

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

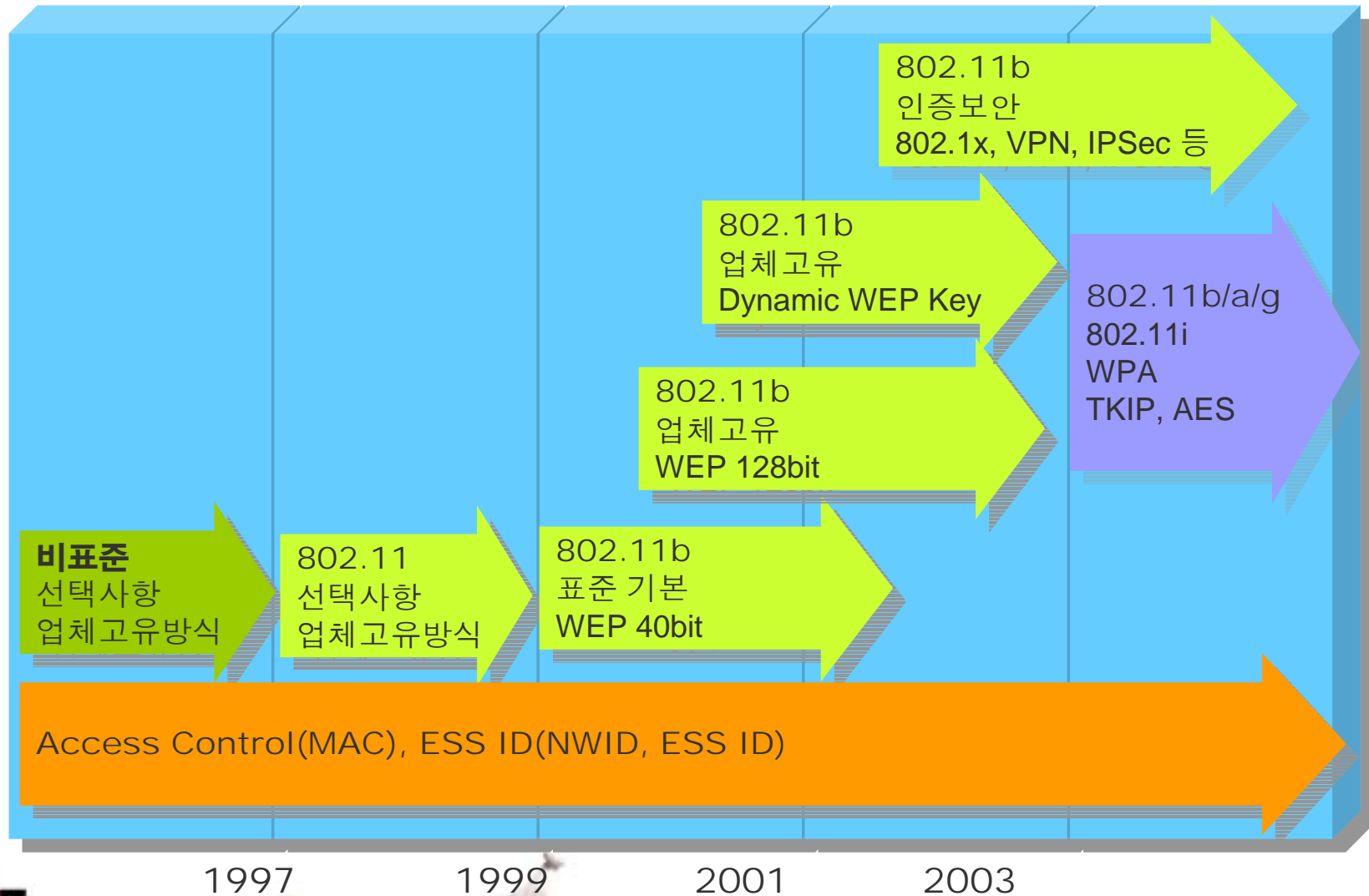
1. 개요
2. ESS ID / Closed System
3. Access Control
4. WEP
5. 인증/보안 솔루션
6. 기타 보안 적용 사례
7. 요약

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

Wireless Security Setup

Closed Wireless System

Enable Encryption

Encryption Key:

1 [XXXXXXXXXX]

2 [XXXXXXXXXX]

3 [XXXXXXXXXX]

4 [XXXXXXXXXX]

