

# 2013 Summer Camp: Wireless LAN Security Exercises

2013 JMU Cyber Defense Boot Camp

# Questions

- Have you used a wireless local area network before?
  - At home?
  - At work?
- Have you configured a wireless AP before?
- Have you heard these terminologies before?
  - WiFi (Wireless Fidelity)
  - Wireless access point (AP), service set identification (SSID)
  - Hot spots, evil twins
  - WEP, WPA, WPA2

# Organization

- Introduction to wireless LAN
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2
- Exercises
  - Cracking captured WEP traffic 1
  - Crack captured WPA-PSK traffic 2
  - Cracking captured WEP traffic 3
  - Crack captured WPA-PSK traffic 4

# Impatient with Background?

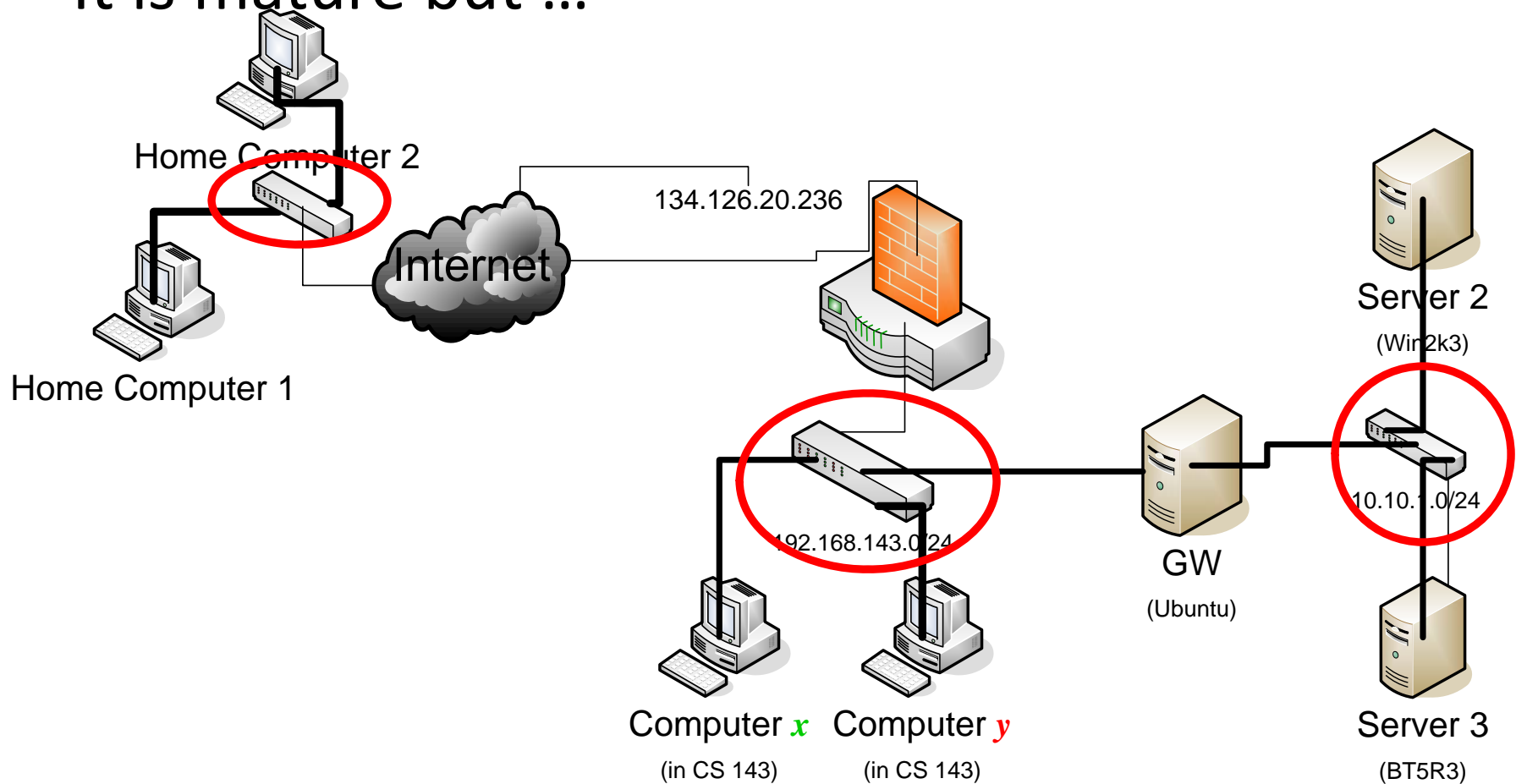
- You can jump to the exercise part ([slide 45](#)) now
  - **IF** you believe that you have all the background

# Road Map

- Introduction to wireless LAN
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2
- Exercises
  - Cracking captured WEP traffic 1
  - Crack captured WPA-PSK traffic 2
  - Cracking captured WEP traffic 3
  - Crack captured WPA-PSK traffic 4

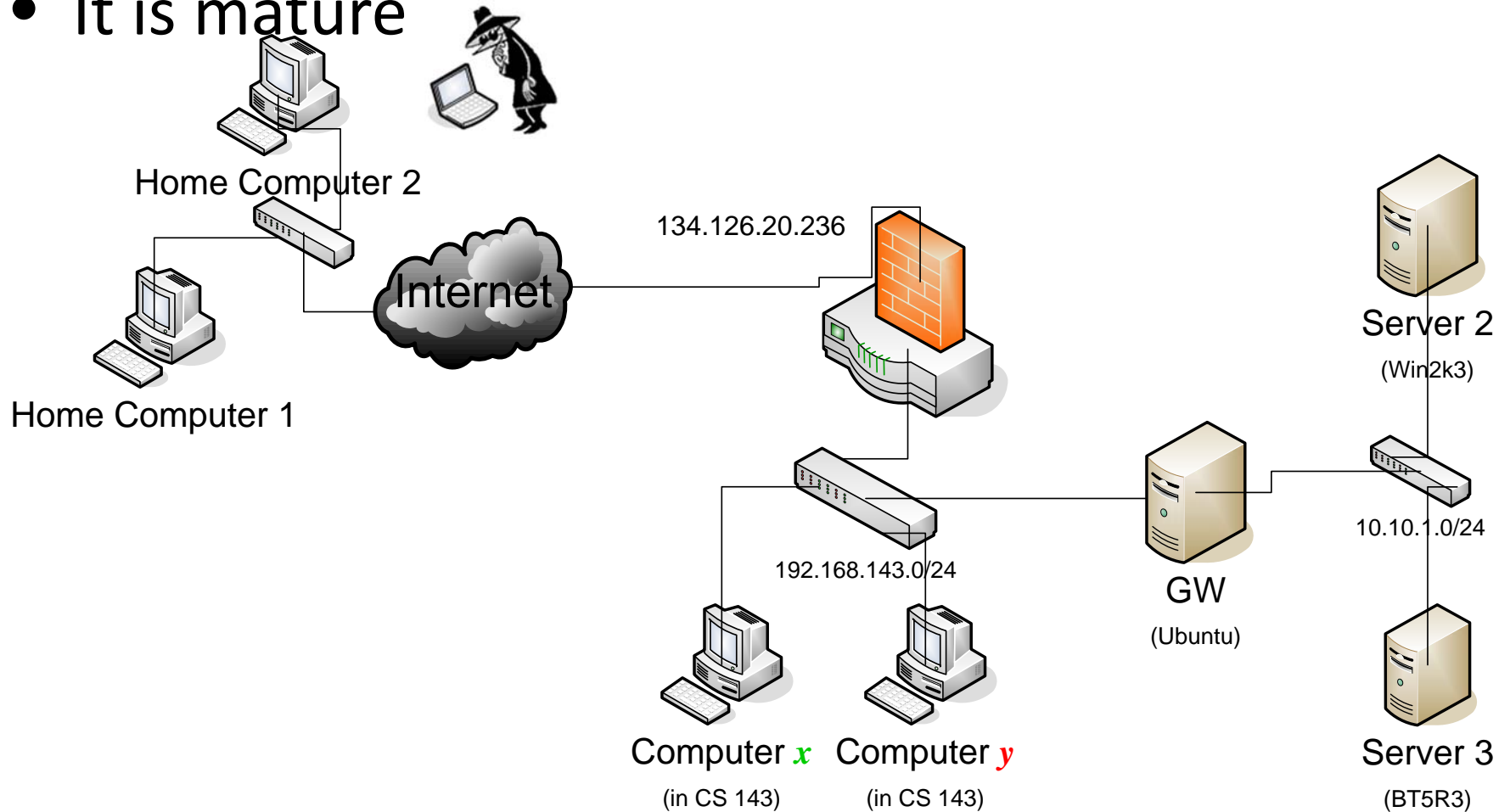
# Wired Computer Networks

- It is mature but ...

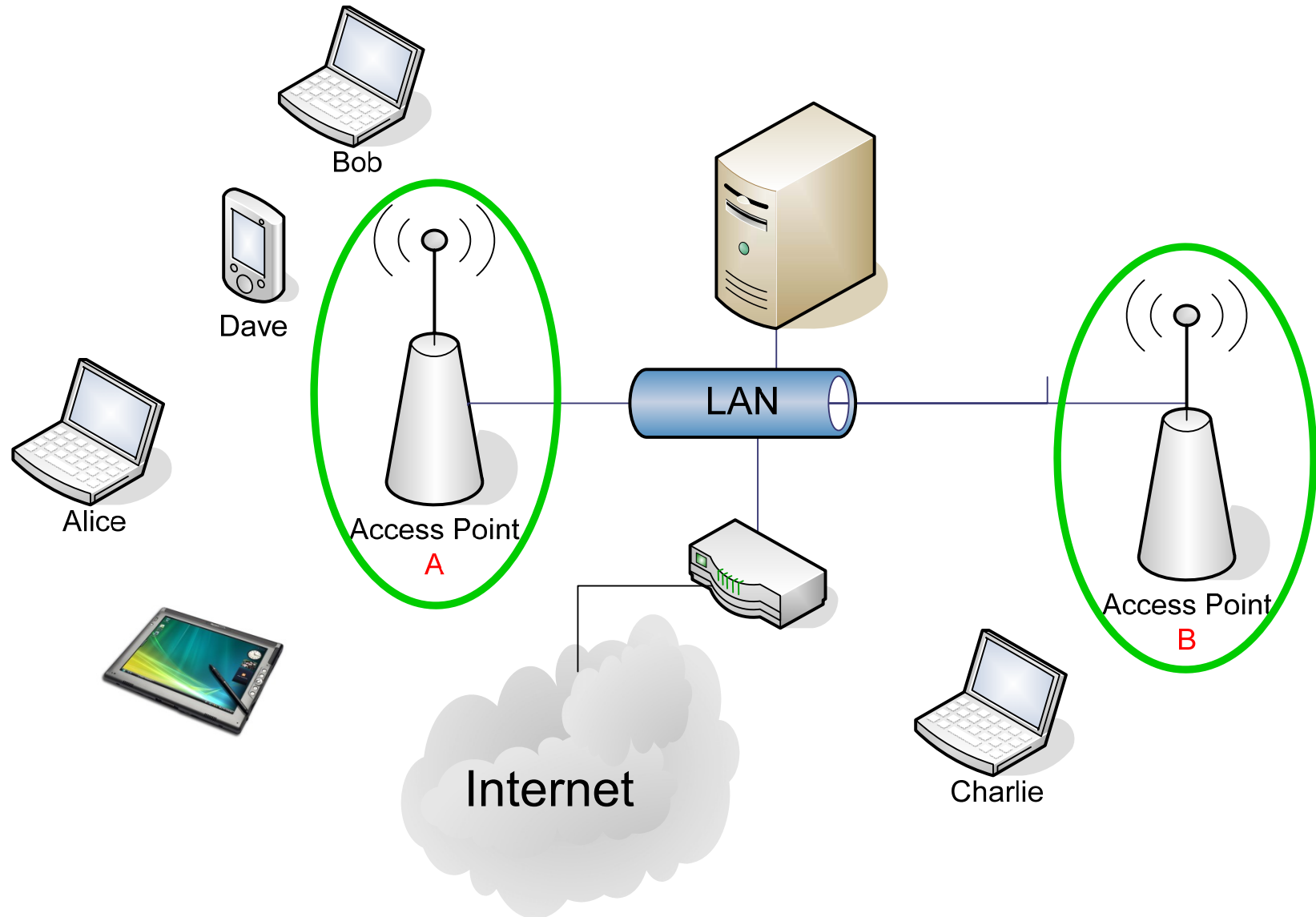


# Wired Computer Network: Inconvenience

- It is mature



# Wireless Would be Nice





# Hardware?



Wireless Access  
Point (AP)

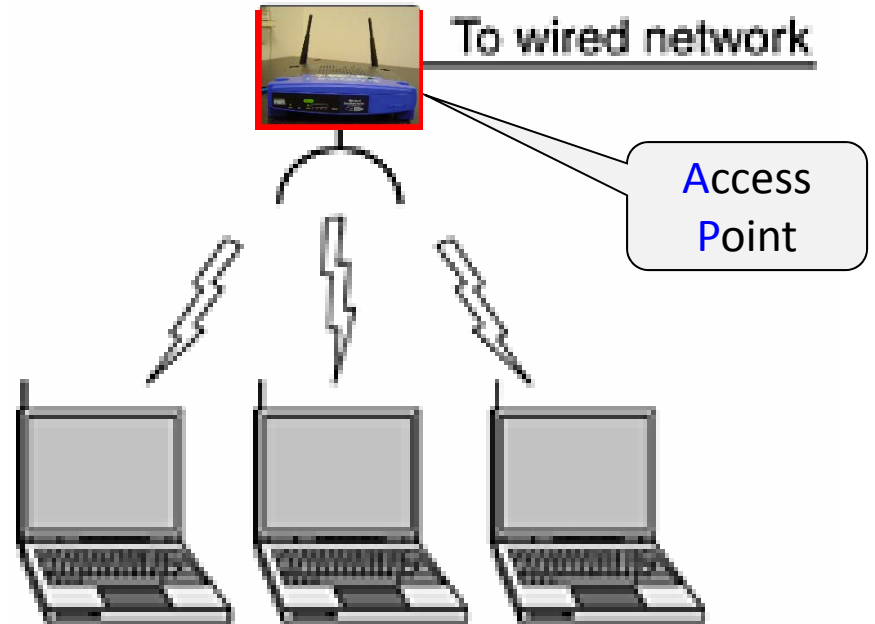


Bob



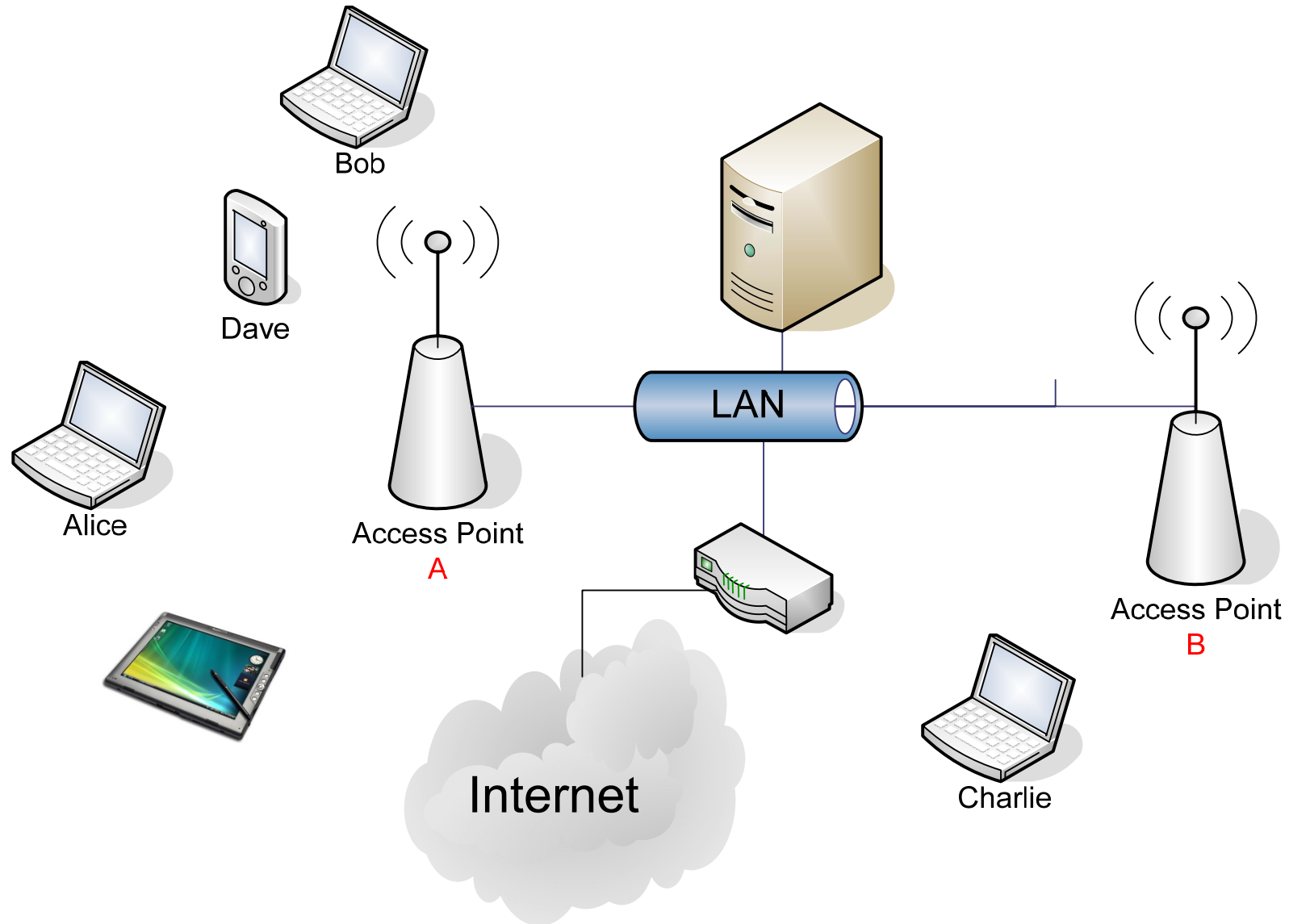
Wireless card (WiFi  
adapter card)

