ReTEC

Revista Electrónica de Tecnología, Educación y Ciencia
ISSN: 2953-5654
http://retec.unsa.edu.ar
Universidad Nacional de Salta

Protocolo ICMPv6: implicancias técnicas del filtrado

Ernesto Sánchez[1 2], Henri Alves de Godoy[3], Daniel Arias Figueroa[1]

[1]C.I.D.I.A. – Centro de Investigación y Desarrollo en Informática Aplicada
[2]Facultad de Ingeniería – Universidad Católica de Salta
[3]Universidade Estadual de Campinas (UNICAMP, Brasil)
{ esanchez , daaf }@cidia.unsa.edu.ar

Revista Electrónica de Tecnología, Educación y Ciencia,

Volumen 1, Número 3, pág. 55-59, jun, 2026. ISSN: 2953-5654

Disponible en http://retec.unsa.edu.ar/

Protocolo ICMPv6: implicancias técnicas del filtrado

Ernesto Sánchez[1 2], Henri Alves de Godoy[3], Daniel Arias Figueroa[1]

[1]C.I.D.I.A. – Centro de Investigación y Desarrollo en Informática Aplicada
[2]Facultad de Ingeniería – Universidad Católica de Salta
[3]Universidade Estadual de Campinas (UNICAMP, Brasil)
{ esanchez , daaf }@cidia.unsa.edu.ar

Resumen: El presente trabajo analiza las implicancias técnicas y operativas del filtrado del protocolo ICMPv6 en redes modernas basadas en IPv6, desmitificando prácticas heredadas del entorno IPv4 que aún persisten en la actualidad. Históricamente, el bloqueo generalizado de ICMP surgió como una respuesta a vulnerabilidades y ataques en redes IPv4; sin embargo, este enfoque resulta inadecuado en el contexto de IPv6, donde ICMPv6 cumple un rol estructural esencial en el funcionamiento de la red. En este estudio se examinan las diferencias fundamentales entre ICMPv4 e ICMPv6, destacando cómo este último integra funciones críticas como el descubrimiento de vecinos mediante el protocolo NDP, la autoconfiguración de direcciones (SLAAC) y la detección del tamaño máximo de transmisión (MTU). A diferencia de IPv4, donde ciertos mecanismos eran auxiliares, en IPv6 estos procesos dependen directamente de ICMPv6, lo que convierte su correcto tratamiento en un aspecto clave para la estabilidad y operatividad de la red. Desde una perspectiva experimental, se diseñó e implementó un entorno de pruebas basado en Containerlab que simula una red corporativa, permitiendo evaluar distintos escenarios de ataque y políticas de filtrado. Para ello, se consideraron lineamientos establecidos en diversas RFCs, particularmente aquellas relacionadas con modelos de confianza en Neighbor Discovery y recomendaciones de filtrado seguro. A través del uso de herramientas especializadas, como el toolkit THC IPv6, se analizaron vectores de ataque y su impacto en la infraestructura. Los resultados obtenidos evidencian que el bloqueo indiscriminado de ICMPv6 genera fallas críticas, tales como la interrupción de procesos de autoconfiguración, errores en la resolución de direcciones, problemas en la detección de MTU y dificultades en la identificación de direcciones duplicadas. En contraste, la implementación de mecanismos de filtrado selectivo —basados en tipos y códigos específicos de mensajes— junto con técnicas como RA Guard, ND Snooping, DHCPv6 Guard y limitación de tasa, permite mitigar amenazas sin comprometer la funcionalidad de la red.

Palabras clave: ICMPv6; IPv6; filtrado de tráfico; seguridad en redes; Neighbor Discovery Protocol (NDP); SLAAC; firewall; Containerlab; análisis de tráfico; mitigación de ataques.

1. Introducción

El protocolo ICMP (Internet Control Message Protocol) se definió en la RFC 792 (1981) como un mecanismo fundamental para que los dispositivos de red pudieran comunicar errores, anunciar problemas de conectividad y permitir el diagnóstico de la red. Fue creado junto con IPv4 para dar soporte durante la transmisión de los paquetes, los cuales viajan sin garantía de entrega en la capa de red. Se utiliza, por ejemplo, para notificar cuando un host no está disponible, para informar cuando se ha excedido un TTL y para indicar problemas de fragmentación.