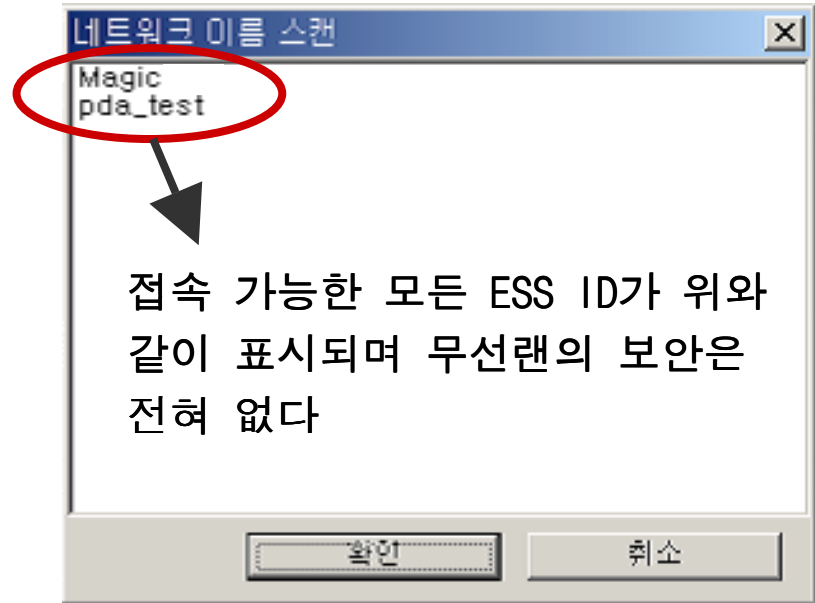
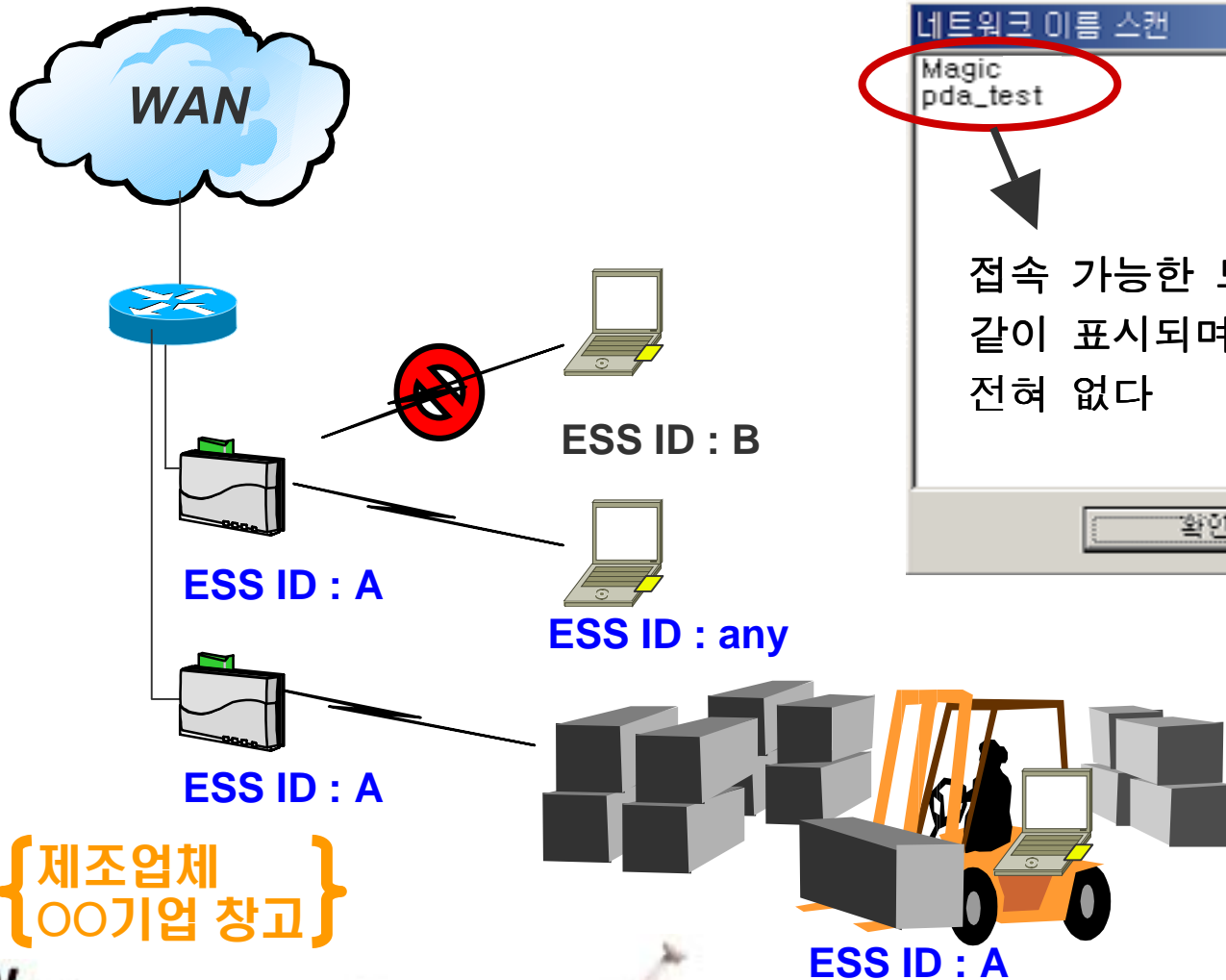
Deny non-encrypted Data

