Resumen Prueba 3 Redes II

IPV6

- Utiliza direcciones de 16 octetos (128 bits).
- 5,3 Sextillones (2^128)

La nueva dirección:

- Antes: 194.153.11.222
- Ahora: 194.153.11.222.128.17.135.22.1.240.36.97.66.205.221.52.4

Formato hexadecimal largo:

- **DEAD:BEEF:0000:0000:0000:0073:FEED:F00D**
  (Notación Hexadecimal separada por : en grupos de 16 bits (8 hextetos))

Compresión de direcciones (Solo un string reemplazado por **::**):

- **DEAD:BEEF:0000::0073:FEED**

Expresión de las “antiguas” direcciones ipv4.
0000:0000:0000:0000:0000:0000:194.153.11.222

Dirección de LoopBack: ::1, esta no puede ser asignada a un nodo, esta sirve para comprobar si la app de entrada y salida funciona.
Se elimina el concepto de nodo, y se empieza a aplicar el concepto de Interfaces

Notacion Hexadecimal

Notación de Direcciones IPv6

- ::01 LoopBack /128
- **Un dígito Hexadecimal equivale a 4 bits**
- Constan de 8 Segmentos o “Hextetos”
- Cada octeto tiene un valor de 16 bits
- IPv6 consta de 128 bits
- Se utilizan “:” para separar cada Hexteto.

Reglas

- **Regla 1:** Todo 0 a la izquierda se omite
  - Ej: 000A => A ….
- **Regla 2:** Dos o más grupos de 0 **(0000:0000**) se pueden omitir con “**::**”, pero esto solo se puede hacer una vez
- Prefijo: representa la porción de prefijo de la dirección y no la notación decimal
  - La ICP proporciona esto
- En IPv6, **no existe Broadcast**, pero si:
  - **Unicast:** identifican de manera única una interfaz de un dispositivo habilitado para IPv6
  - **Multicast:** se usan para enviar un único paquete IPv6 a varios destinos
  - **Anycast:** en cualquier dirección IPv6 de difusión que puede asignarse a varios dispositivos. **El paquete va al host más cercano**

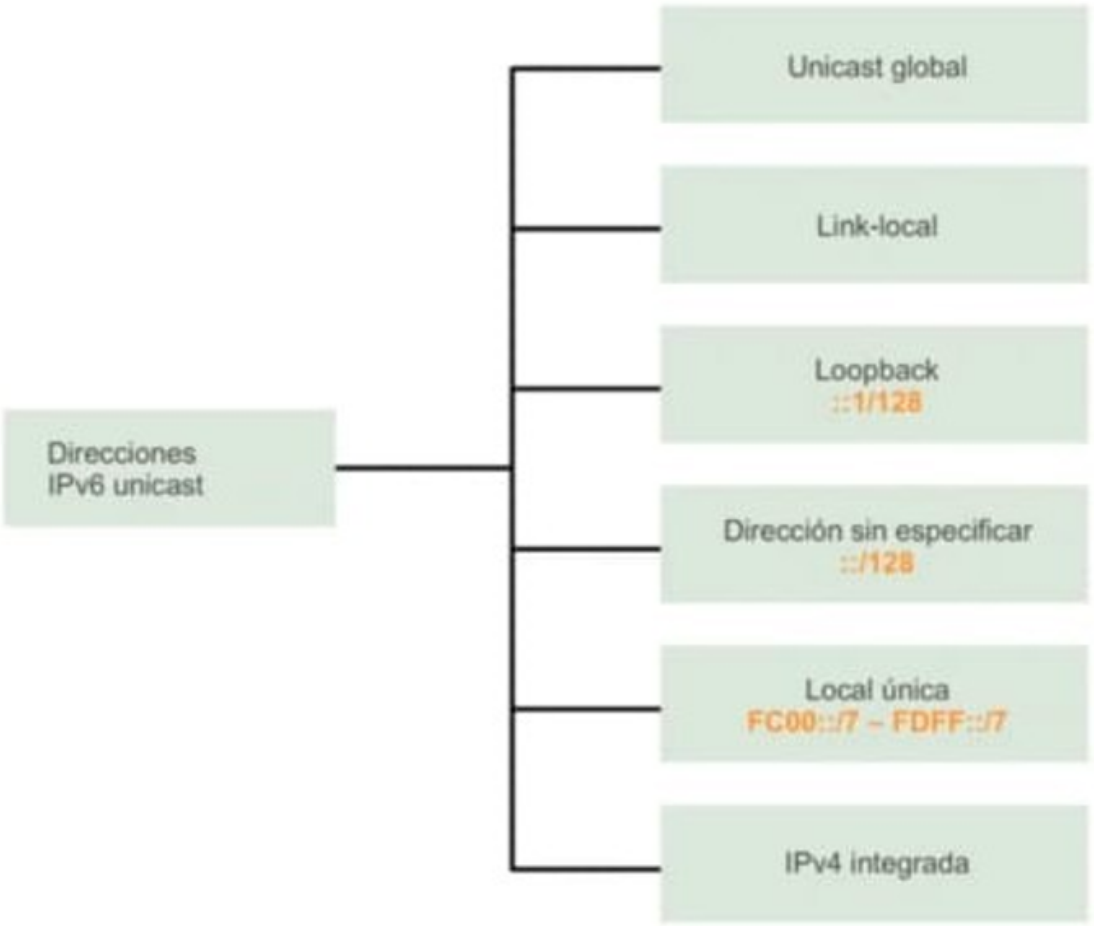
Componentes IPv6

- Parte de Red
  - 48 bits para global
  - 16 bits ID de Subred
- Parte de Interface
  - 64 bits
- Es importante poner prefijo.

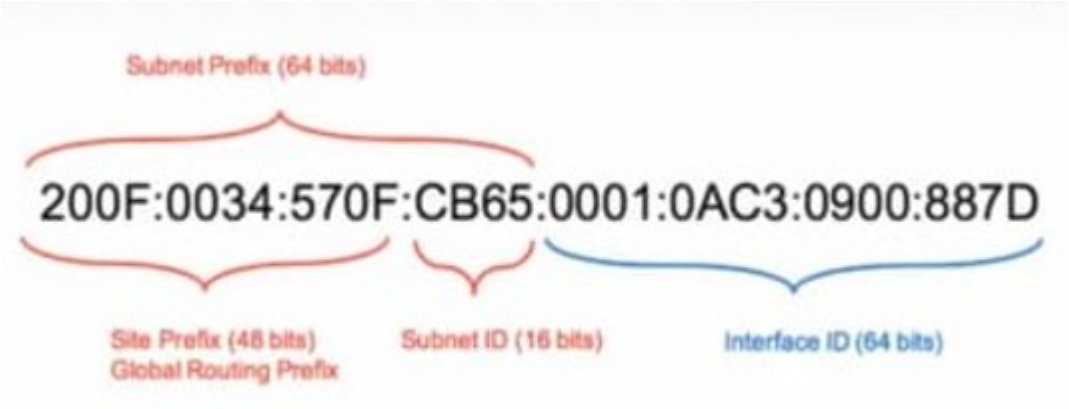
Prefijos IPv6

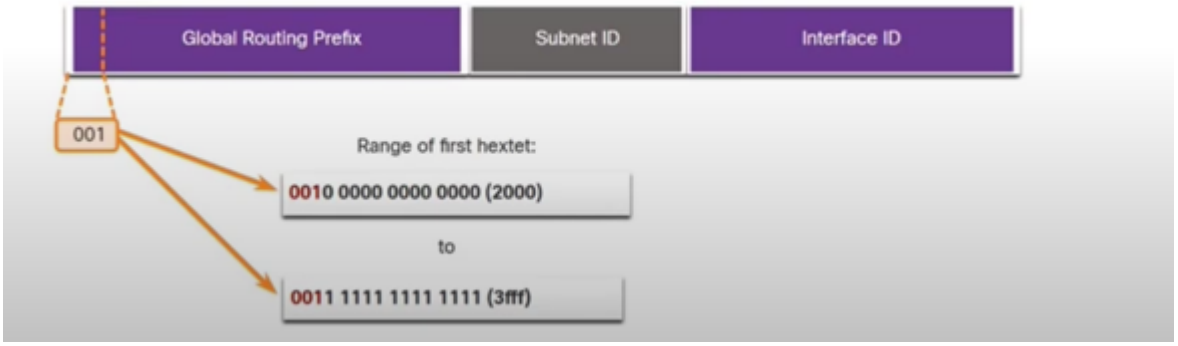
- Longitud de **prefijo** se utiliza para indicar la porción de red de una dirección IPv6 mediante el formato:
  - **200F:1945:1021:A000**:0AC3:0900:560F:000A**/64**

