INSTITUTO POLITECNICO NACIONAL

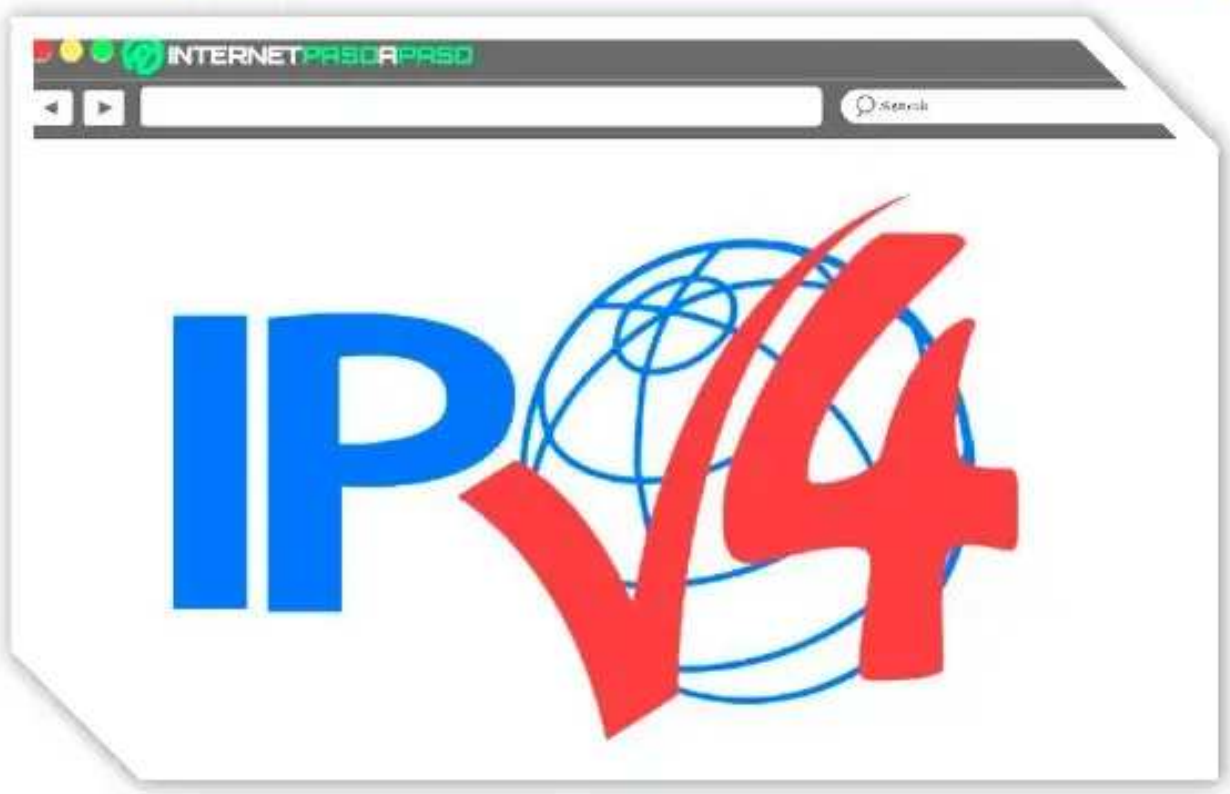
"La Técnica al Servicio de la Patria"

Grupo: **7CV5**

Nombre del protocolo: **IPV4 Y RFC 791**

Alumno: **Porta Pedro Nicolas**

Fecha de entrega: **13 de Marzo del 2024**



ÍNDICE

Introducción

IPv4

La IPv4, o mejor conocido como Protocolo de Internet versión 4, es el protocolo de red más utilizado en el mundo. Se fundó en la década de 1980, (en el año 1978 específicamente) este protocolo ha sido la columna vertebral de las comunicaciones por Internet, haciendo que miles de millones de dispositivos se puedan conectar y comunicar entre sí en todo el mundo. Básicamente, IPv4 es una forma de identificar y enrutar paquetes de datos a través de redes interconectadas, enviando información a todo el mundo.

El formato de dirección IPv4, consiste en una secuencia de números decimales separados por puntos, es quizás el más familiar de los rituales secundarios. Estas direcciones, llamadas direcciones IP, identifican de forma única todos los dispositivos conectados a Internet, incluidos ordenadores, teléfonos inteligentes, servidores y dispositivos IoT.Independientemente de su alcance y uso, IPv4 está en problemas estos días. Uno de los mayores problemas es la falta de direcciones IPv4 disponibles. La explosión de dispositivos conectados a Internet en las últimas décadas ha agotado el suministro limitado de direcciones IPv4.A medida que la demanda de direcciones IP continúa aumentando, la comunidad técnica está trabajando para desarrollar otras soluciones. Una forma es utilizar

IPv6, la última versión del Protocolo de Internet. IPv6 ofrece un rango de direcciones más amplio que IPv4, lo que permite una escalabilidad casi infinita de Internet de las cosas y otros entornos conectados. A pesar de los desafíos y la transición en curso a IPv6, IPv4 sigue siendo esencial para el funcionamiento de Internet en la actualidad. Su legado sigue vivo en la arquitectura de las redes globales y en la forma en que interactuamos con el mundo digital que nos rodea. En otras palabras, IPv4 se ha convertido en una piedra angular importante para el desarrollo y expansión del mundo de las comunicaciones.