Encrypt Data Transmissions Using: Key 1

OK Cancel Help

2. ESS ID / Closed System

Closed System 미적용 사례

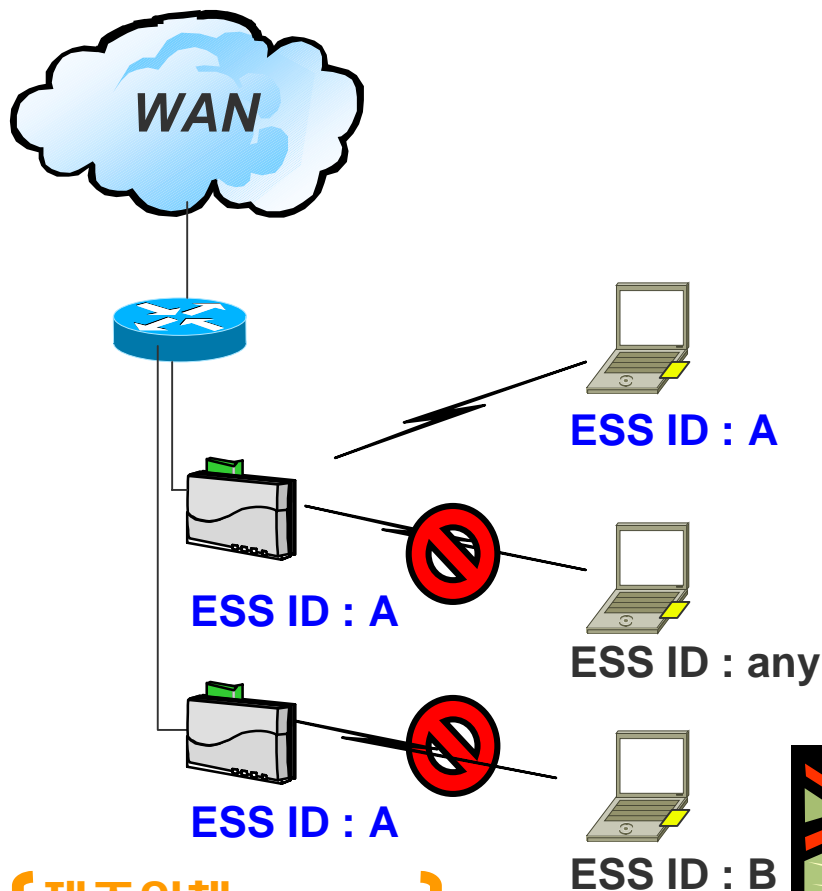


{ 제조업체
OO기업 참고 }

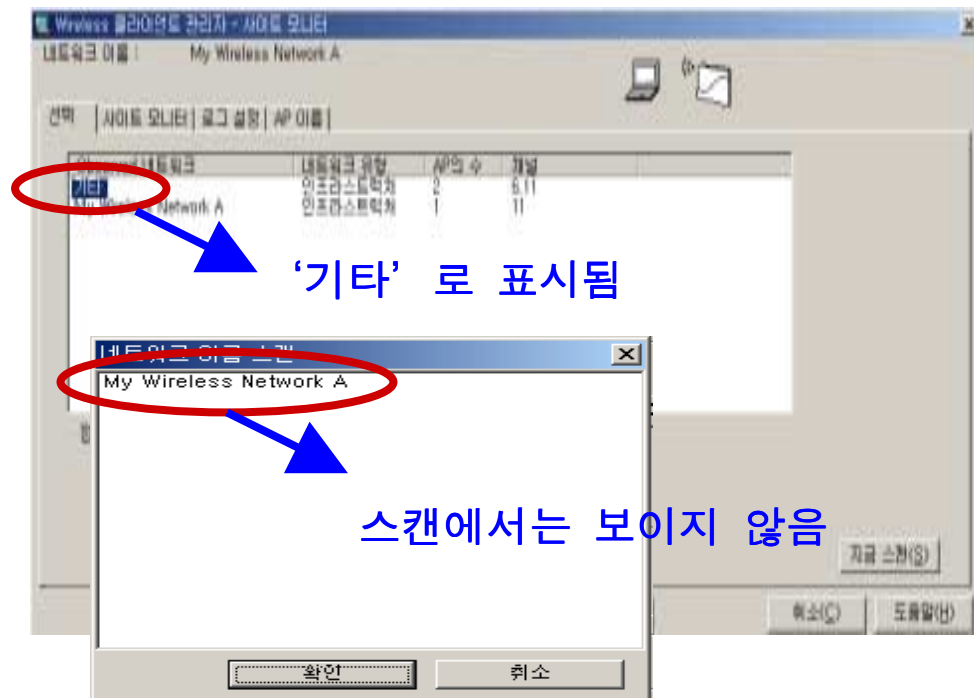
* 상기 설정화면은 물론 이후의 설정화면도 특정 기업과 상관없는 데이터입니다.

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

| 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

| 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

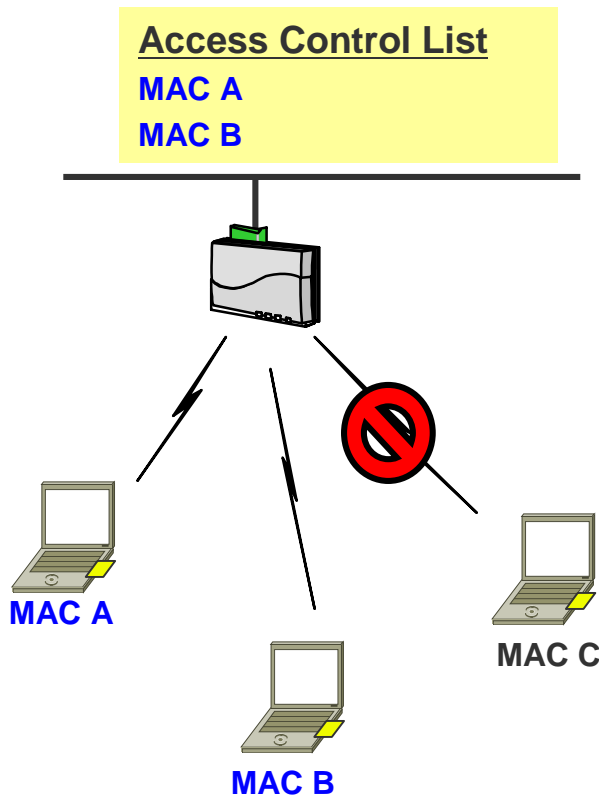
Closed System

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

Sniff2: Decode, 1/17169 802.11 LANs Frames

| 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@..퀵닐
00000040: 2f d5 32 b0 f3 ad f6 55 60 56 a3 8d 67 dc 62 72 /?값?U`V퀵g?r
00000050: da 99 9c a5 4e f5 6d 3b 0d 7b f2 34 11 11 3a e2 2?N2: f2 .

Expert Decode Matrix Host Table Protocol Dist. Statistics

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 image shows a Wireshark packet capture window titled "Sniff2: Decode, 1/389 802.11 LANs Frames". The main pane displays a list of captured packets. A red oval highlights packets 1 through 4, which are BPDUs from source Lucent319419 to destination 0180C2000000. The summary for these packets is "Expert: Same Transmitter And Receiver Address BPDU: S: Pri=8000 Port=8003 Root: Pri=8000 Addr=00601D3194". Packet 5 is a broadcast from Agere 42497D with the summary "Expert: ACK Frame Timeout". A blue oval highlights this summary. The bottom pane shows the protocol tree for packet 5, including LLC and BPDUs.

