



## Configuración de puntos de acceso

**Puntos de Acceso**  
**Desarrollado por: IT +46 ,**  
**Basado en el trabajo original de:**  
**Onno W. Purbo and Sebastian Buettrich**  
**Traducido por Lilian Chamorro**

---

# Objetivos



- ♦ Proveer una metodología general para la instalación y configuración de puntos de acceso
- ♦ Brindar la comprensión técnica de cada opción de configuración
- ♦ Hacer que el lector sea consciente de cada opción de configuración
- ♦ Proporcionar datos y trucos generales

# Tabla de Contenidos



- ◆ Consejos generales antes de comenzar
- ◆ Instalación de hardware y firmware
- ◆ Configuración hardware(modelo OSI)
  - ✓ Capa física (inalámbrica)
  - ✓ Capa de enlace (inalámbrica)
  - ✓ Capa de red (en el dispositivo inalámbrico)
  - ✓ Capa de aplicación (entrada/salida del dispositivo inalámbrico)

# Consejos generales



- ♦ Lea el manual y conozca el punto de acceso
- ♦ Considere el lugar de la instalación física
- ♦ Planee la red (topología, configuración TCP/IP).
- ♦ Tenga acceso físico a la documentación y material (no en línea)
- ♦ Tome nota de cada paso que realice

# Consejos generales

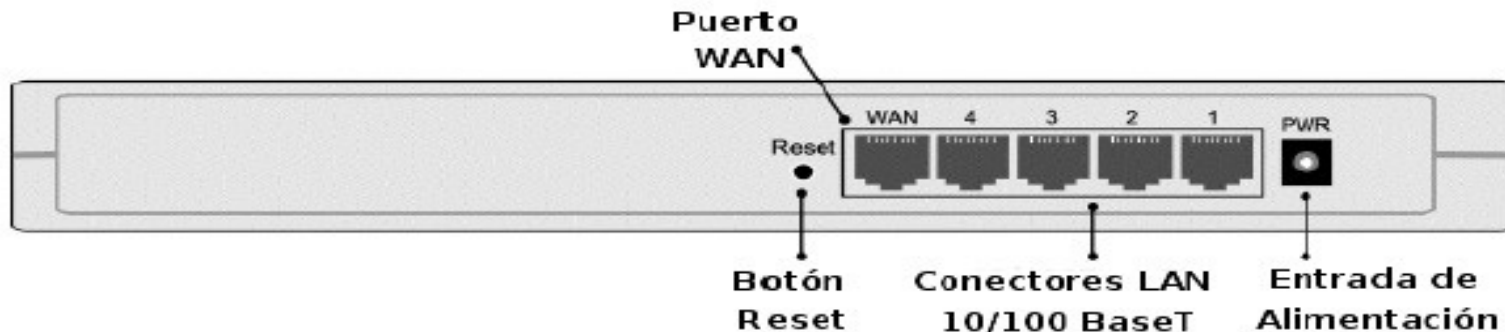


- ♦ Considere el hardware que necesitará (PC/portátil con interfaces Ethernet e inalámbrica)
- ♦ Considere el software necesario:
  - ✓ Herramientas de software TCP/IP (ping, route)
  - ✓ Software específico del vendedor
  - ✓ Software para medir/detectar señales inalámbricas (Kismet, Netstumbler)

# Instalación física: Interfaces



- ♦ Entrada de alimentación (12 V, 6V ...): a la fuente de energía DC
- ♦ Botón de Reset: Usado para reestablecer las opciones de configuración por defecto
- ♦ Conectores LAN (RJ45)
- ♦ Puerto WAN (RJ45): conexión a Internet



# Pasos para configurar un Punto de Acceso



- ♦ **Reestablezca** el dispositivo, si no está seguro/a de que se encuentra en el estado por defecto.
- ♦ **Conecte** su computador al dispositivo por cable o inalámbricamente
- ♦ Primero: **cambie la contraseña** de administración por defecto. Hágalo! **Ahora! :)**
- ♦ Si su dispositivo puede ser más que un Punto de Acceso: **Defina el modo:** Punto de acceso, Puente, Cliente, Repetidor, Pasarela?

