

보안 기술 적용을 통한 국내 무선랜 활용 사례

Free & Safe Networking

(주)에프네트 / 영업부

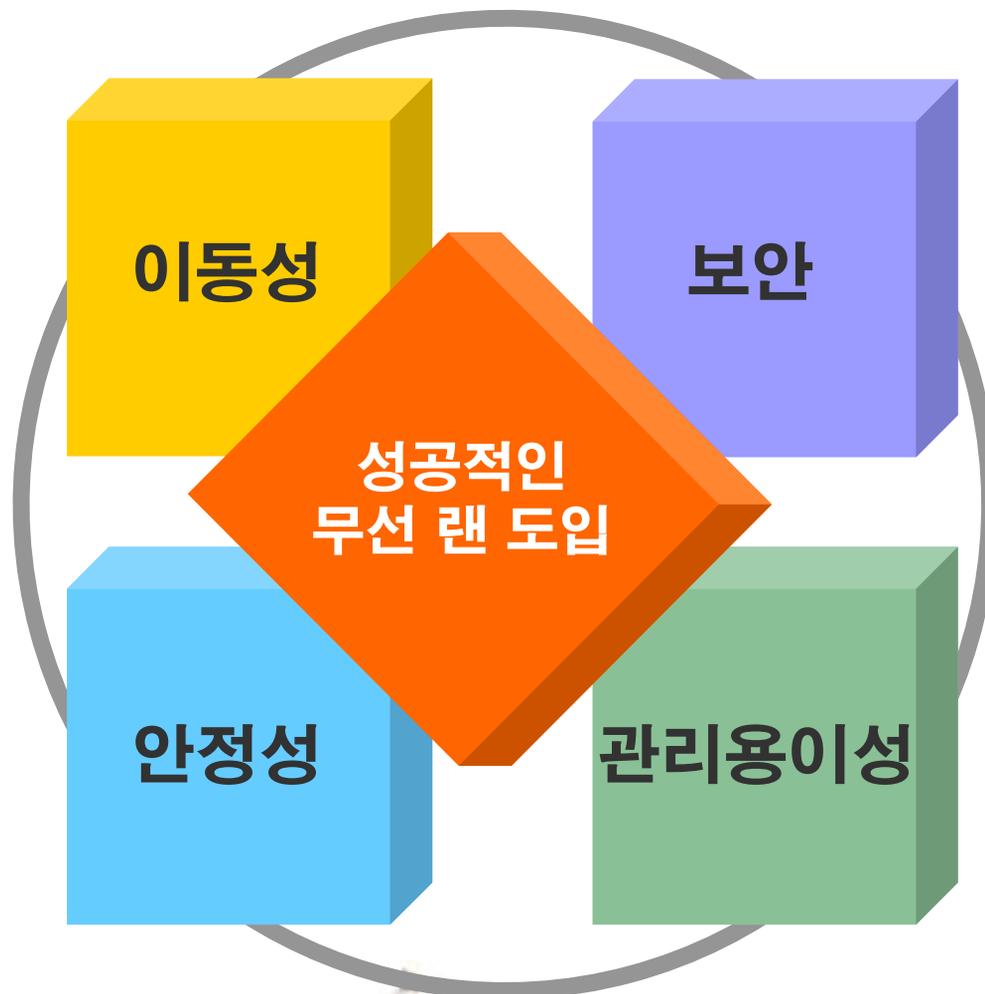
전 창은 이사

cejeon@f-net.co.kr

☎ 02-2167-2860

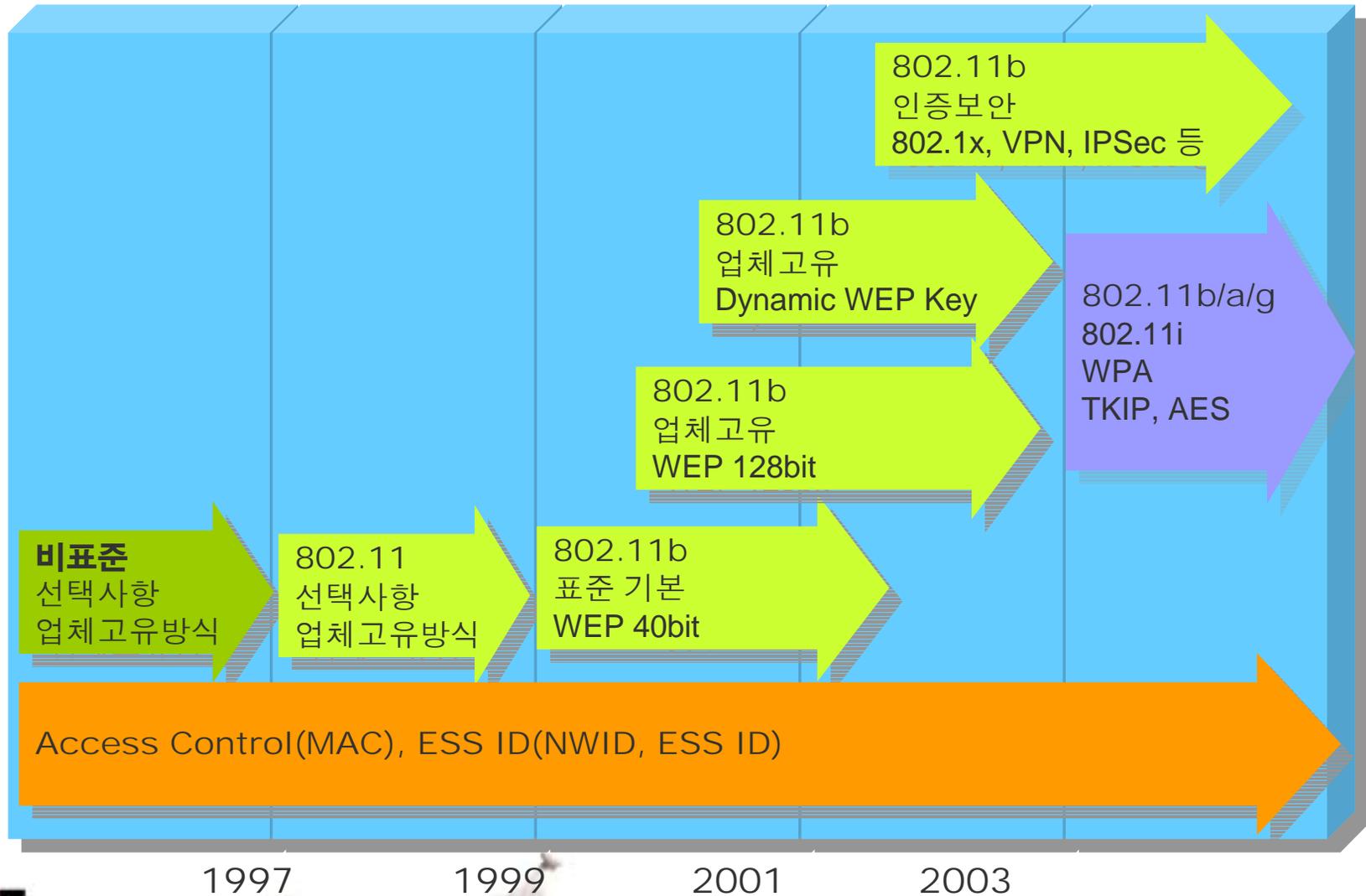
1. 개요
2. ESS ID / Closed System
3. Access Control
4. WEP
5. 인증/보안 솔루션
6. 기타 보안 적용 사례
7. 요약