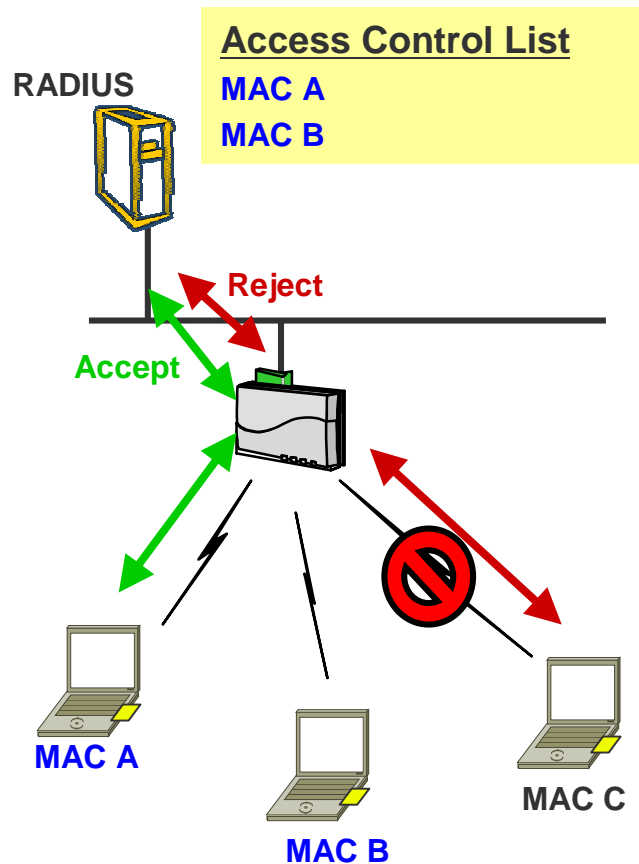
| No. | Source Address | Dest Address | Summary | Len |
|-----|----------------|--------------|---|-----|
| 1 | Lucent319419 | 0180C2000000 | Expert: Same Transmitter And Receiver Address BPDU: S: Pri=8000 Port=8003 Root: Pri=8000 Addr=00601D3194 | 6 |
| 2 | Lucent319419 | 0180C2000000 | Expert: Same 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 |

Protocol Tree for Packet 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
 - LLC:
- BPDUs: ----- Bridge Protocol Data Unit Header -----
 - BPDUs:

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 } * WEP도 함께 적용
OO 전자

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

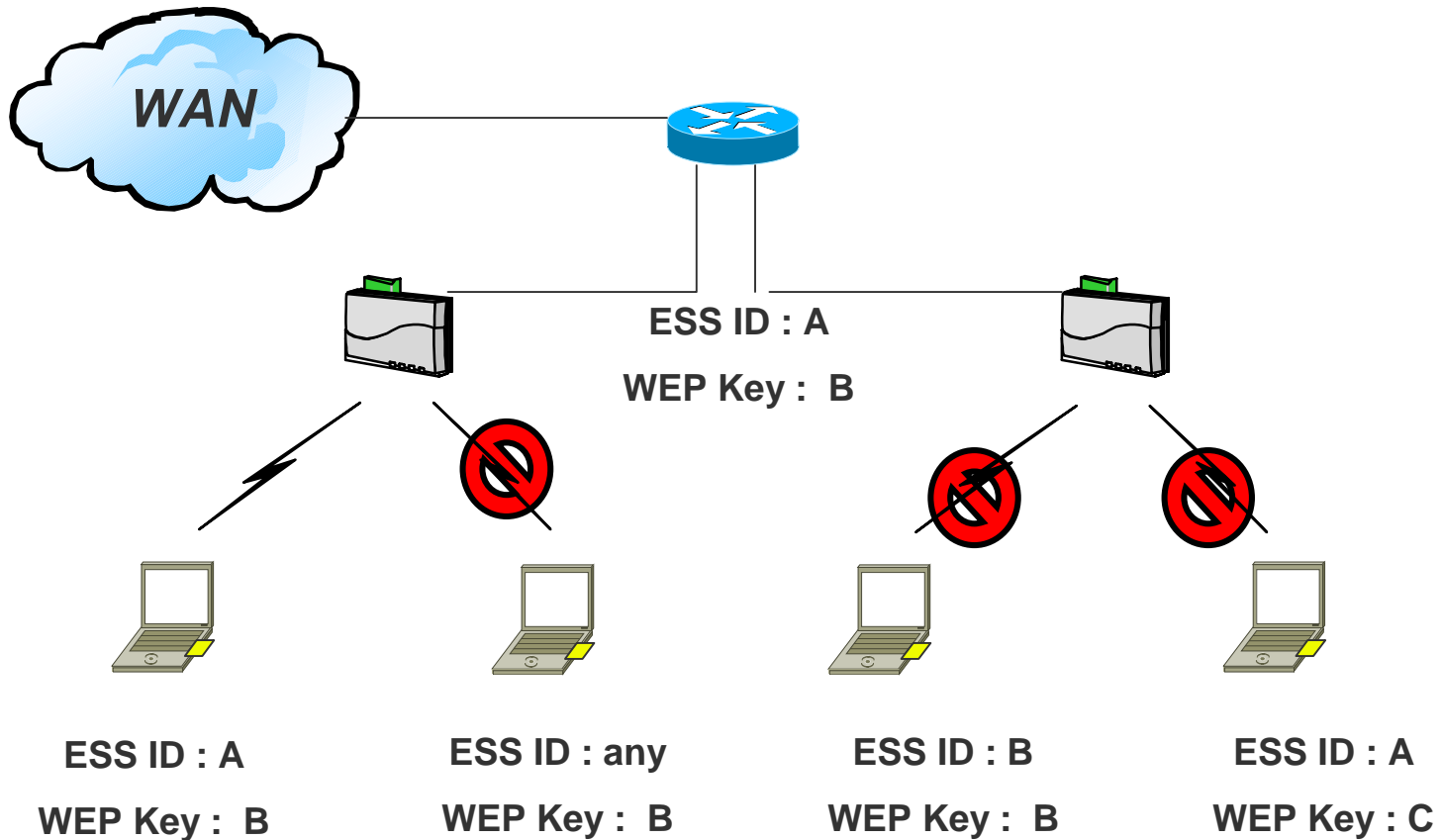
ESS ID

- 
- 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

Sniff1: Decode, 3/11761 802.11 LANs Frames

| No. | Source Address | Dest Address | Summary | Len |
|-----|-----------------|-----------------|---|-----|
| 2 | Agere 42497D | Agere 30DE14 | 802.11: 2.0 Mbps, Signal= 66%, Acknowledgment (ACK) | 10 |
| 3 | [192.168.15.232 | [192.168.15.68] | NETB: Data, 1460 bytes | 153 |
| 4 | Agere 42497D | Agere 30DE14 | 802.11: 2.0 Mbps, Signal= 66%, Acknowledgment (ACK) | 10 |
| 5 | [192.168.15.68] | [192.168.15.232 | TCP: D=1040 S=139 ACK=3439864342 WIN=64240 | 78 |
| 6 | Agere 30DE14 | Agere 42497D | 802.11: 2.0 Mbps, Signal= 69%, Acknowledgment (ACK) | 10 |
| 7 | [192.168.15.232 | [192.168.15.68] | NETB: Data, 1460 bytes | 153 |
| 8 | Agere 42497D | Agere 30DE14 | 802.11: 2.0 Mbps, Signal= 66%, Acknowledgment (ACK) | 10 |
| 9 | [192.168.15.232 | [192.168.15.68] | NETB: Data, 1460 bytes | 153 |
| 10 | Agere 42497D | Agere 30DE14 | 802.11: 2.0 Mbps, Signal= 66%, Acknowledgment (ACK) | 10 |
| 11 | [192.168.15.232 | [192.168.15.68] | NETB: Data, 1460 bytes | 153 |
| 12 | Agere 42497D | Agere 30DE14 | 802.11: 2.0 Mbps, Signal= 66%, Acknowledgment (ACK) | 10 |
| 13 | [192.168.15.68] | [192.168.15.232 | TCP: D=1040 S=139 ACK=3439867262 WIN=64240 | 78 |
| 14 | Agere 30DE14 | Agere 42497D | 802.11: 2.0 Mbps, Signal= 68%, Acknowledgment (ACK) | 10 |
| 15 | Agere 42497D | Broadcast | 802.11: 2.0 Mbps, Signal= 67%, Beacon | 61 |
| 16 | [192.168.15.232 | [192.168.15.68] | NETB: Data, 188 bytes | 260 |

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]

00000000: 08 01 02 01 00 02 2d 42 49 7d 00 02 2d 30 de 14 ... -BI}...-0?
00000010: 00 02 a5 6b 4c 70 d0 7e aa aa 03 00 00 00 08 00 ... 00000020: 45 00 05 dc c0 47 40 00 80 06 94 57 c0 a8 0f e8 E... 00000030: c0 a8 0f e8 04 04 10 00 8b cd 08 35 7e 64 e6 97 39 ... 00000040: 50 10 40 da b3 3f 00 00 a1 15 86 ab ec 65 b8 6a P.@... 00000050: 26 db 94 82 7e 12 68 08 55 d0 23 0a e2 14 a5 f0 &??... 00000060: 65 9e 35 ab 23 79 8f c3 4a 09 c4 6e 74 96 87 40 e??y... 00000070: 1b 3f 25 6c 03 76 0d c1 5d 9c f7 88 55 4f 96 64 .?%l.v.?... 00000080: e1 d5 6c 38 7f e5 38 97 4c 86 b5 8a 43 38 19 35 ... 00000090: 5c b1 13 c3 ef c2 7a 54 77 2d b3 70 25 e8 dd a1 \?... 000000a0: 5f 81 af 5b 95 4b 54 48 d5 71 8c 8c 91 05 62 b2 ... 000000b0: 44 21 a3 6b e9 07 1c 1e 02 74 d1 4f 51 80 59 72 D!... t?Q Yr

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 a sequence of WEP data packets and acknowledgments between Agere and Compaq devices.

| 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 |

The detailed view shows the DLC (Data Link Control) header information for a frame:

- 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

The bottom part of the screenshot shows the raw data in hexadecimal and ASCII. The ASCII column contains garbled characters, indicating that the data is encrypted and not readable without the correct key.

사용중인 MAC 정보 와 KEY 정보만 표시된다

데이터 전송 시 WEP 정보

Packet List:

| 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 Details (Frame 12):

```

DLC:
DLC: WEP (Wired Equivalent Privacy) Header
DLC: ... Initialization Vector #(1-3) = 8FE553
DLC: ... Initialization Vector #4 = 00
DLC: ... 00... .. = 0 (Key ID 1)
DLC: ... ..00 0000 = Pad
DLC: ... [187 byte(s) of encrypted MSDU]
DLC: ... Encrypted Integrity Check Value = 4A25BEBE
DLC:
    
```

Packet Details (Frame 13):

```

DLC:
DLC: WEP (Wired Equivalent Privacy) Header
DLC: ... Initialization Vector #(1-3) = 7F2B81
DLC: ... Initialization Vector #4 = 00
DLC: ... 00... .. = 0 (Key ID 1)
DLC: ... ..00 0000 = Pad
DLC: ... [93 byte(s) of encrypted MSDU]
DLC: ... Encrypted Integrity Check Value = 9DFDE7CA
DLC:
    
```

Packet Details (Frame 17):

```

DLC:
DLC: WEP (Wired Equivalent Privacy) Header
DLC: ... Initialization Vector #(1-3) = 90E553
DLC: ... Initialization Vector #4 = 00
DLC: ... 00... .. = 0 (Key ID 1)
DLC: ... ..00 0000 = Pad
DLC: ... [87 byte(s) of encrypted MSDU]
DLC: ... Encrypted Integrity Check Value = CD24DEB9
DLC:
    
```