RFC 791

RFC 791, titulado "Protocolo de Internet - Especificación del protocolo del programa de Internet DARPA", es uno de los primeros documentos que definen el Protocolo de Internet versión 4 (IPv4). Publicado en septiembre de 1981 por la Agencia de Proyectos de

Investigación Avanzada de Defensa (DARPA), este documento establece los principios básicos y requisitos técnicos de IPv4, que ha sido la columna vertebral de las comunicaciones por Internet durante décadas. de IPv4. Esto será explicado. Operación del encabezado IPv4, que es una parte importante del paquete de datos IPv4. Este encabezado contiene la información necesaria para enrutar y reenviar paquetes a través de redes interconectadas. RFC 791 también cubre aspectos fundamentales del protocolo, como la segmentación de paquetes, la gestión de direcciones IP y el manejo de errores.A lo largo de los años, RFC 791 se ha convertido en el estándar de referencia para la implementación y el desarrollo de redes compatibles con IPv4. Esto sienta las bases para la interoperabilidad de dispositivos y aplicaciones a través de Internet, permitiendo la comunicación entre diferentes dispositivos y sistemas en todo el mundo. Independientemente de la dirección del avance de varios protocolos de Internet como IPv6 y RFC, los documentos 791 todavía están importante de entender. e implementación de IPv4. Su legado sigue vivo en la

infraestructura de red mundial y en la forma en que interactuamos con el mundo digital que nos rodea. En resumen, RFC 791 es un hito en el desarrollo de Internet y sigue siendo una referencia clave en tecnología de redes y comunicaciones.

Marco Teórico

- **¿Qué es la IPv4?**

La IPv4 (o mejor conocido como Internet Protocol Version 4) es un protocolo o formato de dirección (Creada en el año 1978) que nos permite a todas las máquinas y dispositivos comunicarnos entre sí mismos. Este protocolo de internet está definido por la norma RFC 791, van de la mano y de hecho el RFC 791 podría decirse de cierto modo que es la "columna vertebral" de la IPv4. Este protocolo de internet fue el primero de todos, no hay registro de versiones previas a este.

Como lo hemos visto en clase, este protocolo utiliza direcciones de 32 bits, formados en 4 octetos ya sean de 1´s o 0´s (con 8 bits cada octeto) y estos están separados por puntos en notación decimal justo como los ejercicios vistos en clase.

Tenemos direcciones que van desde 0.0.0.0 hasta la 255.255.255.255, esto quiere decir que con esta IPv4 podríamos direccionar 2^32 bits, esto transformándolo, nos daría que este protocolo es capaz de direccionar un total de 4, 294, 967, 296 direcciones únicas.

- **¿Porque se usa?**

Este fue el primer protocolo de internet, fue ampliamente adoptado y se implementó prácticamente en todos los dispositivos de red, en los sistemas operativos y hasta en los equipos de red de todo el mundo.

De igual manera tenía muchas ventajas como la infraestructura, ya que esta se construyó sobre la IPv4 durante muchísimos años, al empezar a incrementar el número de dispositivos y agotarse poco a poco las direcciones, se tuvo que realizar un nuevo protocolo el cual era el IPv6 y el migrar todo de un protocolo a otro es muy costoso y lento. Muchas organizaciones hoy en día todavía dependen de la IPv4 y sería demasiado lento y costoso como ya se mencionó, cambiar de una IPv a otra, por eso estas empresas prefieren seguir usando esta IPv4.

De igual manera hay muchas aplicaciones y dispositivos que están diseñados para funcionar con la IPv4 y no son compatibles con la IPv6, para poder realizar tal compatibilidad deberíamos reestructurar muchas cosas y actualizar dichas aplicaciones o dispositivos para que dicha compatibilidad sea correcta.

El uso extendido de las direcciones privadas y de la NAT (Network Address Translation) han hecho que la vida útil de la IPv4 sea más larga y siga ocupándose hasta el día de hoy ya que permite que muchos dispositivos se conecten a internet utilizando un número limitado de direcciones publicas IPv4. Sin necesidad de hacer una transición total a la IPv6.

- **¿Por qué colapso la IPv4?**

Una de las principales situaciones por las que colapso fue porque la escasez de direcciones ip era demasiada. Ya que en la actualidad es tanto el incremento de los dispositivos que se conectan a internet que el número de IP necesarias ha superado la cantidad de direcciones disponibles en la IPv4.

Otra de las razones por las que colapso tan rápido la IPv4 es que cuando se creo no se esperaba que las direcciones se acabaran, pero con el incremento de dispositivos, el suministro de direcciones se agotó muy rápido ya que esta IPv4 esta limitado a 32 bits.

