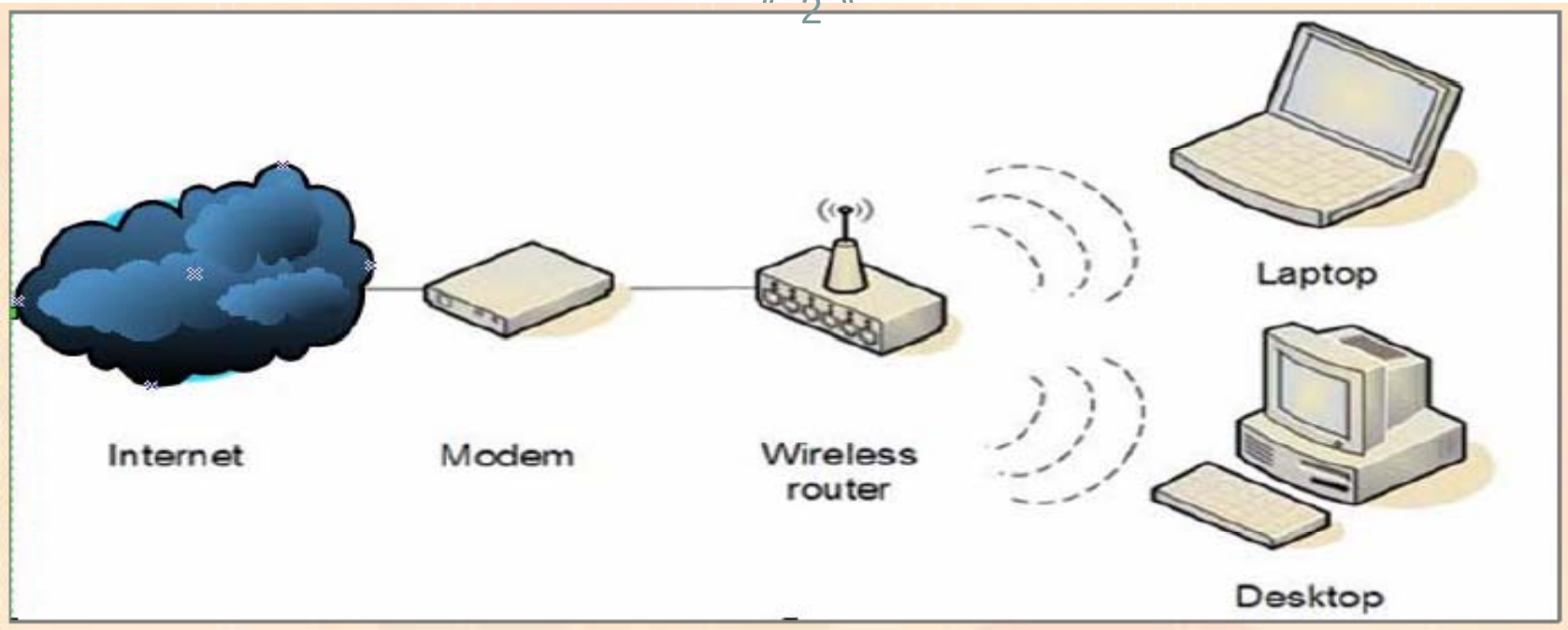
WIRELESS SECURITY

MUHAMMAD ZEN SAMSONO HADI, ST. MSC.
EEPIS-ITS

Typical Home Wireless Network



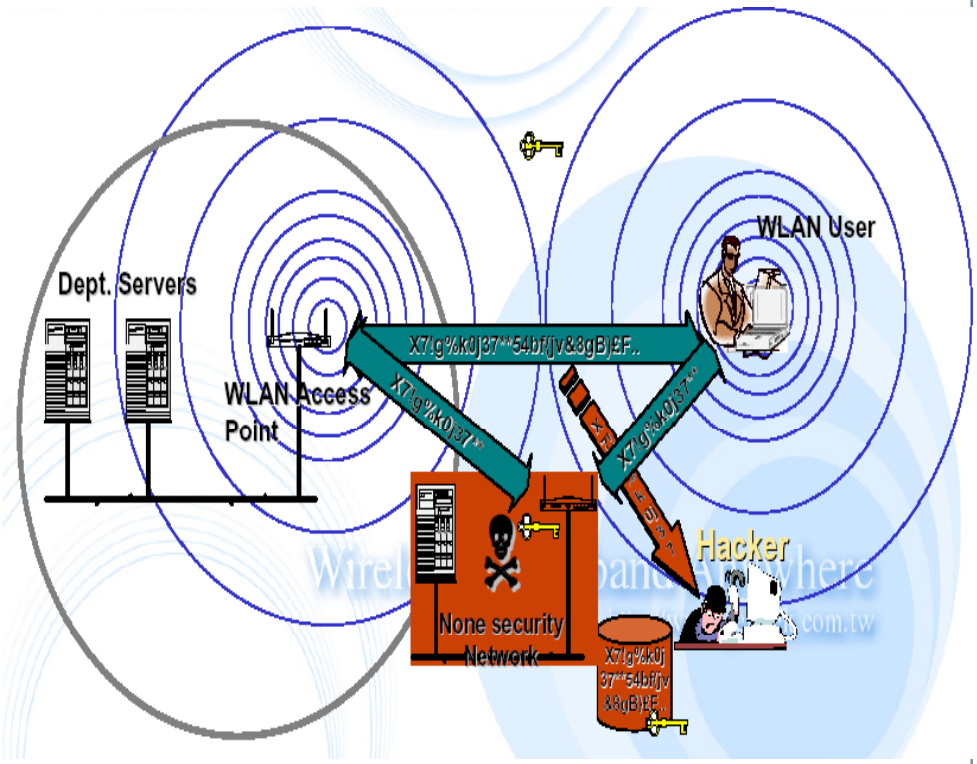
- *Home wireless networks terdiri dari paling tidak satu wireless access point / router dan satu atau lebih komputer yang terhubung ke wireless router.*
- *Access Point / router adalah perangkat untuk mengakses internet atau komputer yang lainnya untuk sharing.*

Standar 802.11

802.11 Standards	
802.11	The original WLAN Standard. Supports 1 Mbps to 2 Mbps.
802.11a	High speed WLAN standard for 5 Ghz band. Supports 54 Mbps.
802.11b	WLAN standard for 2.4 Ghz band. Supports 11 Mbps.
802.11e	Address quality of service requirements for all IEEE WLAN radio interfaces.
802.11f	Defines inter-access point communications to facilitate multiple vendor-distributed WLAN networks.
802.11g	Establishes an additional modulation technique for 2.4 Ghz band. Intended to provide speeds up to 54 Mbps. Includes much greater security.
802.11h	Defines the spectrum management of the 5 Ghz band for use in Europe and in Asia Pacific.
802.11i	Address the current security weaknesses for both authentication and encryption protocols. The standard encompasses 802.1X, TKIP, and AES protocols.