- 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

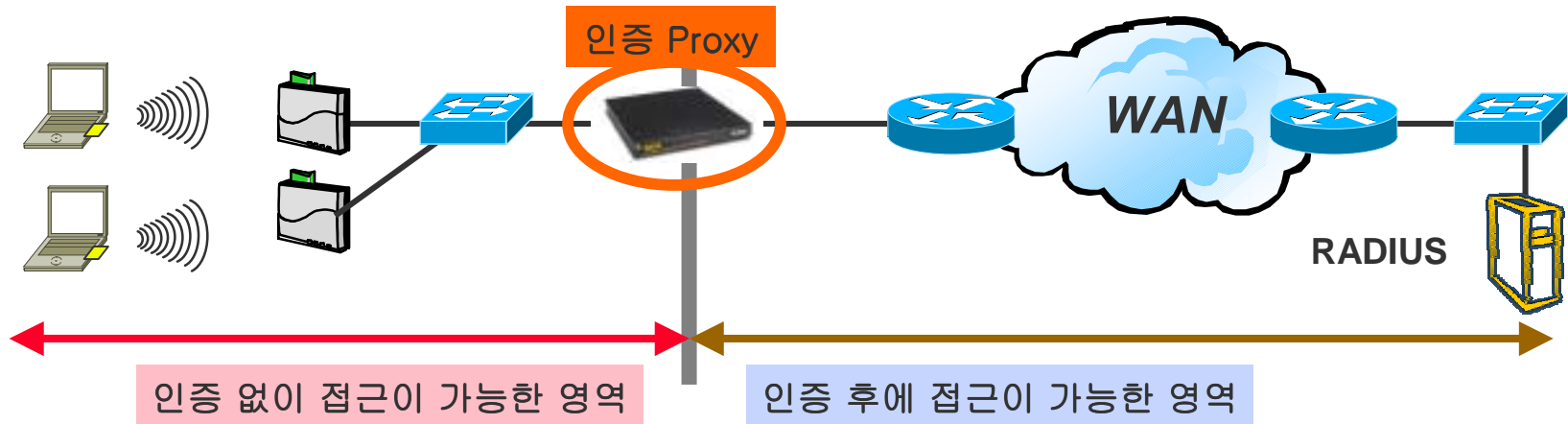
MAC Address 인증

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)

