Wireless LAN Security

Self-Defending *Wireless* Network

Kim, MinSe
mskim@cisco.com
Technical Operations
Cisco Systems Korea

순서

- 무선랜 보안의 역사
- 무선랜 보안 표준 **- 802.11i**
- 불법 **AP,** 문제점과 해결방안
- **Wireless IDS**
- 유무선 통합 보안
- 최적의 무선랜 보안 방안 및 산업군별 고려사항
- 시스코 무선 보안 솔루션 컴포넌트
- 질의 응답

무선랜 보안의 역사

Cisco.com

- 1999~2000
- 무선랜 보안 1세대
- Static WEP

WEP Cracking
도난 대책
키 관리 부재

- 2001~2002
- 무선랜 보안 2세대
- 802.1x / VPN

Session Hijacking
Dictionary Attack
MitM Attack

- 2003~2004
- 무선랜 보안 3세대
- WPA1 / WPA2

Rogue AP
DoS Attack
Scalability / Manageability

- 2004~2005
- 유무선통합 보안

Solved !

시스코 무선랜 보안 아키텍쳐: 4대 영역

Cisco.com

Cisco Prevention Service

Secure the infrastructure

Wireless IDS

Secure the air

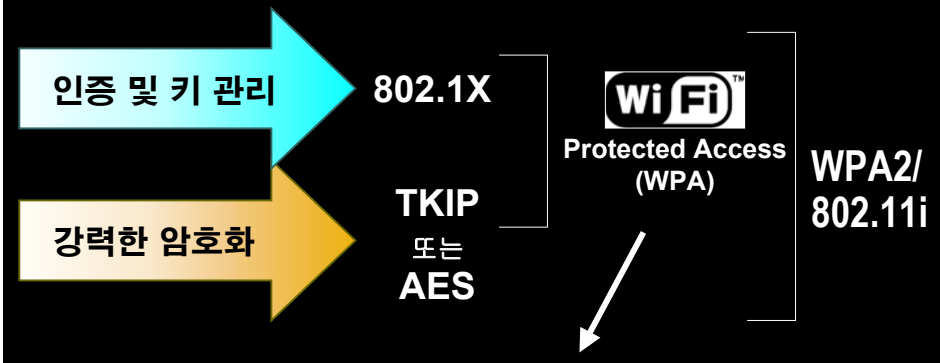
802.11i NAC Guest/

Secure the Data

Secure the Data – 무선랜 보안 표준 IEEE 802.11i

표준 보안 : 802.11i 과 WPA2

Cisco.com



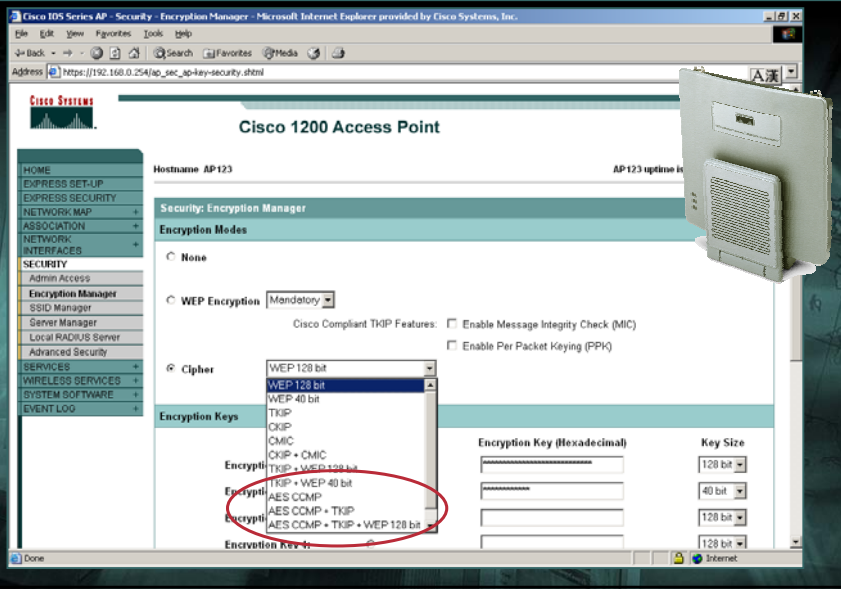
- WPA 은 모든 Wi-Fi 무선랜 제품을 위한 필수 항목
- 2004년 9월부터, 802.11i 규격에 기반한 WPA2 인증 시작

802.11i 특징

- 시스코에서 표준화 그룹의 의장 담당
- 2004년 6월 표준화 완료
- **AES 암호화**
- 인증 방식:
  - **802.1x** (기업용)
  - **Pre-shared key** (개인용)
- **Pre-authentication** 은 옵셔널 항목으로 이동;
- 시스코는 **Fast re-authentication,** 패스트 로밍등을 위한 키 캐싱 기능을 통해 표준 이상의 것을 제공.