무선 랜 도입 시 고려 요소



1. 개요

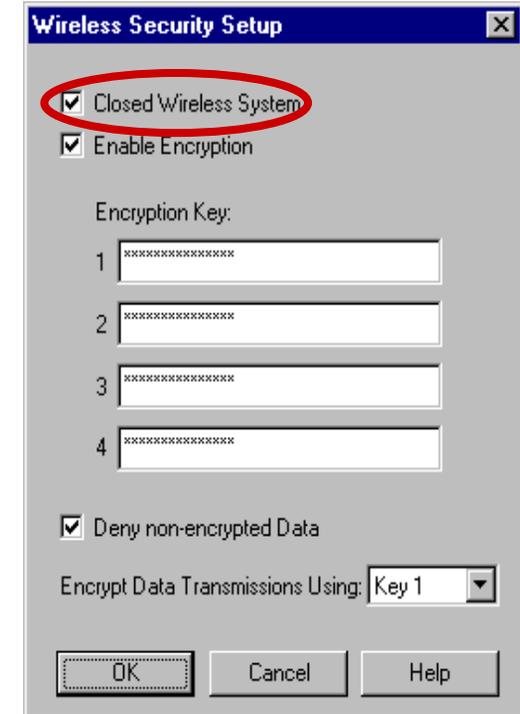
무선 랜 보안 흐름



2. ESS ID / Closed System

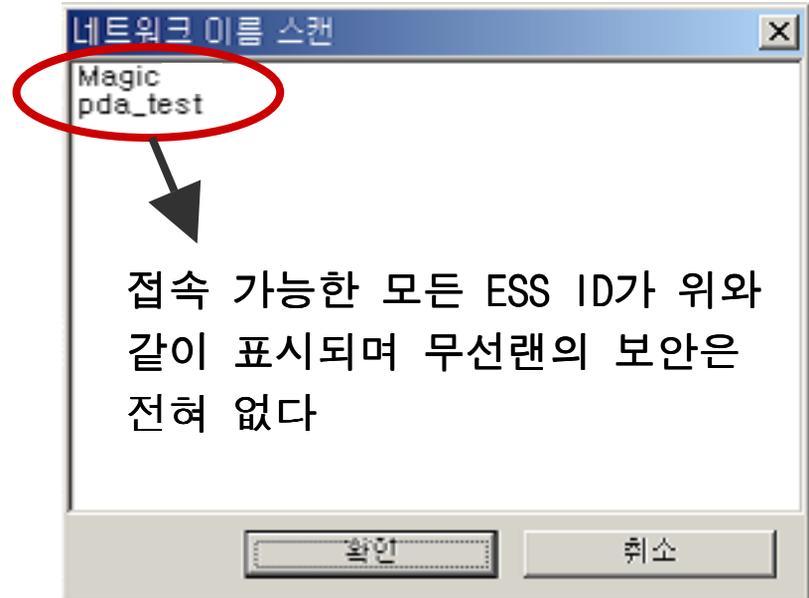
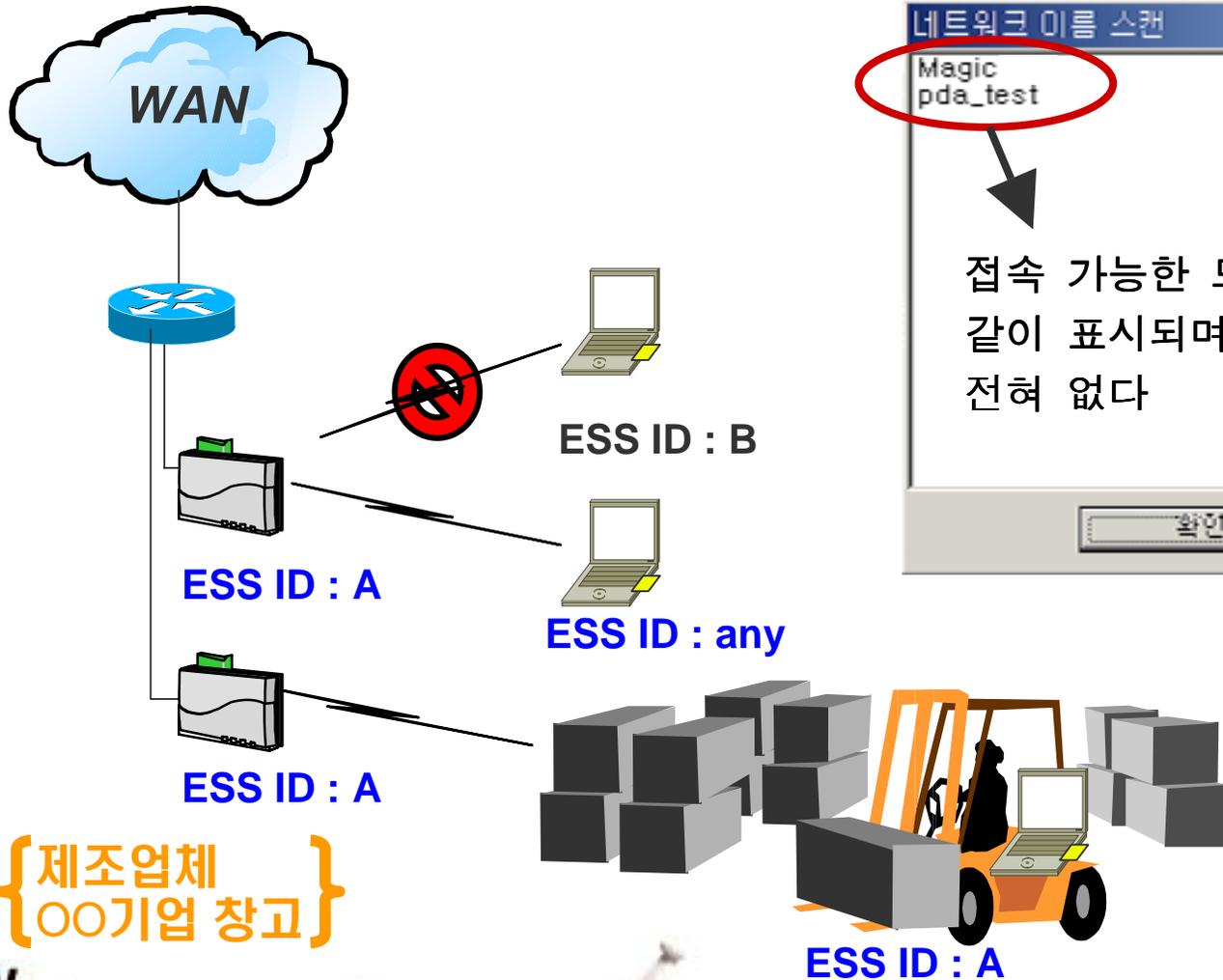
개요

- ◆ ESS ID
 - AP와 Client는 ESS ID가 일치해야 통신 가능
 - 비인가 사용자의 네트워크 사용 방지
 - ESS ID는 통상적이지 않은 문자 사용 권장
- ◆ “ANY”
 - Client가 간편하게 무선 랜에 접속하도록 고안된 표준
 - Default값
 - 특별한 설정이 없다면 Client는 AP의 ESS ID와 상관없이 모든 AP에 접속가능
- ◆ Closed System(비 표준)
 - AP는 정확한 ESS ID를 갖는 Client만 허용
 - “ANY”(broadcast ESS ID)는 거부



