

Tema 10-IPv6

Las limitaciones de IPv4 se deben principalmente a la estructura de direccionamiento de 32 bits, que proporciona un espacio de direcciones relativamente pequeño en comparación con el tamaño de Internet y el creciente número de dispositivos conectados a la red. Algunas de las limitaciones más significativas son las siguientes:

1. **Pocas direcciones:** La estructura de dos niveles de IPv4, con identificadores de red y de host, limita el número de direcciones disponibles a unas 4000 millones. Esto se debe a que, al reservar un identificador de red, se están reservando todos los identificadores de host asociados a esa red. Con el crecimiento exponencial de Internet y la proliferación de nuevas tecnologías (como dispositivos móviles, tablets y televisores inteligentes), la demanda de direcciones IP ha superado con creces la oferta disponible.
2. **Saturación del espacio de direcciones:** La limitación del espacio de direcciones en IPv4 ha llevado a una saturación del espacio de direcciones, lo que ha limitado el crecimiento de Internet. Además, el enrutamiento ineficiente debido a la necesidad de mantener tablas de enrutamiento muy grandes en la red troncal ha provocado tiempos de respuesta lentos. Para abordar este problema, se han utilizado técnicas como NAT (Network Address Translation) para reutilizar direcciones IP privadas y compartir una dirección pública única.
3. **Soporte inadecuado para aplicaciones con restricciones de calidad de servicio (QoS):** IPv4 no proporciona garantías de ancho de banda, tiempo de respuesta ni seguridad para aplicaciones con restricciones de QoS. Esto significa que no hay manera de garantizar que las aplicaciones críticas para la empresa, como las de voz y video, tengan el ancho de banda y la prioridad necesarios para una comunicación efectiva.
4. **Falta de seguridad en la capa de red:** IPv4 no fue diseñado con seguridad en mente. Las direcciones IP se pueden falsificar fácilmente, lo que puede dar lugar a ataques de denegación de servicio y otros problemas de seguridad. Para abordar este problema, se ha desarrollado el protocolo IPsec para proporcionar autenticación, confidencialidad e integridad en la capa de red. Sin embargo, la seguridad también se puede proporcionar en niveles superiores, como TLS (Transport Layer Security), que se utiliza comúnmente en aplicaciones de comercio electrónico y banca en línea.