- 시스코 에어로넷 **AP1200** 은 **WPA2** 의 테스트 베드인 동시에 세계 최초의 제품.

IEEE 802.11i / WPA2 의 레퍼런스 플랫폼, 시스코 무선랜

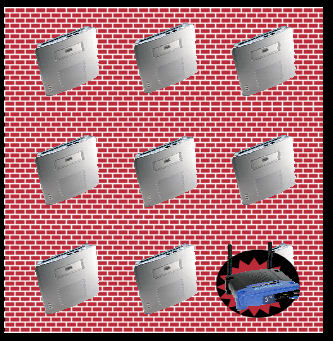


불법(Rogue) AP 문제점과 해결방안

불법(Rogue) AP 란 무엇인가?

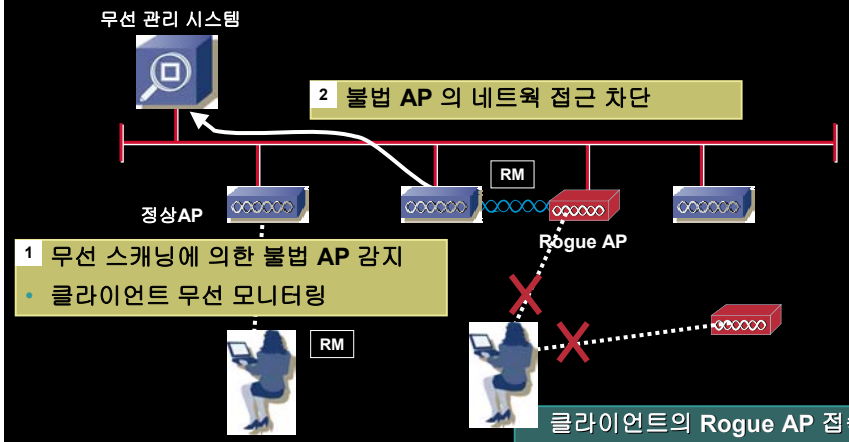
Cisco.com

- 조직내 무선 보안 정책을 따르지 않는 무선 장비 (억세스 포인트, **Ad-Hoc** 노드)
- 네트웍에 무단 설치되어, 내부망으로의 제한없는 억세스 통로가 됨
- 클라이언트의 임의 접속으로 정보 유출 위험
- 불법 **AP** 의 감지 및 차단 솔루션의 필요성 부상