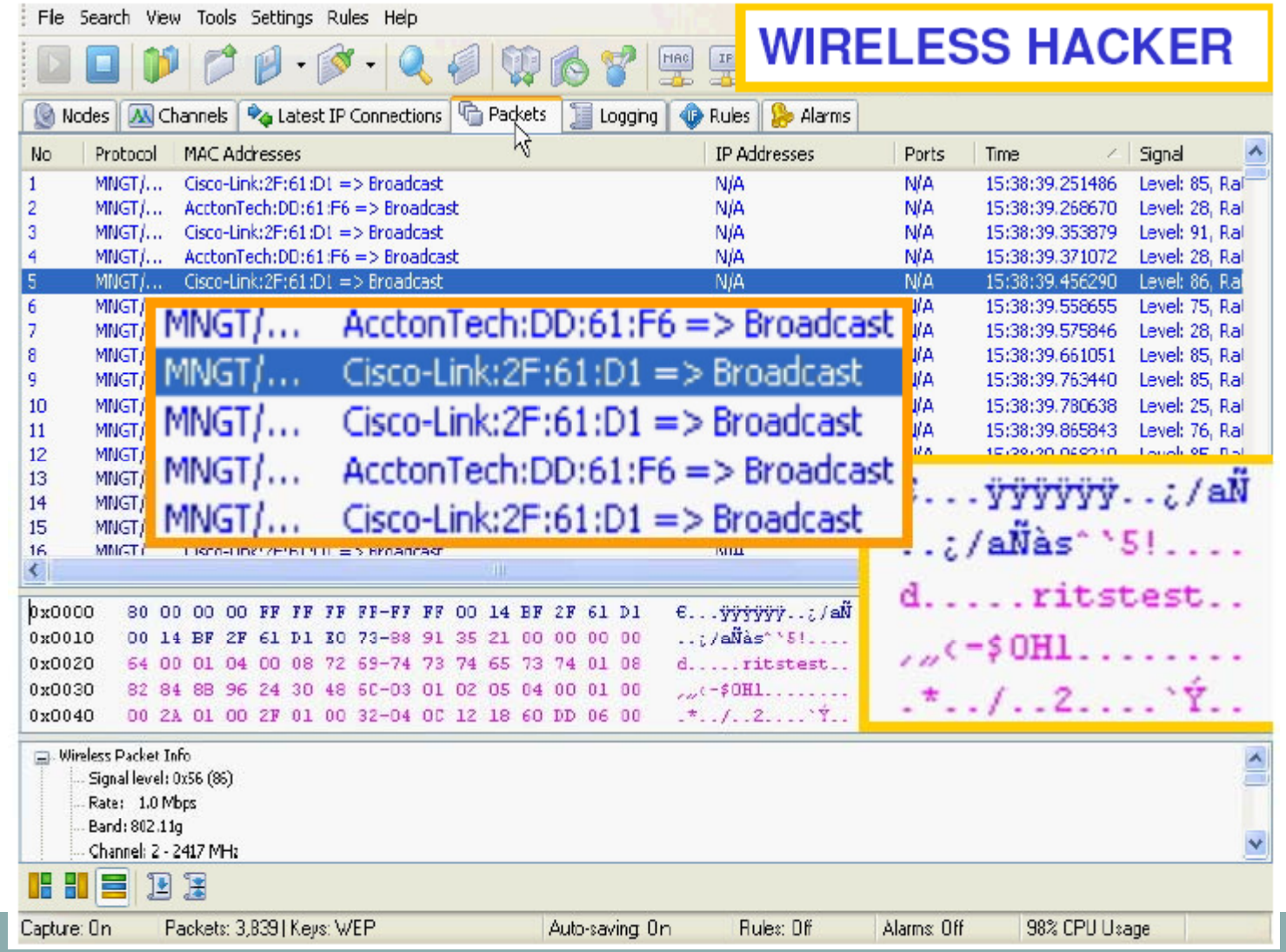
Wireless Security Thread

- Passive Data Sniffing
- Unathorized Access
- Jamming DoS Attack/packet Flood
- User Hijacking & Man In The Middle

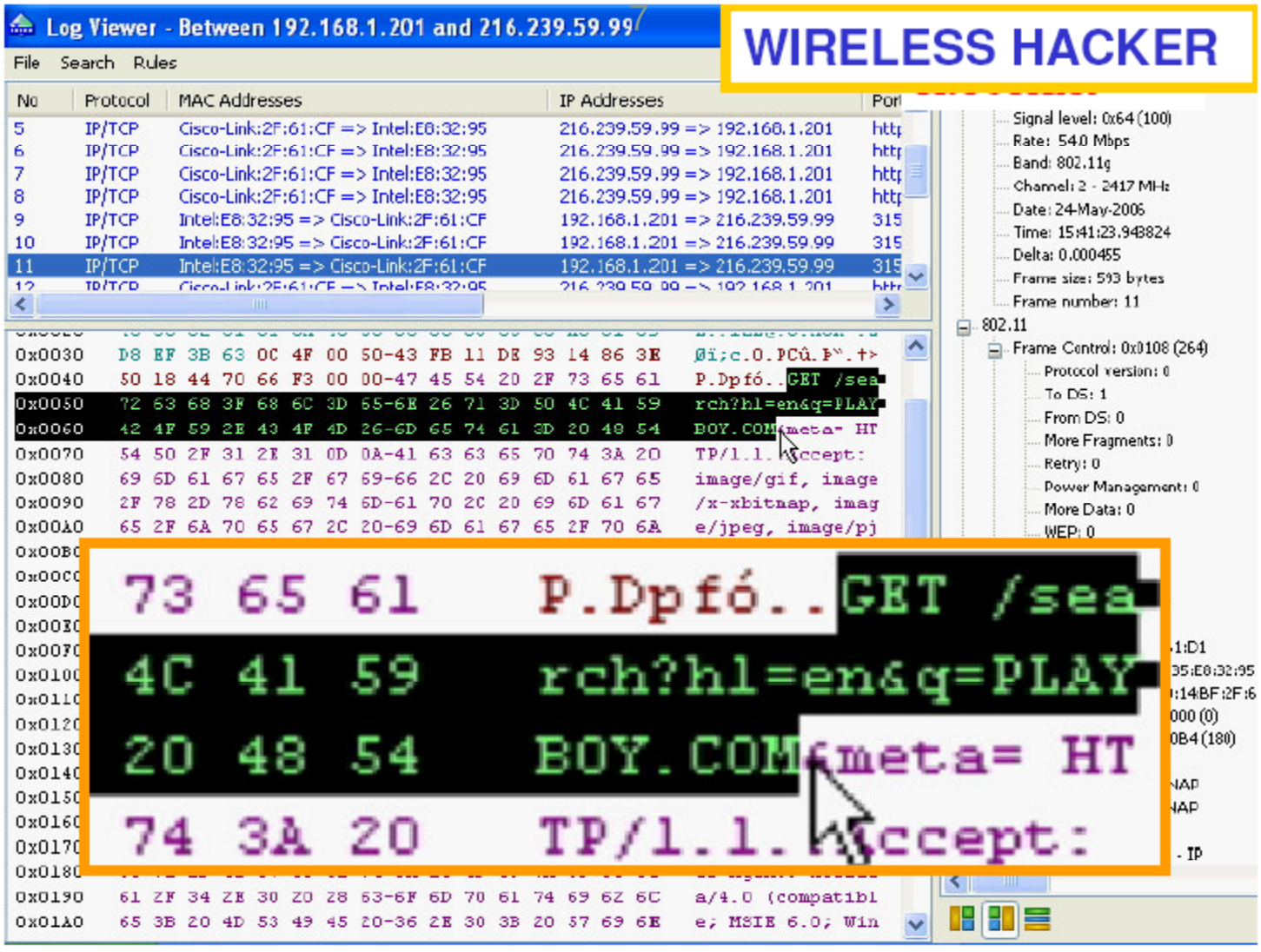


Wireless Sniffing

Wirelesss Sniffing



Wireless Sniffing



Kelemahan Wireless Network

- Kelemahan jaringan wireless secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan.
- Kelemahan tersebut seperti : wireless yang dipasang pada jaringan masih menggunakan setting default bawaan vendor seperti SSID, IP Address , remote manajemen, DHCP enable, kanal frekuensi, tanpa enkripsi bahkan user/password untuk administrasi wireless tersebut.

Kelemahan Wireless Network

- WEP (Wired Equivalent Privacy) yang menjadi standart keamanan wireless sebelumnya, saat ini dapat dengan mudah dipecahkan dengan berbagai tools yang tersedia gratis di internet.
- WPA-PSK (WiFi Protected Access-PreShared Key) dan LEAP (Lightweight Extensible Authentication Protocol) yang dianggap menjadi solusi menggantikan WEP, saat ini juga sudah dapat dipecahkan dengan metode *dictionary attack secara offline*.

