

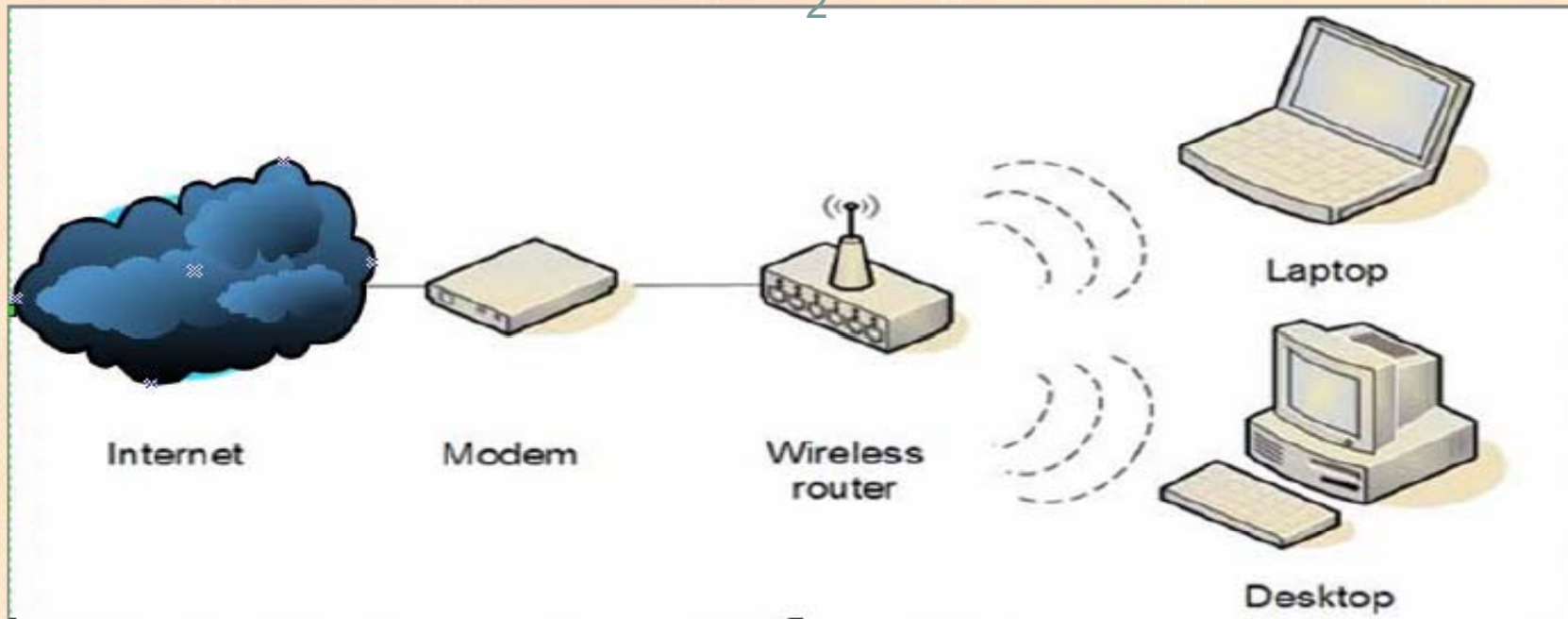
WIRELESS SECURITY

1

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

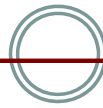
Typical Home Wireless Network

2



- *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



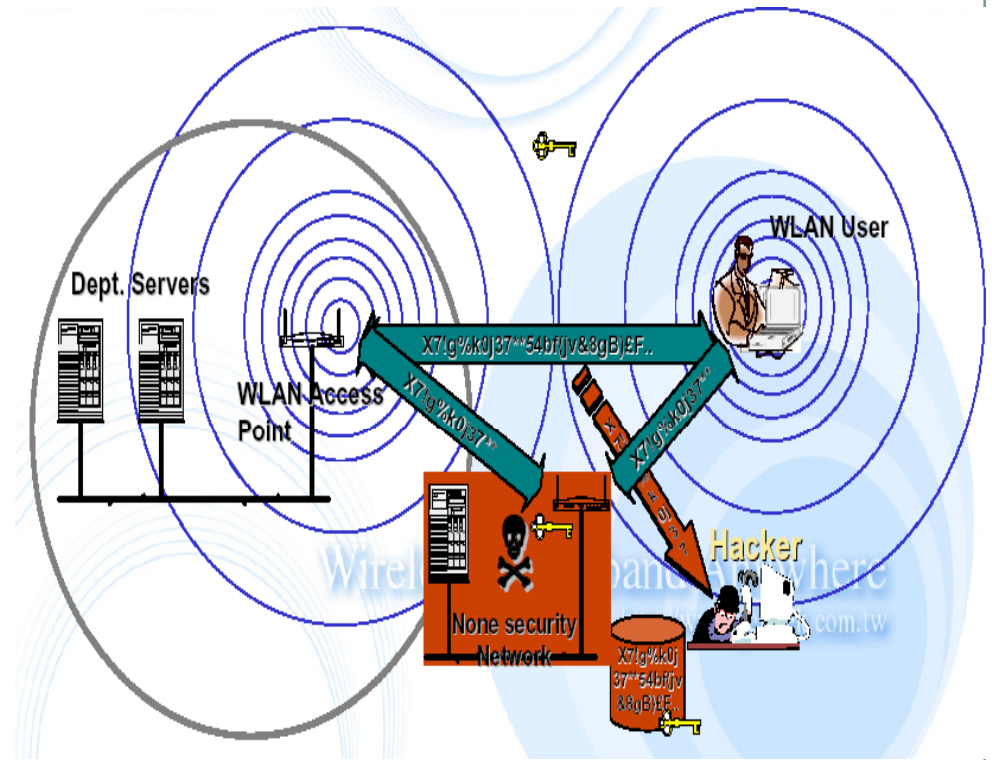
802.11 Standards

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

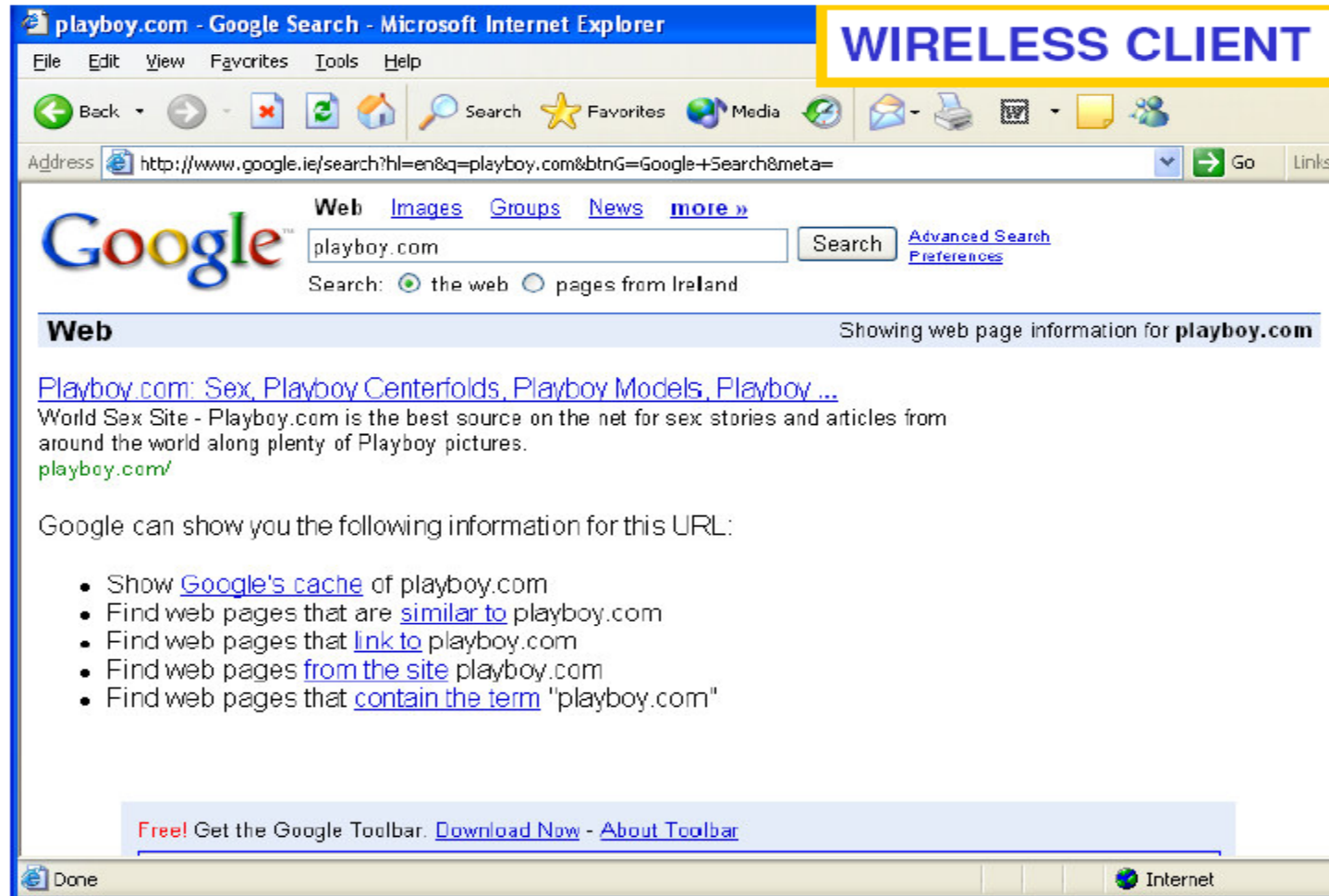
4

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



Wireless Sniffing

5



Wireless Sniffing

6

WIRELESS HACKER

File Search View Tools Settings Rules Help

Nodes Channels Latest IP Connections **Packets** Logging Rules Alarms

No	Protocol	MAC Addresses	IP Addresses	Ports	Time	Signal
1	MNGT/...	Cisco-Link:2F:61:D1 => Broadcast	N/A	N/A	15:38:39.251486	Level: 85, Rai
2	MNGT/...	AcctonTech:DD:61:F6 => Broadcast	N/A	N/A	15:38:39.268670	Level: 28, Rai
3	MNGT/...	Cisco-Link:2F:61:D1 => Broadcast	N/A	N/A	15:38:39.353879	Level: 91, Rai
4	MNGT/...	AcctonTech:DD:61:F6 => Broadcast	N/A	N/A	15:38:39.371072	Level: 28, Rai
5	MNGT/...	Cisco-Link:2F:61:D1 => Broadcast	N/A	N/A	15:38:39.456290	Level: 86, Rai
6	MNGT/...	AcctonTech:DD:61:F6 => Broadcast	N/A	N/A	15:38:39.558655	Level: 75, Rai
7	MNGT/...	AcctonTech:DD:61:F6 => Broadcast	N/A	N/A	15:38:39.575846	Level: 28, Rai
8	MNGT/...	Cisco-Link:2F:61:D1 => Broadcast	N/A	N/A	15:38:39.661051	Level: 85, Rai
9	MNGT/...	Cisco-Link:2F:61:D1 => Broadcast	N/A	N/A	15:38:39.763440	Level: 85, Rai
10	MNGT/...	Cisco-Link:2F:61:D1 => Broadcast	N/A	N/A	15:38:39.780638	Level: 25, Rai
11	MNGT/...	Cisco-Link:2F:61:D1 => Broadcast	N/A	N/A	15:38:39.865843	Level: 76, Rai
12	MNGT/...	AcctonTech:DD:61:F6 => Broadcast	N/A	N/A	15:38:39.865843	Level: 85, Rai