불법 AP Self-Defending 시스템

Cisco.com

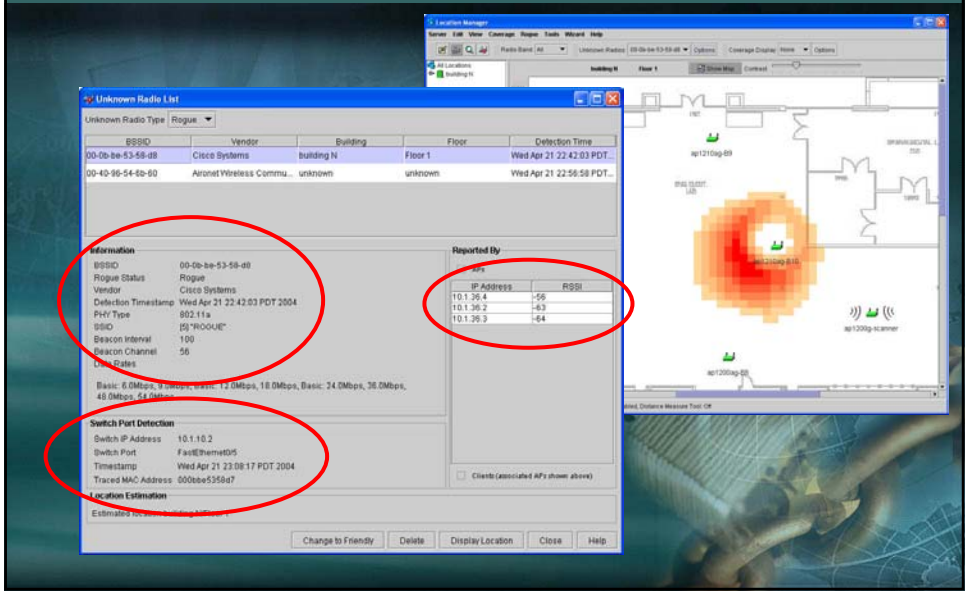


클라이언트의 Rogue AP 접속 제한
- 프로파일 기반 접속
- 양방향 인증

• 클라이언트 RM 모니터링

Cisco Works WLSE 를 통한 불법 AP 탐지 정보 화면

Cisco.com



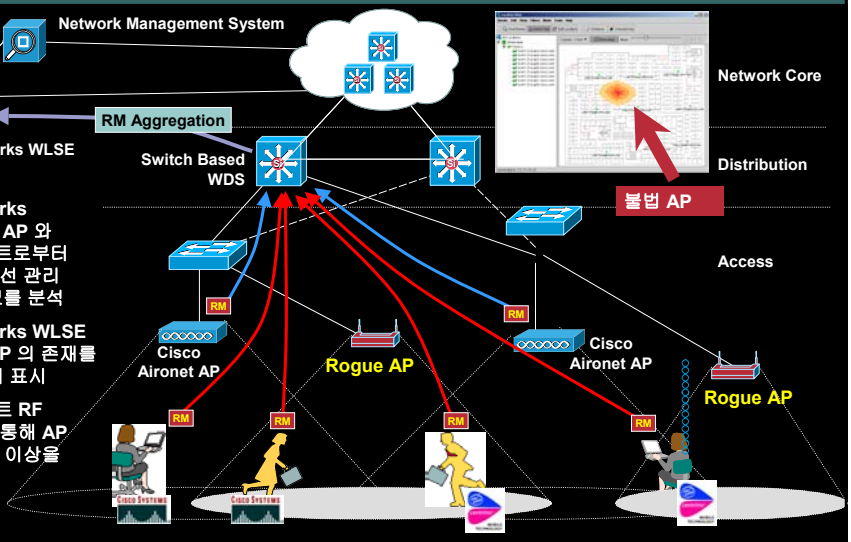
Wireless LAN IDS

왜 **Wireless IDS** 가 이슈가 되는가**?**

Cisco.com

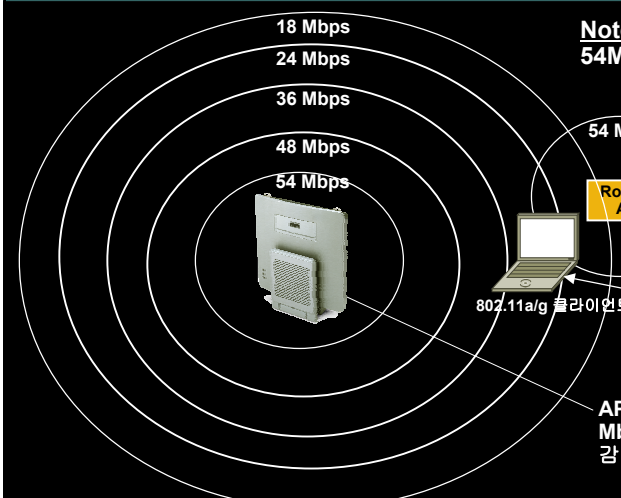
- **802.11** 무선 네트웍의 지속적인 모니터링
  - 인증되지 않은 억세스 포인트
  - **Active attacks**
  - 잘못 구성된 억세스 포인트와 클라이언트
- **Wireless IDS** 기술이 조금씩 등장하고 있다.
  - 공격 도구들에 대한 모니터 **(NetStumbler,** 등**)**
  - 특정한 종류의 공격에 대한 모니터링 **(**대부분 액티브 어택**)**
  - 수동 격리 **(containment) (** 관리자에게 경고 후**,** 대응책을 선택하도록 **) vs.** 자동 격리 **(containment)**

무선 (Air/RF) 모니터링 – AP 와 클라이언트 기반



1. CiscoWorks WLSE 는 AP 와 클라이언트로부터 수집된 무선 관리 (RM) 정보를 분석
2. CiscoWorks WLSE 는 불법 AP 의 존재를 경고, 위치 표시
3. 클라이언트 RF 스캐닝을 통해 AP 감지 범위 이상을 커버 가능

클라이언트 기반 스캐닝의 장점



Note: 불법 AP 는 오직 54Mbps 만 사용하도록 설정!

WLAN 클라이언트는 불법 AP 를 감지하고 시스코 AP 에 이를 보고!

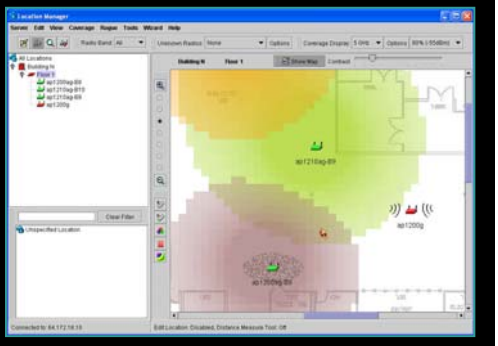
AP 는 불법 AP 감지불능! (54 Mbps 커버리지로는 불법 AP 를 감지할 수 없다.!)

시스코 클라이언트에 더해서, 센트리노 노트북과 같이 CCX 를 지원하는 멀티벤더 클라이언트를 통해 더욱 가속화 !

