Fundamentos de redes

Una red es una estructura compuesta por varios nodos, ya sea: computadoras, dispositivos móviles, servidores o cualquier otro dispositivo que sea capaz de enviar y recibir información. Estos nodos están interconectados entre sí mediante canales de comunicación, pueden ser físicos (cables de cobre o fibra óptica) o inalámbricos (bluetooth o Wi-Fi), la finalidad de toda red es siempre compartir recursos como ficheros, directorios y aplicaciones, así también como facilitar la comunicación electrónica entre los dispositivos y los usuarios de estos. Dentro de una red los datos circulan en forma de paquetes que viajan de un punto a otro siguiendo reglas definidas por protocolos como IP, TCP, UDP, etc.

Tipos de redes

Las redes principalmente se dividen en base al alcance a nivel de tamaño y usuarios que puedan impactar y se dividen en:

LAN o Local Area Network

Son redes de tamaño limitado que usualmente confinados por ejemplo a un edificio o grupo de edificios cercanos. Son ideales para entornos donde se busca más velocidad y seguridad, ya que al ser más pequeñas se puede gestionar de mejor manera

WAN o Wide Area Network

Este tipo de redes funcionan para interconectar ciudades o incluso países. Un ejemplo de esta red es la Internet, ya que conecta a múltiples redes LAN dispersas por todo el mundo.

MAN o Metropolitan Area Network

Es una red que cubre un área más amplia que la LAN, pero no es tan amplia para interconectar ciudades o países como lo haría una WAN.

PAN o Personal Area Network

Es el tipo de red más pequeño existente ya que se limita a los dispositivos personales de un solo individuo que se pueden comunicar entre sí.

VPN o Virtual Private Network

Establece un túnel cifrado para proteger el tráfico de red mientras viaja por una red pública, como Internet. Esto asegura la confidencialidad e integridad de los datos, usando protocolos como IPsec, OpenVPN o WireGuard.

Topologías de red

Una topología describe como se organizan y conectan los dispositivos en una red, ya sea de forma física (disposición real de los cables y dispositivos) o de forma lógica (donde se describe como los datos fluyen a través de la red), existen distintas topologías como son:

- **Bus**: Todos los dispositivos están conectados a un cable central que actúa como una carretera por donde se transporta todos los datos de la red. Es la topología más simple de implementar y la de menor costo, sin embargo, es la que más riesgo posee ya que si el cable central falla la red se pierde.
- **Estrella**: Todos los dispositivos están conectados a un hub o switch que es el centro de la red.
- **Anillo**: Los dispositivos están conectados en forma de anillo y los datos pasan de un dispositivo a otro en una única dirección, esto asegura que los datos tengan que recorrer todo el anillo hasta llegar a su punto final.
- **Malla**: Conecta múltiples dispositivos entre sí, permitiendo varios caminos para el envío de datos. Existen 2 tipos:
  - **Malla completa:** Todos los dispositivos están conectados directamente entre sí, proporcionando máxima redundancia, pero a un costo elevado.
  - **Malla parcial:** Solo algunos dispositivos están interconectados, reduciendo el costo y la complejidad a cambio de menos redundancia.
- **Árbol**: Es una variante de la topología de estrella, donde los dispositivos están organizados en grupos interconectados que se ramifican desde un punto central, combina las ventajas de las topologías de estrella y de bus, esto permite la escalabilidad y flexibilidad para el futuro.

Patrones de distribución de tráfico

Los patrones de distribución de tráfico describen como se van a transmitir los datos entre dispositivos de una red, se pueden dividir en varios tipos dependiendo de cómo se trasmitan los datos, como son:
Unicast: Comunicación de uno a uno entre un emisor y un receptor.
Broadcast: Envío de datos a todos los dispositivos de una red o subred simultáneamente.
Multicast: Envío de datos desde un dispositivo a un grupo específico dentro de una misma red.
Loopback: Permite que un mismo dispositivo se envié datos a sí mismo.
AnyCast: Envío de datos a un grupo de dispositivos, pero solo el nodo más cercano en términos de enrutamiento recibe y procesa la solicitud.
GeoCast: Similar a multicast, pero con la diferencia de que trasmisión está restringida a un área geográfica en específico.
Peer to Peer: Es una comunicación directa entre 2dispositivos donde el camino de la red que sigue la información es establecido.
Point to MultiPoint: Se basa en que un único emisor transmite a múltiples receptores en específico, pero a través de un canal común.