2. ESS ID / Closed System

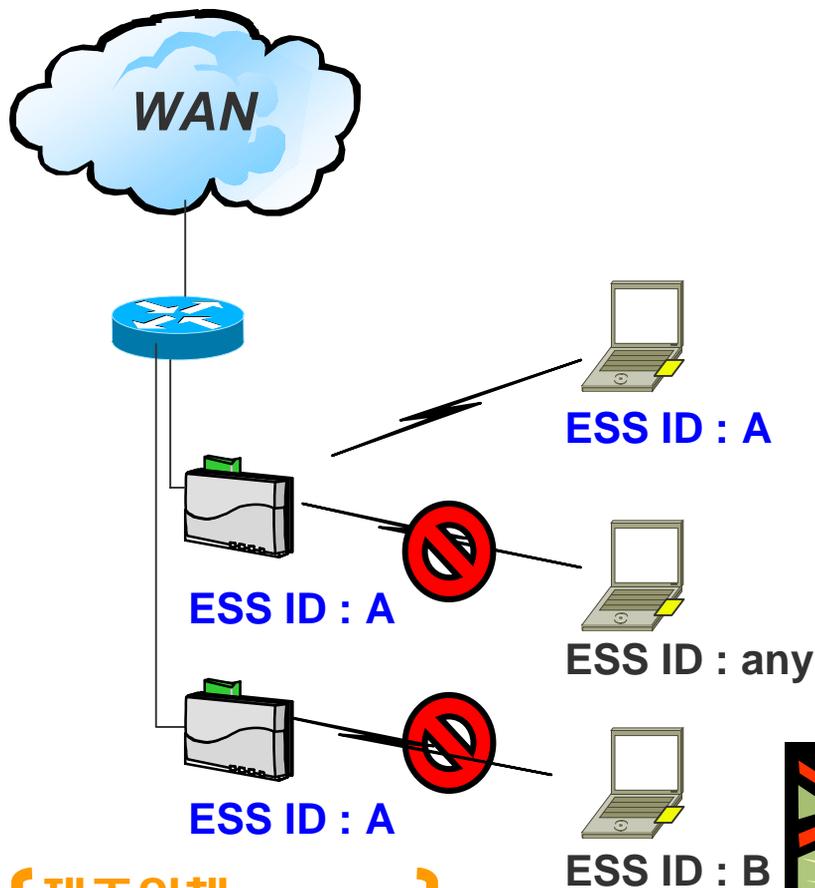
Closed System 미적용 사례



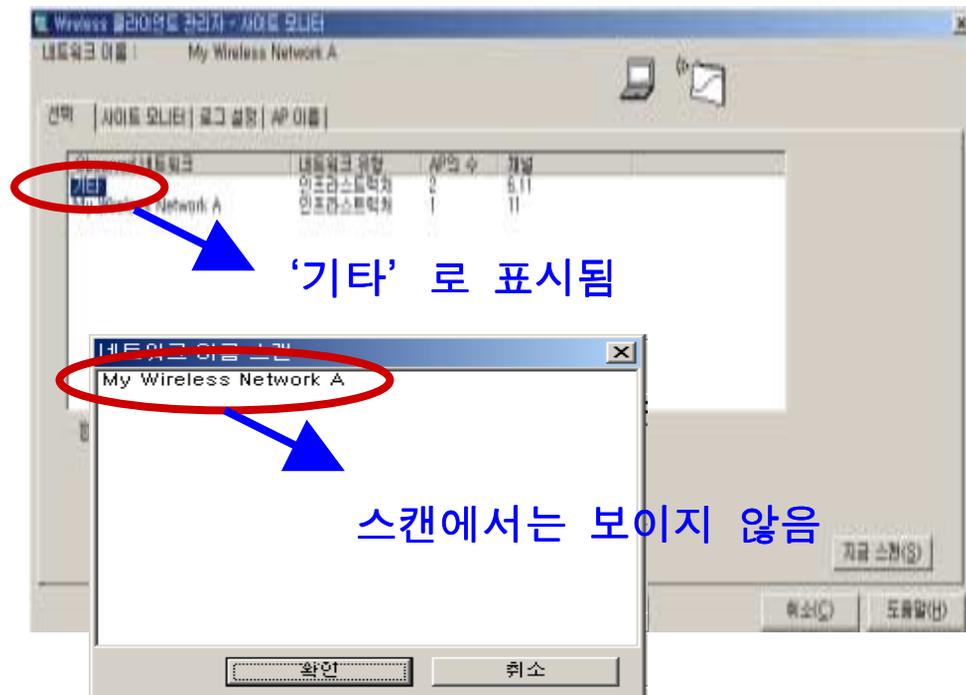
* 상기 설정화면은 물론 이후의 설정화면도 특정 기업과 상관없는 데이터입니다.

2. ESS ID / Closed System

Closed System 적용 사례



{ 제조업체
OO철강 생산공장 }



RF 주파수 및 AP 설치 여부는 표시되나 ESS ID는 보이지 않는다

2. ESS ID / Closed System

Closed System 적용 여부에 따른 Beacon값 변화

Sniff1: Decode, 8/127 802.11 LANs Frames

No.	Source Address	Dest Address	Summary
4	Agere 2C81AF	Broadcast	802.11: 2.0 Mbps, Signal= 22%, Beacon
5	Agere 42497D	Broadcast	802.11: 2.0 Mbps, Signal= 65%, Beacon
6	Agere 2C81AF	Broadcast	802.11: 2.0 Mbps, Signal= 23%, Beacon
7	Agere 42497D	Broadcast	802.11: 2.0 Mbps, Signal= 64%, Beacon

DLC: ...0 ... = No privacy
DLC: ...0... = Short Preamble option is not allowed
DLC: ...0... = Packet Binary Convolutional Coding Mo
DLC: 0... = Channel agility is not in use
DLC: Capability information field #2 = 00
DLC: 0000 0000 = Reserved
DLC: Element ID = 0 (Service Set Identifier)
DLC: ...Length = 21 octet(s)
DLC: ...Service Set Identity = "My Wireless Network A"
DLC: Element ID = 1 (Supported Rates)

Close system 미적용

Expert / Decode / Matrix / Host Table / Protocol Dist. / Statistics /

No.	Source Address	Dest Address	Summary	Len
5	Broadcast	802.11: 2.0 Mbps, Signal= 65%	Beacon	82
6	Broadcast	802.11: 2.0 Mbps, Signal= 23%	Beacon	61
7	Broadcast	802.11: 2.0 Mbps, Signal= 64%	Beacon	82

DLC: 0000 0000 = Reserved
DLC: Element ID = 1 (Supported Rates)
DLC: ...Length = 1 octet(s)
DLC: ...Service Set Identity = ""
DLC: Element ID = 1 (Supported Rates)
DLC: ...Length = 4 octet(s)
DLC: ...Supported Rates information field = 82
DLC: 1... = Basic Service Set Basic Rate
DLC: ...0000 0010 = 1.0 Megabits per second
DLC: ...Supported Rates information field = 84

Close system 적용

2. ESS ID / Closed System

ESS ID / Closed System 요약

인증/보안 Solution

WEP 암호화

MAC Address 인증

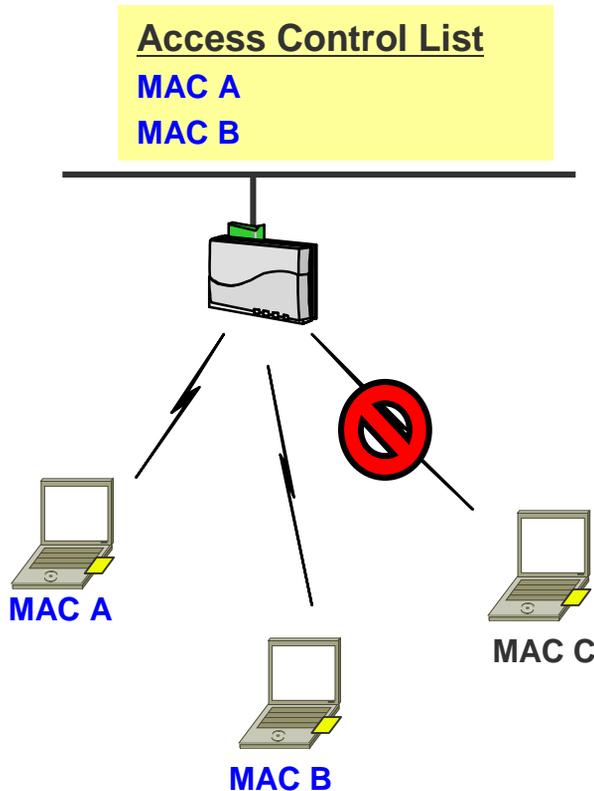
Closed System

ESS ID

- 로밍을 위하여 전사 동일 ESSID 사용
- ESS ID를 전사적으로 관리 필요
- Wireless Sniffing Tool로 데이터 해킹 가능

- ANY로도 접근 가능
- 타 AP를 스캔하여 ESS ID 확인 가능

적용 사례



- ◆ AP 가 인증된 Station의 List 보유
 - MAC Address 사용
 - AP configuration 을 통하여 List를 관리
- ◆ 리스트에 없는 Station은 AP에서 Data Frame 을 Filtering
- ◆ 관리자가 모든 무선 스테이션에 대한 MAC Address를 등록 관리
- ◆ 로밍이 허용된 사용자를 위하여 그들의 이동 경로의 AP들에게 MAC Address를 등록
- ◆ 같은 네트워크에 있는 모든 AP들은 같은 List를 보유해야 하므로 관리 부담이 크다.

{ 금융권 } * WEP도 함께 적용
OO은행

3. Access control

Access Control이 허가된 사용자

The screenshot shows the Wireshark interface with the following details:

- Packet List:** A table with columns No., Status, Source Address, Dest Address, and Summary. A red circle highlights rows 1 through 9.
- Packet Bytes:** A pane showing the raw data of the selected packet, with a red oval highlighting the first few bytes. The data is garbled, indicating WEP encryption.
- DLC Header:** A pane showing details of the Data Link Control (DLC) header, including signal level, noise level, channel, data rate, and frame encryption status.

