



NETGEAR

Everybody's connecting.

LAN

802.11

가 ,

(TCO),

802.11a/b/g

50% WLAN

WEP(Wired Equivalent Privacy)

가

WLAN

가

가

WLAN

WLAN

가 가

가

VPN(Virtual Private Network)

VPN

가

VPN

WLAN

가

NETGEAR WLAN

가

가 가 가

30

WEP

WEP(Wired Equivalent Privacy)

가

가 WEP 가

- :
- : WLAN
- :

가

WEP	802.11b	802.11g	40	128	, 802.11a
152					가

WEP (AP)

WEP

IPSec VPN

IPSec

- DES(Data Encryption Standard): DES 가 DES 56
(8 64)
- 3DES(Triple DES): DES 192
3DES DES

- AES(Advanced Encryption Standard): AES 128, 192 256
 가 . 802.11i AES
 . AES 가 .
 NIST(National Institutes of Standards and Technology) DES
 AES . AES FIPS(Federal Information
 Processing Standard) Publication 197 ,
 2002 5 AES

PKI(Public Key Infrastructure) / (challenge/response) / 가
 CA(Certificate Authority)

SSL(Secure Sockets Layer)

SSL ,
 (negotiate) . IPsec 128 SSL 가 . SSL Ad-Hoc

SSL TCP/IP . SSL
 SSL

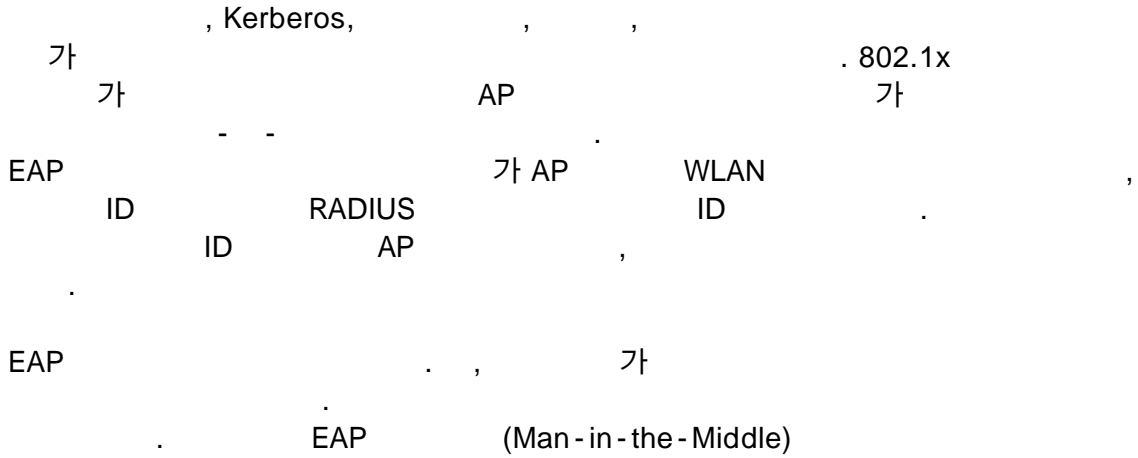
MAC ()
 802.11 가 . MAC ID MAC(Media Access Control)
 . MAC ID . MAC
 MAC

EAP(Extensible Authentication Protocol)

EAP

RADIUS(Remote Authentication Dial-In User Service)