AP 겸용 무선 스캔과 전용 스캔

Cisco.com

- 일반 AP 에 Wireless IDS 기능 적용
  - 무선 클라이언트를 서비스하면서 RF 데이터도 수집 가능한 억세스 포인트
  - AP 가 클라이언트 서비스 도중에 데이터 수집
  - 아이들(Idle) 시간을 활용, 다른 채널에 대해서도 스캔 가능.
- 전용 Wireless IDS
  - AP 를 RF 센서 전용으로 설정
  - 802.11a/b/g 의 모든 채널을 스캔
  - 전용 모드를 통한 특화된 IDS 기능
- 혼합형 배치
  - 예: 802.11g 무선은 통합 모드로, 802.11a 무선은 전용 모드로 배치



무선랜 Wireless IDS 배치 방안

Cisco.com

- 모든 구간에서 RF 모니터링을 사용하라
  - 최신 버전의 WLSE, 스위치 및 AP IOS 릴리즈를 사용, 무선 (RF) 모니터링을 실시하라
  - AP 의 RF 스캐닝을 하고, 이에 더불어 Cisco/CCX 클라이언트를 사용한 클라이언트 기반 스캐닝을 더하라
  - 빌딩과 같은 고밀도 사무실 환경에서는 “프랜들리” AP 들을 파악해 두어야 한다
- WLSE 를 통한 보안 폴리시 모니터링
  - 표준화된 보안 정책을 정의하고, AP 구성상의 헛점을 모니터링
  - RADIUS 서버의 가용성 및 성능을 모니터링

무선 Denial of Service (DoS) 공격

Cisco.com

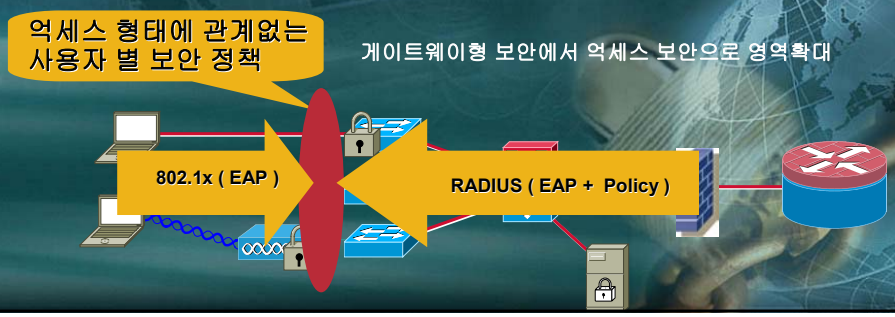
- **RF 재밍(jamming)**
  단순 **RF** 방해 전파 전송 (예: **AP** 주변에 위치한 전자레인지 혹은 **2.4 GHz** 무선전화기)
- **802.11** 매니지먼트 프레임을 사용한 **DoS** 공격
  클라이언트나 **AP** 의 **MAC** 주소를 스푸핑,
  조작된 **802.11** 관리 프레임을 전송
- **802.1x authentication flooding**
  공격자가 **802.1x** 인증 요청을 **DoS** 형태로 **AP** 에 전송
  AP 의 불필요한 인증프레임 처리로 부하 가중

유무선 통합 보안

유무선 통합 보안 – 인증

Cisco.com

- 유무선 통합 인증 클라이언트 (802.1x)
- 인증 서버와 사용자 DB, 정책 서버를 공유
- 유무선 네트워크의 접점에서 공통의 보안 정책 부여 요구
- 유무선 공통의 억세스 정책을 적용 (ex: VLAN Name, GPO)