# Wireless LAN Topology



- ① Independent Basic Service Set (BSS, IBSS): ad hoc mode (independent, peer-to-peer): no access point
- ② **Extended Service Set (ESS): use AP; Infrastructure mode:**  
one access point manages; **greater range**

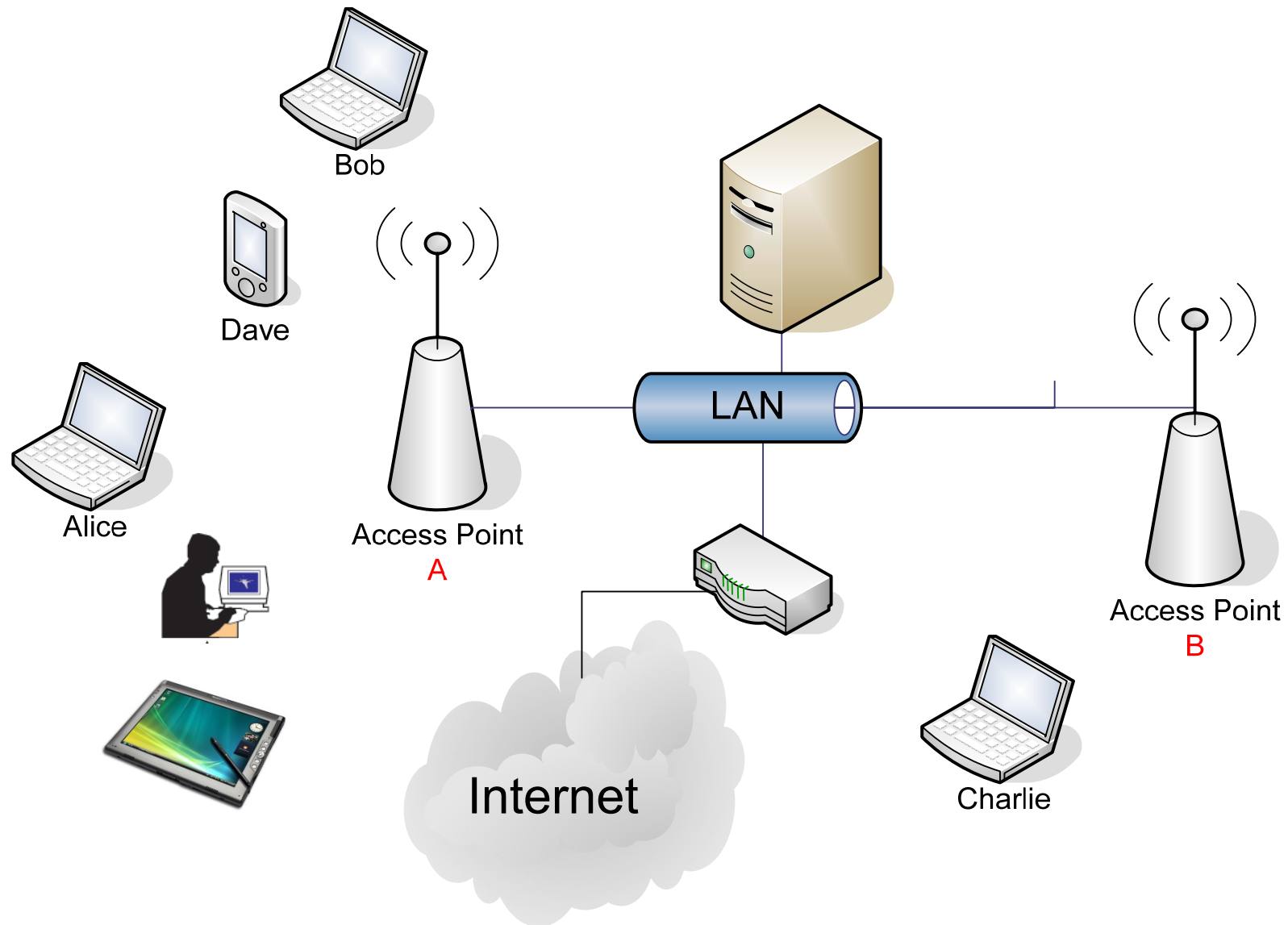
# Typical Wireless LAN Configuration



# Road Map

- Introduction to wireless LAN
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2
- Exercises
  - Cracking captured WEP traffic 1
  - Crack captured WPA-PSK traffic 2
  - Cracking captured WEP traffic 3
  - Crack captured WPA-PSK traffic 4

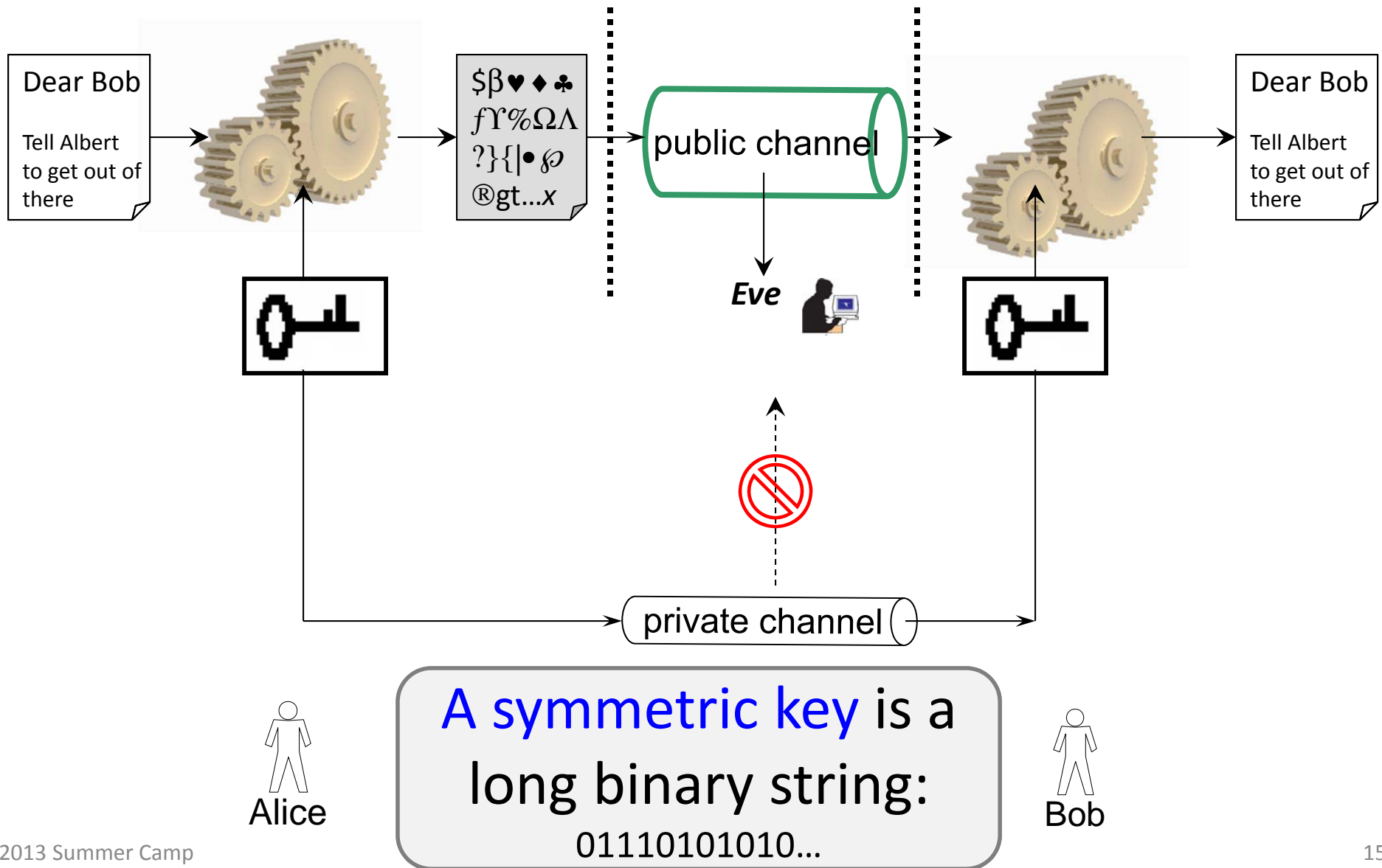
# Wireless LAN Insecurity



# Attacks Against Wireless LAN

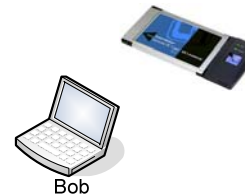
- Hook to your wireless network and steal your data from your servers
- Eavesdrop on your **wireless** channel and steal passwords/secrets in transit

# Symmetric Key Encryption



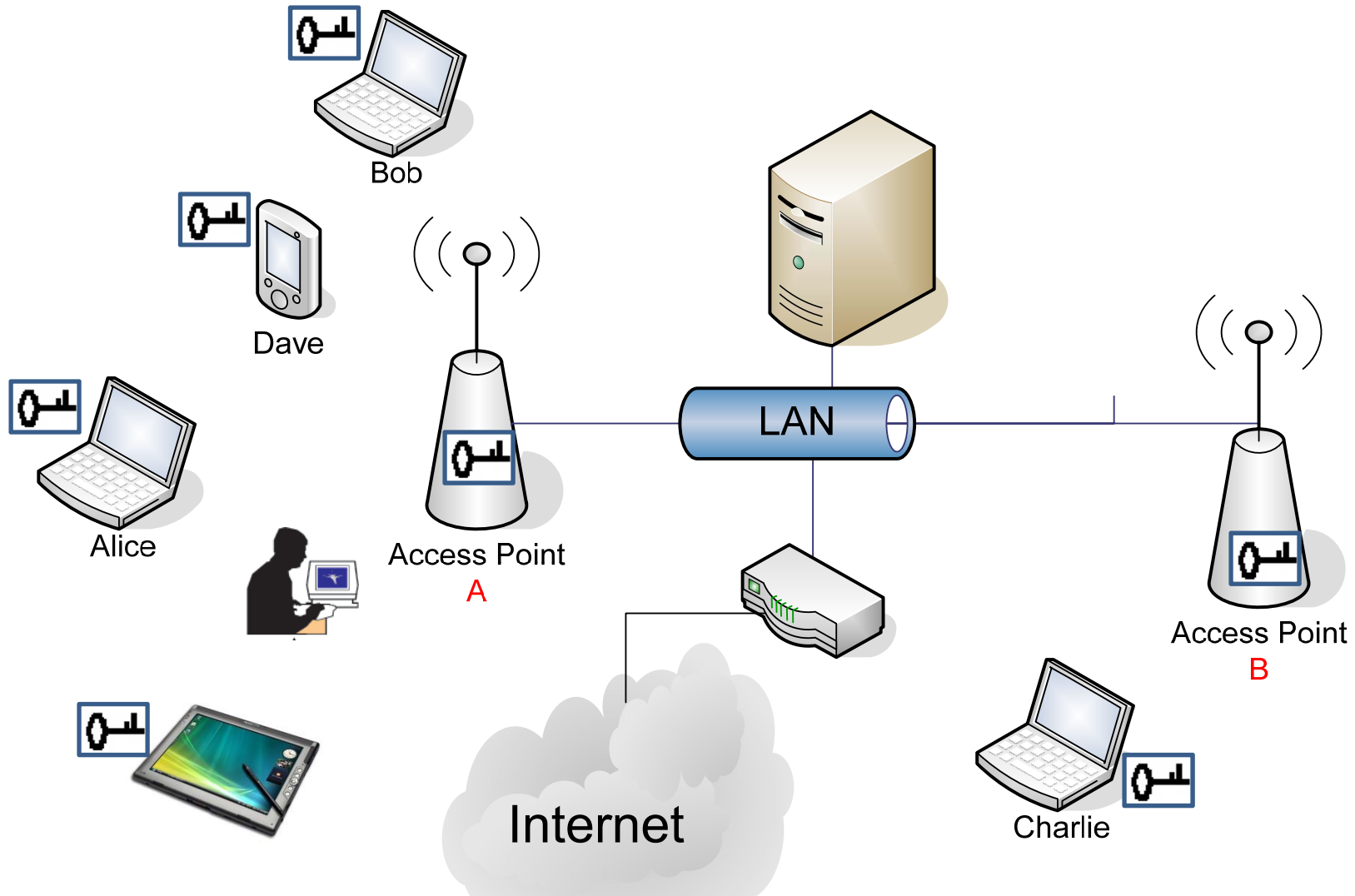
# WEP

- Wired-equivalent privacy (WEP)
  - Security based on a shared secret (WEP key)
- Goals
  - Do not know the WEP key? No association or data transmission
  - Do not know the WEP key? No eavesdropping
  - Do not know the WEP key? No data injection
- Symmetric-key encryption algorithm: RC4
  - Implemented on
    - AP
    - Laptop: implemented by hardware





# WEP: all users share the same key



 A WEP key is either 40 bits or 104 bits

# ① WEP Configuration on AP

① Wire your PC to your AP

– Your PC uses DHCP

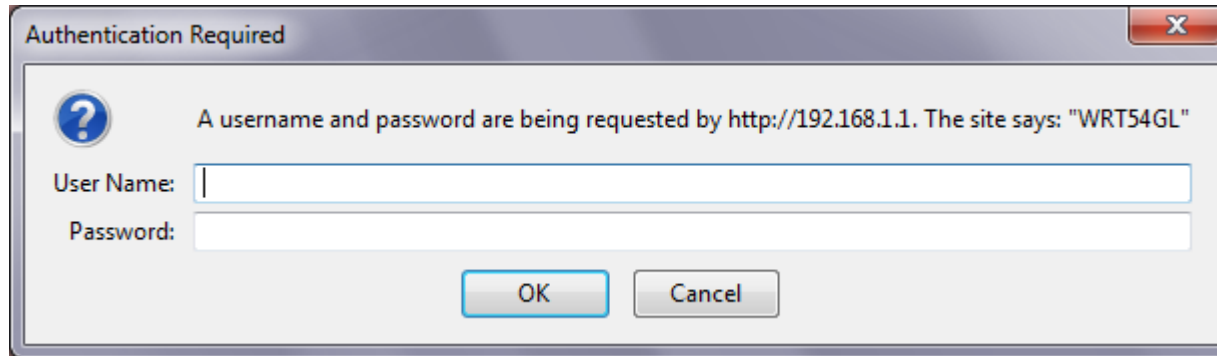
② Check the IP address of your PC – **ipconfig**

```
Ethernet adapter Local Area Connection:
```