. EAP



802.1x

802.1x PC

. 802.1x

WEP, 3DES, AES

. 802.1x

802.1x

EAP

. 802.1x

. 802.1x

RADIUS

LDAP

. 802.1x

EAP-TLS, LEAP

EAP-TTLS

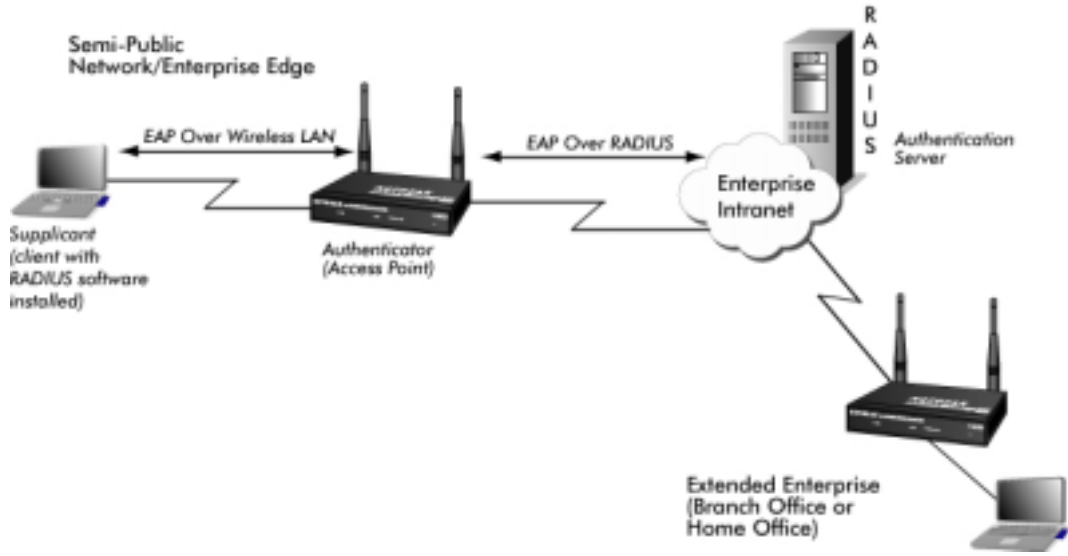
Microsoft

Windows XP

NETGEAR

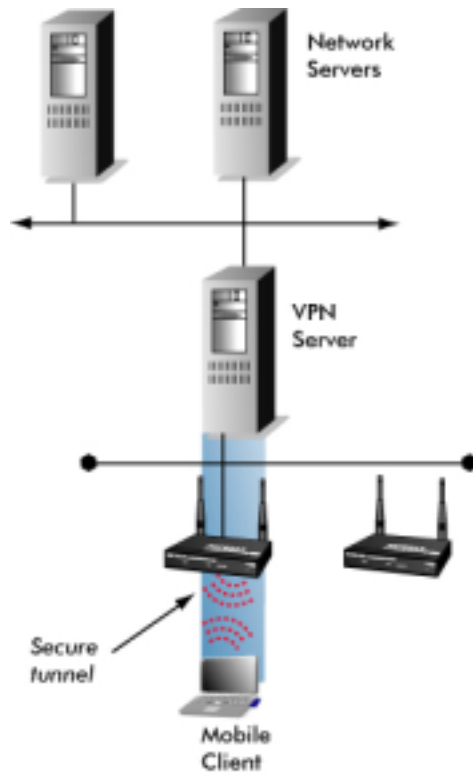
LAN

802.1x



VPN . WLAN 가
 through) . NETGEAR VPN (pass-

가 (VPN)
 VPN WLAN 가 VPN
 . VPN
 . VPN IPSec, L2TP(Layer Two Tunneling Protocol) PPTP(Point-to-Point Tunneling Protocol)
 . VPN WEP 3DES(Triple
 DES) AES
 VPN 가



WLAN

가
WLAN

LAN

WEP

WEP 802.11
WEP

, 1999

WEP

. 802.11

가

WEP

WEP 가
WEP

가

1000

. 500
WEPcrack AirSnort

()

AES : VPN
WEP

WEP

MAC

MAC WEP 가
MAC ID 가
MAC ID
ID MAC

: MAC 802.1x VPN

(Man-in-the-Middle)

가
NIC AP 가
IP , NIC ID
가 (rogue)
가
가
가

" (Man in the Middle)"

: VPN

(Man-in-the-Middle)

(Dictionary)

(challenge) (response)
가
가 /
가
WLAN
:
802.1X VPN (8)

가
(hijacking) 가 . 가
가

LAN

: 802.1X VPN

(DoS)

DoS

가

가

가

: MAC
(stateful)

DoS

AP

LAN

WLAN

WPA(Wi-Fi Protected Access)

WPA Wi-Fi Alliance

802.11i

WEP

WPA

TKIP

WEP

WPA IEEE 802.1x

Wi-Fi Alliance 2003

Wi-Fi

TKIP(Temporal Key Encryption Protocol)

TKIP WEP

(,)
가

WPA

가 . TKIP

TKIP

128

. TKIP

MAC

16

가

. TKIP 10,000

(MIC)

. TKIP

CRC

가

. WEP
TKIP

WEP

TKIP

가

AES

가

, 가 , 가 , 가

가 SOHO-
가 SOHO

가 IT 가

1

- : NIC
- WEP : WEP
- SSID 가
- SSID 가 : Windows XP SSID
802.11 . SSID SSID
- MAC : AP MAC
- AP 가 SOHO 가 20
가
- LAN : WLAN
- WPA LAN
WPA
- : NIC
- WEP : 가 WEP
가

. IT

- VPN: 가 IPsec VPN . VPN
- WPA
- : AP
- PGP
- (가가)
- 가
- 가
- / WLAN -
- (rogue) . WLAN
- 가
- (rogue) . MAC
- : 802.11 802.11 가 NIC ReefEdge, Bluesocket Nomadix RADIUS
- : RADIUS LDAP WLAN
- . EAP . 802.1x (RADIUS)
- : 가
- . 가 AP AP 가

