Lab sessions

Licences Professionnelles IRM et ISVD 2010

Course: Introduction to WiFi networks

Labs contents and schedule:

1. Introduction to lab sessions: instructions and objectives
2. Some tools :
    a. Wireshark
    b. Airodump
    c. NetStumbler
    d. Netperf and Iperf
3. Drivers and Utility installation – First configuration steps
4. Setting up a peer-to-peer ad hoc connection
5. Setting up an infrastructure network: access point basic configuration

1. Introduction to lab sessions: some instructions et objectives

Objectives of the lab sessions

The goal is first to get familiar with basic tools from a user point of view: installation of WiFi NIC driver and configuration of the utility, as well as to use specific tools to analyze more deeply the wireless network functioning.

Then, the settings of different network topologies together with access point configuration are investigated.

Consignes générales

Attention au matériel:

Un point d'accès démarré sans charge (son antenne) peut très mal vivre cette expérience. De plus, le comportement au boot des points d'accès Cisco a tendance à changer d'une version d'IOS à l'autre..., c'est pourquoi il faut toujours monter toutes les antennes avant de mettre sous tension.

Pour les séances de TP qui nous concernent, vous n'aurez pas à toucher aux AP dont qui sont déjà installés avec leurs antennes.

Attention à votre santé:

Rappelez-vous les risques sanitaires et pensez à ne pas rester trop proche des antennes et à rapidement diminuer la puissance d'émission de vos points d'accès et de vos postes clients... sinon, apportez de l'aspirine...

De manière générale, vous pouvez avoir de très bonnes performances avec un niveau de puissance de 5 à 10 mW en raison de la configuration spatiale de vos équipements, plutôt que les 100 mW maximum affectés par défaut.

Note:

Le TP est simple et assez court mais représente le minimum à assimiler. Vous pouvez consacrer le temps restant en TP à utiliser les outils vus dans la 1ère partie pour effectuer des mesures de performance et mette en évidence des phases particulières dans les échanges protocolaires.

2.a. Wireshark

What

Wireshark (http://www.wireshark.org/) is a free protocol analyser (sniffer) available on several OS platforms and producing pcap format dumps.

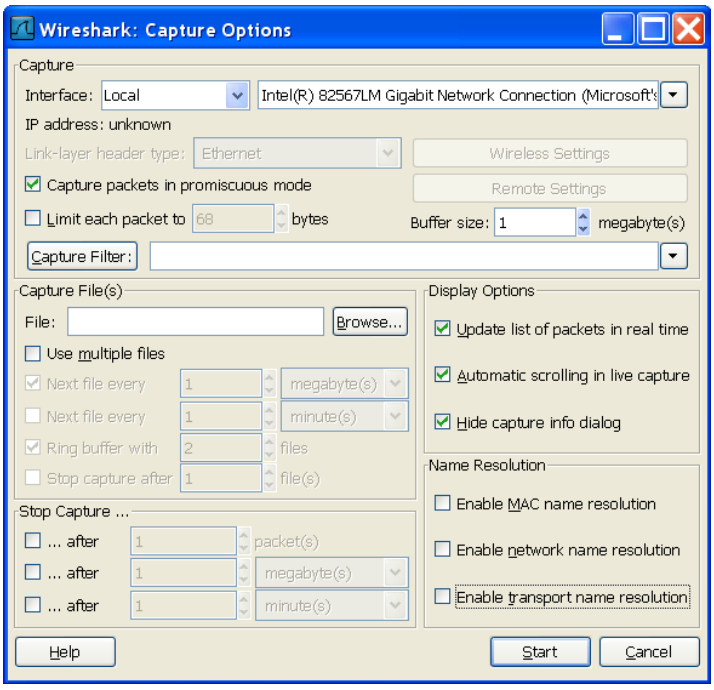
Why

Part of your job is to build and troubleshoot a network. This is a must-have and powerful tool.

How

Download it and the WinPcap if needed additionally.

Select Capture -> Options



Using « Options » button, browse the available options.

1. Try sniffing some traffic from your **ethernet adapter** in normal and promiscuous mode and explain the difference: look for definition of « promiscuous mode » and explain what kind of traffic you are able to capture without and with promiscuous mode.
2. Then connect to Unice-hotspot ESSID thanks to your **wireless NIC** managed through Windows (just associate).
   Test without and with promiscuous mode: what does not work?

In what follows, we are going to see that there are two possible reasons for the problem: one may be Wireshark, i.e., the specific software used for capture; the other may be the wifi card driver.

2.b. Airodump Aircrack

What

All vendors provide drivers that come along the piece of hardware. Cisco, like many others, uses an Atheros chipset in their wireless cards and provides their own driver/firmware for normal and usual use.

Full access to the Atheros chipset API is then hidden to the human being, thereby preventing from dumping wireless network traffic in « promiscuous mode ».

One can find from Atheros WildPacket a more complete driver which allows raw dump of layer 2 WiFi frames.

Moreover, another software than Wireshark will allow us to capture layer 2 frames. This software is Airodump-ng, and is part of the WinAirCrack package.

Why

Replacing the original Cisco with the WildPacket driver on one of the two PC allows you to get a cheap/free wifi protocol analyzer for educational purpose.

How

Provided you have a compatible wifi device.
On Windows:

- Replace default Cisco driver with the Atheros WildPacket driver.
- Download WinAirCrack , start Airodump-ng to get frame dumped into a pcap compatible format file.
- Open the resulting file with Wireshark and enjoy.

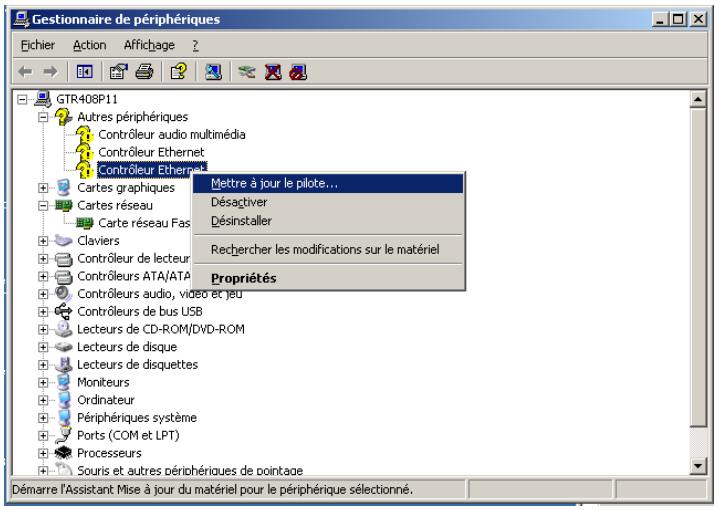
Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng.

