VNNIC
Internet for all

GIẢI PHÁP CHUYỂN TIẾP BẮT BUỘC, BẢO ĐẢM AN TOÀN TRONG TRIỂN KHAI IPv6-ONLY

TP. Hồ Chí Minh, 19/6/2026

Nguyễn Văn Trí, VNNIC

NỘI DUNG

- Bối cảnh, xu hướng
- Vì sao DNS64/NAT64 là "bắt buộc" ?
- Các hạn chế của DNS64/NAT64
- Cơ chế hoạt động của DNS64/NAT64
- Giải pháp ATBM cho DNS64/NAT64
- Kết luận

BỐI CẢNH & XU HƯỚNG

KHÁI QUÁT HIỆN TRẠNG CHUYỂN ĐỔI IPV6 THẾ GIỚI

> 51%
mức độ triển khai IPv6 trong các doanh nghiệp & Chính phủ

~ 48%
Traffic IPv6 toàn cầu

> 95%
Jio Mobile IPv6-Only

> 90%
T-Mobile US IPv6 subscribers

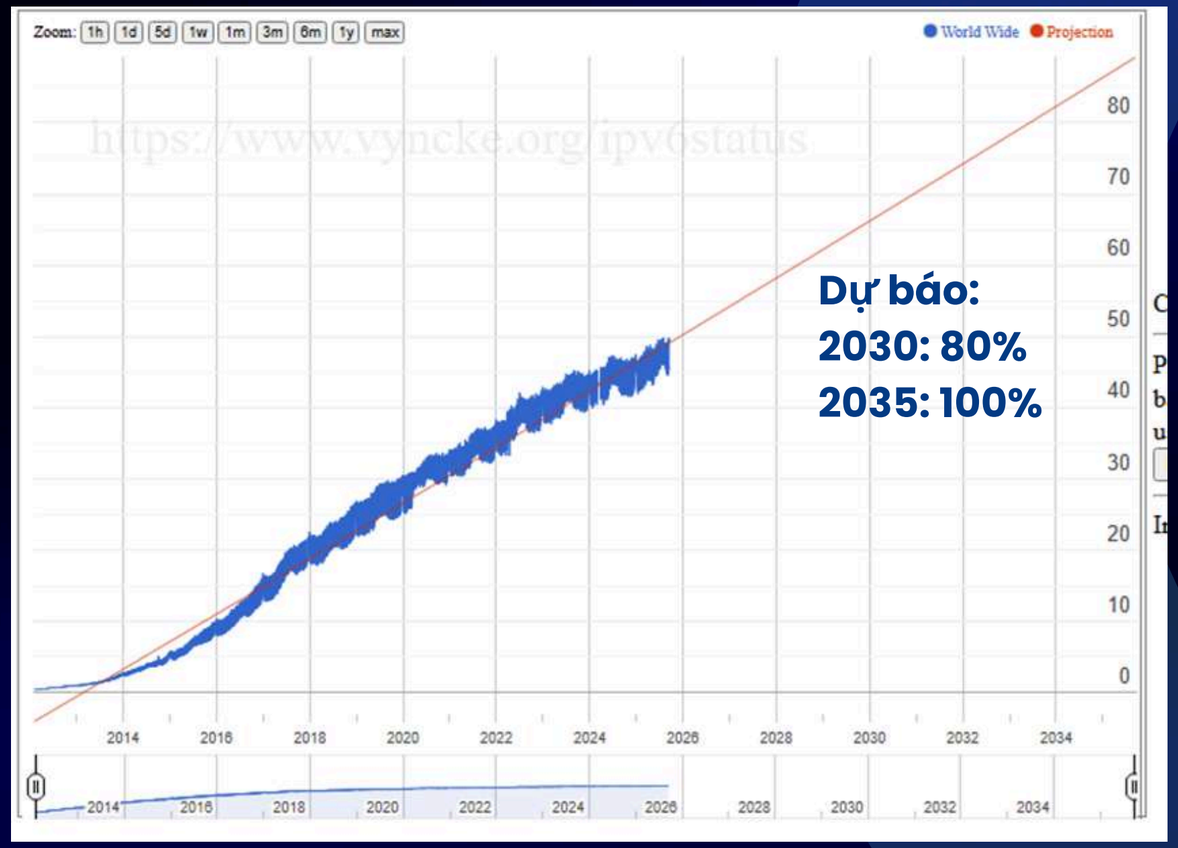
~ 80%
Pháp - dẫn đầu EU

- **IPv6 Forum (11/2025):** "Dual-stack là giải pháp tạm thời với nhiều chi phí và thời gian duy trì IPv4/NAT. IPv6-Only là tầm nhìn cho Internet sản xuất thực sự, phục vụ AI, 6G, Blockchain, P2P IoT, Chuỗi cung ứng, Internet Công nghiệp."
- **Xu hướng 2025:** Google, Microsoft, Apple, Meta, Amazon, Alibaba, Tencent, Huawei đều đang triển khai IPv6-Only nội bộ với DNS64/NAT64 làm cơ chế chuyển tiếp.