13	MNGT/...	AcctonTech:DD:61:F6 => Broadcast	N/A	N/A	15:38:39.865843	Level: 85, Rai
14	MNGT/...	Cisco-Link:2F:61:D1 => Broadcast	N/A	N/A	15:38:39.865843	Level: 85, Rai
15	MNGT/...	Cisco-Link:2F:61:D1 => Broadcast	N/A	N/A	15:38:39.865843	Level: 85, Rai
16	MNGT/...	Cisco-Link:2F:61:D1 => Broadcast	N/A	N/A	15:38:39.865843	Level: 85, Rai

Hex dump view:

```
0x0000  80 00 00 00 FF FF FF FF FF 00 14 BF 2F 61 D1  E...yyyyyy...:/aÑ
0x0010  00 14 BF 2F 61 D1 30 73 98 91 35 21 00 00 00 00  ..:/aÑas^`5!....
0x0020  64 00 01 04 00 08 72 69 74 73 74 65 73 74 01 08  d....ritstest..
0x0030  82 84 88 96 24 30 48 6C 03 01 02 05 04 00 01 00  /<-$OH1.....
0x0040  00 2A 01 00 2F 01 00 32 04 0C 12 18 60 DD 06 00  -*../..2....`Y..
```

Wireless Packet Info

- Signal level: 0x56 (86)
- Rate: 1.0 Mbps
- Band: 802.11g
- Channel: 2 - 2417 MHz

Capture: On Packets: 3,839 | Keys: WEP Auto-saving: On Rules: Off Alarms: Off 98% CPU Usage

Wireless Sniffing

Log Viewer - Between 192.168.1.201 and 216.239.59.99

WIRELESS HACKER

No	Protocol	MAC Addresses	IP Addresses	Port
5	IP/TCP	Cisco-Link:2F:61:CF => Intel:E8:32:95	216.239.59.99 => 192.168.1.201	http
6	IP/TCP	Cisco-Link:2F:61:CF => Intel:E8:32:95	216.239.59.99 => 192.168.1.201	http
7	IP/TCP	Cisco-Link:2F:61:CF => Intel:E8:32:95	216.239.59.99 => 192.168.1.201	http
8	IP/TCP	Cisco-Link:2F:61:CF => Intel:E8:32:95	216.239.59.99 => 192.168.1.201	http
9	IP/TCP	Intel:E8:32:95 => Cisco-Link:2F:61:CF	192.168.1.201 => 216.239.59.99	315
10	IP/TCP	Intel:E8:32:95 => Cisco-Link:2F:61:CF	192.168.1.201 => 216.239.59.99	315
11	IP/TCP	Intel:E8:32:95 => Cisco-Link:2F:61:CF	192.168.1.201 => 216.239.59.99	315
12	IP/TCP	Cisco-Link:2F:61:CF => Intel:E8:32:95	216.239.59.99 => 192.168.1.201	http

