Wireless LAN

- Objetivo:
  - Instalar y configurar redes inalámbricas bajo distintos escenarios, considerando considerando aspectos de roamming y seguridad.

Redes y conectividad-parte2

- Objetivo:
  - Diseñar e implementar redes IP, en base a las necesidades actuales y futuras de la organización.

Docente: Félix Molina Angel

Conceptos

Wireless LAN

- Comparadas con las LAN
  - IEEE creó estandares para ambas, 802.3 para ethernet, y 802.11 para las inalámbricas.
  - Ambos definen un formato de frame, con encabezado y trailer.
  - Ambos tienen reglas que definen como los dispositivos determinan cuando pueden transmitir.
- Difieren de las LAN en que
  - Utilizan ondas de radio para transmitir datos
  - Utilizan el mecanismo de Half-Duplex para trasmitir
  - Utilizan el algoritmo CSMA/CA para el tratamiento las colisiones

Estandares

Wireless LAN

- El estándar para redes inalámbricas locales es 802.11, como el 802.3 es para ethernet
- Estándares avanzados son 802.11b, 802.11a, 802.11g y 802.11n que será aprobado en septiembre de 2009.

Modos de operación

- Pueden utilizar Ad Hoc o Infraestructura
- En modo Ad Hoc un dispositivo wireless puede comunicarse con uno o unos cuantos dispositivos, de manera directa.
- Al Ad Hoc se le conoce como IBSS (Independent Basic Service Set)
- En modo infraestructura, cada dispositivo se comunica con un AP.
- Un AP se conecta por cable al resto de la infraestructura cableada
- Un dispositivo de una WLAN de infraestructura, se comunica con otro dispositivo de la misma WLAN, a través del AP.

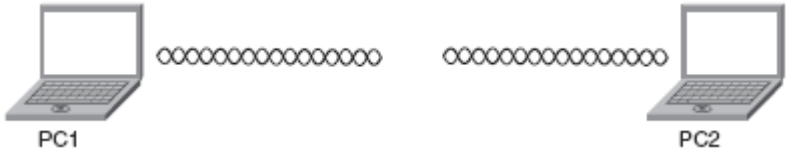
Modo de Infraestructura

- Soporta dos conjuntos de servicios, llamados *Service Sets*
  - BSS (Basic Service Set)
  - ESS (Extended Service Set)
- BSS sólo utiliza un AP para crear una simple WLAN
- ESS utiliza más de un AP, con celdas que se traslapan para permitir roaming en un área más grande.
- En una WLAN ESS pueden moverse dentro del área de cobertura y permanecer conectados a la misma WLAN
- Lo que hace el dispositivo es detectar cuando la señal del AP actual se está debilitando, encuentra un AP con mejor señal, e inicia con éste.

