apuntes:

OSI (El modelo de interconexión de sistemas abiertos)
Tiene 7 capas para normalizar la comunicación entre dispositivos de red. Donde cada capa tiene una función específica.
m

Host (A)

1. Fisica
2. Enlace
3. Red
4. Transporte
5. Sesión
6. Presentación
7. aplicación.

establece que cada dispositivo que están conectado a la red se va o va a llevar el nombre de HOST

Host (B)

1. Fisica
2. enlace
3. red
4. transporte
5. sesión
6. presentación
7. aplicación

El host A y el host B en la capa física se comunican a través de un protocolo. Ej: el protocolo físico del host A se comunica con el protocolo del host B (siempre con la misma capa)

Las diferentes capas de un mismo host se comunican entre sí a través de formas primitivas de comunicación.

Ejemplo de protocolo: es un mecanismo de comunicación estándar que lo definen para poder entenderse.

Los alumnos y el profesor hablan en español y los alumnos entienden, estableciendo de antemano que el idioma va a ser español para entendernos y comunicarnos. Establecimos que en un horario y en un aula se tiene la materia. El protocolo es un acuerdo entre ambas partes para establecer una comunicación.

Que función tiene cada capa del modelo OSI.

1. Aplicación: La capa de aplicación, la función es la interacción con los usuarios.
   Toma los datos que el usuario ingresa en la capa de aplicación.
   Un ejemplo es el protocolo http, utiliza el puerto 80.
   https: seguro, trabaja en el puerto 443. Es otro protocolo, no es lo mismo que http.
   http sería la capa de aplicación.
   dns puerto 53, es el que consultas dominio, te devuelve un IP y viceversa. En la consola: “ping google.com”
   correo electrónico
   ftp
   Término de enviar el correo, presiono enter, arma un paquete, manda a través de la primitiva de comunicación a la capa de presentación.

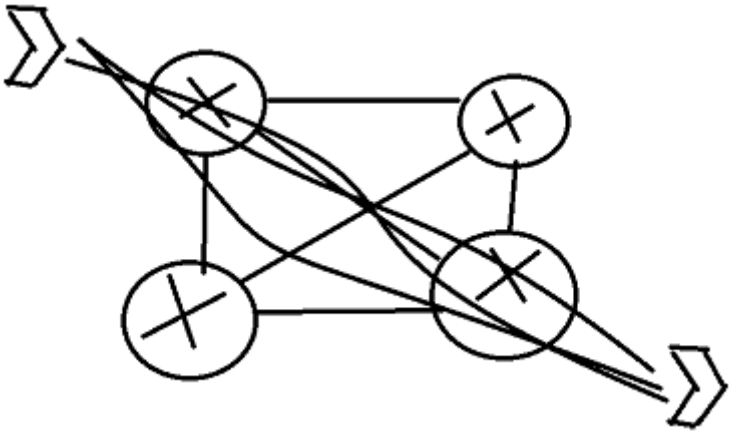
2. Presentación: Lo que hace es estandarizar diferentes codificaciones de sistemas operativos. Siguen habiendo versiones de diferentes marcas que usan sistemas codificaciones no estándar.
   Cuando la capa de de aplicación manda un mensaje a la capa de de presentación y está detecta que es de mackintosh, hace una compatibilización a nivel de codificación (de mackintosh a ASCII). Hay un conversión, si son iguales no hace nada.
   A nivel de capa de presentación es la capa de codificación

3. Sesión: La capa de sesión lo que hace es manejar los timmer, registra las credenciales de acceso, los tiempos y los registros de actividad. Para billetera virtuales, redes, necesitan que estemos registrados
   Pasado un tiempo inactivo, el sistema debe limpiar.

Los protocolos que entran son SCL, SCH.

4. Transporte: La capa de transporte ofrece dos servicios bien definidos al medio de comunicación.
   - Servicio orientado a la conexión: para esto establece el protocolo TCP. Cada vez que se comunica con un dispositivo establece una conexión única y directa.
     Es análogo a teléfonos

Ej: el host A quiere enviar varios paquetes al host B: El host A envía el paquete al host B, se confirma la recepción al host A, y ahi recien envía el paquete 2. Hay un tiempo que espera la respuesta, si el host A no recibe la respuesta en ese determinado tiempo, lo toma como que se perdió o algo pasó.



si otro dispositivo quería comunicarse, en el momento que estaba comunicando con A, el host C no atendía la llamada, le daba un tono de ocupado.