¿Qué es una dirección IP?

Las direcciones IP es un numero único asignado a cada dispositivo conectado a una red que utilice este protocolo para realizar la comunicación, este número además de identificar a dispositivo en la red permite saber su ubicación dentro de la misma red. Esta dirección se puede asignar de manera

estática (Nunca cambia de forma automática) o dinámica (dependiendo del contexto puede cambiar de forma automática) dentro de una red no puede haber 2 dispositivos con la misma IP.
Dentro del protocolo IP existen 2 versiones IPv4 e IPv6. IPv6 se creó ya que las IPv4 ya no poseen suficientes espacios para poder satisfacer las demandas actuales, las IPv4 poseen un límite máximo muy pequeño para las necesidades de hoy en día.

¿Qué es una máscara?

Todas las direcciones IP se dividen en 2, poseen una sección que identifican red y otra que identifica el host. La sección de red es la parte de IP destinada a identificar la red y la sección de host se utiliza para identificar al host específicamente.
La máscara está asociada a una IP y como tal lo que indica es hasta que parte de la IP se toma como identificador de la red, por consiguiente, que parte queda de espacio para poder asignar host.

Tipos de direcciones IPv4

Por uso y patrón de distribución

Direcciones Unicast: Se utilizan para comunicaciones directas entre un emisor y un receptor de forma única, es la más común y se utiliza para el tráfico de red estándar, incluyendo por ejemplo la navegación web.
Direcciones Broadcast: Se utiliza para enviar datos a todos los dispositivos dentro de una red o subred especifica al mismo tiempo.
Direcciones de Multicast: Permite la entrega de información a un grupo especifico dentro de una red. Su rango de IP disponibles es 224.0.0.0 a 239.255.255.255.
Direcciones de Loopback: Se utiliza para que el sistema se envié mensajes a sí mismo. Su rango de IP disponibles es 127.0.0.0 a 127.255.255.255.

Por rango y alcance

Direcciones privadas: Son rangos de direcciones IP reservados para un uso interno, en otras palabras, son direcciones que no son enrutables en internet. Sus rangos son:

- **Clase A:** 10.0.0.0/8 (10.0.0.0 a 10.255.255.255)
- **Clase B:** 172.16.0.0/12 (172.16.0.0 a 172.31.255.255)
- **Clase C:** 192.168.0.0/16 (192.168.0.0 a 192.168.255.255)
  Experimentales y uso futuro: No están destinadas al uso general en internet, su rango es de 240.0.0.0/4 a 255.255.255.254.
  Direcciones CGNAT: Carrier-Grade NAT es una tecnología que están adaptando muchos ISP, esto para que los clientes pueden navegar en internet con una misma IP pública. Para estas direcciones se maneja el siguiente rango 100.64.0.0/10 (100.64.0.0 a 100.127.255.255).
  Direcciones Publicas: Son todas las direcciones IP disponibles y sus rangos son:
  (1.0.0.0 a 9.255.255.255)
  (11.0.0.0 a 172.15.255.255)

(172.32.0.0 a 192.167.255.255)
(192.169.0.0 a 223.255.255.255)

¿Qué es una dirección MAC?

Una dirección MAC (Media Access Control) es un identificador único asignado a la interfaz de red de un dispositivo. Aunque es fija a nivel de hardware, puede ser cambiada temporalmente a nivel de software, práctica común en auditorías de seguridad, aunque puede ser detectada.

¿Qué es un puerto?

Es una especie de canal de entrada y salida de datos para permitir a aplicaciones o servicios comunicarse fuera del dispositivo a través de ellos, el rango de puerto disponibles es de 65536. Los puertos se pueden dividir en 3 categorías: Puertos bien conocidos (desde 0-1023), Puertos Registrados (desde 1024-49151), Puertos dinámicos o privados (desde 49152-65535).