Signal level: 0x64 (100)
Rate: 54.0 Mbps
Band: 802.11g
Channel: 2 - 2417 MHz
Date: 24-May-2006
Time: 15:41:23.94824
Delta: 0.000455
Frame size: 593 bytes
Frame number: 11

802.11

Frame Control: 0x0106 (264)
Protocol version: 0
To DS: 1
From DS: 0
More Fragments: 0
Retry: 0
Power Management: 0
More Data: 0
WEP: 0

0x0030 D8 EF 3B 63 0C 4F 00 50-43 FB 11 DE 93 14 86 3E 0i;c.O.PC&.P".t>
0x0040 50 18 44 70 66 F3 00 00-47 45 54 20 2F 73 65 61 P.Dpfó..GET /sea
0x0050 72 63 68 3F 68 6C 3D 65-6E 26 71 3D 50 4C 41 59 rch?hl=en&q=PLAY
0x0060 42 4F 59 2E 43 4F 4D 26-6D 65 74 61 3D 20 48 54 BOY.COMmeta= HT
0x0070 54 50 2F 31 2E 31 0D 0A-41 63 63 65 70 74 3A 20 TP/1.1.Accept:
0x0080 69 6D 61 67 65 2F 67 69-66 2C 20 69 6D 61 67 65 image/gif, image
0x0090 2F 78 2D 78 62 69 74 6D-61 70 2C 20 69 6D 61 67 /x-xbitnap, imag
0x00A0 65 2F 6A 70 65 67 2C 20-69 6D 61 67 65 2F 70 6A e/jpeg, image/pj
0x00B0
0x00C0
0x00D0 73 65 61 P.Dpfó..GET /sea
0x00E0
0x00F0 4C 41 59 rch?hl=en&q=PLAY
0x0100
0x0110
0x0120
0x0130 20 48 54 BOY.COMmeta= HT
0x0140
0x0150
0x0160 74 3A 20 TP/1.1.Accept:
0x0170
0x0180
0x0190 61 2F 34 2E 30 20 28 63-6F 6D 70 61 74 69 62 6C a/4.0 (compatibl
0x01A0 65 3B 20 4D 53 49 45 20-36 2E 30 3B 20 57 69 6E e; MSIE 6.0; Win

1:D1
35:E8:32:95
0:14BF:2F:6
000 (0)
0B4 (180)
NAP
NAP
..IP

Kelemahan Wireless Network

8

- 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

9

- 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

10

- **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

11

- 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

12

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

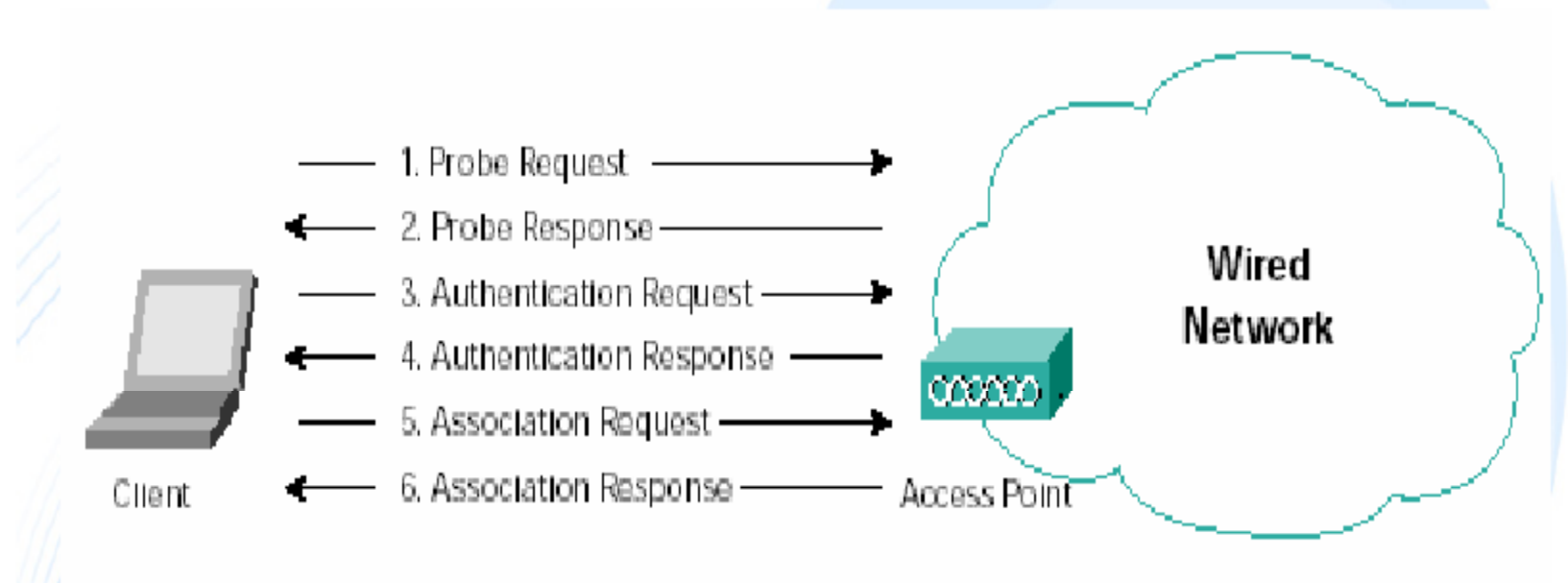


- **802.1x Authentication (2001)**
- **WPA (Wi-Fi Protected Access) (2002)**
- **802.11i (2003-4)**

Association dan Authentication

14

■ 802.11 Client Association and Authentication Process:



Authentication Mechanism

15

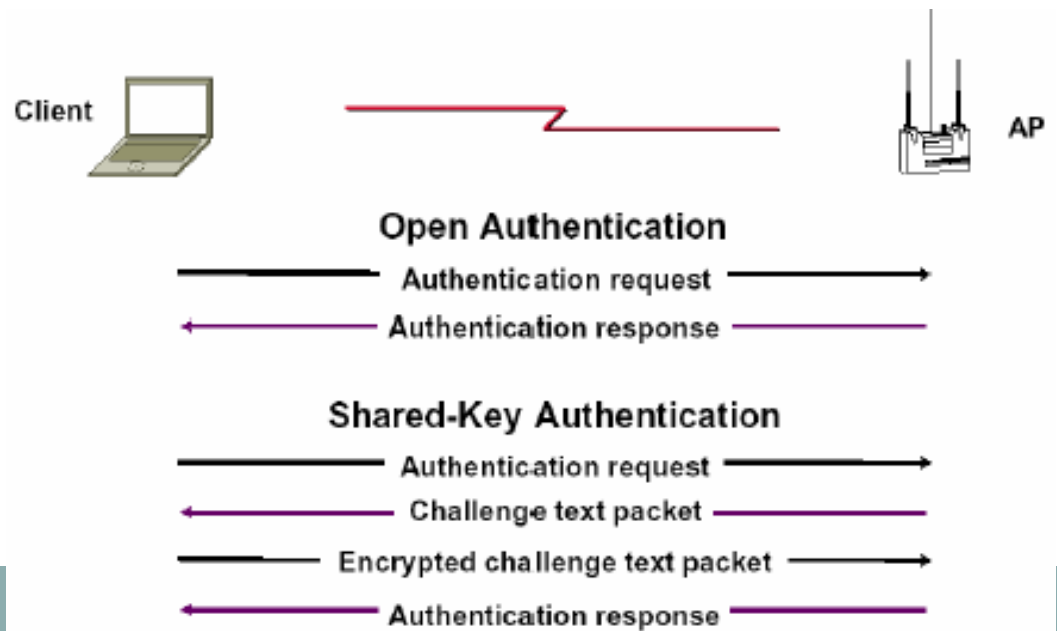
- Spesifikasi 802.11 mempunyai 2 mekanisme untuk otentikasi dari WLAN client:

- ❖ Open Authentication

- Two Way Process

- ❖ Shared Key Authentication

- Four Way Process
 - Diperlukan Security

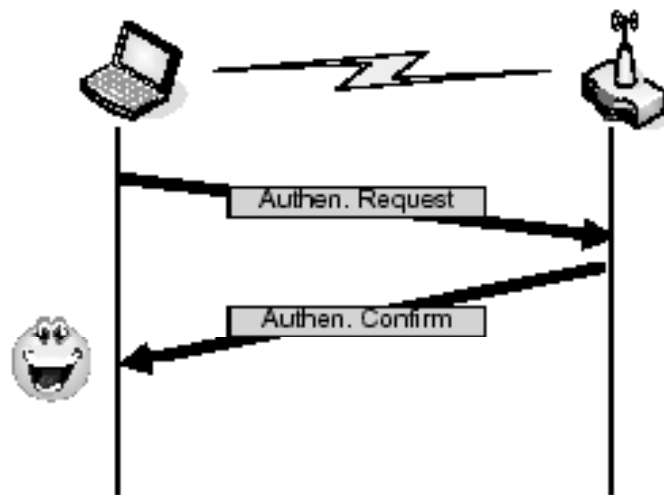


Authentication Mechanism

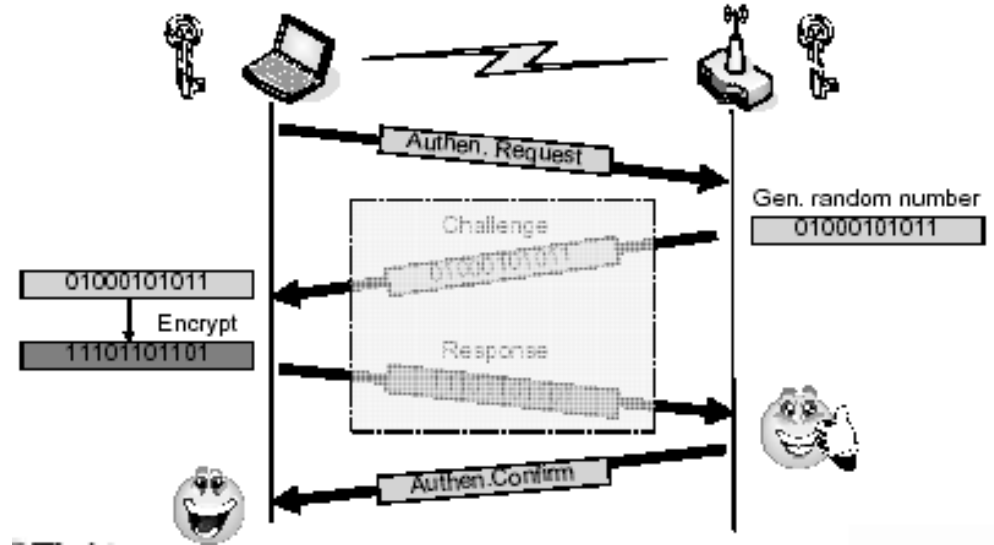
16

WEP Authentication

- Open Authentication – Accept all (no security)

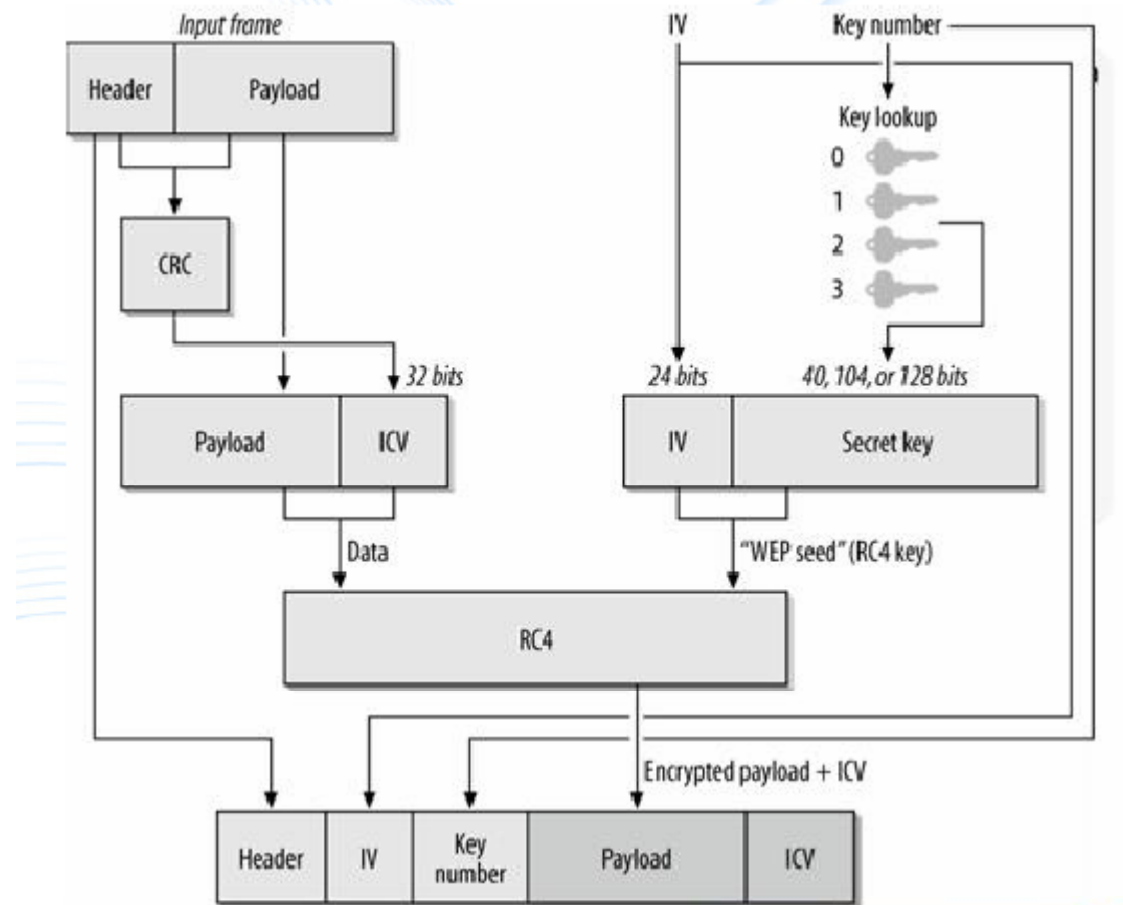


- Shared Key Authentication



WEP Operation

17



WPA (WiFi Protected Access)