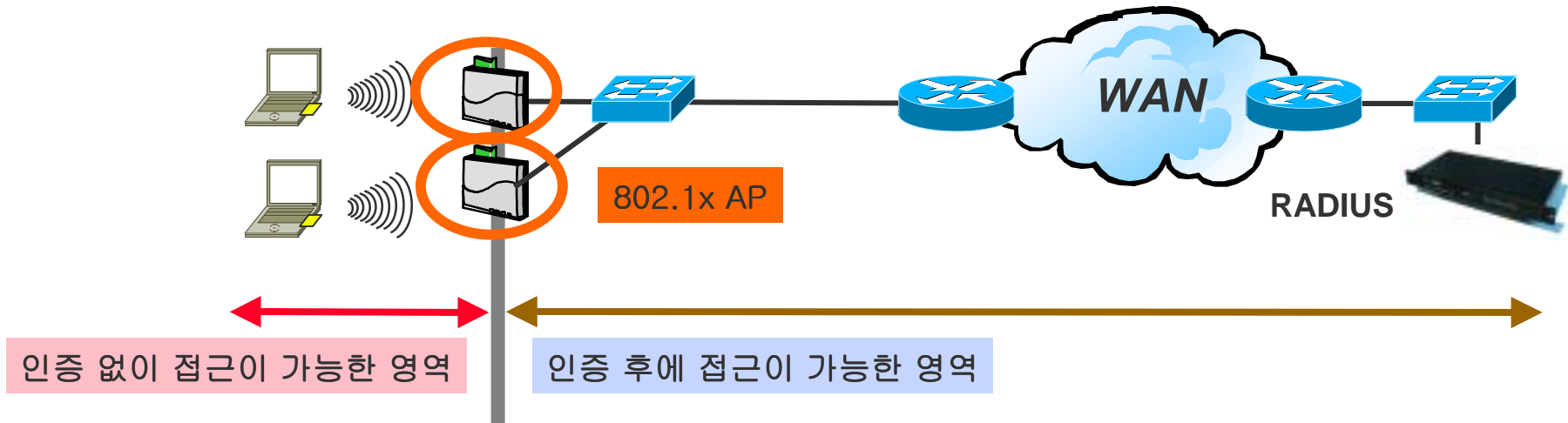
부가 장비

- 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

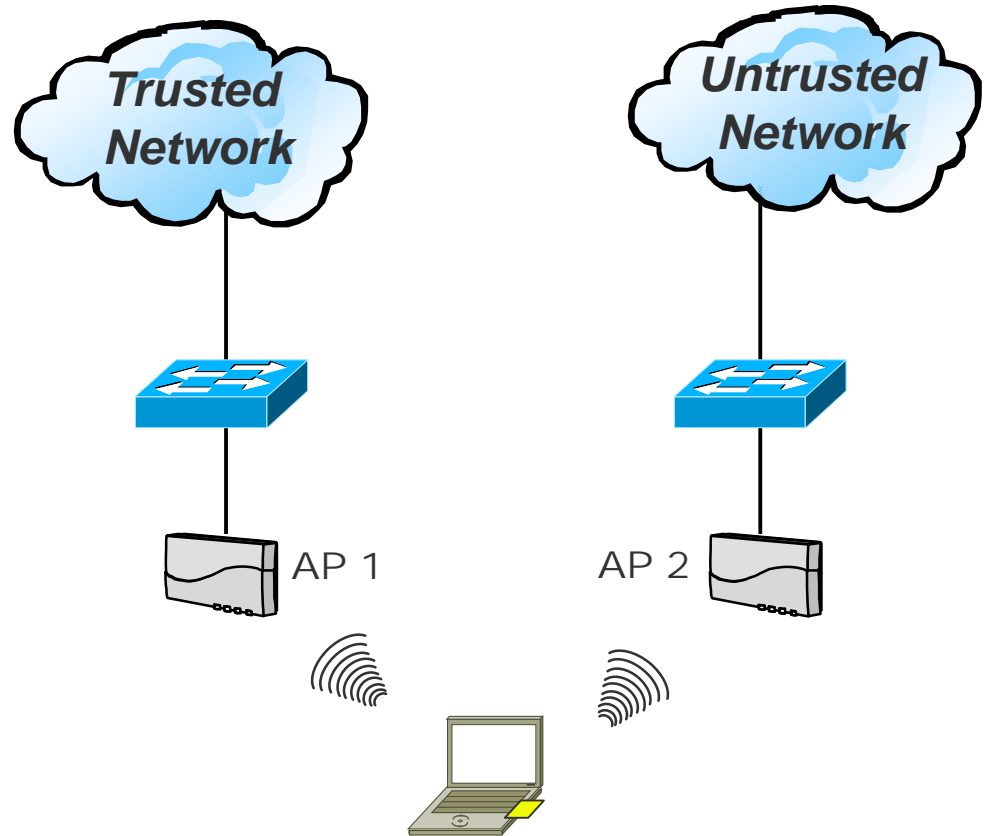
Closed System

ESS ID

- 관리, 보안 상의 장점
- 보안을 위한 비용 과다 발생

분리된 망에서의 무선 적용

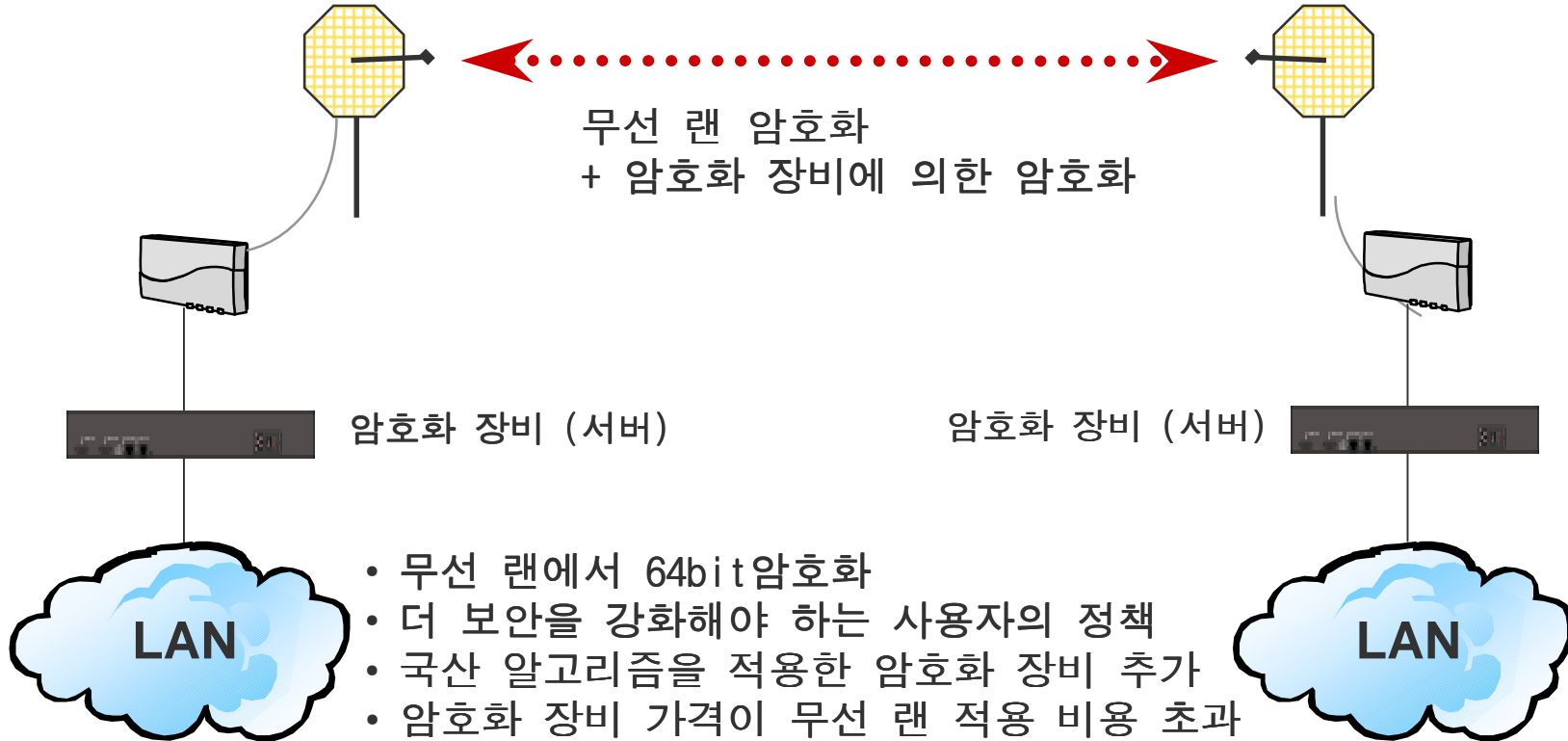
- ◆ 정책에 따라 안전한 네트워크와 안전하지 않은 네트워크를 물리적으로 분리
- ◆ 사용자 PC에서는 필요에 따라 AP 1 또는 AP 2를 선택하고 소프트웨어적으로 네트워크를 전환
- ◆ 사용자는 두 개의 네트워크를 이용할 수 있지만 안전하지 않은 네트워크에서 안전한 네트워크로 접근은 불가