De igual manera, la globalización y expansión del internet llegaba a todos los países por lo que la demanda de direcciones IPv4 aumentaba constantemente hasta que en el año 2011 la ICANN (Corperacion de Internet para la Asignación de Nombres y Números) anunció que formalmente las direcciones IPv4 se habían agotad. Esto marco un punto crítico en la escasez de direcciones disponibles.

Trama de protocolo IPv4

La trama de protocolo IPv4 es una estructura de datos que contiene diferentes campos para el transporte de paquetes de datos a través de una red utilizando el protocolo IPv4. Los campos más importantes presentes en una trama IPv4 son

Versión

Como sugiere el nombre, este campo nos da la versión del protocolo IP al que pertenece el paquete y tiene un tamaño de 4 bits. Si tuviéramos que capturar el tráfico, el campo Versión mostraría un valor decimal de "4", que hace referencia a la versión 4 del protocolo IP. Longitud del encabezado. Su tamaño es de 4 bits, lo que nos da un tamaño de cabecera IPv4 de 32 bits o 4 bytes, lo que como ya sabemos suena complicado. Pongamos algunos ejemplos para explicar este concepto. Digamos que el campo Tamaño del encabezado muestra un valor decimal de 5; para encontrar el tamaño real del encabezado, debemos usar la siguiente fórmula:

Tamaño del encabezado

En este caso, el tamaño de nuestro encabezado es igual a 5 * 32 bits, lo que nos dará un valor real del tamaño del encabezado de 160 bits o igual a 20 bytes, 1 byte son 8 bits. Si observa, el valor de 20 bytes es el tamaño mínimo del encabezado de un paquete IP, lo que significa que no se muestran valores menores a 5 en este campo de longitud del encabezado. Tenga en cuenta que este campo solo incluye el tamaño del encabezado IP, no los datos encapsulados como se muestra en la Figura 4. MTU

DSCP/ECN

Este campo se utiliza para Calidad de servicio (QoS), originalmente llamado Tipo de servicio, y tiene un tamaño de 8 bits, de los cuales los primeros 6 bits se denominan Punto de código DiffServ (DSCP) y los últimos 2 bits se denominan Borrar congestión. Declaración (ECN).

Longitud total o longitud del paquete

Este campo muestra el tamaño total del paquete en bytes. Este tamaño tiene en cuenta el encabezado IP más el encabezado TCP y los datos de la capa de aplicación

El tamaño de este campo es de 16 bits, por lo que el valor decimal máximo que podemos obtener con 16 bits es 65535, lo que significa que el tamaño máximo de un paquete IP es 65535 bytes.

Identificación:

Si el paquete IP está fragmentado, cada paquete fragmentado utilizará el mismo número de identificación de 16 bits para identificar a qué paquete IP pertenecen.

Señaladores (IP Flags):

Hay 3 bits que se utilizan para la fragmentación

El primer bit siempre se establece en 0.

El segundo bit se llama bit DF (Do not Fragment) e indica que este paquete no debe estar fragmentado.

El tercer bit se llama bit MF (Más Fragmentos) y se establece en todos los paquetes fragmentados, excepto en el último.

Desplazamiento de fragmentos (Fragment Offset):

Campo de 13 bits, que indica la posición específica del fragmento en el paquete fragmentado original

Time To Live (Tiempo de vida):

A medida que veamos sobre los protocolos de enrutamiento, nos daremos cuenta de que una mala configuración puede hacer que un paquete circule sin cesar a través de la red sin

llegar nunca al dispositivo de destino. Esto se llama bucle. El propósito de este campo Tiempo de vida es detener el enrutamiento del bucle. Introduzca un valor en este campo. El valor recomendado es 64. Este número se reducirá en una unidad. Siempre que pasa por un enrutador, cuando el campo TTL de un paquete de datos llega a "0", el enrutador, que reduce el valor a 0, descartará los paquetes y enviará un mensaje de error de "tiempo de espera" ICMP al dispositivo que envió el paquete.

Protocolo

Este campo indica qué protocolo está utilizando la capa superior. Su tamaño es de 8 bits. Los números más comunes que encontramos en este campo se muestran en la Figura 6.

Protocolo	Numero
ICMP	1
TCP	6
UDP	17
OSPF	89

Unidad de transmisión máxima

Suma de comprobación

Tiene 16 bits de longitud y ayuda a verificar la integridad del encabezado IP. Esto significa que los datos en el encabezado IP no cambian ni modifican durante la transmisión. La suma de comprobación se calcula en cada salto hasta alcanzar la unidad objetivo. Dirección de destino/dirección de origen

Estos campos son los más importantes para el estudio de CCNA y tienen un tamaño de 32 bits. En el campo Dirección de origen, ingrese la dirección IPv4 del dispositivo que inicia la comunicación y en el campo Dirección de destino, ingrese la dirección IPv4 del dispositivo de destino con el que desea comunicarse.

