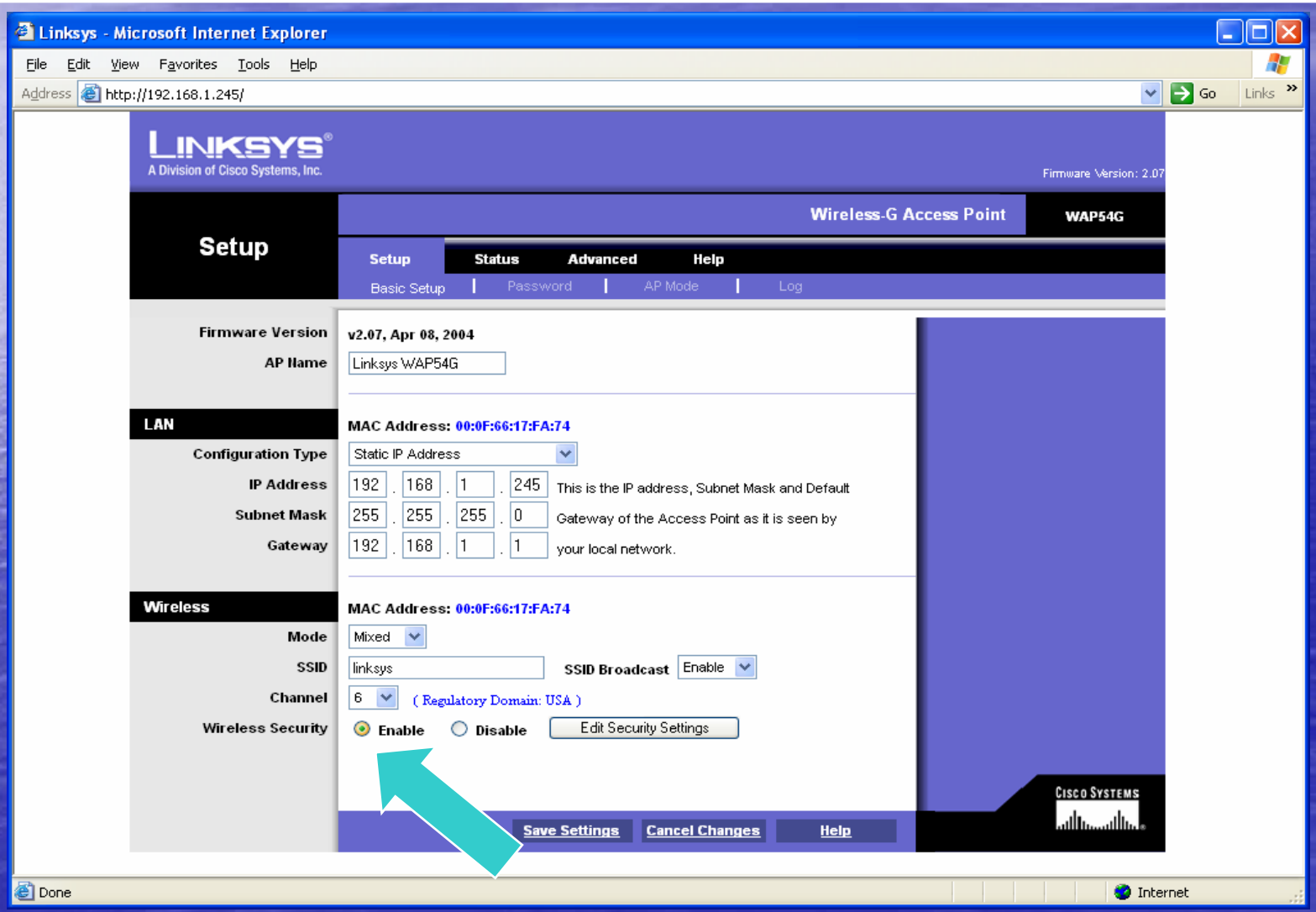
Chaffey College
Chino Information Technology Center
Steve Siedschlag, Associate Professor

Recommendations

- Wireless LAN related Configuration
  - Enable WEP, use 128bit key
  - Disable SSID Broadcasts
  - No SNMP access
  - Use MAC (hardware) address to restrict access
  - Non-default Access Point password
  - Change default Access Point Name
  - Use 802.1x / WPA / 802.11i (when available)