No.	Status	Source Address	Dest Address	Summary
1	M [11]	Agere 30DE14	Compaq6B4C70	802.11: 11.0 Mbps, Signal= 69%, Data, WEP, Retry
2	[11]	Agere 42497D	Agere 30DE14	802.11: 2.0 Mbps, Signal= 63%, Acknowledgment (A
3	[11]	Agere 30DE14	Compaq6B4C70	802.11: 11.0 Mbps, Signal= 69%, Data, WEP
4	[11]	Agere 42497D	Agere 30DE14	802.11: 2.0 Mbps, Signal= 65%, Acknowledgment (A
5	[11]	Agere 30DE14	Compaq6B4C70	802.11: 11.0 Mbps, Signal= 68%, Data, WEP
6	[11]	Agere 42497D	Agere 30DE14	802.11: 2.0 Mbps, Signal= 64%, Acknowledgment (A
7	[11]	Agere 30DE14	Compaq6B4C70	802.11: 11.0 Mbps, Signal= 68%, Data, WEP
8	[11]	Compaq6B4C70	Agere 30DE14	802.11: 11.0 Mbps, Signal= 65%, Data, WEP
9	[11]	Agere 30DE14	Agere 42497D	802.11: 2.0 Mbps, Signal= 68%, Acknowledgment (A

DLC: ----- DLC Header -----

- DLC:
- DLC: Frame 1 arrived at 20:37:15.0010; frame size is 532 (0214 hex) bytes.
- DLC: Signal level = 69 %
- DLC: Noise level = 6 %
- DLC: Channel = 11
- DLC: Data rate = 22 (11.0 Megabits per second)
- DLC: Frame Originally Encrypted with WEP key 1
- DLC:

00000000: 08 4d c6 05 00 02 2d 42 49 7d 00 02 2d 30 de 14 M? .-BI} .-0?
00000010: 00 02 a5 6b 4c 70 c0 db 65 86 7e 00 56 47 1f b6 ..Lp작e?.VG.
00000020: ae 28 7d bb 93 4d 50 35 0a 38 ee 87 c2 30 75 97 ?}괄MP5.8??u
00000030: 57 ed f3 ac aa 27 67 09 4d 40 02 05 af 70 b4 ce W?U'g.M@..윗닐
00000040: 2f d5 32 b0 f3 ad f6 55 60 56 a3 8d 67 dc 62 72 /?값?U`V윗g?r
00000050: da 99 9c a5 4e f5 6d 3b 0d 7b f2 34 11 11 3a e2 2?N2: f2

WEP KEY 사용으로 인하여 데이터 정보는 보이지 않지만 현재 정상적으로 송수신 중인 것을 확인 할 수 있다

3. Access control

Access Control이 허가되지 않은 사용자

The screenshot shows a Wireshark interface with a packet list and a packet details pane. The packet list shows several frames from source Lucent319419 to destination 0180C2000000, all with a summary of 'Expert: Same Transmitter And Receiver Address'. The fifth frame, from source Agere 42497D to Broadcast, has a summary of 'Expert: ACK Frame Timeout'. The packet details pane shows the structure of the fifth frame: DLC, LLC (with DSAP and SSAP addresses), and BPDU (Bridge Protocol Data Unit Header).

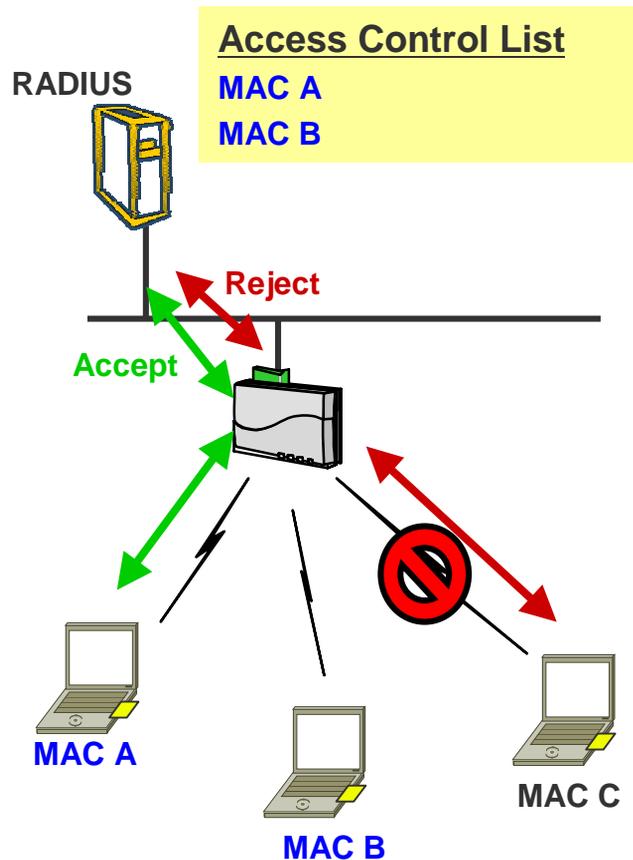
No.	Source Address	Dest Address	Summary	Len
1	Lucent319419	0180C2000000	Expert: Same Transmitter And Receiver Address BPDU: S: Pri=8000 Port=8003 Root: Pri=8000 Addr=00601D3194	6
2	Lucent319419	0180C2000000	Expert: Same Transmitter And Receiver Address BPDU: S: Pri=8000 Port=8003 Root: Pri=8000 Addr=00601D3194	6
3	Lucent319419	0180C2000000	Expert: Same Transmitter And Receiver Address BPDU: S: Pri=8000 Port=8003 Root: Pri=8000 Addr=00601D3194	6
4	Lucent319419	0180C2000000	Expert: Same Transmitter And Receiver Address BPDU: S: Pri=8000 Port=8003 Root: Pri=8000 Addr=00601D3194	6
5	Agere 42497D	Broadcast	Expert: ACK Frame Timeout 802.11: 2.0 Mbps, Signal= 63%, Beacon	6
6	Agere 2C81AF	Broadcast	802.11: 2.0 Mbps, Signal= 23%, Beacon	8
7	Agere 42497D	Broadcast	802.11: 2.0 Mbps, Signal= 63%, Beacon	6
8	Agere 2C81AF	Broadcast	802.11: 2.0 Mbps, Signal= 21%, Beacon	8

Detailed view of frame 5:

- DLC: -----
- LLC: ----- LLC Header -----
 - LLC: DSAP Address = 42, DSAP IG Bit = 00 (Individual Address)
 - LLC: SSAP Address = 42, SSAP CR Bit = 00 (Command)
 - LLC: Unnumbered frame: UI
- BPDU: ----- Bridge Protocol Data Unit Header -----
- BPDU: -----

AP에 MAC이 등록 되지 않은 사용자는 AP에서 접속을 거부한다

사내 RADIUS를 이용한 통합관리



- ◆ Station의 MAC Address 를 RADIUS Server로 부터 인증을 받음.
 - User Name = MAC Address
 - User Password = shared secret
 - 중앙 관리
 - 동적 관리
 - List의 개수 제한은 없음
- ◆ 리스트에 없는 Station은 AP에서 Data Frame 을 필터링 한다.

