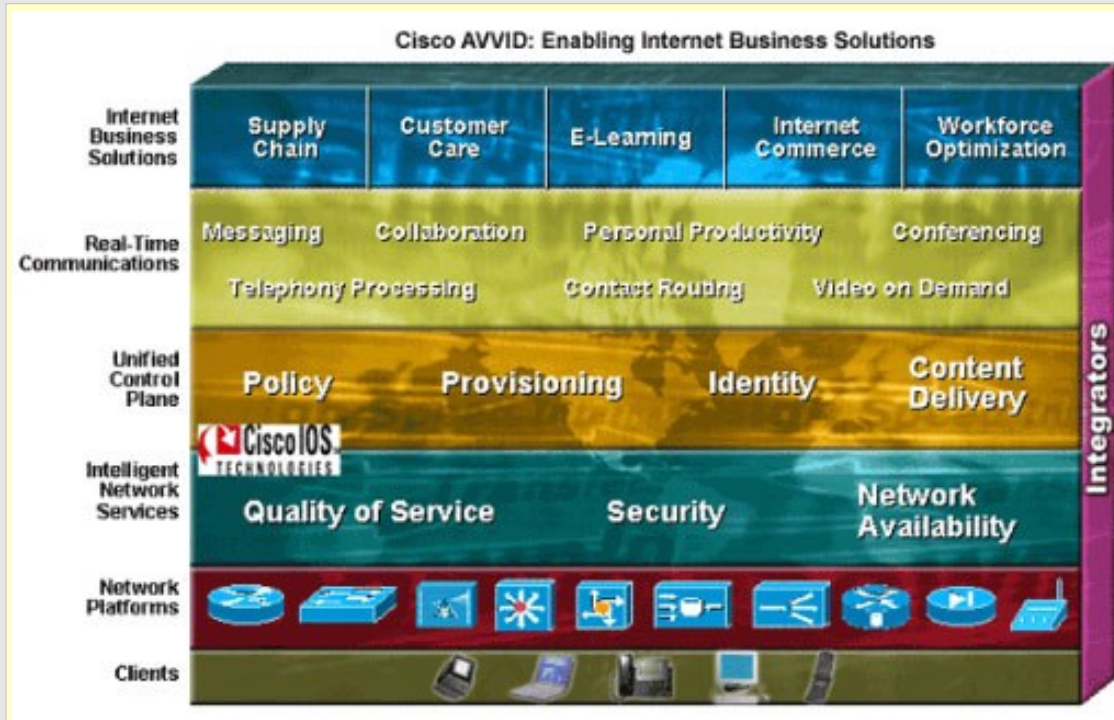


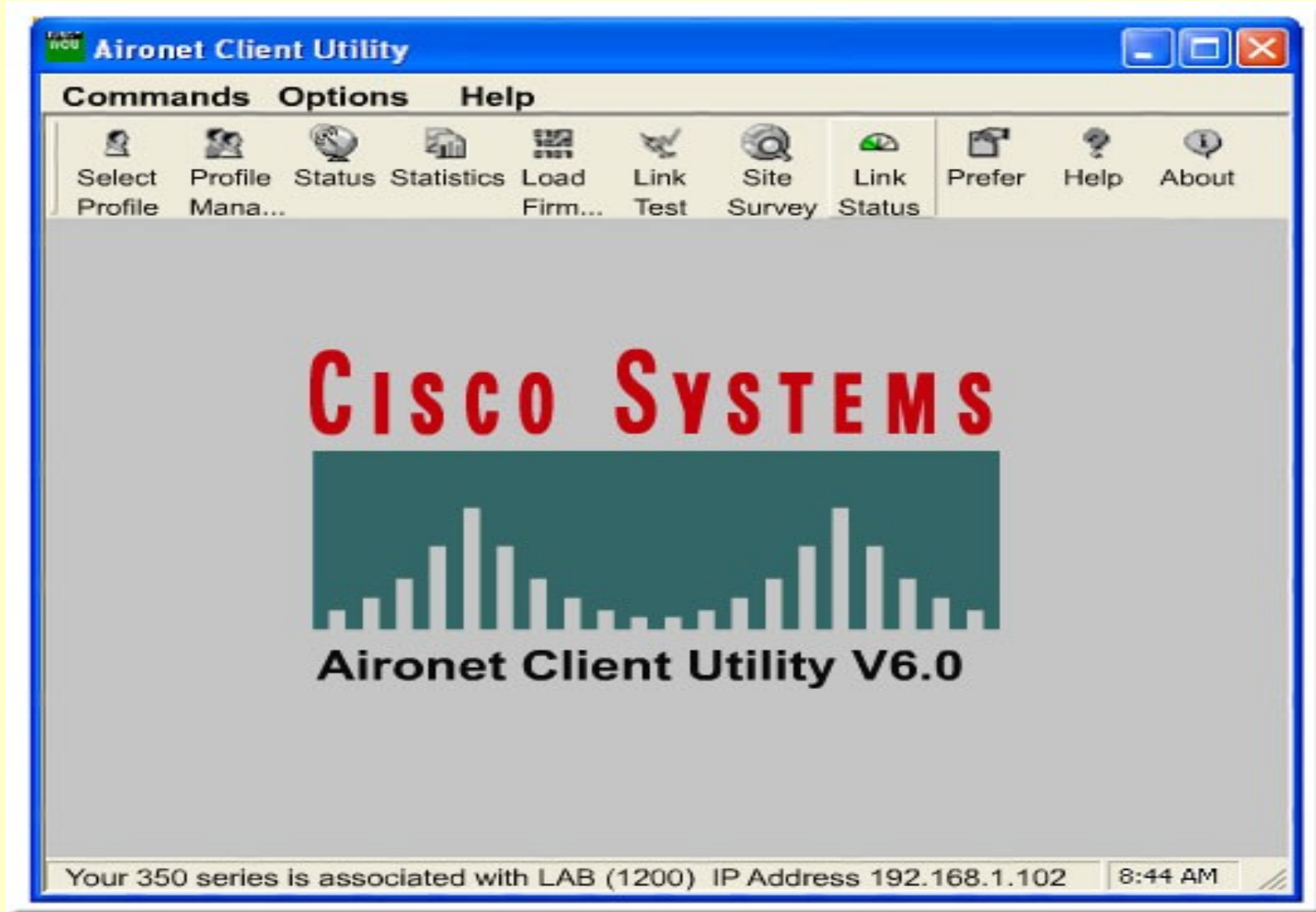
# WLAN: Servicios



César A. Cabrera E.

Ingeniero de Sistemas y Computación UTP  
Instructor Academia Regional de Networking UTP  
CCNP en proceso (BSCI)  
CISCO Certified Networking Associate (CCNA)  
CISCO Certified Academy Instructor (CCAI)  
----- [www.cesarcabrera.info](http://www.cesarcabrera.info) ----- Pereira, 2007 ---

# Configuración de Tarjeta CISCO



# Configuración de Tarjeta CISCO

350 Series Properties - [Office]

System Parameters | RF Network | Advanced (Infrastructure) | Network Security

Client name:

SSID1:

SSID2:

SSID3:

Power Save Mode:

- CAM (Constantly Awake Mode)
- Max PSP (Max Power Savings)
- Fast PSP (Power Save Mode)