Pengamanan yg lemah pada Jaringan Wireless

- Menyembunyikan SSID (Service Set Identifier)
  - Hanya yang mengetahui SSID yang dapat terhubung ke jaringan
  - Beberapa tools yang dapat digunakan untuk mendapatkan ssid yang dihidden antara lain, kismet (kisMAC), ssid_jack (airjack), aircrack , void11.

- Keamanan wireless hanya dengan kunci WEP
  - Masalah kunci yang lemah, algoritma RC4 yang digunakan dapat dipecahkan.
  - WEP menggunakan kunci yang bersifat statis
  - Masalah *initialization vector (IV) WEP*
  - Masalah integritas pesan *Cyclic Redundancy Check (CRC-32)*

Pengamanan yg lemah pada Jaringan Wireless

- Keamanan wireless hanya dengan kunci WPA-PSK atau WPA2-PSK
  - Ada dua jenis yakni WPA personal (WPA-PSK), dan WPA-RADIUS/Enterprise.
  - Saat ini yang sudah dapat di crack adalah WPA-PSK, yakni dengan metode brute force attack secara offline.

- MAC Filtering
  - Pada jaringan wireless, duplikasi MAC adress tidak mengakibatkan konflik. Hanya membutuhkan IP yang berbeda dengan client yang tadi.
  - Bisa diserang dengan arp spoofing

Basic 802.11 Security Control

Encryption

- WEP (64/128 bit WEP -> 40/104 bit really)

  - Lemah di kriptografi -> static key

  - Mudah diserang

Authentication

- SSID
- Open Access /Shared Key
- MAC Address filtering

  - Spoofing

Integrity

- 32bit CRC, CRC pada dasarnya sebagai pengecekan error
- Paket dapat dimanipulasi

Physical Security

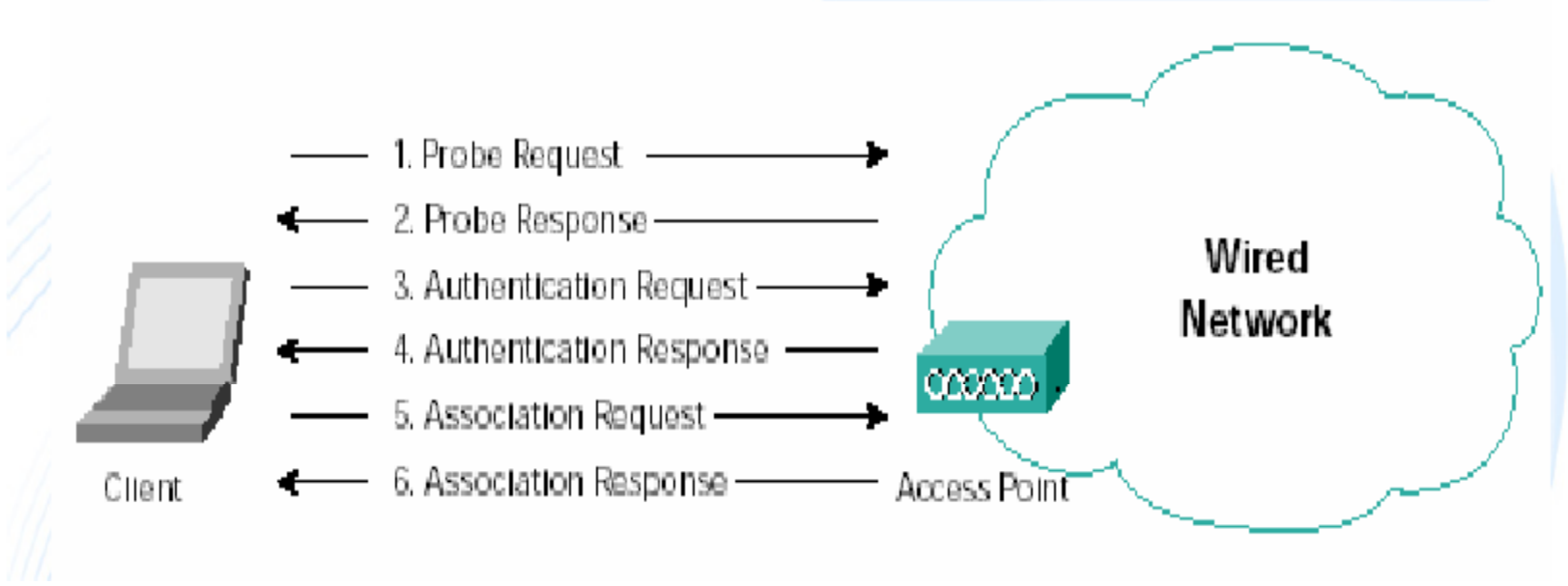
- Pembatasan range dari WLAN – mengurangi power AP

Improved Security Standards

- 802.1x Authentication (2001)
- WPA (Wi-Fi Protected Access) (2002)
- 802.11i (2003-4)

Association dan Authentication

- **802.11 Client Association and Authentication Process:**

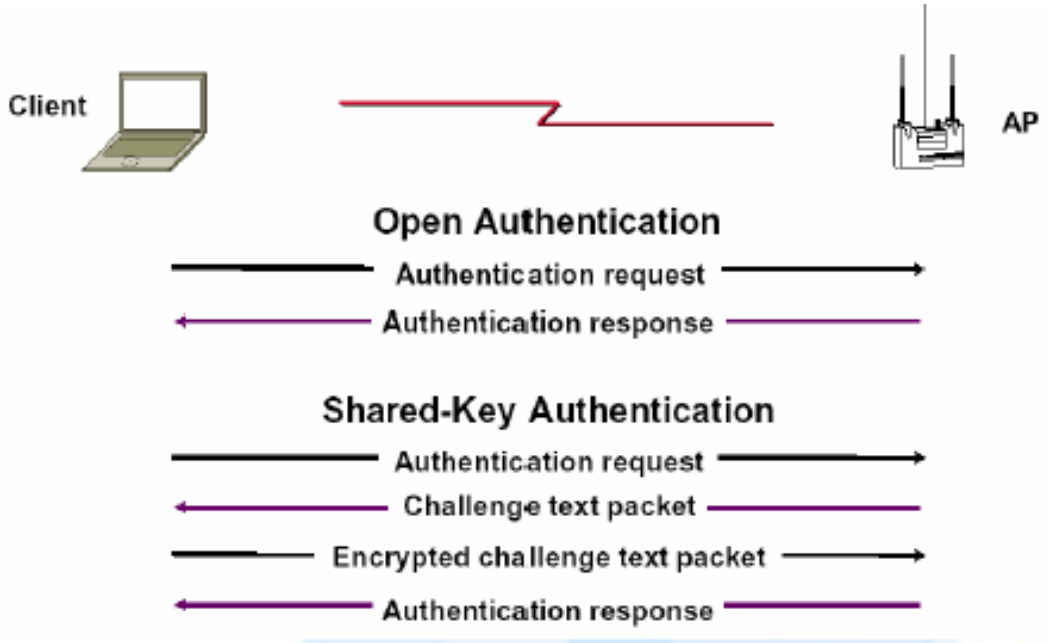


Authentication Mechanism

- Spesifikasi 802.11 mempunyai 2 mekanisme untuk otentikasi dari WLAN client:

❖ Open Authentication
  - Two Way Process

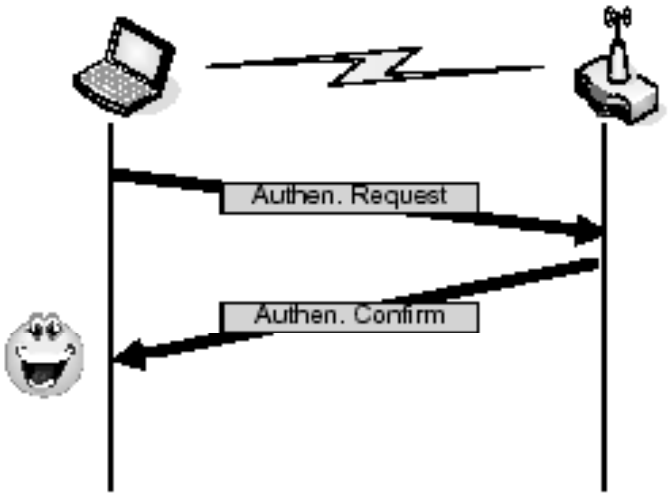
❖ Shared Key Authentication
  - Four Way Process
  - Diperlukan Security



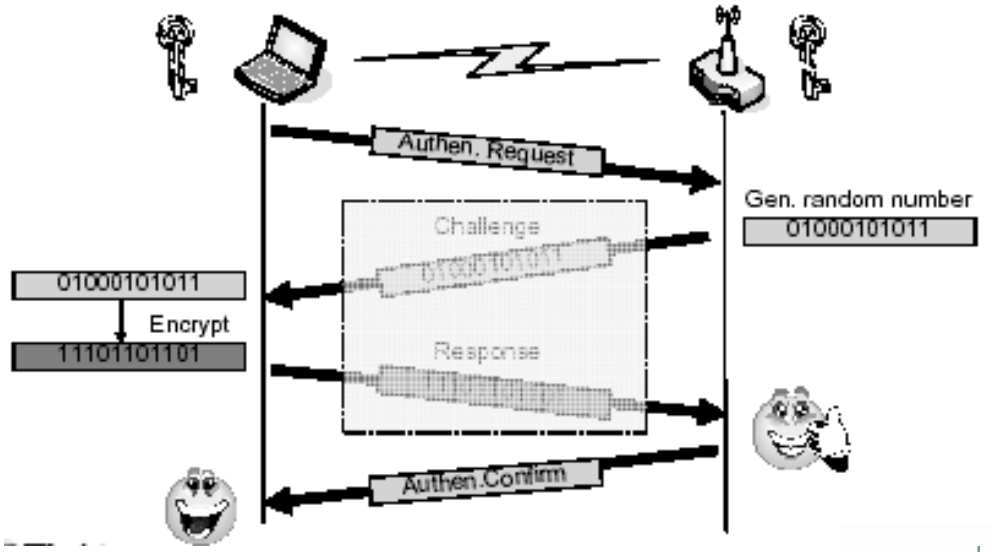
Authentication Mechanism

WEP Authentication

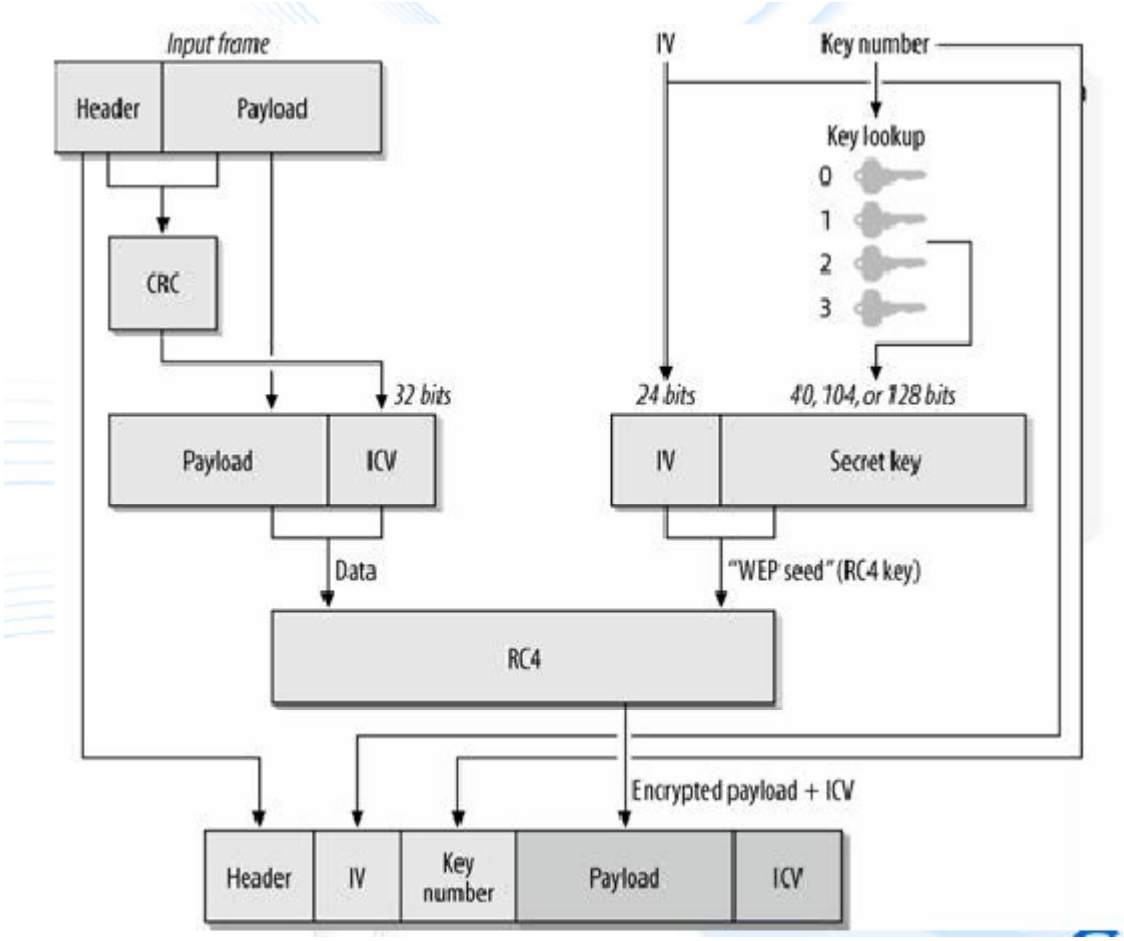
- Open Authentication – Accept all (no security)



- Shared Key Authentication



WEP Operation



WPA (WiFi Protected Access)

WPA(Wi-Fi Protected Access) – Better Security

Main improvements

- Address WEP Weaknesses – TKIP/MIC
- Better Authentication - 802.1X

Temporal Key Integrity Protocol (TKIP)

- Stronger privacy
  - Still uses RC-4 encryption
- Key rotation – (temporal key)
- Per packet keying

Message Integrity Code (MIC) - Stronger integrity

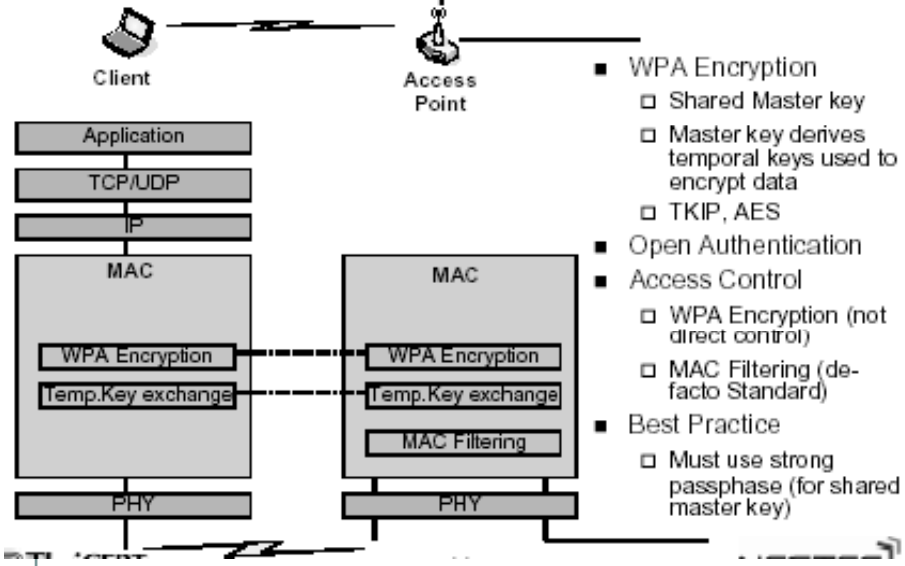
- Message Integrity Code (MIC) - computed with own integrity algorithm (MICHAEL)
- Prevents replay attacks