- Servicio no orientado a la conexión: establece el protocolo UDP. Es todo lo contrario a TCP.
  Envía todos los paquetes de manera desordenada, no espera confirmación de recepción y los caminos para que los paquetes vayan al destino de envío, siempre van en caminos diferentes. Ejemplo: plataforma de películas, si uno de los paquetes se pierde (que contiene todos los píxeles de la peli), no va afectar la película porque se pierde solo un pixel.
  Es análogo al correo tradicional.

No es que un protocolo sea mejor que otro, sino que depende de la funcionalidad que se le de, se utiliza uno u otro.

Cada router tiene muchos vínculos de comunicación.Cada vínculo tiene características y capacidades diferentes.

Cuando llega un paquete, tiene que definir por cual vinculó lo va a mandar, cuál le conviene más. El router ejecuta un algoritmo para determinar el mejor camino para determinado paquete, esto lo hace la capa de RED.

Entonces la capa de transporte se encarga del Direccionamiento y enrutamiento

5. Red: La capa de red, la funcionalidad es el direccionamiento (Protocolo IPv4 - IPv6)

   A partir de eso, se establece mecanismo de enrutamiento, se encarga de definir cuál es el camino para enviar el paquete.
   La función es establecer un mecanismo de direccionamiento donde tiene que definir una dirección y enrutamiento.

   Un ejemplo de una dirección IPv4 : 192.168.10.50 números del 0 - 256.
   Un ejemplo de una dirección IPv6 : 2800:4FE1:0000:0000:2040:8080:7020:0000.
   Si tiene muchos 0 se sustituye con “:” = 2800:4FE1::2040:8080:7020::

Creado de tal forma que todos los dispositivos tengan su IP pública con acceso a internet. No todos los destinos tienen IPv6 por lo que, los dispositivos tienen que "convertir" con IPv4 e IPv6.

Protocolo de enrutamiento estático, donde se define manualmente y protocolo dinámico.

6. Enlace: La capa de Enlace
   el usuario genera la información para la capa de aplicación, depende de la comunicacion que se tenga en el momento, genera la información que va a utilizar la aplicación. el protocolo que estamos viendo en la capa de aplicacion arma un paquete y genera un encabezado. La capa de presentación agarra ese paquete y lo convierte en su payload…

   utiliza técnicas de entramado en base al escenario de la capa física, donde analiza la información de las capas anteriores, recibe el paquete, se fija en la capa física y decide qué técnica o algoritmo utilizar., se va a ocupar de control de errores y la velocidad de transmisión. Se encarga de tomar un paquete y convertirlo en trama y transmitirlo.

7. Física: La capa de Física, la función es el hardware,transmisión de datos de los bits puros a través del vínculo físico (guia: fibra o inalámbrico), la capa física recibe la trama y lo que tiene que hacer es enviar con el medio físico que tiene.
   Protocolos que están en la capa física:
   Medio físico: medio inalámbrico, cable de cobre, fibra óptica.

Estándar: 802. 3 Ethernet

Define el cable UTP como medio físico de comunicación

- Cable UTP (Unshielded Twisted Pair o par trenzado sin cubierta o blindado)

  si miramos la última actualización dice Cable TP.

Se utiliza como medio físico para el vínculo entre los dispositivos en el medio físico. El cable está compuesto por 4 pares de hilos, así que tiene 8 hilos dentro del cable. El cable utp tiene diferentes categorías, actualmente la última categoría está estandarizada, no hay ninguna red utilizando categoría 1, 2 o 3, al menos que hay algo viejo con categoría 3 actualmente, este permitia un vínculo físico con una capacidad de datos de 10 Mbps

Cuando hablamos de transmisión de datos de un dispositivo, la unidad de medida es bit/s no byte/s

- **Cat 3** -> 10Mbps

- **Cat5:** Capacidad maxima de transferencia de datos 100mbps.
- Pegado a la categoria 5, salió **Cat 5.e**, categoria extendida, los cables de esta categoría permite comunicaciones de hasta 1000mbps(1gbps).
- Categoria 6 y categoría 6e, estan fuera de normal, no estan estandarizadas, van a tener uno que otro inconveniente.
- Categoria7,que permite velocidad de 10000 mbps, que seria de 1 a 10 gbps

todos los que son protocolos, los estandares, se tiene que tener en cuenta cuando se diseñan redes, se va a implementar como cuando se va a hacer una auditoría o evocar en algo que ya está implementado.

la distancia maxim aue puede conectar dos dispositivos teniendo en cuenta el estándar es de 100 metros, si se quiere asegurar se hace hasta 80 metros.