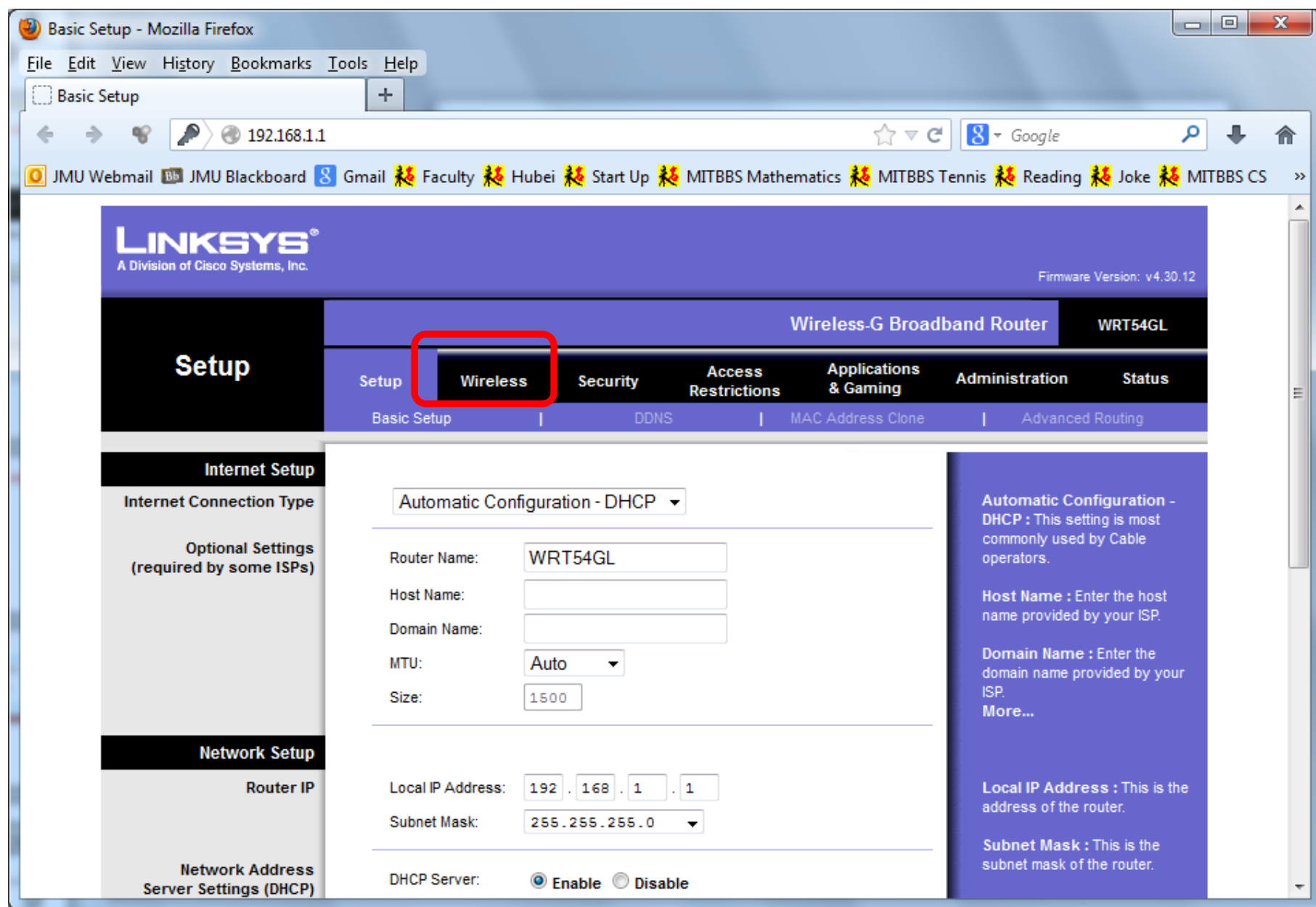
```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::2cf8:20f7:b1b8:5e88%10  
IPv4 Address. . . . . : 192.168.1.100  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.1.1
```

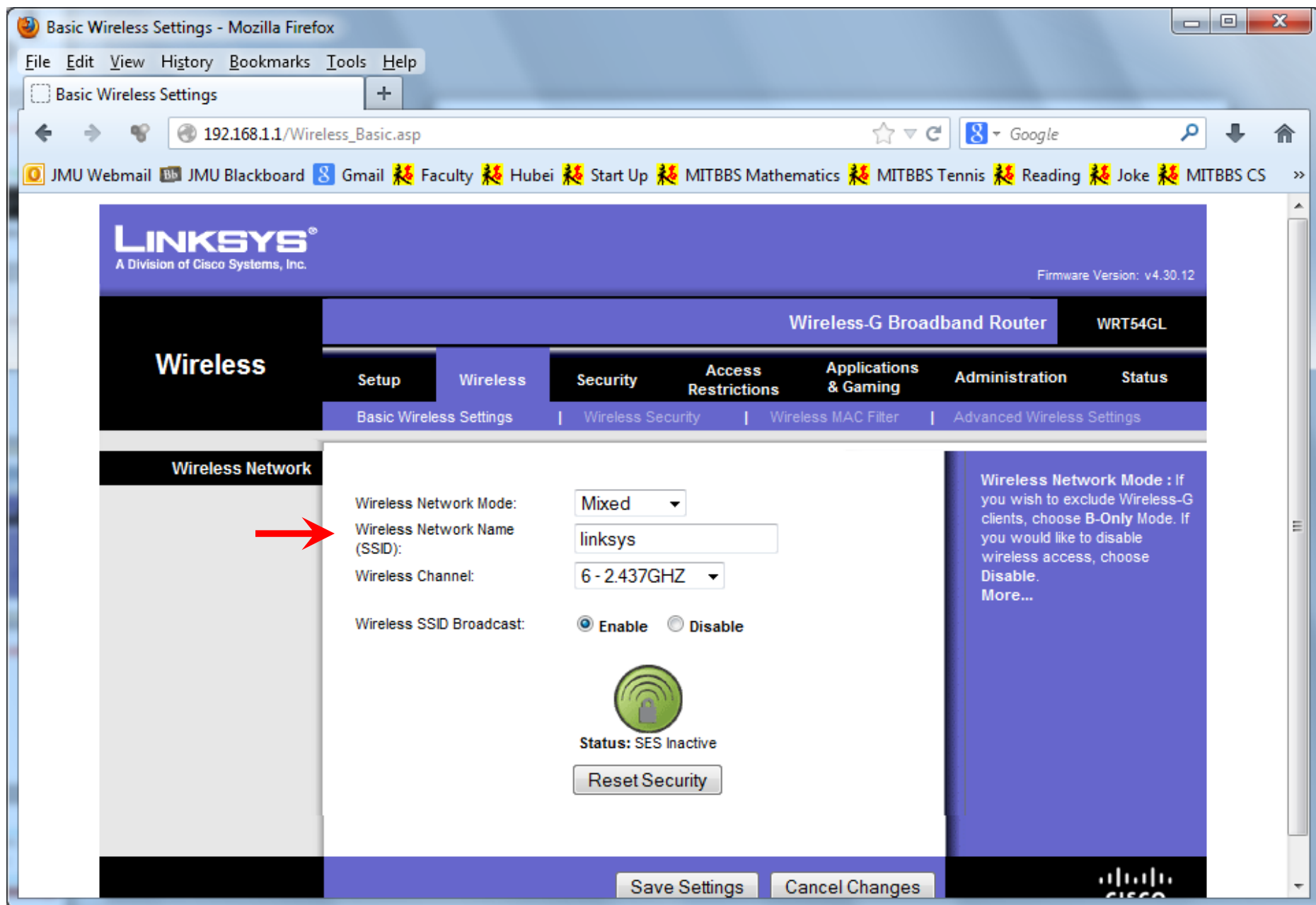
③ Open web browser, type in 192.168.1.1

# WEP Configuration on AP



- ④ Use the default username and password
  - For Linksys, it is admin/admin





Basic Wireless Settings - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Basic Wireless Settings

192.168.1.1/Wireless\_Basic.asp

JMU Webmail JMU Blackboard Gmail Faculty Hubei Start Up MITBBS Mathematics MITBBS Tennis Reading Joke MITBBS CS

**LINKSYS**  
A Division of Cisco Systems, Inc.

Firmware Version: v4.30.12

**Wireless-G Broadband Router** WRT54GL

**Wireless**

Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Wireless Settings Wireless Security Wireless MAC Filter Advanced Wireless Settings


**Wireless Network**

Wireless Network Mode: Mixed

Wireless Network Name (SSID): LionsDen

Wireless Channel: 6 - 2.437GHZ

Wireless SSID Broadcast: ☒ Enable ☐ Disable

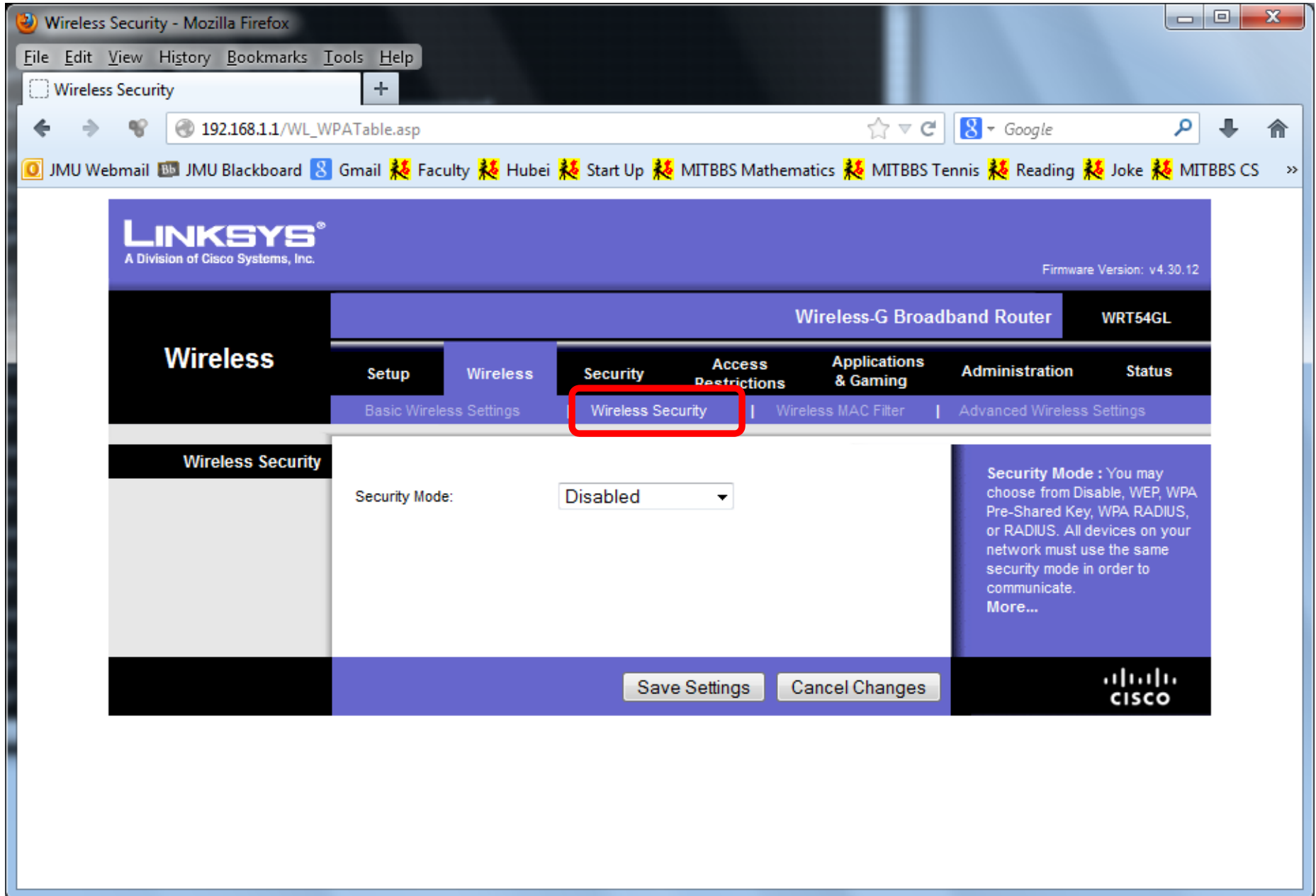


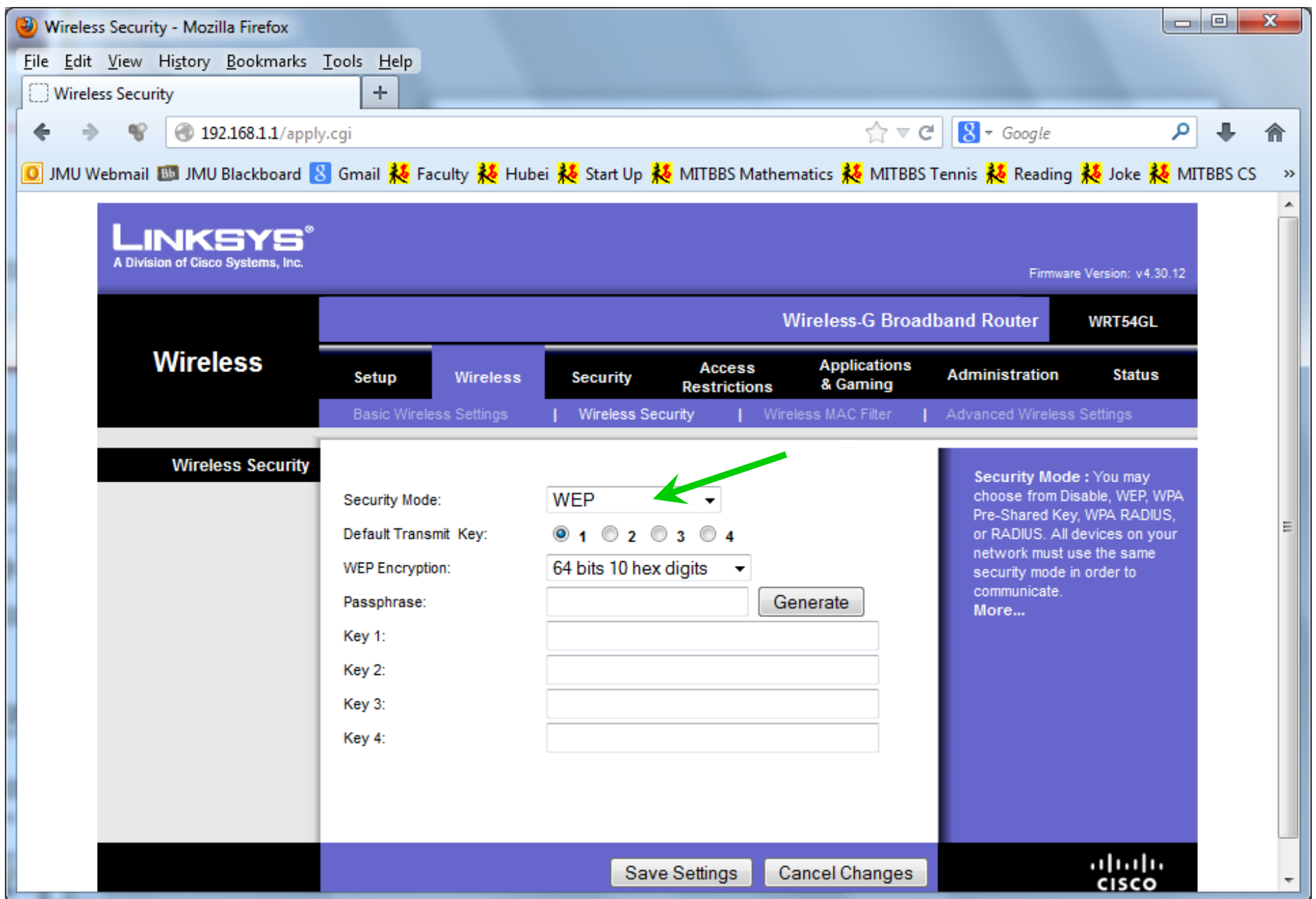
Status: SES Inactive

Reset Security

Wireless Network Mode : If you wish to exclude Wireless-G clients, choose B-Only Mode. If you would like to disable wireless access, choose Disable. More...

Save Settings Cancel Changes







Wireless Security - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Wireless Security

192.168.1.1/apply.cgi

JMU Webmail JMU Blackboard Gmail Faculty Hubei Start Up MITBBS Mathematics MITBBS Tennis Reading Joke MITBBS CS

**LINKSYS**  
A Division of Cisco Systems, Inc.

Firmware Version: v4.30.12

**Wireless-G Broadband Router WRT54GL**

**Wireless**

Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

**Wireless Security**

Security Mode: WEP

Default Transmit Key: 1 2 3 4

WEP Encryption: 64 bits 10 hex digits

Passphrase: 183412jhasfklqui Generate

Key 1: 92D3B168BB

Key 2: 0D29CE68AE

Key 3: 8C0BB7ED8A

Key 4: 285E391F3B

Security Mode : You may choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate. More...