{ 제조업체 }
OO 전자 * WEP도 함께 적용

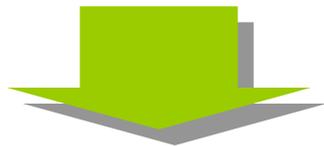
Access Control의 발전 형태

사내 RADIUS 를 이용한 통합 관리



MAC Address 중앙 관리

MAC Address를 통한 인증



Client Software 사용 접속

User ID / Password를 통한 인증



암호화(Dynamic Key Distribution)

802.1x 방향으로 발전

Access Control 요약

인증/보안 Solution

WEP 암호화

MAC Address 인증

Closed System

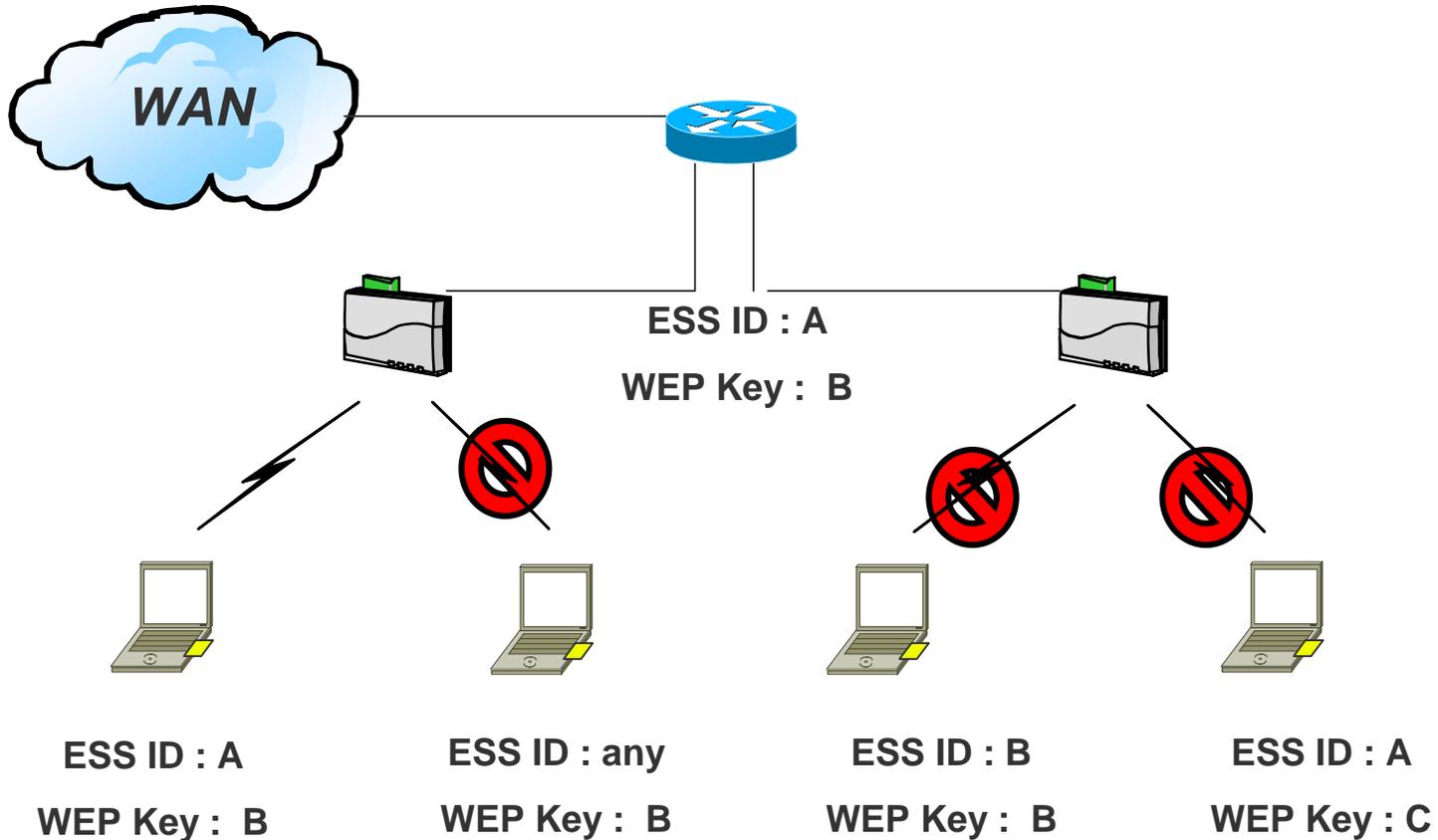
ESS ID

- 
- 암호화 없으면 MAC Address는 평문 전송
 - 간단한 Sniffing Tool로도 확인 가능

개요

- ◆ Wired Equivalent Privacy
- ◆ RC4 알고리즘
- ◆ Mobile 사용자와 AP간에 공유되는 비밀키
- ◆ 64bit WEP
 - 표준
 - 40-bit secret key + 24-bits Initialization Vector (IV)
- ◆ 128bit WEP
 - 비표준 – 제조업체 간 호환 불가능
- ◆ Link Layer Security Protocol

WEP Key와 Closed System 동시 적용



{통신
OO기업 사무실} * 사무실은 주로 WEP 사용

WEP 미 적용 시

The image shows a Wireshark capture of network traffic. The main pane displays a list of packets. Packet 8 is highlighted with a red circle. The packet details pane shows the following structure:

- TCP: Checksum = B33F (correct)
- TCP: Urgent pointer = 0
- TCP: No TCP options
- TCP: [1460 Bytes of data]
- NETB: ----- NetBIOS Session protocol -----
- NETB: [1460 more bytes of user data]

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII column contains garbled characters, likely representing the user data being transmitted.

사용자 IP Address 및 data 전송 상태를 볼 수 있다

WEP 적용 시

The screenshot shows a network sniffer window titled "Sniff2: Decode, 1/17169 802.11 LANs Frames". It displays a list of frames with columns for No., Status, Source Address, Dest Address, and Summary. The frames show communication between Agere and Compaq6B4C70. The summary for frame 1 indicates it is a WEP retry. Below the list, the "DLC" (Data Link Control) details are expanded, showing frame arrival time, signal level (69%), noise level (6%), channel (11), data rate (11.0 Megabits per second), and that the frame was originally encrypted with WEP key 1. At the bottom, a hex dump shows the raw data of the frame, with some characters appearing as garbled text.

No.	Status	Source Address	Dest Address	Summary
1	M [11]	Agere 30DE14	Compaq6B4C70	802.11: 11.0 Mbps, Signal= 69%, Data, WEP, Retry
2	[11]	Agere 42497D	Agere 30DE14	802.11: 2.0 Mbps, Signal= 63%, Acknowledgment (A
3	[11]	Agere 30DE14	Compaq6B4C70	802.11: 11.0 Mbps, Signal= 69%, Data, WEP
4	[11]	Agere 42497D	Agere 30DE14	802.11: 2.0 Mbps, Signal= 65%, Acknowledgment (A
5	[11]	Agere 30DE14	Compaq6B4C70	802.11: 11.0 Mbps, Signal= 68%, Data, WEP
6	[11]	Agere 42497D	Agere 30DE14	802.11: 2.0 Mbps, Signal= 64%, Acknowledgment (A
7	[11]	Agere 30DE14	Compaq6B4C70	802.11: 11.0 Mbps, Signal= 68%, Data, WEP
8	[11]	Compaq6B4C70	Agere 30DE14	802.11: 11.0 Mbps, Signal= 65%, Data, WEP
9	[11]	Agere 30DE14	Agere 42497D	802.11: 2.0 Mbps, Signal= 68%, Acknowledgment (A

DLC: ----- DLC Header -----

- DLC:
- DLC: Frame 1 arrived at 20:37:15.0010; frame size is 532 (0214 hex) bytes.
- DLC: Signal level = 69 %
- DLC: Noise level = 6 %
- DLC: Channel = 11
- DLC: Data rate = 22 (11.0 Megabits per second)
- DLC: Frame Originally Encrypted with WEP key 1
- DLC:

```
00000000: 08 4d c6 05 00 02 2d 42 49 7d 00 02 2d 30 de 14 .M?..-BI}..-0?
00000010: 00 02 a5 6b 4c 70 c0 db 65 86 7e 00 56 47 1f b6 ..Lp작e?VG.
00000020: ae 28 7d bb 93 4d 50 35 0a 38 ee 87 c2 30 75 97 ?}MP5.8??u
00000030: 57 ed f3 ac aa 27 67 09 4d 40 02 05 af 70 b4 ce W'g.M@..헛닐
00000040: 2f d5 32 b0 f3 ad f6 55 60 56 a3 8d 67 dc 62 72 /?U`V헛g?r
00000050: da 99 9c ae 4e fe 6d 3b 0d 7b f2 34 11 11 3a e2 2N?..s?
```