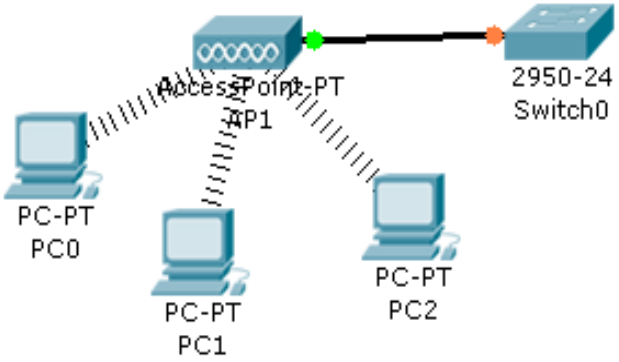
IBSS y BSS

Wireless LAN

Red Ad Hoc o IBSS

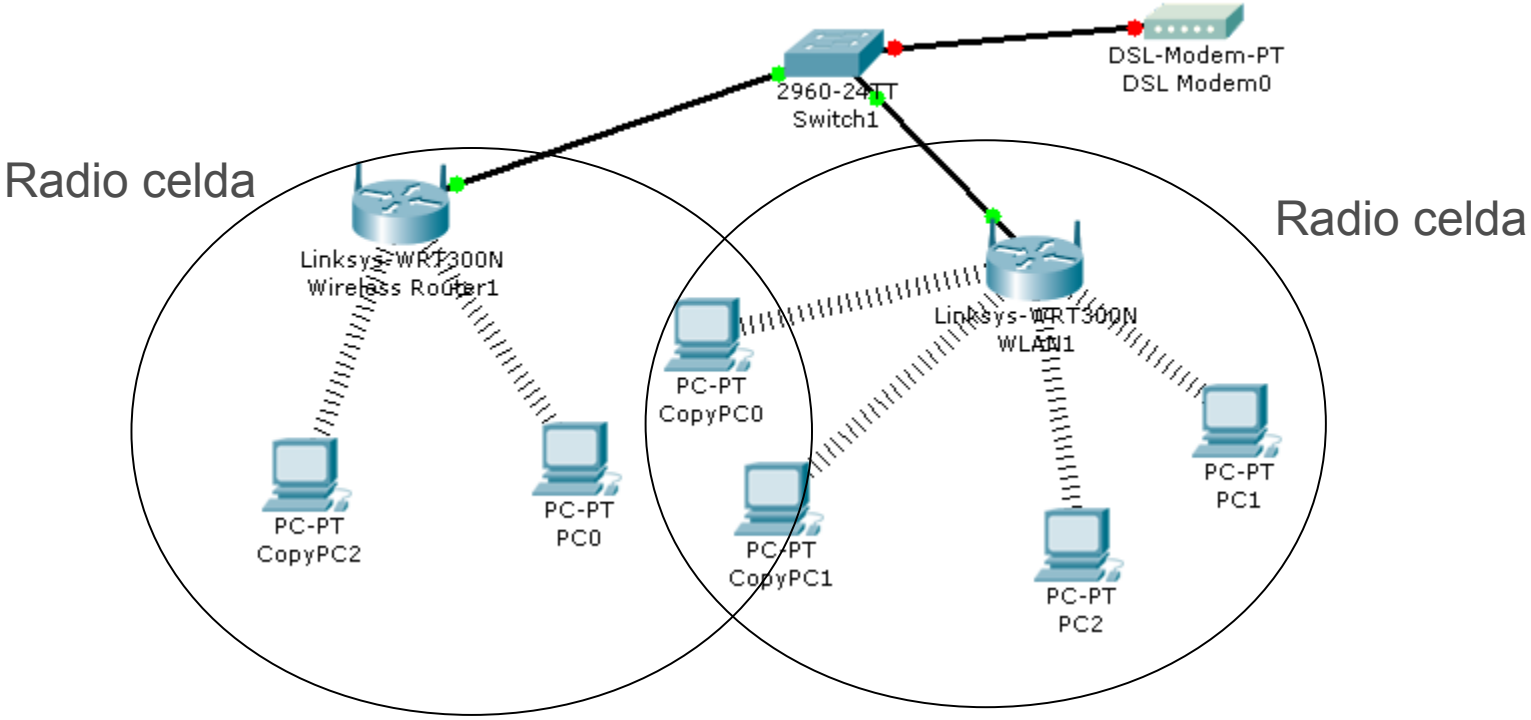


BSS



ESS (Extended Service Set)

Wireless LAN



Transmision Wireless (Capa 1)

Wireless LAN

- Las NIC inalámbricas, Aps y otros dispositivos wireless utilizan un radio y su antena para enviar y recibir ondas de radio, haciendole pequeños cambios para codificar datos.
- Un elemento importante es la frecuencia, medida en hertz.
- Una banda de frecuencia es el rango de frecuencias consecutivas necesarias para transmitir una señal.
- Asi, por ejemplo una estación de radio FM necesita 200 Khz para enviar una señal de radio, si su frecuencia radial es 96.5 FM, entonces su banda de frecuencia está entre 96.4 y 96.6, lo cual da un ancho de banda de 200Khz
- Las WLAN utilizan una banda de frecuencia no licenciada de 2.4 Ghz, pero regulada aún con un rango de potencia tal que no interfiera con otros dispositivos que operan en la misma frecuencia, tales como

Transmision Wireless (Capa 1)

Wireless LAN

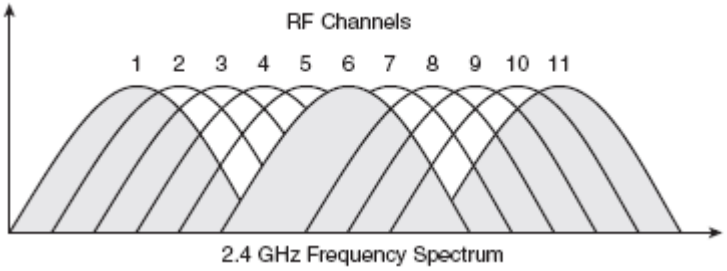
- La FCC define tres bandas de frecuencia no licenciada, pero dos son las actualmente utilizadas.

Rango de frecuencia	Nombre	Dispositivos
2.4 Ghz	ISM	Teléfonos inalámbricos, WLAN 802.11, 802.11b, 802.11g
5 Ghz	Infraestructura de Información Nacional no Licenciada (U-NII)	Teléfonos inalámbricos, WLAN 802.11a, 802.11n

Codificación Wireless: DSSS

Wireless LAN

- Cuando una NIC o un AP envía datos, puede cambiar la frecuencia, amplitud y fase para codificar un 0 o 1.
- DSSS (Direct Sequence Spread Spectrum) fué diseñada para utilizarse en la banda de 2.4 Ghz y utliza varios canales o frecuencias separadas.



  - Esta banda tiene un ancho de banda de 82 Mhz, desde 2.402 Ghz a la 2.483 Ghz y puede tener 11 canales overlapping separados.
  - Aunque muchos de estos canales se traslapan, el 1, 6 y 11 están lo suficientemente separados.