WPA-PSK Mode

Wi-Fi Protected Access (WPA)

- WPA is included in most of new Wi-Fi card
- WPA is based on standard IEEE 802.11i
- Two modes
  - WPA-PSK (WPA Pre-Shared Key) mode
  - WPA Enterprise Mode

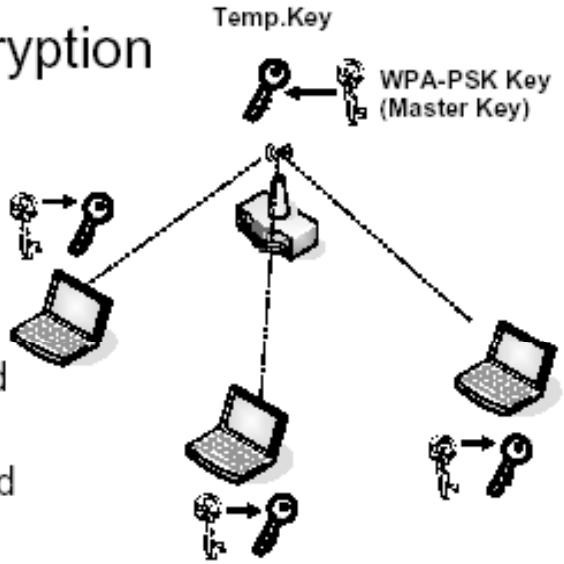
WPA-PSK Concepts



- WPA Encryption
  - Shared Master key
  - Master key derives temporal keys used to encrypt data
  - TKIP, AES
- Open Authentication
- Access Control
  - WPA Encryption (not direct control)
  - MAC Filtering (de-facto Standard)
- Best Practice
  - Must use strong passphase (for shared master key)

WPA-PSK Encryption

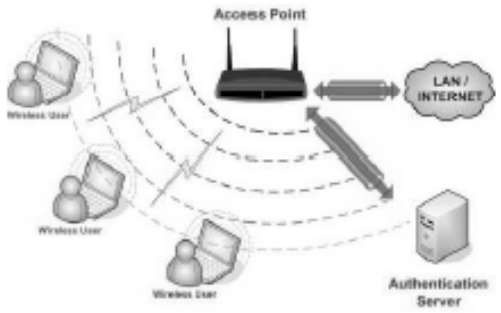
- WPA-PSK Key is static
- WPA-PSK Key is called Master key
- Master key is derived to Temporal Key
- Temporal Key is used to encrypt data



WPA Enterprise / Radius Mode

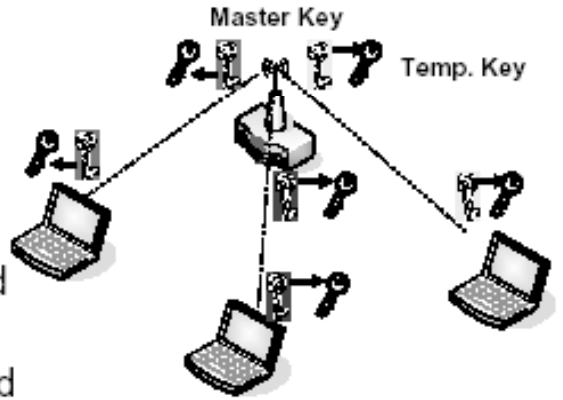
WPA Enterprise Mode

- Very secure
- Require authentication server to provide the user authentication
- Flexible to use the authentication method (i.e., EAP-TLS, EAP-PEAP)
- Key is dynamic



WPA Enterprise Encryption

- WPA Key (Master key) is assigned dynamically during authentication
- Master key is derived to Temporal Key
- Temporal Key is used to encrypt data



WPA-Enterprise / RADIUS Mode

Standar authenticates wireless LAN untuk end users agar dapat mengakses network.

1 Menggunakan Extensible Authentication Protocol (EAP) untuk memerintahkan AP meminta authentifikasi

2 AP melanjutkan permintaan authentifikasi ke radius server

Wireless Access

End-User Station

EAPOL (EAP)

RADIUS (EAP)