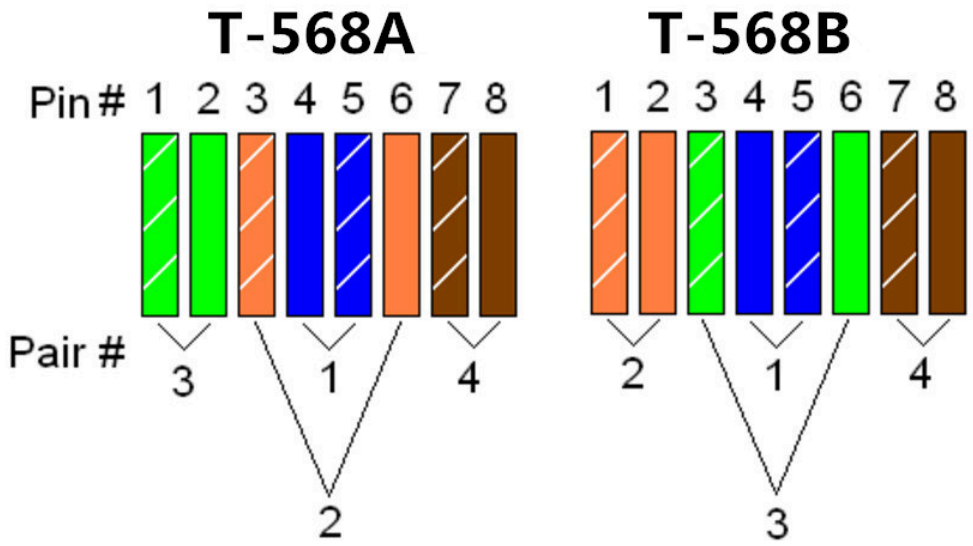
Dentro del estándar para la parte de comunicación? entre los cables hay dos normas:

La norma Tia/eia 568 A/ 568B, vamos a definir como vamos a armar los conectores en los extremos. para eso hay dos normas (las de arriba).

568 A define que los pines deben tener el siguiente orden de los colores de cable:

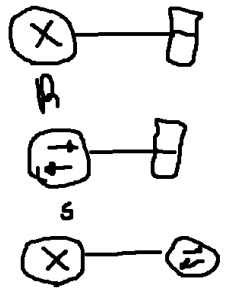
1. —---- Blanco Verde
2. —---- Verde
3. Blanco Naranja
4. Azul
5. azul blanco
6. naranja
7. blanco marron
8. marron

568 B define que los pines deben tener el siguiente orden de los colores de cable:



Importante: estas son las dos normas con las que tenemos que tener en cuenta para armar los conectores. Hay veces que no se sigue esto, entonces está fuera de norma.
la norma me define el tipo de pastcore

Dos tipos de patchcord:
Derecho: en una punta voy armar una norma y en la otra la misma norma A -> A o B ->B.
me permite vincular dispositivos finales con algún dispositivo



El patchcord cruzado, en una punta una norma A y en la otra punta la norma B
A —-- B

Se usa cuando se va a comunicar dos dispositivos finales y no tiene un dispositivo que transmita.

No hay necesidad de enchufar un switcher a una notebook

El patchcord nose cual tipo seria este

los pines no se cruza por la norma POE (power over ethernet)

No todos los dispositivos de red son compatible con POE, no todos generan POE. Hay dispositivos que generan poe y otros que soportan poe.
dd

Otro aspecto importante: no es igual el cable interior que el exterior. con portante
los cables para exterior viene con una malla mas gruesa
los cables con portantes se necesita

Los cable spara interior son mas

Estándar de capa física 802.11 Wireless Lan (WLAN-WIFI)

Redes inalámbricas para redes locales. Para poder transmitir datos entre dos computadoras, surge la necesidad de conectar con LAN.

a. Requerimientos: la frecuencia de transmisión sea de 5.8 Ghz. Capacidad de transferencia de 54 (velocidad real de 22) Mbps. wep/wep (32 bits).
b. Requerimientos: la frecuencia de transmisión sea de 2.4 GhZ, a una velocidad de 10MBPS. Estándar wep 16 bits
g. Frecuencia de 2.4 Ghz. Capacidad de transferencia de 54 Mbps. wep/wep2/wpa/wpa2
n. Frecuencia de 2.4 Ghz / 5.8 Ghz, con capacidad de 300 Mbps. wep/wep2/wpa/wpa2/wifi security.
ac. Frecuencia 5.8 Ghz, capacidad de 1000 Mbps (Gb). Lo real testeado llega como mucho a 600 Mbps.
ax. Frecuencia 2.4 / 5 Ghz, capacidad de 10000 Mbps