사용중인 MAC 정보 와 KEY 정보만 표시된다

데이터 전송 시 WEP 정보

Sniff3: Decode, 13/6195 802.11 LANs Frames

No.	Status	Source Address	Dest Address	Summary
8	[11]	Agere 42497D	Agere 30DE14	802.11: 2.0 Mbps, Signal= 61%, Acknowledgment (A
9	[11]	Compaq6B4C70	Agere 30DE14	802.11: 11.0 Mbps, Signal= 61%, Data, WEP
10	[11]	Agere 30DE14	Agere 42497D	802.11: 2.0 Mbps, Signal= 68%, Acknowledgment (A
11	[11]	Agere 30DE14	Compaq6B4C70	802.11: 11.0 Mbps, Signal= 68%, Data, WEP
12	[11]	Agere 42497D	Agere 30DE14	802.11: 2.0 Mbps, Signal= 60%, Acknowledgment (A
13	[11]	Compaq6B4C70	Agere 30DE14	802.11: 11.0 Mbps, Signal= 60%, Data, WEP
14	[11]	Agere 30DE14	Agere 42497D	802.11: 2.0 Mbps, Signal= 69%, Acknowledgment (A
15	[11]	Agere 30DE14	Compaq6B4C70	802.11: 11.0 Mbps, Signal= 69%, Data, WEP
16	[11]	Agere 42497D	Agere 30DE14	802.11: 2.0 Mbps, Signal= 61%, Acknowledgment (A
17	[11]	Compaq6B4C70	Agere 30DE14	802.11: 11.0 Mbps, Signal= 61%, Data, WEP
18	[11]	Agere 30DE14	Agere 42497D	802.11: 2.0 Mbps, Signal= 69%, Acknowledgment (A
19	[11]	Agere 30DE14	Compaq6B4C70	802.11: 11.0 Mbps, Signal= 68%, Data, WEP
20	[11]	Agere 42497D	Agere 30DE14	802.11: 2.0 Mbps, Si
21	[11]	Agere 42497D	Broadcast	802.11: 2.0 Mbps, Si

Packet 13 Details:

- DLC: WEP (Wired Equivalent Privacy) Header
 - ... Initialization Vector #(1-3) = 8FE553
 - ... Initialization Vector #4 = 00
 - ... [93 byte(s) of encrypted MSDU]
 - ... Encrypted Integrity Check Value = 9DFDE7CA

Packet 15 Details:

- DLC: WEP (Wired Equivalent Privacy) Header
 - ... Initialization Vector #(1-3) = 90E553
 - ... Initialization Vector #4 = 00
 - ... [87 byte(s) of encrypted MSDU]
 - ... Encrypted Integrity Check Value = CD24DEB9

- 전송 중인 **Data**가 암호화 되어 **IV** 정보만 확인
- **IV** 값은 **Data** 전송 시 계속 변하지만,
- 이 정보들을 모아서 분석하면 **WEP Key**가 해독될 수 있다.

WEP의 취약점

무결성
(Integrity)

- WEP Algorithm 상의 문제점
 - Static WEP Key 사용

무결성 / 기밀성
보장 못함

기밀성
(Confidentiality)

- RC4 알고리즘 상의 문제점
 - RC4 Stream Cipher 알고리즘에서 의 Key Scheduling에서의 취약점

WEP의 발전 형태

웹기반 프록시를 통한 인증



WEP 암호화



동적 키분배방식 암호화 개발
- WPA
- 802.11i(TKIP, AES)

802.1x를 통한 인증



Access Point 추가 기능 없음

Access Point에 기능 추가

WEP 요약

인증/보안 Solution

WEP 암호화

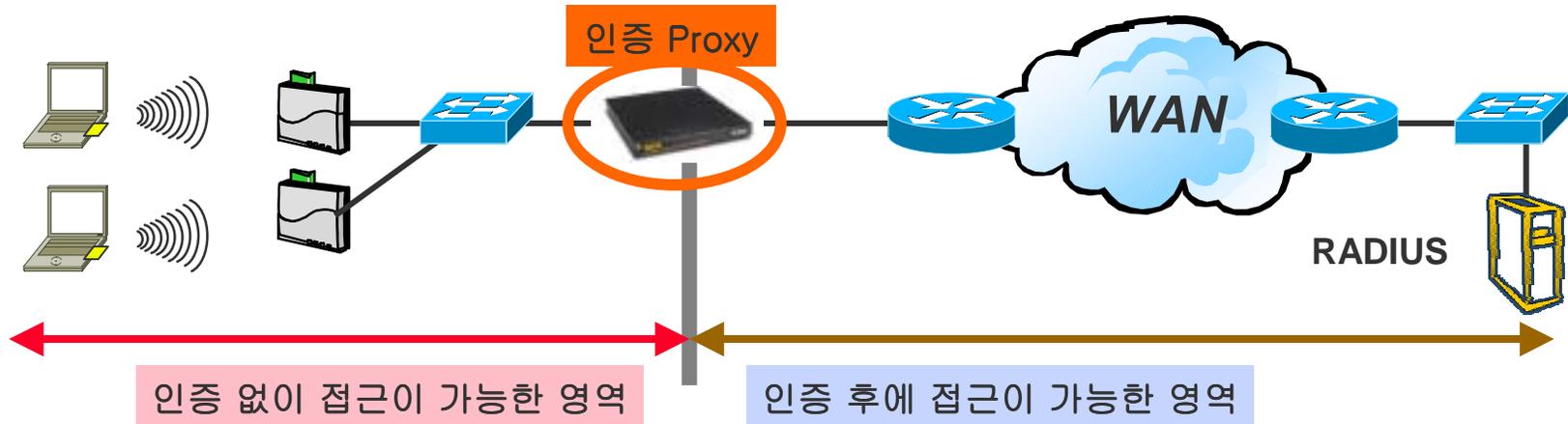
MAC Address 인증

Closed System

ESS ID

- RC4 알고리즘 상의 문제 발생
- **Static Key** 사용으로 인한 취약 요소 발견
- 새로운 알고리즘 개발 과제
- 인증/보안 솔루션도 대안

인증 프록시 (웹기반 인증)



- ◆ Web Browser를 통한 인증
- ◆ OS 및 TCP/IP 환경에 관계없이 인증 가능
- ◆ 다양한 부가기능 : Mobile IP 또는 Web Redirection, 802.1x 지원

{ 관광
OO호텔 }

인증 프록시 (웹기반 인증) 요약

Client 요구사항

- 무선 랜 카드 Driver 설치 필요
- 인증을 위한 별도의 Program 설치 불필요 : Web browse SSL 이용

AP 요구사항

- 802.11b 표준 지원
- SSID 및 WEP 설정 등 인증을 위한 설정 불필요 (별도의 인증서버로부터 인증 절차 수행)

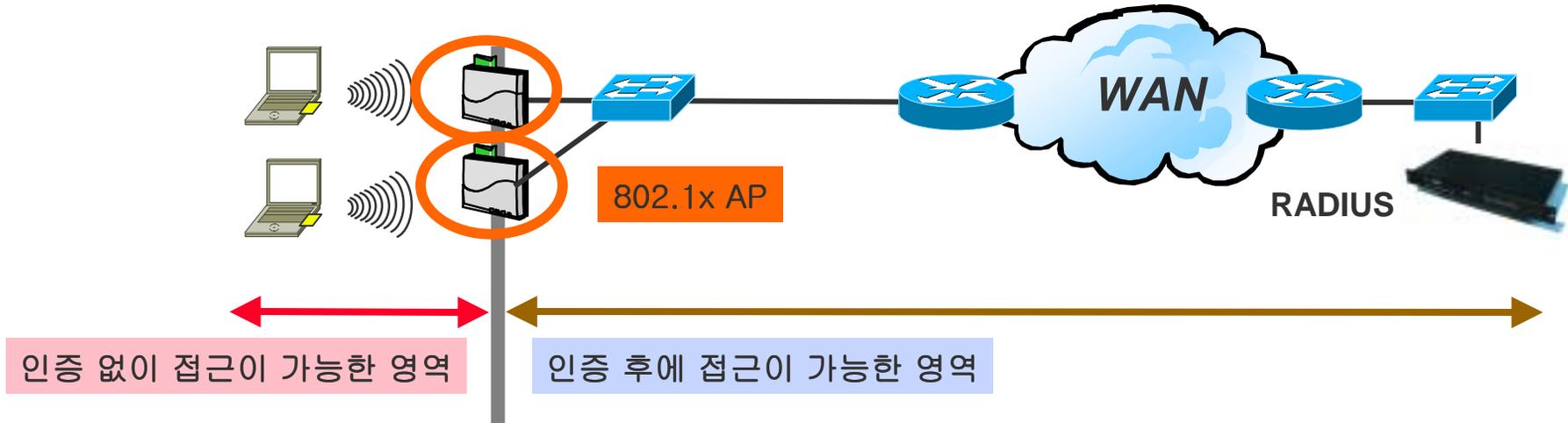
부가 장비

- 인증 Proxy 서버 → Client Traffic을 자동 감지하여 인증 절차를 시도
- 인증 Master 서버 (RADIUS Server)
→ 인증 Proxy 서버의 요청에 따라, Client 인증을 수행
- Portal 서버
→ 인증절차를 시도하는 Client의 초기 WEB 화면을 전송
→ Web Redirection page에 광고 문안 삽입 등 부가가치 창출 가능

특징

- WEB을 통한 현장 등록 가능
- WEB, DNS, Email Redirection 가능,
- USG는 사용자별 대역폭 조정이 실시간으로 가능
- 인증이 필요한 개별 지역에 추가 장비 설치 필요
- 인증 시, MAC 또는 IP에 의존 단말기를 구분하므로, 인증기반은 취약

802.1x 기반 인증



- ◆ 802.1x 지원 Client module, AP, RADIUS로 구성
- ◆ 적용 방안별 보안 수준 상이 : EAP-MD5, TLS, TTLS...