**Your WEP key**

Save Settings Cancel Changes

CISCO

## ② WEP Configuration on Laptop

- Configure your laptop to connect to LionsDen
- With WEP key 92D3B168BB 

# WEP was Broken

## 2001

Borisov, Goldberg, Wagner [BGW01] discovered some practical flaws;  
Arbaugh, Shanker, Wan [ASW01] also observed some flaws  
Fluhrer, Mantin and Shamir [FMS01] found **fundamental** flaws  
Stubblefield, Ioannidis and Rubin implemented the FMS01 attack  
Rager released WEPCrack on August 12  
Airsnot was released

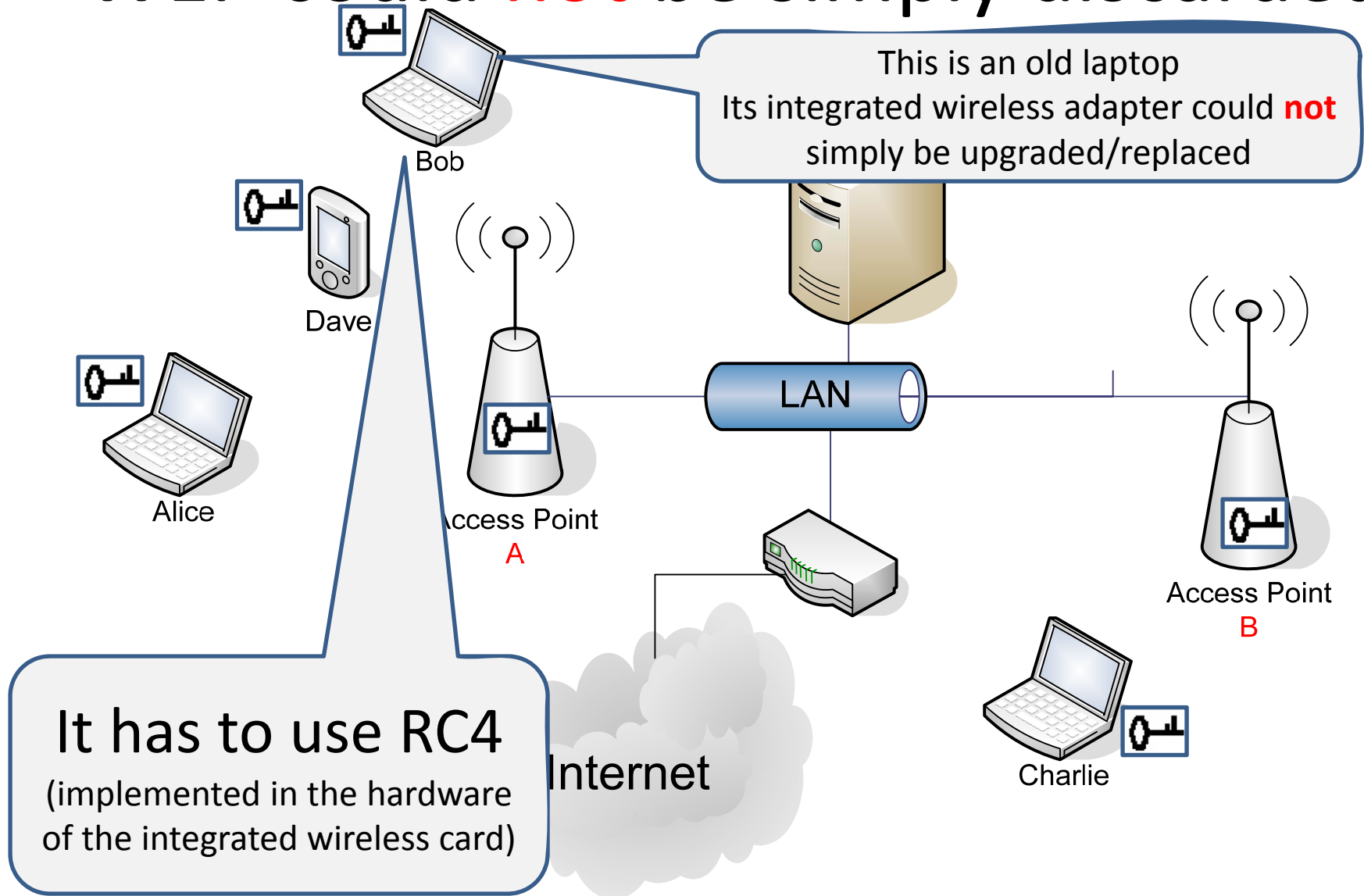
## Timeline



**1999:** ISO standard 802.11b

**1997:** IEEE 802.11 was developed; WEP

# WEP could **not** be simply discarded



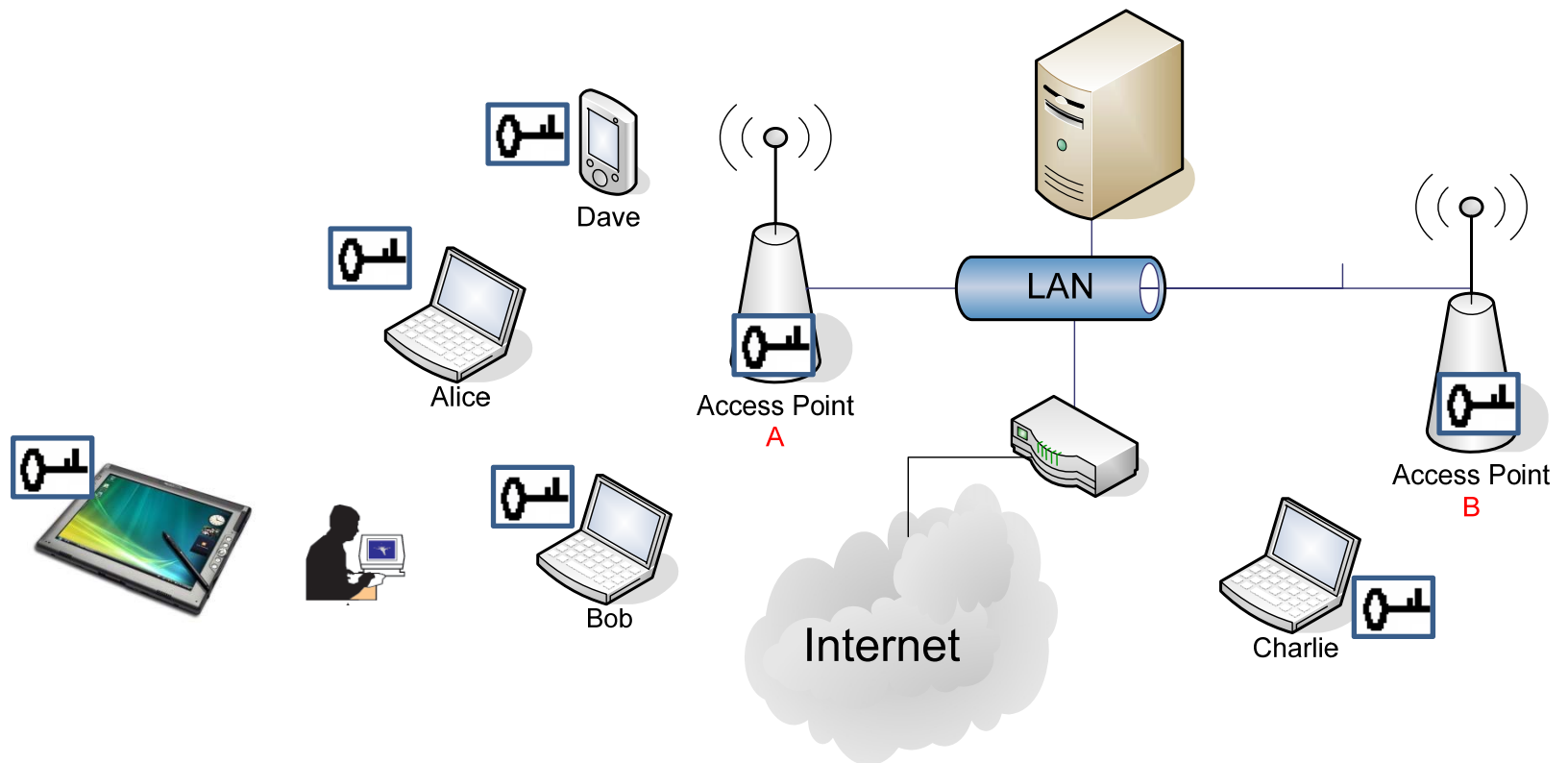
# Short-term Fix: WPA

- Wifi-Protected Access (WPA)
  - Goal: **fix** WEP
  - Use the same encryption algorithm – RC4
- How?
  - Modify the way that packet encryption keys are generated



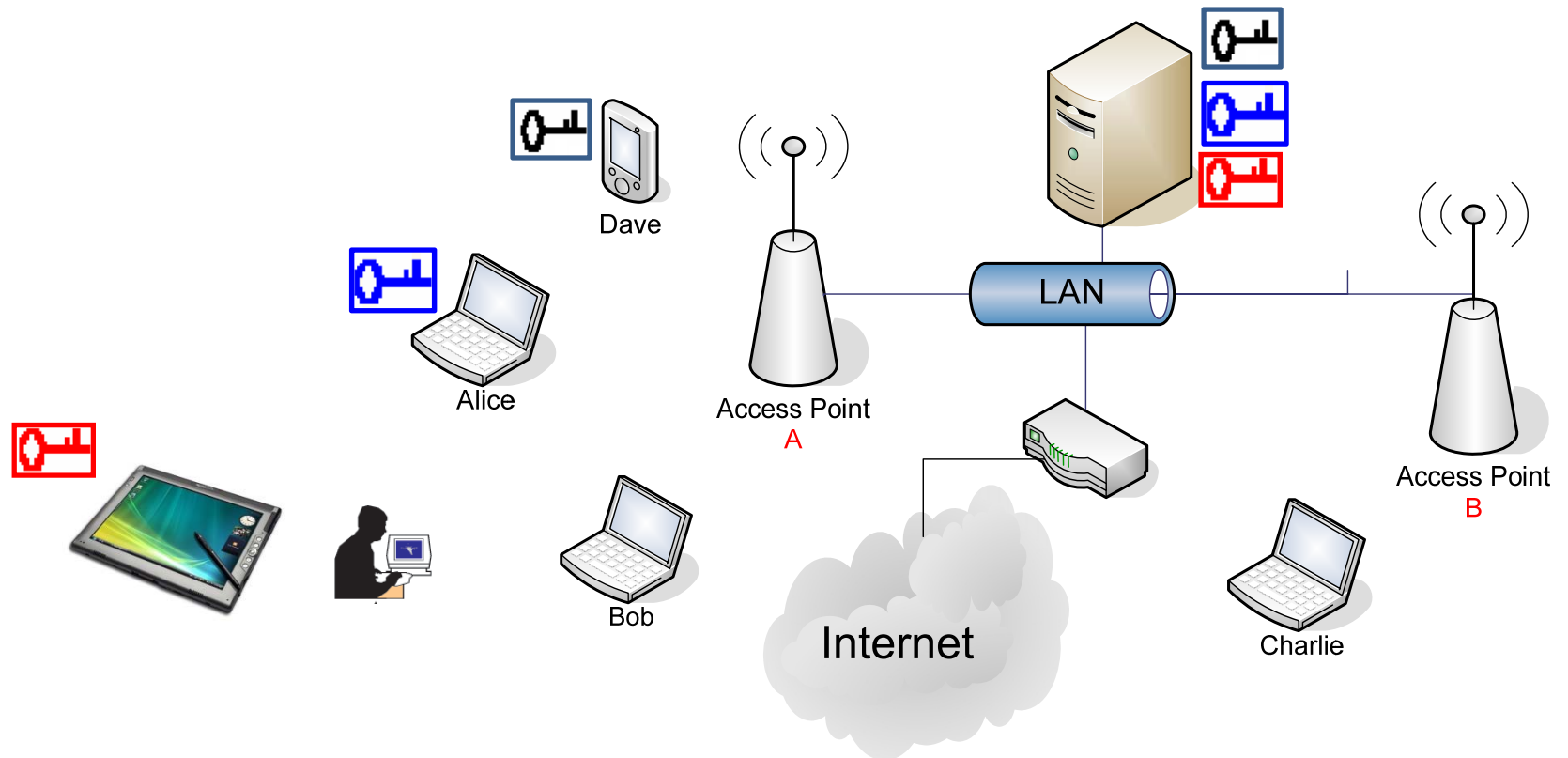
# WPA Mode 1: WPA-PSK

- Pre-shared key (PSK)
- All users share the same passphrase



# WPA Mode 2: WPA-Enterprise

- WPA-enterprise
- Each user has her/his own passphrase



# ① WPA-PSK Configuration on AP

① Wire your PC to your AP

– Your PC uses DHCP

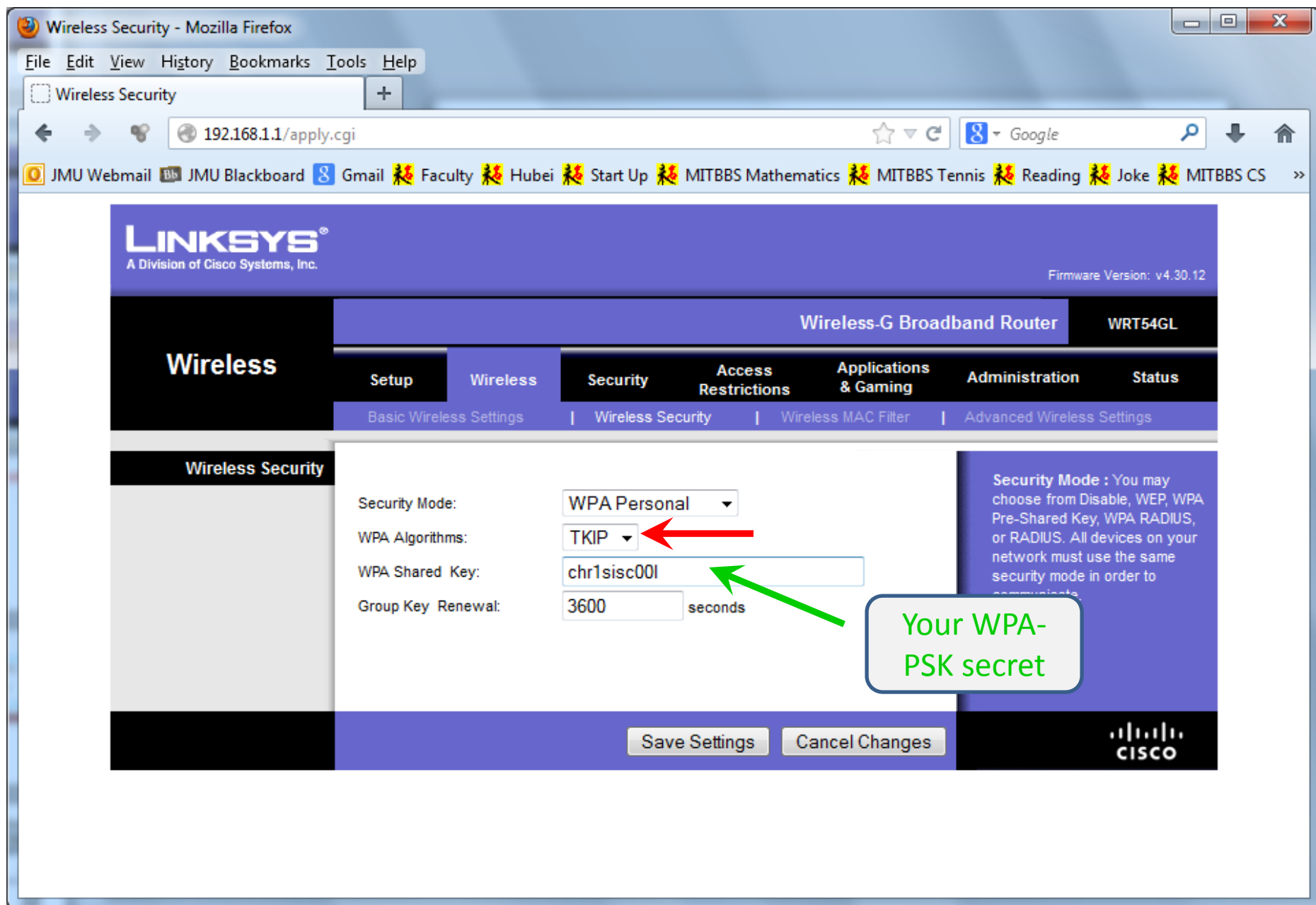
② Check the IP address of your PC – **ipconfig**