Direcciones Unicast



- **Global Unicast Address**:
  - Similares a las direcciones IPv4 públicas.
  - Estas direcciones son enrutables en internet globalmente excluidas
  - Los prefijos de la red asignadas por la IANA es 2000::/3, donde todos
  - comienzan con **001**, es decir 3 bits
  - Varían entre 2 y 3
  - Todas las IP globales comienzan con 001, entonce el rango para
  - direcciones IP global es entre 2 y 3
  - va de 2000::/# a 2001::/16
  - Asignadas por el ISP
  - Un ejemplo de una dirección global sería: **2001:4860:4871::7654**



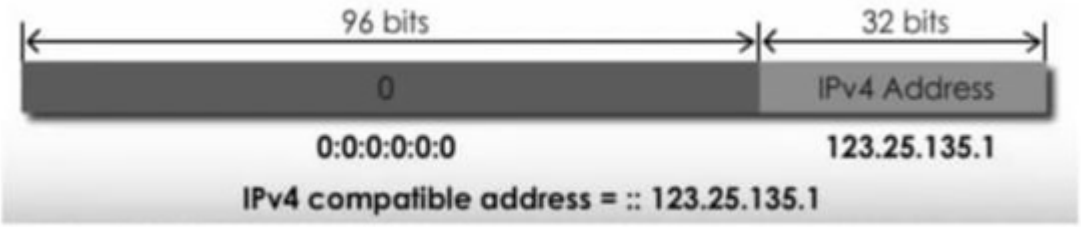


- **Link Local (Dentro de la LAN)**
    - Se requiere para cada dispositivo con IPv6 y se usa para cada dispositivo con IPv6 y se usa para comunicarse con otros dispositivos en el mismo enlace local. Las LLAS no son enrutables y están confinadas a un único enlaces.
    - Las direcciones ipv6 link-local solo son válidas para realizar comunicaciones en un segmento de red local.
    - Routers no redireccionan ningún paquete que se origine desde una dirección link-local
    - Bloque de direcciones FE80:00/10 son direcciones IPv6 Link-Local

- **Local Única (Rango de FC00::/7 - FDFF::/7)**
    - Se pueden enrutar solamente dentro de redes privadas
    - Corresponden a las direcciones IPv4 privadas.
    - Usadas dentro de una organización

- **Unicast LoopBack (::1/128)**
    - ::1/128, corresponde a la dirección ipv4 127.0.0.0/8.
    - ::1/128, es la manera abreviada de 0:0:0:0:0:0:0:1.
    - Se usa para enviar paquetes de regreso a su origen.
- IPV4 Integradas
    - Las direcciones ipv4 compatibles que se asignan a dispositivos que pueden manejar ambos ipv4 e ipv6.

- Empiezan por 96 bits en ceros, seguidos de 32 bits de la dirección ipv4.



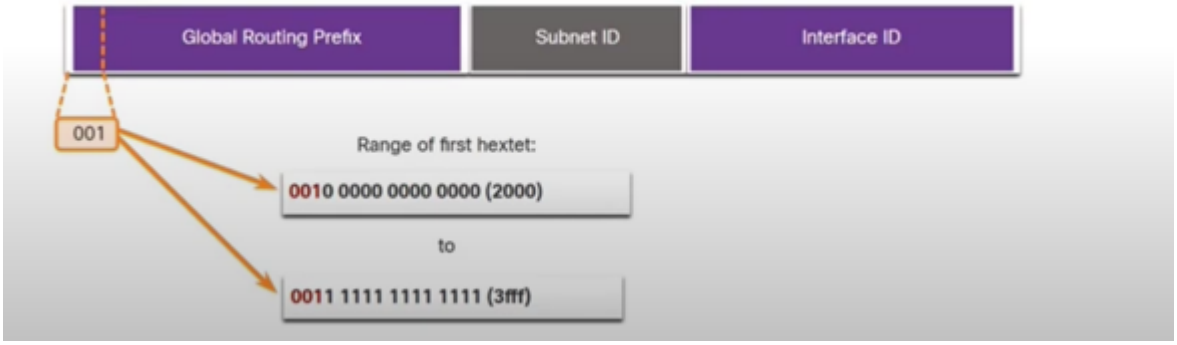
Coexistencia de IPv4 e IPv6

Técnica de migración

- Dual stack: Los dispositivos ejecutan pilas de protocolos IPv4 e IPv6 de manera simultánea.
- Tunneling: Es un método para transportar un paquete IPv6 a través de una red IPv4. El paquete IPv6 se encapsula dentro de un paquete IPv4.
- Translation: Network Address Translation (NAT 64) permite que los dispositivos con IPv6 habilitado se comunique con dispositivos con IPv4 habilitado mediante una técnica de traducción similar a la NAT para IPv4.

IPv6 - GUA
Las direcciónes IPv6 unicast globales (GUA), son globalmente únicas y enrutables en internet IPv6.

- Actualmente, solo se están asignando GUA´s con los primeros tres bits de 001 o 2000::/3.
- Las GUAs disponibles actualmente comienzan con un decimal 2 o un 3 (esto es sólo ⅛ del espacio total de direcciones IPv6 disponibles)



Mensajes RS y RA

Los dispositivos obtienen direcciones GUA dinámicamente a través de mensajes de Internet Control Message Protocol versión 6 (ICMPv6).

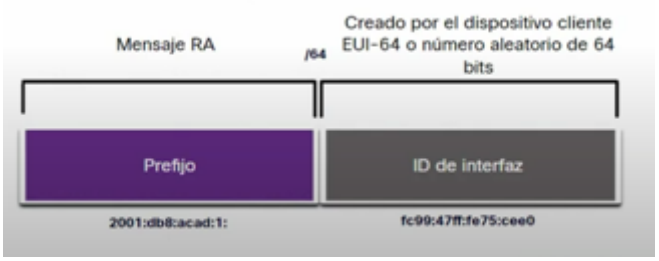
- Los mensajes de solicitud de router (RS) son enviados por dispositivos host para descubrir routers IPv6.

- Los routers envían mensajes de anuncio de router(RA) para informar a los hosts sobre cómo obtener un GUA IPv6 y proporcionar información útil de red, como:

    - Prefijo de red y longitud del prefijo.
    - Dirección del gateway predeterminado.
    - Direcciones DNS y nombre de dominio.
    - El RA puede proporcionar tres método para configurar un GUA IPv6:
        - SLAAC
        - SLAAC con servidor DHCP v6 stateless
        - Staterful DHCP (no SLAAC)

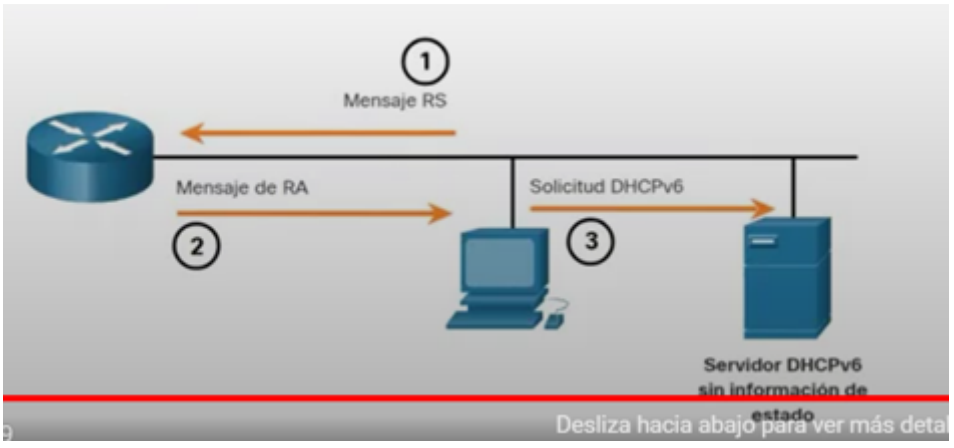
Método 1: SLAAC

- Permite configurar a un dispositivo configurar un GUA sin los servicios de DHCPv6.
- Los dispositivos obtienen la información necesaria para configurar un GUA a partir de los mensajes RA ICMPv6 del router local.
- El predijo lo proporciona el RA y el dispositivo utiliza el método EUI-64 o la
- generación aleatoria para crear un ID de interfaz.



Método 2: SLAAC y DHCP sin estado

- Una RA puede indicar a un dispositivo que use SLAAC y DHCPv6 stateless
- El mensaje RA sugieren que los dispositivos utilicen:
    - SLAAC para crear su propio IPv6 GUA
    - La dirección link-local de router, la dirección IPv6 de origen del RA de dirección del gateway predeterminado.
    - Un servidor DHCPv6 stateless, que obtendrá otra información como la dirección del servidor DNS y el nombre de dominio



Método 3: DHCPv6 con estado

- Un RA puede indicar a un dispositivo que use DHCPv6 Stateful solamente.

