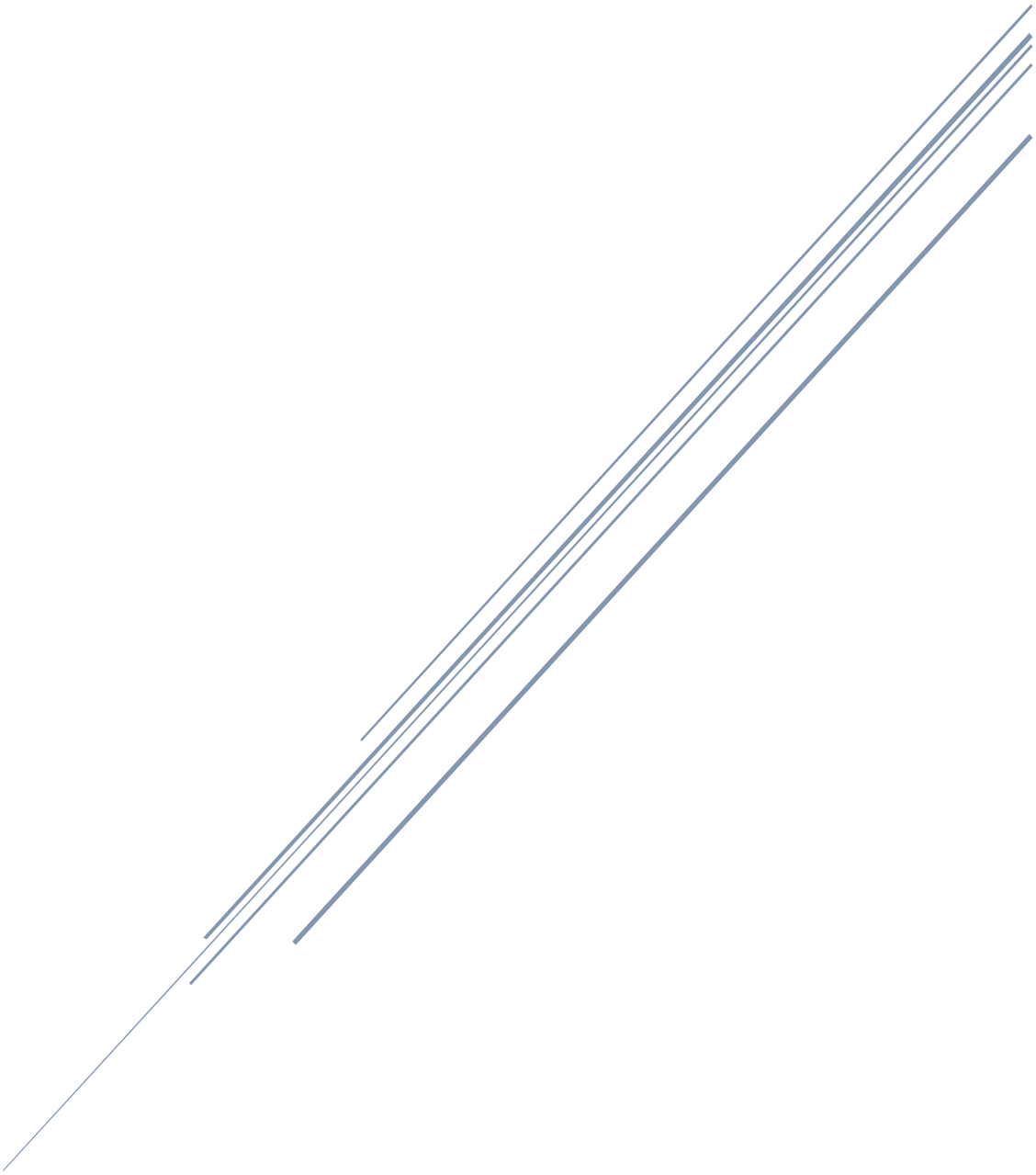
Andrés Montes Álvarez

RESUMEN REDES 1 ASIR

Andrés Montes



IES La Arboleda

Administración de Sistemas de información y Redes

Contenido

Andrés Montes Álvarez

Información de la excursión de 5G

Que es son las redes 5G

El 5G, abreviatura de quinta generación, es la última generación de tecnología de redes inalámbricas móviles. Es la sucesora del 4G LTE y está diseñada para proporcionar una conexión de alta velocidad, menor latencia y mayor capacidad en comparación con sus predecesoras

El 5G Utiliza frecuencias más altas en el espectro radioeléctrico, como las bandas de ondas milimétricas, para transmitir datos a velocidades mucho más rápidas. Estas frecuencias más altas permiten un mayor ancho de banda y una capacidad mejorada para transmitir grandes volúmenes de datos.