Opciones

Tiene un tamaño variable entre 0 y 40 bytes. Los usos principales de este campo son el enrutamiento de origen flexible, el enrutamiento de origen estricto, la marca de tiempo y el enrutamiento de registros. Estas opciones se pueden invocar mediante el comando PING.

Relleno

Este campo simplemente agrega bits de relleno para que el encabezado termine en un límite de 32 bits. Recuerde que el campo Longitud del encabezado nos da un valor para el tamaño del encabezado en palabras de 32 bits, por lo que el tamaño del encabezado no puede ser más que 32 bytes o un múltiplo de 4 bytes, y debido a este relleno, puede alcanzar ese límite.

- **Clases de direcciones IPv4**

Clases de direcciones IPv4: IPv4 se dividió originalmente en cinco clases principales: A, B, C, D y E. Estas clases se utilizaron para asignar direcciones en redes de varios tamaños. Sin embargo, debido a ineficiencias y otros problemas, el concepto de clase fue reemplazado por el método de asignación de direcciones de bloque de Class Interdomain Routing (CIDR). Debido a la ineficiencia y otras razones, se desarrolló la división en subredes y no se utilizó la Clase E para la asignación de direcciones.

- **SUBREDES Y MASCARAS DE SUBRED**

Para optimizar el uso de direcciones IPv4 y proporcionar información sobre redes pequeñas, se utiliza una máscara de subred para separar una dirección IP en un segmento de red y un segmento de host. Esto le permite crear subredes dentro de una red más grande.

- **Direccionamiento privado y público**

Para conservar las direcciones IPv4 públicas y el espacio de direcciones, se reservan bloques de direcciones para redes privadas que no se pueden transferir a través de la Internet pública. Estas direcciones se utilizan en redes domésticas y comerciales y se traducen a direcciones públicas mediante NAT al acceder a Internet.

- **Protocolos y servicios relacionados:**

IPv4 admite una variedad de protocolos y servicios, incluidos el Protocolo de control de transmisión (TCP) y el Protocolo de datos de usuario (UDP), que se utilizan para la transmisión de datos confiable y la deshonestidad. También admite servicios como DHCP para la asignación automática de direcciones IP y el Sistema de nombres de dominio (DNS) para la resolución de nombres de dominio.

- **Problema de escasez:**

La incrementación de dispositivos conectados a Internet ha reducido el conjunto de direcciones IPv4 disponibles. Esto llevó al desarrollo y adopción de IPv6, que proporciona un mayor espacio de direcciones y resuelve muchos de los problemas asociados con IPv4, como la incertidumbre de las direcciones y la necesidad de NAT.

- **CARACTERISTICAS**

Direccionamiento Jerárquico: IPv4 utiliza un esquema de direccionamiento jerárquico que divide el espacio de direcciones en redes más pequeñas, lo que permite una administración más eficiente de las direcciones IP en todo Internet.

Compatibilidad: Aunque IPv4 es el protocolo IP original, es compatible con una amplia gama de dispositivos y sistemas operativos, lo que lo convierte en una opción universalmente aceptada para la comunicación en redes

Encaminamiento: IPv4 utiliza tablas de enrutamiento para determinar la ruta óptima para enviar paquetes de datos de un origen a un destino a través de múltiples redes interconectadas.

Protocolo sin Conexión: IPv4 es un protocolo sin conexión, lo que significa que no establece una conexión previa entre el origen y el destino antes de enviar datos. En lugar de eso, cada paquete de datos se enruta de manera independiente.

Protocolo de Capa de Red: IPv4 opera en la capa de red del modelo OSI (Open Systems Interconnection), proporcionando conectividad y direccionamiento a nivel de red para dispositivos en una red.

Soporte para Protocolos de Capa de Transporte: IPv4 es compatible con una variedad de protocolos de capa de transporte, como TCP (Transmission Control Protocol) y UDP (User Datagram Protocol), que se utilizan para el transporte confiable y no confiable de datos, respectivamente.

NAT (Traducción de Direcciones de Red): IPv4 se puede implementar junto con NAT para superar la escasez de direcciones IP públicas. NAT permite que varios dispositivos en una red privada compartan una única dirección IP pública, lo que conserva las direcciones IPv4.

Escasez de Direcciones: Una de las limitaciones más significativas de IPv4 es la escasez de direcciones IP disponibles debido al agotamiento gradual del espacio de direcciones IPv4. Esto ha llevado a la adopción gradual de IPv6, que ofrece un espacio de direcciones mucho más amplio.

Longitud del Encabezado Variable: El encabezado IPv4 tiene una longitud variable, lo que permite la inclusión de opciones adicionales, como la marca de tiempo, la calidad de servicio (QoS) y la fragmentación de paquetes.

Suma de Verificación de Encabezado: IPv4 utiliza una suma de verificación de encabezado para verificar la integridad del encabezado IPv4 durante la transmisión, lo que garantiza que los paquetes no se hayan corrompido durante el transporte.