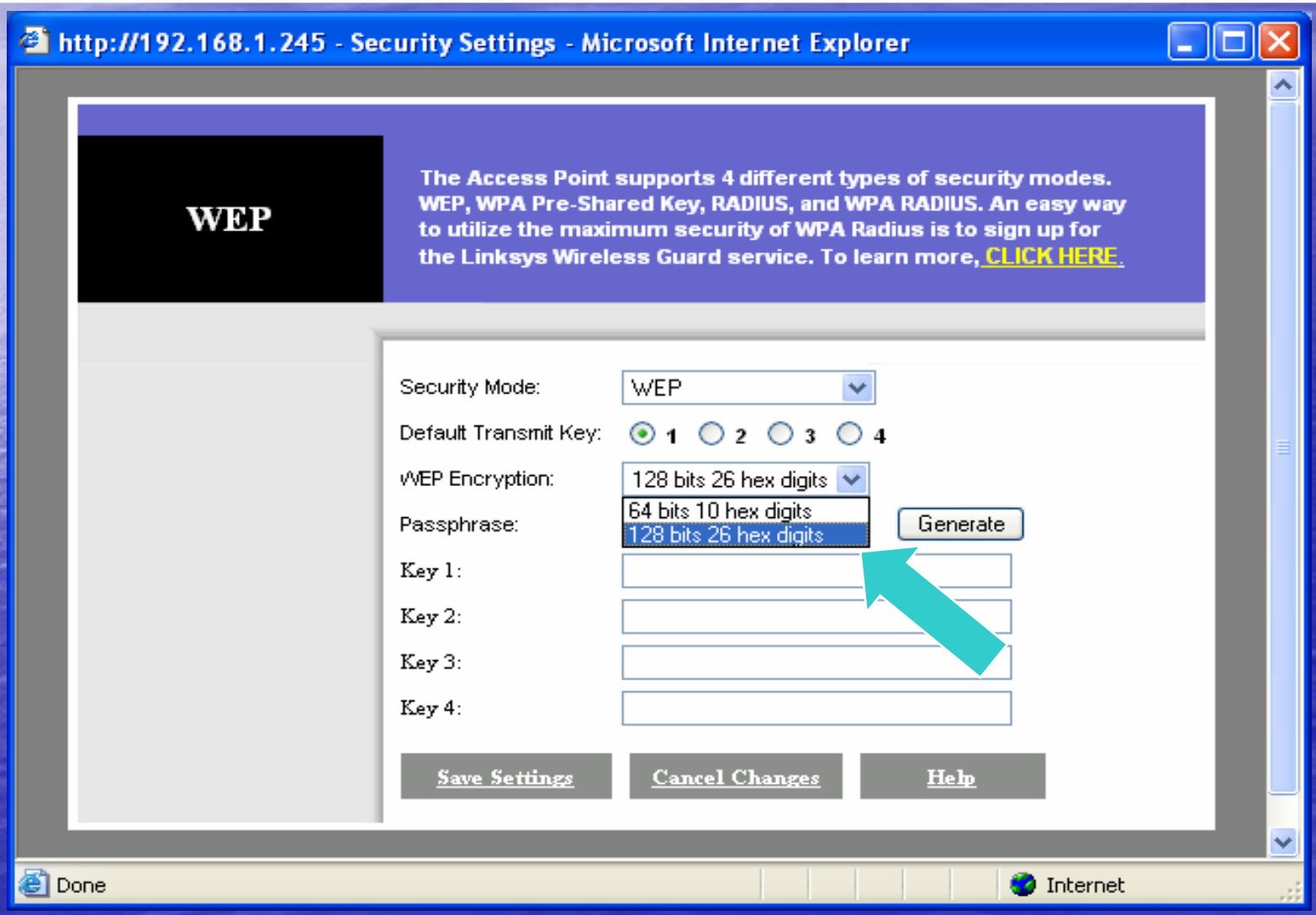
Wireless LAN related Configuration

Enable WEP, use 128bit key



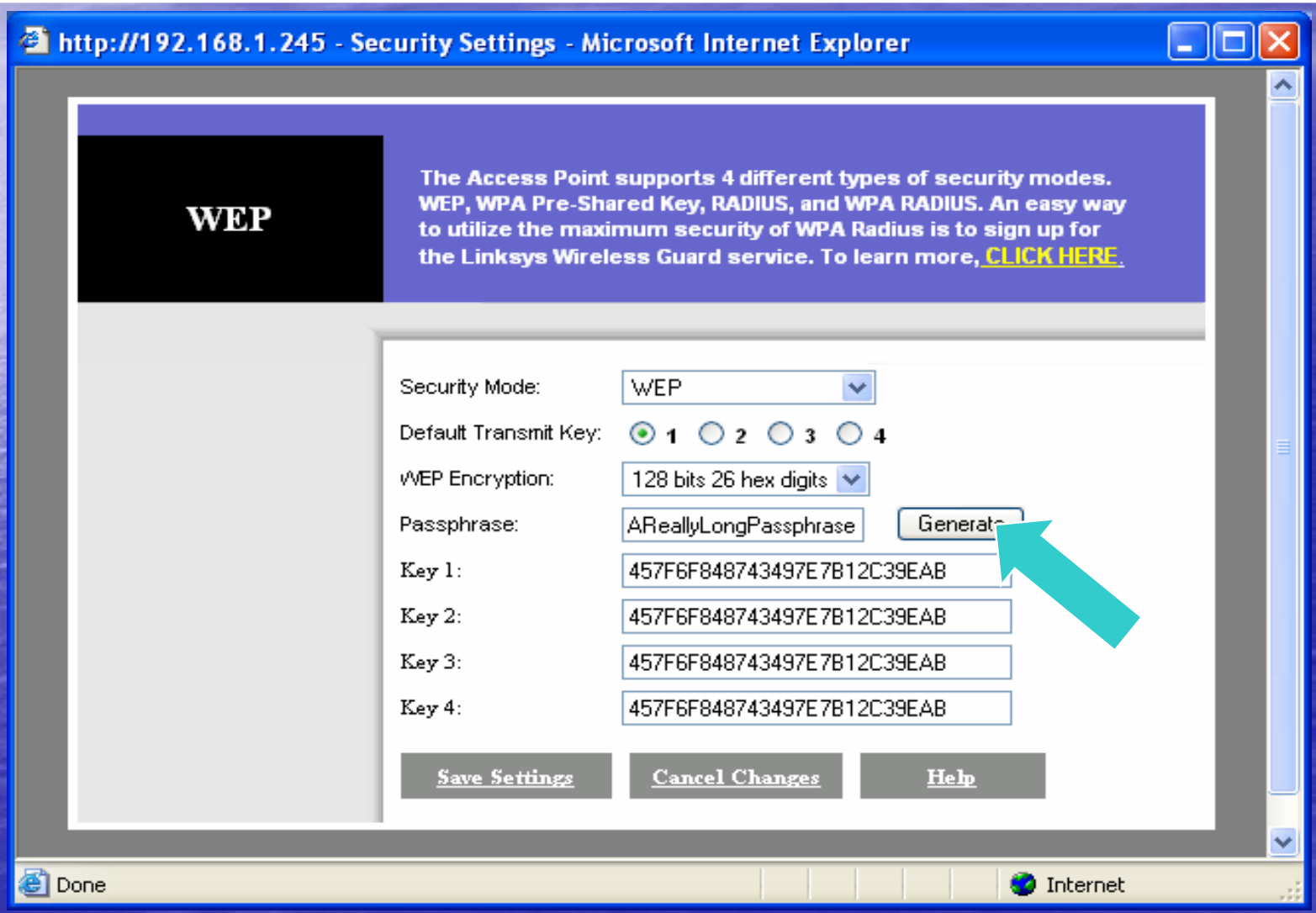