Preguntas de Profe

2-Compartición antenas. Explicación
Que varias empresas comparten la misma antena ya que crear nuevas tienen mucho coste, teniendo en cuenta que la empresa dueña de la antena se coloca en la parte mas alta de la misma para tener la mayor capacidad de conexión
3-Dividendo digital. Explicación
El dividendo digital es la reorganización de la asignación de frecuencias de transmisión de televisión, para liberar una porción de la banda de frecuencia utilizada por la televisión analógica y asignarla a otros servicios de comunicación inalámbricos como la telefonía móvil, internet móvil, entre otros.
4-¿qué funciona con 2G, por qué existe aun?
La mayoría de datafonos utilizan 2G aunque y están usando 4G en los nuevos pero como aun sigue en uso la necesitamos no como la 3G que ya esta casi en desuso
5-Tiempo de concesión banda de 26GHz.
Durante 20 años
6-¿qué significa 4G+?
Que estoy conectado a 4G con cualquiera de los protocolos que me permiten ir un poco mas rápido HSDPA,HSUPA, HSPA +
7-Logo 5G en el móvil. ¿Qué significa cuando aparece?
Aparece cuando aunque la antena no sea 100% 5G tiene el NR del 5G, teniendo en cuenta que no siempre nos conectamos a una antena 100% 5G por lo que siempre que estemos conectados a 1 antena 5g aunque en la caseta tengamos la configuración de 4G nos pondrá que tenemos 5G.
En cualquier caso de los siguientes nos muestra 5G en el dispositivo aunque el núcleo no sea 5G
8-Downlink y uplink
Uplink es cuando nos conectamos desde el móvil a la antena por ejemplo y downlink es cuando la antena se conecta con nuestro dispositivo
9-FDD y TDD
FDD transmisión por frecuencia y TDD transmisión por tiempo
10-Sectorización de antenas
La sectorización de antenas se refiere al proceso de dividir una antena en múltiples sectores de cobertura más pequeños y direccionales, con el fin de mejorar la capacidad, la calidad y la eficiencia de las comunicaciones inalámbricas en una determinada área geográfica.
Por lo general, una antena omnidireccional tradicional emite señales en todas las direcciones, lo que puede provocar interferencias y disminuir la calidad de la señal. La sectorización de antenas permite concentrar la energía de la señal en un área específica, lo que aumenta la eficiencia y la capacidad de la red.
11-Beamforming

Beamforming es una técnica utilizada en sistemas de antenas para enfocar la energía de la señal en una dirección específica, mejorando así la calidad de la señal y la eficiencia del sistema. En lugar de transmitir señales en todas las direcciones, como lo hace una antena omnidireccional tradicional, el beamforming utiliza una matriz de antenas para enfocar la señal en una dirección específica.
12-Mimetizado antenas
Que las antenas se mimetizan con el entorno lo que nos permite esconder las antenas a la vista humana y no son tan llamativa
13-¿Qué es un modelo de propagación?
Un modelo de propagación es un conjunto de ecuaciones matemáticas que se utiliza para predecir cómo se propaga una señal electromagnética en el espacio. Estos modelos se basan en la teoría de ondas electromagnéticas y tienen en cuenta una variedad de factores que pueden afectar la propagación de la señal, como la frecuencia de la señal, la altura y el tipo de antena, el terreno y los obstáculos en el camino de la señal.
14-Antenas omnidireccionales y sectoriales
Las omnidireccionales son las que apuntan a 360ª a a la vez y las sectoriales se divide un área de 360 grados en 120 grados cada uno porque asi mejoramos la eficiencia y dividimos el trabajo entre las antenas correspondientes.
15-¿Para qué sirve el GPS en antenas?
Para aparte de conocer la localización de la misma para sincronizar la hora de un lugar en especifico
16-Foto de antena radioenlace. ¿Ves el otro extremo?
NO he encontrado ninguna radioenlace.
99-Cuenta lo que más interesante te pareció de la visita.
Que nos puedan mentir en la cara las compañías con el 5G

Subneting IPV6

Primero ¿que es el IPv6?