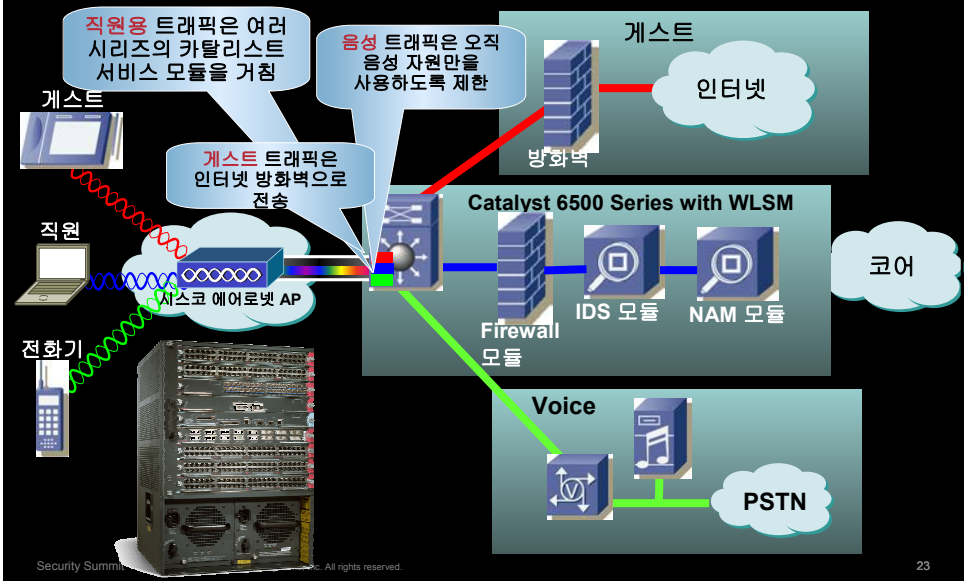


유무선 통합 보안 – 보안 인프라 통합

Cisco.com

- 무선 보안 정책을 유선 네트웍에 적용
  - 다중 사용자/디바이스 그룹
    (SSID/VLANs/mGRE 터널)
- 유선 보안 기능들을 무선랜 환경에 응용
- Fast secure roaming (CCKM)
- 카탈리스트 6500 스위치 통합
  - 제어와 데이터 트래픽의 단일 인입 포인트
  - End-to-end 통합 보안
  - 패스트 시큐어 레이어-3 로밍

카탈리스트 6500 시리즈 무선랜 서비스 모듈 WLSM 보안 정책 분리를 제공하는 모빌리티 그룹



최적의 무선랜 보안 방안 및 산업군별 고려사항

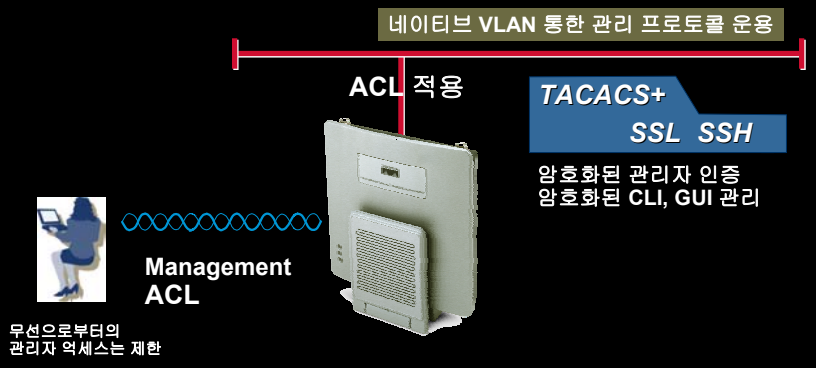
무선랜 보안 Best Practices

Cisco.com

- 표준 무선랜 보안솔루션을 도입
  - EAP/802.1x 인증 프로토콜
  - 데이터 암호화와 무결성: WPA, CKIP, WPAv2
- WPA / WPAv2 도입 방안
  - EAP 클라이언트가 준비되어 있는가 ?
  - RADIUS 서버 확장성과 가용성
  - 패스트 시큐어 로밍
- Guest 네트워킹 검토
- 관리 시스템 보안 적용

관리 시스템 보안을 위한 Best Practices

Cisco.com

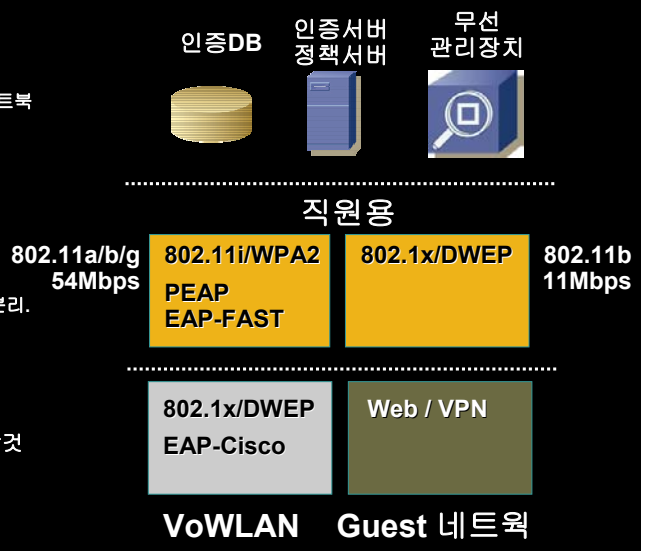


- AP 의 각종 Control 프로토콜은 사용자 네트웍과 분리
- 암호화된 관리 프로토콜을 사용하라
- AP 의 무선을 통한 관리자 접근을 제한하라

무선랜 보안 설계 사례
기업체 오피스 환경

Cisco.com

- 클라이언트 표준화
  - 54Mbps 랜카드 통일
  - 센트리노와 같은 CCX 노트북
  - Windows 2000 및 XP
- 인증 프로토콜 표준화
  - PEAP/MS-CHAPv2
  - EAP-FAST
- VoWLAN
  - 동일 인프라에서 VLAN 분리.
  - 사용자 ID 저장
- 게스트 네트워킹
  - 웹 기반 사용자 인증
- 인증서버 고가용성 검토할것
  - 본사 이중화
  - 각 거점별 인증서버 배치