# Actualización del Firmware



- ◆ Un software escrito en la ROM
- ◆ Es parte permanente del dispositivo
- ◆ Los vendedores actualizan el firmware continuamente
  - ✓ Ofrece la última configuración estable
  - ✓ Corrige errores reportados
- ◆ Mantenga su firmware actualizado



# Conecte su computador al Punto de Acceso



- ◆ Por cable
  - ✓ Cable Ethernet vía HTTP
  - ✓ Ethernet, usando el software específico del vendedor (SNMP)
  - ✓ Cable serial usando HyperTerminal (si el puerto serial está disponible)
- ◆ Inalámbrico (HTTP(S))

# Configuración del Hardware (Modelo OSI)

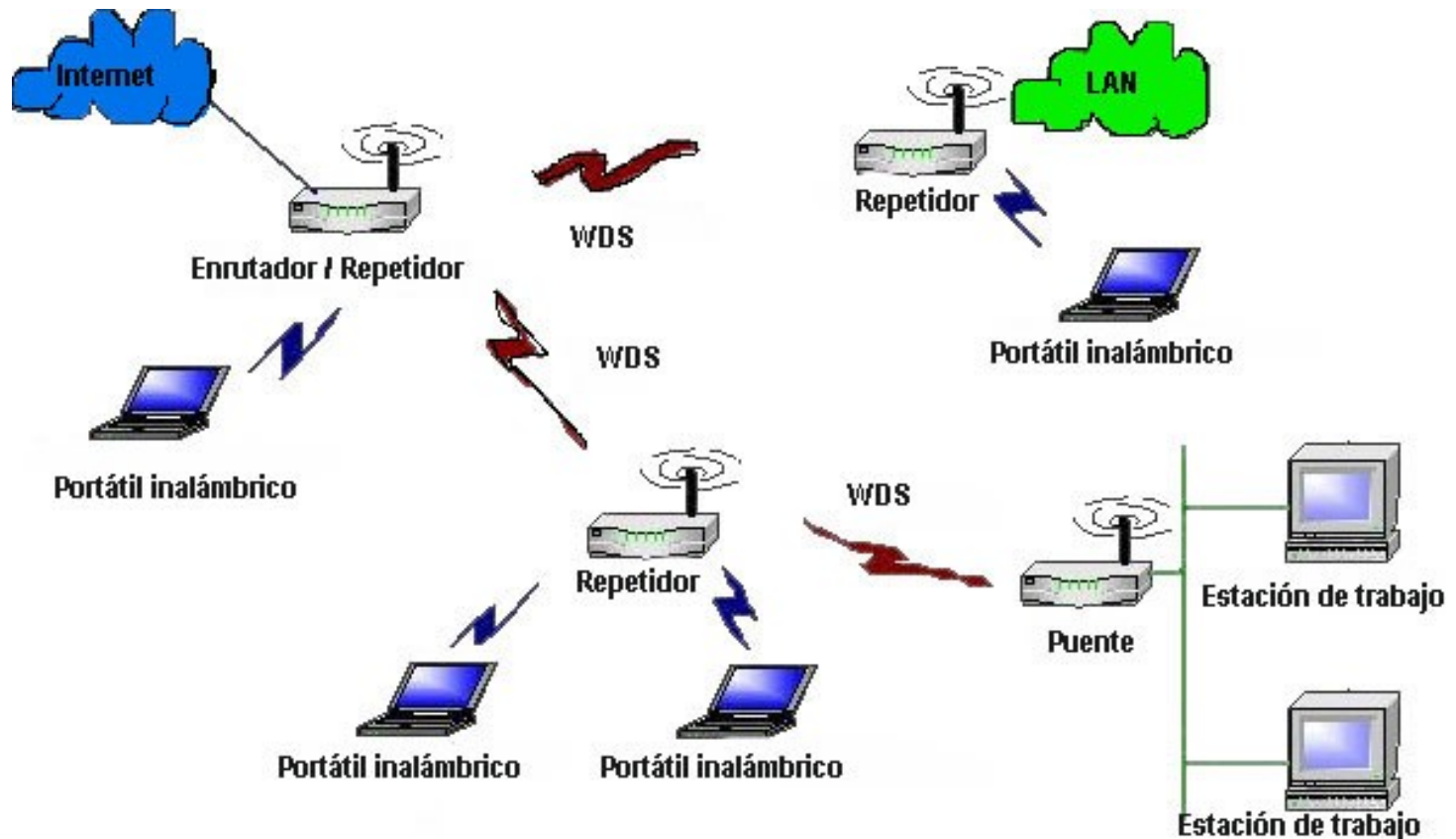


- ♦ Capa física
  - ✓ Canal de frecuencia, Potencia de transmisión, Velocidad
- ♦ Capa de enlace
  - ✓ Modo (AP, GW, PtP...), SSID, filtros MAC, WEP/WPA, WDS
  - ✓ Intervalo de Beacon, RTS/CTS, Fragmentación
- ♦ Capa de red (IP)
- ♦ Capa de aplicación