Tabla de puertos

Protocolo	Acronimo	# de puerto	Conexión	Encriptación
File Transfer Protocol	FTP	20/21	TCP	No
Secure Shell	SSH	22	TCP	Si
Secure File Transfer Protocol	SFTP	22	TCP	Si
Teletype Network	telnet	23	TCP	No
Simple Mail Transfer Protocol	SMTP	25	TCP	No
Domain Name System	DNS	53	TCP/UDP	No
Dynamic Host Configuration Protocol	DHCP	67/68	UDP	No
Trivial File Transfer Protocol	TFTP	69	UDP	No
Hypertext Transfer Protocol	HTTP	80	TCP	No
Post Office Protocol v3	POP3	110	TCP	No
Network Time Protocol	NTP	123	UDP	No
Internet Message Access Protocol	IMAP	143	TCP	No
Simple Network Managemente Protocol	SNMP	161/162	UDP	No
Lightweight Directory Access Protocol	IDAP	389	TCP/UDP	No
Hypertext Transfer Protocol Secure	HTTPS	443	TCP	Si
Server Message Block	SMB	445	TCP	No
System Logging	SYSLOG	514	UDP	No
Simple Mail Transfer Protocol over TLS	SMTPS	587	TCP	Si
LDAP over SSL	IDAPS	636	TCP/UDP	Si
POP3 over SSl	POP3S	995	TCP	Si
IMAP over SSL	IMAPS	995	TCP	Si
Structured Query Language Server	SQL	1433	TCP	No
SQLnet (Oracle Network Service)	SQLNet	1521	TCP	No
MySQL	MySQL	3306	TCP	No
Remote Desktop Protocol	RDP	3389	TCP/UDP	Si
Session Initiation Protocol	SIP	5060/5061	TCP/UDP	No

¿Qué es un servicio?

Un servicio es una función ofrecida por un dispositivo para otros dispositivos dentro de una misma red o a través de internet, algunos ejemplos son: compartir archivos, impresoras, correos electrónicos, bases de datos, acceso administración remota, accesos a sitios web y demás.

¿Qué es un protocolo?

Un protocolo de red define el formato y el orden de los mensajes a nivel de intercambio de 2 o más entidades que se puedan comunicar, así como las acciones que se van a tomar dura la transmisión y recepción de dichos mensajes. En otras palabras, el protocolo establece las directrices por las que se rige la comunicación.

Modelo OSI

El modelo Open System Interconnection (OSI) es un modelo conceptual creado por la Organización Internacional para la Estandarización, el cual permite que diversos sistemas de comunicación se conecten usando protocolos estándar. El modelo OSI se puede ver como lenguaje universal para la conexión de las redes de equipos. Se basa en el concepto de dividir un sistema de comunicación en siete capas, cada una de estas capas tiene una función especifica y se comunica con las capas superiores e inferiores.

¿Por qué es importante el modelo OSI?

Aunque el Internet moderno no sigue estrictamente el modelo OSI, este modelo sigue siendo muy útil para resolver problemas de red. Ya sea una persona que no puede lograr que su computador de conecte a Internet o un sitio web que está caído para miles de usuarios, este modelo puede ayudar a desintegrar el problema y aislar la fuente. Si el problema existente se puede reducir a una capa específica del modelo, se puede llegar a evitar mucho trabajo innecesario.

¿Cuáles son las capas del modelo OSI?

El modelo OSI posee 7 capas, que son las siguientes:

7. Capa de aplicación

Es la única capa que interactúa directamente con los datos del usuario. Las aplicaciones de software como navegadores web y clientes de correo electrónico dependen de la capa de aplicación para iniciar la comunicación. Debe de estar claro que las aplicaciones de software de cliente no forman parte de esta capa; mas bien, la cala de aplicación es responsable de los protocolos y la manipulación de datos de los que depende el software para presentar datos significativos al usuario.

6. Capa de presentación

Es principalmente responsable de preparar los datos para que los pueda usar la capa de aplicación, en otras palabras, esta capa hace que los datos se preparen para su consumo por las aplicaciones. Es responsable de las traducciones, el cifrado y la comprensión de los datos. Si los dispositivos se comunican a través de una conexión cifrada, esta misma capa es responsable de añadir el cifrado en

el extremo del emisor, así como de decodificar en el extremo del receptor, para poder presentar a la capa de aplicación datos descifrados y legibles. Otra función de esta capa es comprimir los datos que recibe de la capa de aplicación antes de ser enviados a la capa 5, esto ayuda a la mejorar la velocidad y la eficiencia de la comunicación.