La comisión b finaliza primero y saca el estándar 800.11, y aplica una tecnica de seguridad estandar para conexion de datos web 16 bits. La comision A sin terminar la produccion, poner en porducciòn con el beneficio que ofrecia capacidad de transferencia de hasta 22 (según wiki 54) mbps, el doble que la b y para ese entonces ya habian encontrado como romper la seguridad web de la b. Entonces, era compatible con web y sacaron web 32 bits, duplicaron la codificación.

g- Surge el estándar 802.11 g, se basó en la frecuencia de 2.4 ghz de hasta 54 mbps, compatible con web/webP2, implementó medidas de seguridad de WPA/WPA2. Es compatible hacia atras con el estandar b pero no con el a, es compatible por la frecuencia baja (g: 2.4, a: 5.8),
el estándar g y cuando setea los puntos de acceso para que sea compatible con un estandar b, aceptamos que se conecte con b, lo que hace es bajar la velocidad de transmision a los dispositivos de estandar mas bajo. Se adapta

Es decir, si estamos implementando todo los dispositivos en estándar g, la capacidad de transmisión es de 54, pero si se conecta un dispositivo que sea en b y aceptamos la compatibilidad entonces la capacidad de transmisión va a bajar a 10, se adapta a esa capacidad.

cada dispositivo de red, sale de fabrica con una dirección mac (Media Access Control) quemada. Cada que un usuario se registra,, un ente regula la dirección mac y asigna uno

Los tres primeros digitos, representan a la empresa, los ultimos 3 la empresa se encarga de representar al dispositivo, para identificarlo de manera unica. Los otros dos, seguidos del primero, se utiliza para el modelo de ese dispositivo.

direccionamiento:

- IPv4: 192.168.10.50

- IPv6.

Aplicacion: www.google.com.ar

comandos en la terminal:
ipconfig
ipconfig -all
Esto tira las interfaces de red conectadas con su dirección mac.

página: MAC VENDOR, se utiliza para buscar la direcciòn

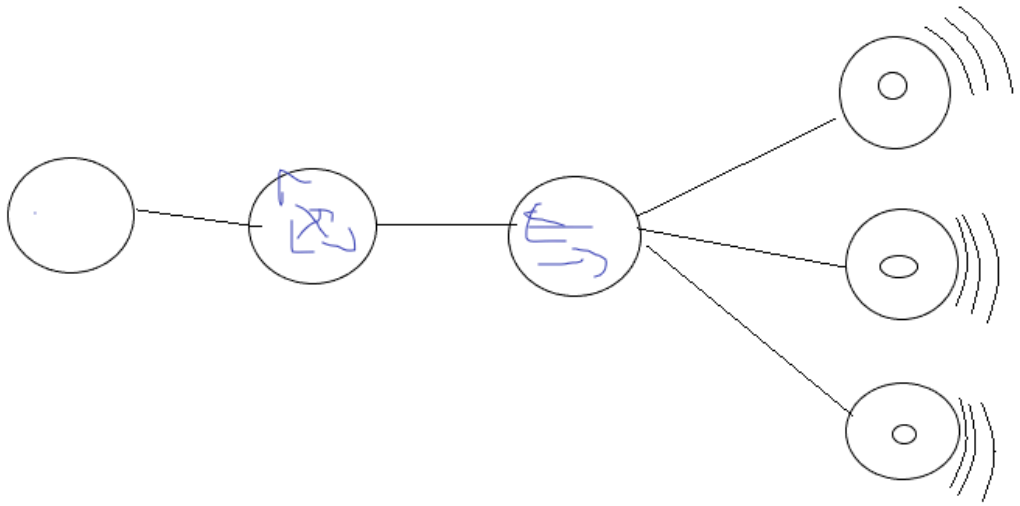
mac: nos referimos a la dirección quemada que ya viene en el dispositivo y que no se repite en el mundo.

una notebook tiene 2 interfaz minimo, placa ethernet y lan. Cada interfaz de red de la computadora tiene una direccion mac y la direccion cableada tiene otra direccion mac. Al tirar el comando muestra las interfaces con sus direcciones de mac.