CHUYỂN ĐỔI IPv6, TRIỂN KHAI IPv6 ONLY TRÊN THẾ GIỚI

TT	Quốc gia/Nền kinh tế	Tỷ lệ IPv6
1	Ấn Độ	80.00%
2	Pháp	79.93%
3	Ả Rập Xê Út	70.86%
4	Malaysia	70.64%
5	Bỉ	68.84%
6	Đức	68.08%
7	Việt Nam	67.68%
8	Israel	62.73%
9	Uruquay	61.41%
10	Nhật Bản	59.12%

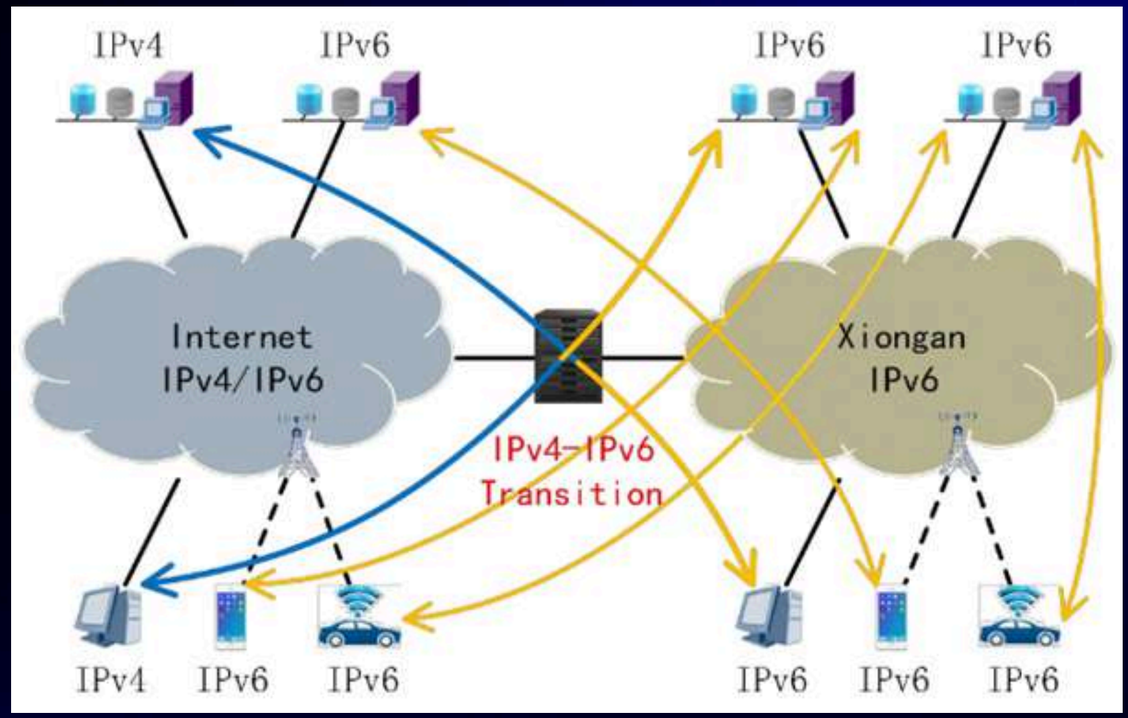
Top 10 quốc gia về triển khai IPv6 (nguồn APNIC)



Dự báo chuyển đổi IPv6 thế giới (nguồn Google và vyncke.org)

KINH NGHIỆM QUỐC TẾ

- Để triển khai IPv6 hiệu quả, các nước có nhiều chính sách, định hướng, yêu cầu thúc đẩy IPv6, IPv6 only (Trung Quốc năm 2021, Mỹ năm 2020/2024, Malaysia năm 2025, Séc năm 2024, Đức năm 2025 ...).
- Các doanh nghiệp lớn toàn cầu, đã bắt đầu triển khai IPv6 only từ sớm (Facebook từ năm 2017, T-mobile từ 2014, China Telecom từ 2020, Telstra từ 2020, AWS, Microsoft đề đã triển khai cho các trung tâm dữ liệu...); tuy nhiên, chưa toàn diện, chủyếu ở một phạm vi nhất định.
- IPv6 only là đích đến chung



City of the future Xiong'an

- Xâydựng thành phốmới Xiongan – Hùng An (2017) (100 km2, 1.3 triệu dân)
- Triển khai 198,000 sensors/km2, mục tiêu 1 triệu sensors/km2.
- Hạ tầng IPv6-only.