El Protocolo de Internet versión 6, en inglés: Internet Protocol versión 6 (IPv6), es una versión del Internet Protocol (IP) y diseñada para reemplazar a Internet Protocol versión 4 (IPv4)

Principales diferencias entre IPv6 u IPv4

-La primera y mas notoria de todas es que IPv6 utiliza hexadecimal como los números que definen una red ETC mientras que IPv4 utiliza número decimales.

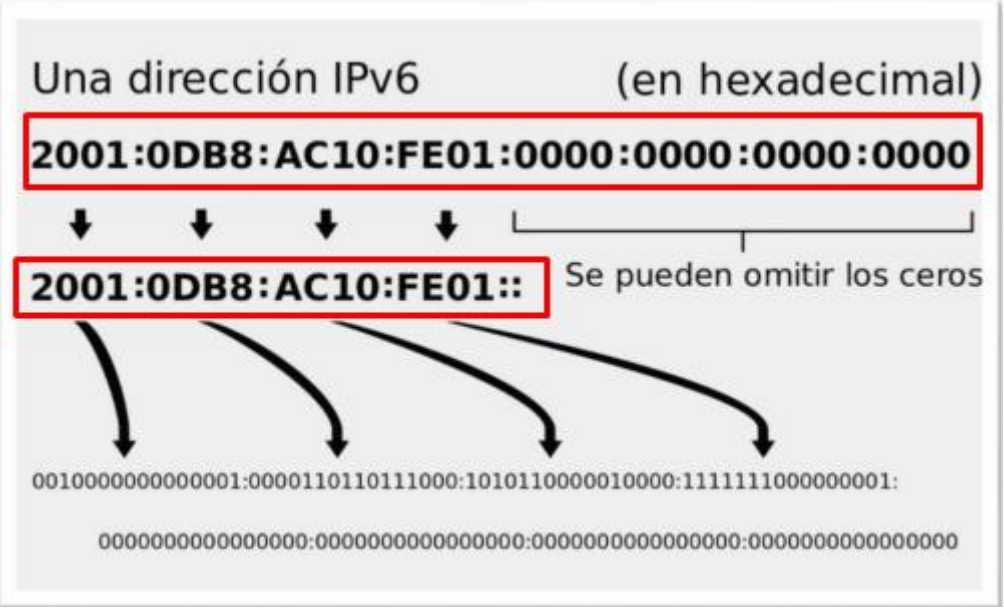
-La longitud de las mismas es distinta en el caso de la IPv6 son 128 bIts por IP mientras que las IPv4 son 32bits por red.

-Al tener mas bits por IP nos permite enviar mas datos en menos tiempo ya que las caebceras de información y los datos que podemos enviar son mayores.

-La longitud de las cabeceras IPv4 son de 32 bits mientras que las de IPv6 son de 128 bits.

-La IPv6 se divide en 8 hextetos mientras que los IPv6 son 4 octetos .

Características de las redes IPv6.



-La IPv6 se divide en 8 hextetos de 16 bits por campo.

-Las redes IPv6 si los últimos dígitos son ceros se pueden omitir poniendo ::

¿Cómo se expresan las direcciones IPv6?

Puede expresarse de esta forma:

- 2001:CB:1:1108: BA:0000:0000:A00.

Tambien podemos expresar un conjunto de hextetos con solo 0 con ;; esto abrevia la configuración de las derecciones IPv6.

- 2001:CB:1:1108:00BA:0000:0000:A00

Aquí te dejo un ejemplo.

- 2001:CB:1:1108:BA::A00

Esos dos puntos significa toda esta ristra de 0.