Todos los disposito de red vienen con la direccion de mac quemada, ahora, estamos trabajo en entornos virtuales, donde puedo pedir que tenga 10 servidores virtuales, tiene la capacidad que virtualmente lo pueda utilizar, si seteo el IP tiene que machear con una direccion mac, esa direccion mac se da de manera aleatoria del dispositivo fisico, que no son ilimitadas.

Por más que sean virtuales, coinciden con una dirección física.

TOPOLOGÍA:



En el punto de acceso inalámbrico (primero a la derecha) es donde se setea.

Luego surge el estandar n, el cual usamos actualmente, es compatible hacia atras con g, b y a tiene una frecuencia de 2.4 ghz/5.8 ghz, logra una velocidad de hasta 300 mbps el 5.8 y el 2.4 hasta 100 mbps, es compatible con WEP/WEP2/WPA/WPA2/WIFI SECURITY

pero sigue manteniendo lo mismo, si permito que se conecte con g, se baja la velocidad estándar, se “adapta”.

Despues tenemos el estandar ac, tiene una frecuencia de 5.8 ghz, la capacidad de transmision es de 1000 mbps (gb), llega como mucho a 600 mbps. No se puede conectar con ningun dispositivo de atrás, se tiene que setear para que sea compatible

en caso de etener estandar n y se conecta un dispositivo con b, ya es compatible y hay que setear para que no sea compatible o es al revés? preguntar a chat

Se conecta a traves de un cable.

Estandar ax, tiene una frecuencia de 2.4 y 5. ghz, logra llegar a una velocidad de hasta 10000 mbps.
Para que a partir del estandar g, que trabajan con 2.4 y 5.8 y logra transmision de velocidad muy alta, viene con soporte de software para lograr esa velocidad, sino que viene con soporte a nivel hardware, y viene con antena de tipo mimo. los dispositivos con estandar n trabaja con 2 antenas.

mimo (Multiple Input / multiple Output)

otro punto importante: a partir del estandar g, WDS(Wirless Distribution System), no todos los dispositivos son compatibles, es el repetidor inalámbrico, tiene dos antenas, una trabaja como punto de acceso y la otra se conecta al router?

no conviene utilizar esta tecnologia, conviene cablear.

TP2:

- Fundamentar por qué elegimos la distribución. sincera
- capturas de la instalación.
- instalar gns3, una herramienta que virtualza.
- definir una interfaz
- informe que documente todo el paso a paso
- linea de comando de la configuracion de los scrips

cuando generas una máquina virtual generas una vps

Fibra óptica: la importancia de la fibra frente a otras tecnologías es que la transmisión de bits puros no es a través de ondas electromagnéticas o radiofrecuencia, sino a través de **luz**.

La fibra óptica está compuesta por un núcleo (por donde viaja la luz) y un revestimiento, la luz va viajando sobre el cable rebotando.
No se puede doblar a 90º pq la luz va a chocar y regresar.

La fibra óptica tiene ocho hilos, de ahí se va multiplicando. Hay cables de fibra de 8 hilos, 16, 32, 128. Cuando se tiene más de 8 hilos se organiza de manera diferente.

Cuando empezaron las redes de comunicaciones, desde un principio querían conectar las computadoras a través de luz, ya que siempre se estuvo atado a la electrónica. En su momento no lograron que las computadoras procesen la luz, pero si lo lograron en la comunicación (con los cables de fibra).

Hay que tener en cuenta la longitud de onda al conectar dos dispositivos con un cable de fibra óptica, los módulos sfp tienen que tener la misma longitud de onda.

cable utp max distancia: 100m.

Codigo de color: ITU-T y IEEE

Tipos de F.O:

- **multimodo**: su tamaño permite que la luz viaje rebotando a través de núcleo, en cada rebote hay una pequeña ***absorción*** de la intensidad de la luz, va perdiendo intensidad, haciendo que disminuye veloc y distancia, por eso esta fibra se utiliza para corta distancia (para mayor velocidad), en entornos de data center.
- **Monomodo**: viaja en forma directa porque es muy pequeño el núcleo, permite viajar a la misma velocidad pero mayor distancia.

No son compatibles las dos entre si

hay varios tipos de pulidos: apc, upc
Tipos de conectores: lc (con pulido upc), sc(con pulido apc)

odf: donde ordena los cables de fibra.