18

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

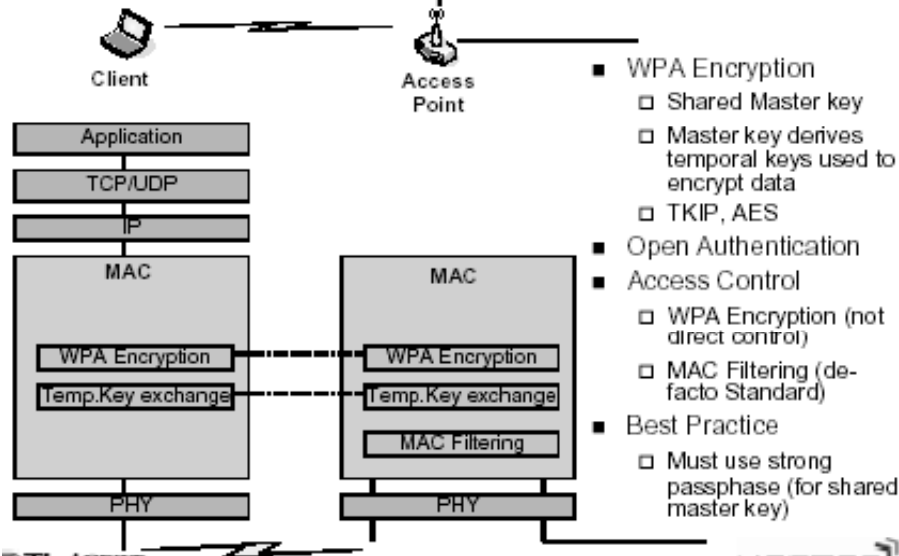
WPA-PSK Mode

19

Wi-Fi Protected Access (WPA)

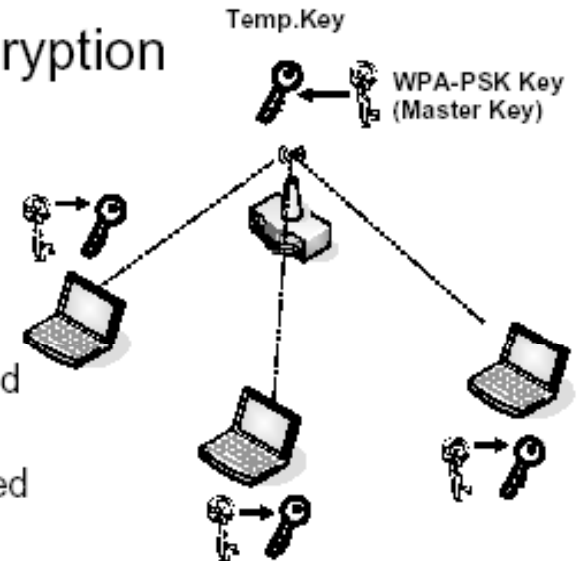
- WPA is included in most of new Wi-Fi card
- WPA is based on standard IEEE 802.11i
- Two modes
 - WPA-PSK (WPA Pre-Shared Key) mode
 - WPA Enterprise Mode