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::2cf8:20f7:b1b8:5e88%10  
IPv4 Address. . . . . : 192.168.1.100  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.1.1
```

③ Open web browser, type in 192.168.1.1





## ② WPA-PSK Configuration on Laptop

- Configure your laptop to connect to LionsDen
- With WPA-PSK secret chr1sisc00l

# WPA-PSK is Weak Too!

- WPA's data integrity mechanism, Temporal Key Integrity Protocol (TKIP), is a temporary fix
  - It is vulnerable to more complex attacks
- WPA-PSK is based on shared secret
  - It may be susceptible to dictionary attacks and brute-force attacks

# WPA2

- It uses a different encryption algorithm:  
Advanced Encryption Standard (AES)
  - More secure, standard
- It uses a more secure data integrity algorithm
  - CBC-MAC
- ⇒ Counter Cipher Mode with Block Chaining  
Message Authentication Code Protocol (CCMP)
- Like WPA, WPA2 supports two modes
  - WPA2-PSK
  - WPA2-Enterprise

# ① WPA2-PSK Configuration on AP

① Wire your PC to your AP

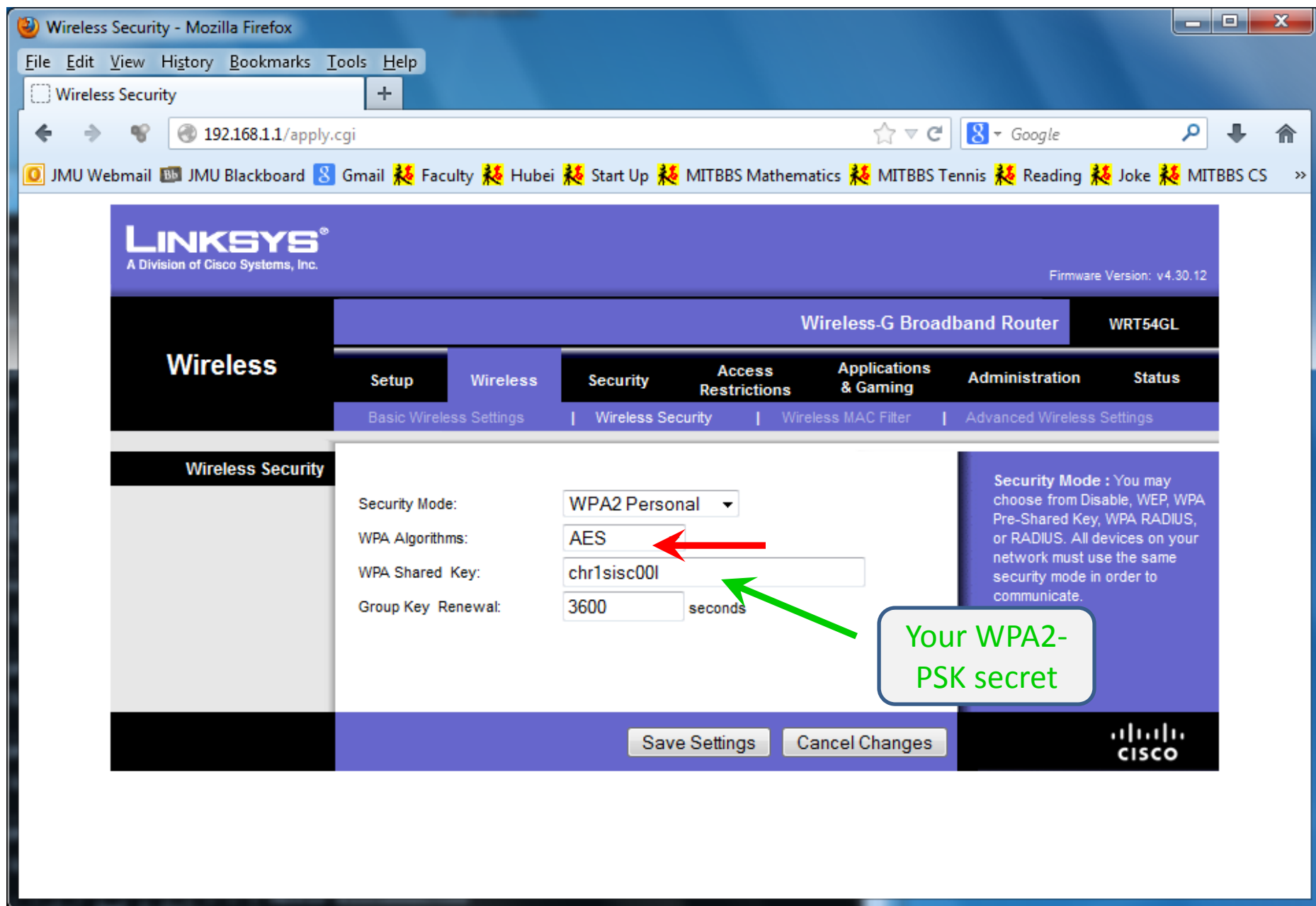
– Your PC uses DHCP

② Check the IP address of your PC – **ipconfig**

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::2cf8:20f7:b1b8:5e88%10  
IPv4 Address. . . . . : 192.168.1.100  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.1.1
```

③ Open web browser, type in 192.168.1.1



## ② WPA2-PSK Configuration on Laptop

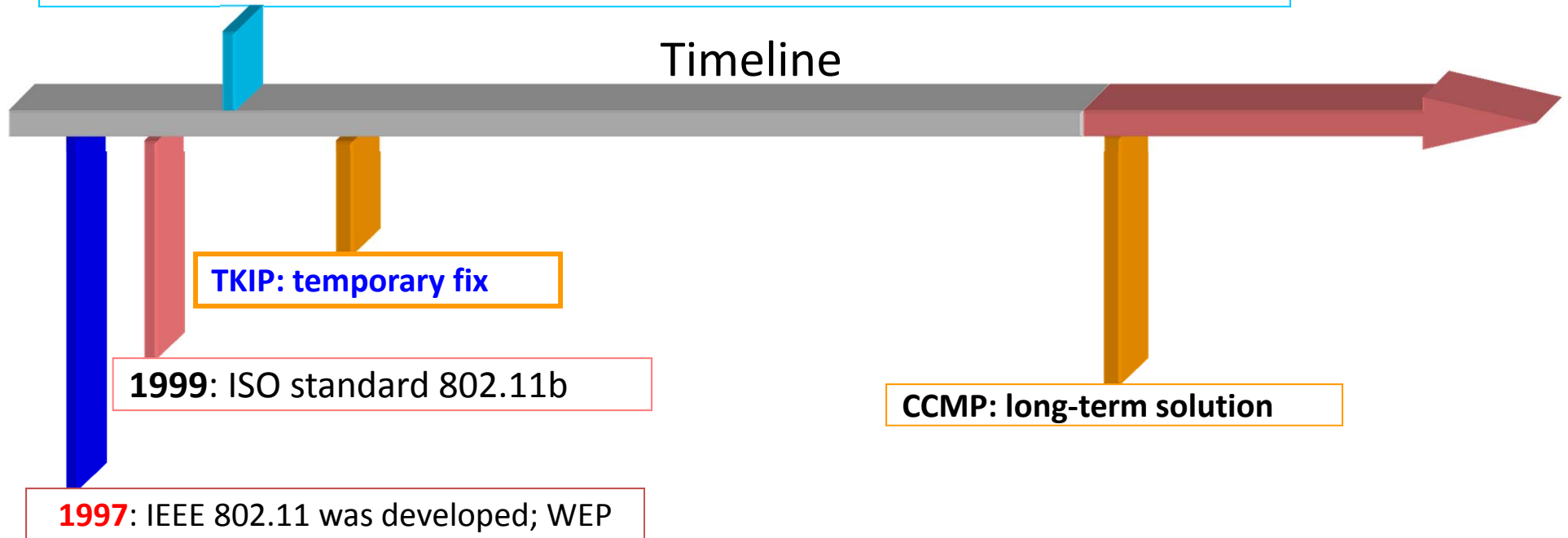
- Configure your laptop to connect to LionsDen
- With WPA2-PSK secret chr1sisc00l

# Wireless LAN Security: Summary

## 2001

Borisov, Goldberg, Wagner [BGW01] discovered some practical flaws;  
Arbaugh, Shanker, Wan [ASW01] also observed some flaws  
Fluhrer, Mantin and Shamir [FMS01] found **fundamental** flaws  
Stubblefield, Ioannidis and Rubin implemented the FMS01 attack  
Rager released WEPCrack on August 12  
Airsnot was released

## Timeline







# Buzzwords: Business vs. Technical

- WIFI
- Channel
- Wireless access point, wireless station (wireless cards)
- SSID
- ESSID
- WEP
- WPA
- WPA2
- Association/reassociate/disassociate
- RC4, TKIP, CCMP
  - AES, CTR, CBC-MAC
- 802.11
- 802.11i
- 802.11x
- MAC spoofing, MAC filtering
- Chipsets
- Managed mode
- Monitor mode

# Summary

[illegible]

# Summary

BUSINESS PEOPLE	ENCRYPTION	INTEGRITY	USER AUTHENTICATION	
WEP	RC4	Encrypted CRC	All users share the same key	
WPA-PSK	RC4	MIC	All users share the same key	
WPA-Enterprise	RC4	MIC	Each user is separately authenticated	
WPA2-PSK	AES-CTR	(CBC-MAC)	All users share the same key	 home
WPA2-Enterprise	AES-CTR	(CBC-MAC)	Each user is separately authenticated	

# How to Find Target AP's MAC

- Need a computer with wireless support
- On Windows
  - Netstumbler: freeware;  
<http://www.netstumbler.com/downloads/>
- On Linux
  - `ifconfig wlan0 down`
  - `iwconfig wlan0 mode managed`
  - `sudo iwlist wlan0 scan`

# Road Map

- Introduction to wireless LAN
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2
- **Exercises**
  - Cracking captured WEP traffic 1
  - Crack captured WPA-PSK traffic 2
  - Cracking captured WEP traffic 3
  - Crack captured WPA-PSK traffic 4

# Step 0

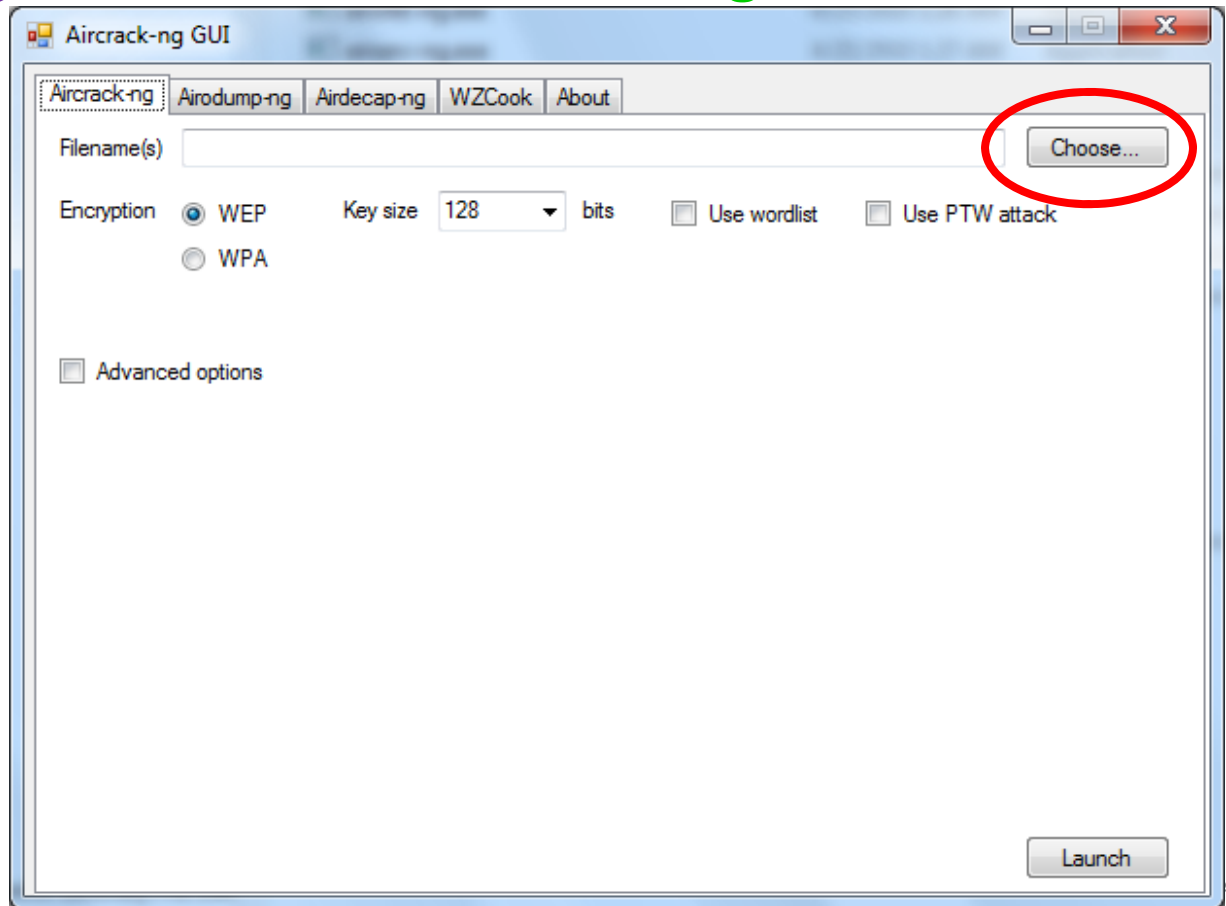
- Run Firefox to log into your vCenter server and find your Windows 2003 VM
- Use the “**WLAN and Crypto Security**” VM snapshot

# Aircrack-ng for Windows (1/2)

- Download aircrack-ng for Windows
  - <http://www.aircrack-ng.org/doku.php?id=main>
- Install it
- **NOTE:** This software has already been installed on your Windows 2003 VM under the “**WLAN and Crypto Security**” VM snapshot

# Aircrack-ng for Windows (2/2)

- Run `c:\wireless\wireless\aircrack-ng-1.1-win\aircrack-ng-1.1-win\bin\Aircrack-ng GUI.exe`
- (You can also run it directly from a shortcut on your Desktop)





# Exercises

- In this unit, we will crack some real-world wireless local area networks with traffic **captured** in files
  - **Not** live traffic
- These traffic packets were captured with **Wireshark**

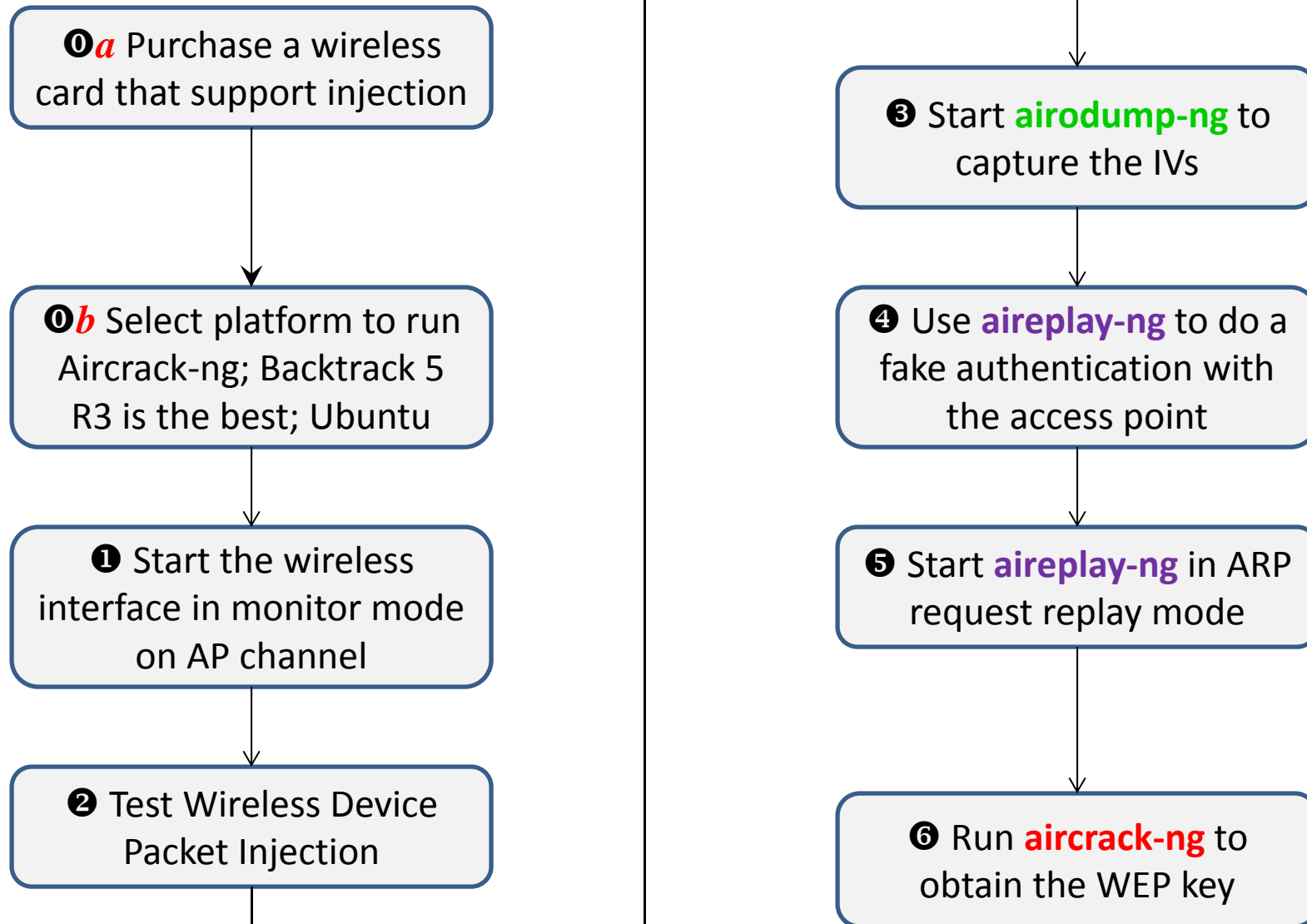
# Road Map

- Introduction to wireless LAN
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2
- Exercises
  - ① Cracking captured WEP traffic 1
  - Crack captured WPA-PSK traffic 2
  - Cracking captured WEP traffic 3
  - Crack captured WPA-PSK traffic 4