Monomodo: en una punta tiene sc y en la otra lc, o si es para conectar electrónica va a ser lc-lc dos y es para odf va a ser sc-sc

Primer Práctica

Compu A —--- Compu B

A:
Dirección IPy4: 192.168.10.1
Mascada de Subred: 255.255.255.0

Gateway (ahora no es necesario, pero algunas versiones pueden requerir): 192.168.10.2 o 7?
DNS:

B:
Dirección IPv4: 192.168.10.2
Mascada de Subred: 255.255.255.0

Gateway (ahora no es necesario, pero algunas versiones pueden requerir): 192.168.10.1
DNS: 8.8.8.8

En la terminal
A:
>ping 192.168.10.2
>ARP -all

B:
>ping 192.168.10.1

OSI:
Aplicación: usuario
Presentación
Sesión
Transporte
Red: Direccionamiento IPv4/IPv6
Enlace: ARP
Física: 802.3 Ethernet

Hay que desactivar el firewall para que funcione.
En realidad esto no es correcto pq desactivamos toda la seguridad, entonces agregamos una excepción el firewall para que podamos acepte el comando ping
https://www.redeszone.net/tutoriales/seguridad/permitir-firewall-windows-10-ping/
https://www.sysadmit.com/2018/03/windows-habilitar-ping-icmp.html

Cómo funciona el comando ping: desde la pc de origen envía un paquete consultando a la pc de destino por la ip, esta le responde. Hay una comunicación de doble destino.
El firewall cuando está activado controla los paquetes que salen y vuelven, las reglas se hacen sobre el origen y sobre el destino y el protocolo que se utiliza para el comando es ping ICMP.

ICMP no utiliza puertos, pero utiliza el puerto 8 para…

Se vuelve hacia atrás, firewall activado y con internet.

gráfico:

Se utiliza el dispositivo de firewall para proteger la red, si no la configuramos bien cualquier dispositivo puede atacar.

Investigar firewall recomendado para software tango

VLAN, sobre mi red física puedo generar redes virtuales, esto es una recomendación de seguridad inicial. Antes de poner mi red de producción se debe poner VLAN funcionando, permite segmentar las redes en formas lógicas sobre el plano físico

VLAN 10 -> Parte administrativa
VLAN 20_> Parte de cortesia
VLAN 30-> Parte alumnos
VLAN 40-> Parte profesores
…
en firewall cuando genero la regla de acceso para el tango no solo macheo origen y destino sino también macheo con el VLAN

Cuando desarrollamos Front y Back se tiene que poner otro firewall para back y permitir que se hagan consultas sql desde el front y no permitir que el usuario pueda hacer consultas sql

Base de datos de Tango: ver que puertos utiliza PCP 1433

Capa de Enlace.

Aplicación
Presentación
Sesión
Transporte
Red
Enlace
Fisica

Función principal:

1. entramado (ver que es). Enviar todas las tramas al destino y esperar a que el destino le diga que la trama tiene un error y vuelva a enviar.

La tasa de error en un medio de cobre es de 0, 01.
La tasa de error en un medio de fibra es 0,0..

Cuando el medio de comunicación es inalámbrico, la capa de enlace utiliza una técnica de entramado y si ve un error aplica un algoritmo para arreglarlo.

2. Controla que un transmisor rápido no sature a un receptor lento, define el tamaño de las tramas que va a utilizar,
   el estándar 802.11g trabaja a 54mb y el estándar

802.11g y conecto un dispositivo con 8.02.11b, toda la red baja a la velocidad del 802.11b
A qué velocidad trabaja el estándar 802.11… 10 megabytes

Por ejemplo: enviar por whatsapp web, desde la compu tiene una mayor velocidad pero el envio hacia el teléfono va a ser con menor velocidad, va a haber una saturación al teléfono.

Si tengo un teléfono con 802.11b pero está bajo al punto de acceso, la intensidad va a ser del 100% con respecto al punto de acceso,
Si más lejos tengo otro teléfono con 802.11 g, la intensidad de señal con respecto al punto de acceso y más si se pone abajo del aire, por la distancia al punto de acceso, no le va a permitir transmitir a 54 mb. Al contrario, al estar más cerca, si nos permite transmitir a 54gb.

En el punto de acceso se puede configurar los estándares que pueden conectarse. Por ejemplo configurar para que trabaje con 802. n y permita hasta 802.11 g, pero no permita 802.11a y b.

Otra cosa que se puede configurar es los parámetros de la señal, donde nos podemos asegurar que dispositivos que estén muy lejos no se puedan conectar, la red la pueden ver pero no se pueden conectar.