CHUYỂN ĐỔI IPv6 TẠI VIỆT NAM

TT	AS Name	Tỷ lệ IPv6
1	VNNIC-VN	100.00%
2	BNNMT-VN	66.20%
3	DSP-VN	52.54%

- Khối CQNN tiêu biểu

TT	AS Name	Tỷ lệ IPv6
1	MOBIFONE-VN	76.14%
2	FPT-VN	67.48%
3	VIETEL-VN	65.62%
4	VNPT-VN	53.65%

- Các doanh nghiệp lớn

Kết quả tiêu biểu:

- Tuoitre.vn, zalo.me, sctv.vn ... chuyển đổi IPv6
- Biên tập sách IPv6, sách DNS
- Thí điểm IPv6 only, nhân rộng mô hình IPv6 only
- Triển khai nền tảng DNS64, Đào tạo IPv6 only

- Tuoitre.vn, zalo.me, sctv.vn ... chuyển đổi IPv6
- Biên tập sách IPv6, sách DNS
- Thí điểm IPv6 only, nhân rộng mô hình IPv6 only
- Triển khai nền tảng DNS64, Đào tạo IPv6 only

TẠI SAO DNS64/NAT64 LÀ "BẮT BUỘC"

CÁC CƠ CHẾ CHUYỂN TIẾP IPv6

Dual-Stack

- Vẫn tiêu thụ IPv4 — không giải bài toán cạn kiệt. Chỉ là trạng thái trung gian. Không dùng khi đã IPv6-Only.

Tunnel 6in4/DS-Lite

- Không dịch địa chỉ. Vẫn cần IPv4 ở một đầu. Không phục vụ client IPv6-Only thuần túy.

SIIT / IVI / Stateless

- Yêu cầu ánh xạ địa chỉ tĩnh 1:1. Không scale cho hàng triệu client động. Cần IPv4 public cho mỗi client.

Proxy / ALG tầng App

- Chỉ xử lý một số giao thức. Phải cấu hình từng ứng dụng. Không trong suốt. Không phủ toàn bộ traffic.

MAP-T / MAP-E

- Yêu cầu CPE đặc biệt hỗ trợ MAP. Không phục vụ client thông thường. Rất phức tạp khi cấu hình.

DNS64/NAT64 & CÁC CƠ CHẾ CHUYỂN TIẾP IPv6

Cơ chế	Cần IPv4 client?	Trong suốt client/server?	Scale động?	Không phụ thuộc App?	Hoạt động khi IPv6-Only?	Đánh giá
Dual-Stack	✅ Có	✅ Có	✅ Có	✅ Có	❌ Không	Tạm thời
Tunnel 6in4/DS-Lite	✅ Có	✅ Có	✅ Có	✅ Có	❌ Không	Không phù hợp
SIIT / IVI	❌ Không	✅ Có	❌ 1:1 only	✅ Có	✅ Có	Không scale
Proxy / ALG	❌ Không	❌ Không	⚠️ Hạn chế	❌ Chỉ HTTP...	✅ Có	Không toàn diện
MAP-T / MAP-E	❌ Không	⚠️ Cần CPE	✅ Có	✅ Có	✅ Có	Cần CPE đặc biệt
DNS64 + NAT64 ★	❌ **Không**	✅ **Hoàn toàn**	✅ **Stateful**	✅ **Có**	✅ **Có**	✅ **KHUYẾN NGHỊ**

- DNS64+NAT64: Là cơ chế DUY NHẤT không cần IPv4 ở client, trong suốt hoàn toàn, scale stateful, hoạt động ở tầng mạng, hoạt động tốt khi đã IPv6-Only.

4 LÝ DO KỸ THUẬT KHIẾN DNS64/NAT64 LÀ BẮT BUỘC

①Trong suốt hoàn toàn

- Client IPv6-Only KHÔNG biết NAT64 đang tồn tại. Server IPv4-Only KHÔNG biết client đang dùng IPv6. Không một dòng code ứng dụng nào phải thay đổi. Đây là điều không có cơ chế nào khác đạt được mà không cần thay đổi phía client hoặc server.

②Can thiệp tại đúng điểm — tầng DNS

- DNS là lớp mà 99% kết nối đều đi qua. DNS64 hoạt động ngay tại đây — intercepting AAAA query và synthesizing địa chỉ — mà không cần chạm vào ứng dụng. Đây là điểm kiểm soát tự nhiên nhất và hiệu quả nhất.