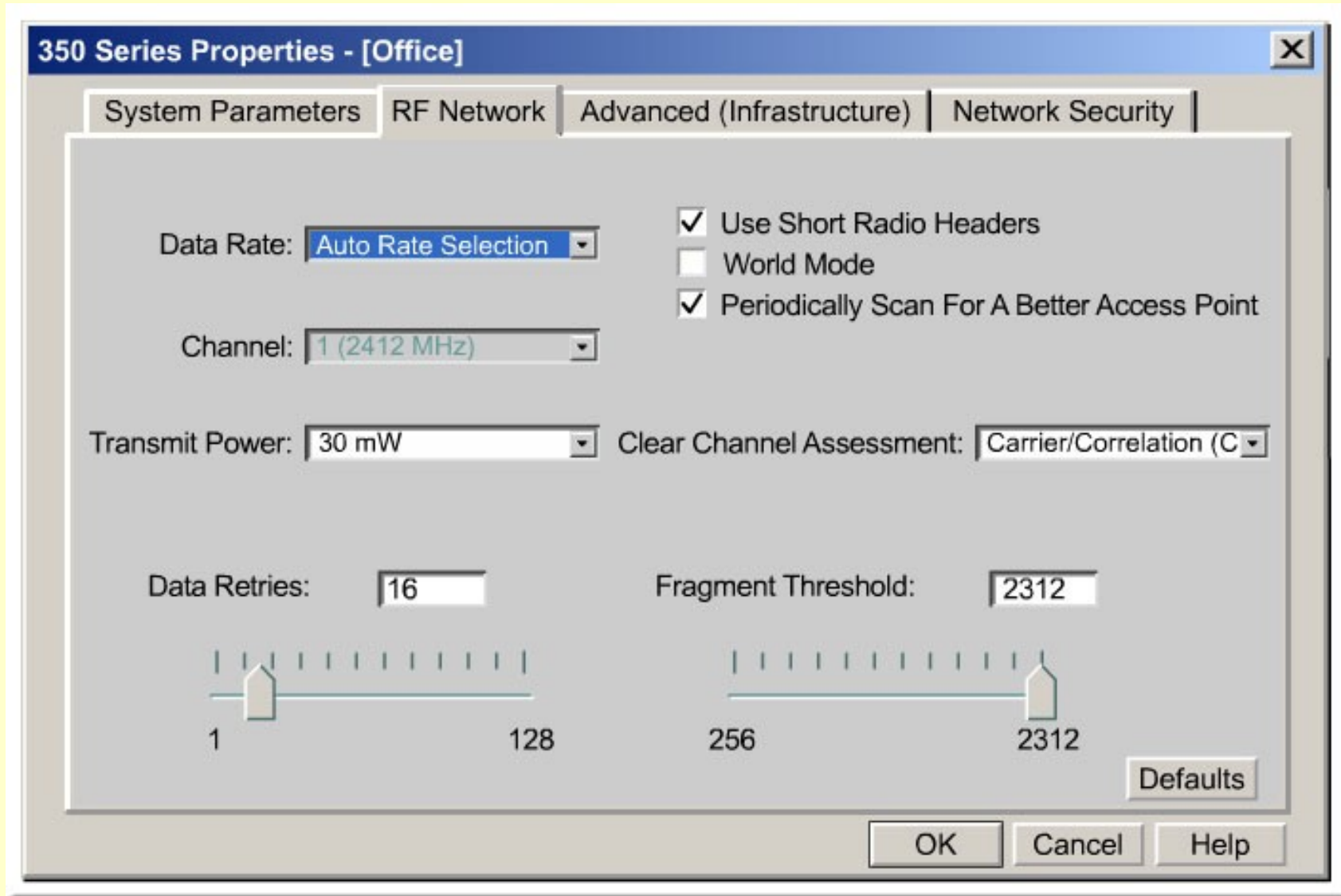
Network Type:

- Ad Hoc
- Infrastructure

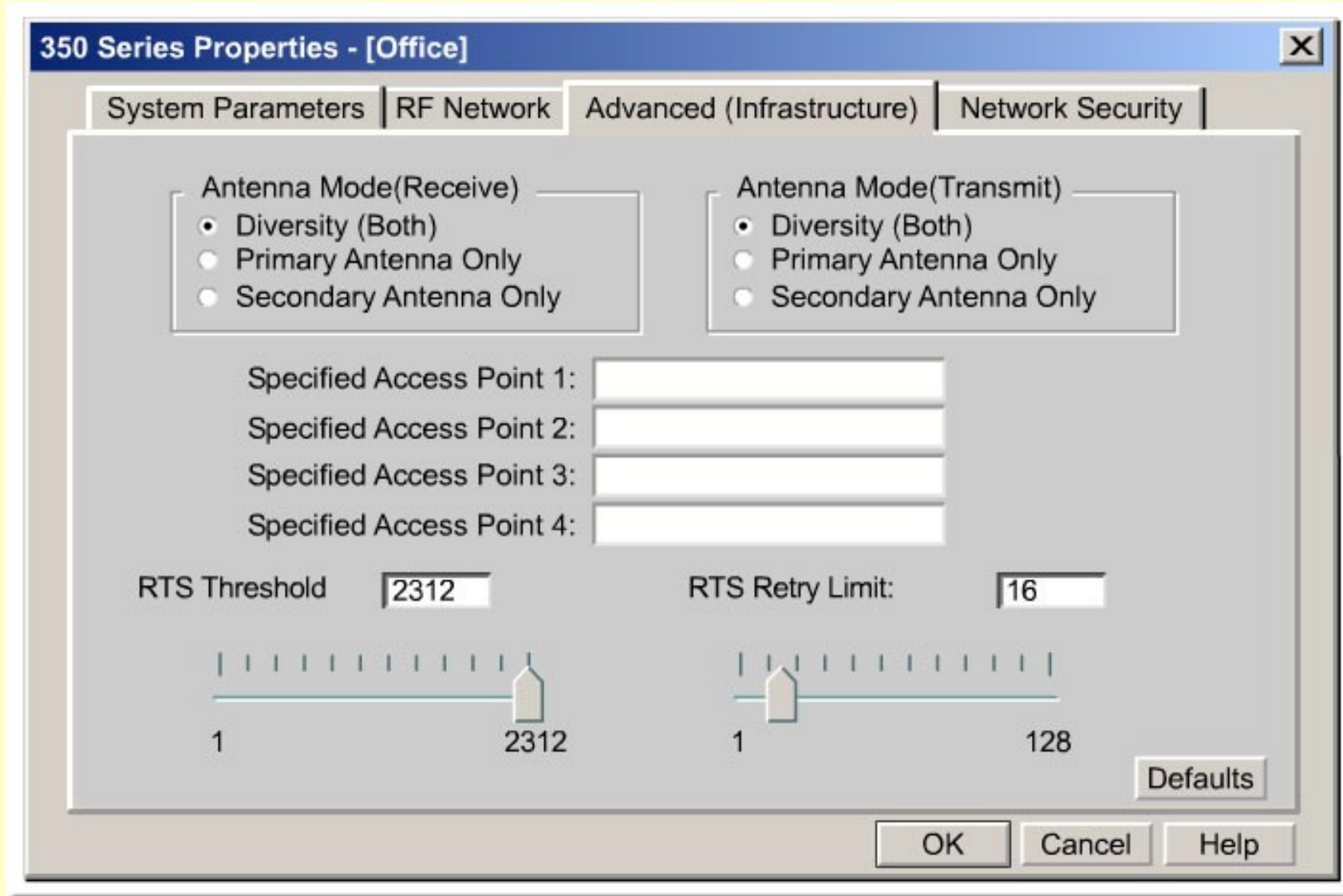
Defaults

OK Cancel Help

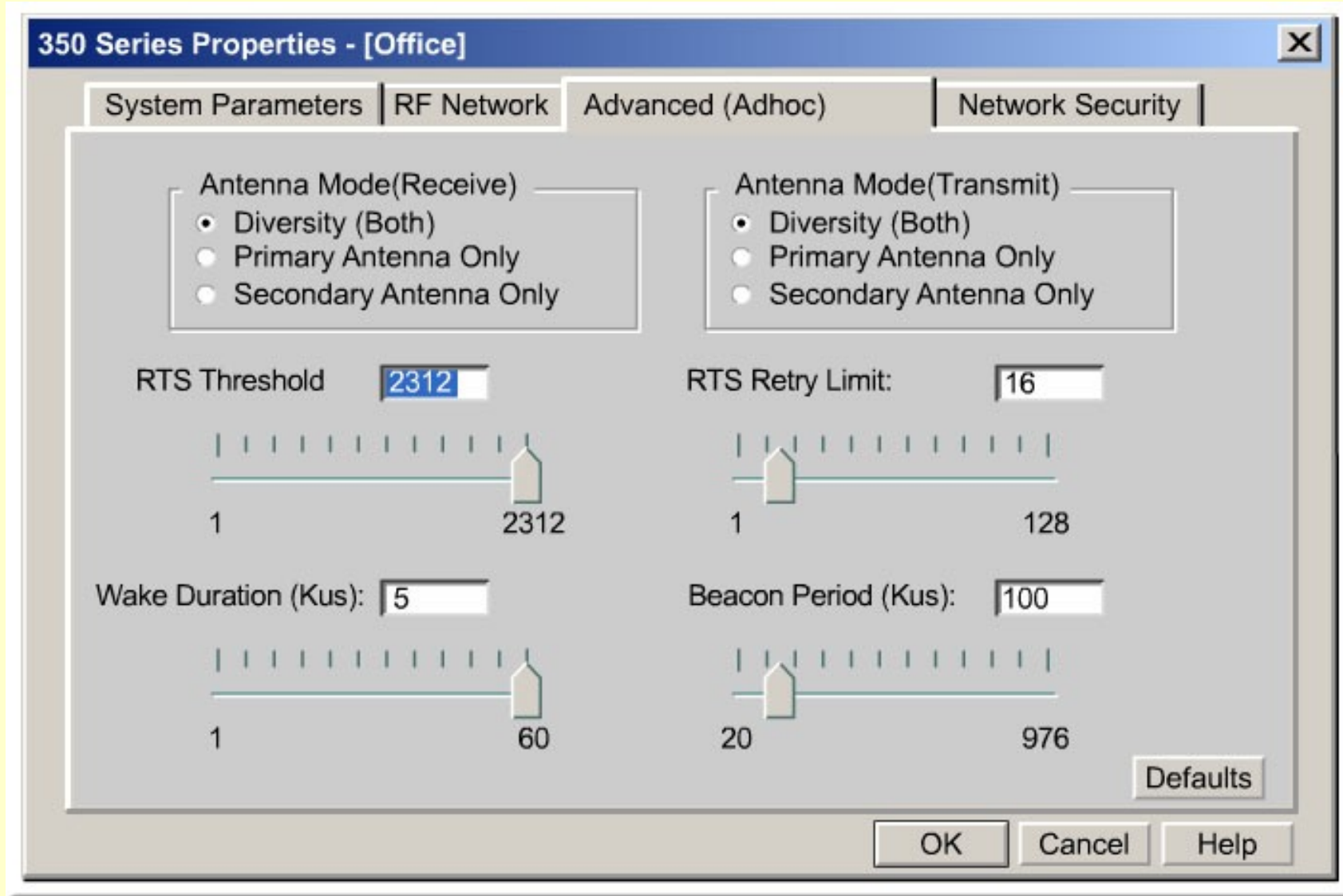
# Configuración de Tarjeta CISCO



# Configuración de Tarjeta CISCO



# Configuración de Tarjeta CISCO



# Configuración de Tarjeta CISCO

**350 Series Properties - [Office]**

System Parameters | RF Network | **Advanced (Infrastructure)** | Network Security

Network Security Type:

WEP:

- No WEP
- Use Static WEP Keys
- Use Dynamic WEP Keys

Static WEP Keys

WEP Key Entry Method:

- Hexadecimal (0-9, A-F)
- ASCII Text

Access Point Authentication:

- Open Authentication
- Shared Key Authentication

Already Set ?	Transmit Key	WEP Key Size
		40 128
<input checked="" type="checkbox"/> WEP Key 1:	<input checked="" type="radio"/>	<input type="radio"/> <input checked="" type="radio"/>
<input checked="" type="checkbox"/> WEP Key 2:	<input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/>
<input checked="" type="checkbox"/> WEP Key 3:	<input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/>
<input checked="" type="checkbox"/> WEP Key 4:	<input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/>

Allow Association to Mixed Cells

# AVVID: Architecture for Voice, Video and Integrated Data

Cisco AVVID: Enabling Internet Business Solutions



# SNMP: Simple Network Management Protocol

- Estándar de administración
  - Recuperar información estadística
  - Establecer parámetros de funcionamiento
  - Administración centralizada
  - Modelo de admin. Centralizada
  - Inseguro:
    - Versión 1 y 2 no encripta contraseñas, Versión 3 sí.
    - Los dispositivos que lo usan vienen con contraseñas por defecto
  - La mayoría del software administrativo se basa en ICMP y SNMP.

# Servicios por defecto

- HTTP
- FTP/TFTP
- CDP
- NTP
- Pequeños servicios TCP (echo, date, caracteres, etc.)
- ¿Por qué?: Porque la programación puede tener debilidades que bajo ataques pueden abrir huecos de acceso.

# Seguridad: Balance entre necesidades y riesgos

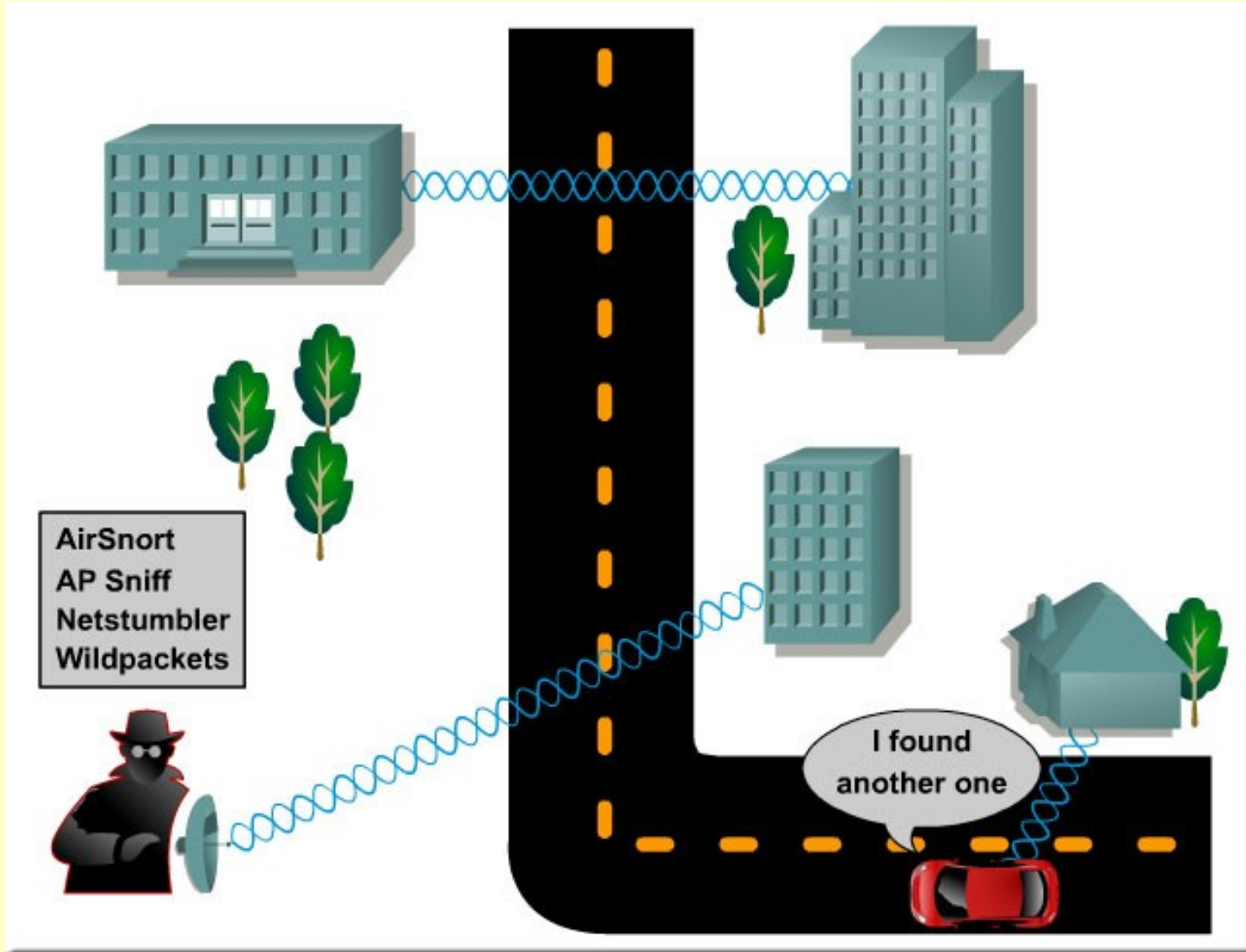
- Acceso transparente:
  - Conectividad
  - Desempeño
  - Facilidad de uso
  - Administrabilidad
  - Disponibilidad
- Seguridad
  - Autenticación
  - Autorización
  - Contabilización
  - Aseguramiento
  - Confidencialidad
  - Integridad de los datos