Una de las herramientas más usadas y de fácil manejo incluso para usuarios no experto son los comandos ping (Echo Request/Reply) y traceroute (Time Exceeded), que utilizan directamente el protocolo ICMP. Estas herramientas son muy usadas en nuestra vida cotidiana y son indispensables para verificar la conectividad de forma rápida y sencilla.

Con el crecimiento de Internet y la posibilidad de navegar por la Web (antes limitada a las universidades y los centros de investigación) y el surgimiento de los pequeños proveedores de acceso a Internet (ISP) regionales a mediados de los 90, cada usuario recibía una dirección IPv4 pública en su hogar. Los usuarios residenciales todavía no conocían NAT y tenían una conexión directa de extremo a extremo, sin traducción de direcciones y sin que una misma IP fuera compartida por muchas personas, como sucede hoy.

En esa época también comenzaban a surgir los ataques de denegación de servicio (Denial of Service o DoS), que explotaban dispositivos conectados, como los smurf attacks, con los que se enviaban paquetes ICMP Echo Request a direcciones broadcast. Este tipo de ataques se conocen como ataques de amplificación y su objetivo es paralizar una red local.

Otro incidente importante y con repercusión histórica fue el “ping de la muerte”, que explotaba fallas en la implementación del protocolo IP en diversos sistemas operativos, especialmente Windows 95, y el atacante creaba un paquete ICMP Echo Request de un tamaño mayor al permitido por el estándar IP (65.535 bytes).

Con el tiempo, se creó un movimiento que sostenía que “hacer ping es peligroso”. En este contexto, muchos comenzaron a aplicar un bloqueo generalizado de ICMP, algo que durante muchos años se consideró una buena práctica de seguridad.

Sin embargo, esta decisión se basó más en el pánico que en un análisis técnico. Como consecuencia de ello, ahora es difícil distinguir entre una falla de conectividad y el filtrado del tráfico ICMP, creándose así redes invisibles para dificultar el mapeo de la red interna, donde el diagnóstico se ha vuelto ineficiente.

Muchos scripts de firewall (iptables, ipchains) y tutoriales empezaron a promover la práctica de bloquear por completo el protocolo ICMP, sin explicar las consecuencias técnicas. La influencia de esta cultura fue tan grande que hasta el día de hoy, 30 años después, todavía hay muchos que bloquean completamente ICMP en sus redes, creando así una falsa sensación de seguridad.

2. ICMPv6: más que un simple reemplazo para el ICMP de IPv4

En IPv4, el descubrimiento de vecinos en una red local se realizaba mediante el protocolo ARP (Address Resolution Protocol) definido en la RFC 826. Este protocolo funciona con mensajes broadcast, es decir, mensajes que se envían a todos los dispositivos de la red.

Contrariamente a la creencia popular, IPv6 no es solo una versión ampliada de IPv4. Por el contrario, reestructura muchos de los principios de la comunicación en red, y ahora incluye el protocolo ICMPv6, al que se le han agregado nuevas funciones, es más robusto, y ya no es solo un reemplazo de su predecesor, ICMP. ICMPv6 ahora incluye:

- El descubrimiento de vecinos y enrutadores: a través de NDP (RFC 4861).
- Autoconfiguración de direcciones: a través de SLAAC (RFC 4862).
- Descubrimiento de MTU: esencial ya que IPv6 no permite la fragmentación intermedia.

Con IPv6 se eliminó por completo el uso de broadcast, que se sustituyó por un modelo mucho más controlado y eficiente basado en multicast.

El Neighbor Discovery Protocol (NDP), definido en la RFC 4861, reemplaza las funciones de ARP y va más allá, ya que ofrece descubrimiento de vecinos y enrutadores, así como detección de direcciones duplicadas (DAD).

Los mensajes de NDP se transportan dentro de ICMPv6 y utilizan direcciones multicast específicas (prefijo FF02::/16), optimizando el tráfico de descubrimiento en la red. Esto evita los problemas de transmisión al segmentar la comunicación solamente entre los dispositivos interesados.

Estos enfoques reducen drásticamente la carga de la red y permiten implementaciones más escalables y seguras, algo que beneficia a los dispositivos con recursos limitados (como los sensores de IoT) y a entornos como centros de datos y redes empresariales.