WPA-PSK Concepts



WPA-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

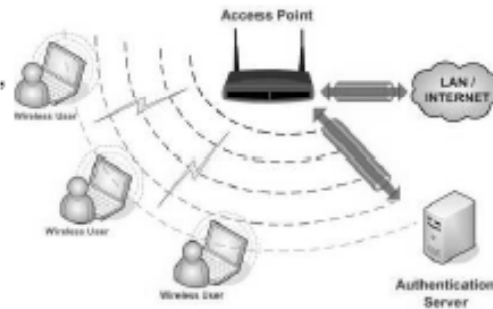


WPA Enterprise / Radius Mode

20

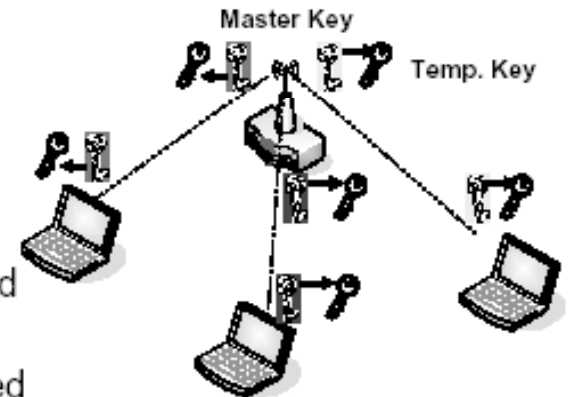
WPA Enterprise Mode

- 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



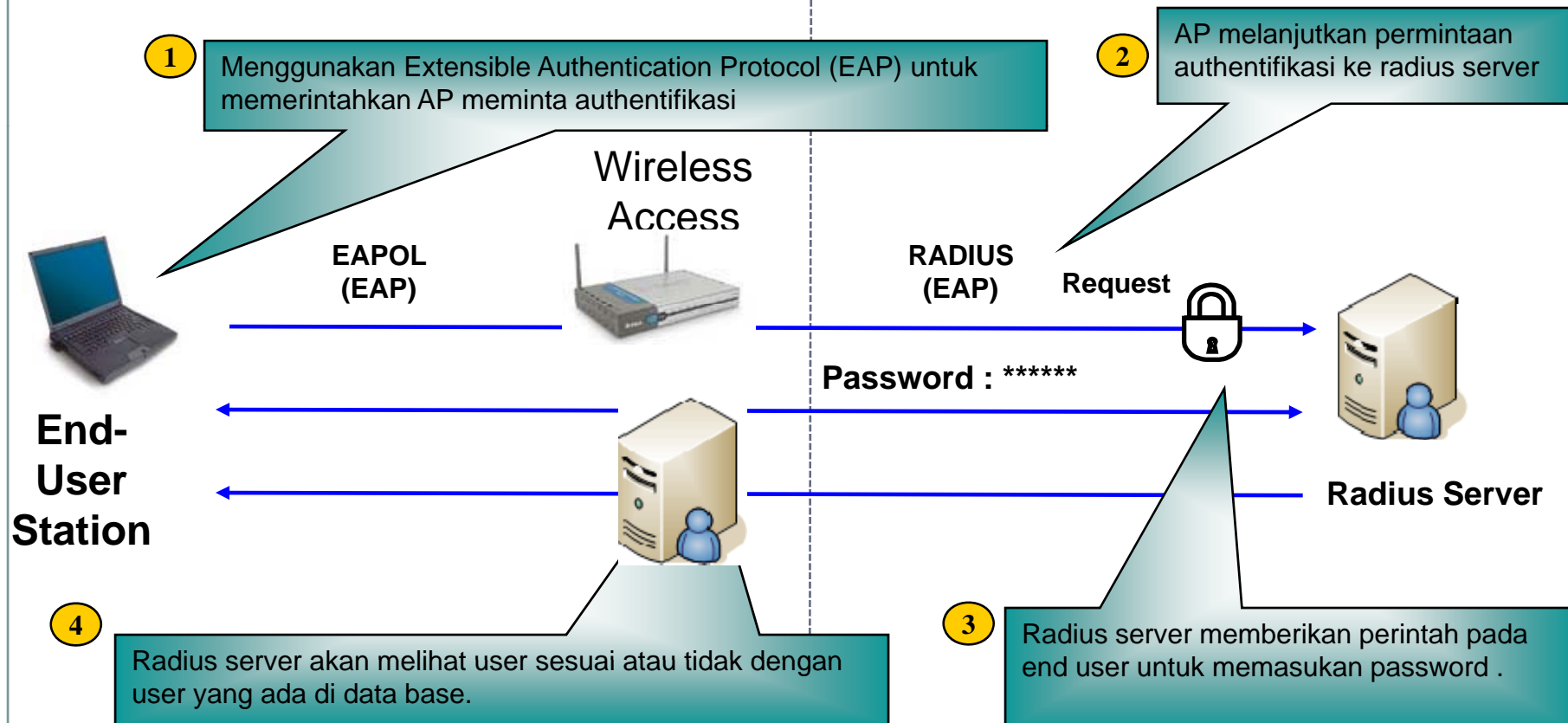
WPA Enterprise Encryption

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



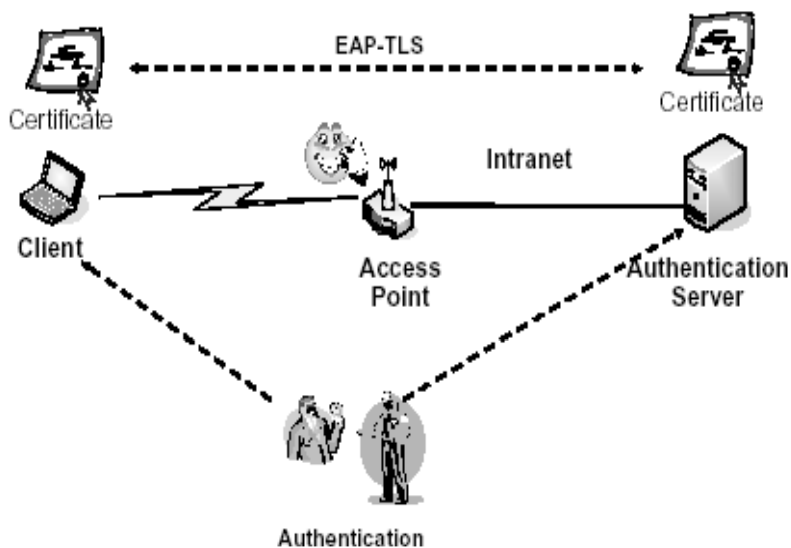
WPA-Enterprise / RADIUS Mode

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



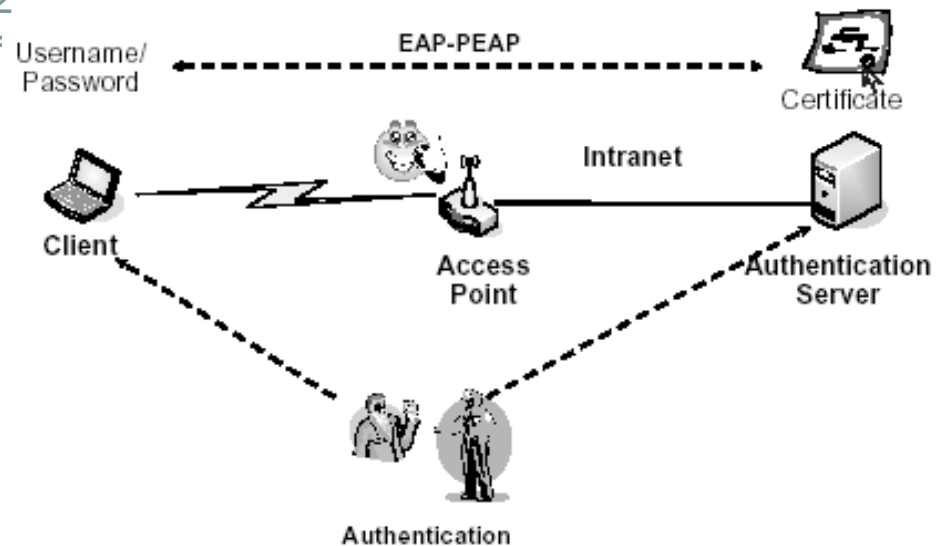
WPA Enterprise / Radius Mode

WPA Enterprise Concept - Authentication

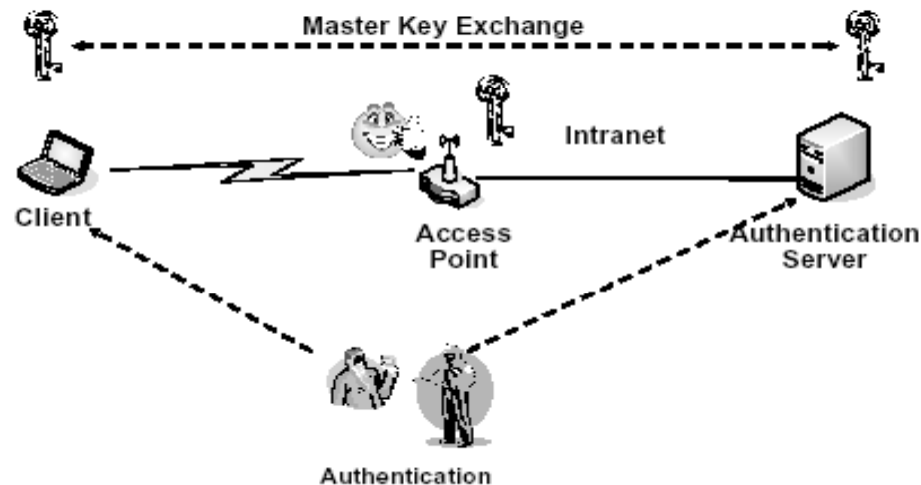


22

WPA Enterprise Concept - Authentication



WPA Enterprise Concept - Authentication



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

24

- *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.



The screenshot shows the D-Link Setup Wizard interface. At the top, the D-Link logo is on the left and the number '25' is on the right. Below the logo, it says 'WELCOME TO THE D-LINK SETUP WIZARD' and 'This wizard will guide you through a step-by-step process to configure your new D-Link router and connect to the Internet.' The main section is titled 'STEP 1: SET YOUR PASSWORD'. It contains a paragraph: 'By default, your new D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below:'. There are two input fields: 'Password : ' followed by a masked field with 10 dots, and 'Verify Password : ' followed by another masked field with 10 dots. At the bottom of these fields are three buttons: 'Prev', 'Next', and 'Cancel'.