- DHCPv6 Stateful es similar a un DHCP para IPv4. Un dispositivo puede recibir automáticamente un GUA, longitud de prefijo y las direcciones de los servidores DNS desde un servidor DHCPv6 Stateful.
- Los mensajes RA sugiere que los dispositivos utilicen:
    - La dirección LLA del router, que es la dirección IPv6 de origen del RA, para la dirección de gateway predeterminado.
    - Un servidor DHCPv6 Stateful, para obtener una GUA, otra información como la dirección del servidor DNS y el nombre de dominio.

ID de interfaz generados aleatoriamente

Según el sistema operativo, un dispositivo puede utilizar una ID de interfaz generada aleatoriamente en lugar de utilizar la dirección MAC y el proceso EUI-64.

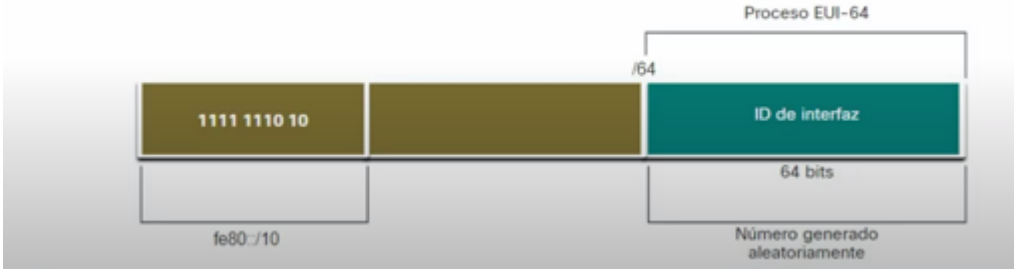
A Partir de Windows Vista, Windows utiliza una ID de interfaz generada aleatoriamente en lugar de una ID de interfaz creada mediante EUI-64.

DAD -> (Detección de Direcciones Duplicadas) Sirve para garantizar la exclusividad de cualquier dirección unicast de IPv6. Similar a una solicitud de ARP para su propia dirección. Si no se obtiene una respuesta, la dirección es única.

LLA´s Dinámicas

- Todas las interfaces IPv6 deben tener una LLA IPv6.
- Al igual que las GUA IPv6, las LAs se pueden configurar dinámicamente.

- La figura muestra que el LLA se crea dinámicamente usando el prefijo fe80 :: / 10 y la ID de interfaz usando el proceso EUI-64, o un número de 64 bits generado aleatoriamente.



Proceso EUI-64

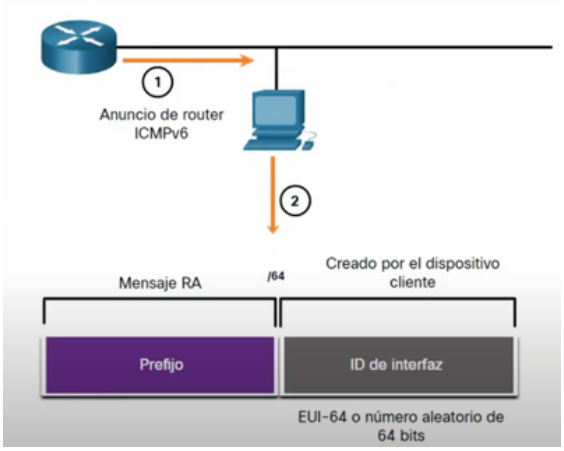
El IEEE definió el identificador único extendido (EUI) o el proceso EUI-64 modificado que realiza lo siguiente:

- Un valor de 16 bits de FFEE (en hexadecimal) se inserta en el centro de la dirección MAC Ethernet de 48 bits del cliente.
- El 7° bit de la dirección MAC del cliente se invierte del binario 0 al 1.
    - Ejemplo:

MAC de 48 bits	fc: 99:47:75:ce:e0
Id. de interfaz EUI-64	fe: 99:47:ff:fe:75:ce:e0

Proceso EUI-64 v/s Generado aleatoriamente

- Cuando el mensaje RA es SLAAC o SLAAC con DHCP v6 stateless, el cliente debe generar su propia ID de interfaz.
- La ID de interfaz se puede crear utilizando el proceso. EUI-64 o un número de 64 bits generado aleatoriamente.



LLAs dinámicas en Windows.

Los sistemas operativos, como Windows, suelen utilizar el mismo método tanto para una GUA creada por SLAAC como para una LLA asignada dinámicamente.

ID de interfaz generada mediante EUI-64

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix.
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:fc 99:47ff:fe75:cee0
Link-local IPv6 Address. . . . .: fe80::fc 99:47ff:fe75:cee0
Default Gateway . . . . . . . . . : fe80::1
C:\>
```

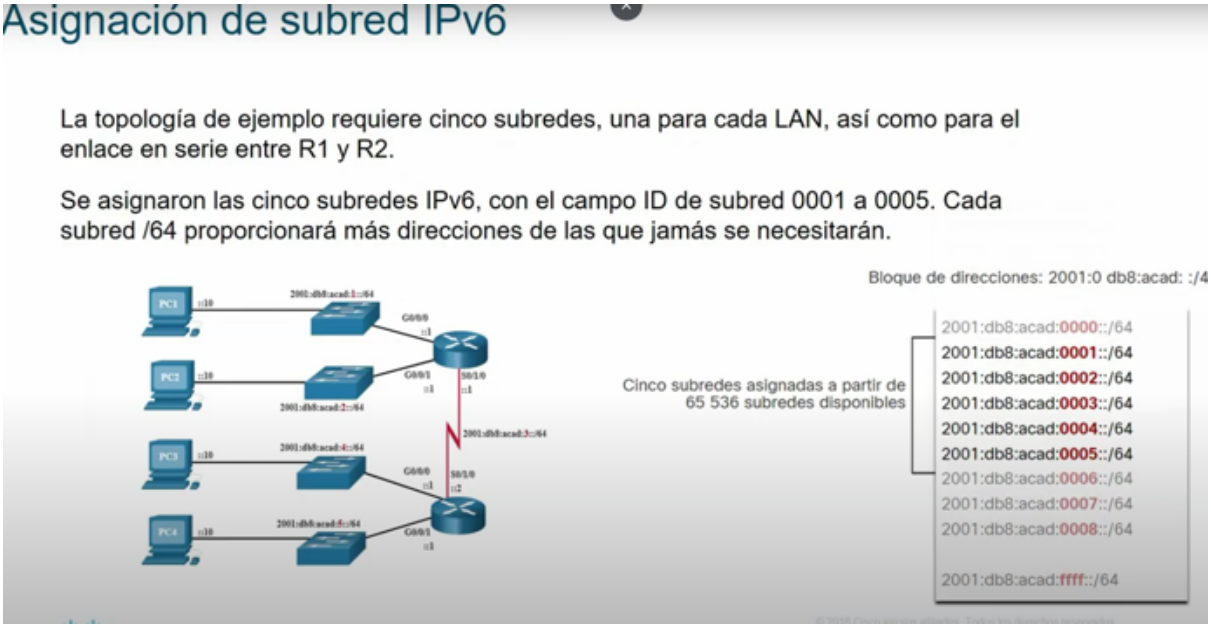
ID de interfaz de 64 bits generada aleatoriamente

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix.
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a 5:8 a35:a5bb:66e1
Link-local IPv6 Address. . . . .: fe80::50a 5:8 a35:a5bb:66e1
Default Gateway . . . . . . . . . : fe80::1
C:\>
```

Ejemplo de subneteo IPv6

Dado el prefijo de enrutamiento global 2001:db8:acad:: / 48 con un ID de subred de 16 bits.

- Permite 65.536/ 64 subredes.
- El prefijo de enrutamiento global es igual para todas las subredes.
- Solo se incrementa el hexteto de la ID de subred en sistema hexadecimal para cada subred.