2001:CB:1:1108:00BA:0000:0000:A00

Direcciones Unicast Global: Estas direcciones son parecidas a las direcciones públicas IPv4. Se pueden enrutar hacia el internet y son asignadas por un ISP.

Direcciones Link Local: Estas direcciones son usadas por los dispositivos para comunicarse con otros que se encuentran en el mismo segmento (subred) . No se pueden enrutar fuera de un determinado segmento. Estas direcciones se encuentran en el rango FE80::/10, esto significa: FE80:/10, los primeros 10 bits son fijos, no sufren modificación.

¿Como hacemos Subneting con estas redes ipv6?

Si tenemos la siguiente IPv6:

2001:DB8::/32

Y quiero que esta IP se divida para que tengamos :

/32 => /48

/48=> /56

/48 =>/50

Entonces debemos hacer lo siguiente(Las siguientes son todas direcciones de RED).

2001:DB8:0000::/48

2001:DB8:0001::/48

2001:DB8:0002::/48

2001:DB8:0003::/48

Ahora vamos a coger la que acaba con 0001 ya que no nos piden limite de redes por suneteo sino que nos dan via libre por lo cual 2^16 bits por octeto tenemos 65550 Ips asignables, asi que ahora vamos a delimitar la primera IP disponible la ultima IP disponible la de red y la de broadcast.

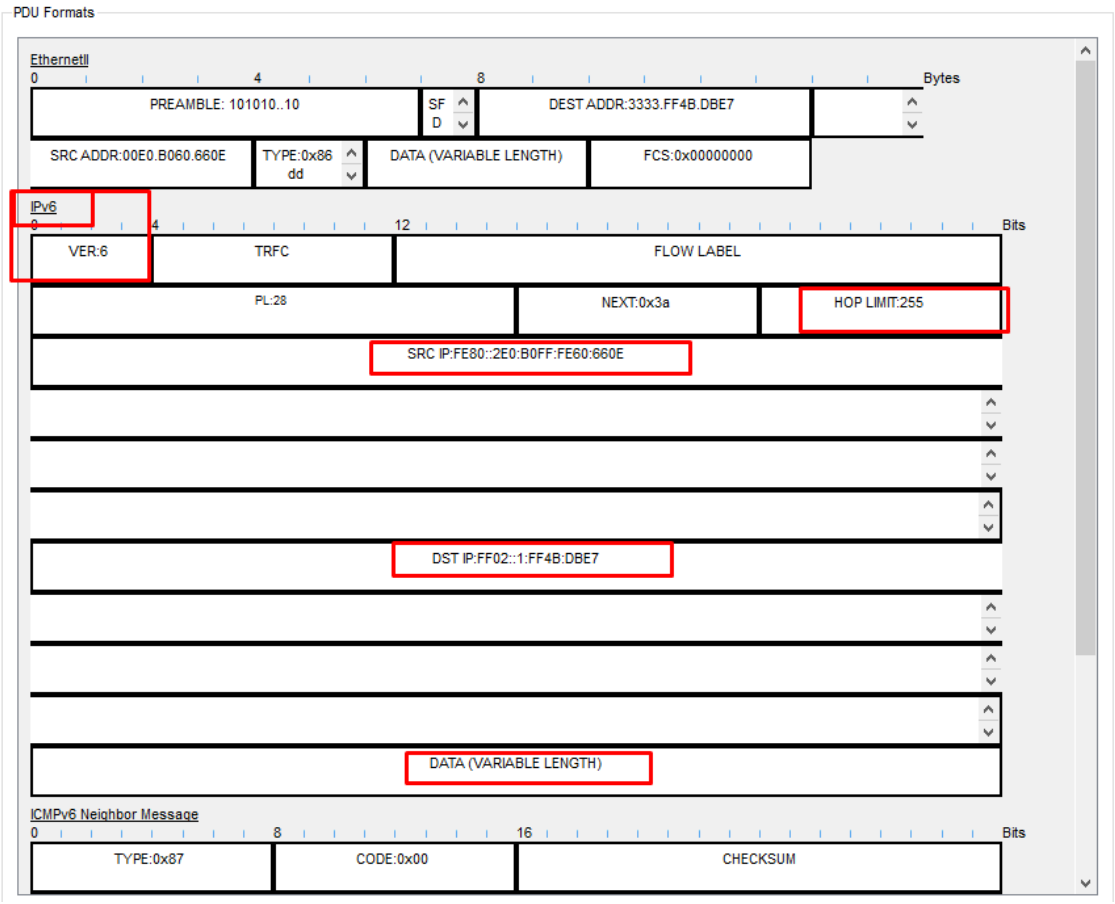
Primera IP	Ultima IP	Broadcast	Red
2001:DB8:0001:0001::/48	2001:DB8:0001:65549/48	2001:DB8:0001:65549/48	2001:DB8:0001::/48

