Seguridad en Redes Wireless

RAUL BAREÑO GUTIERREZ

INTRODUCCION

- Conceptos y funcionamiento de redes Wireless
- Seguridad en 802.11
- Ataques típicos a redes Wireless basadas en 802.11
- Técnologías Wireless Seguras: WPA, WPA2, 802.11i
- Cómo montar una red Wireless Segura

Introducción

- **Las Wireless LAN se están convirtiendo poco a poco en parte esencial de las redes LAN tradicionales:**
  - Bajos costes de instalación
  - Disponibilidad
  - No requiere de software adicional
  - Movilidad

- **La implantación se esta realizando a mayor velocidad en los entornos domésticos y PYMES que en las grandes empresas**

- **Este mercado esta menos consciente de los problema de seguridad**
  - El aire es un medio inseguro.
  - Los estándares iniciales tienen muchos problemas de seguridad.

Introducción: IEEE 802.11

- Estándar de la IEEE: frecuencias de 2.4 a 5 GHz
- **802.11:** 1 a 2 Mbps a 2.4GHz
- **802.11a:** 54 Mbps a 5GHz
- **802.11b:** 11Mbps a 2.4GHz
- **802.11g**: 54 Mbps a 2.4GHz
- Además: d (Cambios de MAC), e (QoS), j (Japón), n (x4, x8) ...
- Cada fabricante implementa sus propias soluciones para mejorar el rendimiento en la transferencia de datos. (208 Mbps)

D-Link Air

AirPlus XTREME G

Componentes

- **Routers/Gateways, Puntos de acceso (AP), Repetidores**
  - Equivalente al HUB de la tecnología ETHERNET.
  - Ojo, no es un Switch por lo que los usuarios comparten el ancho de banda total
- **Adaptadores WIFI**: PC Cards, PCI, Integradas, USB....
- **Antenas**: unidireccionales y omnidireccionales

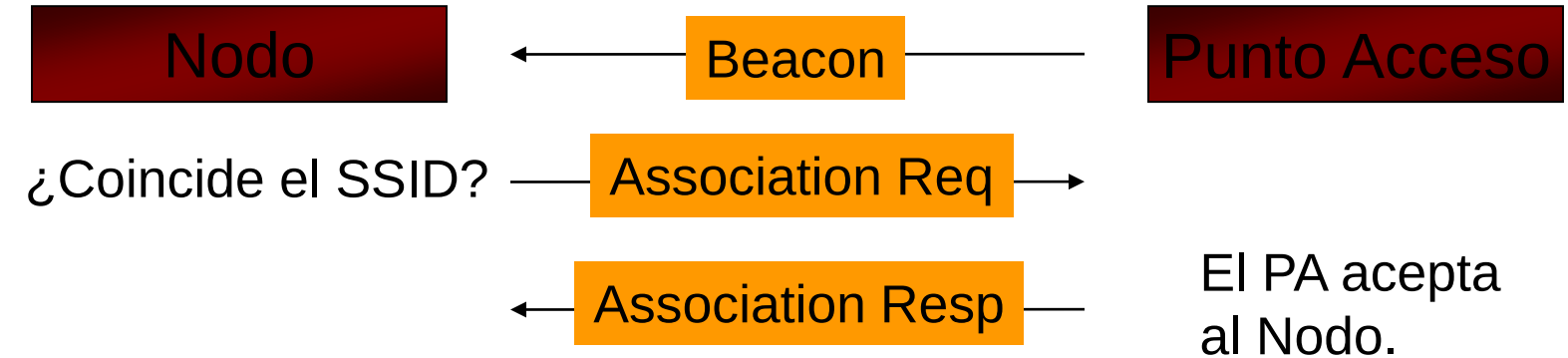
Conceptos:

- **Frecuencia:** de 2 a 5 GHz (Radio)
- **Canal:** Una porción del espectro de radiofrecuencias que usan los dispositivos para comunicarse. El uso de diferentes canales ayuda a reducir interferencias
- **BSSID (Basic Service Set Identifier):** Dirección única que identifica al Router/AP que crea la red Wireless. Tiene formato de MAC address
- **ESSID (Extended Service Set Identifier):** Nombre único de hasta 32 caracteres para identificar a la red wireless. Todos los componentes de la misma red WLAN deben usar el mismo.
- **SSID (Service Set Identifier):** Equivalente a ESSID