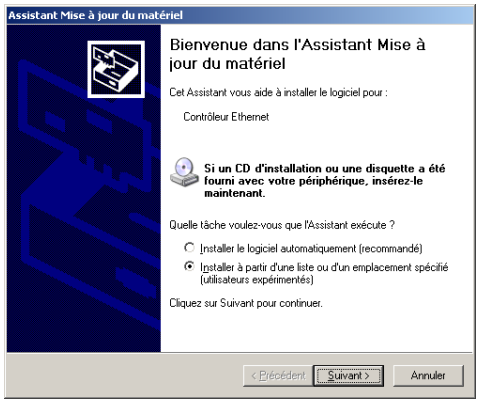
Current limitations: only 802.11g traffic can be dumped. Windows version cannot insert fake IV in WEP traffic to increase speed of WEP cracking.

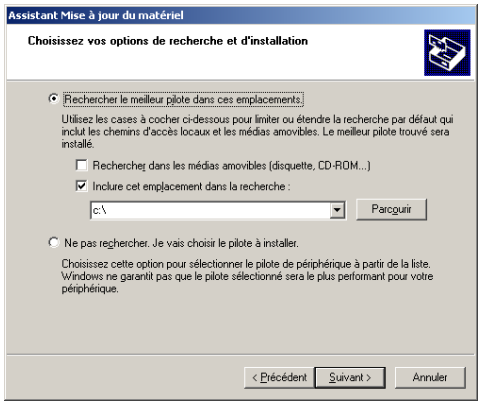
Download all necessary software:

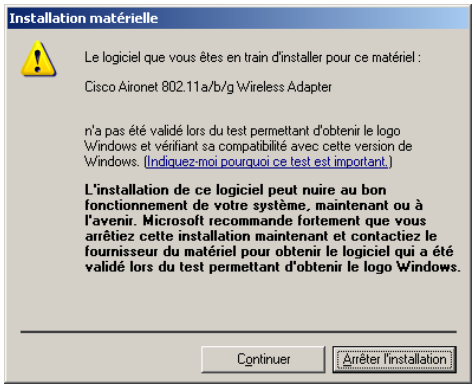
- WildPackets Atheros driver package : http://mkcomputers.nl/wildpackets/atheros4229.zip
  - Select your WiFi adapter (unknown or recognized as a Cisco wireless NIC) and update the driver with the one provided by WildPackets (see the following screenshots).

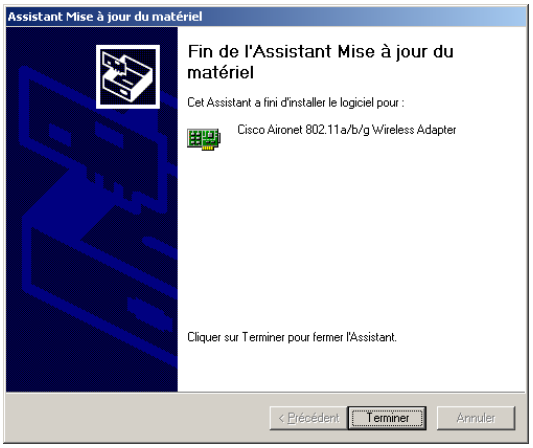
- WinAirCrack package : http://www.aircrack-ng.org/doku.php?id=downloads (version 0.9.3 for windows)
  - Once you unzipped the directory, go into the *bin* directory, and launch *airodump-ng.exe*. At the first run, you are asked for the peek files. Go back to the link below, download the *Peek.zip*, unzip it and copy-paste the files in the previous *bin* directory.
  - Launch again airdump-ng.exe, it should work.
  - For how to use it, see the following screenshots.



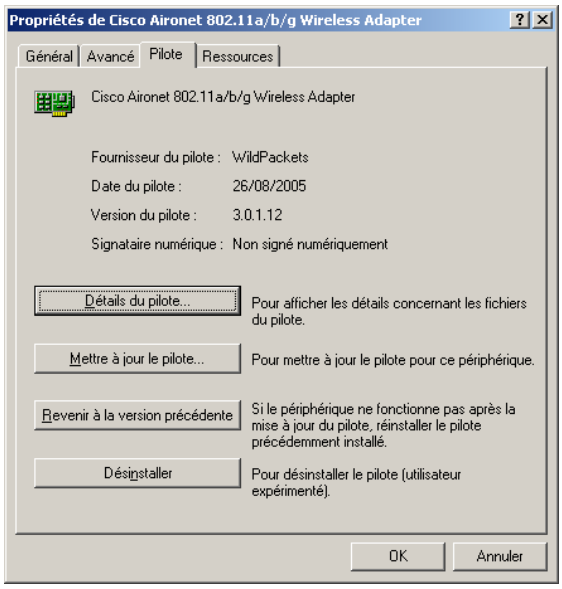






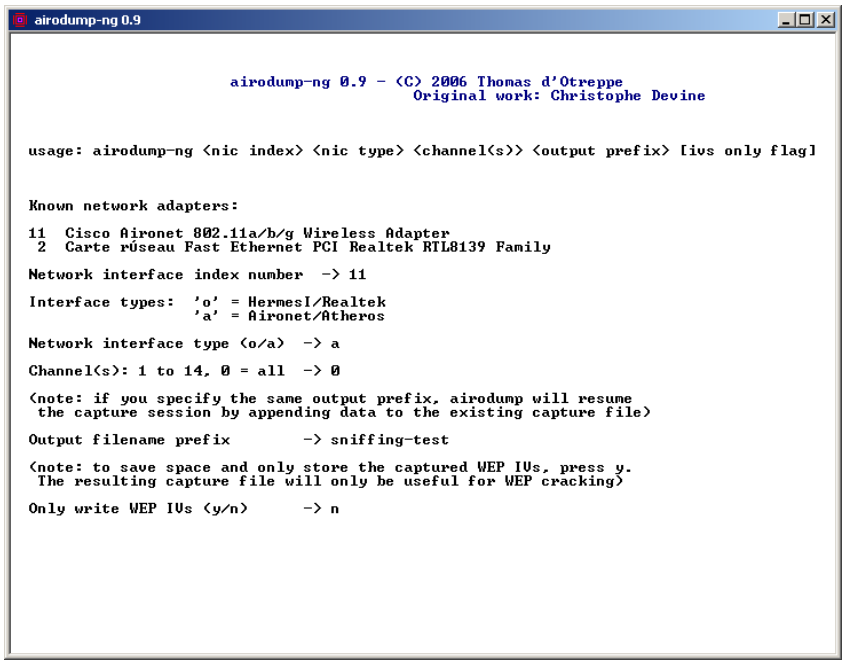


Check the name of the software vendor is now « WildPackets »



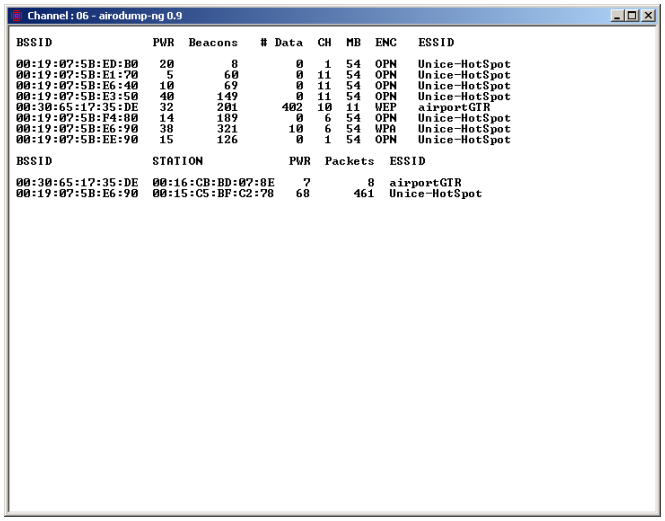
After installing WinAirCrack or aircrack-ng, launch airodump:

- select the appropriate wireless adapter
- select atheros driver
- select all channels
- give a file name
- answer « no » to only collect WEP Initialization Vectors



Check the file is growing live... and (E)SSID are discovered.