{통신
외국계기업 사무실}

802.1x 기반 인증 요약

Client 요구사항

- 무선랜카드 Driver 설치 필요
- 802.1x 지원 필요 (Windows XP 기본, 기타 OS 추가 Patch 필요)

AP 요구사항

- 802.1x 지원 필요
- SSID 및 WEP 설정 등 인증을 위한 설정 옵션

부가 장비

- 802.1x 지원 인증 서버 (RADIUS Server)
- 802.1x를 지원하는 AP의 인증 요청에 따라, Client 인증을 수행

특징

- 각 Client가 인증을 위하여 802.1x Client 프로그램이 인스톨 되어야 함.
- 현장 등록 불가능
- EAP-TLS, EAP-TTLS는 Dynamic WEP 지원

인증/보안 솔루션 요약

인증/보안 Solution

WEP 암호화

MAC Address 인증

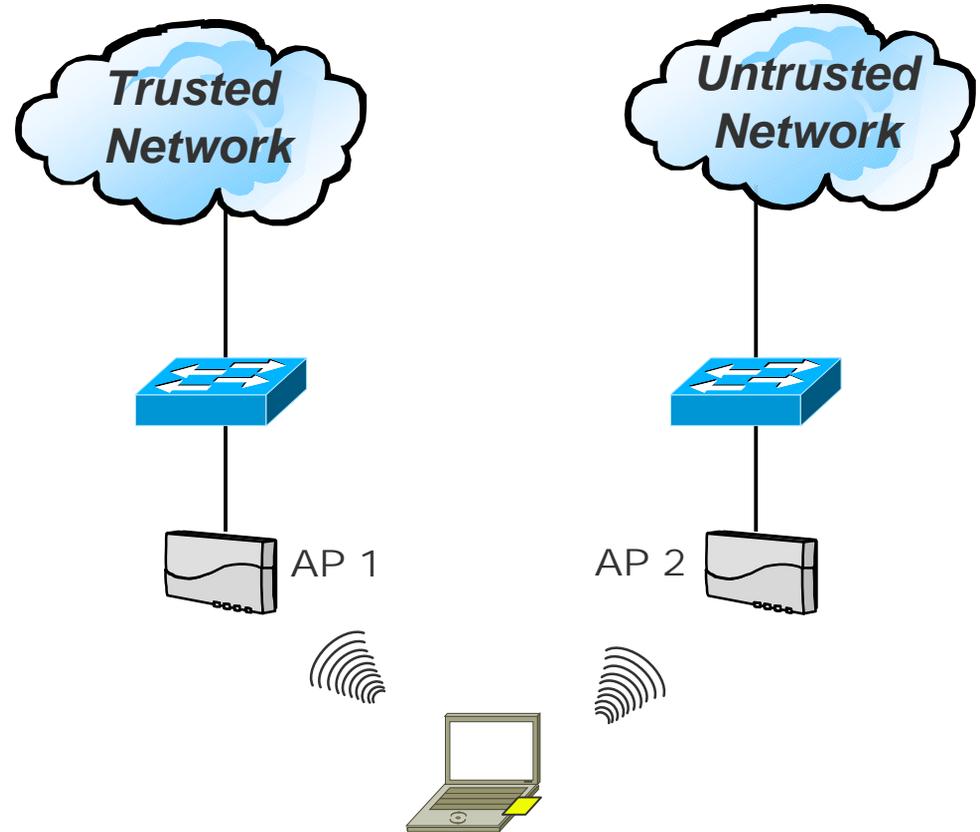
Closed System

ESS ID

- 관리, 보안 상의 장점
- 보안을 위한 비용 과다 발생

분리된 망에서의 무선 적용

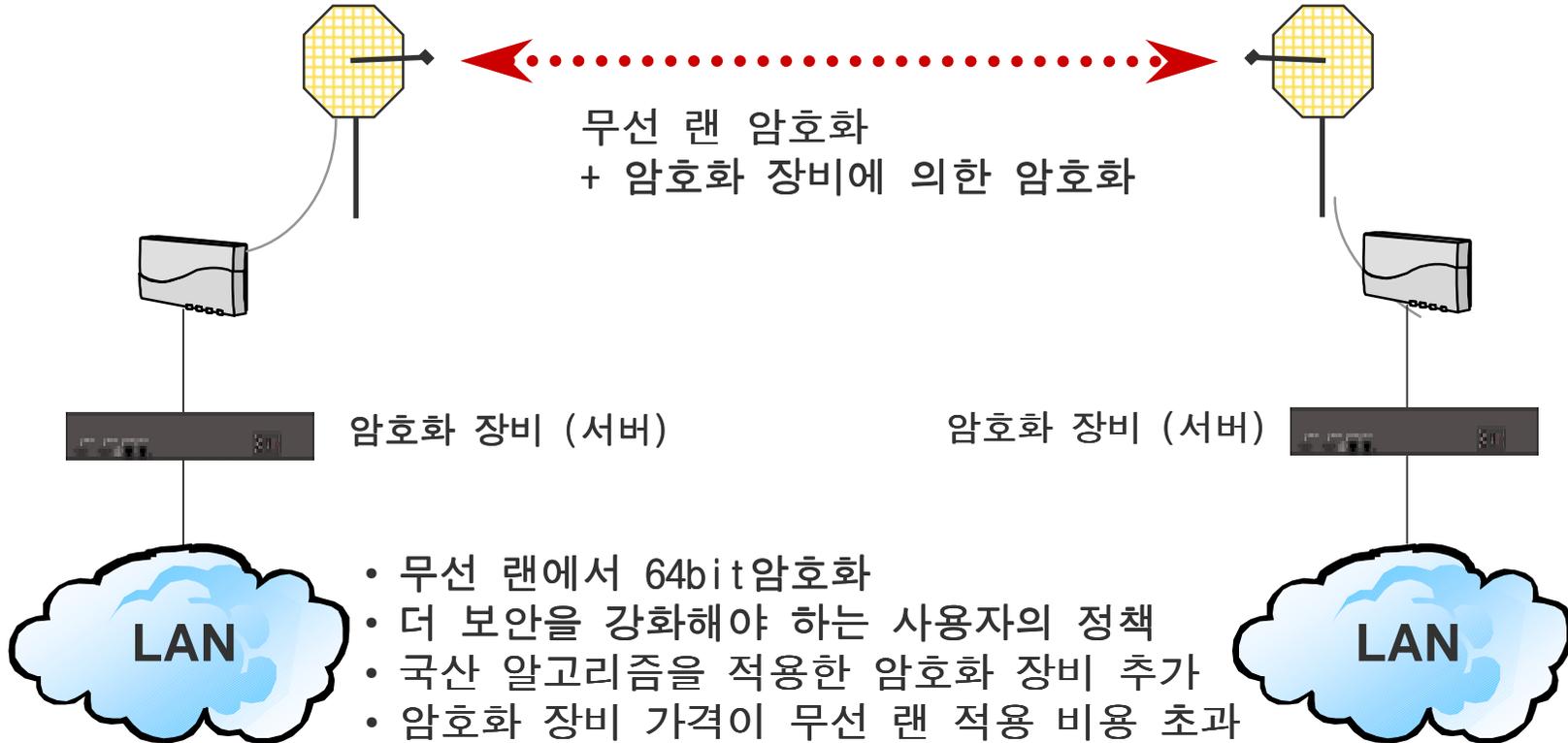
- ◆ 정책에 따라 안전한 네트워크와 안전하지 않은 네트워크를 물리적으로 분리
- ◆ 사용자 PC에서는 필요에 따라 AP 1 또는 AP 2를 선택하고 소프트웨어적으로 네트워크를 전환
- ◆ 사용자는 두 개의 네트워크를 이용할 수 있지만 안전하지 않은 네트워크에서 안전한 네트워크로 접근은 불가