Wireless LAN related Configuration

Enable WEP, use 128bit key



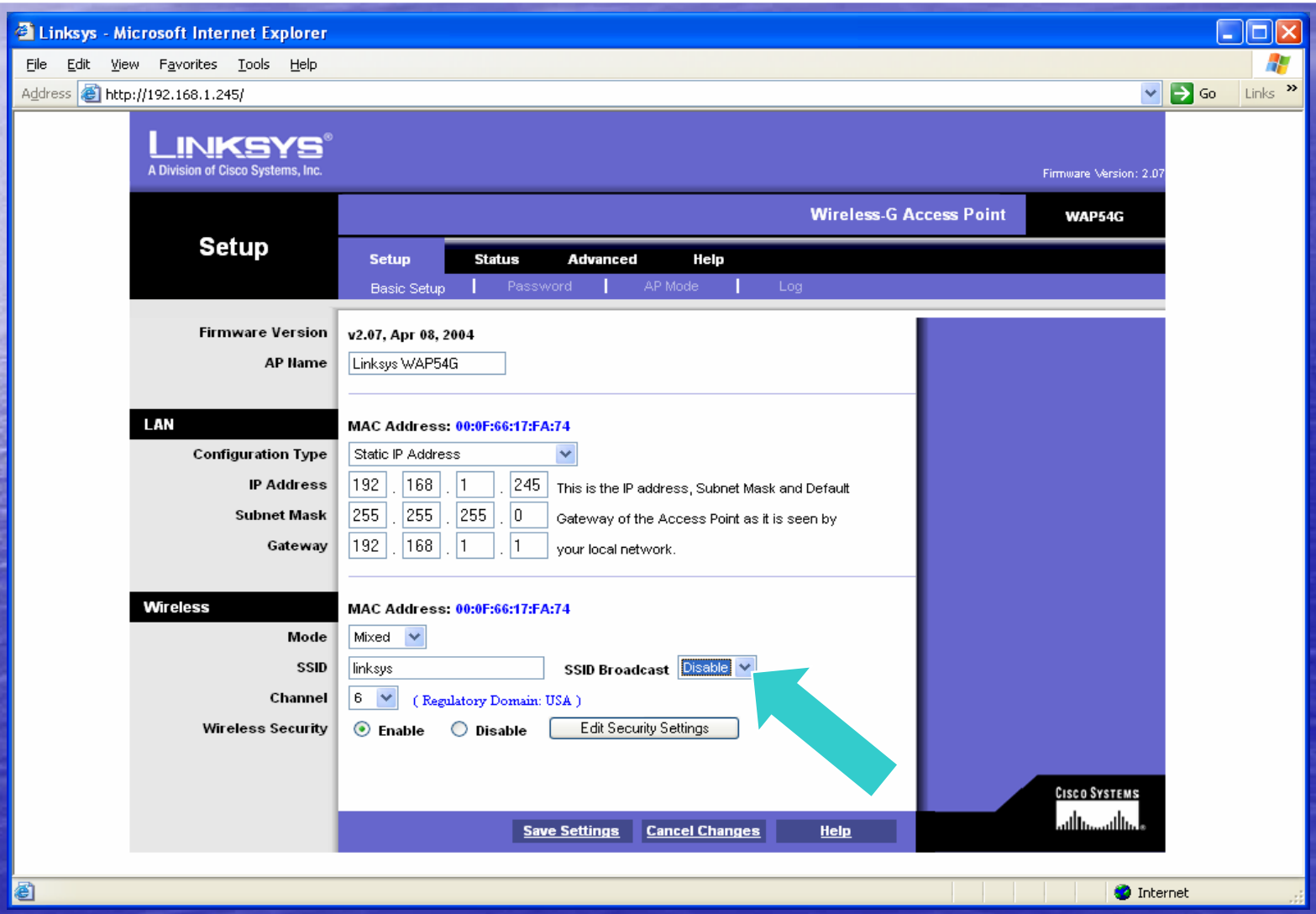
Wireless LAN related Configuration