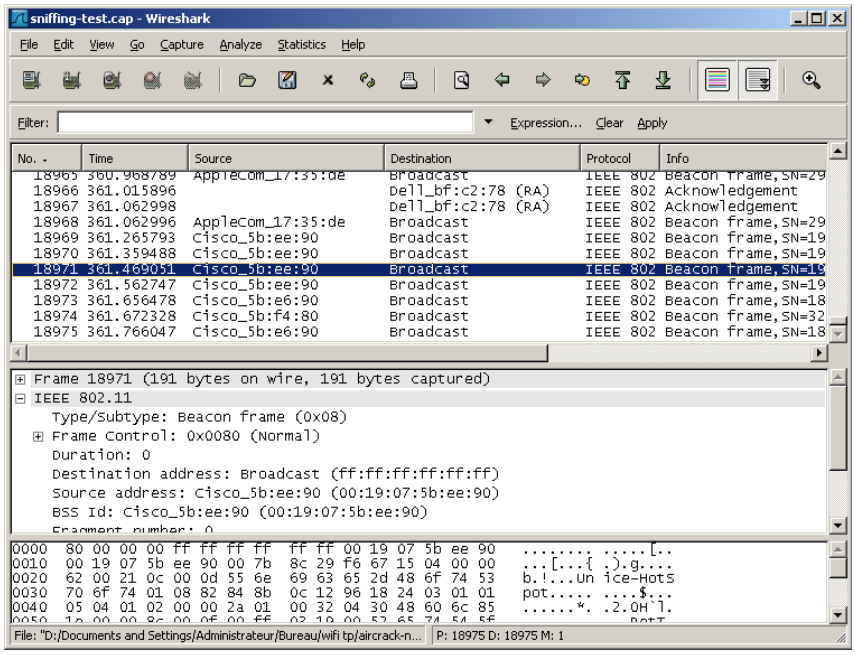
Get familiar with columns' names and meanings, get a clear understanding of what is representing a client, an AP.



When enough data is collected, stop airodump and look at the two resulting files:

- .cap file recognized by Wireshark (Windows association if Wireshark installed)
- .txt file containing capture informations

Open the .cap file with Wireshark and see what is displayed... much more than usually with a standard driver, isn't it?



2.c. NetStumbler

What

NetStumbler is a useful freeware when you want to know whether wireless networks are available in your geographic area. It uses active scanning (sends probes) and, if connected to a GPS, it's also a good wardriver utility.

Why

Never wonder what SSID are available at your place?

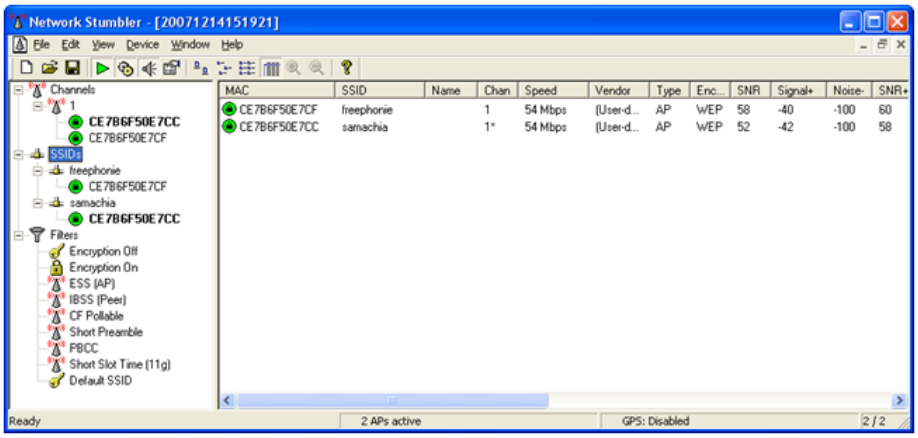
How

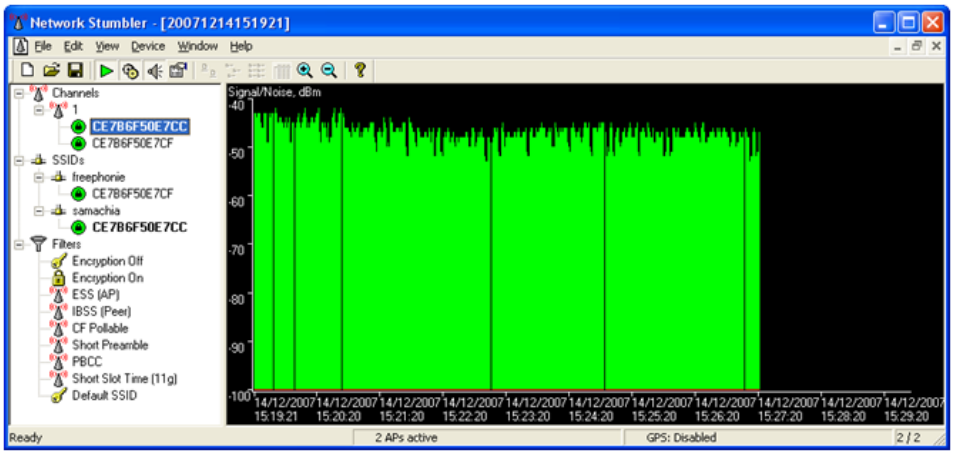
Download and install Netstumbler: http://www.netstumbler.com/downloads/

Select adapter (« Device » menu) and display result on screen or store it in a file.

Note: Coexistence with « Windows Zero Config » management of your wireless adapter may lead to tricky situations.

Note: Ctrl+B disables the scan





2.d. Netperf and iperf

What

Netperf and iperf are common client/server sets of tools which allow to make some performance measurements at the transport layer, on a network link between two end hosts (whatever the underlying physical connections at each hop: ethernet, wifi, CPL, aDSL…).

Why

Evaluate the throughput you get at the transport layer, apart from what sellers claim reachable at the physical layer (11 Mbps to 300-600 Mbps).

How

In what follows, "server" and "client" denote the lest-hand side and right-hand side PCs, respectively.

1-Download and install **Netperf** on server and client: http://iutsa.unice.fr/~frati/_TOOLS/stress/

- Connect the two PCs to their respective IUT plugs. The two PCs are then connected through the central switch of the class room.
- Run netserver.exe server on the left-hand side PC: find appropriate options to start as a server and look for appropriate default protocol and port used
- Run netperf.exe client on the right-hand side PC : find appropriate options to start as a client pointing to the appropriate server.