4 LÝ DO KỸ THUẬT KHIẾN DNS64/NAT64 LÀ BẮT BUỘC

③Scale được với tài nguyên IPv4 tối thiểu

- Stateful NAT64 cho phép hàng triệu client IPv6 chia sẻ một pool nhỏ địa chỉ IPv4 public thông qua port multiplexing (mỗi IP = ~64K ports).
- Reliance Jio: 500M+ subscriber IPv6-only, chỉ cần vài ngàn IPv4 public.

④Đã chuẩn hóa và kiểm chứng thực tế

- RFC 6146 (NAT64) + RFC 6147 (DNS64) từ năm 2011 — 14 năm ổn định.
- Triển khai thực tế:
  - T-Mobile US
  - Reliance Jio
  - Apple
  - Google
  - VNNIC.

AI ĐANG TRIỂN KHAI DNS64/NAT64? — BỨC TRANH TOÀN CẦU

US Hoa Kỳ	EU Châu Âu	CN Trung Quốc	JP Nhật Bản	SA Ả Rập Saudi
Doanh nghiệp	Doanh nghiệp	Doanh nghiệp	Doanh nghiệp	Doanh nghiệp
Google, Microsoft, Apple, Meta, Amazon	DT, Orange, SAP, Bosch, Siemens	Alibaba, Tencent, Huawei, Baidu	NTT Docomo, KDDI, SoftBank, Rakuten	stc, Mobily, Zain, Saudi Aramco
Chính phủ	Chính phủ	Chính phủ	Chính phủ	Chính phủ
DoD, GSA, NIST, OMB M-21-07	EC, BSI, GÉANT, ENISA	MIIT, CAC, CERNET2	MIC, SINET, Chính quyền địa phương	CST, NCA, NEOM

CÁC HẠN CHẾ & THÁCH THỨC CỦA DNS64/NAT64

THÁCH THỨC — DNS GAP VÀ IPV4 LITERAL

① DNS Gap - thiếu bản ghi AAAA

- Vấn đề:
  - Client IPv6-only query AAAA record cho domain X. Nếu domain X chỉ có A record → DNS trả NXDOMAIN → kết nối thất bại. Không phải lỗi network mà là lỗi DNS.
  - → Client IPv6-only không thể kết nối
- Hậu quả:
  - User experience kém — nhiều website không truy cập được
  - Enterprise app legacy thường thiếu AAAA
  - IoT device firmware server thường IPv4-only
- Giải pháp:
  - DNS64 tổng hợp AAAA giả từ A record

② Hardcoded IPv4 Literal — DNS64 bị bypass

- Vấn đề:
  - Ứng dụng dùng địa chỉ IPv4 (không qua DNS): DNS64 không thể can thiệp. Kết nối thất bại hoàn toàn trên mạng IPv6-Only.
- Các trường hợp phổ biến:
  - VoIP/SIP app hardcode SIP server IP
  - Game client hardcode game server IP
  - IoT firmware hardcode update server
  - Legacy enterprise app dùng IP thay hostname
- Hậu quả:
  - App crash hoặc feature không hoạt động
  - Khó debug vì không có DNS trace
- Giải pháp:
  - 464XLAT (CLAT phía client)

THÁCH THỨC — DNSSEC, HAIRPIN, ALG

③ DNSSEC vs DNS64 Conflict

- DNS64 tạo AAAA record tổng hợp không có RRSIG. DNSSEC-validating resolver sẽ SERVFAIL.
- Giải pháp:
  - RFC 7050: client tự detect DNS64, tắt validation
  - Tắt DNSSEC cho DNS64 domain (compromise)
  - Dùng 464XLAT (bypass DNS64 hoàn toàn)

④ NAT64 Hairpinning

- Client A (IPv6-only) muốn nói chuyện với Server B (IPv6-only cùng mạng) nhưng qua địa chỉ NAT64 tổng hợp → gói đi vòng qua NAT64 gateway không cần thiết → latency tăng, BIB tốn tài nguyên.
- Giải pháp:
  - Split-DNS: trả AAAA thật cho host nội bộ
  - Hairpin routing support trên NAT64 device
  - DNS Views: phân biệt internal/external clients

⑤ Application Layer Gateway (ALG)

- FTP Active Mode, SIP, H.323, STUN nhúng địa chỉ IPv4 trong payload → NAT64 phải rewrite payload (ALG). Phức tạp, tốn CPU, không phải tất cả vendor hỗ trợ đầy đủ.
- Giải pháp:
  - Dùng Passive FTP thay Active
  - SBC (Session Border Controller) cho VoIP
  - STUN/TURN server hỗ trợ IPv6
  - WebRTC: ICE candidate gathering đúng IPv6