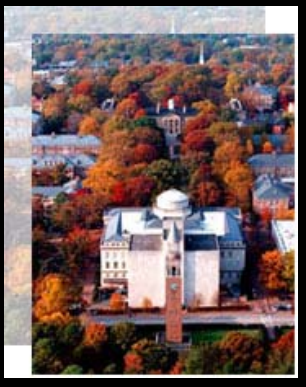


무선랜 보안 설계 사례
대학, 교육 기관

Cisco.com

- 학생용, 교직원, 학교 안내 키오스크 및 모바일 단말등 IT 담당자의 관리 외 영역에 있는 수많은 이기종 환경
- 클라이언트의 표준화가 되기 어려움
- 하나의 무선 인프라에서 다양한 조직별 보안 정책을 구분하여 정의

	클라이언트 환경	보안	접근 허용 망
학생용	예측 불가	MAC 인증, Web 기반 인증	인터넷 Only
교직원	Windows 2000 / XP 이상	WPA2 (802.11i)	업무용 및 인터넷
모바일 PDA	PDA, WinCE, PocketPC	MAC 인증 WPA	인터넷 Only
웹 키오스크	Windows 2000 이상	WPA2 (802.11i)	업무용



무선랜 보안 설계 사례
병원, 의료기관

- 표준화
  - 시스코 랜카드 또는 센트리노
  - 802.1x 를 지원하는 PDA
  - LEAP 이나 EAP-FAST 인증
- 고속 로밍 – 실시간 어플리케이션
  - 환자 모니터링 시스템
  - VoWLAN 장치
- 고가용성
  - 인증서버, 억세스 업링크 이중화
- Guest 네트워킹
  - 입원 환자들을 위한 서비스
  - QoS 적용한 단일 인프라 권장

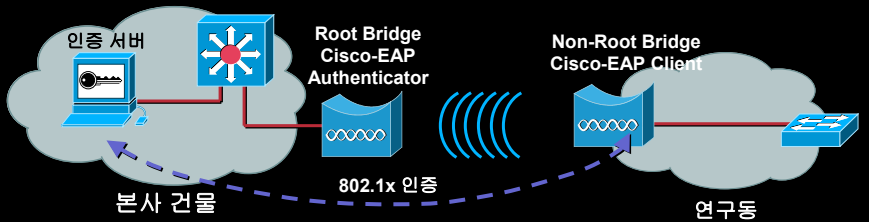
PDA

VoWLAN

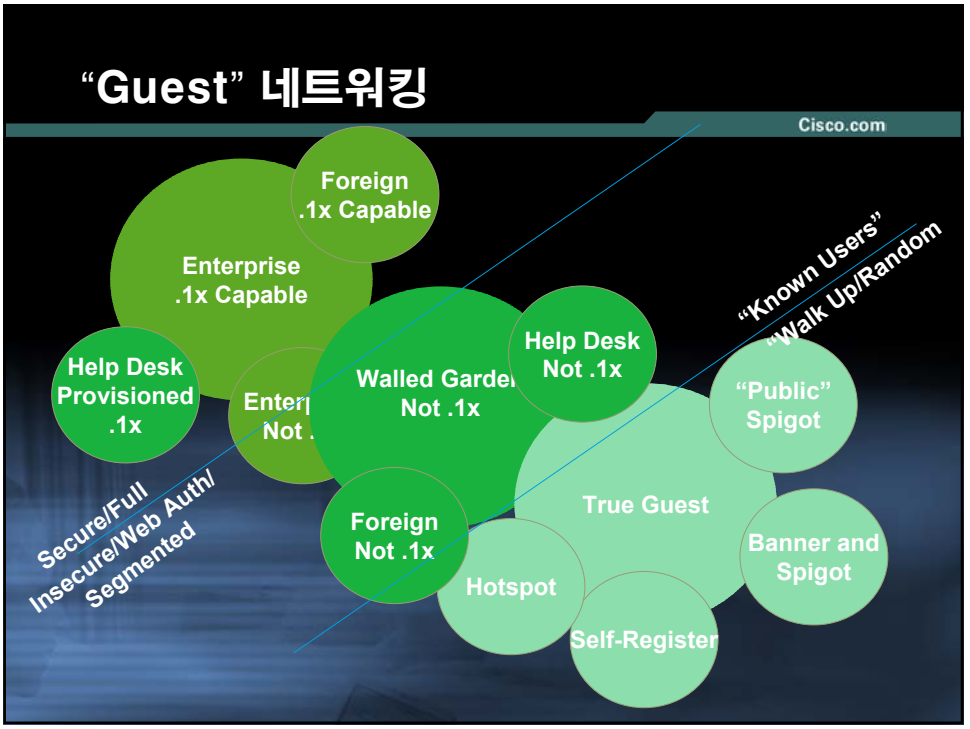
무선랜 보안 설계 사례
옥외 브릿지 환경

- 무선랜 브릿지도 무선랜과 “동일한” 수준의 보안 레벨이 필요합니다.
- No Broadcast SSID
- No Static WEP
- 최소한 WPA 사용할것