# Seguridad: Vulnerabilidades

Mecanismos previstos por el estándar:

- Autenticación débil de sólo dispositivo: No se autentica el usuario
- Encriptación de datos débil: WEP es un método débil de autenticación
- No integridad de mensaje: ICV (Integrity Check Value) es inefectivo para asegurar la integridad de los paquetes.

# Seguridad: Vulnerabilidades



# Seguridad: amenazas

## Clasificación de las amenazas

- No estructuradas/Estructuradas
  - Según sean intencionadas y con conocimiento de los sistemas.
- Internas/externas
  - Según provengan de personas con autorización de acceso o no.
- FBI: 60% a 80% de los reportes de violaciones de seguridad provienen de acceso interno o mal uso.

# Seguridad: Ataques

## Tipos de ataque

- Reconocimiento
- Ataque de acceso
- Denegación de servicio

# Ataques

## Reconocimiento

- Recolección de información de protocolos, servicios y topología de una red.
- Usualmente precede un ataque de denegación de servicio.
- Herramientas usadas:
  - Pasivas/Activas
  - Olfateadores (Sniffers/Eavesdropping)
- Se conoce con el nombre de wardriving

# Ataques

## Acceso

- Intrusión sin autorización.
- Permite instalar exploits o robar información.
- Explota contraseñas débiles o no existentes.
- Explota debilidades conocidas de servicios de la red (HTTP, FTP, SNMP, CDP, and Telnet)
- Rogue AP
- WEP: Encriptación débil, muchas debilidades bien documentadas (si bien muchas no han salido del laboratorio).

# Ataques

## **DoS: Denial of Service -Denegación de servicios-**

- Deshabilitar o corromper los servicios.
- Generar tráfico indeseado o interferencia.
- Reservar recursos no usados a una tasa más alta de la que se liberan.
- Ataque más temido:
  - No se necesita autorización previa, sólo una vía de acceso.
  - Es fácil de llevar a cabo (cualquier dispositivo a 2.4/5GHz puede ser usado para enviar paquetes de desasociación).

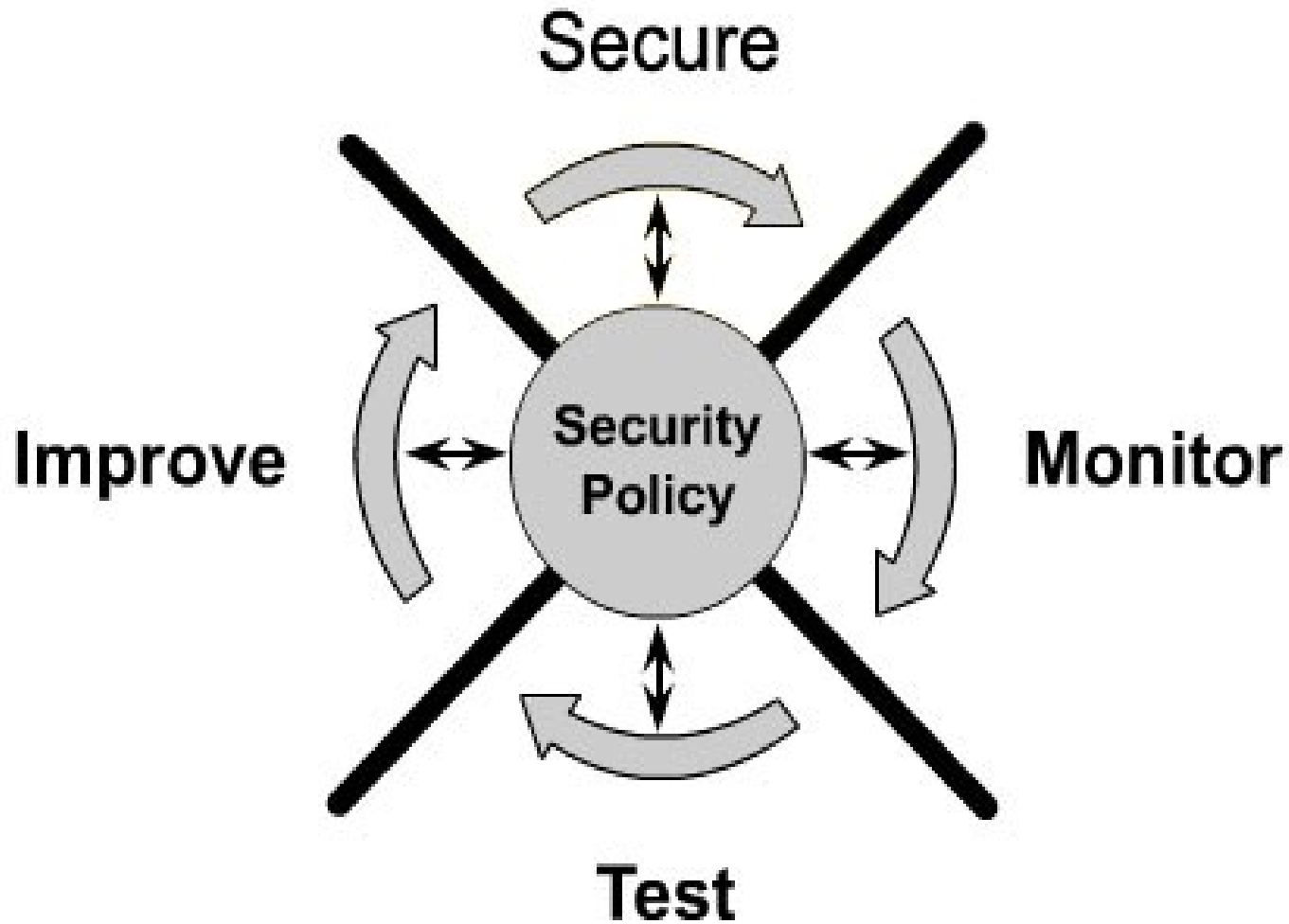
# Ciclo de aseguramiento de red

- Desarrollar una política de seguridad
  - Mapear los dispositivos a proteger, priorizar, documentar.
- Ventajas de una buena política de seguridad
  - Provee proceso de auditoría
  - Provee un marco general para la implementación de más políticas
  - Define claramente lo que se puede o no hacer
  - Ayuda a determinar herramientas y procedimientos
  - Cohesiona a los cuadros directivos y define responsabilidades
  - Define procesos de administración de violaciones
  - Crea la base para acción legal.

# Ciclo de aseguramiento de red

- **Asegurar**
  - Establecer autenticación, autorización y contabilización
  - Definir funciones y ubicación de Firewalls
  - Definir VPNs
  - Parchar los sistemas contra vulnerabilidades
  - Detección de intrusos
- **Monitorear**
  - Auditar, Detección de intrusos en tiempo real, validar el aseguramiento inicial
- **Probar**
  - Validar efectividad de las políticas: auditoría y exploración de vulnerabilidades
- **Mejorar**
  - Ajustar las políticas y medidas a los riesgos encontrados

# Ciclo de aseguramiento de red



Ciclo repetitivo y permanente de ajuste y definición de políticas

# Reomendaciones CISCO

- Autentique la administración de todos los dispositivos
- Use contraseñas difíciles de adivinar (un patrón)
- No deje claves por defecto en ningún dispositivo o protocolo (SNMP)
- Deshabilite cualquier servicio o protocolo no esencial para la operación del dispositivo
- Limite el tráfico administrativo a una subred y VLAN
- Encripte cualquier tráfico administrativo
- Use encriptación de tramas si es posible.