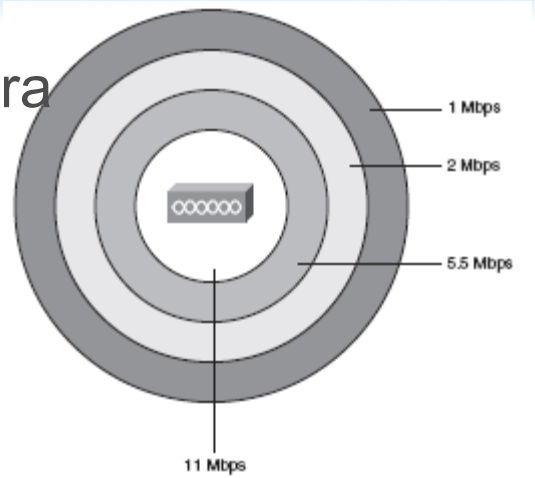
Codificación Wireless: OFDM

- A diferencia de DSSS, utiliza múltiples canales que no se traslapan.
- Es utilizada por 802.11a y 802.11g,
- El estandar emergente 802.11n también utiliza OFDM con múltiples antenas, tecnología conocida como MIMO (Multiple Input, Multiple Output)

Area de cobertura y velocidad

Wireless LAN

Area de cobertura



Velocidad y frecuencia

Estandar	Velocidad máxima	Otras velocidades	Frecuencia	Canales sin traslapar
802.11b	11 Mbps	1, 2, 5.5	2.4 GHz	3
802.11a	54 Mbps	6,9,12,18,24,36,48	5 GHz	12
802.11g	54 Mbps	6,9,12,18,24,36,48	2.4 Ghz	3

Acceso al medio (capa 2)

Wireless LAN

- En Wireless, si dos o más dispostivos transmiten al mismo tiempo en canales que se traslapan, ocurre una colisión. Pero además, los dispositivos enviantes no tienen forma de enterarse que ocurrió una colisión.
- La solución a este problema, es el algoritmo CSMA/CA, el cual reduce las posibilidades de una colisión.
- CSMA no evita las colisiones pero define un proceso a seguir cuando estas ocurren.
- Debido a que un dispositvo emisor, no puede saber si un frame enviado, se colisionó, requiere un acuse por cada frame.
- Si el acuse no se recibe se asume que se perdió o se colisionó y por tanto se retransmite.

Como opera CSMA/CA

1. Escucha que el medio no esté ocupado (Ninguna onda se está recibiendo en las frecuencias utilizadas).
2. Establece un temporizador de espera aleatorio, antes de enviar el trame, para reducir las posibilidades que otro dispositivo trate de enviar al mismo tiempo.
3. Cuando se agota el temporizador, escucha nuevamente, que el medio no esté ocupado. Si no lo está, transmite.
4. Después que se completó de enviar el frame, espera el acuse.
5. Si no recibe un acuse, reenvía el frame, utilizando la lógica CSMA, esperando el tiempo apropiado para enviar de nuevo.

Utilizando WLANs

Wireless LAN

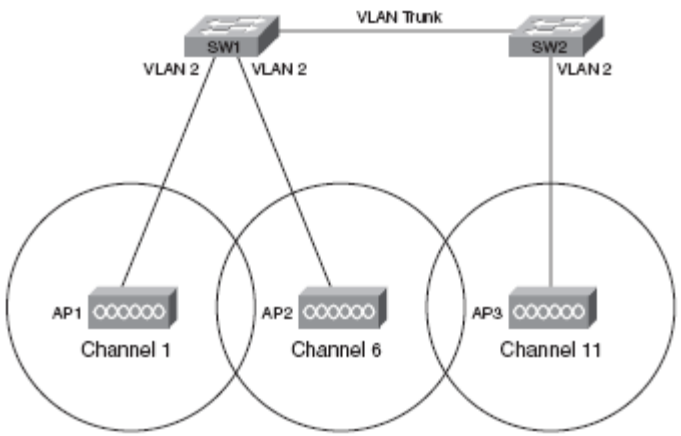
- La seguridad es un elemento crucial en WLAN, ya que son más vulnerables que las LAN.
- Para instalar una WLAN, deberías seguir este orden

1. Verificar que la red cableada trabaje, incluyendo DHCP, VLANs e Internet.
2. Instala, configura y verifica la conectividad del AP, hacia la red cableada, incluyendo dirección IP del AP, máscara de subred y default gateway.
3. Configura y verifica los settings wireless del AP, incluyendo SSID, pero sin seguridad.
4. Instala y configura un cliente wireless, pero sin seguridad
5. Verifica que la WLAN trabaja, desde la portátil.
6. Configura seguridad wireless en el AP y en el cliente
7. Verifica que la WLAN trabaje con los rasgos de seguridad.

Verificar la red cableada existente

Wireless LAN

- El puerto del switch al que debes conectar el AP, debe ser un puerto de acceso, es decir debe pertenecer a una VLAN.
- En un diseño ESS, todos los APs, de la misma WLAN, deben estar en la misma VLAN.
- Para probar podrías conectar tu portátil en cada puerto, donde pretendas conectar un AP, y checar que te asigne direccionamiento válido en la misma subred.



Instalación y configuración de la interfaz local del AP

- Utiliza un cable directo para conectar el AP al Switch LAN.
- Configura la interfaz local del AP, asignándole una IP, máscara de subred, gateway por default, dirección de DNS si es necesario.

Detalles de configuración WLAN del AP

- Aunque un AP puede trabajar sin ninguna configuración, se recomienda configurar las características que se mencionan.
  - Estandar IEEE (a,b,g o múltiple)
  - Canal wireless
  - SSID Es un identificador de 32 caracteres máximo
  - Potencia de transmisión
- El SSID se utiliza para identificar a cada WLAN.
- En un diseño ESS, todos los AP de la misma WLAN, deben tener el mismo SSID.