  ➔**Once found, write down the option for future and further use.**

What performance result do you get? Comment in terms of what was theoretically expected.

2- Download and install **iperf** on server and client: (same location for downloads)

- Run iperf.exe on the server : find appropriate options to start as a server and look for appropriate default protocol and port used (type « help » option to have all options described)
- Run iperf.exe on the client: find appropriate options to start as a client pointing to the appropriate server. Try various window sizes up to 65500.

  ➔**Once found, write down the option for future and further use.**

What performance result do you get? Comment in terms of what was theoretically expected.

Note: When there is a client/server pair supposed to work together, the server must be started and in listening mode before any client can connect to.

In the following lab sessions, you will use those measurement tools in various wireless configurations: you considered 2 wired hops in what you just did, you will then consider one direct wireless hop (in ad hoc mode), one wired hop and one wireless hop and two wireless hops (both through the AP).

3. Drivers and Utility installation – First configuration steps

Repérage des installations

Installation was already done by instructor to avoid cabling and screwdrivers injuries issues.
• « Vérification du matériel installé et repérage »
- cartes réseau (filaires, sans-fil)
- hub, switch, câbles
• « Architecture initiale de la salle 408 et des labs »,
-hardware locations
-OS

Resources

http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guide_book09186a0080184b6e.html for Official Cisco Web site
http://kheops.unice.fr/~frati/_TOOLS/ for networking and performance tools
http://kheops.unice.fr/~frati/_DRIVERS/ for Cisco, NetGear and 3Com softwares, drivers, docs, ...

Installing Aironet Client Utility (ACU) or the latest release renamed Aironet Desktop Utility (ADU)

Objective

The student will learn the procedures for installing the Aironet Client/Desktop Utility (ACU/ADU), the software that manages the Cisco Aironet wireless network card.
Also, the student will configure, select, and manage profiles.

Scenario

Install and configure the ACU/ADU and additional software options to allow a user to configure, manage, and monitor wireless connections.
Two client utilities are available for use with the client adapters: **Aironet Desktop Utility (ADU)** and **Aironet System Tray Utility (ASTU)**. These utilities are optional applications that interact with the client adapter's radio to adjust settings and display information.
ADU enables you to create configuration profiles for your client adapter and perform user-level diagnostics. Because ADU performs a variety of functions, it is documented by function throughout the manual.
ASTU, which is accessible from an icon in the Windows system tray, provides a small subset of the features available through ADU. Specifically, it enables you to view status information about your client adapter and perform basic tasks.
ADU is used in what follows.

Preparation

This lab will require the following materials:
• Desktop PC
• Cisco Aironet Client Adapter Network Interface Card on all machines

• Cisco Aironet Client/Desktop Utility installer (directory _DRIVERS or CD)

• Configured AP that the instructor had setup in order to simulate Home, Office and a public network like in an airport:
o « Office » network with SSID: **InTheOffice**
Note: Keep in mind that SSIDs are case sensitive.

1. Step 1 Configure XP to use the ADU

Note When reading ACU, keep in mind this also means **ADU: Aironet Desktop Utility** as ACU was the previous name of the utility

To configure the client adapter through ACU instead of through Windows XP, follow the steps below:
a. Double-click My Computer, Control Panel, and Network Connections. Click **Start>Control Panel** then double-click **Network Connections**.
For Windows XP, click **Start>My Computer>Control Panel>System**.

b. Right-click Wireless Network Connection and click Properties.
c. Select the Wireless Networks tab.
d. Deselect the **Use Windows to configure my wireless network settings** check box.
e. Follow the instructions in the "Installing ACU" section to install ACU.

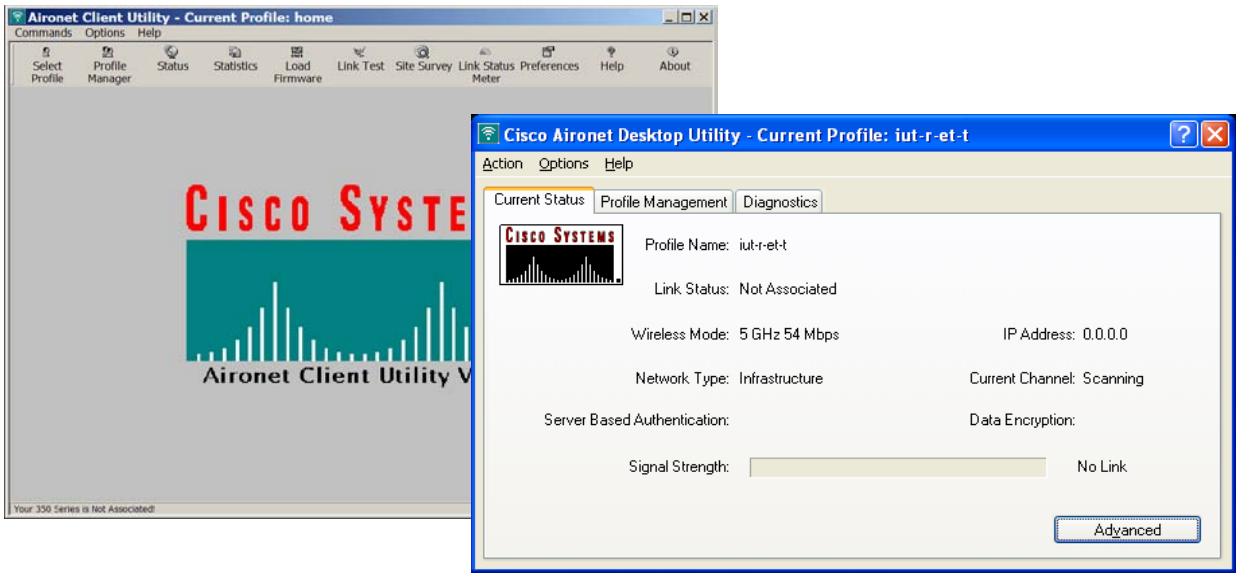
Note If you are planning to configure the client adapter through Windows XP but you want to use ACU's diagnostic tools, then install ACU but do not create any profiles and let it be managed bu the « Windows Zero Config » service.

Note Check in managed services what is the status of the « Windows Zero Config » service.

2. Step 2 Install the Aironet Client Utilities (ACU) or the latest Aironet Desktop Utilities (ADU)

The most recent version of the ACU can be obtained through the Software Center on the Cisco Connection Online (CCO). In this lab, you use the release `WinClient-802.11a-b-g-Ins-Wizard-v35.exe` located at:
http://iutsa.unice.fr/~frati/_DRIVERS/Cisco/Cisco%20Aironet%20CB21AG%20and%20PI21AG%29/

Note To install or use the client utilities on Windows NT or Windows 2000 systems, a user must log onto the system as a user with administrative privileges. The utilities do not install or operate correctly for users not logged in with administrative rights.