# Seguridad inalámbrica de primera generación

- SSID: 1 a 32 Caracteres ASCII que deben coincidir para establecer el enlace.
  - La mayoría de los APs tienen la opción de difundir SSID
- Filtrado por MAC: Permitir la asociación sólo a las MAC de clientes autorizados
  - La MAC se puede falsear (phishing).
  - El filtrado por MAC se debe considerar como medida de seguridad complementaria.
- WEP: Wired Equivalent Privacy

# Seguridad inalámbrica de primera generación

- WEP
  - Encripta el contenido para que si es interceptado no sea visible.
  - Es necesario que coincida tanto en la estación como en el AP.
  - Encriptación con una clave de 40/128Bits
  - Usa encriptación simétrica (RC4)
  - Las claves son estáticas (manuales y no cambian durante la sesión).

# Seguridad: Autenticación

- La autenticación es un proceso administrativo previo al envío de datos.
- Una vez la estación se autentica, queda asociada al AP
- Dos tipos:
  - Open: Autenticación en texto plano (sin encriptar), la estación se asocia así no coinciden las claves WEP.
  - Shared: Usa las claves WEP para realizar la autenticación, la asociación no ocurre si no coinciden las claves WEP.

# Seguridad: Autenticación

- Solución a corto plazo: Mejoras en WEP (WPA/SSN)
- Solución a más largo plazo: 802.11i
- Seguridad de segunda generación:
  - Autenticación centralizada basada en usuarios
  - WEP Dinámico de 128 bits
  - VPNs
  - Listas de control de acceso

# Seguridad: Debilidades de WEP

- Autenticación
  - Basada en dispositivos no en usuarios
  - Estaciones no autentican la infraestructura
  - No se apoya en bases de autenticación existentes
- Administración de claves
  - Claves estáticas
  - Claves compartidas entre múltiples AP
  - Todos los APs y STAs deben configurarse manualmente
- Algoritmo de encriptación débil y no verifica integridad del paquete

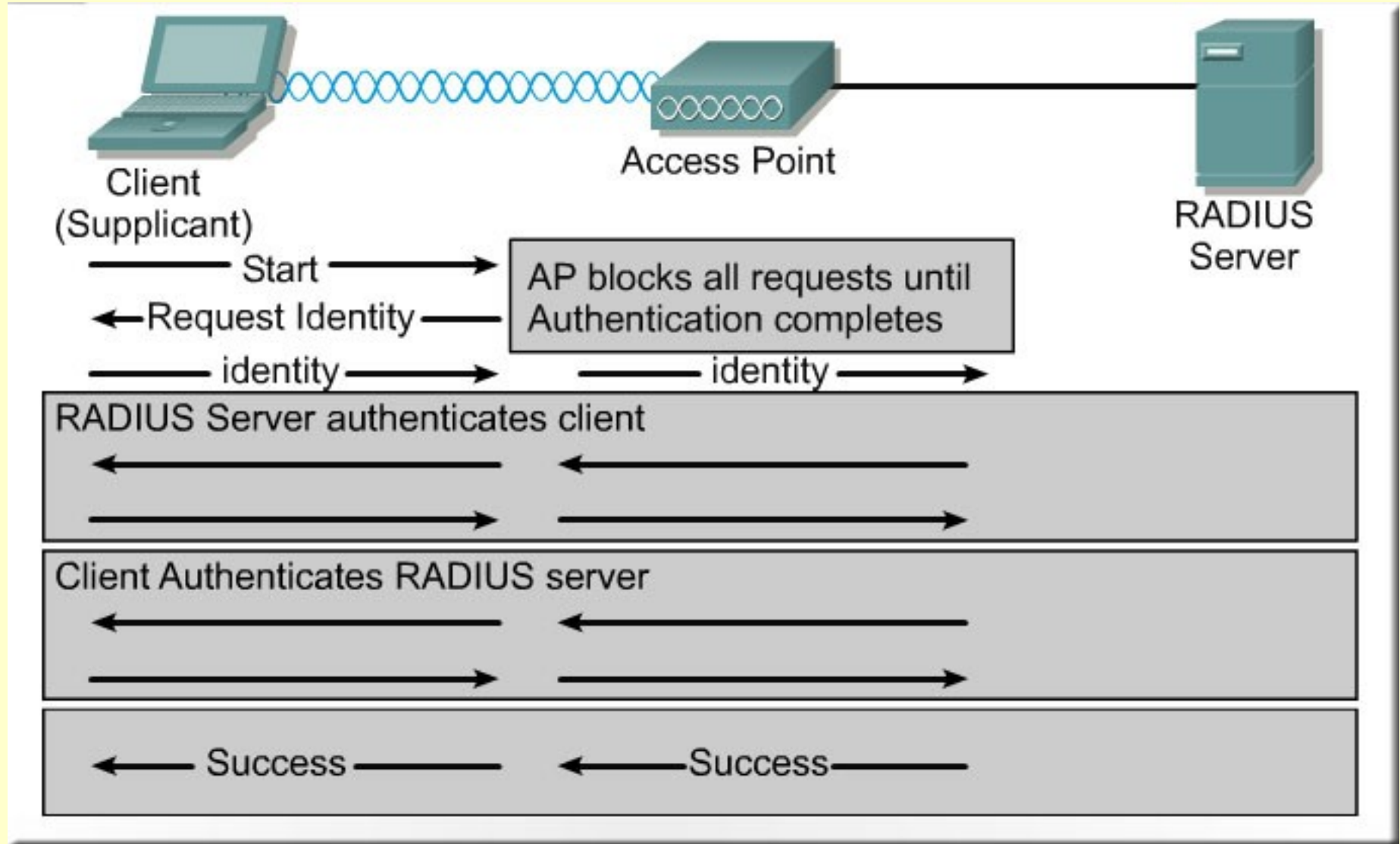
# Seguridad: Debilidades de WEP

- La seguridad depende de los requerimientos del cliente: se puede instalar las mejoras de WEP o se puede esperar 802.11i
- 802.11x:
  - Permite autenticar contra servidores de autenticación centralizados
  - Hace parte del estándar 802.11i
  - Usa encriptación e integridad de trama durante la autenticación
  - Si la STA no soporta 802.11x debe instalar un *supplicant*
  - Se usa en la Universidad

# Seguridad: Mejoras a WEP

- TKIP: Usa encriptación dinámica usando las mismas claves WEP configuradas
- MIC -Message Integrity Check-: Evita ataques de bit-flip, garantizando que el paquete sí es enviado por quien dice ser.
- BKR -Broadcast key rotation-: Evita que se envíe un broadcast rotando las claves WEP

# 802.11x



# 802.11x

- Usa diferentes esquemas de autenticación basados en EAP (Extensible Authentication Protocol)
  - LEAP: Light EAP o CISCO EAP, ideal para entornos Windows con Active Directory.
  - EAP-TLS: Infraestructura y STAs, Usa certificados digitales.
  - PEAP: Infraestructura y STAs, usa certs.
  - EAP-SIM

# Seguridad inalámbrica de segunda generación

- AES -Advanced Encryption Standards
- AES es un estándar (FIPS) de Procesamiento de información en EUA.
- Requiere hardware adicional.
- Sucesor del actual estándar recomendado por NIST -National Institute Standards in Technology-.

# VPNs: Virtual Private Networks

- Usa IPSec
- Asegura Confidencialidad, integridad y autenticidad de la información en Internet.
- IPSec tiene procedimientos para establecer túneles a través de WLANs, por lo tanto se puede filtrar el tráfico para permitir sólo tráfico de VPNs.
- Filtro: permitir sólo IKE/ESP -Encapsulated Security Payload-.