5. Capa de sesión

Es la responsable de la apertura y cierre de comunicaciones entre 2 dispositivos. El tiempo que transcurre entre la apertura de la comunicación y el cierre de esta se conoce como sesión. Esta capa garantiza que la sesión permanezca abierta el tiempo suficiente como para transferir todos los datos que se están intercambiando, cuando acaba el intercambio cerrará sin demora la sesión para evitar desperdicio de recursos. También sincroniza la transferencia de datos utilizando puntos de control, para que en caso de desconexión o caída la sesión se pueda iniciar desde el punto en el que se quedó.

4. Capa de transporte

Es la responsable de las comunicaciones de extremo a extremo entre 2 dispositivos. Esto implica, antes de proceder a ejecutar él envió a la capa 3, tomar datos de la capa de sesión y fragmentarlos seguidamente en trozos más pequeños llamados segmentos. La capa de transporte del dispositivo receptor es la responsable luego de rearmar tales segmentos y construir con ellos datos que la capa de sesión pueda consumir.
También es la responsable del control de flujo y el control de errores. El control de flujo determina una velocidad optima de transmisión para garantizar que un emisor que un emisor con una conexión rápida no abrume a un receptor con una conexión más lenta. Realiza un control de errores en el extremo receptor al garantizar que los datos recibidos estén completos y solicitar una retransmisión si no lo están.

3. Capa de red

Esta capa es la responsable de facilitar la transferencia de datos entre 2 redes diferentes. Si los dispositivos que se comunican se encuentran en la misma red, entonces la capa de red no es necesario. Esta capa divide los segmentos de la capa de transporte en unidades más pequeñas, llamadas paquetes, en el dispositivo del emisor y vuelve a juntar estos paquetes en el dispositivo del receptor. También busca la mejor ruta física para que los datos lleguen a su destino, esto se conoce como enrutamiento

2. Capa de enlace de datos

Esta facilita la transferencia de datos entre 2 dispositivos dentro de la misma red, esta toma los paquetes de la capa de red y los divide en partes más pequeñas que se denominan tramas. Al igual que en la capa de red, esta capa también es responsable del control de flujo y el control de errores en las comunicaciones dentro de la red.

1. Capa física

Esta capa incluye el equipo físico implicado en la transferencia de datos, tal como los cables y los conmutadores de red. En esta capa es donde los datos se convierten en una secuencia de bits.

Modelo TCP/IP

Actualmente es el estándar de facto para la comunicación de redes de computadoras en el mundo, es un conjunto de protocolos de red que determina los requisitos para que se establezca una transferencia de datos online de forma segura y eficiente

Principales características.

- **Compatibilidad de dispositivos**: Al ser convertido en el estándar la mayoría de los dispositivos actuales y sistemas operativos están diseñados para ser compatibles con este modelo, lo que facilita la comunicación entre diferentes proveedores.
- **Interoperabilidad**: Esto permite que una comunicación entre diferentes sistemas operativos utilizando el mismo conjunto de protocolos TCP/IP.
- **Flexibilidad**: Permite admitir una amplia gama de aplicaciones y servicio, este mismo proporciona una base sólida para la navegación web, la transmisión de video o transferencia de archivos.
- **Fiabilidad y control de errores**: Ofrece múltiples mecanismos para garantizar una entrega confiable de los datos, le ofrece a cada segmento enviado una enumeración, trazabilidad y seguimiento para asegurarse de que todos los datos lleguen de manera correcta.

¿Cuáles son las capas del modelo TCP/IP?

Este modelo consta de 4 capas, las cuales son:

Capa de aplicación

Se ocupa de la interacción entre las aplicaciones y la red. Los protocolos que interactúan con esta capa tienen la finalidad de establecer reglas y formatos necesarios para que las aplicaciones puedan intercambiar información de manera efectiva, ofreciendo la interoperabilidad.

Capa de transporte

Se gestionan las conexiones de extremo a extremo y se garantiza una entrega confiable de los datos.