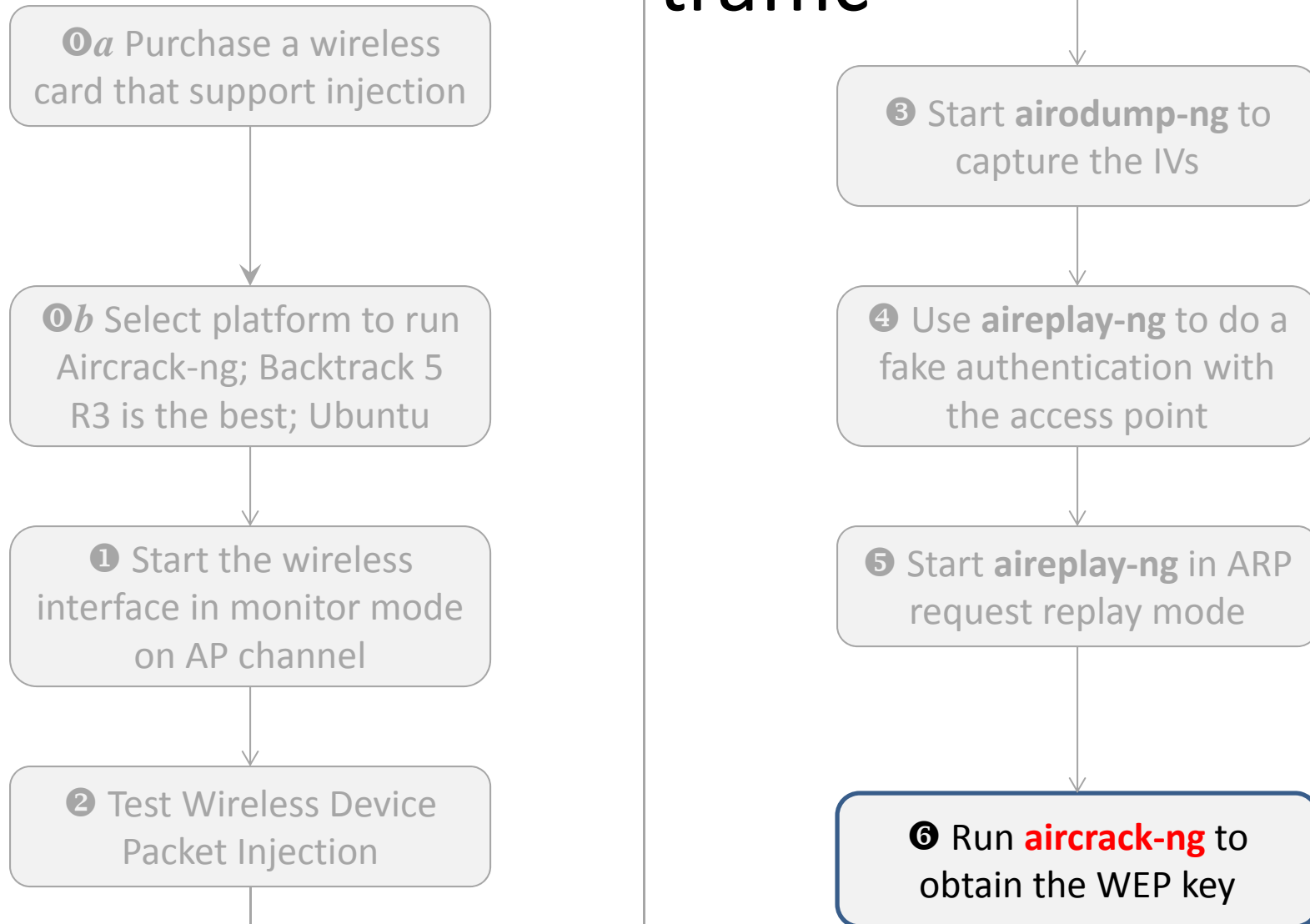
# Task ❶: WEP Cracking

- The target wireless network is using WEP

# WEP Cracking Steps

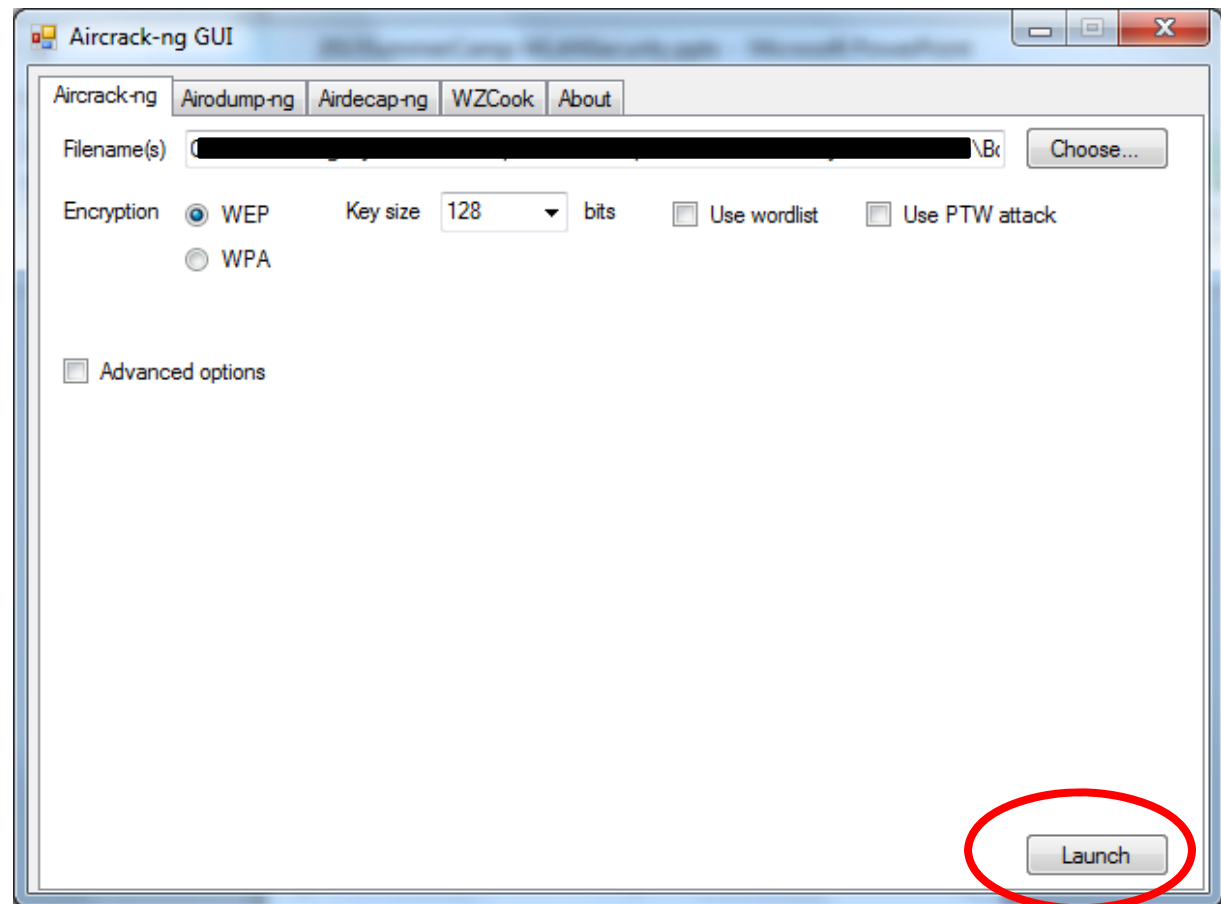


# WEP Cracking Steps with captured traffic



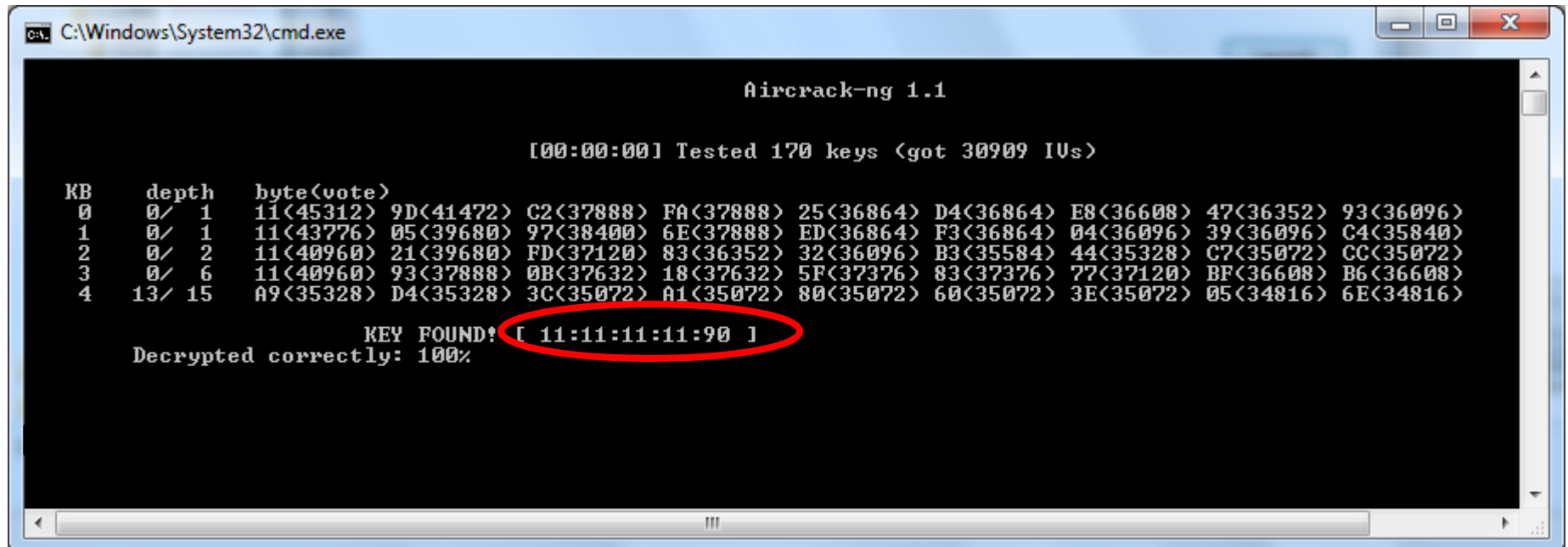
# Task ①: WEP Cracking

- Filename(s) `c:\wireless\wireless\WEPFile01\wep3-01.cap`



# What did you get?

- Mine



```
C:\Windows\System32\cmd.exe

Aircrack-ng 1.1

[00:00:00] Tested 170 keys (got 30909 IVs)

KB    depth  byte(vote)
0      0/ 1    11<45312> 9D<41472> C2<37888> FA<37888> 25<36864> D4<36864> E8<36608> 47<36352> 93<36096>
1      0/ 1    11<43776> 05<39680> 97<38400> 6E<37888> ED<36864> F3<36864> 04<36096> 39<36096> C4<35840>
2      0/ 2    11<40960> 21<39680> FD<37120> 83<36352> 32<36096> B3<35584> 44<35328> C7<35072> CC<35072>
3      0/ 6    11<40960> 93<37888> 0B<37632> 18<37632> 5F<37376> 83<37376> 77<37120> BF<36608> B6<36608>
4     13/ 15  A9<35328> D4<35328> 3C<35072> A1<35072> 80<35072> 60<35072> 3E<35072> 05<34816> 6E<34816>

KEY FOUND! [ 11:11:11:11:90 ]
Decrypted correctly: 100%
```

Now, close Aircrack-ng GUI.exe

# Now What?

- You can use the cracked WEP key
  - To connect to the target AP
  - To find other vulnerable computers on the network
  - To steal data from the target network



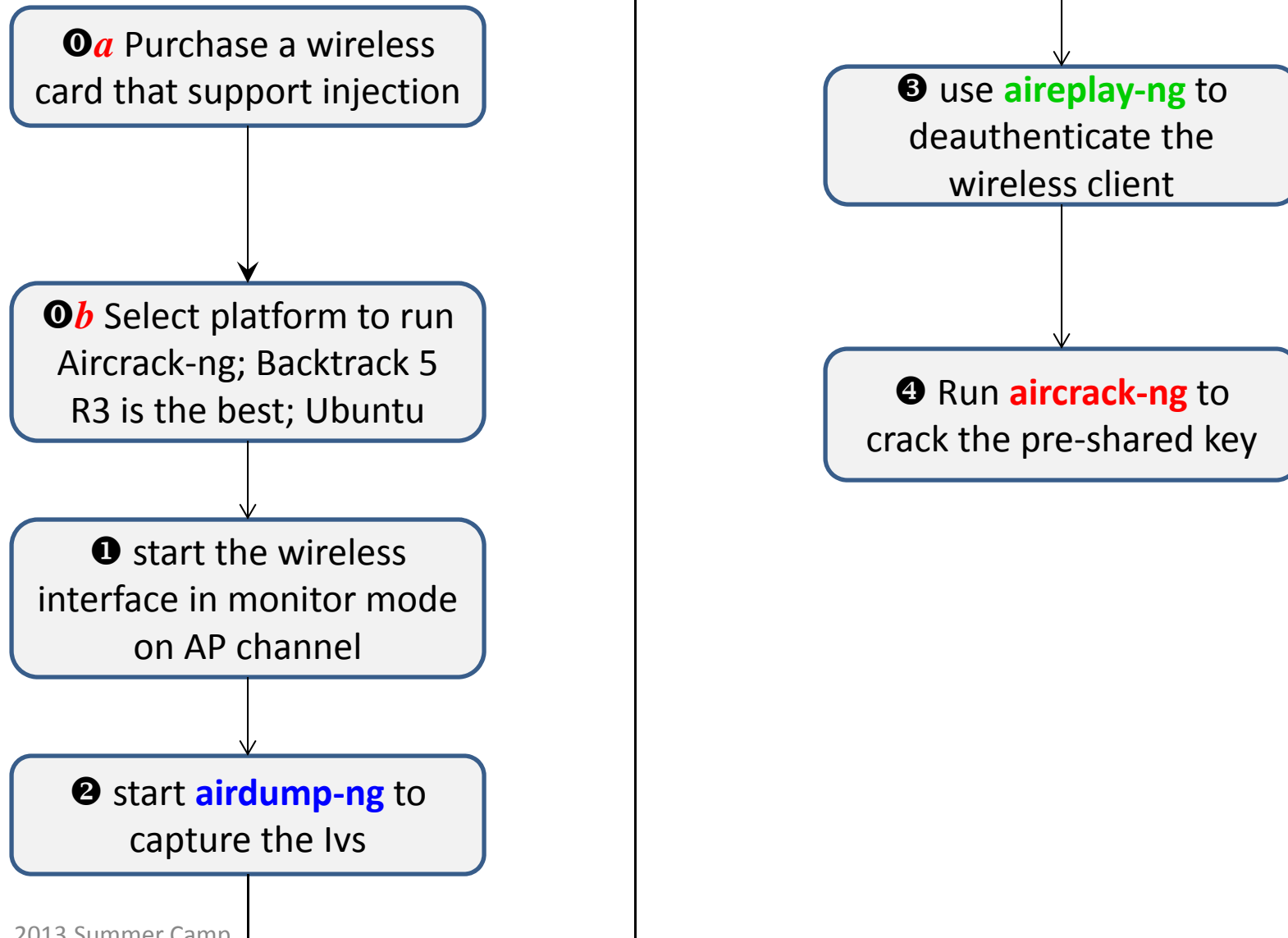
# Road Map

- Introduction to wireless LAN
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2
- Exercises
  - ① Cracking captured WEP traffic 1
  - ② Crack captured WPA-PSK traffic 2
  - Cracking captured WEP traffic 3
  - Crack captured WPA-PSK traffic 4