Ubiquiti Unifi:

- Lite: un lugar con menos personas conectadas, ejemplo una casa
- LR: para un lugar que tenga más personas
- Pro: auditorio, mas de 100 personas

Para poder soportar 2.4 y 5.8 tiene dos antenas diferentes. De esta forma, maneja los dos protocolos de manera diferente. IPV4 e IPV6, trabajan de manera paralela, va a recibir dos direcciones IP, verifica cual es el destino (4 o 6) y ahi accede (tienen funcionamientos diferentes).

3. Control de Errores.

- ARP.
- STP.
- RSTP.
- VLAN.

255	255	0	0
11111111	11111111	00000000	00000000

Mayor cantidad de direcciones para los dispositivos:

Red		Dispositivos	
obs1	obs2	obs3	obs4
192	168	10	1

Esto sirve cuando hay muchos dispositivos, en donde, no alcanza utilizar solo un objeto para “dispositivos”, se va a necesitar utilizar obs3 y obs4.

También puede ser

Red	Dispositivos		
obs1	obs2	obs3	obs4

Ahora:

define:

Máscara= segmento y dirección de la red de subred

ID: 192 168 10.0/24

Máscara de Subred: 255 255 255 0

Máscara de Subred en Binario: 11111111 11111111 11111111 00000000

1er IP: 192 168 10.1

IP: 192 168 10 254

Breadcost: 192 168 10 255

Cantidad de dispositivos: 254

Modelo OSI: 7 capas

Aplicación
Presentación
Sesión

T
Red
Enlace
Física

En red tenemos:

- Direccionamiento 2 protocolos:
  - IPv4
  - IPv6
- Enrutamiento.

Protocolo IPv4.

Ejemplo.

ID de red: [192.168.100].[0] /24 (Los primeros 3 octetos pertenecen a red y el cuarto a host)
/24 es la máscara de subred, es la cantidad de bits 1 que tiene la máscara de subred

Máscara de subred binario: 11111111 11111111 11111111 00000000

Máscaraen … de red: 255.255.255.0

1° Host direccionable: 192.168.100.0

Último Host direccionable: 192. 168. 100. 254

D**irección Broadcast:** 192.168.100.255

$2^8 = 256 \rightarrow$ valores posibles dentro del rango, pero hay que reservar 2 (el primero para el ID y el último para el Broadcast).
En realidad del total de 255 solamente puedo utilizar 254, solo puedo direccionar 254 dispositivos.

Red deficiente: se llena de mensajes de broadcast.

Ahora:
ID Red: 192. 168. 100. 0/25 ->se achica el espacio de direccionamiento
Máscara de subred en binario: 11111111 11111111 11111111 0000000 (no voy a poder usar el cuanto obj de forma completa, solo utilizo 7 bits para poder hacer la combinación y direccionar dispositivos)

Máscara de Subred: 255. 255. 255. 128

128 se calcula como $2^7 = 128$, se reserva dos, el primero para el ID y el último para el Broadcast), se direccionan 126 dispositivos.

1er host direccionable: 192.168.100.1

Último Host direccionable: 192. 168. 100. 126

D**irección Broadcast:** 192.168.100.127

De un segmento /24 vamos a tener dos segmentos /25 → 192.168.100.128/25
→ 11111111 11111111 11111111 0000000
→ 255. 255. 255. 128
→ 192.168.100.129
→ 192.168.100.254
→ 192.168.100.255

Cada segmento de red puede tener 126 dispositivos.

Tenemos 40 computadoras, el segmento /25 sigue quedando grande, así que lo achicamos con /26

Ahora /26:
ID Red: 192. 168. 100. 0/26 ->se achica el espacio de direccionamiento
Máscara de subred en binario: 11111111 11111111 11111111 11000000 (no voy a poder usar el cuarto octeto de forma completa, solo utilizo 6 bits para poder hacer la combinación y direccionar dispositivos)

Máscara de Subred: 255. 255. 255. 192 $(256/2 = 128 + 64 = 192)$

128 se calcula como $2^7 = 128$, se reserva dos, el primero para el ID y el último para el Broadcast), se direccionan 126 dispositivos.

1er host direccionable: 192.168.100.1

Último Host direccionable: 192. 168. 100. 62 ($2^6 = 64$, dos se reservan y solo quedan disponibles 62)

D**irección Broadcast:** 192.168.100.63

del /24 fuimos a dos segmentos /25, ahora se tienen 4 segmentos /26 dentro del /24.