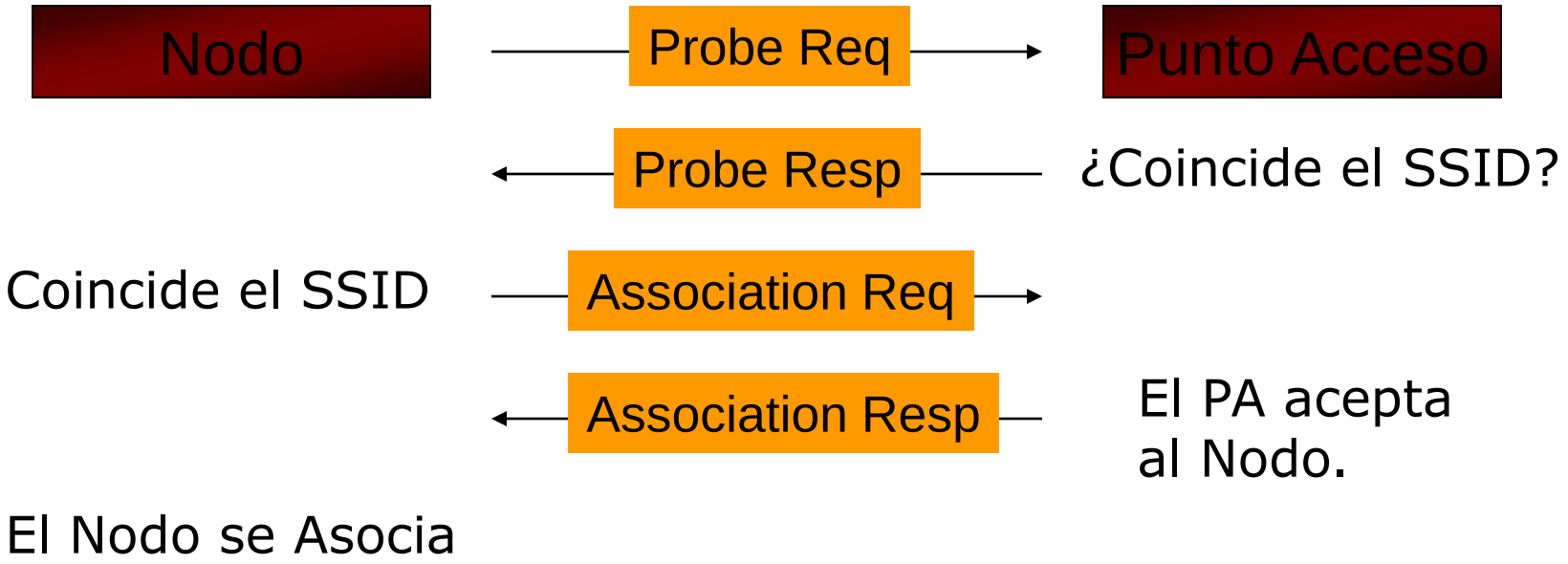
Funcionamiento (I)

- **Descubrimiento**: La estación ha de conocer la existencia del PA al que conectarse.
  - **Descubrimiento Pasivo**: Espera recibir la señal de PA
  - **Descubrimiento Activo**: La estación lanza tramas a un PA determinado y espera una respuesta
- **Autenticación**: La estación ha de autenticarse para conectarse a la red
- **Asociación**: La estación ha de asociarse para poder intercambiar datos con otras.
- **Cifrado**: Protección de los datos que se envían a través de la red.

Descubrimiento Pasivo



Descubrimiento Activo



Tipos de tramas Wireless

- **Tramas de Gestión:**
  - Ayudan a las estaciones a localizar y asociarse a PA disponibles.
  - Se transmiten igual que las demás pero no se envía a las capas superiores. Nivel 2
  - Tramas Baliza o “Beacon Frames” envían:
    - Sincronización horaria
    - Anchos de banda, canal, tipo de señal, etc..
    - SSID
  - Las redes que no emiten el SSID en las BFs se denominan “redes cerradas” (Requieren Descubrimiento Activo)
- **Tramas de Control:** para el control de acceso al medio.
- **Tramas de Datos:** para la transmisión de los datos

Seguridad IEEE 802.11

- **Inciso:** Autenticación, Cifrado, Firmado

- **Autenticación**

  - Open System Authentication
  - Shared Key Authentication (WEP)
  - Ambos permiten autenticación por filtrado de MAC

- **Encriptación e Integridad de datos**

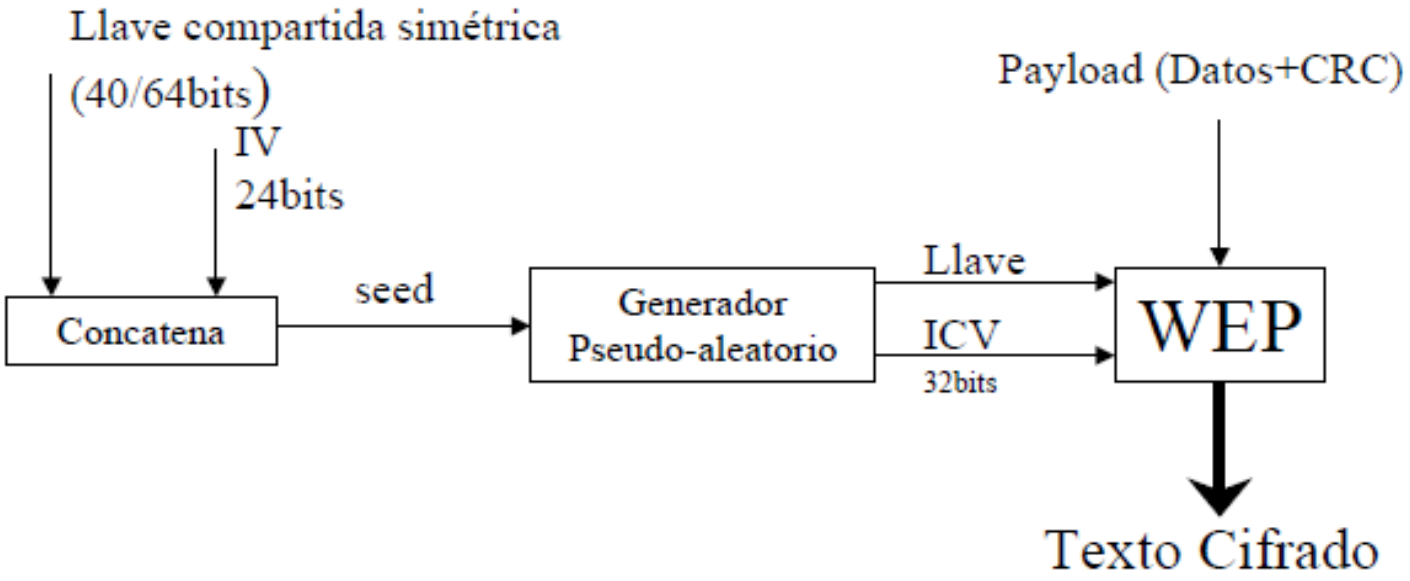
  - WEP (Wired Equivalent Privacy)
    - Usa un algoritmo RC4 de cifrado con claves de 40-bit o 104-bit
    - Calcula un ICV de 32-bit a partir de los datos a enviar
    - Genera un IV de 24-bit