	WPA	VPN
적용계층	L2	L3
네트워크	브릿지 네트워크	라우팅 네트워크
멀티캐스트	Yes	No
오버헤드	No	Latency, Throughput
암호화	TKIP / AES (soon)	3DES / AES



“Guest” 네트워킹



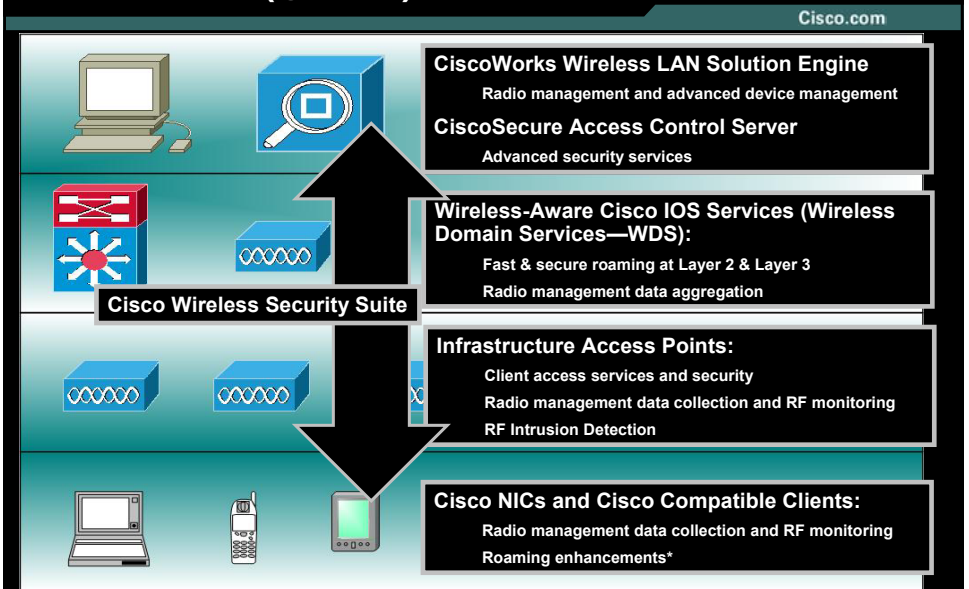
“Guest” 네트워킹 구현 방안

Cisco.com

- 1단계: Wired 유선 백엔드 측 작업
  - – 유선상에서 별도 VLAN, 별도 IP 서브넷, 보안, QoS 정의
- 2단계: AP 측 작업
  - AP 상에 Guest SSID / VLAN 정의
  - AP Guest 보안 설정 – Broadcast SSID , PSPF 사용
- 3단계: Guest 인증 백엔드 (Optional)
  - HTTP Redirect / Web 인증
  - Billing / Accounting

시스코 무선 보안 솔루션 컴포넌트

Cisco Structured Wireless Aware Network (SWAN)



CiscoWorks WirelessLAN Solution Engine 2.9

Cisco.com

- 무선랜 관리 어플라이언스
  - Not NMS, No Install, No Server Management !
- SWAN 아키텍쳐의 콘트롤 센터
  - AP / SWAN 시스템의 중앙 관리
- RF 관리 – 채널중첩, 간섭 탐지, AP 무선 파라미터 자동 조정, 디렉셔널 안테나 지원
- 불법AP 탐지 및 차단
- Self-Healing