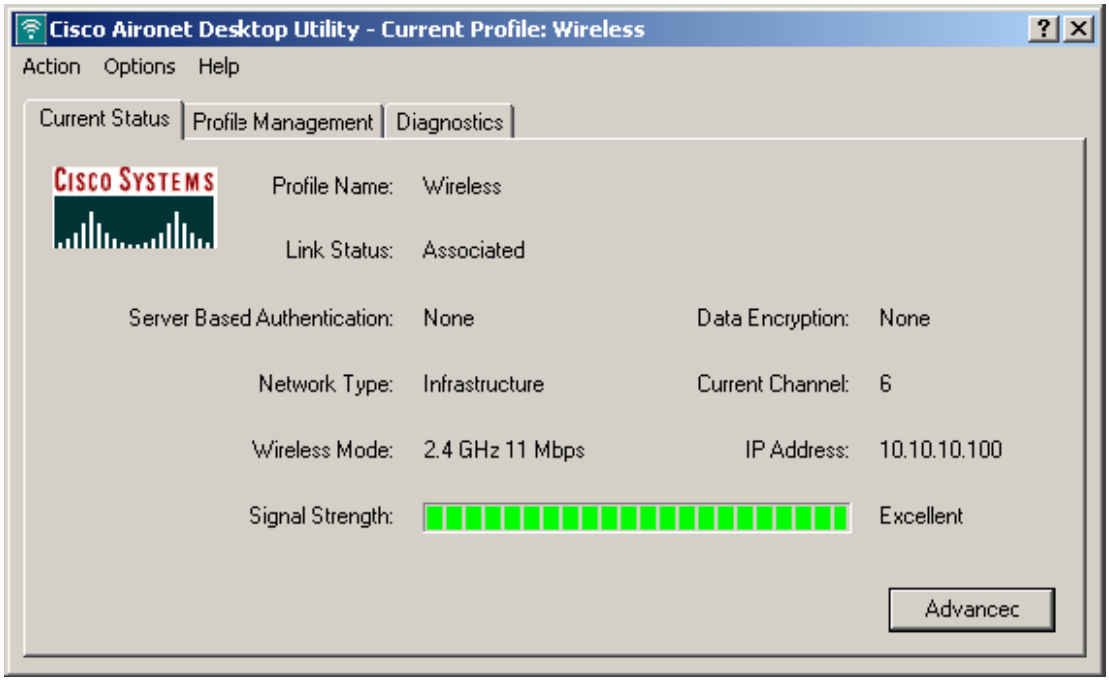


When the computer reboots, Windows *may* recognize that hardware has been installed.
a. Click **Cancel** on the **Windows Found New Hardware Wizard** to continue.
b. Navigate to the installation file for the client adapter. This file can be found either on the CD that came in the package with the CD or on a network server like Kheops as if this file was downloaded from Cisco.com.
Note It is usually recommended to download the lastest release as the CD was printed when the hardware shipped:modifications/bug-fixings have probably happened since.
c. Double click the approprioate file to start installation.

d. From the available Setup types, select the first option: **Install Client Utilities and Driver**.
e. Choose ADU as the tool to configure the client adapter.
f. Install ASTU and the Site Survey option too.

3. Step 3 Running ADU

To open the ADU double-click the desktop icon or navigate to the program shortcut from the **Start** button: Start>Programs>Cisco Aironet>Aironet Desktop Utility. Alternately, the **System Tray** icon can be used to launch the desktop utility (via ASTU).



The tabbed interface of the ADU allows access to each of the necessary tasks to configure and monitor the client adapter.

a. Click the **Advanced** button to view detailed setting information for the card. The Advanced Status tab can provide useful information about the current SSID as well as association information for the card. Click **OK** to close the window and return.
Write down what's in front of the following fields and explain the current status displayed:
SSID Channel: Frequency: Channel Set:

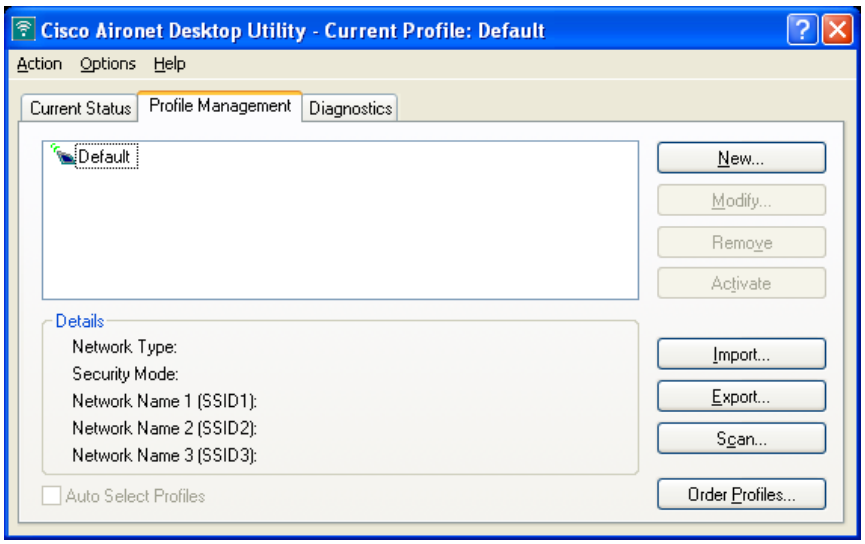
4. Step 4 Using the Profile Management

The Profile Management tab allows the creation, modification, removal or activation of client adapter profiles. Each profile can contain a unique set of authentication and encryption settings.
When installed, your client software is already configured with a built-in profile.

When starting the ADU, is there an already preselected profile ?

What are the name and properties of this built-in profile ?

What is the default behavior when no SSID is provided in the profile (3 SSID fields empty) ?

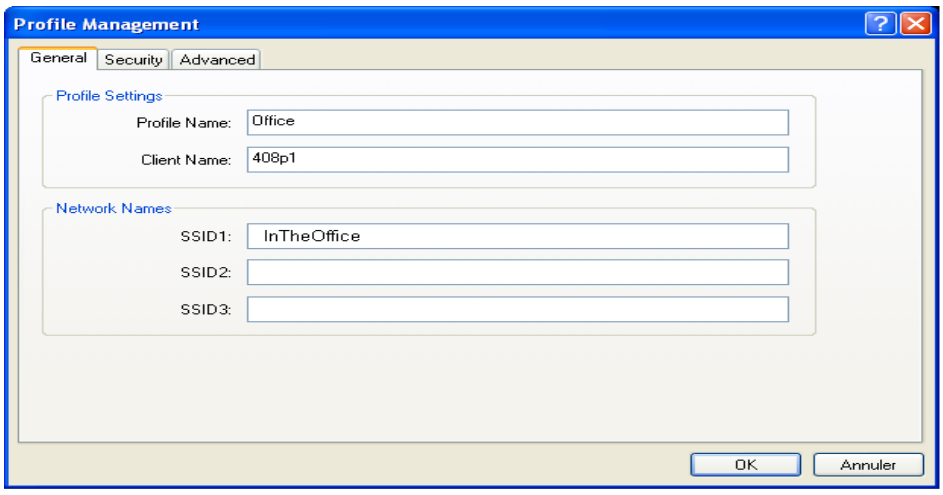


What tasks does the Profile manager allow?