- ¡Se usa el mismo secreto compartido tanto para autenticar (en el desafío/respuesta) como para encriptar!

WEP - Funcionamiento

- Concatena la **llave simétrica compartida**, de 40 o 64 bits, de la estación con un **vector de inicialización** aleatorio (**IV**) de 24 bits, esta estructura se denomina '**seed**'
- El **seed** se utiliza para generar un número pseudo-aleatório, de longitud igual al **payload** (datos + CRC), y un valor de 32 bits para chequear la integridad (**ICV**)
- Esta llave y el ICV, junto con el payload (datos + CRC), se combinan a través de un proceso XOR que producirá el texto cifrado
- La trama enviada incluye el texto cifrado, y el IV e ICV sin encriptar

WEP - Funcionamiento



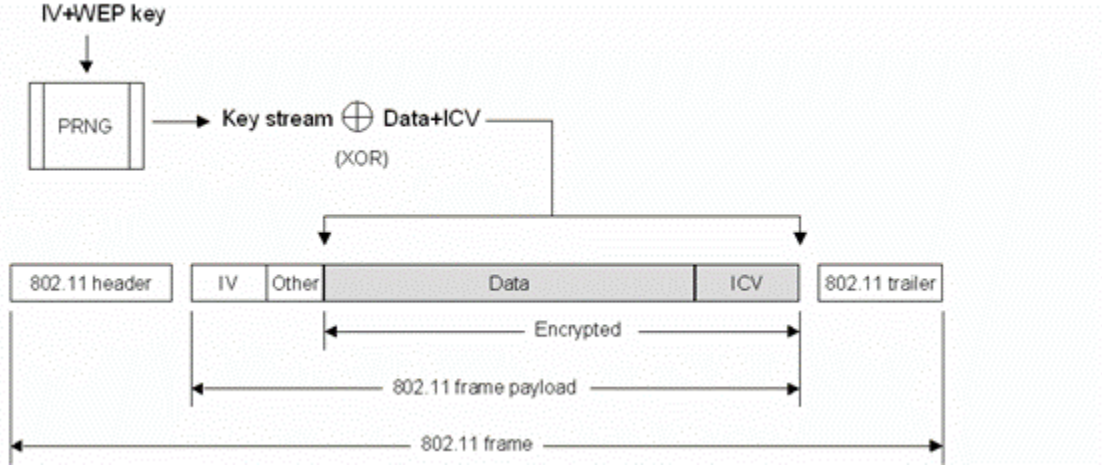
La trama enviada contiene el IV y el ICV sin encriptar junto al texto cifrado

WEP - Funcionamiento

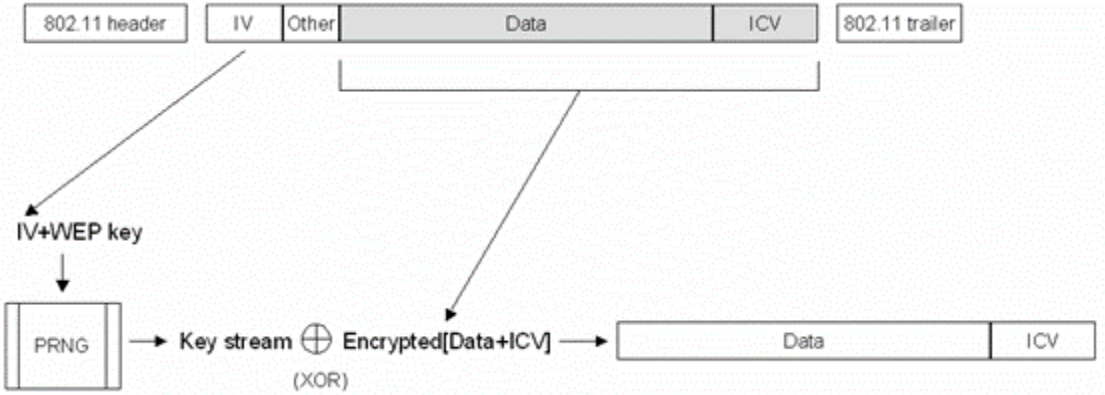
- El **ICV** actúa como checksum, será utilizado por la estación receptora para recalcularlo y compararlo con la recibida
- Si el **ICV** no concuerda con el ICV calculado, se descarta la trama e incluso al emisor de la misma
- El **IV** se utiliza para desencriptar, junto con la llave simétrica compartida, los datos y el CRC de la trama