- **RFC 791**

RFC 791, el "Protocolo de Internet - Especificación del protocolo del programa de Internet DARPA", fue el primer documento que describio los requisitos técnicos y los principios básicos del Protocolo de Internet versión 4 (IPv4). El
RFC 791, publicado en septiembre de 1981 por la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA), es uno de los documentos más importantes en el desarrollo de Internet.

RFC 791 detalla la estructura y función del encabezado IPv4. Es una parte básica del paquete de datos IPv4. Este encabezado contiene la información necesaria para enrutar y reenviar paquetes a través de redes interconectadas. RFC 791 también aborda aspectos fundamentales del protocolo, como la segmentación de paquetes, la gestión de direcciones IP y el manejo de errores.

Este documento también aborda IPv4, incluida su arquitectura de información. Astronomía, comunicación inalámbrica y mejores prácticas. . Basado en enrutamiento, comunicación entre dispositivos en diferentes redes.

La RFC 791 describe el formato del encabezado IPv4, que es la parte fundamental de un paquete de datos IPv4.

En esta estructura: Versión: un campo de 4 bits que indica la versión del protocolo IP (en este caso IPv4).

IHL (Internet Long Header): este campo de 4 bits indica la longitud del protocolo IP. El encabezado es una palabra de 32 bits. Un encabezado IPv4 puede tener un tamaño de hasta 60 bytes (15 palabras de 32 bits), pero normalmente un mínimo de 20 bytes (5 palabras de 32 bits).

Tipo de servicio: campo de 8 bits que proporciona información sobre: información sobre la calidad de servicio deseada, como la prioridad de los paquetes, la velocidad de transmisión y la fiabilidad.

Longitud total: un campo de 16 bits que representa la longitud total de un paquete IPv4, incluidos encabezados y datos. Este se mide en octetos

Identificador, indicador y delimitador: estos campos están relacionados con la segmentación de paquetes IPv4.

TTL (Tiempo de vida): un campo de 8 bits que limita el TTL (Tiempo de vida) de un paquete en la red.

Protocolo: Un campo de 8 bits que especifica el protocolo de capa por encima del cual se

entrega el paquete. Después del procesamiento IPv4.
Suma de Verificación del Encabezado (16 bits): Se utiliza para verificar la integridad del encabezado IPv4 durante la transmisión.

Verificar encabezado: un campo de 16 bits utilizado para verificar la exactitud del encabezado IPv4.Dirección de origen y dirección de destino: un campo de 32 bits que identifica la dirección IP de origen y destino.

Dirección IP de Origen (32 bits): Indica la dirección IP del remitente del paquete.

Dirección IP de Destino (32 bits): Indica la dirección IP del destinatario del paquete.

Opciones y relleno: estos campos son opcionales. . , esta estructura puede existir si el

encabezado IPv4 contiene otras opciones.
Esta estructura es la base de los paquetes de datos IPv4 enviados a través de Internet.

DUDAS

¿Porque el ping envía 4 paquetes?

Para probar la accesibilidad de una computadora, Ping en su configuración predeterminada envía cuatro paquetes de solicitud de eco ICMP de 32 bytes cada uno a la dirección especificada como parámetro.

ICMP (Protocolo de mensajes de control de Internet) es un protocolo utilizado para intercambiar información y mensajes de error en redes IPv4. Para redes informáticas

basadas en IPv6, se puede utilizar el futuro protocolo ICMPv6.

¿Porque en la trama del protocolo no hay mascara?

Hay dos tipos de máscaras de subred, la del host y la de la red, en este caso los paquetes no necesitan llevar una máscara, esto se debe a que cuando un dispositivo IPv4 recibe un paquete, examina la dirección ip de donde vino junto con su máscara para así determinar si la dirección IP de destino está en la misma red local o necesita ser enviada a través de routers para ser recibido,

¿Por qué al enviar un ping nos da un TTL?

El tiempo de respuesta es el tiempo que tarda un paquete de datos en llegar a la computadora de destino y transmitirse de regreso. La fecha de vencimiento representada

por TTL corresponde a la fecha de vencimiento del paquete de datos. El valor predeterminado es hasta 255. Las implementaciones con TTL predeterminados de 31, 63 o 127 son comunes. Cada vez que un paquete pasa a través de un nodo de red, el TTL disminuirá en una unidad. En este caso hablamos de lúpulo. Si el TTL se reduce a 0, el paquete se descarta.

¿Porque al desconectar la tarjeta de red, sigue funcionando?

Si desconecta físicamente la tarjeta de red del dispositivo, pero todavía parece funcionar, puede haber varias razones:

Caché ARP: el dispositivo mantiene una tabla de caché del Protocolo de resolución de direcciones (ARP) que asigna direcciones IP a direcciones MAC. Si se ha comunicado recientemente con otros dispositivos en la red, es posible que su sistema aún almacene en caché las entradas ARP. Por lo tanto, incluso si la NIC no funciona, las entradas ARP almacenadas en caché aún se pueden usar para comunicarse con dispositivos en la misma subred.