Instalar y configurar un cliente wireless

- Para ser un cliente wireless, el dispositivo necesita una NIC que soporte el mismo estandar que el AP.
- Por default los clientes no traen ningún protocolo de seguridad habilitado.
- Al iniciar el cliente, éste podría descubrir más de un AP en la misma red, pero escoge el que tenga mayor potencia.
- Con Microsoft OS, la NIC puede no necesitar ser configurada debido a la Zero Configuration Utility (ZCF).

Verificar que la WLAN trabaja desde el cliente

- En caso que alguna prueba no tenga éxito, puedes realizar una encuesta de sitio, para encontrar la mejor ubicación para el AP. Si un cliente nuevo no se comunica, checa lo siguiente:
  - Está el AP en el centro del área donde están los clientes?
  - Está el AP o el cliente cerca de muchos objetos metalicos.
  - Está el AP o el cliente cerca de fuentes de interferencia, tales como hornos de microondas?
  - Es el área de cobertura lo suficientemente grande para alcanzar al cliente?

Verificar que la WLAN trabaja desde el cliente

- Algunos problemas comunes con una nueva instalación son:
  - Asegurate que los radios de la NIC y el AP están habilitados. Muchas portátiles tienen un switch físico para habilitar o deshabilitar el radio. O un software para habilitar y deshabilitar el radio.
  - Asegurate que el AP tenga la última versión de firmware.
  - Revisa la configuración del AP, en particular la configuración del canal. Podría traslparse con otros AP.

Seguridad Wireless

Wireless LAN

- Una Wireless LAN tiene vulnerabilidades adicionales a las encontradas en una red cableada, por ejemplo:
  - War driver. Atacante que sólo busca navegar gratis. Se dedica a buscar AP sin seguridad, o débiles. Se apoya en herramientas y antenas direccionales de alta ganancia, para lograr su propósito.
  - Hackers, Que buscan información o negar servicio. Su propósito puede ser dejar servidores comprometidos.
  - Empleados. Pueden inconscientemente ayudar a los hackers para entrar a la red empresarial. Si instalan un AP sin ningún parámetro de seguridad.
  - Rogue AP. El atacante puede capturar paquetes desde una wireless, encontrar el SSID y romper claves si es necesario. Luego el atacante puede instalar un AP falso, donde los empleados podrían

Herramientas que reducen los riesgos de ataques

Wireless LAN

- Autenticación mutua. Se utiliza entre el cliente y el AP. El proceso usa un password en ambos; cliente y AP. Mediante un algoritmo, el AP determina que el cliente conoce el valor correcto de la clave. Y algo similar determina el cliente. El proceso nunca envía la clave.
- La encripción utiliza una clave secreta y un algoritmo para codificar cada frame. El receptor utiliza otro algoritmo para descifrar el frame.
- Herramientas de intrusión. Utilizan IDS, IPS y otras herramientas WLAN.

Vulnerabilidades WLAN y soluciones

Wireless LAN

Vulnerabilidad	Solución
War drivers	Autenticación fuerte
Hackers robando información	Encripción fuerte
Hackers teniendo acceso al resto de la red	Autenticación fuerte
Instalación AP del empleado	Sistemas de detección de intrusos (IDS)
AP falso	Autenticación fuerte

Estandares de seguridad

- WEP Primer estandar definido por IEEE ha sido catalogado con una autenticación y cifrado débil, debido a
  - La PSK (Private Static Key), configurada en cada cliente y AP, no tiene un modo de intercambiar la clave.
  - Claves facilmente descifrables. Su tamaño (64 bits) y al ser estáticas, las hace vulnerables.
- La creación de estandares con características de seguridad mejoradas, han motivado a dejar de usar WEP.

Estandares de seguridad

- Ocultamiento de SSID. Aunque no son parte de algún estandar cambian el proceso de asociación de los clientes con el AP.
  - El AP envía un frame beacon periódicamente, con su SSID y otra información de configuración.
  - El cliente escucha los beacons en todos los canales para aprender los AP, en su área.
  - El Cliente se asocia con el AP de señal más fuerte, o con el AP de señal más fuerte y SSID preferido.
  - El proceso de autenticación ocurre tan pronto como el cliente se asocia.
- Aunque ocultar el SSID evita que el AP se anuncie, basta configurar el cliente con un SSID Null, para que envíe un mensaje de prueba, y el AP responda con su SSID.
- Filtrado de MACs permite listar sólo los hosts autorizados

WPA -Wi-Fi Protect Access

- Cisco adoptó una solución propia, con mejoras como: intercambio dinámico de claves, autenticación de usuario mediante 802.1x, una nueva clave de encripción por cada paquete.
- La alianza Wi-Fi creó un estándar de facto (WPA), con características similares a las del protocolo de Cisco
- WPA incluyó la opción para intercambio dinámico de claves, usando TKIP (Temporal Key Integrity Protocol), el uso de IEEE 802.1x, y el algoritmo de encripción MIC (Message Integrity Check)

IEEE 802.11i y WPA2

- El IEEE ratificó el 802.11i en 2005. Al igual que WPA y la solución de Cisco, incluye intercambio dinámico de claves, encriptación y autenticación más fuerte, pero no es compatible con éstos.
- Una mejora importante es la inclusión de AES -Advanced Encription Estandar.
- La alianza WI-FI continúa con la certificación para 802.11i, pero con un cambio en el nombre.
- Debido al éxito de WPA, llama 802.11i WPA2

Comparación de características de seguridad

Wireless LAN

Distribución de clave	Autenticación de dispositivo	Autenticación de usuario	Cifrado
Estática	Si (debil)	Ninguna	Si (debil)
Dinámica	Si	802.1.x	TKIP
Ambas	Si	802.1.x	TKIP
Ambas	Si	802.1.x	AES

Direccionamiento y Subneteo IP

- Objetivo
  - Desarrollar habilidades para identificar las clases de redes IP, direccionamiento privado,y la capacidad de crear y enrutar subredes.