Request

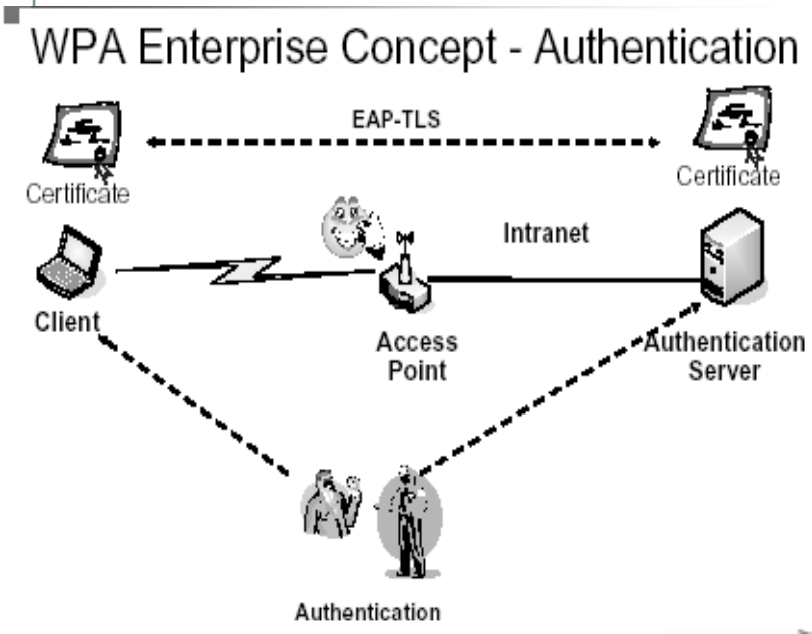
Password : ****

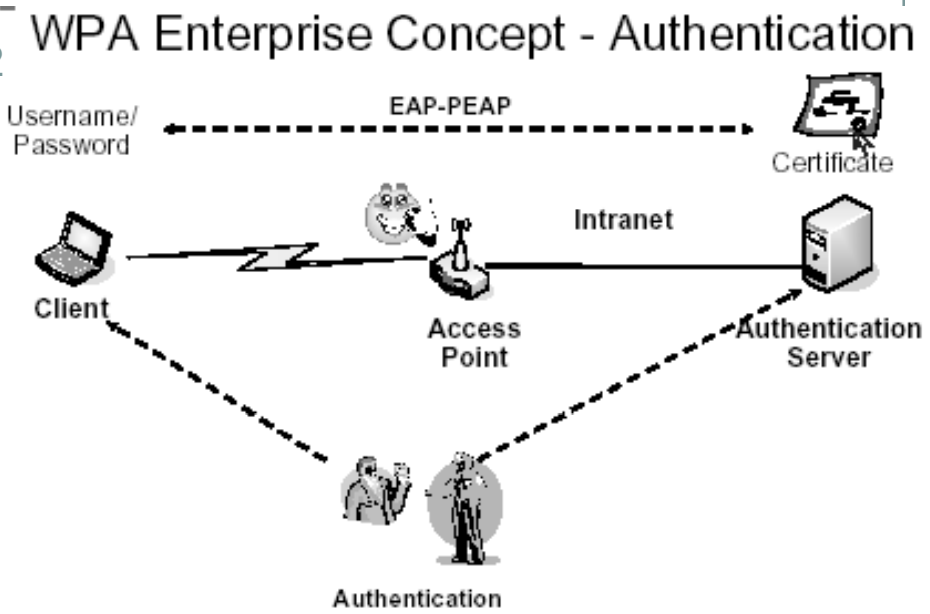
Radius Server

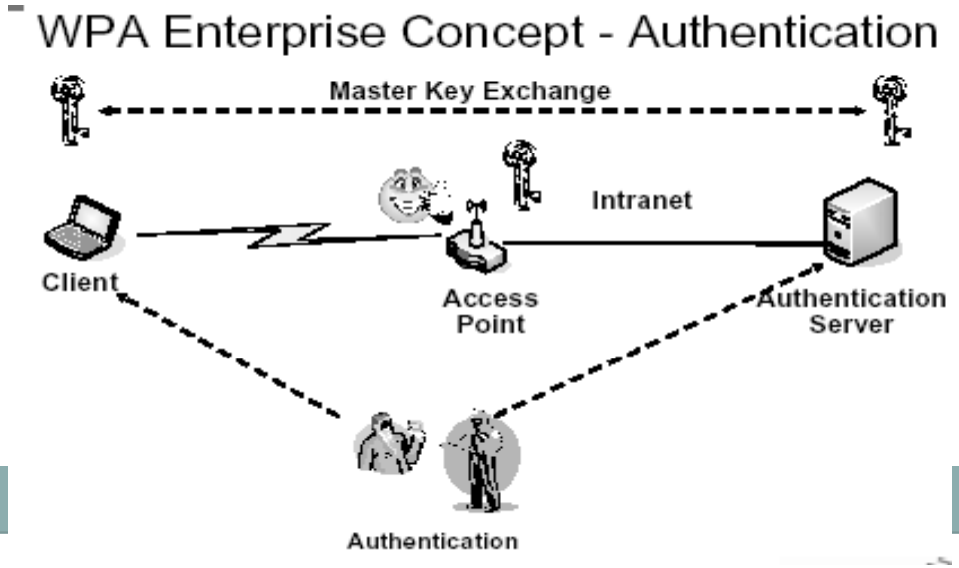
3 Radius server memberikan perintah pada end user untuk memasukan password .

4 Radius server akan melihat user sesuai atau tidak dengan user yang ada di data base.

WPA Enterprise / Radius Mode







WEP vs. WPA vs. WPA2

	WEP	WPA	WPA2
Encryption	RC4	RC4	AES
Key rotation	None	Dynamic session keys	Dynamic session keys
Key distribution	Manually typed into each device	Automatic distribution available	Automatic distribution available
Authentication	Uses WEP key as AuthC	Can use 802.1x & EAP	Can use 802.1x & EAP

Rekomendasi untuk Pengamanan Jar. Wireless dari Konfigurasi Dasar

- *Rubah password default router*
- *Rubah nama SSID dan disable SSID broadcast.*
- *Setup MAC filters untuk membatasi komputer mana yang dapat terkoneksi*
- *Turn on WPA atau WPA2 encryption.*
- *Review wireless logs.*
- *Lihat upgrade dari manufacturer.*
- *Aktifkan security lainnya spt firewall*

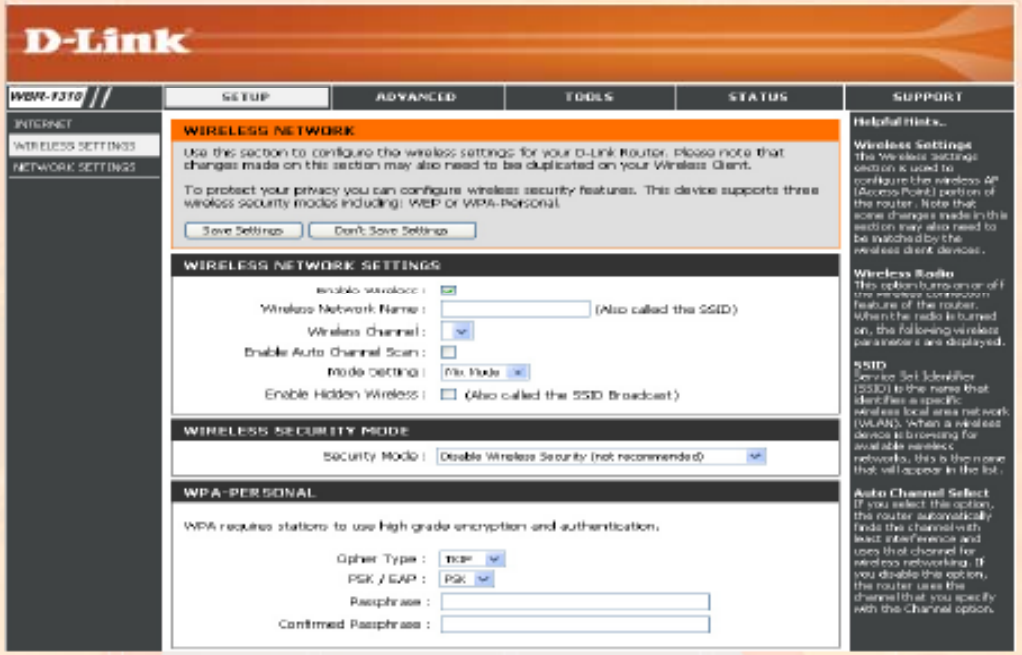
Step 1. Change the router's default passwords.

Most wireless router manufacturers provide Web pages that allow owners to enter their network address and account information. These Web tools are protected with a login screen (username and password) so that only the rightful owner can do this. Right out of the box, however, they are usually configured with a default password that is too simple and very well-known to hackers on the Internet. Change these settings immediately.

Step 2. Change the SSID name and disable SSID broadcast.

Access points and routers all use a network name called the SSID. Manufacturers normally ship their products with the same SSID set. For example, the SSID for Linksys devices is normally "Linksys." When someone finds a default SSID, they see it is a poorly configured network and are much more likely to want to snoop around.

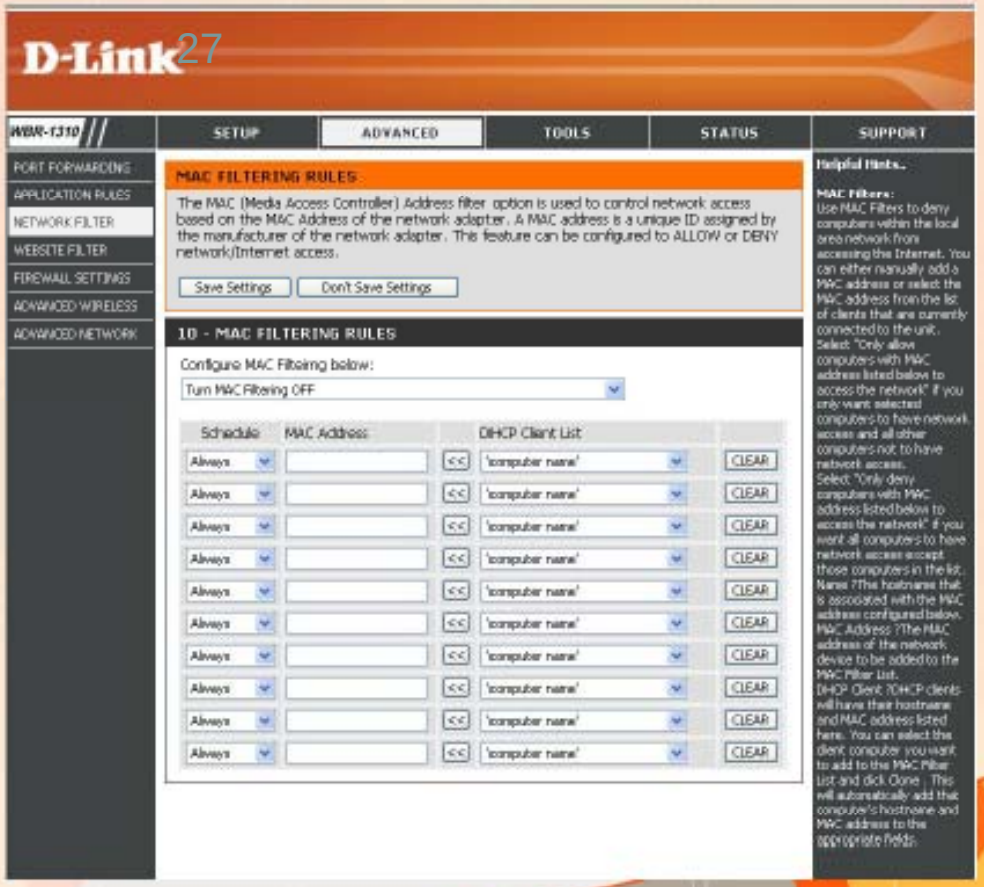
In Wi-Fi networking, the access point or router typically broadcasts the network name (SSID) over the air at regular intervals. In the home, this feature may be unnecessary, and it increases the likelihood an unwelcome person will try to log in to your home network.