Routing

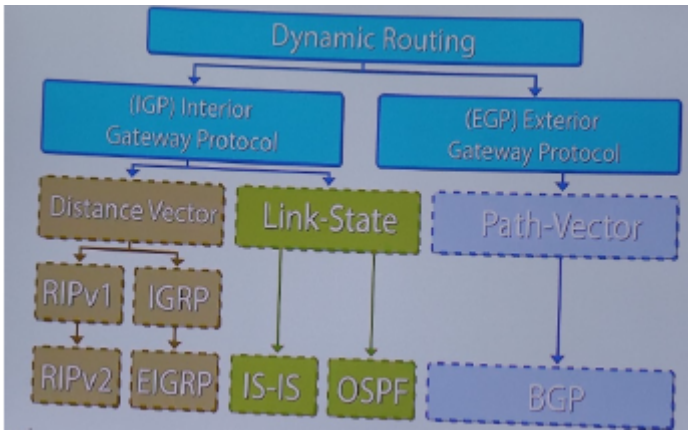
Sistema Autónomo

- Un AS está formado por un conjunto de routers que tienen
    - Un protocolo de routing común (también rutas estáticas)
    - Una gestión común
- La idea es:
    - conjunto de redes bajo una única administración técnica y política, caracterizada por compartir un protocolo de enrutamiento común.

Tipos de Sistemas Autónomos

- De conectividad Única
- De Tránsito
- De Múltiples conexiones sin tránsito (MultiHomed)

Dynamic Routing



Clasificación de los protocolos de enrutamiento Dinámico

- Interior Gateway Protocols (IGP)
    - Se utilizan para el enrutamiento dentro de un sistema autónomo
    - Utilizan sólo direccionamiento privado
    - Protocolos
        - RIP (Routing Information Protocol)
            - Protocolo de vector de distancia
            - Utiliza el algoritmo Bellman-Ford.
            - Envía actualizaciones periódicas de la tabla de enrutamiento.
            - Limitado en redes grandes debido a su conteo máximo de saltos.
        - OSPF (Open Shortest Path First)
            - Protocolo de estado de enlace
            - Utiliza el algoritmo de Dijkstra.
            - Crea un mapa completo de la topología de la red.

            - Eficiente al enviar actualizaciones solo cuando hay cambios en la topología.
        - EIGRP (Enhanced Interior Gateway Routing Protocol)
            - Protocolo híbrido.
            - Combina elementos de vector de distancia y estado de enlace.
            - Utiliza el algoritmo DUAL.
            - Actualiza rutas solo cuando es necesario y se adapta rápidamente a cambios en la topología.

- Exterior Gateway Protocol (EGP)
    - Enrutamiento en sistemas autónomos
    - Direccionamiento público
    - Protocolos
        - BGP (Protocolo de Gateway de Borde)
            - Permite que distintas redes intercambien información de enrutamiento, establezcan políticas y mantengan la estabilidad, siendo vital para la conectividad entre sistemas autónomos en la red global.

IGP Interior Gateway Protocol

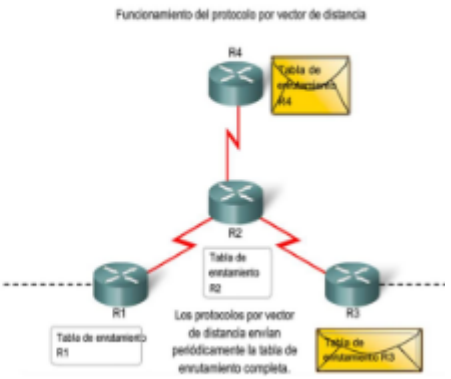
- Comparación de los protocolos de enrutamiento de vector distancia con los de ***estado de enlace***
- Se divide en
    - Distance Vector
        - RIPv1
            - RIPv2
        - IGRP
            - EIGRP
    - Link-State

Vector de distancia

- Las rutas se anuncian como vectores de distancia y dirección
- Brinda una vista incompleta de la topología de la red
- Por lo general, se realizan actualizaciones periódicas

Estado de enlace

- Se crea una vista completa de la topología de la red
- Las actualizaciones no son periódicas



Enrutamiento

- Clases de protocolos
    - Vector Distancia
        - Mejor ruta es la más corta
        - Envían completa tabla de enrutamiento
    - Híbridos
    - Estados de Enlace
        - El router crea tres tablas de enrutamiento
            - Neighbors
            - Topology
            - Internetwork
        - Conocen la red completa

Clasificación de los protocolos de enrutamiento

- Por cálculo de su métrica
    - Vector Distancia
        - RIP (Routing Information Protocol)
        - EIGRP (Enhanced Interior Gateway Routing Protocol)
    - Estado de enlace
        - OSPF (Open Shortest Path First)
- Por direccionamiento utilizado
    - ClassFul
        - IGRP: El Protocolo de Enrutamiento Gateway Interior Mejorado (IGRP) desarrollado por Cisco. Fue diseñado para encontrar rutas en redes de área extensa (WAN) y se basa en el concepto de vector de distancia, pero con mejoras significativas en comparación con los protocolos de enrutamiento tradicionales.
        - RIPv1
    - ClassLess
        - RIPv2
        - OSPF
        - EIGRP
        - IS-IS

Protocolos enrutamiento ClassFul

- **NO ENVIAN** la máscara de subred durante las actualizaciones de enrutamiento

Protocolos enrutamiento ClassLess

- **ENVÍAN** la máscara de subred durante las actualizaciones de enrutamiento

Criterios de Enrutamiento

- Métricas
    - Vector Distancia
        - RIP
        - EIGRP
    - Estado de enlace
        - OSPF
- Direccionamiento utilizado

    - ClassFul
        - RIPv1
            - No transmiten la máscara
    - ClassLess
        - RIPv2
        - OSPF
        - EIGRP

Métricas de Protocolos de Enrutamiento

- Métrica se usa para cada protocolo de enrutamiento
    - RIP
        - Número de saltos
    - IGRP y EIGRP
        - Usan ancho de banda, retraso, carga, confiabilidad
    - IS-IS y OSPF
        - Implementación de Cisco
- MÉTRICA
    - Es un valor que usan los protocolos de enrutamiento para determinar que rutas son mejores que otras
- Algunas métricas de enrutamiento son:
    - Ancho de Banda
    - Delay (retardo)
    - Load (carga)
    - Reliability (confiabilidad)
    - Hop Count (Saltos)
    - Cost (Costo)

Distancia Administrativa

Origen	Distancia Default
Directamente Conectado	0
Ruta Estática	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120

Tabla de Rutas

- Routers y host mantienen en todo momento una tabla de rutas que indica por cual interfaz deben mandar un paquete, en función de la dirección destino.

3 Tipos de Rutas

Rutas C (redes directamente conectadas)

- Aparecen automáticamente al configurar la dirección IP

Rutas S (estáticas)

- Se a;aden en la configuración del equipo mediante el comando route

Rutas Dinámicas

- Son todas las demás
- No figuran en la configuración del equipo y pueden variar con el tiempo

Enrutamiento

Protocolos Vector Distancia

- Enrutamiento por rumor
- Envían Actualizaciones cada x segundos
- Su convergencia es lenta
- Problemas
  - Inconsistencia en la tabla de enrutamiento
  - Loops

RIP (Routing Information Protocol)

- Sufre de problemas típicos del vector distancia
- Solo útil en redes pequeñas (5 - 10 routers)
- No permite usar múltiples rutas simultáneamente (algunas si)
- No soporta Subredes con máscaras de tamaño variable
- RIPv1
  - Classfull
  - BroadCast
  - No autentificación
  - Bellman-Ford
  - AD 120
  - UDP 520
  - Hop Count

- RIPv2
  - ClassLess
  - MultiCast 224.0.0.9
  - Autentificación MD5
  - Bellman-Ford
  - AD 120
  - UDP 520
  - Hop Count

IGRP y EIGRP (Interior Gateway Routing Protocol y
Enchanced IGRP

- Protocolos propietarios de Cisco
- Resuelven problemas de RIP
  - Métrica sofisticada
- Incluye soporte multiprotocolo
- Mejoras de EIGRP sobre IGRP
  - Soporta Subredes
  - Incorpora diversos mecanismos para evitar el problema de la cuenta a infinito

OSPF (Open Shortest Path First)

- Protocolo estandar
- Protocolo de estado de enlace
- Utiliza algoritmo Dijkstra SPF
- ClassLess
- Autenticación: plain MD5
- Descripción general
    - Basado en el algoritmo estado de enlace
        - Dos Niveles Jerárquicos
        - Área 0 o Backbone
        - Áreas adicionales

    - Utiliza algoritmo distancia Dijkstra SPF
        - Velmanfor
        - Resuelve los problemas de RIP
        - Rutas de red, subred, host
        - Admite métricas complejas. Prácticamente solo se usa ancho de
        - banda
        - Tráfico repartido en múltiples rutas si tienen mismo costo

- Usa 3 tablas
    - Neighbor
    - Topology
    - Routing
    -

Clases de routers en OSPF

- Backbone
    - se encuentran en el ÁREA 0
- Internos
    - Pertenecen a una sola área
- Frontera de Área
    - conectan dos o más áreas
        - Una de estas debe ser backbone
- Frontera de AS
    - conectan con otros ASes.
    - Pueden serta en backbone o en alguna otra área