Note Starting from now, you'll define several profiles in order to simulate real life use and situations. Imagine you have a wireless connection **in the Office** when working during the day with your laptop. When **back to Home**, you also have a Box working as an Access Point. Then, when you travel a lot, while waiting in public places, you want to be able to connect to public hotspots like the one you'll find at the **Airport**.
So, you'll configure enough profiles in this aim and have them automagically selected as you are moving from one place to another.

First, follow the steps below to create a new profile.
a. Select the **Profile** Management tab.
b. Click **New** and enter the name for the first new **Profile Name** named "Office" corresponding to the InTheOffice SSID as described below.

Note To use the default values, click **OK**. The profile is added to the list of profiles on the Profile Manager screen.



d. Check you have configured the Client name and SSID for the Office profile described above in order to

connect to the appropriate AP. Remember that configuring your Profile manages your level one (physical/802.11) connectivity but does not manage your level three (network/IP) connectivity.
e. Click **OK** to save your profile.

Can you activate several profiles at a time?

When would you consider entering multiple SSIDs instead of a single one?

5. Step 5 Selecting profile activation

Now you have created several profiles, you'll select manually the one you're interested in at a time.
Follow the steps below to specify the profile that the client adapter is to use.
a. Open ADU; click the **Profile Management** tab.
b. Now select the **Office** Profile
c. Click **Activate** to save the selection.
d.The client adapter starts using a profile based on the option selected above.

Note Use double-click for selction and activation on the fly.

What are the benefits of being able to define several profiles ?

Why is this better to use three different profiles with one SSID in each rather than creating one single profile including all the three SSID ?

Note Other tabs of the ADU will be covered later in the upcoming sessions: browse through them but be patient.

Note If the client adapter cannot associate to an AP or looses association while using the selected profile, the adapter does not attempt to associate using another profile. To associate, a different profile must be manually selected. But have a look on the next paragraph.

6. Step 6 Scanning for available networks

The Profile Management tab also includes a **Scan** button that displays Available APs and Ad Hoc Networks. Those network names listed with a key icon demonstrate that the network is secured. If no key is displayed, the network is not secured and will likely accept guest associations.
Highlight a network name (Unice-Hotspot for instance) and click the **Activate** button to connect to an available network. If no configuration profile exists for that network, the Network Configuration Settings window opens to the General tab. Fill in the network name and click OK to create the configuration profile for that network.

Click the Scan button and write down what are the available Infrastructure and Ad Hoc networks that broadcast their SSIDs, and the number of networks not broadcasting their SSIDs.

7. Step 7 Managing the Wireless adapter using the native Windows Zero Config wizard and service

Or « how to use Another Application To Configure My Wireless Settings »
This option allows another application (not the ADU/ACU) to configure the client adapter, like a multi-seller piece of software or a snap-in directly included in the OS itself. Examples of such applications include Windows XP Zero Configuration Wizard.

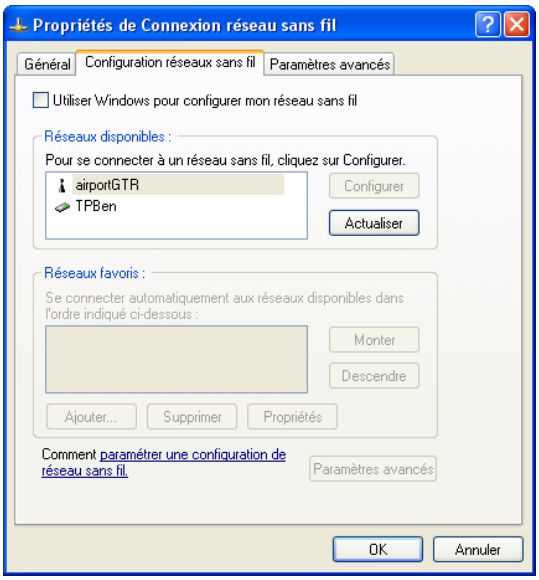
You can manage your wireless adaptor using **one software or the other but not the two in the same time**:

- Windows Zero Config: this windows service is implemented as a wizard that detects Wireless networks and offers you a connection using windows built-in driver.
- ACU/ADU software: the software and driver provided by your wireless hardware seller.

How to decide to activate/deactivate the WZC service

You must tick this option « Utiliser Windows pour configurer mon réseau sans fil » if you are configuring your card through Windows XP Windows Zero Config service (but do not want to use ACU's configuration and diagnostic tools). In ADU, the tab “Options” allows to choose what tool you will use to configure your client adapter (“Choose client utility”).

Note Be careful, when you have several wireless adapters, activating the WZC activates it for all wireless adapters.



4. Setting up a peer-to-peer ad hoc connection

Creating an Ad Hoc Network using ADU

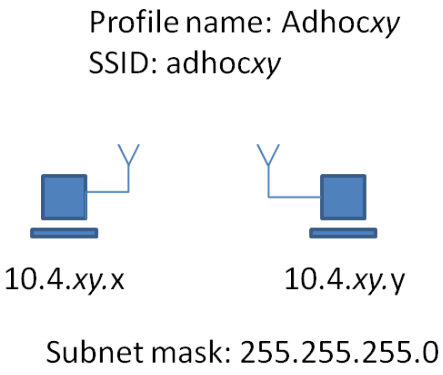
Objective

Each team will configure several personal computers to communicate with each other without an AP or cables.

Scenario

Previously used PCs equipped with wireless client adapters will be needed. This lab will cover the Cisco® Aironet® IEEE 802.11a/b/g Wireless Adapter and how to configure the associated Aironet Desktop Utility (ADU) to allow them to connect together as a network without an AP.

Topology



Preparation

Unique IP Addresses should be assigned to each client adapter or personal computer within each team to avoid IP conflicts.

Each team should use the same SSID for each PC in the pairing devices to ensure that the computers associate to each other. The SSID to be used for all PCs is **adhocXY** (where XY is the group number assigned by the instructor).

Team	Client Name	Profile name	SSID	IP addresses
12	408p1 & 408p2	Adhoc12	adhoc12	10.4.12.1 & 10.4.12.2
34	408p3 & 408p4	Adhoc34	adhoc34	10.4.34.3 & 10.4.34.4
56	408p5 & 408p6	Adhoc56	adhoc56	10.4.56.5 & 10.4.56.6
78	408p7 & 408p8	Adhoc78	adhoc78	10.4.78.7 & 10.4.78.8
910	408p9 & 408p10	Adhoc910	adhoc910	10.4.91.9 & 10.4.91.10
1112	408p11 & 408p12	Adhoc1112	adhoc1112	10.4.111.11 & 10.4.111.12

Step 1 Create a profile named adhocP (where P is the team number)

On the Cisco Aironet equiped machine:
a. Open the Cisco Aironet Desktop Utility.
b. Click on the **Profile Management** tab.
c. Click on the **New…** button.
d. Complete the **Profile Name**, **Client Name** and **SSID1** fields with the settings provided in the previous table.
e. Click the **Advanced** tab to set the Network Type for **Ad Hoc**, 802.11g, 54Mbps and 10mW.
The default setting is Infrastructure. Click **OK** to save your settings.
f. Operate the same instructions in sequence on the other computer.