Conexiones establecidas: si el dispositivo tenía conexiones de red activas antes de quitar la tarjeta de red, esas conexiones pueden continuar funcionando por un tiempo porque el sistema operativo todavía tiene recursos asignados para procesarlas. Sin embargo, estas conexiones pueden fallar eventualmente cuando el sistema se da cuenta de que el adaptador de red no está disponible.

Otras interfaces de red activas: algunos dispositivos pueden tener múltiples interfaces de red (como Ethernet y Wi-Fi). Si una de las interfaces se desconecta, el dispositivo puede cambiar automáticamente a la otra interfaz que todavía está disponible y funciona correctamente.

Sistema operativo y configuración de red: el comportamiento puede depender del sistema operativo y de cómo esté configurado el dispositivo para manejar las interrupciones de la tarjeta de red. Algunos sistemas operativos pueden tener configuraciones que permiten que ciertas operaciones de red continúen incluso cuando el adaptador de red está desconectado.

En cualquier caso, aunque el dispositivo pueda seguir funcionando temporalmente después de desconectar la tarjeta de red, es importante tener en cuenta que una vez que el sistema se dé cuenta de la falta de conectividad de la red, el funcionamiento normal de la red eventualmente se verá afectado y la comunicación cesará. Deja de funcionar correctamente.

¿Por qué este protocolo es hackeable?

IPv4, al igual que cualquier otro protocolo de red, no es intrínsecamente "hackeable", sino que puede ser vulnerable a ciertas vulnerabilidades y ataques debido a su diseño y su implementación en la red. Algunas razones por las cuales IPv4 puede ser considerado más vulnerable en comparación con IPv6 incluyen:

Direcciones IP estáticas y limitadas: IPv4 tiene un espacio de direcciones IP limitado, lo que puede llevar a la asignación de direcciones IP estáticas y la reutilización de direcciones IP, lo que facilita la identificación y el rastreo de dispositivos en la red. Esto puede ser explotado por los atacantes para dirigir ataques específicos a dispositivos individuales.

Ausencia de autenticación y cifrado: IPv4 no proporciona mecanismos integrados para autenticar o cifrar el tráfico de red, lo que deja abierta la posibilidad de ataques de suplantación de identidad (spoofing) y escuchas de tráfico (sniffing). Los atacantes pueden interceptar y modificar el tráfico de red sin ser detectados.

Fragmentación de paquetes: IPv4 permite la fragmentación de paquetes, lo que puede ser utilizado por los atacantes para enviar paquetes maliciosos que eviten la detección por parte de los sistemas de seguridad de red.

Protocolos y servicios obsoletos: Algunos protocolos y servicios asociados con IPv4 pueden ser obsoletos o no seguros, lo que puede dejar abiertas vulnerabilidades en la red. Por ejemplo, el Protocolo de Control de Mensajes de Internet (ICMP) se ha utilizado en ataques de denegación de servicio (DDoS).

Falta de soporte para seguridad integrada: IPv4 no incluye características de seguridad integradas, como la autenticación de paquetes o la integridad de los datos. Si bien se pueden implementar soluciones externas, como firewalls y sistemas de detección de intrusiones (IDS), la seguridad de IPv4 a menudo depende de la configuración y la implementación de estas soluciones adicionales.

Es importante tener en cuenta que la seguridad de cualquier red, incluida la que utiliza IPv4, depende en gran medida de la implementación adecuada de medidas de seguridad, como el cifrado, la autenticación y la segmentación de red, así como de la actualización regular de software y parches de seguridad para mitigar vulnerabilidades conocidas.

¿Por qué este protocolo no es confiable?

IPv4, como cualquier otro protocolo de red, no es inherentemente "no confiable". Sin embargo, varios factores pueden contribuir a la percepción de que IPv4 es menos confiable que otras tecnologías de red. Algunas razones:

Falta de direcciones IP: el espacio de direcciones IP en IPv4 es limitado, lo que resulta en una falta de direcciones IP disponibles. Esto ha llevado a la reutilización de direcciones IP y al uso de NAT (traducción de direcciones de red) para permitir que varios dispositivos compartan una única dirección IP pública. Este enfoque puede complicar la administración de direcciones IP y causar problemas de conectividad.

Fragmentación de paquetes: IPv4 proporciona fragmentación de paquetes durante la transmisión de datos. Esto puede causar problemas de rendimiento y confiabilidad, especialmente en redes con condiciones variables, como alta latencia o pérdida de paquetes. Los atacantes también pueden utilizar la fragmentación para evitar la detección y el filtrado de tráfico malicioso. Falta de soporte para funciones de seguridad avanzadas: IPv4 carece

de funciones de seguridad integradas, como autenticación de paquetes e integridad de datos. Aunque se pueden implementar otras soluciones como firewalls y sistemas de detección de intrusos, la seguridad IPv4 muchas veces depende de la configuración e implementación adecuadas de estas soluciones externas. Problemas de enrutamiento: Los protocolos de enrutamiento utilizados en IPv4, como el Protocolo de enrutamiento de puerta de enlace interior (IGRP) o el Protocolo de enrutamiento de vector de distancia dinámica (RIPv2), pueden tener limitaciones en términos de escalabilidad, convergencia y seguridad. Esto puede causar problemas de enrutamiento y dificultades para mantener una red confiable y eficiente. Aunque IPv4 se usa ampliamente y ha demostrado ser confiable durante muchos años, su diseño y limitaciones inherentes pueden causar problemas en un entorno de red moderno y cambiante. Como resultado, muchas organizaciones están migrando gradualmente a IPv6, que proporciona un espacio de direcciones IP más amplio y características de seguridad mejoradas.