Tipos de Rutas en OSPF

- Intra-Área :
    - Las determina directamente el router
- Inter-Área
    - Se resuelven en 3 fases
        - Hacia el router backbone en el área
        - Hacia el área de destino en el backbone
        - Hacia el router en el área destino

IS-IS Intermediate System - Intermediate System

- IS significa router en “ISOese” (Host es ES, End System)
- Muy similar OSPF
- Protocolo habitual en las grandes redes (ISPs). Se utiliza en RedIRIS
- Soporte multiprotocolo

BGP Border Gateway Protocol

- Algoritmo de vector distancia modificado: además de la interfaz y el costo se incluye la ruta completa en cada caso
- La métrica suele ser número de saltos (por ser vector distancia)

Protocolo de Routing Externo (entre ASes): BGP

- Usado en prácticamente todos los proveedores de internet en la comunicación de rutas entre ASes

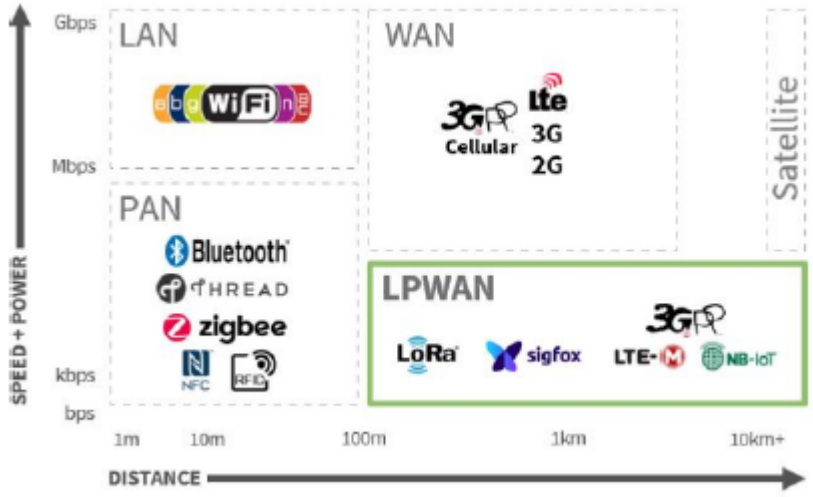
Protocolos de Routing de Internet

Protocolo	Algoritmo	Subredes	Métrica compleja	Notifica Actualiz.	Niveles jerárquicos	Estándar
RIPv1	Vector Distancia	NO	NO	NO	NO	SI
RIPv2	Vector Distancia	SI	NO	NO	NO	SI
IGRP	Vector Distancia	NO	SI	NO	NO	NO
EIGRP	Vector Distancia	SI	SI	SI	NO	NO
OSPF	Estado Enlace	SI	SI	SI	SI	SI (Internet)
IS-IS	Estado Enlace	SI	SI	SI	SI	SI (ISO)

Redes inalámbricas - próxima generación
Gracia de redes inalámbricas

- Pueden ser Fijas
- Móviles (Primordial)

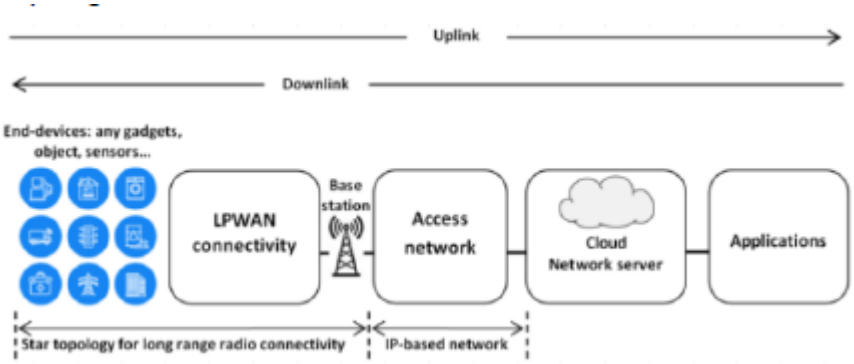
#Red wifi funciona en modo infraestructura



LP WAN Wide area network

- Low Power Wide Area Network, Red de área amplia de baja potencia u ancho de
- banda
- Redes de bajo consumo
- Amplia Cobertura
- Redes exclusivas para el IoT
- Mínimo ancho de banda
    - Ya que manda un chorro discontinuo

Topología LPWAN



Dispositivos Finales

- Sensores
- Actuadores
- Esta base Station muestra que es una Punto Multipunto
- Uplink: acceso
- Downlink: comando
- Cloud Network Server: Es una red de datacenter
    - Aqui dentro esta el servidor de aplicaciones
- Si es monitoreo, es de endevices a aplicaciones

LoRa

- Long Range
- Es una tecnología inalámbrica que emplea un tipo de modulación en radiofrecuencia patentado por smetch.
- Modulación CSS (Toma datos Análogos o discretos, y los transforma en señales)

LoRaWAN

- Es una red para conectar dispositivos finales IoT y conectar dispositivos IoT
- Son los gateways y nodos de red que usa la tecnología LoRa, para redes LPWAN.
- LoRaWAN es empleado para comunicar y administrar dispositivos LoRa

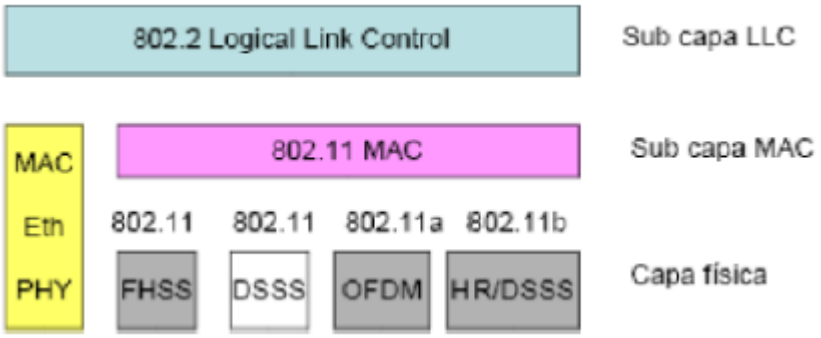
#Ventajas redes anilladas, no importa donde se corte, siempre tiene respaldo

Introducción

- Las redes inalámbricas IEEE 802.11 presentan una gran ventaja sobre las redes ethernet
- Ejemplo:
    - Acceso inalámbrico a base de datos permite a los usuarios agregar desde dispositivos móviles pequeñas cantidades
- El mayor uso de redes WLAN es extender redes de cobre proporcionando movilidad a los usuarios

Arquitectura

- Las especificaciones IEEE 802 se focalizan en las dos capas inferiores de la arquitectura ISO OSI. Todas las LAN comparten capa MAC



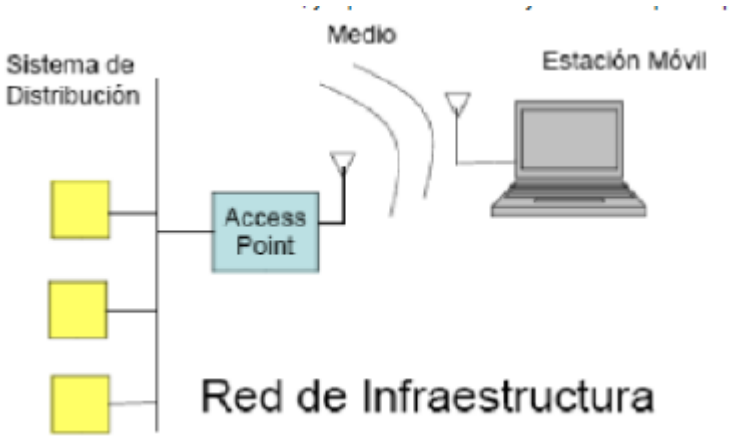
#Capa 2 se divide en Sub capa MAC (más cercana a la física), y Logical Link Control

Capa Física

- Las ondas de radio imponen requerimientos complejos a la capa física
- Esta se separa en 2
    - PLCP
        - Procedimiento de convergencia (Mapeo de frames MAC al medio)
    - PMD
        - Dependencia del medio (Se ocupa de la transmisión del frame)

Componentes de una LAN 802.11

- Líneas son los switch
- Cuadrados son los PC (LAN)
- Lo mas importante es la movilidad
    - WIMAX
- Acces Point genera un área básica de servicios, su característica principal es que es intrínsecamente difusa, ya que en las áreas hay obstáculos que bloquean la señal