Direccionamiento IP

- Ya hemos visto que las direcciones IP se clasifican en clase A, B y C.
- Un elemento que va ligado a la dirección IP, es la máscara de red o de subred, que se utiliza para poder determinar la parte de red o de subred de la dirección IP, y la parte de host.
- Los 1's en la máscara definen la parte de red, de la dirección IP, y los 0's indican la parte de host en la dirección IP.
- Cuando no se utilizan subredes, se tienen máscaras por default de acuerdo a la clase de red.

Clases de redes y máscaras por default

Direccionamiento IP y Subneting

Clase de dirección	Tamaño de la parte de red en bits	Tamaño de la parte de host en bits	Máscara por default
A	8	24	255.0.0.0
B	16	16	255.255.0.0
C	24	8	255.255.255.0

Direccionamiento público y privado

- Cualquier host es alcanzable en Internet, gracias a que cuenta con una dirección IP pública.
- El direccionamiento IP público es controlado por la ICANN, a traves de sus similares en cada país.
- Las direcciones IP públicas son enrutables, o sea que cualquier red conectada a Internet puede determinar hacia donde enviar un paquete con IP pública.
- Sin embargo, la ICANN tambien reservó grupos de direcciones conocidas redes privadas para utilizarse en interredes sin conexión a Internet.
- Este conjunto de redes, definido en el RFC1918, no es controlada por la ICANN, de modo que cualquier organizado, puede hacer uso de ellas.

Espacio de direccionamiento privado

Direccionamiento IP y Subneting

Redes IP privadas	Clase de redes	Número de redes
10.0.0.0	A	1
172.16.0.0 a la 172.31.0.0	B	16
192.168.0.0 192.168.255.0	C	255

IP Versión 6

- El principal objetivo de IPv6, es el incremento de Ips
- Utiliza Direcciones IP de 128 bits, lo que permitira 10^{38} direcciones disponibles.
- IPv6 se creó para resolver el problema de agotamiento de Ipv4.
- Muchos proveedores ya ha han migrado a IPv6, para soportar los dispositivos móviles.

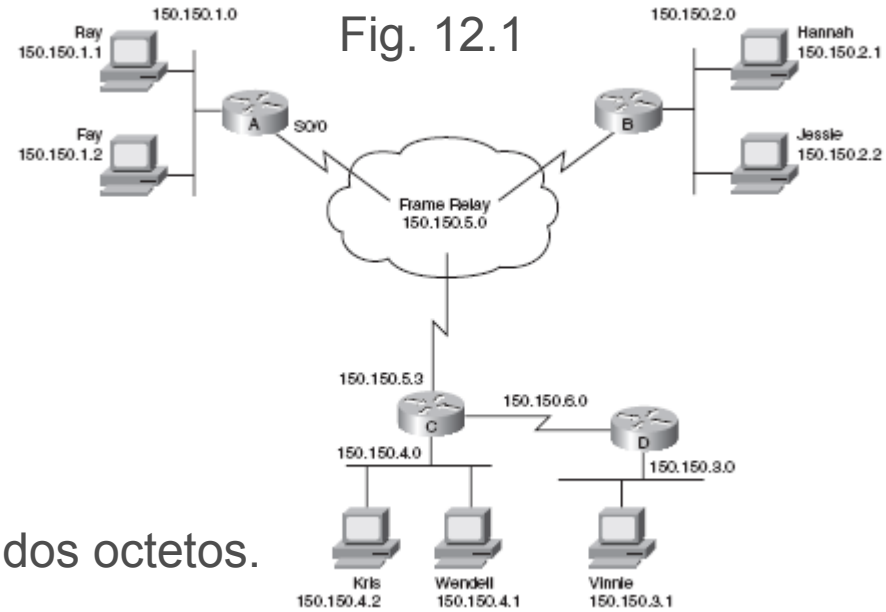
Tamaño de	32 bits	128 bits
Ejemplo	10.20.20.10	0000:0000:0000:0000:FFFF:FFFF:0A01:0101
Dirección abreviada	----------	::FFFF:FFFF:0A01:0101

IP Subnetting

Direccionamiento IP y Subneting

- El subneteo permite dividir una red de clase A, B, y C en un conjunto de redes más, pero sin perder la parte de red.

•Considerando la red IP de la figura, la dirección 150.150.0.0, se ha tomado el tercer octeto para creación de subredes, de modo que la máscara de subred 255.255.255.0



•La parte de red, siguen siendo dos octetos.