Step 3. Setup MAC Filters.

All network communication devices have unique hard coded numbers assigned to them. This number is called the "MAC" address.

If your router is capable of MAC filtering you should only allow devices that you expect to appear connect to your wireless network and deny all others.



Step 4. Turn on WPA / WEP Encryption.

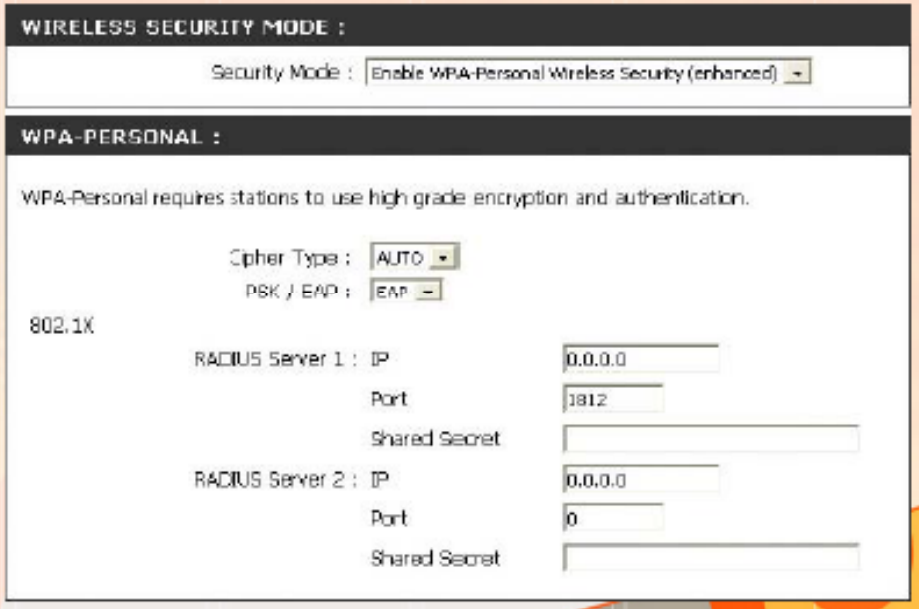
All Wi-Fi equipment supports some form of "encryption", which scrambles the information sent over the wireless network so that it can't be easily read. WEP or WPA are the most common encryption schemes found on home wireless systems. For most routers, you will provide a passphrase that your router uses to generate several keys. Make sure your passphrase is unique, not a dictionary word and at least 10 characters long – the longer, the better!

Understanding WEP vs. WPA2

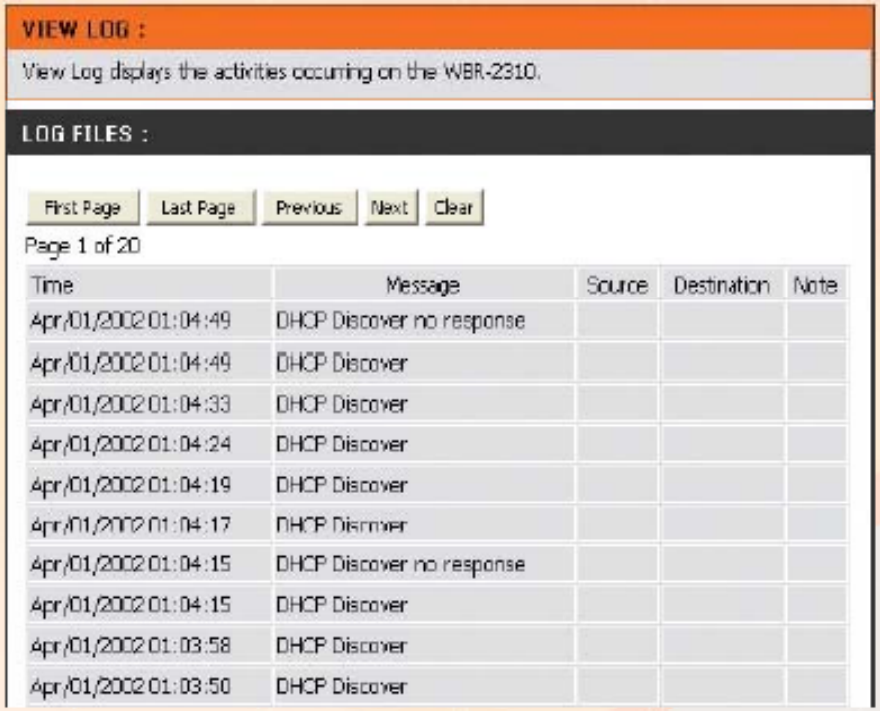
WEP *(wired equivalent privacy) was the encryption scheme included with the first generation of wireless networking equipment. It was found to contain some serious flaws which make it relatively easy to crack, or break into within a matter of minutes. However, even WEP is better than nothing and will keep casual snoopers and novice hackers out of your wireless network. Using encryption with a longer key length will provide stronger security, but with a slight performance impact.*

WPA *(WIFI protected access) is a much stronger security protocol than WEP and should be used instead of WEP if your wireless router and network adapters will support it. Some routers may refer to this as WPA-PSK.*

You should always consider using the router's strongest encryption mechanism.



Step 5. Review wireless Logs.



VIEW LOG :

View Log displays the activities occuring on the WBR-2310.

LOG FILES :

First Page | Last Page | Previous | Next | Clear

Page 1 of 20

Time	Message	Source	Destination	Note
Apr/01/2002 01:04:49	DHCP Discover no response			
Apr/01/2002 01:04:49	DHCP Discover			
Apr/01/2002 01:04:33	DHCP Discover			
Apr/01/2002 01:04:24	DHCP Discover			
Apr/01/2002 01:04:19	DHCP Discover			
Apr/01/2002 01:04:17	DHCP Discover			
Apr/01/2002 01:04:15	DHCP Discover no response			
Apr/01/2002 01:04:15	DHCP Discover			
Apr/01/2002 01:03:58	DHCP Discover			
Apr/01/2002 01:03:50	DHCP Discover			

Most routers will keep track of what systems have been successful or have failed to connect to your router.

Reviewing your logs can help identify a possible intruder or misconfiguration in your routers security.

Step 6. Watch for firmware upgrades for devices.

Network hardware is run by software called firmware. Just like computers, flaws may be found in the software that would allow people to bypass security mechanisms built into your router or network adapter. You should regularly check your wireless manufacturer's website for updates and apply when appropriate.

Step 7. Practice good computer security.

Don't rely only on your router/access point to protect your computers inside your wireless network. Even the most secure wireless network typically won't stop a determined hacker.