¿Por qué este protocolo es enrutable?

Dirección IP jerárquica: las direcciones IP IPv4 se crean en un formato jerárquico con una parte de red y una parte de host. Esto permite a los enrutadores tomar decisiones de enrutamiento basadas en la dirección de destino de un paquete IP. Los enrutadores utilizan tablas de enrutamiento para determinar la mejor ruta para llevar un paquete a su destino en función de la parte de red de la dirección IP.

Tablas de enrutamiento: los enrutadores en una red IPv4 mantienen tablas de enrutamiento que contienen información sobre diferentes redes y cómo llegar a ellas. Estas tablas de datos se actualizan y mantienen dinámicamente mediante protocolos de enrutamiento como OSPF, EIGRP, RIP y BGP. Los enrutadores utilizan estas tablas para tomar decisiones sobre el reenvío de paquetes y el enrutamiento a sus destinos. Protocolos de enrutamiento: IPv4 admite varios protocolos de enrutamiento diferentes que permiten el intercambio de información de enrutamiento entre enrutadores. Estos protocolos permiten a los enrutadores aprender rutas en redes remotas y compartir esta información con otros enrutadores de la red. Los enrutadores utilizan esta información para crear y mantener sus tablas de enrutamiento.
Protocolo de Internet (IP): el protocolo IP en sí proporciona las capas de direccionamiento y enrutamiento en la capa de red del modelo OSI. Determina cómo se direccionan y enrutan los paquetes a través de la red. Cada paquete IP contiene una dirección IP de origen y una dirección IP de destino, lo que permite a los enrutadores tomar decisiones de enrutamiento basadas en estas direcciones. En resumen, IPv4 es un protocolo de red enrutable porque puede dividir direcciones IP en partes de red y partes de host, mantener tablas de enrutamiento dinámicas, usar protocolos de enrutamiento para intercambiar mensajes de enrutamiento entre enrutadores y proporcionar direccionamiento y enrutamiento jerárquico de red. Esto permite al enrutador tomar decisiones de enrutamiento y enrutar paquetes IP al destino apropiado en la red.

¿Por qué se puede utilizar este protocolo de forma remota?

IPv4 es un protocolo de red diseñado para admitir la comunicación entre dispositivos en una red IP (local o remota). IPv4 se puede utilizar externamente por varios motivos:

Conectividad global: IPv4 permite conexiones y comunicación entre dispositivos de todo el mundo a través de Internet. Esto significa que un dispositivo que utiliza una dirección IPv4 puede comunicarse con otros dispositivos en diferentes ubicaciones geográficas siempre que tenga una conexión a Internet.

Protocolos de enrutamiento: los protocolos de enrutamiento IPv4, como Border Gateway Protocol (BGP) y Open Shortest Path First (OSPF), permiten a los enrutadores compartir información de enrutamiento y determinar la mejor ruta para enviar datos entre redes distantes. Facilita la comunicación entre dispositivos ubicados en diferentes redes y ubicaciones geográficas.

Acceso remoto: IPv4 admite protocolos y tecnologías que permiten el acceso remoto a dispositivos, como SSH (Secure Shell) y VPN (Virtual Private Network). Estas tecnologías permiten a los usuarios acceder y controlar de forma remota dispositivos a través de Internet, incluso si están ubicados en diferentes ubicaciones físicas.

Servicios en la nube: muchos servicios en la nube utilizan IPv4 para proporcionar acceso remoto a recursos y aplicaciones alojados en servidores remotos. Los usuarios pueden acceder a estos servicios a través de Internet utilizando direcciones IPv4 y protocolos estándar.

Tecnologías de túnel: IPv4 es compatible con tecnologías de túnel como IPv4 sobre IPv6 (también conocido como 6to4) y VPN basadas en IPv4, que permiten encapsular y transportar el tráfico IPv4 a través de redes IPv6 o redes privadas virtuales. En resumen, IPv4 es un protocolo de red versátil que permite la comunicación entre dispositivos en redes locales y externas, lo que lo hace adecuado para una variedad de aplicaciones y escenarios, incluido el acceso remoto y la conectividad global a Internet.