464XLAT – GIẢI PHÁP HỖ TRỢ

464XLAT hỗ trợ (RFC 6877)

IPv4 App (Hardcode IP)

CLAT (on device)

IPv6 Network

PLAT (= NAT64)

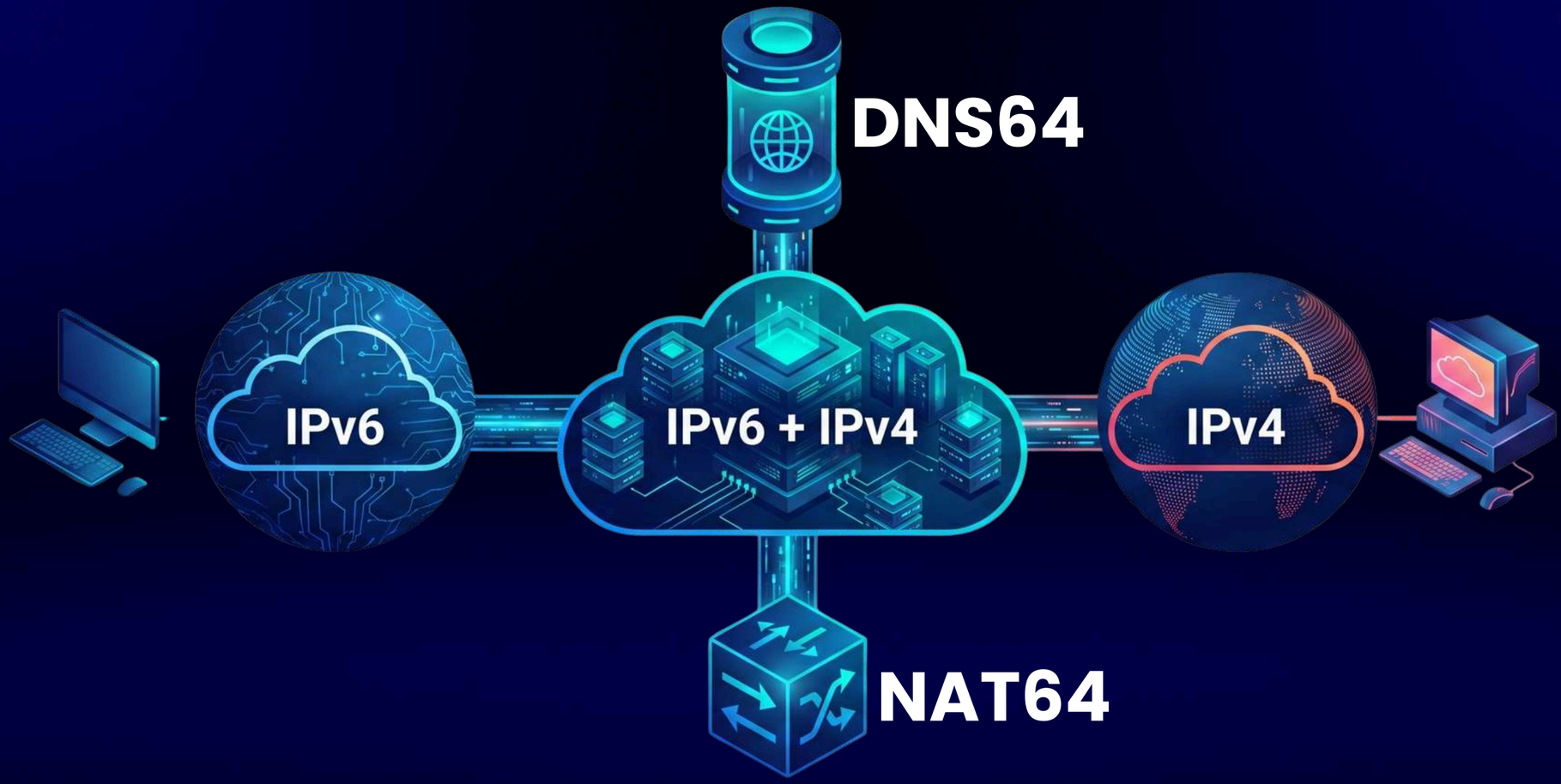
- 464XLAT giải quyết: IPv4 literal, legacy apps, IPv4-only socket API — mà không cần sửa app hay server.
- CLAT tích hợp: Android 4.3+, iOS 9+, Windows 11, Linux.

Mối quan hệ DNS64/NAT64 & 464XLAT

- DNS64/NAT64 = LÕI: Phục vụ 95%+ traffic. Không cần thay đổi ở phía client hay server.
- 464XLAT = BỔ TRỢ: Xử lý 5% còn lại — ứng dụng legacy, IPv4 literal. CLAT chạy trên client, PLAT chính là NAT64 đã có sẵn.