- *Enable System Firewalls*
- *Use accounts protected with a strong password*
- *Apply security patches to your OS in a timely manner*
- *Ensure you have antivirus up to date on your system*
- *Avoid using open shares on your computers to share files*
- *Be on the lookout for malicious websites, spyware/adware, phishing and scams*

Windows Users

http://www.microsoft.com/protect/default.mspx

Mac

http://www.apple.com/macosx/features/security/

How can I confirm my setup is secure?

When connecting to your wireless network. Look for "Security-enabled wireless connection".

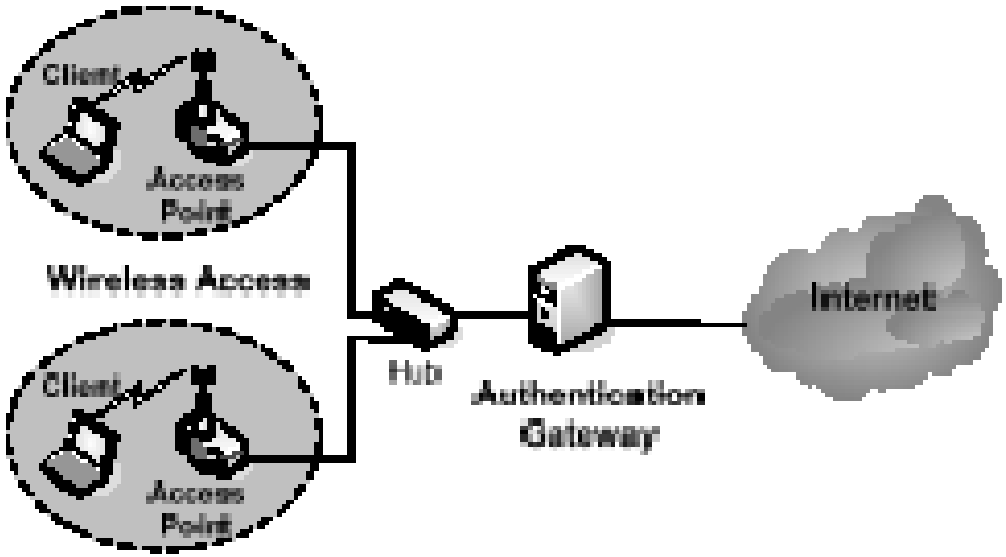
If your home network connection is listed as "Unsecured", you may be a sitting duck to individuals free-loading off your internet connection or snooping around on your computer.

Teknologi Security di Wireless

- MAC Filtering
- Authentication Gateway
- Wireless VPN
- Firewall
- VLAN, Virtual AP
- Upper layer security
- Personal Firewall

Authentication Gateway

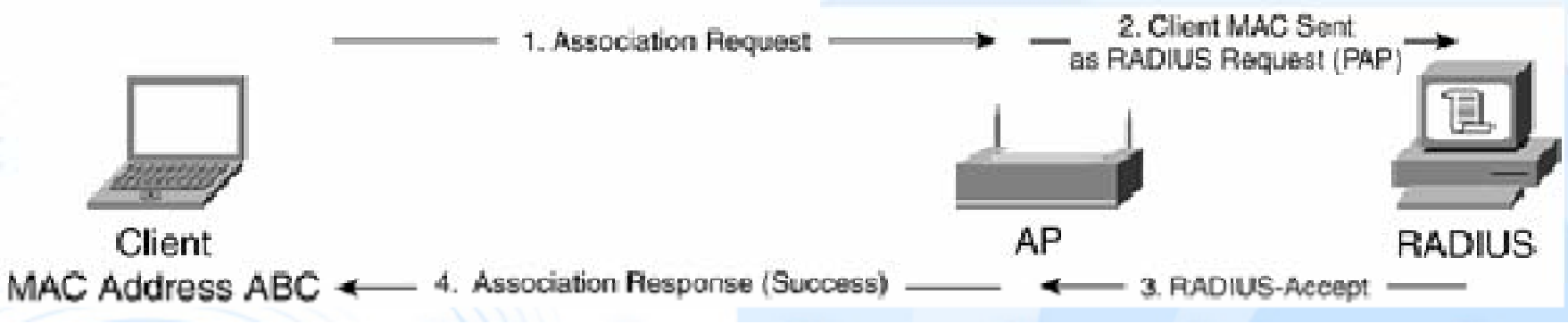
Authentication Gateway



- Commonly used in Wi-Fi hotspot
- User login is required before access the Internet
- User credential is transmitted to the gateway via SSL

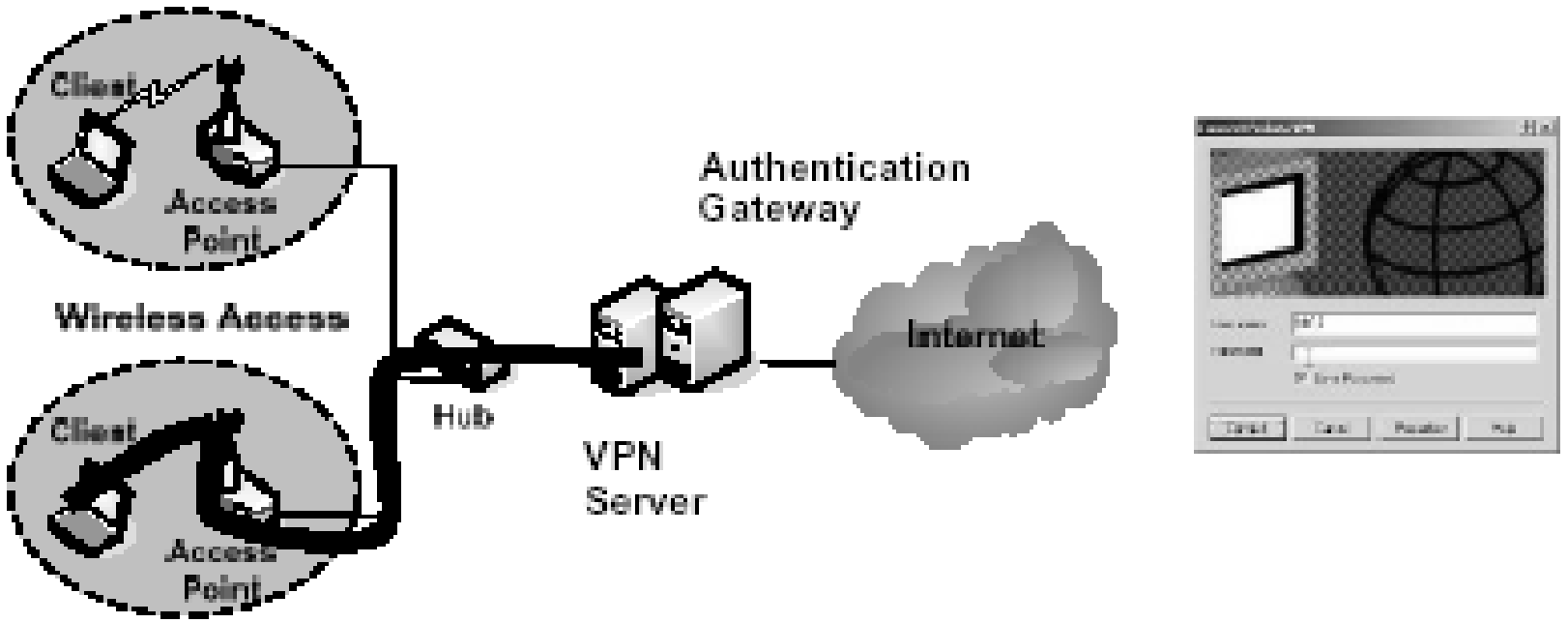
MAC Authentication

- **MAC Address Authentication**



Wireless VPN

Wireless VPN



- Create secured tunnel to protect wireless communication
- PPTP, L2TP/IPSec, IPSec, SSLVPN