3. Impactos del bloqueo de ICMPv6

En IPv4, incluso sabiendo que no era una práctica correcta, el impacto del bloqueo de ICMP no era tan alto. Por el contrario, bloquear completamente ICMPv6 puede provocar una serie de fallas y problemas en la red, como por ejemplo:

- Interrupción de SLAAC: los hosts no reciben automáticamente el prefijo de red
- Falla de NDP: sin esto, no hay resolución de direcciones MAC
- Imposibilidad de detectar la MTU adecuada
- Error en la detección de direcciones duplicadas (DAD)

En entornos corporativos o académicos con redes de doble pila, las fallas intermitentes y difíciles de diagnosticar pueden deberse únicamente al bloqueo inadecuado de ICMPv6.

4. Pruebas de filtrado de ICMPv6 con Containerlab

Con el propósito de analizar el comportamiento de ataques basados en mensajes ICMPv6, se creó una topología de red basada en la herramienta Containerlab y considerando las siguientes RFCs:

La RFC 3756, “IPv6 Neighbor Discovery (ND) Trust Models and Threats“, donde se describen tres entornos de red a considerar en función de tres niveles de confianza.

La RFC 4890 proporciona una base sólida para un filtrado seguro y funcional de ICMPv6. En lugar de bloquear todo ICMPv6, recomienda un enfoque basado en el conocimiento de los tipos y códigos de los mensajes. Por ejemplo:

- Type 133: Router Solicitation
- Type 134: Router Advertisement
- Type 135/136: Neighbor Solicitation/Advertisement
- Type 2: Packet Too Big
- Type 1: Destination Unreachable

El laboratorio de pruebas propuesto simula un entorno de red corporativa, integrando las herramientas THC IPv6 del kit de herramientas IPv6 para simular escenarios de ataque y dispositivos de red que funcionan con Nokia SRL Linux y Aruba-CX OS, lo que permitió configurar los mecanismos de protección que se enumeran a continuación.

Uso de mecanismos de protección especializados:

- RA Guard: bloquea mensajes RA maliciosos en puertos no autorizados
- ND Snooping: inspecciona mensajes NS/NA para prevenir spoofing
- DHCPv6 Guard: detecta y bloquea servidores DHCPv6 falsos
- ACL basadas en tipo/código/puerto de VLAN
- Rate-limiting inteligente: evita los ataques por inundación sin bloquear la funcionalidad

Las pruebas realizadas permitieron analizar diferentes vectores de ataque y determinar una combinación eficiente de los mecanismos antes descritos para un correcto filtrado de los mensajes ICMPv6.

5. Consideraciones finales

El bloqueo de ICMPv4 fue una reacción histórica para proporcionar seguridad de forma provisoria en un momento en que Internet empezaba a llegar a los hogares. Con el paso del tiempo y los hábitos adquiridos, mantener la misma lógica con ICMPv6 es un error tanto técnico como operativo. Más que nunca, debemos basar la seguridad en el conocimiento de buenas prácticas con fundamento técnico, no en el miedo.

En base a los resultados obtenidos, Containerlab demostró ser una herramienta versátil y 100% funcional para la creación de laboratorios de pruebas controlados donde simular ataques sin comprometer entornos reales. Además, la captura y el análisis del tráfico de red es fundamental para la inspección de campos de encabezado y la posterior definición de reglas de filtrado seguras sin entorpecer el normal funcionamiento de ICMPv6.

En este artículo se resume lo presentado en el Foro Técnico de LACNIC 43. Observamos que hoy en día ICMPv6 es fundamental y que está presente en las redes de computadoras, donde la seguridad ya no se basa en el concepto de bloqueos, sino en el monitoreo y el filtrado inteligente.

Referencias

1. [RFC 792] – Internet Control Message Protocol
2. [RFC 4443] – ICMPv6
3. [RFC 4861] – Neighbor Discovery for IPv6
4. [RFC 4890] – Filtering Recommendations.
5. [RFC 3756] – IPv6 Neighbor Discovery (ND) Trust Models and Threats
6. [RFC 8200] – IPv6 Specification
7. [RFC 4862] – IPv6 Stateless Address Autoconfiguration
8. Documentos y mejores prácticas operativas del Grupo de Trabajo sobre v6ops
9. ContainerLab – https://containerlab.dev/
10. Tutorial y laboratorios – https://github.com/ernestosanchezv/icmpv6filter