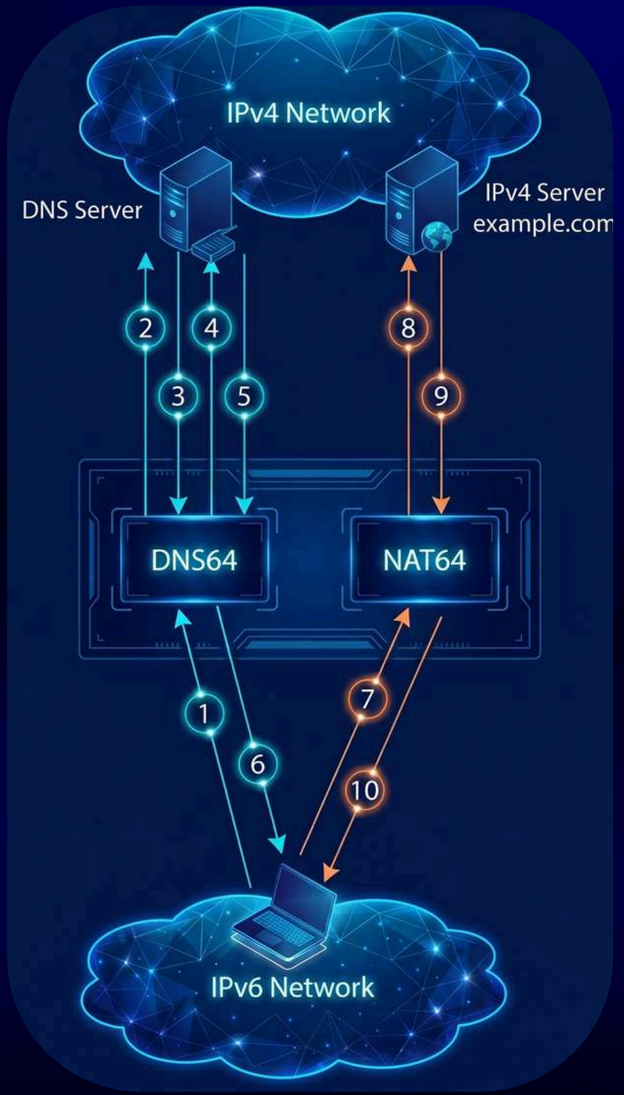
CƠ CHẾ HOẠT ĐỘNG DNS64/NAT64

MÔ HÌNH KIẾN TRÚC DNS64/NAT64



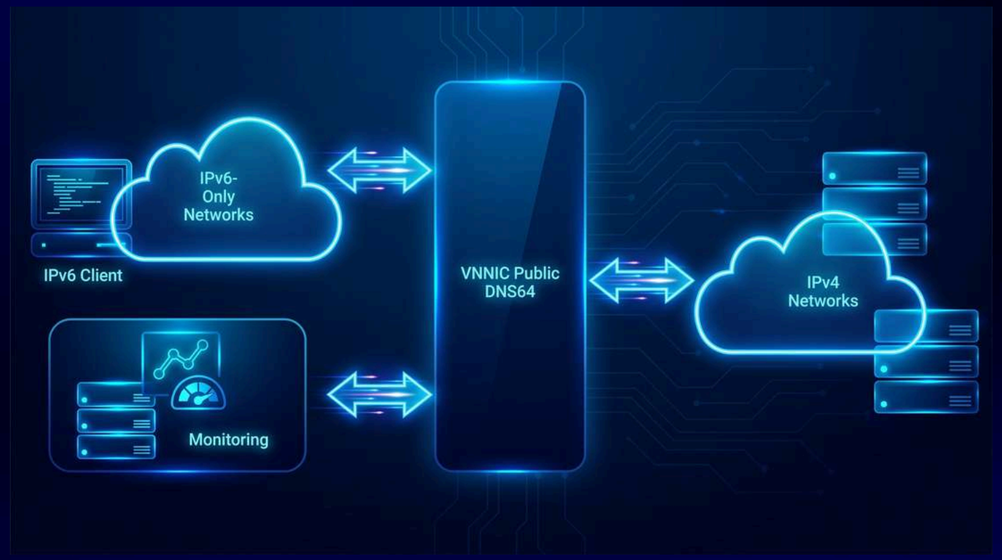
HOẠT ĐỘNG CỦA DNS64/NAT64

- IPv6 Client gửi yêu cầu tìm kiếm thông tin tên miền example.com (khai báo trỏ tới máy chủ IPv4 server).
- DNS64 thực hiện tìm kiếm bản thông tin bản ghi AAAA cho địa chỉ IPv6 của máy chủ.
- DNS Server trả lời bằng 1 thông báo lỗi (hoặc câu trả lời trống, không có thông tin).
- DNS64 thực hiện tìm kiếm thông tin bảnghi A cho địa chỉ IPv4.
- DNS Server trả lời địa chỉ IPv4 của tên miền example.com.
- DNS64 trả về thông tin bảnghi AAAA từ việc tổ hợp địa chỉ IPv4 với 96 bit của IPv6 prefix đã cấu hình trước đó.
- IPv6 Client thiết lập kết nối tới địa chỉ IPv6 tương thích ở trên.
- NAT64 nhận dạng prefix và thực hiện biên dịch thành địa chỉ IPv4 trước khi gửi tới IPv4 Server
- IPv4 Server gửi thông tin trả lời theo quá trình tương tác IPv4 thông thường
- NAT64 thực hiện biên dịch ngược và gửi gói tin phản hồi về Client.



VNNIC PUBLIC DNS64

VNNIC Public DNS64



Monitoring DNS64 Traffic

Kết nối sử dụng DNS64 tại VIC2025

ATBM CHO DNS64/NAT64

CÁC MỐI ĐE DỌA CỦA DNS64/NAT64

CRITICAL | HIGH | MEDIUM

T1 — DNS64 Prefix Hijacking / Rogue DNS64

CRITICAL

RFC 6147 §8 · NSA IPv6 Guide 2023

Attacker dựng rogue DNS64 server, tổng hợp AAAA trỏ đến NAT64 độc hại → Man-in-the-Middle toàn bộ traffic IPv6-Only. Client không phân biệt được AAAA thật hay giả vì DNS64 hợp lệ không có chữ ký DNSSEC.

Impact: Intercepting toàn bộ kết nối. Credential theft, Phishing.

T2 — DNSSEC Bypass qua DNS64 Synthesis

CRITICAL

RFC 6147 §5 · IEEE Xplore · APNIC Blog 2016

AAAA record tổng hợp bởi DNS64 không có RRSIG hợp lệ. Clients dùng DNSSEC validation sẽ bị SERVFAIL → mất kết nối. Hoặc quản trị viên buộc phải tắt DNSSEC validation → mất toàn bộ bảo vệ DNS chữ ký.