{ 정부기관
OO부 교육장 }

XX 공공기관 - 교육장

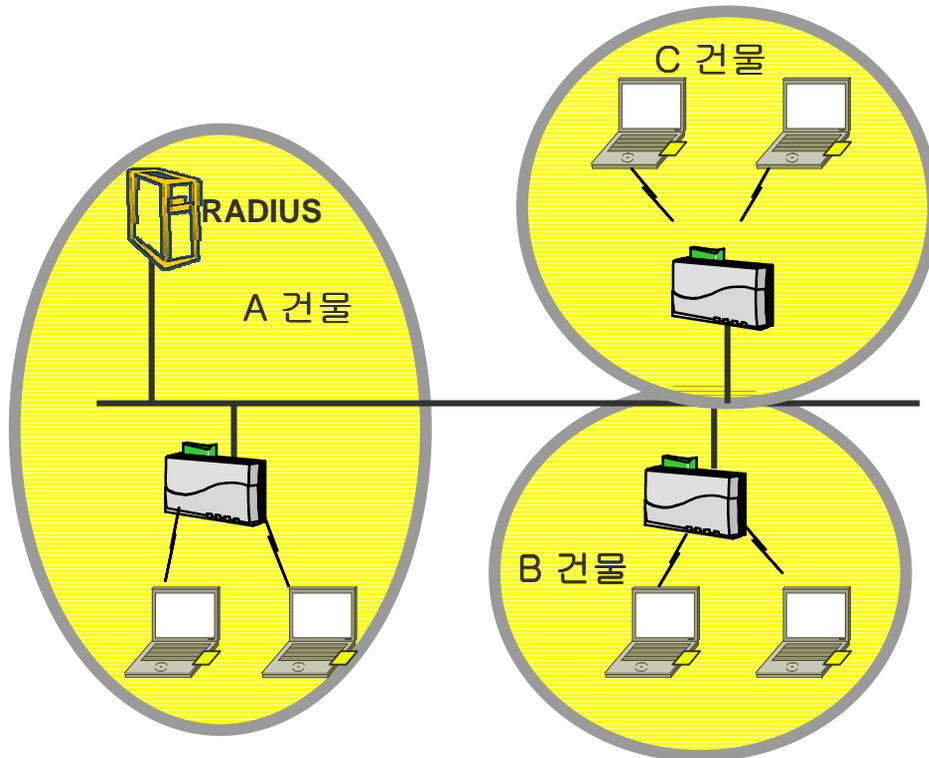
브리지 구간에서 별도 암호화 장비 적용



{군
OO부대 오지연결}

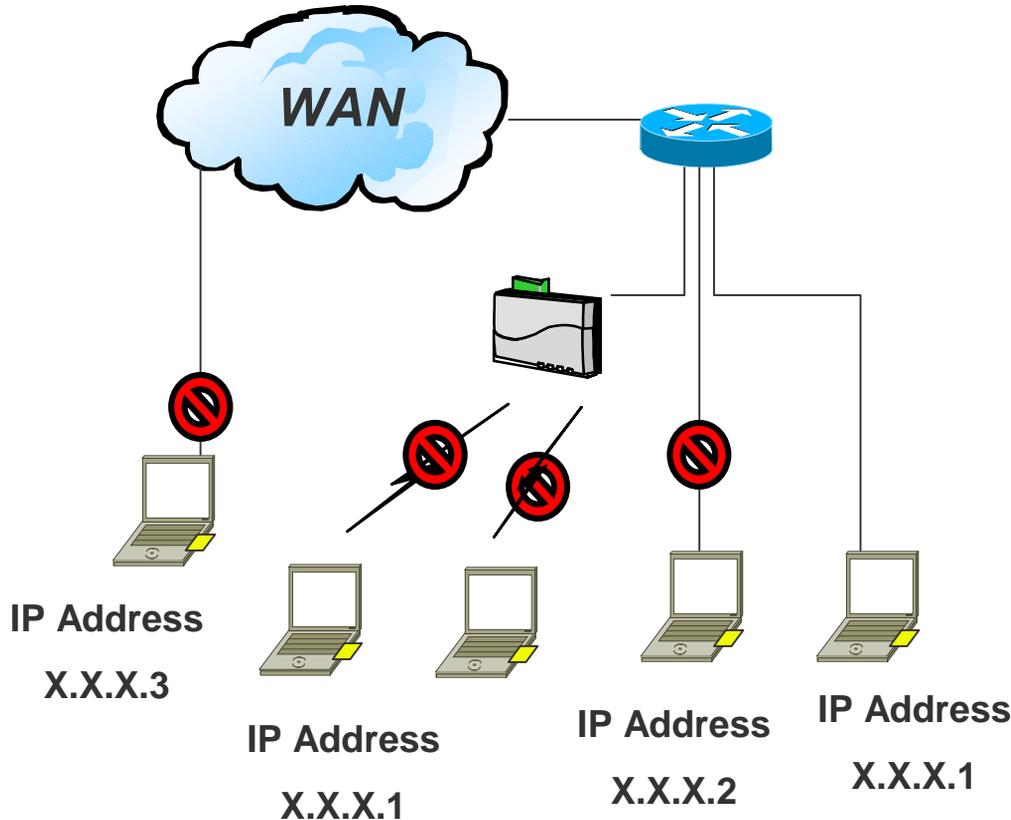
전파 영역 통제

- 건물 또는 지역 밖으로 전파가 나가지 않도록 셀 설계 (출력 조정 등)
- 건물의 벽면에 전파 차폐 장치 설치 검토 중



{ 제조 }
OO전자

Access Point 관리 권한 제어



AP 접속 할 수 있는 IP 및 접근 경로를 별도로 설정하여 외부 사용자 및 내부 사용자의 접근을 차단 한다

실제 사용현장에서 무선 랜 보안의 문제 (1)

◆ 고려할 사항

- 과거 : 무선 랜 사용자도 극소수, 관심이 적은 상황
- 현재 : 무선 랜이 대중화로 보안이 이슈로 등장

◆ 공급자

- 과거의 관행 - 사용자가 적고 이슈화도 안되던 틈새시장 시절의 관성
- 무선 랜에 경험이 적은 공급업체 등장
- 경쟁이 치열해지면서 나타났다가 사라지는 제조/공급업체들
 - 책임이 뒤따르지 않는다
- 무선 랜 보안 단계와 필요성을 고객에게 알려주지만, 고객들이 스스로 가볍게 판단하는 경우
- 공급업체조차 무선 랜 보안에 대해 강력하게 추천하지 못하는 경우

실제 사용현장에서 무선 랜 보안의 문제 (2)

◆ 사용자, 관리자

- WEP 적용
 - 관리의 불편함
 - 속도 감소보다는 성능 중시 : 11Mbps 수준의 속도로 인해 무거운 사내 사용 애플리케이션을 원활하게 지원하기 위해 WEP 기능 미 적용
- MAC Address 적용
 - 관리의 불편함 : AP마다 MAC Address 등록, 변경시에도 AP마다 설정 변경
- 인증/보안 솔루션
 - 비용 측면에서 배보다 배꼽이 더 큰...
 - 약 5,000 무선랜 사용자 기준으로 무선 랜 도입 비용에서 인증/보안 솔루션 도입 비용이 25~30% 가량 차지할 것으로 예상
 - 소규모일 수록 비중은 더 높아질 것.
 - 네트워크 접속의 불편함 – Client S/W, id, password 등

◆ 결론

- 유선과 마찬가지로 장비의 문제가 아닌 보안 의식의 문제
- 정책과 명확한 기준/원칙으로 현장에 적용 과제

자본금

33 억

직원수

35 명

매출액

2000년 55억 / 2001년 56억 / 2002년 93억

무선랜

94년 국내 최초로 무선랜 사업 수행



감사합니다.

질문과 응답

Free & Safe Networking

(주)에프네트 / 영업부

전 창은 이사

cejeon@f-net.co.kr

☎ 02-2167-2860