•Al crear subredes, es la parte de hosts la que se modifica, aquí, se han tomado prestados 8 bits para crear subredes

Enrutamiento IP

- Para poder enrutar correctamente, el proceso de enrutamiento se apoya en la información almacenada en la tabla de enrutamiento. Para una mejor comprensión, veamos un ejemplo.
  - De la fig. 12.1, considera una ruta a la subred 150.150.4.0 255.255.255.0. En la tabla de enrutamiento, se lista cada subred destino y su máscara, más otros datos de como el router debe reenviar paquetes a dicha subred.
  - Las instrucciones de reenvío, incluyen la dirección ip del siguiente router al debe reenviarse el paquete, y la interface local del router por donde reenviar el paquete.
  - Por ejemplo: Una ruta hacia dicha subred, en

Subnet and Mask	Next-hop Router	Outgoing Interface
150.150.4.0, 255.255.255.0	150.150.5.3	S0/0

Enrutamiento IP

- Para ver como la información anterior se relaciona con subredes, considera un paquete enviado desde la 150.150.1.1 a la 150.150.4.2.
- El paquete se envía al router A, porque está en una subred diferente.
- Cuando el router A toma el paquete, no busca la direccion, 150.150.4.2, más bien determina a que subred pertenece, y luego esta la compara con la lista de subredes que conoce.
- En este caso la subred es la 150.50.4.0, de modo que según la tabla, tiene que reenviar el paquete al router 150.150.5.3, a través de su interfaz serial s0/0.

Operaciones utilizadas para subnetear

- Convirtiendo direcciones IP y máscaras de decimal a binario y viceversa.
  - Recuerda que cada número de la dirección IP, equivale a 8 bits.
  - IP en decimal IP en binario
  - 150.20.30.45
  - 201.34.111.127
  - 20.200.255.20
  - 234.34.56.13
  - 260.45.23.56

Conversion de binario a decimal

- Repaso de conversión binario-decimal, aplicado a direcciones IP
  - 10011011.10010010.00101101.10101011
  - 00110111.01010101.11111100.11001011
  - 11111010.11100001.11001100.11100010

Operación lógica AND

- Esta es la operación que aplican los routes para poder determinar la subred a la que pertenece la direccion IP destino de un paquete que llega.Se utiliza la dirección IP y la máscara de subred.
- Aplicada entre dos dígitos binarios, el resultado es 1, siempre que ambos operandos sean 1, de lo contrario el resultado será 0.
- Aplicada entre una dirección IP y la máscara, resultará la subred a la que pertenece el host.
- Ejemplo: Dada la IP, y la máscara en binario.
- IP: 10010101.10010110.11100110.11001100
- M: 11111111.11111111.11100000.00000000
- S: 10010101.10010110.11100000.00000000

Notación prefijo/notación CIDR

- La máscara de red o subred, se escribe generalmente en notación decimal, por ejemplo: 255.255.255.0
- Sin embargo, otro modo de representarla, es notación prefijo o también llamada CIDR.
- Para entender la notación prefija, recuerda que la máscara se forma por un número consecutivo de 1's más un número consecutivo de 0's, completando 32 bits.
- Entonces, la notación prefija simplemente describe la cantidad de 1's en la máscara.
- Por ejemplo: dada la máscara 255.255.255.0 , convertida a binario es: 11111111.11111111.11111111.00000000
- Entonces, la notación prefijo será /24

Como convertir entre notación decimal y prefijo

- Debes estar preparado para manejar tanto la notación decimal, como prefijo, dado que los routers manejan ambas.
- Sigue este sencillo procedimiento
  - Convierte la máscara a notación binaria
  - Cuenta el número de 1's. Este es el valor del prefijo
- Ejemplo: Cual es el prefijo de 255.255.255.192 ?
- Conversión a binario
  - 11111111.11111111.11111111.11000000
- Cuantos 1's? 26 o sea /26

Conversión de prefijo a notación decimal

- Escribe la cantidad de 1's que dicta el prefijo, agrupándolos de 8 en 8
- Rellena con 0's hasta completar los 32 bits.
- Convierte cada octecto a su correspondiente decimal
- Ejemplo: Cual es la máscara en decimal de /21
- 11111111.11111111.11111000.00000000
- La máscara en decimal es: 255.255.248.0

Análizar la máscara en un diseño de subredes existente

- Al crear subredes, el número de bits para la red de clase no cambia, ya las subredes se crean tomando bits prestados de la porción de hosts.
- Entonces, para determinar el no. de bits de subred, se aplica la formula No. bits subred = 32-(No.bits red+No. De bits de hosts).
- Ejemplo: Sea 129.23.45.45 255.255.255.0
- No.Bits red= 16 Porque es una red de clase B
- No. de bits de host = 8 Porque son hay 8 bits disponibles para crear hosts.
- No. de bits de subred =32-(16+8)= 8

Encontrar el no. de bits para red, subred y hosts: proceso binario

- Cuando la máscara se compone sólo por 255's y 0's, es fácil determinar el no. de bits para hosts, subred y red, pero cuando además incluye otros números, ya se complica el cálculo.
- Entonces, es más fácil convertir la máscara a binario y aplicar el procedimiento que sigue:
  - Convierte la máscara a binario, completando con 0's a 32 bits
  - Separa o marca el no. de bits 1 para identificar a la red de clase.
  - Cuenta el no. de bits en 1, restantes, estos representan los bits de subred.
  - Cuenta el no. de ceros, que representa los bits de la parte de hosts.