Cifrado y descifrado WEP

- **Cifrado**



- **Descifrado**



Configuración insegura de una infraestructura Wireless

Disección de un Ataque a Redes Wireless 802.11

- Uso de herramientas para obtener el SSID oculto y tipo de cifrado
  - El cliente DEBE enviar el SSID para asociarse
  - Hay información disponible en las Beacon Frames
- Uso de Sniffers para averiguar canales de emisión y los BSSID y MAC address de clientes válidos:
  - El aire es de libre acceso
  - WEP cifra la información a nivel 3 (IP).
- Uso de herramientas que capturan tráfico de red y derivan la clave WEP a partir de una cantidad suficiente del mismo
  - El IV se repite y va sin cifrar
- Configuramos los parámetros del cliente de red Wireless con los datos recogidos y nos asignamos una MAC válida con una herramienta de spoofing

La raíz de los problemas de 802.11

- La clave WEP es compartida entre todos los clientes
- No se contempla la forma de distribuirla ni su cambio en el tiempo.
- ¡El estándar 802.11 especifica que cambiar el IV en cada paquete es opcional!. Y cada fabricante es libre de gestionarlo como quiera.
- Reutilización del IV
  - El IV es de 24-bit -> se repite cada 16.777.216 tramas!
- Debilidad de RC4
- El ICV es un CRC32 independiente del secreto compartido
  - Conocido el texto de una trama puede sacarse el de cualquiera sin conocer la clave WEP (bit-flipping)

- http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Crackearlas es “trivial”

Así es que con 802.11…

- "Rogue APs".
- DoS, ataques por Asociación/Disociación.
- Fácil monitorización.
- No extensible a otros métodos de autenticación.
  - Imposible autenticar por usuario o equipo
- No extensible a otros métodos de gestión de la clave compartida
- Hay que implementar nuevos mecanismos de Autenticación, Cifrado y Firmado

Tecnologías Wireless Seguras

Soluciones Wireless Seguras WPA y WPA2

- **WPA:** Certificación de la **WI-FI Alliance** para las soluciones Wireless que cumplan ciertos requisitos de seguridad. Surgió mientras se trabajaba sobre el estándar **IEEE802.11i**

- **WPA2:** Certificación de la **WI-FI Alliance** para las soluciones Wireless que cumplan los requisitos de seguridad dictados por **IEEE 802.11i**

Cambios requeridos por WPA y WPA2 (IEEE802.11i)

- **Autenticación**
  - WPA y WPA2:
    - Open System Authentication para la asociación
    - Para la autenticación mutua y del usuario:
      - Enterprise → 802.1X sobre 802.11
      - Personal → PSK (Pre-Shared Key) ¡Ojo!
- **Cifrado** e **Integridad de Datos**
  - WPA: TKIP (Temporary Key Integrity Protocol)
  - WPA2: AES (Advanced Encryption Standard), aka Counter Mode Cipher Block Chaining-Message Authentication Code (CBC-MAC) protocol (CCMP)