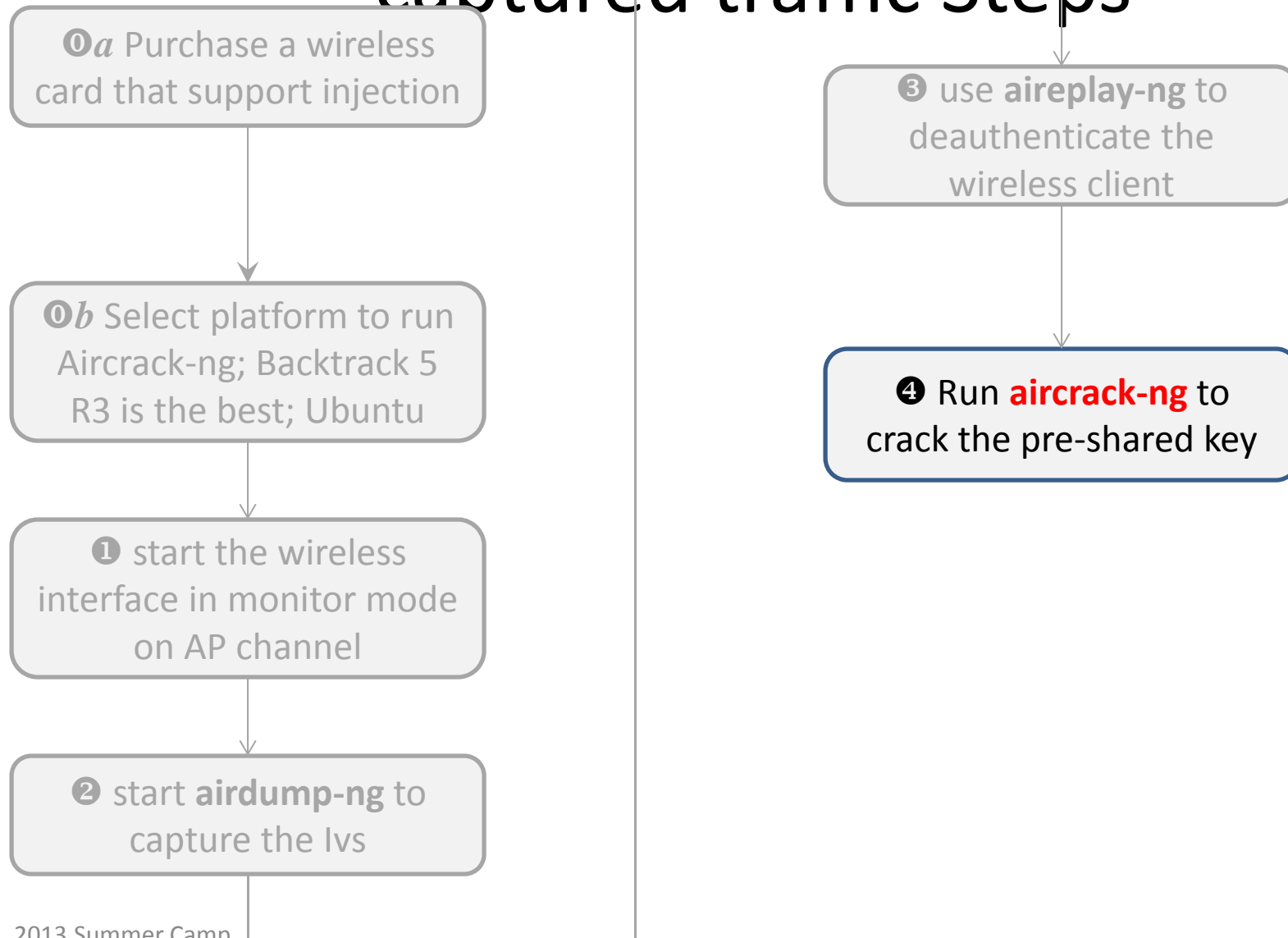
## Task ②: WPA-PSK Cracking

- The target wireless network is using WPA-PSK

# WPA-PSK Cracking Steps

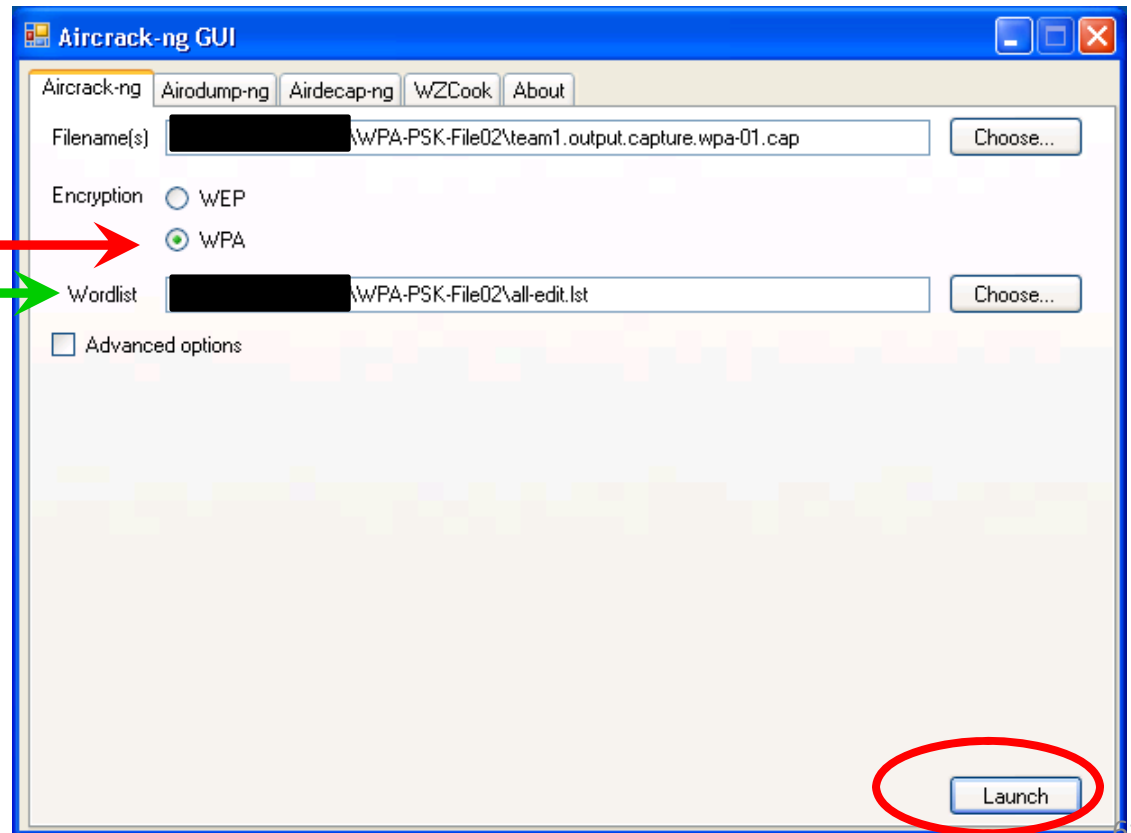


# Task ②: WPA-PSK Cracking with captured traffic Steps



# Task ②: WPA-PSK Cracking

- Filename(s): c:\wireless\wireless\WPA-PSK-File02\team1.output.capture.wpa-01.cap
- Wordlist:  
c:\wireless\  
wireless\  
WPA-PSK-File02  
\all-edit.lst
  - Do not use all.lst



# Task 2: WPA-PSK Cracking

- Choose index 2 if you get prompted

## Task ②: What did you get?

This is almost 10 minutes

- Mine

```
C:\WINDOWS\System32\cmd.exe
Aircrack-ng 1.1
[00:09:28] 198768 keys tested (362.13 k/s)

KEY FOUND! [ abcdefghijklmnop ]

Master Key      : BA 06 B8 CB F6 ED 05 78 C2 88 CC AB 3F 1A B0 0C
                  BE C5 A5 63 3A 10 F5 42 64 F1 2E 95 FF B1 69 89

Transient Key   : 5D 92 59 36 2F B6 F5 A8 E5 48 16 55 64 0B 98 28
                  C7 89 5C 13 2C CC 23 DE CC 23 DA 6C B9 49 DD 3A
                  7F 69 D2 94 F4 1A 91 57 1B 35 A0 52 48 F6 2F D9
                  7A 29 EB 59 AD 92 D4 11 6A 14 DE CF 18 D9 9D 3A

EAPOL HMAC      : 1C 98 79 4F DD 7D 3E AD F7 F5 42 4B 72 68 35 CB
```

Now, close Aircrack-ng GUI.exe

# Now What?

- You can use the cracked WPA-PSK key
  - To connect to the target AP
  - To find other vulnerable computers on the network
  - To steal data from the target network



# Road Map

- Introduction to wireless LAN
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2
- Exercises
  - ① Cracking captured WEP traffic 1
  - ② Crack captured WPA-PSK traffic 2
  - ③ Cracking captured WEP traffic 3
  - Crack captured WPA-PSK traffic 4

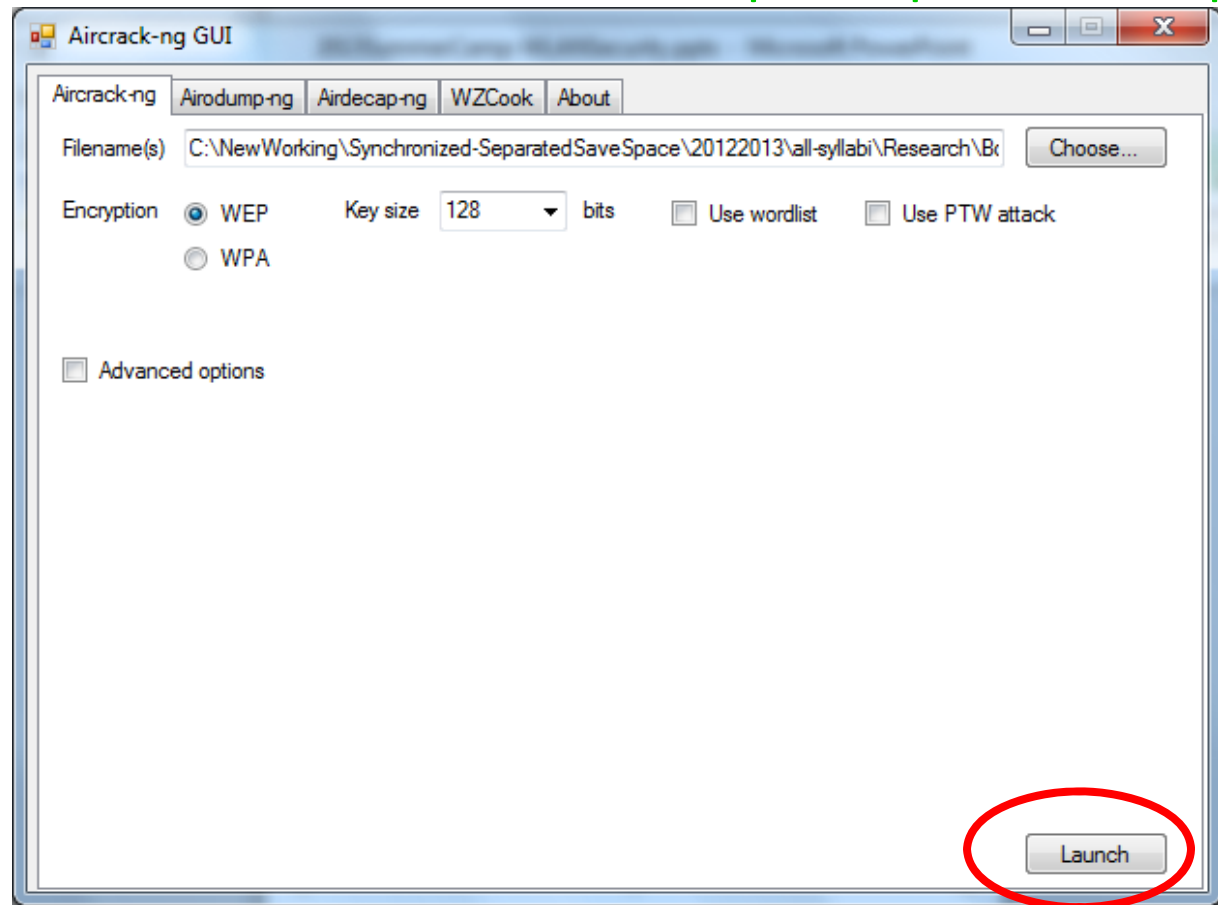
# Task ③: WEP Cracking

- The target wireless network is using WEP

# Task ③: WEP Cracking – File 3

- Filename(s)

c:\wireless\wireless\WEPFile03\team4.output.capture-03.cap

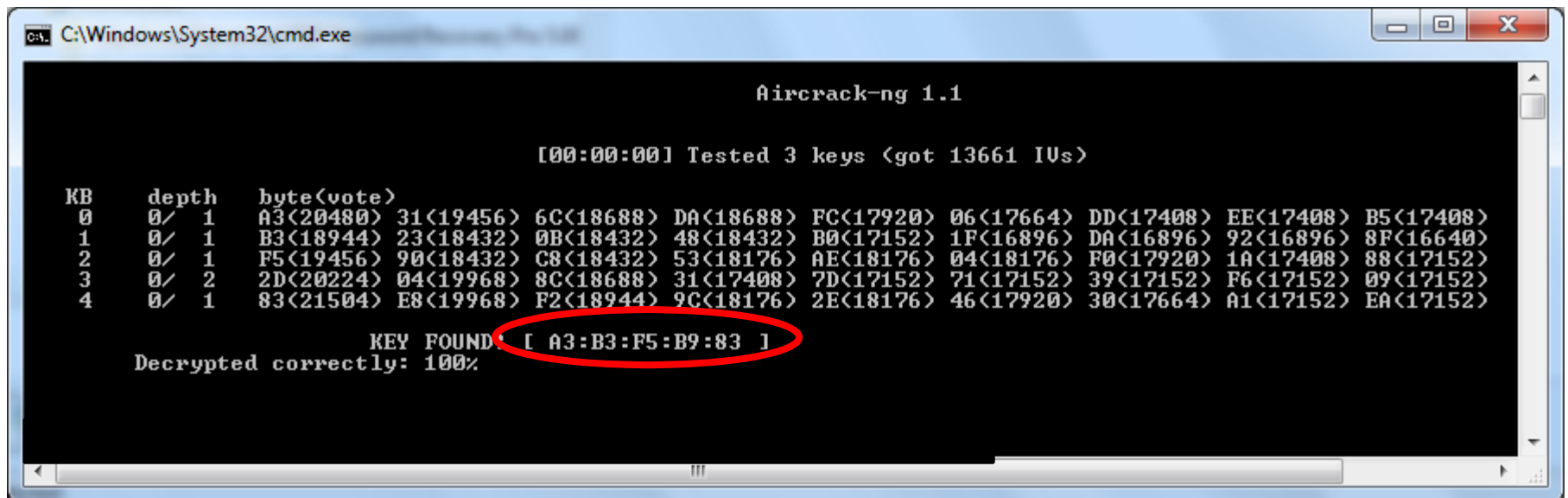


## Task ③: WEP Cracking – File 3

- Choose index 2 if you get prompted

# What did you get?

- Mine



```
C:\Windows\System32\cmd.exe

Aircrack-ng 1.1

[00:00:00] Tested 3 keys (got 13661 IVs)

KB    depth  byte(vote)
0     0/ 1    A3<20480> 31<19456> 6C<18688> DA<18688> FC<17920> 06<17664> DD<17408> EE<17408> B5<17408>
1     0/ 1    B3<18944> 23<18432> 0B<18432> 48<18432> B0<17152> 1F<16896> DA<16896> 92<16896> 8F<16640>
2     0/ 1    F5<19456> 90<18432> C8<18432> 53<18176> AE<18176> 04<18176> F0<17920> 1A<17408> 88<17152>
3     0/ 2    2D<20224> 04<19968> 8C<18688> 31<17408> 7D<17152> 71<17152> 39<17152> F6<17152> 09<17152>
4     0/ 1    83<21504> E8<19968> F2<18944> 9C<18176> 2E<18176> 46<17920> 30<17664> A1<17152> EA<17152>

KEY FOUND: [ A3:B3:F5:B9:83 ]
Decrypted correctly: 100%
```