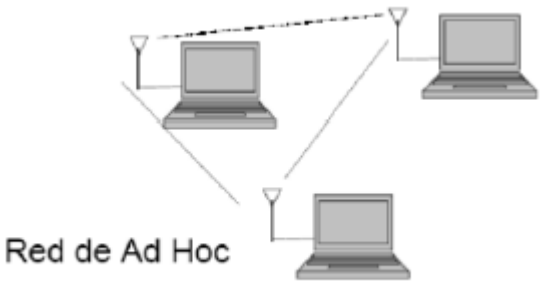
BSS (Conjunto básico de servicios)

- El bloque constructivo de una red inalámbrica es llamado Conjunto Básico de servicios BSS
    - BSS es una bloque constructivo de red inalámbrica
- BSS es un conjunto de estaciones que se comunican unas a otras
- Comunicación tiene lugar dentro de un área de límites difusos llamada Área Básica de Servicios

Dos tipos de BSS

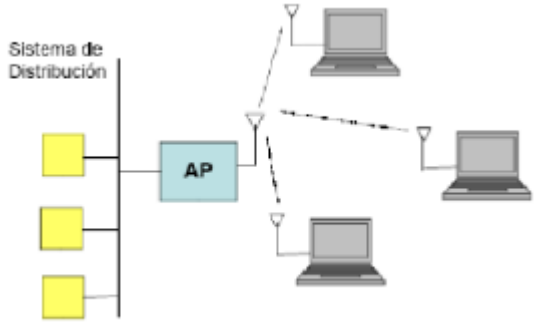
Redes Ad-hoc o independientes

- Son redes entre maquinas moviles
- Se llaman Ad-hoc porque no requieren access point
- Se puede hacer mediante la tarjeta de red



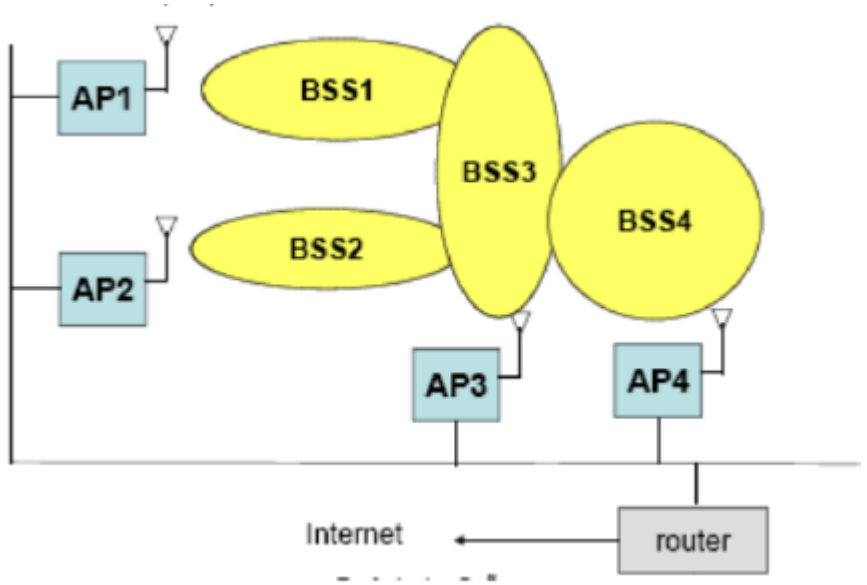
Redes de infraestructura

- Utilizan el dispositivo Acces Point
- Comunicación entre dos estaciones dentro de una misma área de servicios necesita dos saltos (YO - Acces Point - Otro)
- BSS se define por el área del AP
- AP está en condiciones de asistir a las estaciones móviles frente a problemas de energía



Área de Servicio Extendidas (ESS)

- Los BSS solo pueden cubrir áreas limitadas
- ESS es un conjunto de BSS, los cuales son generados por access point
- 802.11 puede extender su área de servicios a través del Conjunto Extendido de servicios (ESS)



- LOS AP ACTÚAN COMO BRIDGES

El sistema de Distribución

- Es responsable de actualizar la ubicación física de las estaciones y despachar correctamente los frames.
- El ESS entrega soporte de movilidad a estaciones (Roaming)
    - Para que haya roaming debe hacer comunicación entre Access points

La Subcapa MAC

- A dif de ethernet, las redes 802.11 son altamente parametrizables
- Necesariamente, por razones de crecimiento, llegará el momento de hacer una sinfonía final a la red para mejorar su desempeño
- Para ajustar una red, es necesario involucrarse y entender su funcionamiento

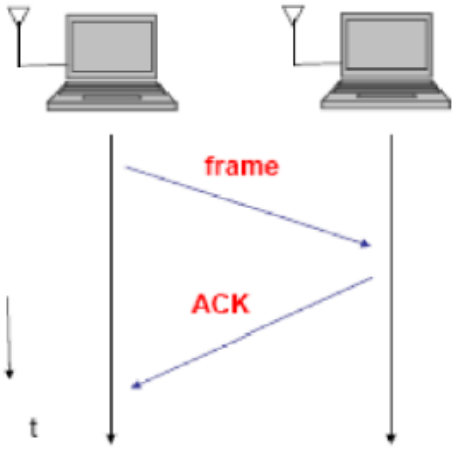
CSMA/AC

- A diferencia de ethernet, las colisiones no se detectan sino que se EVITAN
    - Ya que los pc saben cuando y cuando no deben transmitir
- Al igual que ethernet, 802.11 usa CSMA para lograr acceso al medio de transmisión.
- Protocolo de acceso al medio es distribuido

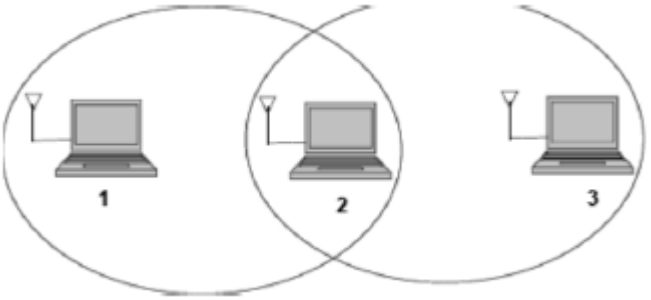
Interferencias

- Para la transmisión se utiliza una banda de frecuencia sin licencia llamada ISM
    - ISM -> 2400 - 2483 mHz
        - -> 900 MHz
        - -> 5.8 Ghz

      Investigation Scientifical Medical
- 802.11 está sometida a muchas fuentes de interferencia
    - Hornos de microondas
    - Teléfonos inalámbricos
    - dispositivos bluetooth
- Debido a estas condiciones agresivas, 802.11 incorpora ACK, a todo frame transmitido
    - ACK: manda una trama y le pregunta al receptor “llego bien?”, si es positivo, retorna un ACK, sino es positivo entonces
- Interferencias causas errores



Problema del nodo oculto

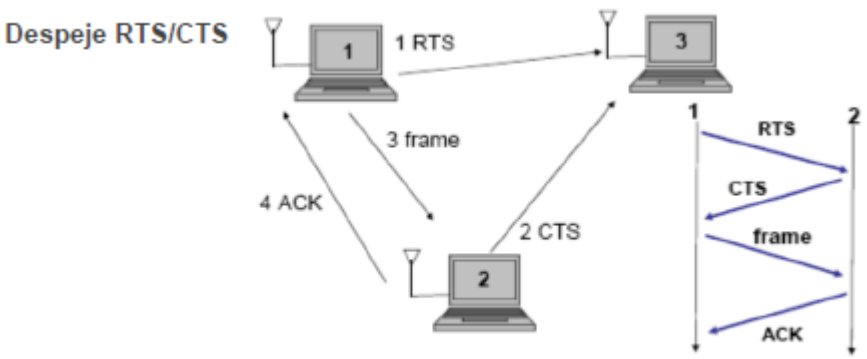


- Desde la perspectiva del nodo 1, el 3 está oculto y por lo tanto es posible que ambos se transmitan simultáneamente en cuyo caso se produce una “colisión” difícil de detectar.
- A dif de Ethernet, las colisiones no se pueden detectar porque los transceivers de radio son Half Duplex
- Existen fronteras difusas donde existen nodos que no se pueden comunicar con otros

Procedimiento RTS/CTS

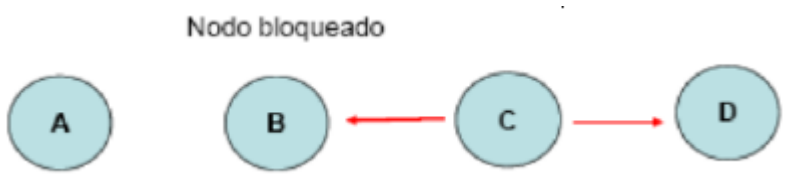
- RTS (Request to send)
- CTS (Clear to send)
- Para solucionar este problema, es necesario “Despejar” el área de transmisión utilizando frames RTS y CTS
- Estación que quiera transmitir, envía un RTS, un campo de este frame indica el tiempo de transmisión NAV