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.

26

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.

The screenshot shows the D-Link WRT54GL web interface. The top navigation bar includes links for WIRELESS NETWORK, WIRELESS SECURITY MODE, and WPA-PERSONAL. The left sidebar contains links for INTERNET, WIRELESS SETTINGS, and NETWORK SETTINGS. The main content area is titled 'WIRELESS NETWORK' and contains the following settings:

- Wireless Network Name:** A text input field with the value 'D-Link' and a note '(Also called the SSID)'.
- Wireless Channel:** A dropdown menu set to '1'.
- Enable Auto Channel Scan:** A checkbox that is unchecked.
- Mode Setting:** A dropdown menu set to '11b Mode'.
- Enable Hidden Wireless:** A checkbox that is unchecked, with a note '(Also called the SSID Broadcast)'.

Below these settings is the 'WIRELESS SECURITY MODE' section, which includes a 'Security Mode' dropdown set to 'Disable Wireless Security (not recommended)'. The 'WPA-PERSONAL' section is also visible, showing 'Cipher Type' set to 'TKIP' and 'PSK / EAP' set to 'PSK'.

On the right side of the interface, there is a 'Helpful Hints...' section with links to 'Wireless Settings', 'Wireless Router', and 'SSID'. The 'Wireless Settings' link is highlighted.

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.

The screenshot shows the D-Link WBR-1310 Advanced Network Setup page. The left sidebar contains navigation links: PORT FORWARDING, APPLICATION RULES, NETWORK FILTER, WEBSITE FILTER, FIREWALL SETTINGS, ADVANCED WIRELESS, and ADVANCED NETWORK. The main content area is titled "MAC FILTERING RULES" and includes a description of MAC filtering, "Save Settings" and "Don't Save Settings" buttons, and a section for configuring MAC filtering rules. The "10 - MAC FILTERING RULES" section includes a "Configure MAC Filtering below:" instruction, a "Turn MAC Filtering OFF" dropdown, and a table for adding rules. The table has columns for Schedule, MAC Address, and DHCP Client List. The right sidebar contains "Helpful Hints..." and "MAC Filters:" sections.

D-Link²⁷

WBR-1310

SETUP ADVANCED TOOLS STATUS SUPPORT

MAC FILTERING RULES:

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.

Save Settings Don't Save Settings

10 - MAC FILTERING RULES

Configure MAC Filtering below:

Turn MAC Filtering OFF

Schedule	MAC Address	DHCP Client List	
Always		<< 'computer name'	CLEAR
Always		<< 'computer name'	CLEAR
Always		<< 'computer name'	CLEAR
Always		<< 'computer name'	CLEAR
Always		<< 'computer name'	CLEAR
Always		<< 'computer name'	CLEAR
Always		<< 'computer name'	CLEAR
Always		<< 'computer name'	CLEAR
Always		<< 'computer name'	CLEAR
Always		<< 'computer name'	CLEAR

Helpful Hints...

MAC Filters:

Use MAC Filters to deny computers within the local area network from accessing the Internet. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the unit.

Select "Only allow computers with MAC address listed below to access the network" if you only want selected computers to have network access and all other computers not to have network access.

Select "Only deny computers with MAC address listed below to access the network" if you want all computers to have network access except those computers in the list.

Name: This hostname that is associated with the MAC address configured below.

MAC Address: The MAC address of the network device to be added to the MAC Filter list.

DHCP Client: DHCP clients will have their hostname and MAC address listed here. You can select the client computer you want to add to the MAC Filter list and click Done. This will automatically add that computer's hostname and MAC address to the appropriate fields.

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.

WIRELESS SECURITY MODE :

Security Mode :

WPA-PERSONAL :

WPA-Personal requires stations to use high grade encryption and authentication.

Cipher Type :

PSK / EAP :

802.1X

RADIUS Server 1 : IP

Port

Shared Secret

RADIUS Server 2 : IP

Port

Shared Secret

Step 5. Review wireless Logs.

29

VIEW LOG :				
View Log displays the activities occurring 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.

D-Link 30

WBR-1310 //

SETUP ADVANCED **TOOLS** STATUS SUPPORT

ADMIN
TIME
SYSTEM
FIRMWARE
SYSTEM CHECK

FIRMWARE UPGRADE

There may be new firmware for your WBR-1310 to improve functionality and performance. [Click here to check for an upgrade on our support site.](#)

To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Apply button below to start the firmware upgrade.

CURRENT FIRMWARE INFO.

Current Firmware Version
Firmware Date

Helpful Hints..

Firmware Upgrade
You can upgrade the firmware of the device using this tool. Make sure that the firmware you want to use is saved on the local hard drive of the computer. Click on **Browse** to search the local hard drive for the firmware to be used for the update. Upgrading the firmware will not change any of your system settings but it is recommended that you save your system settings before doing a firmware upgrade. Please check the D-Link support site for

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

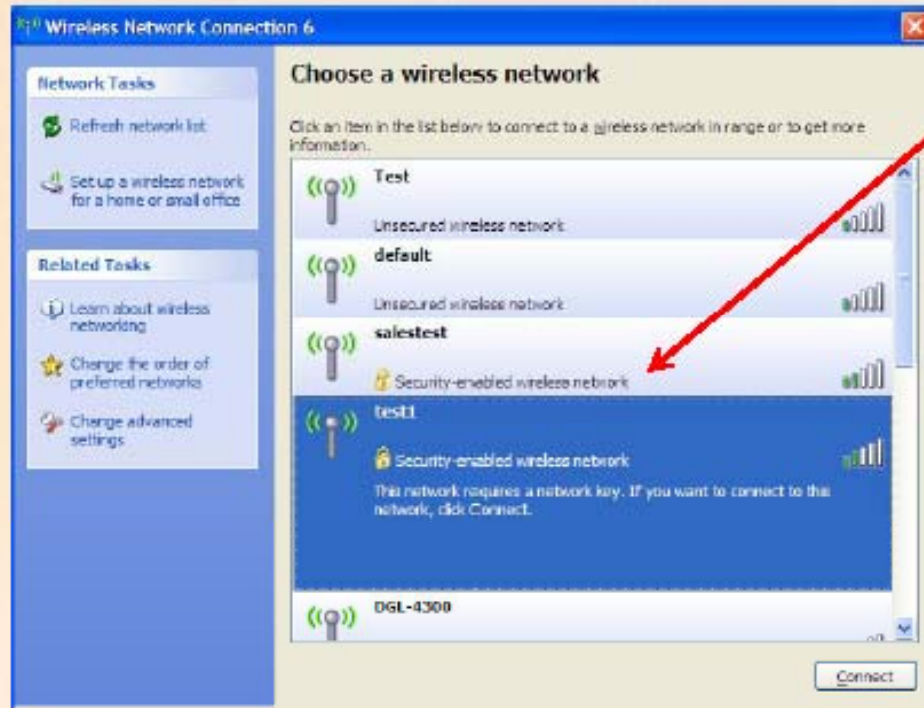
<http://www.microsoft.com/protect/default.mspx>

Mac

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

How can I confirm my setup is secure?