{ 정부기관
OO부 교육장 }

XX 공공기관 - 교육장

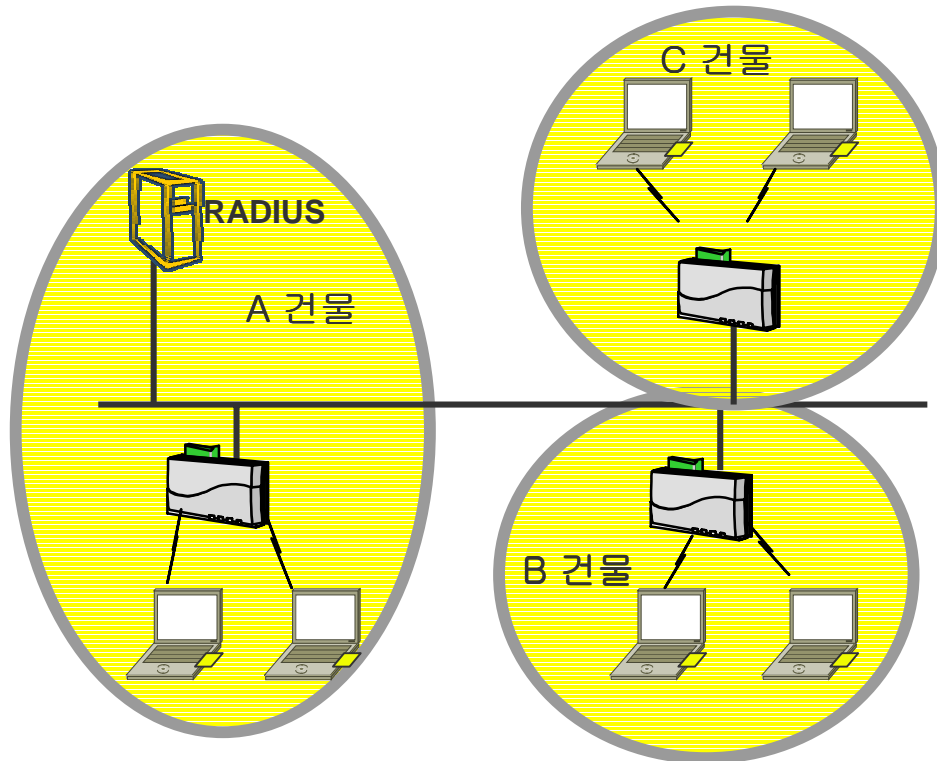
브리지 구간에서 별도 암호화 장비 적용



{ 군
OO부대 오지연결 }

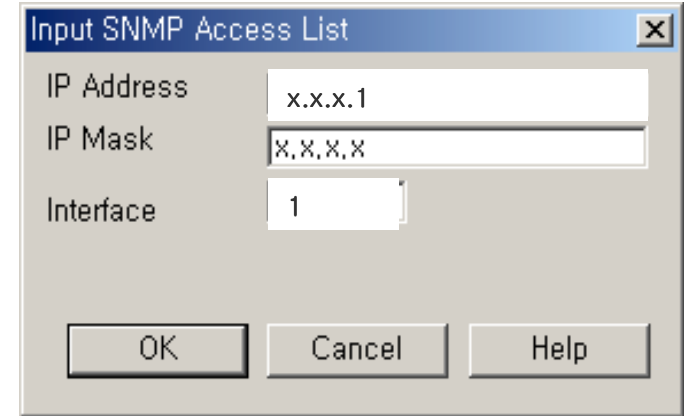
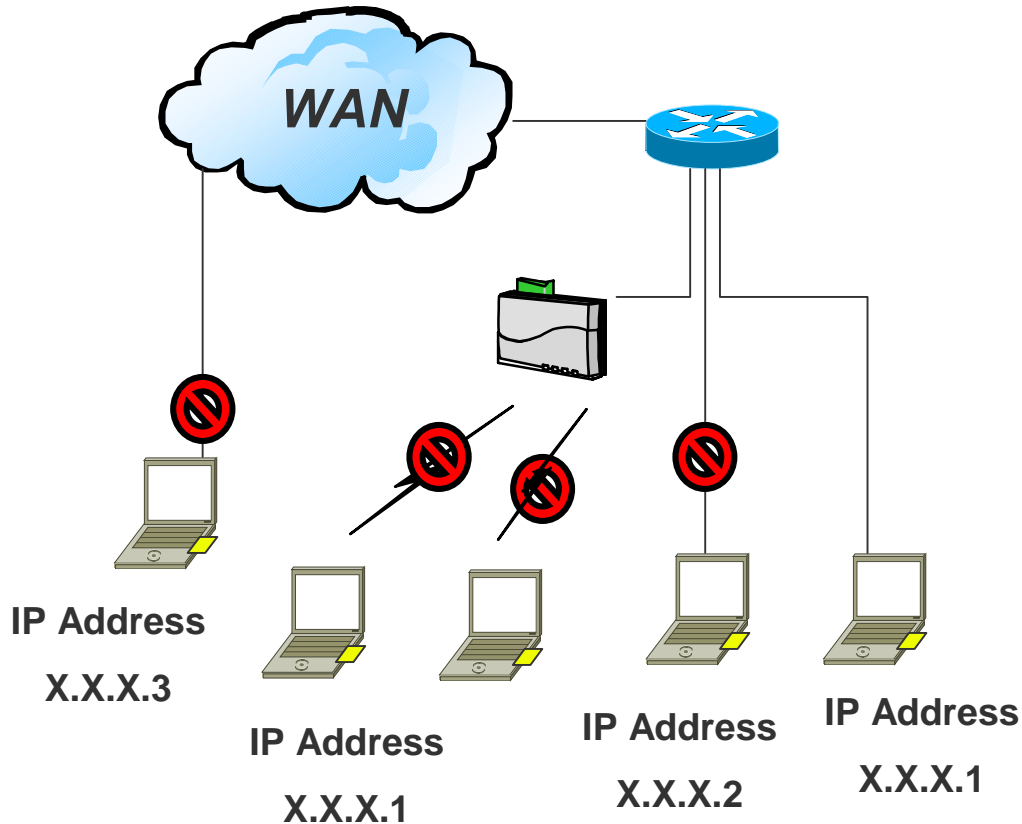
전파 영역 통제

- 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