Protocolo ICMPv

Transcribed on July 16, 2025 at 9:44 PM by Minutes AI

Speaker 1 (00:06)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a hablar sobre una parte fundamental de las redes IPV, el Protocolo de Mensajes de Control de Internet versión 6, también conocido como ICMP V.

Veremos cómo este protocolo es la base de otro denominado NDP o lo que es lo mismo, el Protocolo de Descubrimiento de Vecinos.

Conoceremos los mensajes más importantes de este protocolo, así como el conocido ataque de envenenamiento de vecinos o Naples Puffy.

Así que vamos a comenzar con esta sesión.

Comenzamos hablando de ICMPV.

Este protocolo juega un papel crucial en la administración y el mantenimiento de las redes ICV y su importancia se ve especialmente reflejada en el correcto funcionamiento del Protocolo de Descubrimiento de Vecinos.

En primer lugar, hablemos sobre las funciones principales de ICMPV.

Este protocolo se utiliza para enviar mensajes de control y error entre nodos dentro de una red IPV.

Estos mensajes son esenciales para la comunicación y la administración de la red.

Gracias a IGMP, nos facilita las tareas como la verificación de la conectividad, el diagnóstico de problemas de red, la administración de dispositivos, etc.

De hecho, vamos a comentar algunas de las principales funcionalidades.

Por ejemplo, los errores en la entrega de paquetes.

ICMPV es el responsable de informar sobre cualquier error en la entrega de paquetes IPV.

Por ejemplo, si un paquete IPV no puede ser entregado a su destino por algún motivo, como una ruta incorrecta o un tiempo de vida expirado, etc.

Un nodo puede enviar un mensaje ICMP V de error es particularmente un error de destino inalcanzable o bien tiempo de vida excedido al nodo de origen.

Por otro lado, algunas de las otras funcionalidades serían las redirecciones, ya que ICMPV también puede utilizarse para redirigir paquetes dentro de una red IPV.

Cuando un router determina que un paquete debería ser enviado por un camino diferente al especificado en el paquete, se podría enviar un paquete IGMP o V de redirección al nodo de origen para informarle sobre la mejor ruta a seguir.

Por otro lado, y similar a ICMP en redes IPV, en ICMP V se incluyen también los mensajes de solicitud de eco y respuestas de eco, en inglés el ECO Request y ECO Reply, que son comúnmente conocidos como los paquetes PIN.

Estos mensajes se utilizan para verificar la conectividad entre dos nodos y medir la latencia de la red.

Por otro lado, otra de las funcionalidades sería, por ejemplo, la gestión de mensajes multicast.

Y es que ICMP versión 6 también se utiliza para la gestión de mensajes multicast, como la membresía de grupos de multidifusión y la detección de nodos vecinos, como vamos a ver a continuación.

Y por último, la última funcionalidad que podemos destacar de IGMPV es que puede transportar mensajes de información y de diagnóstico sobre el estado y la configuración de la red, como el mensaje de solicitud de información de enlace, lo que sería la solicitación Router Solicitation y también el mensaje de anuncio de información de enlace, que sería el Router Advertisement.

Una de las funciones más destacadas de ICMPV es su papel en el mantenimiento del protocolo de descubrimiento de vecinos.

MDP es un protocolo de capa de enlace que se encarga de varias funciones esenciales en una red IPV.

Su principal objetivo es facilitar la comunicación entre nodos en la misma red local.

Ahora centrémonos en las funciones clave de NDP y por qué son tan importantes para las redes iCloud 6.

En primer lugar, como se ha comentado, NDP se encarga del descubrimiento de vecinos.

Esto significa que permite a los nodos descubrir otros nodos que están activos y disponibles dentro de la misma red local.

Este proceso es fundamental para establecer la conectividad entre dispositivos de la red.

Otra función esencial de NDP es la resolución de direcciones.

Cuando un nodo necesita comunicarse con otro nodo de la misma red local, necesita traducir la dirección de capa 3, es decir, la dirección IPV, a la dirección de capa 2, lo que sería la dirección Mac.

De esta manera, NDP facilita este proceso de resolución de direcciones asegurando que los nodos puedan comunicarse eficientemente entre sí.