- 사양
  - Dual Pentium 4 3.06 Ghz
  - 3GB Memory
  - Dual 10/100/1000 Ethernet

Wireless LAN Service Module – 카탈리스트 6500 용 유무선 통합 모듈

Cisco.com

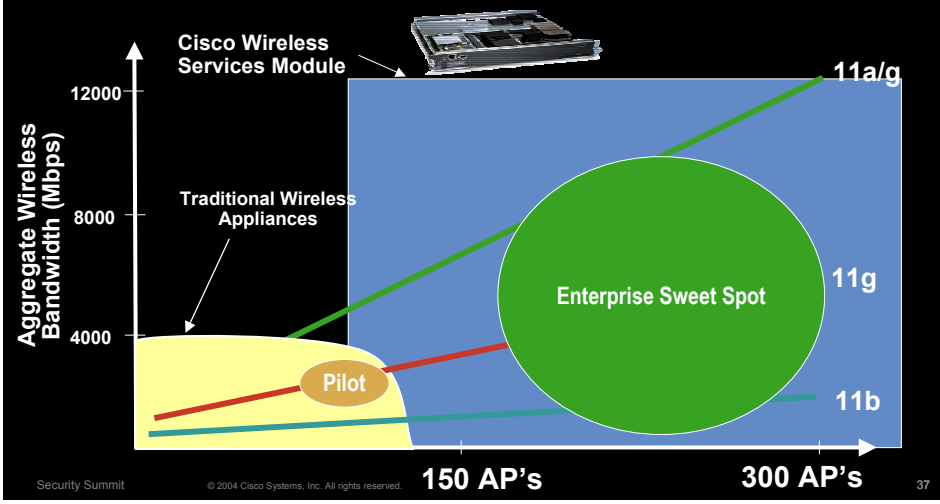
High-End 유무선 장비의 통합

- No Sweeping Infrastructure Changes
  - No Campus Spanning VLANs
  - No requirement for parallel infrastructure
- Industry-Leading
  - Scalability - 300 APs and 6000 users at introduction
  - Fast Secure L3 Mobility – sub 50ms handoff times
- Superior Operation and Manageability
  - Supported with Cisco IOS Software and Cisco management tools
  - No Single Point of Failure
  - Separation of Control Plane and Data Plane
- Enhanced Wireless Security
  - Up to 16 mobility groups, each with a single point of policy enforcement for all traffic
  - Catalyst 6500 Services Modules - Firewall, IDS, NAM and More

Scaling to Enterprise Bandwidth Requirements

Cisco.com

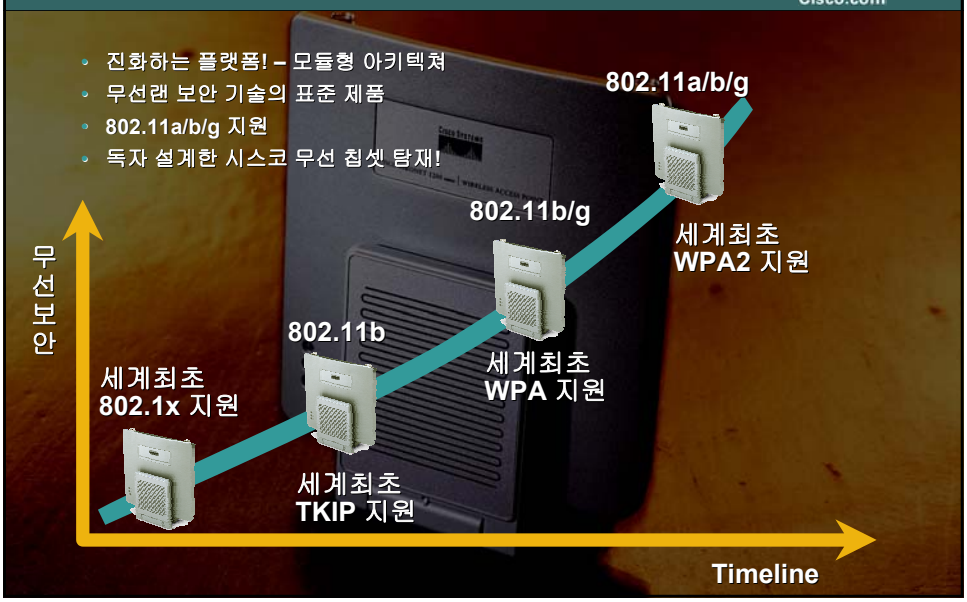
Rapidly expanding AP deployments and the migration to dual radio AP's drive bandwidth and performance requirements



Cisco Aironet 1200

Cisco.com

- 진화하는 플랫폼! – 모듈형 아키텍쳐
- 무선랜 보안 기술의 표준 제품
- 802.11a/b/g 지원
- 독자 설계한 시스코 무선 칩셋 탑재!



요약
올바른 무선랜 보안 정책

Cisco.com

1. 표준화
   1. 무선 인프라 / 클라이언트 환경 표준화.
   2. 호환성을 고려한 표준 무선 보안 기술 적용
2. 불법 AP 문제에 대응하라
   1. 무선 인식 인프라에 의한 불법 AP 탐색 및 차단
   2. Integrated Wireless IDS
3. 유무선 통합 보안
   1. 사용자 인증
   2. 단일 인프라 기반의 Trusted 망 적용

❖ 산업군 별 보안 적용 검토

질의 응답

자주 있는 질문

Cisco.com

- 전파 간섭 때문에 자주 다른 무선 네트웍에 접속합니다.
  - 프로파일 기반 무선네트웍 접속
  - **Windows XP SP2** 설치
- 올바른 **SSID** 정책은 무엇인지요?
  - 게스트 네트워킹에 국한된 **Broadcast SSID** 가 적합합니다.
- 센트리노 노트북을 사용중인데, 무선 보안 적용이 가능합니까?
  - **PC** 제조사 또는 인텔 홈페이지에서 **Intel Pro*set** 을 다운로딩 받으세요.
- 추천하는 인증 프로토콜이 있다면 ?
  - **LEAP, PEAP**