Impact: ~1.7% DNSSEC zones bị break (APNIC). Chuỗi xác thực bị phá vỡ.

T3 — DoS/Resource Exhaustion trên NAT64

HIGH

RFC 6146 §1.2.3 · RFC 7269 §9

Attacker gửi hàng loạt connection requests để gây cạn kiệt tài nguyên: IPv4 address pool, Port resources (64K ports/IP), BIB/Session Table memory, CPU từ excessive translation. RFC 6146: không có rate-limit → NAT64 bị ngưng trệ.

Impact: Service outage toàn bộ mạng IPv6-Only. Denial of Service diện rộng.

T4 — IPv4 Prefix Spoofing qua NAT64

HIGH

RFC 6146 §9 · RFC 7269 §9

Kẻ tấn công craft IPv6 packet với dst=64:ff9b::/96 để bypass firewall IPv4. NAT64 dịch sang IPv4 → traffic độc hại đến được server IPv4 nội bộ. uRPF chưa được cấu hình → không detect spoofed source.

Impact: Bypass network security policy. Lateral movement vào IPv4 segment.

T5 — BIB/Session Table Manipulation

HIGH

RFC 6146 §3 · RFC 7269

NAT64 dùng Endpoint-Independent Filtering → IPv4 node có thể initiate session ngược vào IPv6 host nếu tồn tại stale BIB mapping. NAT Traversal techniques (ICE, STUN) tạo lỗ hổng allow inbound từ Internet IPv4.

Impact: Unauthorized inbound access vào mạng IPv6-Only qua stale BIB entry.

T6 — Mất truy vết, Gian lận & Tuân thủ policy

MEDIUM

RFC 6302 · RFC 7422 · Canadian CCS

BIB events (source IPv6, port, timestamp) → không thể truy vết khi xảy ra abuse, tấn công

Impact: Legal non-compliance. Không thể điều tra sự cố.

BIỆN PHÁP PHÒNG THỦ & HARDENING

Bảo mật DNS64

ACL nghiêm ngặt
RFC 8683 §4.1.5

Chỉ cho phép client tin cậy dùng DNS64 server. Từ chối query từ external/Internet. BIND9: allow-query { internal_nets; }

DNSSEC-aware DNS64 (vDNS64)
RFC 6147 §5.5

Triển khai vDNS64: resolver vừa làm DNS64 vừa validate DNSSEC. Dùng RFC 7050 để client tự detect Pref64 thay vì tắt validation hoàn toàn.