Dirección LOOP BACK IPv6

Loopback Al igual que en IPv4, cada dispositivo tiene una dirección loopback, que es usada por el nodo mismo. En IPv6 se representa en el formato preferido por el prefijo 0000:0000:0000:0000:0000:0000:0000:0001 y en el formato comprimido por ::1

Paquete IPv6 en Cisco Packet Tracer:

En este paquete podemos distinguir muchas cosas entre ellas la dirección IP origen y destino, que es IPv6, la versión del ICMP el limite de saltos en la red, y los datos .



¿Que es NDP?

El Neighbor Discovery Protocol (“protocolo de descubrimiento de vecinos”) se utiliza junto con la versión más reciente del protocolo de Internet IPv6. Su principal objetivo es resolver las direcciones IPv6 en direcciones MAC válidas, que son las direcciones de hardware propias de cada dispositivo. En IPv4, el encargado de esta función era el Address Resolution Protocol (ARP).

Cualquier dispositivo que implemente el Neighbor Discovery Protocol para la comunicación en red, gestiona su propio neighbor cache. En este figuran todos los dispositivos conocidos de su red, verificables por su dirección de dispositivo único (MAC).

Hay tres tipos:

-Caché de destino: este incluye entradas para los nodos de la red a los que ya se han enviado paquetes de datos. A su vez, cada una de estas entradas se refiere a una dirección en el neighbor cache, que se utiliza al enviar paquetes de datos al puerto de destino .

-Caché de prefijo: la lista de prefijos sirve para gestionar todos los prefijos válidos para la red en donde se encuentra el cliente. Esta lista es necesaria porque IPv6 soporta el multihoming (la accesibilidad de la red a través de dos proveedores diferentes)y porque permite la división del espacio de direcciones en diferentes prefijos. Con los registros en la caché de prefijo, el NDP se asegura de que el host de destino se encuentre en la misma subred

-Default Router List: esta lista incluye todos los routers conocidos que tienen contacto regularmente con el dispositivo. Cada entrada en esta lista está vinculada a una entrada en el neighbor cache.

¿Qué tipos de ICMPv6 existen?

¿Qué es ICMPv6?

ICMPv6 (Internet Control Message Protocol version 6) es un protocolo de control de mensajes utilizado en redes IPv6. Es una versión actualizada del ICMP, que se utilizaba en redes IPv4. ICMPv6 se utiliza para enviar mensajes de control y notificaciones de error entre dispositivos de una red IPv6.

Algunas de las funciones de ICMPv6 incluyen:

Descubrimiento de vecinos (Neighbor Discovery): ICMPv6 se utiliza para descubrir y mantener información sobre los vecinos (dispositivos) en una red IPv6. Esto incluye la resolución de direcciones (similar al ARP en IPv4), la detección de duplicados de direcciones y el anuncio de rutas.

Envío de mensajes de error: ICMPv6 proporciona mecanismos para enviar mensajes de error y notificaciones cuando ocurren problemas en la comunicación IPv6. Por ejemplo, si un paquete no puede ser entregado a su destino, se genera un mensaje de error ICMPv6 que informa al remitente sobre el problema.

Redireccionamiento de rutas: ICMPv6 también se utiliza para enviar mensajes de redireccionamiento de rutas. Estos mensajes permiten a un router advertir a los dispositivos en la red acerca de una ruta más eficiente para alcanzar un destino específico.