Enable WEP, use 128bit key



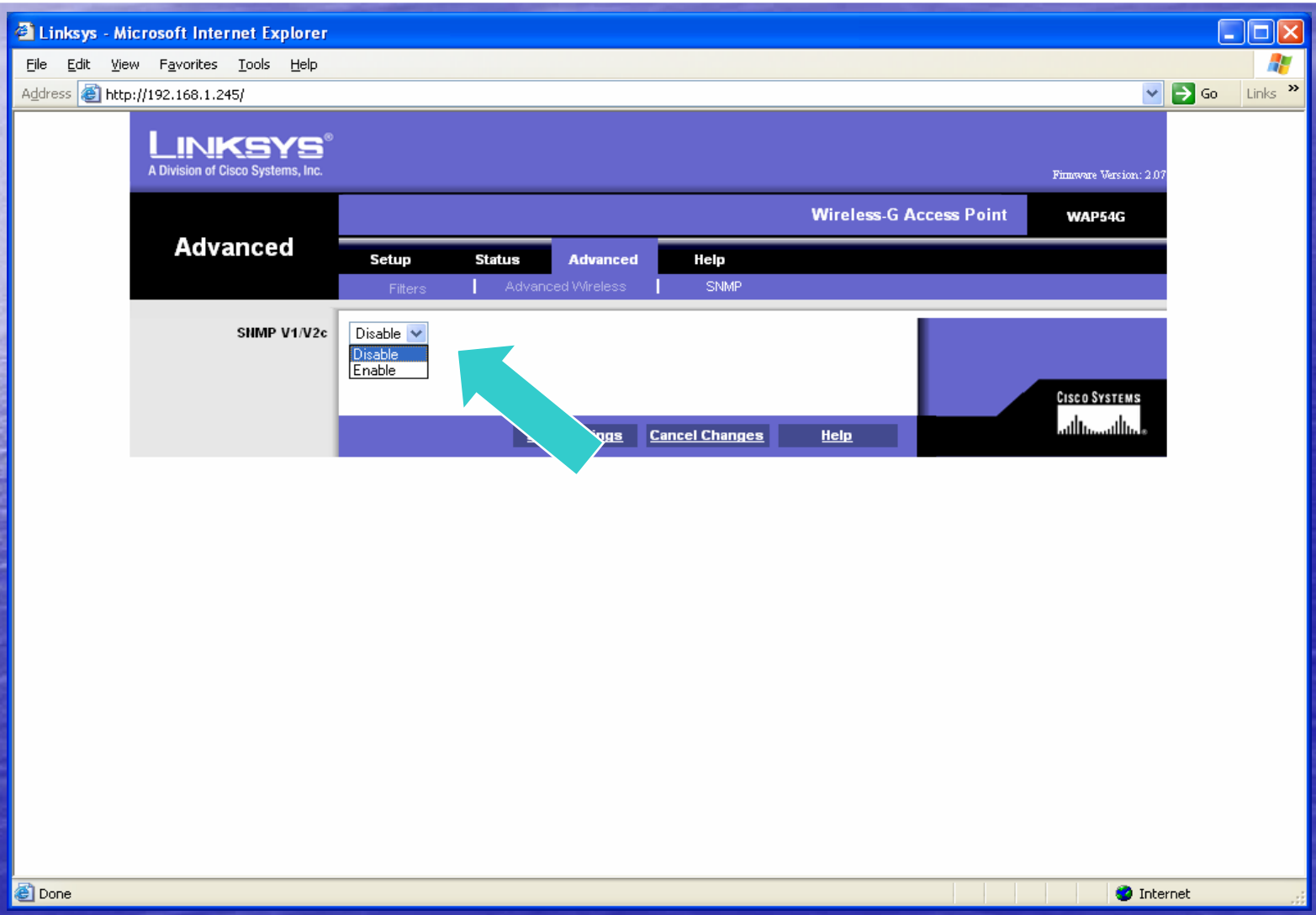
Wireless LAN related Configuration

Disable SSID Broadcast



Wireless LAN related Configuration

No SNMP access



Wireless LAN related Configuration

Use 802.1x / WPA / 802.11i (when available)