# VPNs: Virtual Private Networks

## Step 1: Association Process

Wireless LAN Client authenticates and associates with the access point

## Step 2: IPsec Tunnel

(1) Client obtains IP Address via DHCP request

(2) Layer 3 tunnel is set up and authenticated with VPN gateway using IKE

## Step 3:



User Authentication using OTP

## Step 4: User IP Traffic Flow

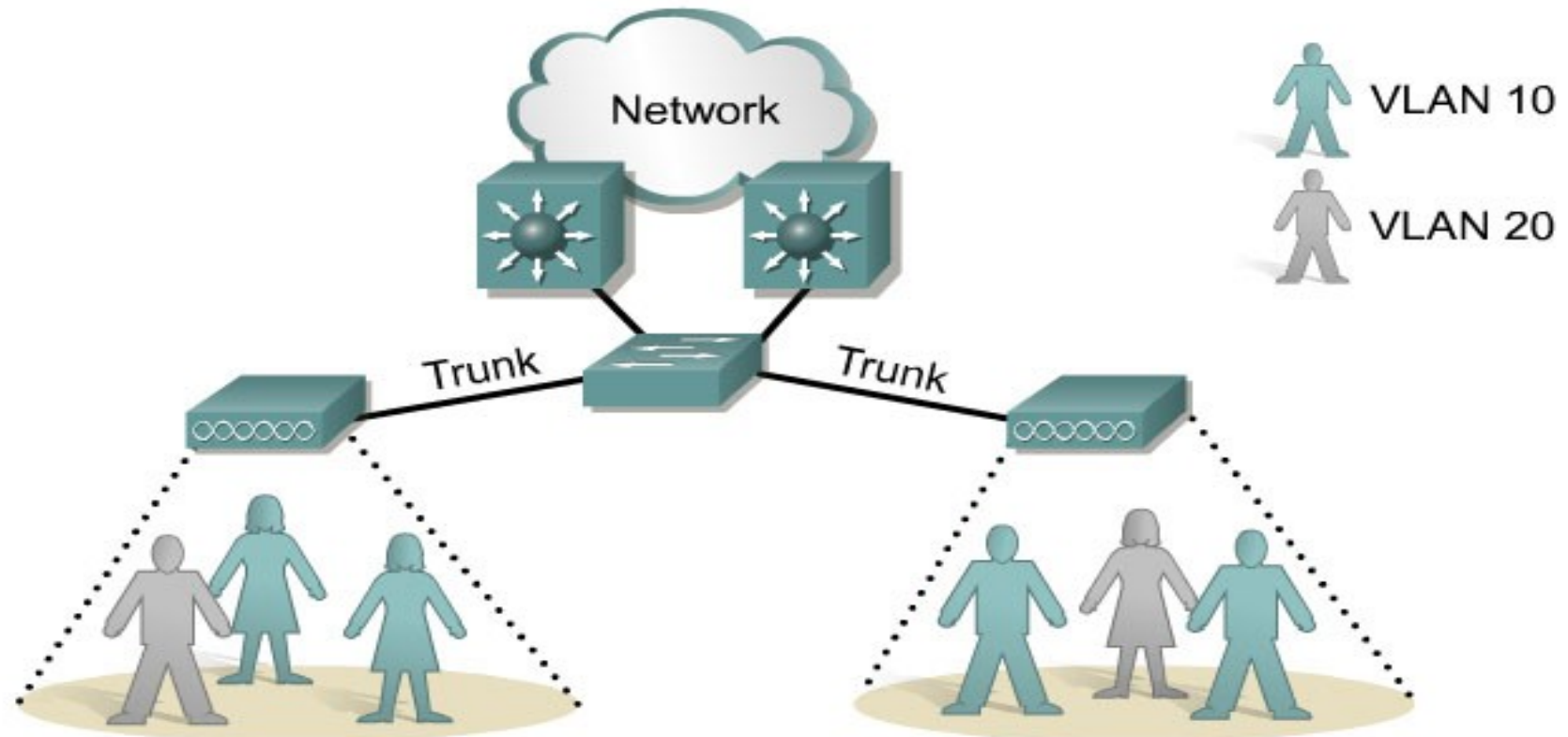
Clients software uses the IPsec ESP tunnel with the VPN gateway to pass IP traffic over the wireless LAN



# VPNs: Virtual Private Networks

- El primer y mínimo elemento de seguridad es vincular VLANs y SSIDs
- Ventajas de las VLANs:
  - Segmentación de la LAN
  - Más Seguridad
  - Control de Broadcasts
  - Mejor Desempeño
  - Mayor administrabilidad
  - Control de la comunicación entre VLANs

# VPNs: Virtual Private Networks



## Enterprise Services: VLANs

- Cisco provides for up to 16 separate VLANs, each with a different SSID
- May be statically or dynamically configured from a RADIUS server, may be mapped to 802.1Q VLANs on switches
- Supports different encryption levels and authentication types on individual segments

# Bitácora/Registro de eventos

- Cada dispositivo es configurable sobre qué eventos registrar y cómo hacerlo.
- Por defecto: registrar eventos graves en la consola del sistema.
- Bitácora centralizada con controla de alertas

# Syslog

- Servidor de registro
- C/dispositivo se configura para enviar la información al servidor (con la IP)
- Diferentes SW para registro (Pueden registrar SNMP).
- Niveles de registro:
  - Emergencia
  - Alerta
  - Crítico
  - Error
  - Advertencia
  - Notificación
  - Información
  - Depuración