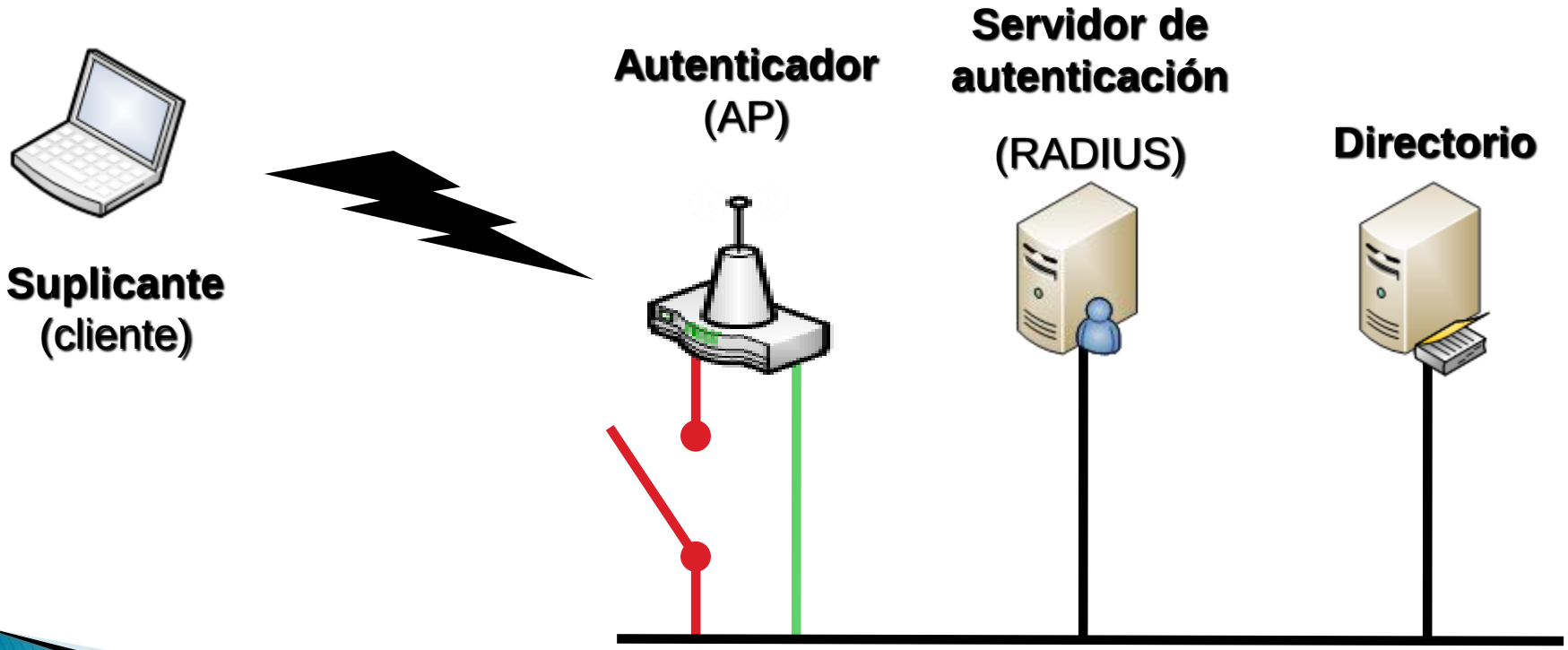
Autenticación 802.1X

- 802.1X surge como un método de autenticación de “puertos” en redes LAN

- Implementa un Protocolo de Autenticación Extensible (EAP) → Nivel 2
  - EAP fue diseñado originalmente para ser usado en PPP y adaptado por 802.1X para ser encapsulado y enviado en redes LAN o Wireless
  - No tiene seguridad “built-in”. Los protocolos de autenticación deben implementar sus propios métodos de seguridad. El método de autenticación es elegido por los equipos durante la negociación de forma transparente al AP

Roles de los “Puertos” en una Autenticación 802.1x

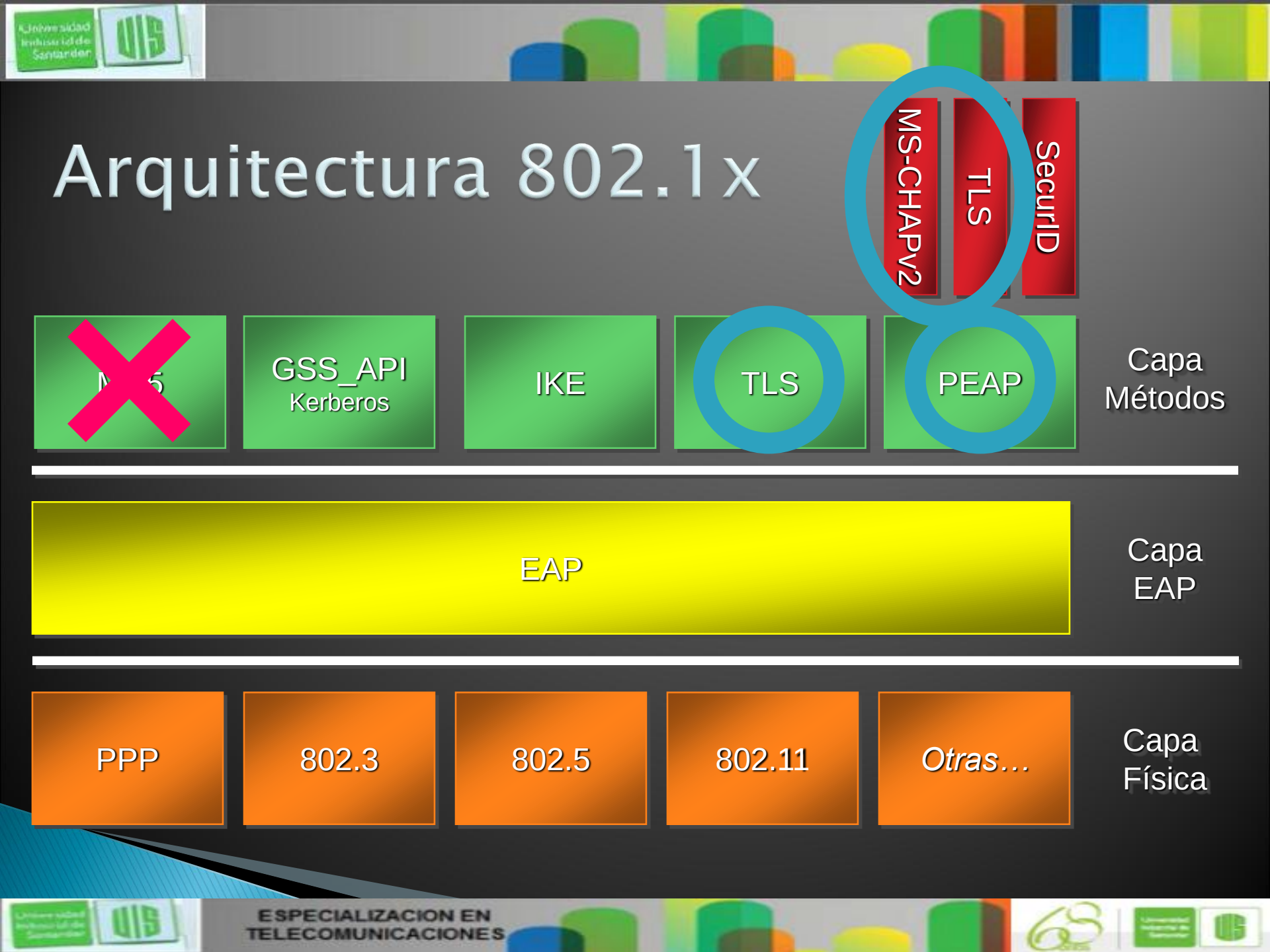
- Los puertos Controlados evitan el acceso del cliente a la LAN hasta que no se han autenticado correctamente
- Los puertos no controlados permiten al cliente contactar directamente con el servidor de autenticación