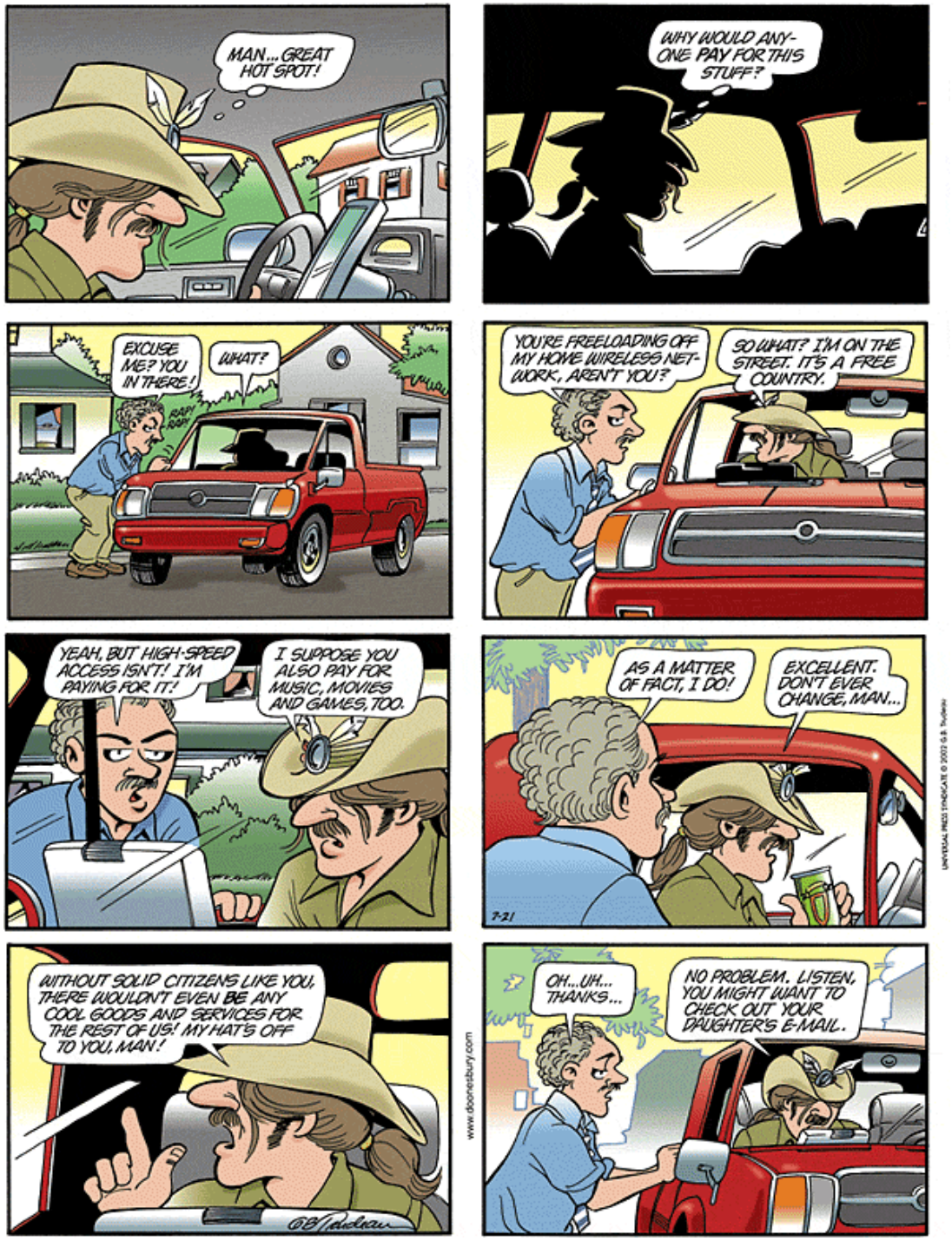
General Recommendations

- Always (wired or wireless)
  - Install virus protection software plus automatic frequent pattern file update
  - Shared folders must impose password
- Management Issue
  - Prohibit installation of AP's without authorization
  - Discover any new APs constantly (NetStumbler is free, Antenna is cheap)
  - Power off Access Point when not in use
  - Carefully select the physical location of your AP, not near windows or front doors.

Thank You!

- Computer Network Security Resources at the Robert Pile Chaffey College Chino Information Technology Center
  - CIS-420 PC Security & Privacy
  - CISNTWK-440 Fund. Of Network Security (Security+)
  - CISNTWK-441 Firewalls & Intrusion Detection
  - CISNTWK-442 Disaster Recovery Planning
  - CISNTWK-445 Windows Security Administration
  - CISNTWK-447 Linux Security Administration

Steve Siedschlag steve.siedschlag@chaffey.edu
Associate Professor


MAN... GREAT HOT SPOT!
WHY WOULD ANY-ONE PAY FOR THIS STUFF?
EXCUSE ME? YOU IN THERE!
WHAT?
RAP! RAP!
YOU'RE FREELOADING OFF MY HOME WIRELESS NET-WORK, AREN'T YOU?
SO WHAT? I'M ON THE STREET. IT'S A FREE COUNTRY.
YEAH, BUT HIGH-SPEED ACCESS ISN'T! I'M PAYING FOR IT!
I SUPPOSE YOU ALSO PAY FOR MUSIC, MOVIES AND GAMES, TOO.
AS A MATTER OF FACT, I DO!
EXCELLENT. DON'T EVER CHANGE, MAN...
7-21
WITHOUT SOLID CITIZENS LIKE YOU, THERE WOULDN'T EVEN BE ANY COOL GOODS AND SERVICES FOR THE REST OF US! MY HAT'S OFF TO YOU, MAN!
OH...UH... THANKS...
NO PROBLEM. LISTEN, YOU MIGHT WANT TO CHECK OUT YOUR DAUGHTER'S E-MAIL.
UNIVERSAL PRESS SYNDICATE © 2007 G.B. Trudeau
www.doonesbury.com