Loại trừ RFC1918 khỏi synthesis
RFC 8215

Không synthesize AAAA cho A record là địa chỉ private. Dùng 64:ff9b:1::/48 riêng cho private IPv4 nội bộ. Ngăn prefix confusion.

DNS Rate Limiting (RRL)
RFC 8683

Chống DNS amplification qua NAT64. BIND9: rate-limit { responses-per-second ...; }. Giảm nguy cơ DDoS reflection.

Giám sát synthetic AAAA ratio
RFC 8683

Alert khi tỉ lệ AAAA tổng hợp/thật tăng đột biến — dấu hiệu DNS64 bị dùng sai mục đích hoặc đang bị quét.

Bảo mật NAT64 Gateway

Block 64:ff9b::/96 inbound từ Internet
RFC 6146 §1.2.3

Rule firewall bắt buộc: không cho phép traffic từ Internet vào có dst trong 64:ff9b::/96. Ngăn attacker craft traffic bypass. NSA IPv6 Guide: critical control.

Address-Dependent Filtering (ADF)
RFC 6146 §5

Bật ADF thay Endpoint-Independent: chỉ cho phép IPv4 node reply về nếu IPv6 client đã initiate session đến đúng IPv4 node đó. Ngăn unsolicited inbound.

uRPF + Rate Limiting
RFC 7269 §9

Unicast RPF chống IP spoofing ở IPv6 side. Rate limit new session creation per source IPv6 (/64 hay /128). RFC 7269: uRPF là mandatory control cho NAT64-CGN.

SYN Proxy/Cookie
RFC 7269

Load balancer hoặc NAT64 cần SYN proxy để chống TCP SYN flood exhaustion. RFC 7269: mandatory cho NAT64-FE deployment. Cisco/F5/Jool hỗ trợ.

Fragment storm protection + MTU
RFC 6146 §5.1.3

Giới hạn fragment reassembly buffer. Set MTU=1260 byte và bật ICMP PTB. Ngăn memory exhaustion qua crafted fragments.

Logging, Giám sát & Tuân thủ

Bắt buộc log BIB events đầy đủ
RFC 6302

Log: {timestamp, protocol, IPv6-src:port, IPv4-mapped:port, IPv4-dst:port}. Yêu cầu bởi RFC 6302 và quy định chính sách policy. Không có log → không thể truy vết abuse hay tấn công.

Lưu trữ log ≥ 6 tháng
RFC 6302

GDPR/PCI-DSS yêu cầu audit trail. Dùng IPFIX/NetFlow v9 với NAT logging option. Tích hợp SIEM (Splunk/ELK). GDPR: anonymize PII khi không cần forensics.

Monitor pool exhaustion liên tục
RFC 8683

Alert khi IPv4 pool >80% ports sử dụng. BIB table utilization >80% → nguy cơ từ chối dịch vụ thực người dùng.

BIB stale entry cleanup định kỳ
RFC 6146 §4

TCP timeout=7200s, UDP=300s, ICMP=60s — tuân thủ RFC 6146. Cleanup stale entries. Ngăn attacker giữ stale BIB để duy trì inbound access lâu dài.

Audit định kỳ NSP/WKP prefix
RFC 8781

Xác minh Pref64 đang dùng không bị thay đổi trái phép. Kiểm tra RA PREF64 option (RFC 8781). Alert khi phát hiện rogue DNS64 server trong mạng.

Tham khảo: NSA IPv6 Guide 2023, CISA/Canadian CCS

KẾT LUẬN

- Hiện nay, cộng đồng sử dụng Internet đang phải đối mặt với sự cạn kiệt của nguồn tài nguyên địa chỉ IPv4, việc triển khai thế hệ địa chỉ mới IPv6 là một yêu cầu tất yếu. Cùng với đó là thách thức làm thế nào để quá trình chuyển sang IPv6 diễn ra ổn định, thuận lợi mà vẫn đảm bảo người sử dụng Internet gần như không nhận thấy sự thay đổi nào.
- Với giải pháp NAT64/DNS64, chúng ta hoàn toàn có thể xây dựng được hệ thống mạng mới IPv6 mà vẫn đảm bảo giao tiếp với hệ thống mạng IPv4 hiện tại một cách thuận tiện. Các nhà cung cấp dịch vụ có thể chạy máy chủ của họ trên IPv4 và NAT64/DNS64 sẽ giúp kết nối các máy chủ này với người dùng sử dụng IPv6.

THANK YOU !