Encontrar el no. de bits para red, subred y hosts: proceso decimal

- Identifica la clase de red, y escribe el no. de bits de red (NBR).
- Si la máscara esta en decimal, conviertela en prefijo, y calcula el no. de bits de host aplicando la formula NBH=32-prefijo
- El no. de bits de subred se calcula aplicando NBS=prefijo-NBR

Encontrar el no. de bits para red, subred y hosts: proceso decimal

Direccionamiento IP y Subneting

- Ejemplo: Sea la IP: 135.23.45.50
  - Con mascara: 255.255.224.0
  - NBR = 16, puesto que es una red clase B
  - Mascara en prefijo = /19, porque:
  - 255 .255 .224 .0
  - 11111111.11111111.111 00000.0000 0000

NBR NBS NBH

Cálculo de no. de subredes y no. de hosts

- Dada una red de clase, y una máscara de subred, Cuantas subredes pueden crearse en dicha red classful y cuantos hosts puede haber por cada subred?
- Dos fórmulas sencillas sirven para responder a estas preguntas. Si llamamos s, al no. de bits de subred y h al no. de bits para hosts,, tenemos las fórmulas que proporcionan las respuestas:
  - No. de subredes = 2^s
  - No. de hosts por subred = $2^h - 2$
  - Para direccionamiento de hosts, se reservan dos direcciones: el número más bajo o sea 0's en parte de host, y el número más alto o sea 1's en el campo de hosts.
  - El no. más bajo se utiliza para identificar a la subred, y el número más alto como dirección de broadcast de la subred

Número de subredes: restar 2 o no?

- En algunos casos, dos de las subredes de una red clasful son reservadas y por tanto no se usan, pero porque?
- La primera posiblemente reservada se conoce como *subred 0* y siempre es el mismo número que identefica a la red classful, y esto trae confusión.
- La otra subred que puede reservarse se conoce como *subred de broadcast* es la última subred en la red, y en un tiempo no se usó, porque al enviar un paquete a todos los hosts de dicha subred, se confundia con la dirección de broadcast de la red classful.
- Sin embargo, hoy, debes determinar si se utilizan o, para aplicar la fórmula 2^s o 2^s-2.
- Otro factor que determina si se usa o no la subred cero, es el comando *ip subnet zero* en el router.

Cuál fórmula utilizar para el no. de subredes

Direccionamiento IP y Subneting

Utilizar $2^s - 2$	Utilizar 2^s
Protocolo de enrutamiento Classful	Protocolo de enrutamiento Classless
RIP Ver. 1 o IGRP	RIP Ver. 2, EIGRP, OSPF
Se configura el comando no ip subnet zero	Se configura el comando ip subnet zero (por default)

Ejemplos analizando máscaras de subredes

- Determina el no. de bits de red, subred y de hosts, y el no. de subredes y no. de hosts por subred de las siguientes direcciones IP.
  - 20.30.50.100/16
  - 50.45.255.220/24
  - 145.255.24.200/22
  - 190.90.30.200/25
  - 200.20.30.50/27
  - 222.255.20.177/23

Determinación de la máscara de subred que cubra los requerimientos de diseño

- Cuando un Ingeniero de redes diseña una nueva interred, una de las primeras tareas es determinar la máscara de subred a utilizar, basado en los requerimientos.
- La máscara necesita definir la cantidad de bits suficientes para subredes y para hosts que cubran los requerimientos expresados.
- Supongamos que se tiene una red clase B, y se necesitan 150 subredes, cada una con al menos 200 hosts
- Lo primero que necesitas es determinar cuantos bits de subred y hosts son suficientes para cubrir el requerimiento.
- Básicamente es aplicar la fórmula 2^s o 2^s-2 y $2^h - 2$, cuyos resultados sean al menos 150 y 200 respectivamente.

Determinación de la máscara de subred que cubra los requerimientos de diseño

- Ejemplo completo. Dada la red 150.20.0.0, determinar la máscara a aplicar, si se necesita crear 150 subredes con 200 hosts cada una, y se conviene en utilizar todas las subredes.
- 1. Se debe determinar cuantos bits de subred, cubren 150 subredes. Para ello, en este caso aplicamos 2^s, donde s debe ser número tan pequeño, tal que 2^s>=150, en este caso, si s=8, 2^s=256, por tanto se necesitan 8 bits para identificar subredes.
- De manera similar aplicamos ahora 2^s – 2, donde s, deber tan pequeño, tal 2^s – 2 >=200, en este caso tambien es s=8.
- Ahora, poniendo todo junto, como la red es clase B, se tienen 16 bits de red, 8 subred y 8 de host, por tanto la máscara a plicar es: 11111111.11111111.11111111.00000000 o sea 255.255.255.0

Encontrando múltiples máscaras posibles

- El diseño requiere de 50 subredes, con 200 hosts la subred más grande. Suponiendo que la red IP es
  - 140.20.0.0
- Aplicando las fórmulas ya vistas, se tiene NBS=2^6=64 y
  - NHS =2^8 – 2 = 254, por tanto representando los bits de red, subred y hosts, queda así:
  - NNNNNNNN.NNNNNNNN.SSSSSS—HHHHHHHH. Aquí vemos dos posiciones vacías que bien pueden utilizarse para representar subredes o para representar hosts.