Multicast Listener Discovery (MLD): ICMPv6 se utiliza en el proceso de descubrimiento de oyentes multicast en una red IPv6. Los mensajes de MLD permiten a los dispositivos informar a los routers sobre su interés en unirse o dejar un grupo multicast.

ICMPv6 desempeña un papel importante en la comunicación y el funcionamiento de las redes IPv6, permitiendo la detección y resolución de vecinos, la corrección de errores y la administración de rutas.

Los 5 tipos de ICMPv6

Tipo 134: Router Advertisement.

Periódicamente, los routers envían los llamados anuncios de enrutador o router advertisement (mensajes ICMPv6 del tipo 134) para informar a los participantes de la red sobre su presencia. De este modo, y entre otras cosas, distribuyen los datos de su enrutamiento y los parámetros necesarios para la configuración automática de la IP. El destino del mensaje es el rango de direcciones multicast estándar “ff02::01”, con el cual se establece la comunicación con todos los puertos relevantes en cada área de validez. De esta manera se obtiene también la dirección del router (puerta de enlace predeterminada) y el prefijo global.

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
0	Tipo	Código	Suma de comprobación ICMP	
32	Hop Limit	M | O | HA | Pref | Proxy |Reservado	Vida útil del router	
64	Tiempo máximo de accesibilidad			
96	Tiempo máximo de resolución			
...	Opciones			

Tipo 133: Router Solicitation

Las solicitudes del router son mensajes que permiten al host pedir a todos los routers de su red que envíen los router advertisements. Estos responden con un mensaje del tipo 134 exclusivo para el host solicitante (unicast) o para todos los usuarios de la red (multicast). Con este tipo de mensajes, el host no tiene que esperar a la notificación automática del router de la red en el caso de una nueva conexión

La estructura estándar de un mensaje ICMPv6 para NDP del tipo 133 tiene una longitud mínima de 64 bits. “Tipo” contiene el valor de solicitud 133, mientras que “código” se ajusta nuevamente a 0. Los otros dos campos obligatorios son la suma de comprobación ICMP (16 bits) y un campo de 32 bits “reservado” que se queda sin utilizar.

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
0	Tipo	Código	Suma de comprobación ICMP	
32	Reservado			
...	Opciones			

Tipo 135: Neighbor Solicitation

Los clientes de la red envían Neighbor Solicitations para conseguir la dirección MAC de destino del host y, opcionalmente, transmiten a cambio su propia dirección. Si los equipos quieren encontrar una dirección, pueden transmitir este tipo de mensajes ICMPv6 por multicast o por unicast si solo quieren comprobar la disponibilidad de un vecino. siendo su longitud total de al menos 192 bits

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
0	Tipo	Código	Suma de comprobación ICMP	
32	Reservado			
64	Dirección de destino			
96				
128				
160				
...	Opciones			

Tipo 136: Neighbor Advertisement

Por un lado, los dispositivos de red envían Neighbor Advertisements como reacción a las Neighbor Solicitations entrantes y, por otro, sin que se solicite, informan a otros participantes sobre los cambios en la configuración de la dirección.

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
0	Tipo	Código	Suma de comprobación ICMP	
32	R | S | O Reservado	Reservado		
64	Dirección de destino			
96				
128				
160				
...	Opciones			

Tipo 137: Redirect

Los routers tienen la posibilidad de informar a los hosts de la red acerca del primer mejor hop en el camino hacia las direcciones de destino.

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
0	Tipo	Código	Suma de comprobación ICMP	
32	Reservado			
64	Dirección de destino (hop)			
96				
128				
160				
192	Dirección de destino			
224				
256				
288				
...	Opciones			

¿Que es una VLAN?

Una VLAN (Virtual Local Area Network) es una red local virtual que permite segmentar y aislar el tráfico de red dentro de una red física. En lugar de dividir una red física en subredes físicas separadas, una VLAN crea grupos lógicos de dispositivos que pueden comunicarse entre sí como si estuvieran en su propia red independiente.

Estos grupos pueden abarcar varios puertos en múltiples switches, incluso si están físicamente separados. A través de la configuración de la VLAN, los dispositivos pueden comunicarse entre sí dentro de la misma VLAN, mientras que el tráfico entre VLANs se puede controlar mediante reglas y políticas.