32



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

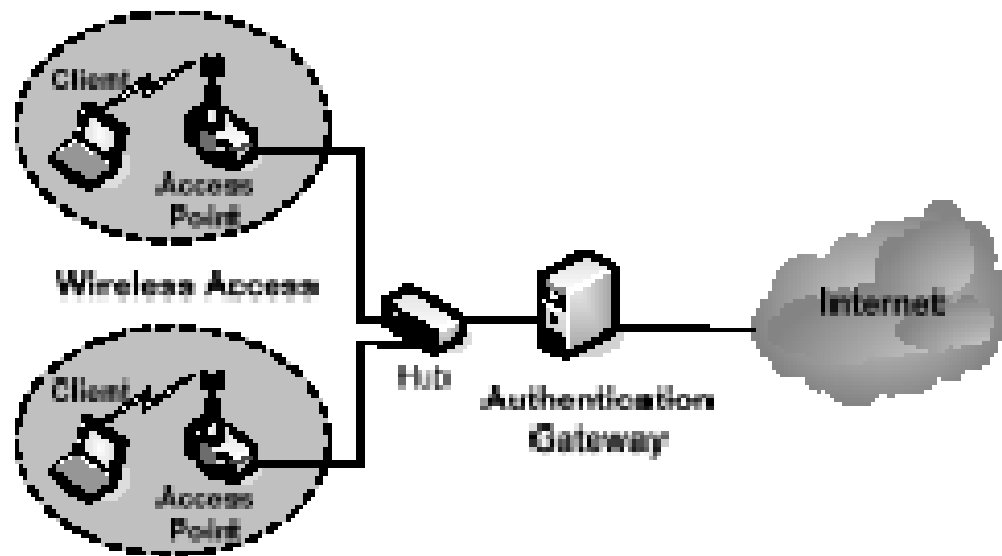
33

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

Authentication Gateway

34

Authentication Gateway

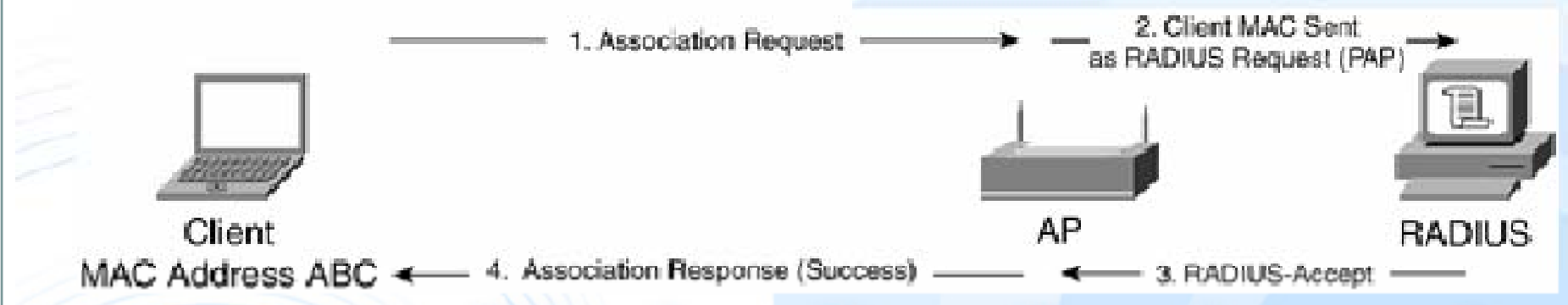


- Commonly used in Wi-Fi hotspot
- User login is required before access the Internet
- User credential is transmitted to the gateway via SSL

MAC Authentication

35

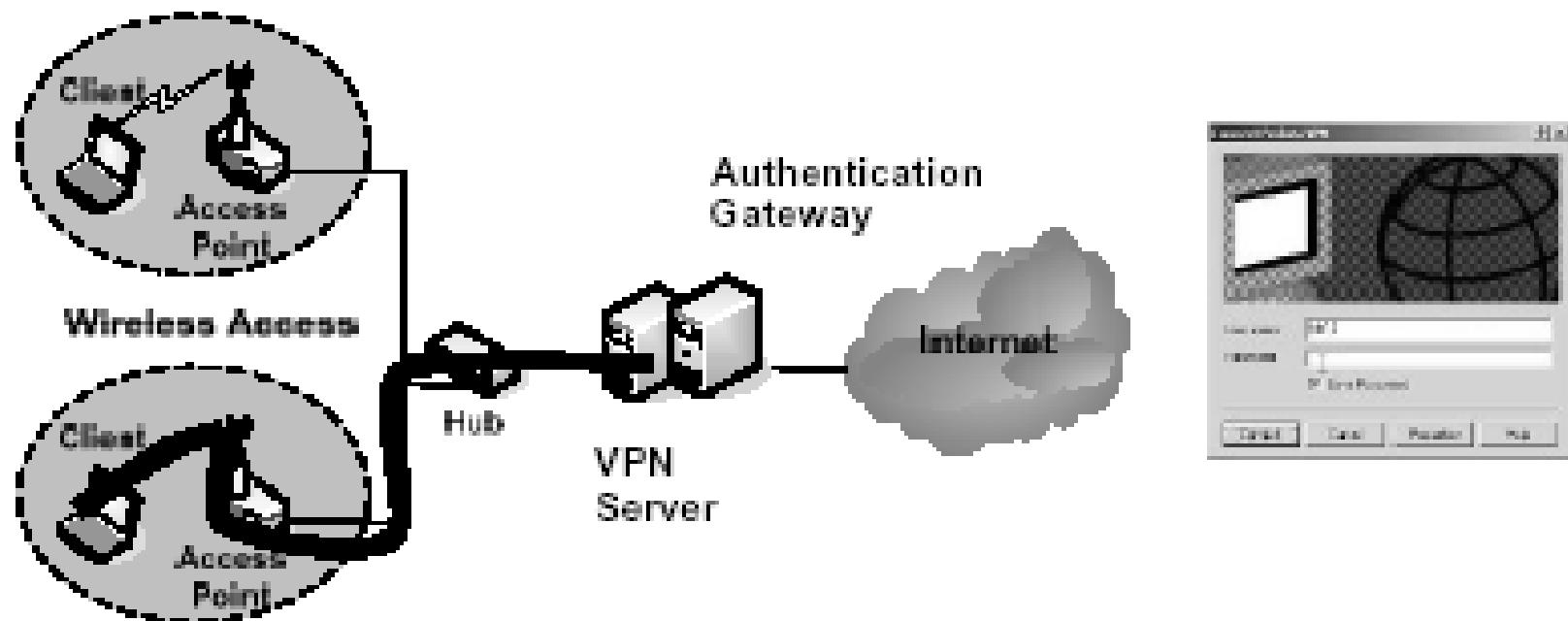
■ MAC Address Authentication



Wireless VPN

36

Wireless VPN



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