Métodos de Autenticación (EAP)

- EAP nos permite elegir virtualmente cualquier método de autenticación que queramos implementar
  - TLS: Transport Layer Security (certificados de cliente y servidor)
  - IKE: Internet Key Exchange
  - Kerberos
  - Otros (MD5, LEAP, etc.)
- PEAP: Protected Extensible Authentication Protocol. Evita que la conversación EAP vaya sin cifrar
  - Genera un canal TLS usando el certificado del servidor RADIUS
  - Posteriormente podemos implementar de nuevo un método EAP de autenticación mutua
    - MS-CHAP v2 (usuario y contraseña)
    - TLS (certificados de cliente y servidor)

Arquitectura 802.1x

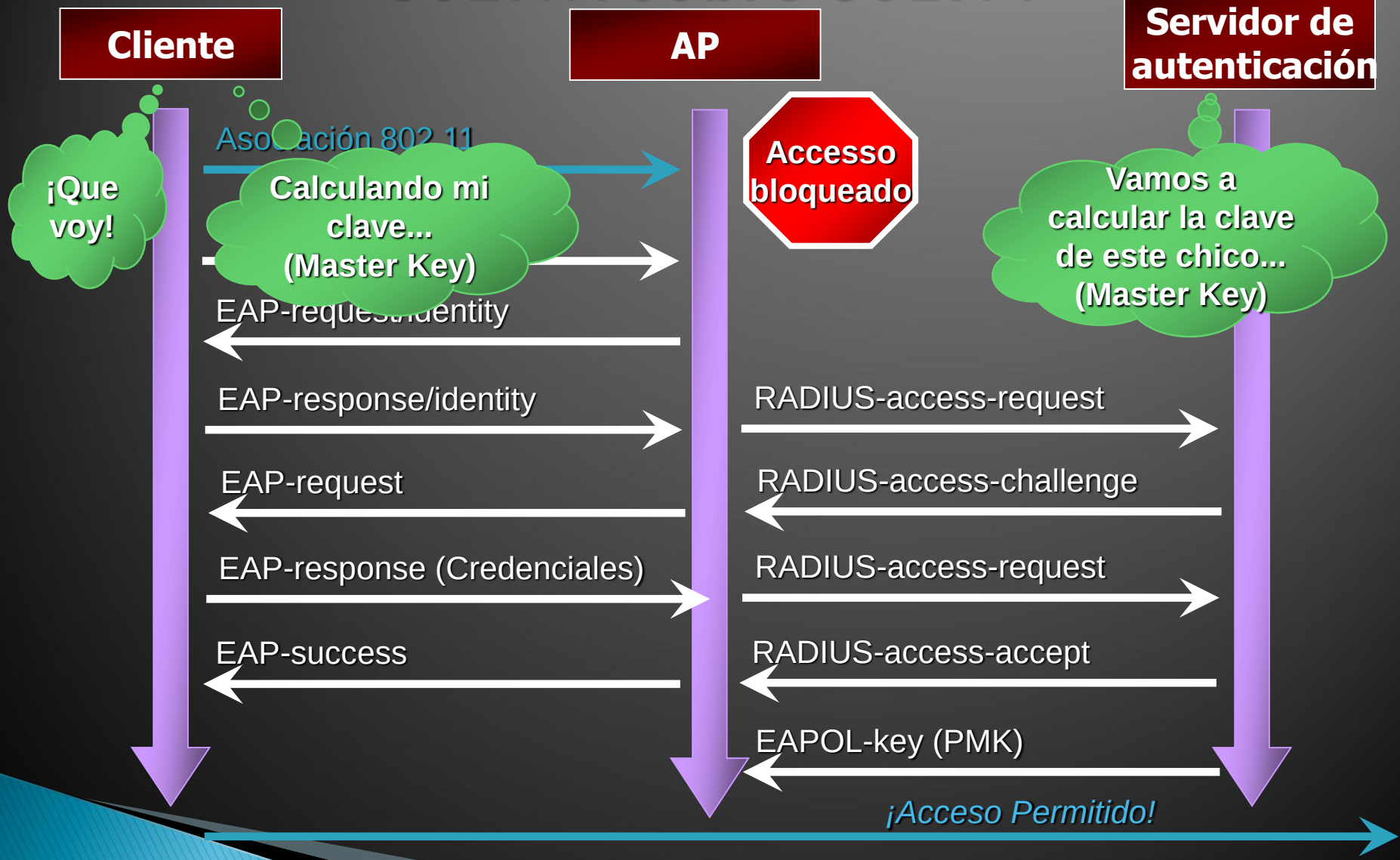


Ejemplo de Autenticación PEAP-MS-CHAP v2

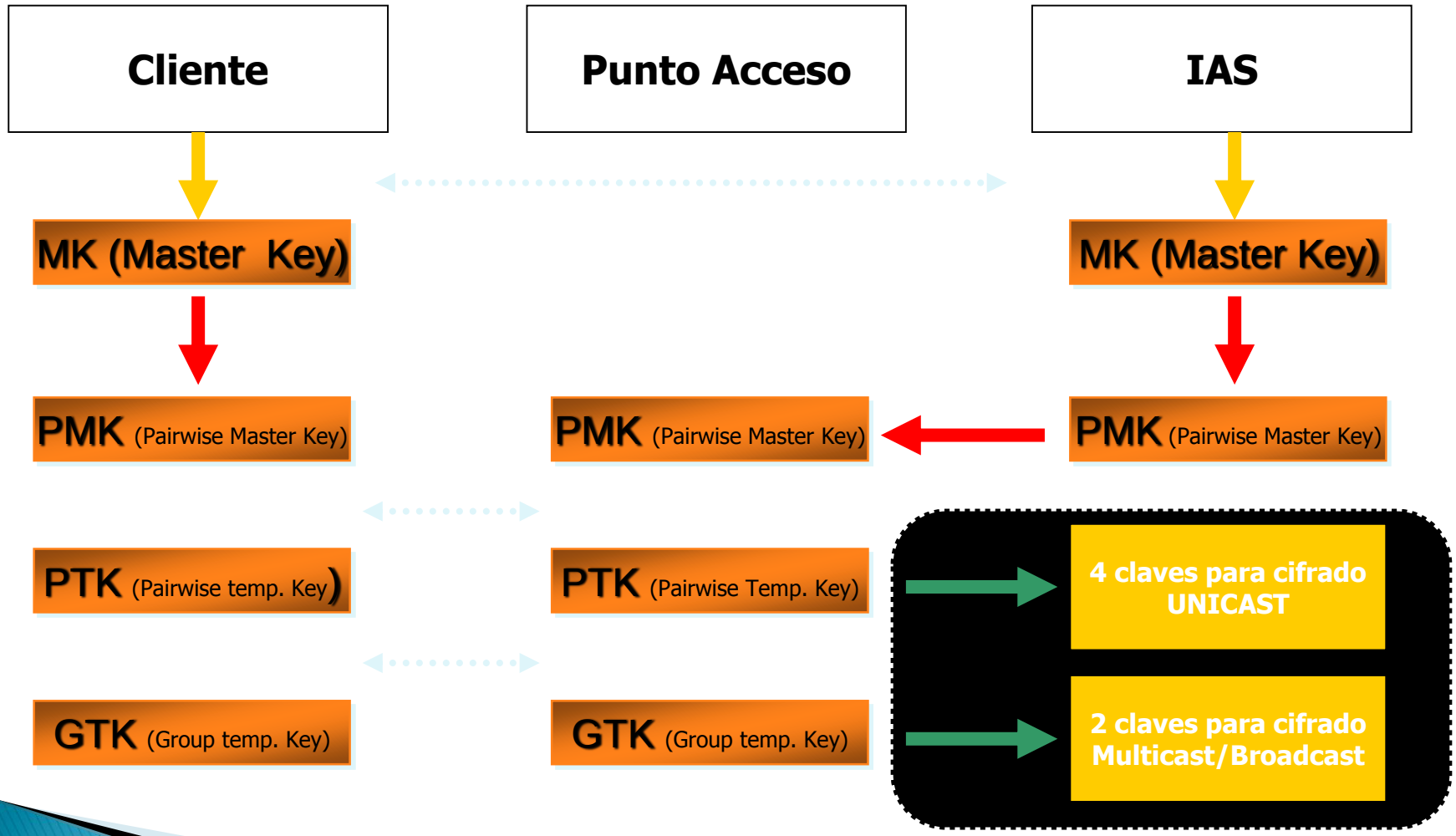
802.1x aplicado a redes Wireless 802.11

- Evita la aparición de Rogue APs usando autenticación mutua.
- Evita accesos no autorizados autenticando tanto a los usuarios como a sus equipos.
- Produce una PMK (Pairwise Master Key) de 256-bit por **cada sesión** para **cada cliente.** Se transmite en el mensaje EAPOL-Key