# Configuración del Hardware (Modelo OSI)



- ♦ WDS: Permite la conexión inalámbrica entre puntos de acceso, ya sea como puente o como repetidor



# Capa física



- ◆ Canal
  - ✓ ¿Qué frecuencia está disponible?, haga un site survey del sitio, inspeccione los canales disponibles
- ◆ Tecnología TDD
- ◆ Potencia de transmisión
  - ✓ Regulaciones
  - ✓ ¿Cuál es su propósito? ¿Mayor cobertura o capacidad? No sature el espectro!
- ◆ Tasa de transmisión: Velocidad vs Estabilidad

# Capa de enlace: Modos de operación



- ♦ Punto de acceso (Access Point Bridging)
- ♦ Puente punto a punto (Repetidor, Ad-Hoc)
- ♦ Enrutamiento punto a punto
- ♦ Adaptador inalámbrico Ethernet (Cliente inalámbrico)
- ♦ Extension del punto de acceso (WDS)
- ♦ Pasarela (Gateway, Router)

# Capa de enlace: SSID



- ◆ SSID = Service Set Identifier
  - ✓ El nombre de la LAN inalámbrica
  - ✓ Usado para asociar/conectar a una u otra red
  - ✓ Sensible a mayúsculas, 32 caracteres alfanuméricos
- ◆ ¿Difundido (broadcasted) o no?

# Capa de enlace: Control de acceso al medio



- ♦ Intervalo de Beacon
  - ✓ Incrementar la movilidad
- ♦ Acceso al medio: CSMA/CA
- ♦ RTS/CTS
  - ✓ Nodos ocultos
- ♦ Fragmentación
  - ✓ Interferencia o áreas pobremente cubiertas

# Capa de enlace: Filtros MAC



- ♦ Sólo permite un conjunto limitado de direcciones MAC
- ♦ Una débil medida de seguridad
  - ✓ Los clientes pueden capturar los paquetes y encontrar que dirección MAC tiene garantizado el acceso
  - ✓ Cambian su dirección MAC a una aceptada “engañar” al punto de acceso



# Capa de enlace: WEP y WPA



- ◆ WEP: Débil protocolo de encriptación pero usado frecuentemente
  - ✓ Claves de 64 o 128 bit (hexadecimal)
  - ✓ Fácilmente puede ser rota por un crack

# Capa de enlace: WEP y WPA



- ♦ WPA: Wireless Privacy Access
  - ✓ Maneja las debilidades de WEP, es más robusto WPA
  - ✓ Autentique su red con WPA + PSK y encripte la llave con TKIP, es el método más seguro de protección de las redes WiFi, implemente radius en la red
- ♦ La misma llave para el AP, el cliente, equipo bridge, equipo WDS
- ♦ Actualice la clave frecuentemente

# Capa de Red (IP)



- ♦ La Capa de Red no es parte de la red inalámbrica
- ♦ Los puntos de acceso con enrutador incorporado incluyen funcionalidades para enrutamiento, servidor DHCP y enmascaramiento(NAT):
  - ✓ Dirección IP/Máscara de red
  - ✓ Gateway/Enrutamiento
  - ✓ DNS para DHCP

# Capa de Aplicación



- ♦ Contraseña del punto de acceso
  - ✓ Cambie la contraseña por defecto
  - ✓ Seleccione una contraseña segura
  - ✓ Previene el “secuestro” de su punto de acceso

# Conclusiones



- ♦ Siga las instrucciones generales para configurar dispositivos inalámbricos
- ♦ Recuerde los pasos generales(conceptos) para poner a funcionar un punto de acceso o un enrutador inalámbrico
- ♦ Proteja su red inalámbrica contra intrusos, no comparta la llave de seguridad con usuarios, genere llaves conformada entre letras, números y caracteres especiales.

# Conclusiones/recomendaciones



- ♦ Enfóquese en comprender que hace cada parámetro y cómo éste depende de los otros
- ♦ Los “Conceptos” no son específicos al vendedor o interfaz – lo importante es reconocer las configuraciones básicas, aún si éstas tienen diferentes nombres o colores
- ♦ Desactive el broadcast SSID, así un hacker no verá fácilmente el nombre de su red.