- ACOMPLETA
- La estación receptora contesta con CTS. Al igual que RTS, CTS indica el tiempo restante que es necesario silenciar el área
- El intercambio RTS/CTS consume una fracción importante de la capacidad del canal
    - Por ello, se configura el umbral RTS threshold para ser utilizado solo por frames mayores que este umbral



Problema del Nodo Expuesto

- Estación C esta transmisión a D
- B está escuchando y queda bloqueado
- B no puede transmitir a A, por estar bloqueado por C



Acceso al medio Inalámbrico

- Es controlado por funciones de coordinación
    - “Función de coordinación”
        - Provee acceso al medio similar a Ethernet
- Antes de transmitir, verifica si medio está ocupado.
    - Evita colisiones mediante Backoff aleatorio después de cada frame

Detección de Portadora

Dos formas de detectar una portadora:

Real

- Utiliza las capas físicas los adaptadores pueden saber si el medio está ocupado. No proporciona toda la información

Virtual

- Esta forma es provista por el campo NAV de un frame de esta forma se sabe si el canal esta ocupado o no.

NAV

- Campo del frame y representa un timer que indica Tiempo de Reserva
    - Si este es 0, el medio está disponible

Espaciamiento Interframe

DIFS

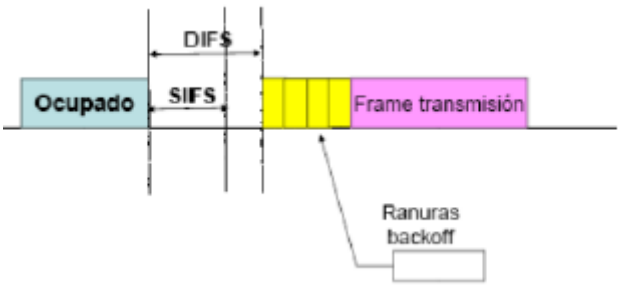
- DCF Interface space. Estaciones tienen acceso inmediato al médio si está libre

EIFS

- No es fijo y se usa solo cuando se registra un error en la transmisión

Diagrama de tiempos

- SIFS Short interface system:
    - Tiempo en microsegundos requerido por una interfaz inalámbrica para procesar un marco recibido y responder con un marco de respuesta

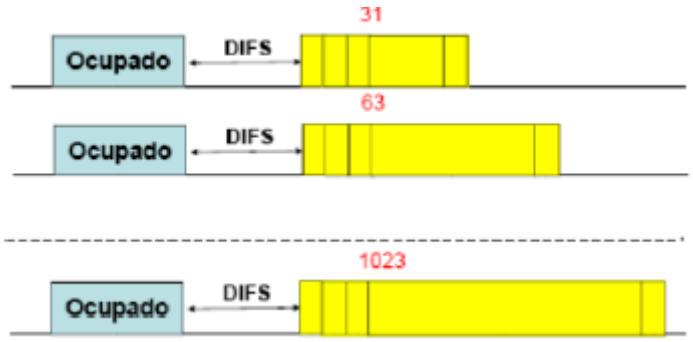


Acceso basado en contención

- Algoritmo de acceso es el siguiente:
    - Se debe verificar que medio esté desocupado antes de transmitir, esto mediante backoff exponencial, para evitar colisiones
    - Si tiempo del medio desocupado > DIFS => Transmite inmediatamente.
- Cada trama o fragmento de trama tiene asociado un contador de reintentos
- De los errores se responsabiliza la estación que envía el frame
- Todos los frames Unicast deben ser reconocidos

Backoff en DCF

- Si estación móvil quiere transmitir y medio está ocupado => Entra en contención
- El tiempo que sigue a continuación de DIFS se denomina ventana de contención.
    - Ventana de contención depende de las ranuras de tiempo de la capa física.
    - Moneda al aire aleatoria que determina cuando voy a ocupar el canal
- Cada vez que falle la transmisión, se duplica la contención



Fragmentación y Reensamblado

- Es en la subCapa MAC de la ISO/OSI
- Las tramas muy largas tienen mas probabilidad de echarse a perder, ya que aumenta la cantidad de kb, y con ello aumenta la probabilidad de que se interfiera
- La fragmentación mejora el desempeño porque permite retransmitir sólo el fragmento del frame.
- Usualmente el umbral de fragmentación tiene mismo valor que RTS/CTS Threshold

La Capa Física

- ¿Qué es eficiencia espectral?
    - Se mide en Bits por Hz
- Los moduladores tienen distintas performance, que en un espectro meten pocos bps, pero hay otros que pueden agregar muchos mas bps, estos son llamados inteligentes
    - Las señales que salen de los moduladores pueden ser Discretas
    - Los “Data” pueden ser Digitales o
- Inicialmente se establecieron 3 capas físicas
    - FHSS
        - Frequency-Hopping spread-spectrum

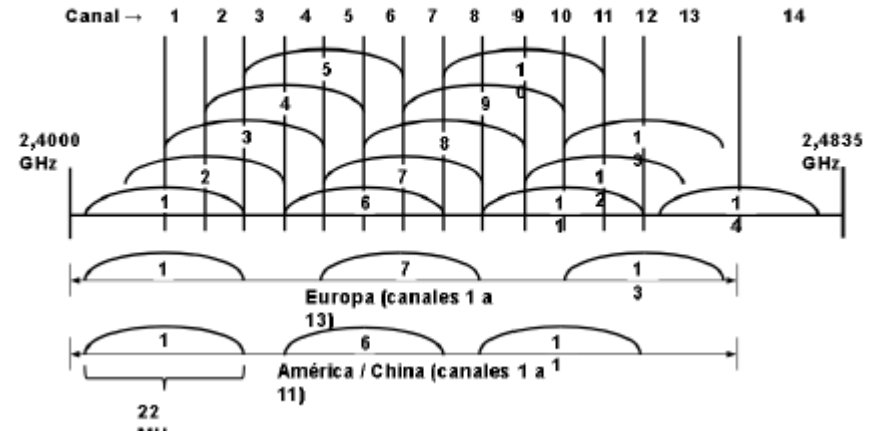
- DSSS:
  - Direct-Sequence Spread-spectrum
- IP
  - Infrarrojo
- OFDM
- High-Rate Direct Sequence Spread-Spectrum
  - Estos son los equipos WIFI (802.11b)
- Capas en investigación
  - UWB
    - Ultra Wideband
- MIMO
  - Utilizan múltiples antenas para la transmisión
  - WIFI 6 utilizan varias MIMO

LA TECNOLOGÍA MÁS UTILIZADA EN LA BANDA ISM ES SPREAD SPECTRUM.

DSSS

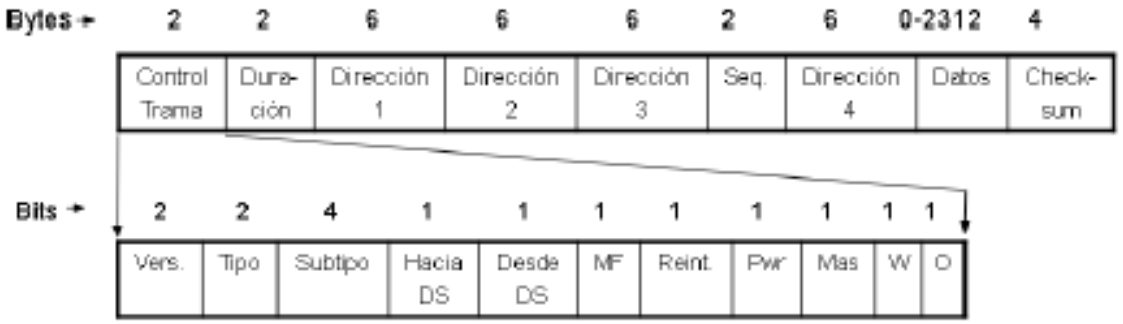
- Trabaja en la banda llamada ISM en 2.4Ghz
- Determina la señal en un ancho de banda de 22 Mhz
- Las tasas de transmisión pueden ser de 1, 2, 5.5, y 11Mbps dependiendo de la calidad del link.
- Un AP tiene un rango de 10 a 300m, dependiendo del ambiente
- Las distintas frecuencias que utilizas DSSS se denominan canales.
- Potencia máxima aprox 100mW
- **Normalmente** los equipos vienen con canales del 1 al 11