Step 2 Select the profile named adhocP (where P is the team number)

In order to connect to the peer, the adhoc profile on both computers must be activated.
a. From the **Profile Management** tab, click the appropriate adhoc profile and then click the **Activate** button to use the ad hoc profile.
b. The computers should associate. If association does not occur, troubleshoot as needed.

Step 3 Obtain the MAC address of the PC

Once the computers are associated, you can view information about the peer computer.
Use appropriate command and write down the results

Step 4 File share in Ad Hoc Mode

Setup the left-hand side (PCx) as a FTP server. To do so, install Filezilla server on that PC.
Try to transfer a file by FTP between PCy and PCx. (see ftp command line help).

Step 5 Performance measures

Perform a rate measurement thanks to netperf or iperf between the two PC, connected in ad hoc mode.
Comment the results.

Step 5 Create an AdHoc Network with Internet Connection Sharing

Is it necessary to purchase an AP in order to share the fast broadband connection at home? This lab is very similar to using a cross-connect cable for a small PC network, but without the use of the router or additional cables.

a. Once PCx and PCy are connected in ad hoc mode, setup the wired connection by NIC IUT on PCx, so as to get proper Internet connection.
b. Share the Internet connection on PCx
c. Configure PCy so as to get full Internet connection **with the specified above IP addresses**. (Beware that Windows set up its own IP addresses. Do not let it do that). Check the traffic on PCx with Wireshark, while connecting to the Internet with PCy.

5. Setting up an infrastructure network: access point basic configuration

Configuring Basic AP Settings

Objective

In this lab, the student starts getting familiar with the access point. Student will assign basic parameters to the AP using the Web GUI (graphical user interface) and then do similar configuration using the IOS CLI (command line interface).
First, the « Express Setup » page will be accessed through a web browser to assign some network parameters, and SSID to the AP. Then the student will step into the detailed configurations menus and tabs.

Scenario

Basic configuration of an AP can be done through the GUI or IOS CLI.
Each group of student will be responsible for its own **isolated** network: the wired and the wireless part.
Using dedicated hardware available in room 408, the student will be responsible for connecting devices and managing the resulting networks.

Command List

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
`configure terminal`	Enter Global configuration mode
`hostname`	Set the hostname on the device
`interface bvi1`	Enter the virtual interface for the AP
`ip address`	Set the IP address and subnet mask on the device
`interface dot11radio 0`	Enter the device radio interface
`station role repeater | root [ fallback { shutdown | repeater } ]`	Set the AP role. Set the role to repeater or root. (Optional) Select the fallback role of the radio. If the Ethernet port of the AP is disabled or disconnected from the wired LAN, the AP can either shut down its radio port or become a repeater AP associated to a nearby root AP.
`ssid ssid-string`	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. **Note:** Do not include spaces or underscore characters in SSIDs.
`enable password password`	The default password is Cisco. This commands allows an administrator to change the password
`enable secret password`	The default enable password is *Cisco*.
`enable password level level password`	The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
`show dot11 associations`	View the connected wireless clients
`show running-config`	Display the current configuration of the device
`show startup-config`	Display the startup configuration of the device
`copy running-config startup-config`	Save the entries into the configuration file
`show interfaces`	Display interface information of the device

Step 1 Connect to the AP using a console

a. Connect a cable between the console port of the AP and the serial port of the left hand side PC.
b. Open a terminal emulator, like Hyperterminal on Windows (Démarrer->Programmes->Accessoires)
c. Enter these settings for the connection:
- Bits per second (baud rate): 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none

d. Press return to get started
e. One you get a prompt (remember default passwords), type:
APname>enable
APname# erase startup-config
APname# reload

Step 2 Configure the PC for a web connection

Team	x=	y=	AP Name	SSID	AP address	408px address	408py address
12	1	2	ap12	s408tp12	10.0.12.100/24	10.0.12.1/24	10.0.12.2/24
34	3	4	ap34	s408tp34	10.0.34.100/24	10.0.34.3/24	10.0.34.4/24
...							

Note
Without a DHCP server connected to, the AP is supposed to default to 10.0.0.1/27 IP address when it does get replies to its DHCP requests. It actually takes hours because of large timeouts. That is why we directly set up an IP address according to the above table, so as to acces the AP through the network.
To do so, we configure the Bridge Virtual Interface (BVI):
The BVI allows all interfaces to be grouped under one IP address.
This single IP address will be used for AP management through wireless or ethernet interfaces.
Enter the bvi1 interface mode to configure the ip address, subnet mask settings:
Assign an IP address and address mask to the BVI.
APname#configure terminal
APname(config)#interface bvi1
APname(config-if)#ip address 10.0.XY.100 255.255.255.0
APname(config-if)#no shutdown
APname(config-if)#end

Step 3 Connect to AP using the web browser

a. Connect the NIC TP of the left-hand side PC (PCx) to the Ethernet connection of the AP.
b. Deactivate all network connections on PCx, except the “connexion au réseau local 2” that you must configure as described in the table above.
c. Open an Internet browser and type the IP address of the AP.
Note If using Internet Explorer or Mozilla, beware of proxy settings if any and allowing Javascripts.
d. A log in screen appears. Type in the password of **Cisco** (case sensitive) and click OK (username remains empty).
e. When the AP HOME page appears, click **Express Setup** if the Express Setup does not appear.
f. Type a system name of **apXY** (where **XY** is the Team number) for the AP in the System Name field.

Step 4 Assigning the static IP addresses and SSID

a. Select the **Express Setup** menu and type the IP address in the **IP Address** field.
What IP address is assigned to this AP according to the graphic interface?

_____

b. Check the IP subnet mask in the **IP Subnet Mask** field too.
What subnet mask is assigned to this AP? Write the answer in dotted decimal notation.

_____

Express the subnet mask in binary notation.

_____

c. Enter the IP address of the default Internet gateway in the **Default Gateway** field. Let's assume the router address in your simulation network is 10.0.xy.254.
d. Leave the **SNMP Community** field alone at this time (do not modify it).
e. Select the **Express Security setup** menu and type an SSID for the AP in the **Radio Service Set ID** (SSID) field.
What SSID is assigned to this AP?

_____

f. Verify the **Access Point or AP Root**: as the network role for the AP from the **Role in Radio Network** of the Express Setup menu.
What are the other options?

_____
_____
_____
_____
_____

g. Select **Throughput**: as the **Optimize Radio Network**.
What are the other options?

_____
_____
_____
_____

h. Click **OK**.