- : IT 가 가 DMZ . WLAN VPN LAN MAC IP DHCP LAN DHCP SSID . DHCP IP IP 192.168.0.1

가
가 Microsoft Windows

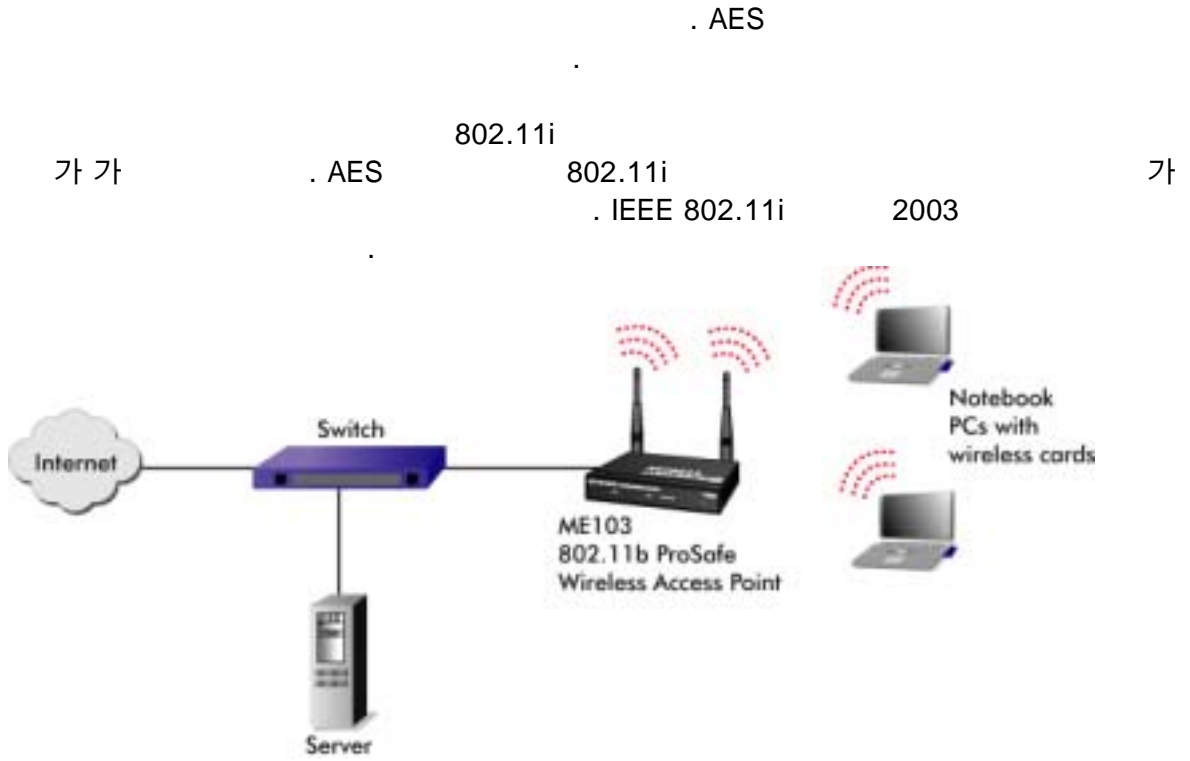
WLAN VPN

Wi-Fi 가

AP
Layer 2

WLAN WLAN . 802.11i 가

RSN(Robust Security Network) IEEE 802.11i . RSN 가 TKIP AES 가 WEK . TKIP



WLAN

WLAN
NETGEAR

:

IT

,

LAN

IT

가

가

(:

,

CRC(Cyclic Redundancy Check)

/

(CA)

(

)

가

X.509

(

)

가

가

(stateful)

. WLAN

Kerberos

IT

가 Kerberos

. Kerberos

Kerberos KDC(Key Distribution Center)

가

KDC

IKE(Internet Key Exchange)

VPN

. IKE IPsec

. IKE
가

IPsec

IPsec IP

. IPsec

IPsec

IP

. IPsec

가

가

IPsec IP
VPN

LEAP

Cisco 802.1x

MAC(Media Access Control)

01:23:45:67:89:ab

48

MAC

. MAC

MAC

PEAP(Protected Extensible Authentication Protocol)

PEAP EAP

TLS(Transport Level Security)

. PEAP

EAP

가

. PEAP 802.11

VPN

. PEAP TTLS

PKI(Public Key Infrastructure)

VPN 가 , PKI 가
ID , .

RADIUS(Remote Authentication Dial-In User Service)

RADIUS 가 , RADIUS 가
RADIUS 가
가
가

SSID(Service Set Identifier)

LAN ID , BSS
(BSS) ,
SSID

TLS(Transport Layer Security)

Netscape SSL(Secure Socket Layer) IETF . TLS
가
TLS

- 가 .
- 가
- (negotiate)
-

TTLS(Tunneled Transport Layer Security)

Funk Software Certicom , . TTLS
EAP-TTLS