Reparto de canales a 2.4Ghz



Formato de Trama 802.11

- Checksum detecta errores mediante CRC, mediante un polinomio matemático
- Cantidad máxima de Bytes de una trama 2346
    - Un bitio dura $[1/11 * 10^{11,-1}]$ segundos

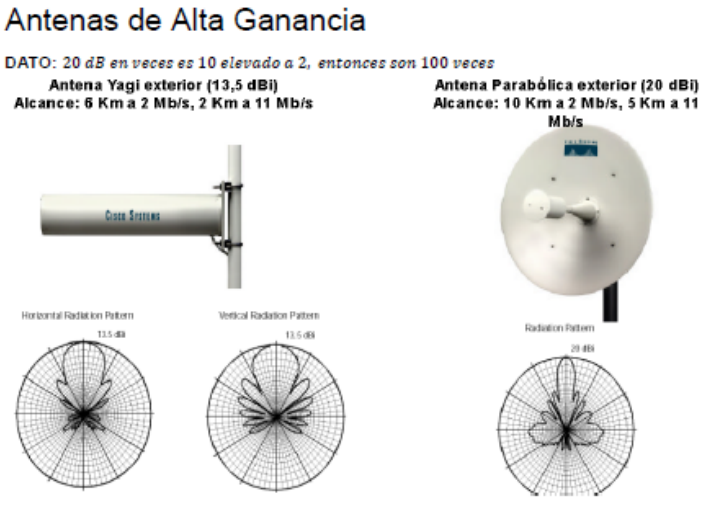


- VERS, permite la coexistencia de varias versiones del prototipo
- TIPO, indica si es una trama de datos, de gestión o de control
- SubTipo, indica si es una trama RTS o CTS
- Hacia DS
- Desde DS
- MF
- Reint
- Pwr
- Mas
- W
- O; las tramas que tengan puesto este bit se han de procesa por orden
- Duración
    - Dice cuánto tiempo va a estar ocupado el canal por esta trama
- Dirección 1,2,3,4
- Seq

Antenas

- Tienen dos características
  - Ganancias referido a lo isotrópico
    - Antenas isotrópicas tienen un radio, ya que reparten la señal por todo el radio. Antenas reales no se parecen a las isotropicas
  - Lobulo de Radiacion

- Los tipos de antenas utilizados en redes 802.11 son los siguientes:
  - Omnidireccionales, transmite en todas direcciones en un plano horizontal
  - Antenas de Parche
  - Antenas Yagi
  - Antenas parabólicas
- Antena es un dispositivo pasivo, normalmente const|ruida de metales, la cual recibe potencia electromagnética que transforma a señal electromagnética radiada.
  - En simples palabras palabras, es un transformador de energía
- WIFI trabaja a 100mW



Relación antena-potencia

- Fijan una potencia máxima para no afectar la salud de las personas

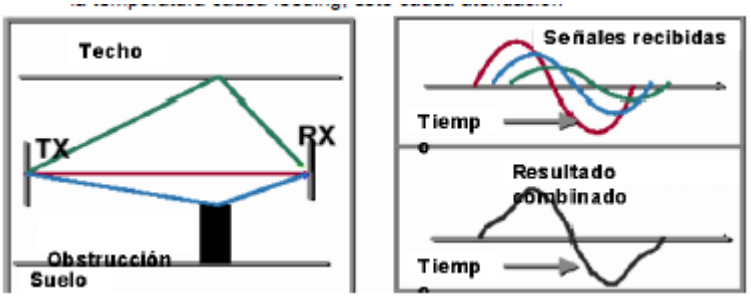
Ganancia (dBi)	Pot. Máx. (mW)
0	100
2,2	50
5,2	30
6	30
8,5	5
12	5
13,5	5
21	1

Interferencias

- las WLAN están sometidas a muchas fuentes de interferencias, pero una de ellas es la misma red
- Las interferencias generan distorsión
- Existen dos interferencias internas
    - Co Canal
        - causada por dispositivos transmitiendo en el mismo canal
    - InterCanal:
        - Causadas por dispositivos transmitiendo en canales adyacentes

Interferencia debido a la multitrayecto

- Las diferencias de temperatura hacen que la reflexión cambie… mientras más baja la temperatura causa feeding, esto causa atenuación.



● FHSS es más resistente a la interferencia multitrayecto que DSSS

Administración

- Establecer un nuevo enlace inalambrico en una red de infraestructura se requieren los siguientes pasos
    - Scanning
        - Identificar redes disponibles.
    - Joining
        - Seleccionar una red para conectarse.
    - Autenticación
        - ¿Quién sos vos?
        - Autorización
    - Asociación
        - Registrar la estación con un punto de acceso y asignarle un identificador único. Permite el acceso completo a la red.

Scanning

- #SSID: Nombre que le ponemos a la WLAN
    - Si se desea conectarse a cualquier red, este valor se configura como SSID de broadcast
- El scanning es el proceso de identificar WLAN existentes dentro de un area.
- Parámetros más utilizados en el Scanning
    - BSSType: busca el tipo de red (ad hoc, infraestructura, cualquiera)
      BSSID: identificado de BSS: 48 bits, especifica la red a buscar
    - SSID
    - ScanType:
        - Pasivo: Trama beacon está avisando “aquí estoy yo”, es una luz de faro que va dirigida a los que están en el área de cobertura
        - Activo: utiliza la transmisión de un frame llamado ProbebRequest para descubrir redes.
    - ChannelList Lista de canales que escucha una estación móvil para encontrar alguna WLAN
    - ProbeDelay: Retardo en microsegundo antes del comienzo de un scanning activo.
- MinChannelTime y MaxChannelTime
        - Establecen tiempos minimos y maximos de scan sobre cualquier cana
          l

Scanning Pasivo

- No envía una petición de búsqueda, sólo escucha
- Ahorra energía porque está en modo “escucha”
- Estación móvil recorre canal por cable del ChannelList y escucha frames Beacon. Registra la información de los frames que recibe

Joining

- Al terminar Scanning, se genera un reporte de Scan. Con esto se realiza un Join.
- Una estación móvil puede hacer un Join con algunos BSS
- No es suficiente para lograr acceso, requiere los pasos de autenticación y asociación
- Elegir BSS para Join es una decisión específica de cada implementación que puede involucrar al usuario.

Autentificación

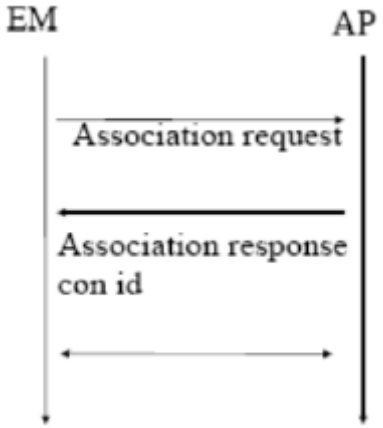
- 2 Aproximaciones para la autenticación WI-FI
    - Autenticación Abierta
        - AP acepta una estación móvil sin verificar su identidad
    - Autentificación por llave compartida
        - Se basa en el protocolo WEP (wireless equivalent protocol) y requiere que ambos dispositivos implementan WEP
        - Wired Equivalent Privacy: 1er Estándar de seguridad para redes WIFI

Asociación

EM: Estaciones móviles

- Mantención de un registro de asociación le permite al sistema de distribución hacer un seguimiento de las EM para despachar correctamente los frames
    - La asociación z es propia de las redes de infraestructura
    - 802.11 no especifica como la asociación se puede garantizar
    - La Asociación permite el acceso completo a la red

Procedimiento de Asociación



Reasociación

- Consiste en llevar una EM desde un AP a otro
    - Inalámbricamente, el procedimiento es similar a la asociación
    - El procedimiento se inicia cuando una estación móvil detecta que otro ap tiene una señal con mayor potencia
    - En sistema de distribución, AP deben interactuar unos con otros para mover frames

Ahorro de Energía

- Hay que minimizar el tiempo en el cual el dispositivo está en modo activo y maximizar los modos pasivos
- En una red de infraestructura, los AP pueden monitorear la energía de la EM
- Estaciones que operan en ahorro de energía pueden escuchar frames beacon que reportan stas buffers //revisar
    - Frames Beacon
        - Son paquetes de datos transmitidos periódicamente por un punto de acceso (router) en una red inalámbrica.

    - Stats Buffers
        - Almacenamiento temporal utilizados para recopilar y almacenar estadísticas relacionadas con el rendimiento de la red.

- Si AP conoce modos de manejo de energía de todas las estaciones móviles asociadas puede:

    - Almacenar en buffers frames de EM que operan en modo Ahorro de Energía.
    - Enviar anuncios periódicos de estatus de buffers a las EM que están en ahorro de energía