Conclusiones

En conclusión, la IPv4 y el RFC 791 representan pilares fundamentales en el desarrollo y la operación de Internet: IPv4, como el protocolo de red más utilizado durante décadas, ha proporcionado la base para la comunicación efectiva entre dispositivos en redes interconectadas. Su estructura, definida en el RFC 791, establece los principios básicos y las especificaciones técnicas para el funcionamiento del protocolo IPv4, incluyendo el formato del encabezado IPv4 y aspectos clave como el enrutamiento, la fragmentación de paquetes y el manejo de direcciones IP. El RFC 791 ha sido una guía esencial para la implementación y el desarrollo de sistemas de red compatibles con IPv4. Además, ha sentado las bases para la interoperabilidad de dispositivos y aplicaciones en Internet, permitiendo la comunicación efectiva en una escala global. Sin embargo, a medida que Internet ha crecido y evolucionado, IPv4 ha enfrentado desafíos significativos, como la escasez de direcciones IP disponibles. Aunque IPv4 sigue siendo ampliamente utilizado, la

adopción de IPv6, un protocolo con un espacio de direcciones mucho más amplio, se ha vuelto cada vez más importante para abordar estas limitaciones y garantizar el crecimiento continuo de Internet. En resumen, la IPv4 y el RFC 791 han sido elementos cruciales en el desarrollo y la expansión de Internet, proporcionando la base técnica y los estándares necesarios para la conectividad global. Aunque enfrentan desafíos, su legado perdura en la infraestructura de red global y continúan siendo referencias fundamentales en la ingeniería de redes y comunicaciones.

Recomendaciones

Daré varias recomendaciones para el uso y conocimiento de la IPv4 y la RFC 791 las cuales podrían ser el migrar a la IPv6 ya que migrar nuestros sistemas y redes a IPv6. Aunque IPv4 se usa ampliamente, IPv6 tiene un espacio de direcciones más grande y garantiza la continuidad y el crecimiento de Internet. Actualice sus conocimientos: mantener actualizados nuestros conocimientos de IPv4 y RFC 791 nos ayudará a comprender mejor los principios y las mejores prácticas para diseñar, implementar y administrar redes IPv4.

Y por último la Seguridad en las redes IPv4 requiere mucha seguridad, como firewalls, detección de intrusiones, sistemas de prevención de intrusiones y autenticación de usuarios. Ya que como sabemos la seguridad es esencial para proteger sus sistemas y datos de las amenazas cibernética

BIBLIOGRAFIA

1. Castillo, J. A. (2020, febrero 29). *IPv4 vs IPv6 – Qué es y para qué se utiliza en redes*. Profesional Review; Miguel Ángel Navas. https://www.profesionalreview.com/2020/02/29/ipv4-vs-ipv6/
2. *Conceptos Básicos de la Dirección IP*. (s/f). Temastecnologicos.com. Recuperado el 13 de marzo de 2024, de https://www.temastecnologicos.com/internet/direccion-ip/
3. Freda, A. (2021, marzo 11). *¿Qué diferencia hay entre IPv4 e IPv6?* ¿Qué diferencia hay entre IPv4 e IPv6?; Avg. https://www.avg.com/es/signal/ipv4-vs-ipv6

4. *¿Por qué los bits son contados en potencias de 2?* (s/f). Quora. Recuperado el 13 de marzo de 2024, de https://es.quora.com/Por-qu%C3%A9-los-bits-son-contados-en-potencias-de-2
5. Walton, A. (2017, noviembre 20). ▹*Paquete IPv4 y Paquete IPv6: Encabezados* ». CCNA desde Cero. https://ccnadesdecero.es/encabezado-paquete-ipv4/
6. Wikipedia contributors. (s/f). *Agotamiento de las direcciones IPv4*. Wikipedia, The Free Encyclopedia. https://es.wikipedia.org/w/index.php?title=Agotamiento_de_las_direcciones_IPv4&oldid=153784115
7. (S/f). Rfc-es.org. Recuperado el 13 de marzo de 2024, de https://www.rfc-es.org/rfc/rfc0791-es.txt
8. Walton, A. (2022, 17 junio). *¿Qué Pasó con IPv5? ¿Por qué hay IPv4, IPv6, pero no IPv5? » Redes*. CCNA Desde Cero. https://ccnadesdecero.es/que-paso-ipv5/#:~:text=El%20IPv5%20nunca%20ha%20sido,n%C3%BAmeros%20del%200%20al%20255.
9. Equipo editorial de IONOS. (2020, 5 junio). *Cómo utilizar el comando Ping en Windows*. IONOS Digital Guide. https://www.ionos.mx/digitalguide/servidores/herramientas/comando-ping/#:~:text=Para%20comprobar%20la%20disponibilidad%20de,la%20direcci%C3%B3n%20entregada%20como%20par%C3%A1metro.
10. Sepúlveda, M. (2022, 19 agosto). Encabezado de paquetes IPv4 Cisco - eClassVirtual - Cursos Cisco en línea. *eClassVirtual - Cursos Cisco en línea*. https://eclassvirtual.com/encabezado-de-paquetes-ipv4-cisco/
11. AdminNG. (2023, 8 mayo). *INTRODUCCIÓN AL PROTOCOLO IPV4*. Networkgeeks. https://netwgeeks.com/introduccion-al-protocolo-ipv4/

12.