Encontrando múltiples máscaras posibles

- Como las máscaras se forman por una cadena ininterrumpida de 1's, y luego una cadena ininteturrimpida de 0's, podríamos encontrar las siguientes máscaras posibles, considerando las posiciones vacías:
- 11111111.11111111.11111100.00000000 válida
- 11111111.11111111.11111110.00000000 válida
- 11111111.11111111.11111111.00000000 válida
- 11111111.11111111.11111101.00000000 inválida
  - Porque los 1's no son consecutivos

Seleccionando una máscara de subred que maximice o minimice el no. de subredes o el no. de hosts

- Considerando el ejemplo anterior, con dos posiciones wildcard.
  - NNNNNNNN.NNNNNNNN.SSSSSSXX.00000000
  - **La máscara con el máximo número de bits de subred,** maximizara el no. de subredes y minimizara el no. de hosts. Del ejemplo anterior, se tendría que
  - 255.255.255.0, maximiza el no. de subredes (256)
  - La máscara con más bits de hosts. Si todos los bits de wildcard se establecen en 0, se maximiza el no. de hosts y se minimiza el no. de subredes, asi tendríamos que
  - 255.255.252.0 nos da, 1024 hosts por cada subred
  - Pero en ambos casos se mantiene el requerimiento de diseño

Análisis de subredes existentes

- Una de las tareas más comunes relativas a subneteo, consiste en analizar y entender hechos clave de las redes existentes.
- Aquí veremos tres elementos clave que pueden determinarse, a partir de una dirección IP y máscara de subre dada.
  - Dirección de subred (número de subred)
  - Dirección de broadcasta para esa subred
  - Rango de direcciones válidas para esa subred

Encontrando el no. de subred

- Es la dirección IP que representa una subred.
- Un número de subred puede contener un gran número de direcciones de hosts, pero en la tabla de enrutamiento, sólo se almacena la dirección de subred, junto con la máscara aplicable.
- Dada la dirección IP: 145.30.255.10
- Y máscara 255.255.192.0, aplicamos & para encontrar el no. de subred
- IP en binario: 10010001.00011110.11111111.00001010
- Mascara 11111111.11111111.11000000.00000000
- Resultado 10010001.00011110.11000000.00000000

Encontrar el no. de subred. Atajo binario

- Después de algunos ejercicios, habrás notado que al aplicar AND, cada octecto de la dirección no se altera, cuando el octeto correspondiente en la máscara es 255, y también cuando el octecto en la máscara es 0, el octeto correspondiente en la dirección es 0.
- Por tanto, la aplicación del AND se reduce a los casos en que un octeto de la máscara está entre 0 y 255.
- Ejemplo: Dada la IP: 70.20.0.45 y mascara 255.255.0.0
- Se puede deducir que la subred es 70.20.0.0
- Ahora si la IP es: 100.37.177.29 y máscara 255.255.224.0
- Sólo aplicamos AND aquí en el tercer octeto 10110001
  - 11100000
  - 10100000

    = 160
  - Por tanto la dirección de subred es 100.37.160.0

Método corto: Procedimiento

- Para cada octecto de la máscara cuyo valor sea 255, copia el octeto de la dirección IP que coincida en posición con el octeto de la máscara.
- Para cada octecto de la máscara cuyo valor sea 0, pon un 0 en el octeto de la dirección IP que coincida en posición con el octeto de la máscara.
- Si hay un octeto de la máscara cuyo valor esté entre 0 y 255, conviertelo a binario, convierte a binario el octecto correspondiente de la dirección IP y,
  - Aplica la operación &
  - Convierte a decimal, el resultado,
  - Ahora has completado la dirección de subred.

Encontrando la dirección de broadcast de la subred

- Una vez que se conoce la dirección de subred, y el no. de bits para identificar hosts, lo único que tienes que hacer es poner en 1 la parte de hosts, hacer la conversión a decimal.
- Consideremos la dirección IP:
  - » 145.50.24.10
  - » 255.255.224.0
  - – Obteniendo subred, mediante el método corto tenemos: 145. 50.00011000.00000000
  - – 255.255.11100000.00000000
  - – 145. 50.00000000.00000000
  - – Subred = 145. 50.0.0

Parte de host

Encontrando la dirección de broadcast de la subred

- Del cálculo anterior, basta encender todos los bits de la parte de host
- 145. 50.00000000.00000000
- 145. 50.00011111.11111111 Esta es la dirección de broadcast. Lo que sigue es convertirla a decimal, considerando cada octecto completo, y obtendrás la dirección broadcast en decimal.

145.50.31.255

Rango de direcciones válidas en una subred

- El rango válido de direcciones IP queda comprendido entre la dirección de subred y la dirección broadcast, asi , para determinarlas sólo tienes realizar estas operaciones.
- Primera direccion IP válida = direccion de subred + 1
- Ultima dirección válida = dirección de broadcast -1
- Ejemplo, La primera IP válida de la subred:
- 145.50.00000000.00000000 + 1= 145.50.0.1
- Y la Ultima dirección válida es
- 145.50.00011111.11111111 -1 = 145.50.31.254

Ejercicios de subredes

- Dada la red 200.10.50.0, encontrar el no. de bits de red, subred y de hosts, asi como la máscara de subred, para cubrir 25 hosts por subred.
- Determina la dirección de subred, dirección de broadcast y rango de direcciones válidas de las siguientes IP.
  - 10.40.100.255/23
  - 100.200.128.35/25
  - 150.20.20.50/21
  - 50.200.199.255/22