De un segmento /24 vamos a tener 4 segmentos /26 → ID 192.168.100.64/26
→ 11111111 11111111 11111111 11000000
→ 255. 255. 255. 192
→ 192.168.100.65 (siempre es uno más)
→ 192.168.100.126 (64+64-2)
→ 192.168.100.127

/26 → ID 192.168.100.128/26 (+64 cada cada segmento)
→ 11111111 11111111 11111111 11000000
→ 255. 255. 255. 192
→ 192.168.100.129
→ 192.168.100.190 (128+64-2)
→ 192.168.100.191

/26 → ID 192.168.100.192/26 (+64 cada cada segmento)
→ 11111111 11111111 11111111 11000000
→ 255. 255. 255. 192
→ 192.168.100.193
→ 192.168.100.254
→ 192.168.100.255

192. 168. 100. 0/27
ID Red: 192. 168. 100. 0/27 ->se achica el espacio de direccionamiento
Máscara de subred en binario: 11111111 11111111 11111111 11100000 (no voy a poder usar el cuarto octeto de forma completa, solo utilizo 5 bits para poder hacer la combinación y direccionar dispositivos)

Máscara de Subred: 255. 255. 255. 224 $(256 - 32 = 224)$
32 se calcula como $2^5 = 32$, se reserva dos, el primero para el ID y el último para el Broadcast), se direccionan 32 dispositivos.

1er host direccionable: 192.168.100.1

Último Host direccionable: 192. 168. 100. 30 ($2^5 = 32$, dos se reservan y solo quedan disponibles 62)

Dirección Broadcast: 192.168.100.31.

No nos sirve para redireccionar la red de computadoras (40 dispositivos), ya que nos queda chico el segmento de red, hay 8 segmentos /27 dentro del segmento /24.

10.10.10.0/30

(dibujto de sofi)
tenemos 30 bits 1 y solo 2 bits 0.
$2^2 = 4$
No va a poder acceder a otro direccionamiento IP que no sea el del otro router.

Si ahora se tiene una red más grande con 600 dispositivos, se agranda el espacio de direccionamiento.

Direccionar 600 dispositivos, tenemos que hacer una relación inversa, se utiliza el tercer octeto:

ID: [192 168] [0.0]/16 → octeto 1 y 2 para red y octeto 3 y 4 para el host

Máscara de Subred en Decimal: 255 255 0 0

Máscara de Subred en Binario: 11111111 11111111 00000000 00000000

1er IP: 192 168 0.1

IP: 192 168 255 254

Breadcost: 192 168 255 255

Cantidad de dispositivos: 65534 (65534-2)
Es mucho para 600 dispositivos, sacamos ceros de la máscara de red.

192.168.0.0/17
11111111 11111111 10000000 00000000
255 255 . 128

Si nos pide direccionar 80 000 dispositivos, lo que hacemos es que disminuyamos /8

el problema del /8 es la cantidad de paquetes broadcast que se va a tener, se necesita un equipo con gran capacidad de procesamiento.

https://www.calculadora-redes.com/

Ejemplo:

ID de Red: 10.10.10.0/28
Máscara en Binario: 11111111 11111111 11111111 11110000
Mácara en decimal: 255 255 255 240 (256-16, el 16 es de 2^4)
1er host direccionable: 10.10.10.1
ultimo host direccionable; 10.10.10.14
Broadcast: 10.10.10.15
Cantidad de Host: 14

ID de Red: 10.10.10.0/29
Máscara en Binario: 11111111 11111111 11111111 11111000
Mácara en decimal: 255 255 255 248 (256-8, el 8 es de 2^3)
1er host direccionable: 10.10.10.1
ultimo host direccionable; 10.10.10.6
Broadcast: 10.10.10.7
Cantidad de Host: 6

ID de Red: 10.0.0.0/9
Máscara en Binario: 11111111 10000000 00000000 00000000
Mácara en decimal: 255. 125. 0. 0 (256-8, el 8 es de 2^3)
1er host direccionable: 10.0.0.1
ultimo host direccionable; 10.10.10.6
Broadcast: 10.10.10.7
Cantidad de Host: 6

Trabajo integrador, explicación.

Agenda de los respaldos es distintas, semestral y menstrual.

La idea: Generar la herramienta que permite armar la agenda de planificación.
Que funcione con un solo dispositivo y luego, agregar dispositivos.