Vlans En Packet Tracert.

Andrés Montes Álvarez

VPN (Virtual Private Network)

Una VPN (Virtual Private Network) es una tecnología que permite establecer una conexión segura y cifrada entre dos redes a través de Internet. Proporciona privacidad y seguridad al crear un túnel virtual entre el dispositivo del usuario y el servidor de la VPN, enmascarando la dirección IP y cifrando los datos transmitidos.

Una VPN (Virtual Private Network) es una tecnología que permite establecer una conexión segura y cifrada entre dos redes a través de Internet. Proporciona privacidad y seguridad al crear un túnel virtual entre el dispositivo del usuario y el servidor de la VPN, enmascarando la dirección IP y cifrando los datos transmitidos.

Cuando te conectas a una VPN, tu tráfico de Internet se dirige a través de un servidor VPN antes de llegar a su destino final. Esto significa que tu dirección IP real se oculta.

Hony Pot

¿Quién ataca nuestros sistemas?

Es importante entender el escenario en el que estamos, el cibercrimen es una industria

El negocio del cibercrimen se estima en unos 1.500.000 millones de euros. (13 thGDP)

El costo global de los incidentes de ciberdelincuencia aumentó de $ 3.000 millones a principios de 2015 a $ 6.000 millones en 2022.

Ciberdelincuentes

Cometen delitos comunes apoyados en los sistemas digitales y redes

Hacktivistas

Realizan acciones reivindicativas en el ciberespacio

Ciberterroristas

Utilizan el ciberespacio para cometer actos de terrorismo

Estados

Realizan acciones ofensivas en el ciberespacio para ganar ventaja geoestratégica

Tipos de Ataques

Dirigidos

Ataques que tienen un objetivo concreto, como en el caso de las auditorías de seguridad, las APT’s u otros ataques con un objetivo definido a priori

No Dirigidos

Ataques que buscan sistemas que puedan ser comprometidos, con múltiples fines

Usar recursos para realizar ataques DDoS u otras campañas, spam, clicks etc

Cifrar la información que contienen y pedir un rescate, caso del Ransomware

Usarlo para compartir recursos ilegales, como pornografía infantil u hospedar un sitio de Phishing

Usar los recursos computacionales para el minado de criptomonedas

Metodología y técnicas TTP’s

Metodología de hacking

Reconocimiento pasivo Búsqueda de información sin “ la víctima Esencial en ataques dirigidos

Reconocimiento activo Escaneo de puertos, enumeración de servicios, usuarios Todo interactuando con el sistema objetivo Esencial en todo ataque

Explotación Obtención de la primera conexión a los sistemas de la víctima

Postexplotación EoP pivoting uso de los sistemas para los objetivos descritos, medidas antiforenses

El término información debe diferenciarse del de inteligencia. Información equivale a noticia de un hecho en su sentido más amplio. El concepto información debe entenderse, por tanto, como el elemento de partida para la elaboración de inteligencia , considerada ésta como el resultado de valorar, analizar, integrar e interpretar la información.

¿Qué es un honey Pot?

Se trata de un sistema informático trampa o señuelo, (Deception) expuesto con atractivos para el atacante de forma que resulta atacado antes que cualquier otro sistema de la organización.

Los objetivos principales son dos:

1.Detectar intrusiones en la organización, monitorizando el Honeypot, antes de que lleguen a sistemas reales

2. Investigar sobre las técnicas utilizadas por los atacantes como fuente de inteligencia y TTP’s

Atractivos para el atacante:

Exponer vulnerabilidades conocidas y fáciles de atacar

Es una estrategia habitual, válida para atraer los sistemas automáticos y a los atacantes no altamente cualificados No válido para actores estado, por ejemplo Muy adecuada para la obtención de inteligencia

Simular un sistema de alto interés, por su información, actividad y protección

Al contrario de lo anterior, busca simular un sistema lo más real posible, reduciendo la desconfianza del atacante de estar ante un señuelo.

Exponer muchos servicios, incluso una red con múltiples dispositivos y servicios, Honeynet Invita al atacante a realizar múltiples tareas de escaneo y enumeración de servicios, lo que incrementa la obtención de información para generar inteligencia