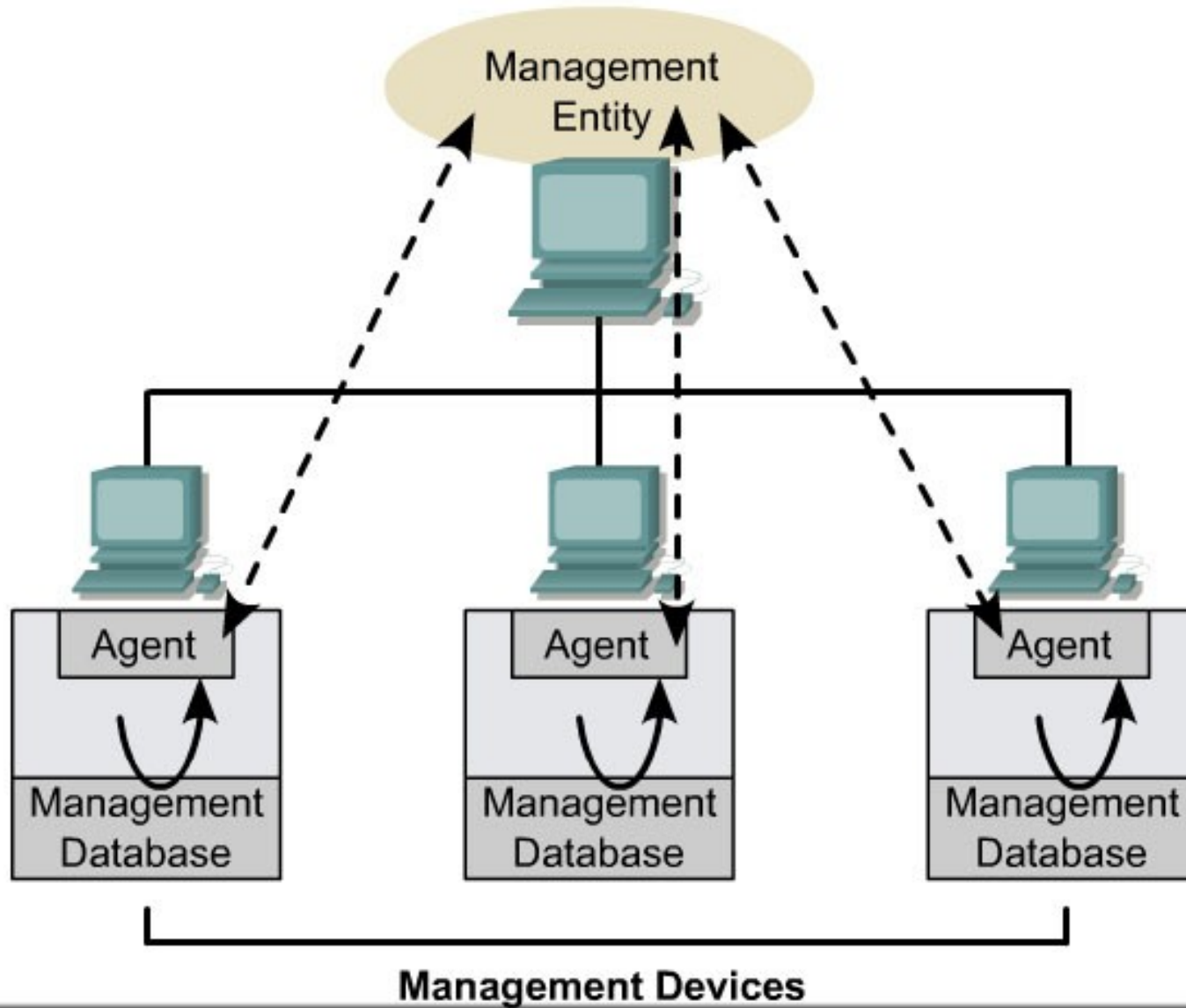
# Syslog

Program	Program	Web Site
Windows	Kiwi	<a href="http://www.kiwisyslog.com">http://www.kiwisyslog.com</a>
	WinSyslog	<a href="http://www.winsyslog.com">http://www.winsyslog.com</a>
	SolarWinds.Net	<a href="http://www.solarwinds.net/">http://www.solarwinds.net/</a>
Macintosh	Netlogger	<a href="http://www.laffeycomputer.com/netlogger.html">http://www.laffeycomputer.com/netlogger.html</a>
Unix	Syslogd	<a href="http://www.classicalguitar.net/brian/apps/syslogd">http://www.classicalguitar.net/brian/apps/syslogd</a>

# SNMP

- Estándar de administración de la industria
- Inseguro
- Elementos:
  - Dispositivos administrados
  - Agentes
  - Estación de administración (NMS -N. Man. Sys.)
- MIB, Trap, Community, lectura/escritura
- Versión 3 no muy difundida

# SNMP



# SNMP

## Applications that Manage SNMP

### Windows

- 3COM Transcend Network supervisor
- BTT Software SNMP Trap Watcher
- Accton AccView/Open (SW6102)
- Lorient

### Macintosh

- Dartware SNMP Watcher

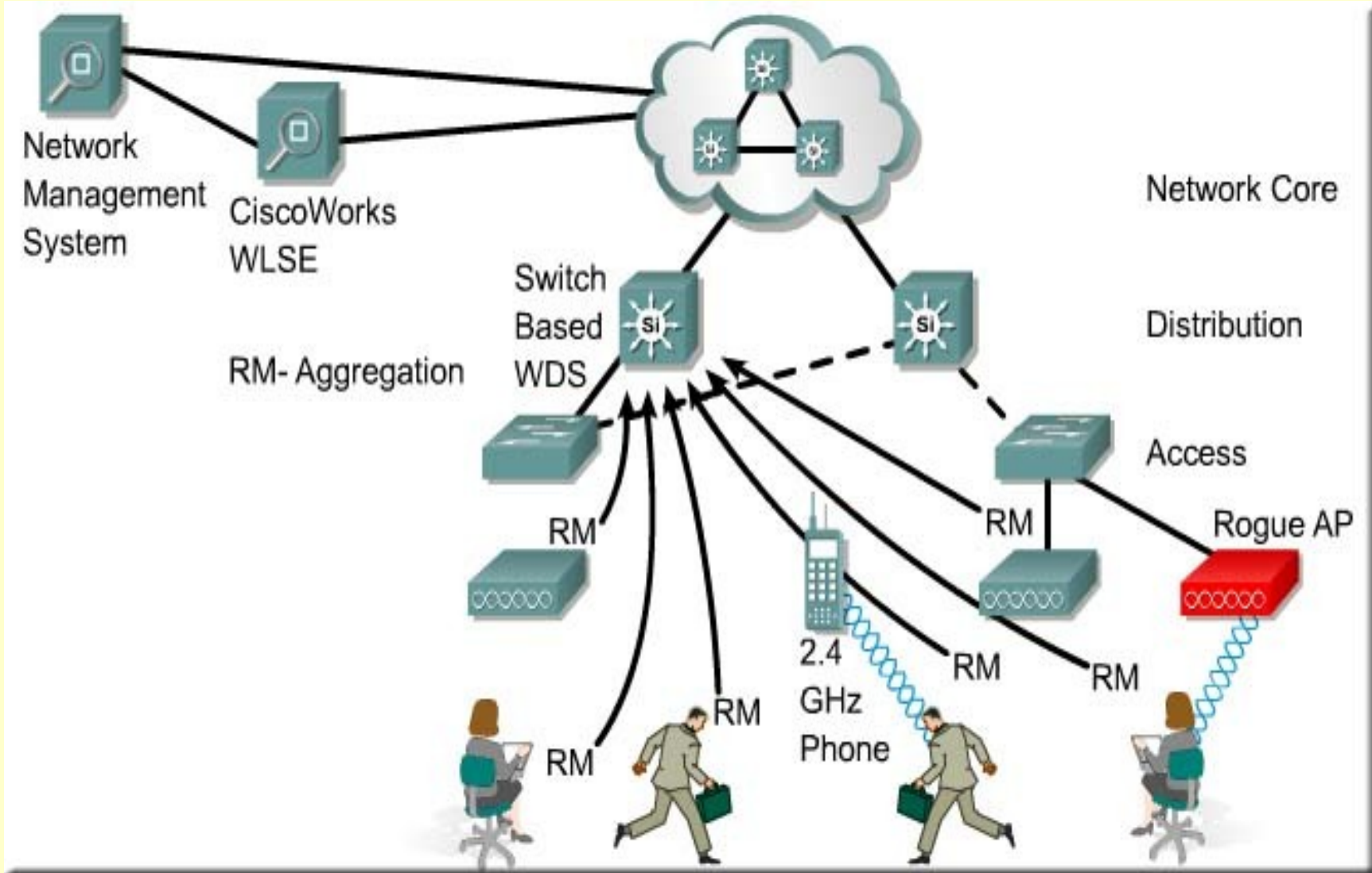
### Linux

- snmptraplogd 1.0-6.1
- NET-SNMP
- Multi Router Traffic Grapher (MRTG)