- Mas detalles sobre su funcionamiento en:
  - http://www.microsoft.com/technet/community/columns/cableguy/cg0402.mspx

802.1X sobre 802.11



Generación de las claves de cifrado



TKIP (Temporary Key Integrity Protocol)

- El IV dobla su tamaño respecto a WEP (48-bit)
  - Utiliza 6 claves distintas entre Punto de Acceso y cada Cliente Wireless
    - 4 para tráfico Unicast, de 128-bit
      - **Data encryption key: Para cifrar tramas Unicast.**
      - **Data integrity key: Para el MIC de las tramas Unicast.**
      - **EAPOL-Key encryption key: Para cifrar los mensajes EAPOL-Key.**
      - **EAPOL-Key integrity key: Para el MIC de los mensajes EAPOL-Key.**
    - 2 para tráfico broadcast y/o multicast.
  - Las claves se recalculan para cada paquete con una función de mezclado
- Michael:
  - Provee de integridad y "antireplay"
  - Calcula un "Message Integrity Code" (MIC) de 8 bytes
  - Estos 8 bytes se introducen entre los datos y los 4 Bytes del ICV de la trama 802.11
  - Se cifra junto con los datos y el ICV
  - http://www.microsoft.com/technet/community/columns/cableguy/cg1104.mspx