Now, close Aircrack-ng GUI.exe

# Now What?

- You can use the cracked WEP key
  - To connect to the target AP
  - To find other vulnerable computers on the network
  - To steal data from the target network

# Road Map

- Introduction to wireless LAN
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2
- Exercises
  - Cracking captured WEP traffic 1
  - Crack captured WPA-PSK traffic 2
  - Cracking captured WEP traffic 3
  - Crack captured WPA-PSK traffic 4

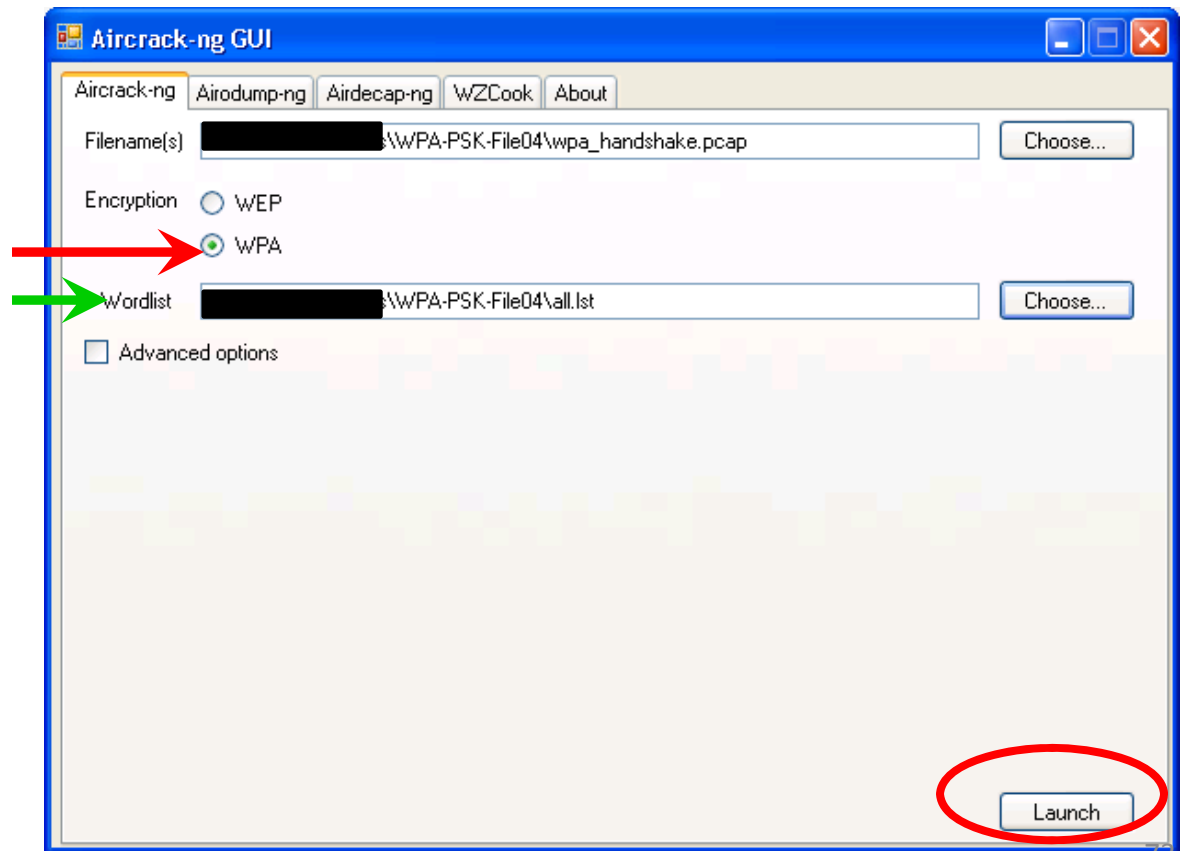
# Task 4: WPA-PSK Cracking

- The target wireless network is using WPA-PSK



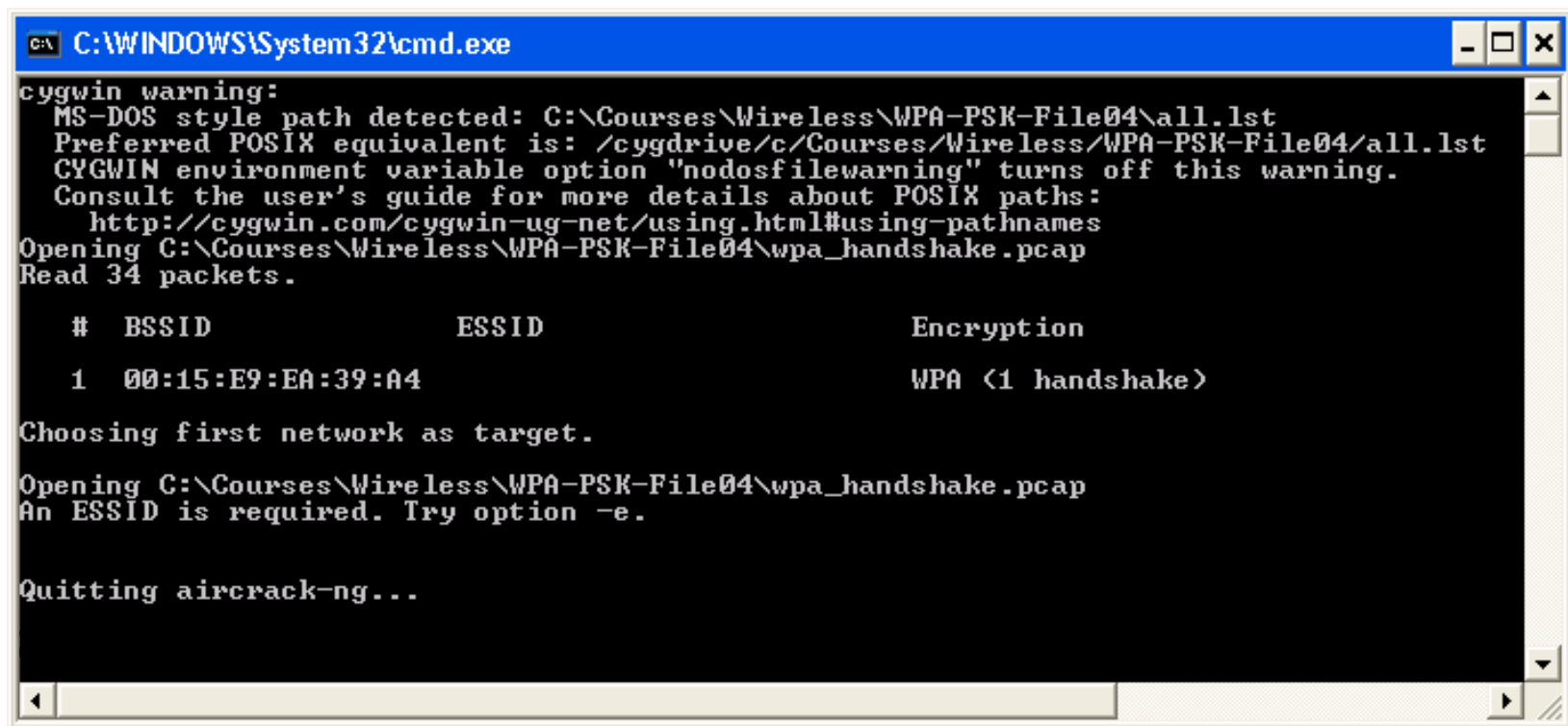
# Task ④: WPA-PSK Cracking

- Filename(s) `c:\wireless\wireless\WPA-PSK-File04\wpa_handshake.pcap`
- Wordlist:  
`c:\wireless\wireless\WPA-PSK-File04\all.lst`



# Task ④: What did you get?

- What?



```
C:\WINDOWS\System32\cmd.exe
cygwin warning:
MS-DOS style path detected: C:\Courses\Wireless\WPA-PSK-File04\all.lst
Preferred POSIX equivalent is: /cygdrive/c/Courses/Wireless/WPA-PSK-File04/all.lst
CYGWIN environment variable option "nodosfilewarning" turns off this warning.
Consult the user's guide for more details about POSIX paths:
  http://cygwin.com/cygwin-ug-net/using.html#using-pathnames
Opening C:\Courses\Wireless\WPA-PSK-File04\wpa_handshake.pcap
Read 34 packets.

#   BSSID           ESSID           Encryption
1   00:15:E9:EA:39:A4      WPA <1 handshake>

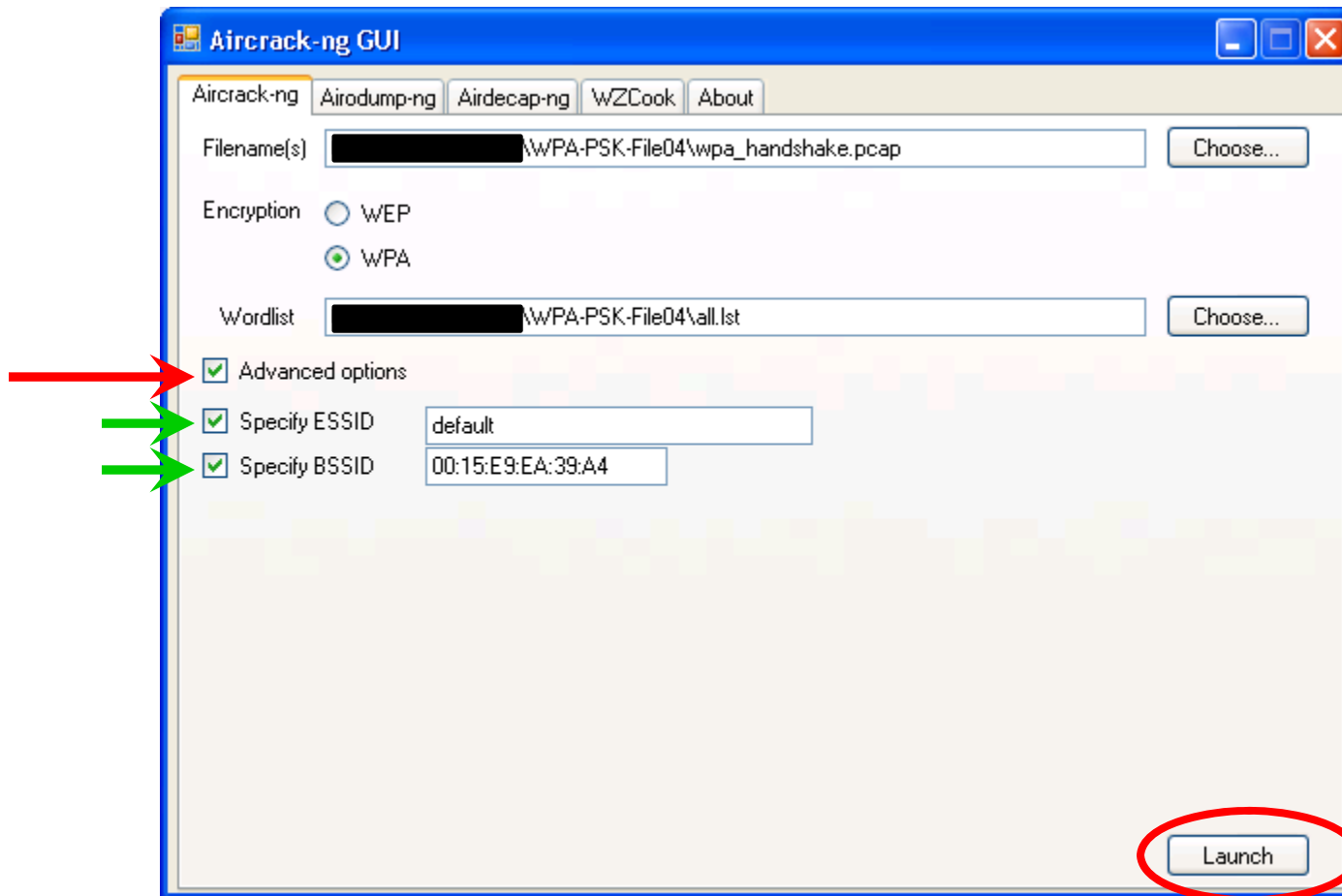
Choosing first network as target.

Opening C:\Courses\Wireless\WPA-PSK-File04\wpa_handshake.pcap
An ESSID is required. Try option -e.

Quitting aircrack-ng...
```

# Task 4: WPA-PSK Cracking

- Advanced



# Task ④: What did you get?

- Mine

This is almost 1.5 hours

```
C:\WINDOWS\System32\cmd.exe
Aircrack-ng 1.1
[01:28:56] 1868648 keys tested (356.76 k/s)
KEY FOUND! [ sc00byd00 ]

Master Key   : FA 38 AB 07 80 4B D8 BD AA 07 92 BE 82 3C 58 4F
               18 19 4C AA 9B 85 BD 12 93 E1 1A 42 09 0E 76 85

Transient Key : A6 B5 DF 63 9F 55 45 9F C1 66 7B D6 FF C5 CA A0
               D0 E9 6D 0A 09 B3 A9 D8 51 02 CE 43 F5 C1 0E F7
               56 2D 1B C8 24 C7 12 E9 5E 8F 12 40 65 2C 05 D1
               E7 65 0B FA 0A C2 07 0B 15 F8 24 1A 58 36 E3 CA

EAPOL HMAC   : 62 B1 F9 B6 74 05 AB 90 E3 34 60 27 02 B3 D5 6D
```

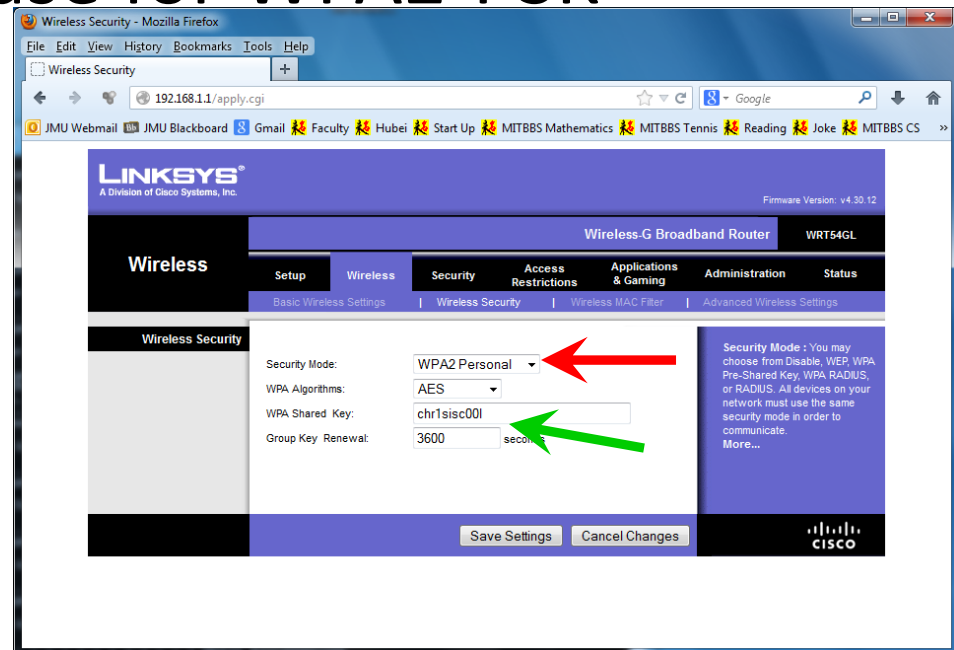
Now, close Aircrack-ng GUI.exe

# Now What?

- You can use the cracked WPA-PSK key
  - To connect to the target AP
  - To find other vulnerable computers on the network
  - To steal data from the target network

# Lesson to protect your wireless LAN?

- Use WPA2 if you can
  - Definitely **no** WEP
  - Avoid WPA-PSK if you can
- Use a long passphrase for WPA2-PSK
  - ❖ 8 ~ 63 characters



# Summary

- Introduction to wireless LAN
- Overview of wireless LAN security
  - WEP
  - WPA-PSK
  - WPA2
- Exercises
  - Cracking captured WEP traffic 1
  - Crack captured WPA-PSK traffic 2
  - Cracking captured WEP traffic 3
  - Crack captured WPA-PSK traffic 4