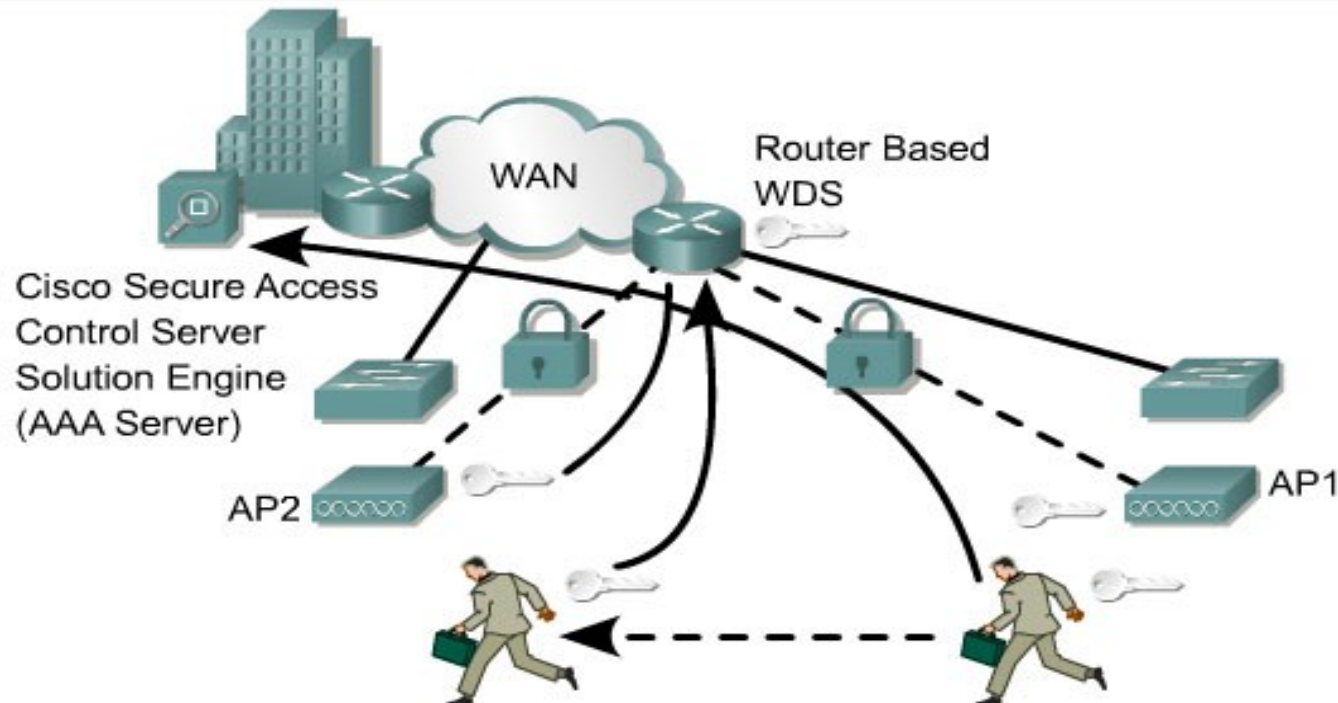
**Also, there are a wide variety of retail packages that include the following:**

- CiscoWorks (CiscoView)
- Solarwinds Professional
- HP Openview

# WLSE: WireLess Solutions Engine



# WDS: Wireless Domain Server



**Note:** Because the WDS handles roaming and reauthentication, the WAN link is not used

1. Access Point must now 802.1X authenticate with the WDS Access Point (AP1) to establish a secure session
2. Initial client 802.1X authentication goes to a central AAA server (-500ms)
3. During a client roam, the client signals to the WDS it has roamed and WDS will send the client's key to the new Access Point (AP2)
4. The overall roam time is reduced to <150ms, and in most cases, <100ms

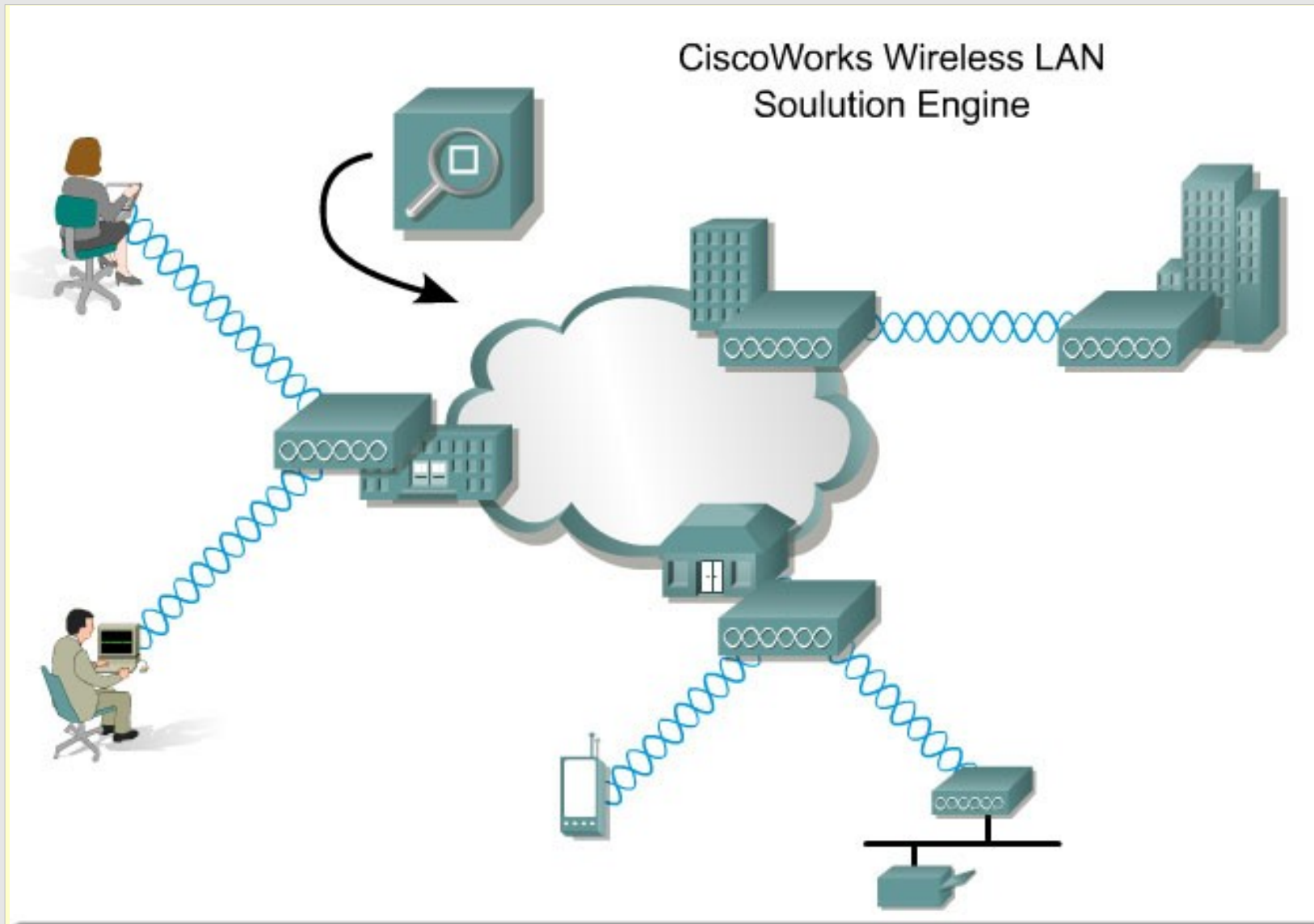
# WDS: Wireless Domain Server

- Se selecciona un AP que sirva de WDS en la red inalámbrica.
- El WDS Autentica tanto a los dispositivos clientes como a los de infraestructura
- Se pueden configurar varios como respaldo estableciendo prioridades de servicio

# WLSE: Wireless LAN Solutions Engine

- Dispositivo (Appliance) de administración, monitoreo y seguridad de redes inalámbricas
- CISCO 1105/1130
- Envía verificación de seguridad a intervalos configurables para detectar vulnerabilidades en toda la red inalámbrica
- Soporta hasta 2500 Aps
- Para mercados verticales como servicios financieros, salud, gobierno, educación y manufactura

# WLSE: Wireless LAN Solutions Engine



# WLSE: Wireless LAN Solutions Engine



- Administración remota por Web usando HTTPS
- Configuración de dispositivos basado en plantillas
- Monitorea las políticas de seguridad y genera alertas cuando hay cambios no autorizados
- Interopera con aplicaciones de administración basadas en Syslog y SNMP y genera notificaciones por email
- Exporta datos en XML, PDF y CSV
- Administra la actualización del firmware de los dispositivos



# Otras alternativas de admin

- ACAT: Generación de archivos de actualización para los usuarios.
- Wavelink Mobile Manager: Aplicación comercial multivendedor
  - Administración
  - Servicio de alertas
  - Agente remoto (Configuración por plantillas, razonamiento basado en reglas)
  - Servicios remotos (actualización y restauración de firmware)
- Airwave: Aplicación comercial multivendedor
  - Soporta de 25 a 500 dispositivos de marcas como CISCO, OriNOCO (Agere/Proxim) Symbol, Intel, HP/Compaq, Dell, Avaya y 3e Technologies International