En este proceso se envían mensajes IGMP, como son los mensajes de Neighbor Solicitation, conocido como NS y Neighbor Advertisement, que es NA.

De esta manera se solicita y se anuncia la información de vecinos necesaria.

Esto permite que los nodos construyan y mantenga una tabla de vecinos actualizada, lo que es fundamental para el enrutamiento y para la comunicación eficiente en una red IPV.

Y ahora pasamos a hablar de estos mensajes NS y NA o Network Solicitation in Network Advertisement.

Y es que estos mensajes serían esa pregunta ¿Hay alguien ahí?

En lo que sería una red IPV, cuando un nodo necesita comunicarse con otro nodo en la misma red local, pero no tiene su dirección Mac, su dirección de capa 2, va a enviar un mensaje NS solicitando esta información.

Este mensaje incluye la dirección IP del nodo destino y la dirección IP del nodo que envía la solicitud.

Por otro lado tendríamos los Network Advertisement, los mensajes NA, que es la respuesta a estas solicitudes.

De tal manera que cuando un nodo recibe un mensaje NS dirigido a él, responde con un mensaje NA.

Este mensaje NA va a contener su propia dirección de capa 2, lo que va a permitir al nodo que ha enviado la solicitud actualizar su caché de vecinos y con esta información va a poder continuar con la comunicación.

Los mensajes NA también pueden enviarse de forma proactiva, simplemente para anunciar la presencia de un nodo en la red.

Y es que esto es muy útil para asegurarse, entre otros nodos, que tiene la información de capa 2 necesaria para comunicarse, incluso si no la han solicitado explícitamente.

Ahora, tras conocer el protocolo de descubrimiento de vecinos y cómo funcionan los mensajes NSIMA, tenemos que hablar del término envenenamiento o suplantación de vecinos, o bien en inglés naplespoofing.

El naplespoofing ocurre cuando un atacante falsifica los mensajes o bien en ES o bien en EA para suplantar la identidad de un nodo legítimo en la red.

En otras palabras, el atacante engaña a otros nodos de la red haciéndole creer que es él el nodo legítimo al que se están intentando comunicar.

Esto sería algo parecido a un envenenamiento de la tabla ARP en IPV.

Por supuesto, se trata de un ataque peligroso, ya que cuando un atacante logra suplantar la identidad de un nodo legítimo puede llevar a cabo una serie de actividades maliciosas, como por ejemplo poder interceptar y manipular el tráfico de red, robar información confidencial si esta viaja sin cifrar o incluso lanzar ataques de denegación de servicio para interrumpir el funcionamiento normal de la red.

También tenemos que saber que tenemos varias medidas para poder mitigar este tipo de ataques.

Por ejemplo, podemos implementar la autenticación de mensajes NDP utilizando mecanismos como Secure Network Discovery o bien la configuración de listas blancas de direcciones Mac para limitar qué nodos se pueden comunicar entre sí.

A lo largo de esta sesión hemos cubierto una variedad de temas importantes relacionados con las redes y tu, incluyendo el protocolo de Mensajes de Control de Internet versión 6 y GMPV, el protocolo de descubrimiento de vecinos NLP, los mensajes Neighbor Solicitation NS y Neighbor Advertisement y por último, el término de envenenamiento o suplantación de vecinos.

En primer lugar, hemos aprendido que ICMPV desempeña un papel fundamental en la administración y en el mantenimiento de las redes IPV.

Hemos visto cómo es el responsable de enviar mensajes de control y también de error y que por supuesto, es crucial para el funcionamiento adecuado del NDP.

En cuanto al NDP, hemos comprendido que es una parte integral de IPV y facilita funciones clave como es el descubrimiento de vecinos, la resolución de direcciones y la detección de duplicados.

Estas funciones son esenciales para la configuración y el mantenimiento de las redes IPV, y esto es posible gracias a los mensajes NS y NA.

Los mensajes NS se utilizan para solicitar la dirección capa 2 de un nodo en la misma red local, mientras que los NA se utilizan para responder a estas solicitudes y también para anunciar la dirección de capa 2 de un nodo.

Por último, hemos hablado del envenenamiento de vecinos, que básicamente es una técnica de ataque que va a permitir suplantar estos nodos legítimos simplemente enviando por ellos mismos esta serie de mensajes NS y NA.

Y con esto llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.