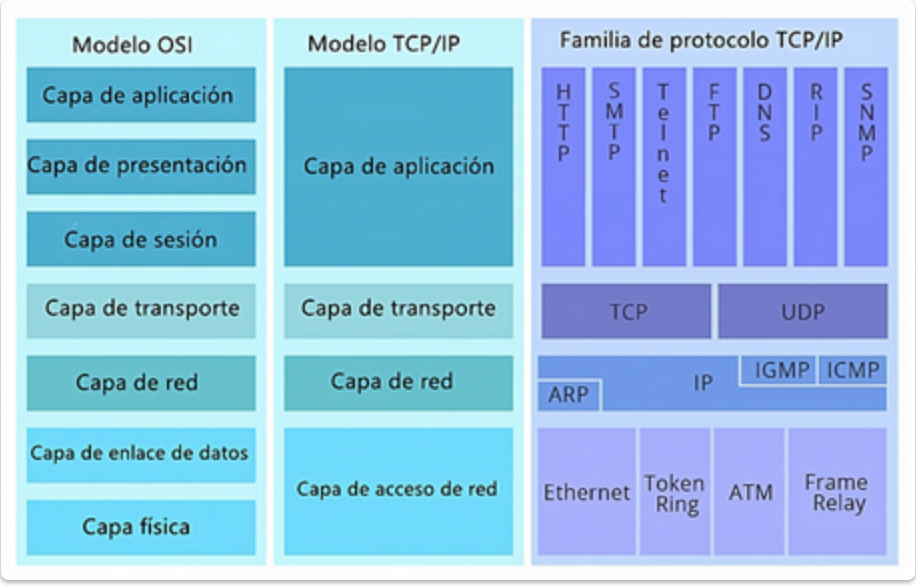
Capa de internet

Es la responsable del enrutamiento de los paquetes de datos a través de la red. Además, se encarga de dividir y ensamblar los datos en paquetes más pequeños para su transmisión

Capa de enlace de datos

Se encarga de la transmisión física de datos a través de un medio de red, como Ethernet. Wi-Fi o fibra óptica. En la misma se especifican los detalles técnicos y los protocolos utilizado para la comunicación en la red local.

Distribución de los protocolos



Protocolos

Capa de aplicación

- **HTTP** y **HTTPS**: Hypertext Transfer Protocol o Hypertext Transfer Protocol secure, son los protocolos o conjunto de reglas de comunicación cliente-servidor.
- **SMTP:** Simple Mail Transfer Protocol, es un protocolo de comunicación que se utiliza para enviar y recibir mensajes de correo electrónico a través de Internet.
- **SSH**: Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores a través de Internet con un mecanismo de autenticación.
- **FTP**: File Transfer Protocol, se utiliza para transferir todo tipo de archivos entre equipos conectados a una red.
- **DNS**: Domain Name System, se encarga de traducir los nombres de dominios aptos para la lectura humana a direcciones IP aptas para la lectura por parte de las maquinas.
- **DHCP**: Dynamic Host Configuration Protocol, es el encargado de asignar direcciones IP a los nuevos dispositivos en una red o dispositivos que soliciten una nueva IP.
- **RIP**: Routing Information Protocol, se usa para administrar información de enrutadores en una red autocontenida.
- **SNMP**: Simple Network Management Protocol, es un protocolo destinado para la gestión de la transferencia de información en redes, especialmente para uso en LAN.

Capa de transporte

- **TCP**: Transmission Control Protocol, es un estándar de comunicaciones para entrega de datos y mensajes a través de la red. (confiable, orientado a conexión)
- **UDP**: User Datagram Protocol, se utiliza en Internet para transmisión sujetas a limitaciones temporales. (rápido, sin conexión)

Capa de red

- **IP**: Internet Protocol, es el conjunto de reglas que rigen el formato de los datos enviados a través de internet o la red local.
- **ARP**: Address Resolution Protocol, se encarga de convertir dinámicamente las direcciones de Internet en las direcciones de hardware exclusivas de las redes de área local.
- **IGMP**: Internet Group Management Protocol, permite que varios dispositivos compartan la misma dirección IP para que todos puedan recibir los mismos datos.
- **ICMP**: Internet Control Message Protocol, proporciona un mecanismo estandarizado para que los dispositivos de red comuniquen información crucial, como la conectividad y el estado de la red.

Capa de acceso a la red

- **ETHERNET**: Permite que los dispositivos intercambien paquetes de datos entre sí a través de una red para comunicarse.
- **Frame Relay**: Es una tecnología de conmutación de paquetes que se utiliza en redes WAN para transmitir datos de manera eficiente y confiable.