AES

- Counter Mode Cipher Block Chaining-Message Authentication Code (CBC-MAC) protocol (CCMP) o “Rijndael” (Joan Daemen y Vincent Rijmen).
- Algoritmo de cifrado por bloques que permite claves de 128, 196 y 256 bits.
- Protocolo sustituto de DES como estándar de cifrado por el NIST.
- Al igual que TKIP usa las 6 claves derivadas de la PMK obtenida en el mensage EAPOL-Key de la autenticación.
- Es el algoritmo de cifrado más seguro que podemos utilizar en redes WLAN.

http://www.microsoft.com/technet/community/columns/cableguy/cg0805.mspx

Otras opciones interesantes

- PMK Caching
  - Cliente y Radius mantienen en cache la PMK.
- Pre-Autenticación
  - El cliente se pre-autentica con Puntos de Acceso dentro de su alcance.
- Esto permite:
  - Fast Roaming a otros AP.
  - Fast Reconnect a un AP al que ya hemos estado conectados.
  - Deben ser activadas tanto en el cliente como en el RADIUS.
- Limite de tiempo de sesión
  - Forzar la re-autenticación del cliente cada cierto tiempo.
    - Obtendremos una nueva PMK de la que derivar nuevas claves.
  - Deben especificarse los siguientes atributos Radius.
    - Session Timeout
    - Termination Action = “Radius-Request”

RESUMEN:

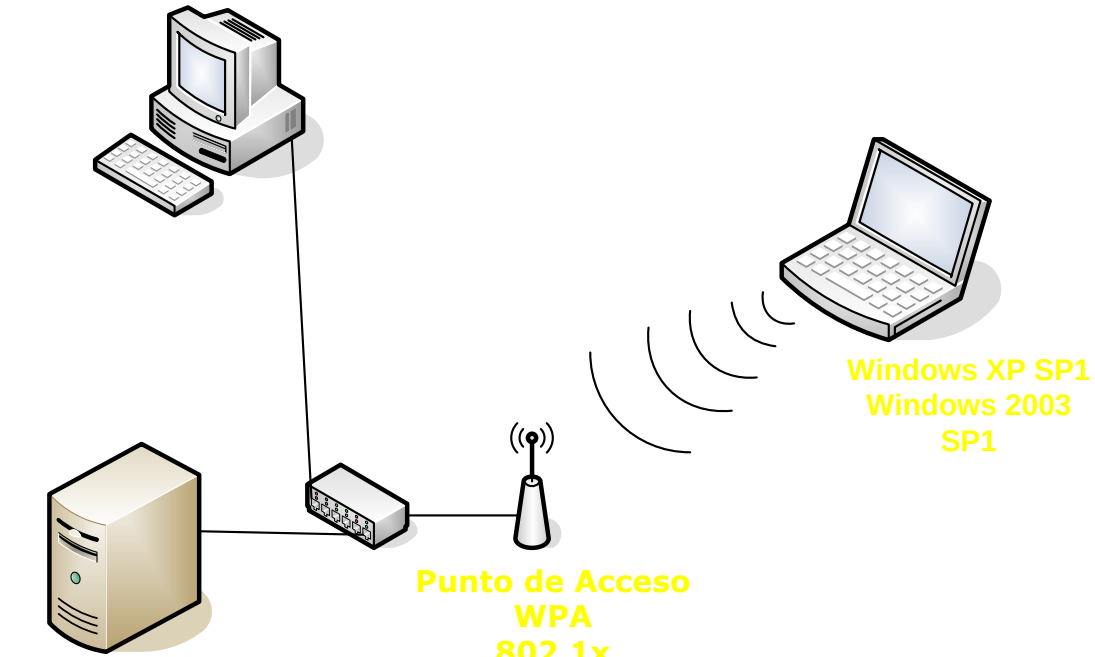
Acuerdo	Estándar Wireless	Estándar Autenticación	Métodos Autenticación	Cifrado/ Firmado
Wireless Original	802.11	-	Open	WEP
			Shared	
Mundo Real	802.11	802.1x	EAP-TLS	WEP
			PEAP-TLS	TKIP
			PEAP-MS-CHAP-v2	AES
WPA	802.11	802.1x	EAP-TLS	TKIP
			PEAP-TLS	
			PEAP-MS-CHAP-v2	
WPA2	802.11i	802.1x	EAP-TLS	AES
			PEAP-TLS	
			PEAP-MS-CHAP-v2	

RECOMENDACIONES (de mas a menos seguras):

- Empresa:
  1. WPA2: AES y PEAP-TLS
  2. WPA2: AES y PEAP-MS-CHAP v2
  3. WPA: TKIP y PEAP-TLS
  4. WPA: TKIP y PEAP-MS-CHAP v2

- SOHO (Small Office, Home Office)
  1. WPA2: AES y secreto compartido
  2. WPA: TKIP y secreto compartido

Implantación de una red Wireless Segura



Pasos

1. Configurar puntos de acceso
2. Agrupar usuarios y máquinas
3. Configurar IAS (RADIUS)
    1. Dar de alta los AP como clientes
    2. Configurar la política de acceso
4. Definir políticas Wireless
5. Definir políticas para obtención de certificados

Cisco | Networking Academy®

Mind Wide Open™

MUCHAS GRACIAS

CONSTRUIMOS FUTURO

UIS