Step 5 Connect to the AP by way of a wireless PC

Connect PCy to your respective AP.
Make sure the wireless device is the only network adapter enabled on the workstation (disable the other network adapters to be sure of it).

a. Configure (see how to configure a profile using the ADU in the previous TP) and select a **tp** profile to connect to the AP. Make sure the **SSID** is configured in the **tp** profile to match the AP.
b. Configure a unique **Client Name** in the profile, such as **s408pZ** where Z is the PC official number.
c. Make sure to check or configure the TCP/IP settings to connect to the proper IP network.

Step 6 Performance measurement at the transport layer

a. While PCx is connected through a wired to the AP and PCy is wireless connected to the AP, perform an iperf (or netperf) measure of the rate, and write down the result. Perform the experiment for various window ssizes up to 65500.
b. Connect PCx through a wireless link to the AP, and do again the measurement between PCx and PCy. Perform the experiment for various window sizes up to 65500.
c. Comment the results.

_____
_____
_____
_____
_____

Step 7 Draw a current topology

Now we have built a simulation network, it is time to make a wrap-up of the installation and sketch a scheme representing the current topology.
Using the space below, use the existing topology and draw an updated topology with the IP addresses and subnet masks.

Step 8 Verify the wireless connection

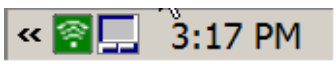
a. Using 408px computer, go to the **ASSOCIATIONS Page** on the AP using the web connection (http://10.0.XY.100) to check the wireless connection: this pages lists all associated wireless stations.
1. Does the Client Name appear which was previously configured?

_____

2. Record the MAC Addresses of the device(s) associated to your AP.
One of these addresses should be the MAC Address of desktop 408py configured in Step 4.

MAC ADDRESS

b. Now check to see if the ACU icon in the system tray is green, which indicates a successful link to the AP.



Double click on the icon to verify the correct **AP Name** and **AP IP Address.**

c. Now check to see if a connection to the AP using a web browser can be achieved from the wireless device.
d. Test connectivity to other devices by way of ping, telnet, http, and ftp. This will vary depending on the devices connected and configured on the wired network.
e. Make a backup of the access point configuration:
Using 408px computer, go to the **SYSTEM SOFTWARE Page** on the AP using the web connection (http://10.0.XY.100). Click on **System Configuration** subsection and click on « **config.txt** » link representing the « **Current startup configuration file** »: save it on local hard disk with name **config.txt.tp002.2.wri**.

Step 9 Access the AP through IOS CLI

Now everything is configured via the web interface and working fine, the student will erase the whole configuration in order to return to factory settings and rebuild a new similar configuration using the command line interface.

Open the HyperTerminal window on 408px. It should still be connected to the console port.
Enter privileged mode with the following command. **Cisco** is the default password.
apXY>**enable**
Password:
apXY#

Step 10 Erase the configuration through CLI

Erase the configuration with the following commands:
apXY#**erase startup-config**
Erasing the nvram filesystem will remove all files! Continue?
[confirm] (press Enter)
[OK]
Erase of nvram: complete
apXY# **reload**
System configuration has been modified. Save? [yes/no]: **N**
Proceed with reload? [confirm] (press Enter)
Radio system is preparing for reload...
Radio system is ready for reload.
*Mar 1 00:31:09.103: %SYS-5-RELOAD: Reload requested by console.
...

Step 11 Configure Hostname

The system name, while not an essential setting, helps identify the AP on your network. The system name appears in the titles of the management system pages.
a. Enter into configuration mode
ap>**enable**
Password:
ap#
ap#**configure terminal**
ap(config)#
b. Now configure the host name with the following command:
ap(config)#**hostname s408apXY** (where XY is the team number)
s408apXY(config)#

Step 12 Configure passwords

Now configure the enable password to *cisco*. Also, configure the secret password to *class*:
s408apXY(config)#**enable password cisco**
s408apXY(config)#**enable secret class**

Step 13 Configure SSID for 802.11b/g interface

Enter configuration of 802.11b/g interface (b/g is Radio0, a is Radio1 when available).
s408apXY(config)#**interface dot11radio 0**
Name an SSID for this interface only.
s408apXY(config-if)#**ssid s408tpxy** (where x and y are replaced by appropriate number)
Set authentication mode to open authentication for this SSID
s408apXY(config-if-ssid)#**authentication open**
Set the maximum number of client devices that can freely associate using this SSID to 15
s408apXY(config-if-ssid)#**max-associations 15**

Allow broadcast of SSID:
s408apXY(config-if-ssid)#**guest**
s408apXY(config-if-ssid)#**end (or Ctrl-Z)**
s408apXY#

Step 14 Check the running configuration and interface status

Display the current configuration of the device

s408apXY#**show running-config**
Browse the result of this command. Search for your inputs and the additional inputs that are inserted by default in the configuration

Display the condition and information of the device interfaces

s408apXY#**show interfaces**
Write the result of the command down here below with your comments

« show interfaces »: interresting lines of the output	Comments

Step 15 Save and verify the configuration is saved to Flash

Save the current configuration of the device into the configuration file.
s408apXY#**copy running-config startup-config**
Verify the startup configuration is saved in Flash.
s408apXY#**show startup-config**

Explain the difference between startup-config and running-config

_____
_____
_____

Step 16 Connect to the AP using a wireless PC (408py)

Using 408py with a wireless adapter, connect to the correct AP. Make sure the wireless device is used for connection and that you are not connected through the wired network...
a. Configure and select a profile to connect to the AP. Make sure the SSID is configured in the profile to match the AP.
b. Configure a unique **Client Name** in the profile, such as **client408py**
c. Make sure to check or configure the TCP/IP settings of the workstation to connect to the proper IP network.

Step 17 Verify the Associations

View the current device associations. The wireless device configured in previous step should appear in the association output of your AP.

apXY#**show dot11 associations**

Step 18 Connect to the AP remotely through Telnet

Follow these steps to open the IOS CLI with Telnet.
a. From PC 408py, Open a Telnet session to the AP located at 10.0.XY.100
b. At the username and password prompts, enter your administrator username and password. The default username is Cisco, and the default password is Cisco. (The default enable password is also Cisco.) The enable secret password is class. Remember usernames and passwords are case sensitive.

From a security point of view, what would you suggest instead of using telnet?

_____
_____

Step 19 Performing a Carrier Busy test

You can perform a carrier busy test to check the radio activity on wireless channels.
During the carrier busy test, the wireless device **drops all associations** with wireless networking devices for **4 seconds** while it conducts the carrier test and then displays the test results.
In privileged EXEC mode, enter this command to perform a carrier busy test:
APname#dot11 interface-number carrier busy
For interface-number, enter:
Dot11radio0 to run the test on the 2.4-GHz radio,
or enter **Dot11radio1** to run the test on the 5-GHz radio.

a.Use the **show dot11 carrier busy** command to re-display the carrier busy test results.

Used 802.11b/g channels	AP names and mode (i=infra, ah=ad'hoc)
Used 802.11a channels	AP names and mode (i=infra, ah=ad'hoc)

b.Compare with NetStumbler results: anything else ?

c.Compare with Airodump results: anything else ?