¿Qué es TTL?

Time To Live se utiliza para limitar la duración o número de saltos que un paquete puede dar dentro de la red antes de ser descartado, esto es útil ya que se evita que el paquete salte de forma indefinida y se evita la creación de bucles de enrutamiento.

Mecanismos de establecimiento de conexión

Son los procesos y protocolos diseñados para iniciar una sesión de comunicación entre 2 puntos en una red, en otras palabras, es el proceso inicial donde los dispositivos negocian los parámetros necesarios para poder empezar y asegurar la transmisión de datos entre ellos, existen muchos tipos, entre los que están:

- TCP Handshake: Conocido como el Three-Way Handshake, es operado por el protocolo TCP, este asegura una conexión confiable, para que este mecanismo funcione se necesitan 3 pasos: Paso 1: Envió del segmento SYN, Paso 2: Respuesta con SYN-ACK, Paso 3: Recepción del segmento SYN-ACK y envió del segmento ACK.
- UDP: A diferencia de TCP este mecanismo no establece una conexión previa, acá el handshake no existe, los datagramas se envían directamente sin garantizar la entrega, el orden o la integridad.

Firewalls

Es un sistema o grupo de sistemas que impone una política de control de acceso entre redes.

Propiedades comunes de los Firewall

- Resisten ataques de red.

- Son el único punto de tránsito entre las redes corporativas internas y las redes externas.
- Aplican la política de control de acceso.

Ventajas de los Firewalls

- Evitan la exposición de hosts, recursos y aplicaciones confidenciales a usuarios no confiables.
- Sanean el flujo de protocolos, lo que evita el aprovechamiento de las fallas de protocolos.
- Bloquean los datos maliciosos de servidores y clientes.
- Simplifican la administración de la seguridad.

Limitaciones de los Firewalls

- Un firewall mal configurado puede tener graves consecuencias para la red, por ejemplo, convertirse en un punto único de falla.
- Los datos de muchas aplicaciones no se pueden transmitir con seguridad mediante firewalls.
- Los usuarios pueden buscar maneras de esquivar el firewall para recibir material bloqueado, lo que expone a la red a posibles ataques.
- Puede reducirse la velocidad de la red.
- El tráfico no autorizado se puede tunelizar u ocultar como tráfico legítimo a través del firewall.

Tipos de Firewalls

Firewall basado en host

Es una solución de seguridad que se instala directamente en un dispositivo individual, protege específicamente al host en el que este instalado . Filtra el tráfico de red entrante y saliente según reglas predefinidas, protegiendo al dispositivo contra accesos no autorizados. Ejemplos comunes incluyen Windows Defender Firewall y iptables en sistemas Linux.

Firewall para filtrado de paquetes (Sin estado)

Suelen formar parte de un firewall de router, que autoriza o rechaza el tráfico a partir de la información de las capas 3 y 4. Utilizan una simple búsqueda en la tabla de políticas que filtra el tráfico según criterios específicos.

Firewall activo o con estado

Son los más versátiles y las tecnologías de firewall más comúnmente usadas. proporcionan un filtrado de paquetes utilizando la información de conexión que se mantiene en una tabla de estados. El filtrado con estado es una arquitectura de firewall que se clasifica en la capa de red. También analiza el tráfico en las capas 4 y 5 de OSI.

Firewall del Gateway de aplicaciones

Filtra la información en las capas 3, 4, 5 y 7 del modelo de referencia OSI. La mayor parte del control y filtrado del firewall se realiza en el software.

Firewall de próxima generación

Los firewalls de próxima generación (NGFW) van más allá de los firewalls tradicionales al incluir capacidades avanzadas como:

- **Inspección profunda de paquetes (DPI):** Analiza el contenido de los paquetes más allá de las cabeceras para detectar amenazas avanzadas.
- **Prevención de intrusiones (IPS):** Detecta y bloquea actividades maliciosas en tiempo real.
- **Control de aplicaciones:** Identifica y regula el tráfico basado en aplicaciones específicas, no solo en puertos o direcciones IP.
- **Análisis de amenazas en la nube:** Consulta bases de datos externas para identificar patrones de ataque emergentes y amenazas nuevas.
- **Políticas basadas en usuarios:** Aplica reglas de seguridad según la identidad del usuario, no solo la dirección IP.