2025 Call for Final Action:

Move to Native IPv6-Only

November 2025

We are crossing in the big countries 51% IPv6 penetration in the big enterprise and some government networks. Therefore, it is the right time for the IPv6 Forum to call for a worldwide full transition to IPv6-Only for any enterprise and government networks for a number of reasons especially that the dual stack deployment is just a temporary solution with a lot of expenses, cost and massive time spent maintaining IPv4/NAT while v6 Only is the vision for the new and real production Internet to cater for new technologies such as AI,6G, Blockchain, P2P IoT and all enterprise verticals (Supply chains, Industrial Internet) to name a few .

The IPv6-Only transition is supported by NAT64 and DNS64: NAT64 (Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers) and DNS64 (DNS extensions for NAT64) are key IPv6 transition mechanisms that enable IPv6-only clients to access IPv4-only resources. They are widely deployed in mobile networks for IPv6-only connectivity, often combined with 464XLAT for broader application compatibility, voir Annex at the end.

1 - The US

The adoption of NAT64 and DNS64 is a well-established best practice among leading US technology companies and within specific branches of the US government, particularly as a strategy for modernizing network infrastructure.

Here's a breakdown of the usage in both sectors.

US Companies Using NAT64/DNS64

Leading US tech companies are at the forefront of deploying NAT64/DNS64, primarily to streamline their internal corporate networks and cloud infrastructure.

1. Google:

· Usage: A pioneer and very public user. Google has extensively deployed IPv6-only corporate networks where employee devices rely solely on NAT64/DNS64 to reach the IPv4 internet.

· Public Service: They operate a public, well-documented DNS64 service at 2001:4860:4860::6464 and a corresponding NAT64 gateway, which anyone can use for testing or on their own IPv6-only networks.

2. Microsoft:

· Usage: Microsoft is a major user, especially within its Azure cloud platform. They offer NAT64/DNS64 as a service to their customers who deploy IPv6-only virtual networks and need to connect to IPv4 resources. Internally, it's a key technology for their own network modernization.

· Public Documentation: Microsoft's Azure documentation provides detailed guides on how to configure and use NAT64/DNS64 for outbound connectivity from IPv6-only subnets.

3. Apple:

· Usage: While not a direct user in the same way as a cloud provider, Apple has been a massive driver of NAT64/DNS64 adoption through its products. Since 2016, iOS and macOS devices include a "Happy Eyeballs" algorithm that is specifically optimized for networks that use NAT64/DNS64. This ensures a seamless user experience on IPv6-only cellular and Wi-Fi networks, pushing carriers and enterprises to deploy it.

4. Facebook (Meta) & Amazon:

· Usage: These companies operate some of the world's largest data centers. It is a standard and documented practice within such environments to use IPv6-only server fleets for new deployments, with NAT64/DNS64 providing controlled access to legacy IPv4 systems. This reduces complexity and operational cost.

Common Driver for Companies: The primary motivation is operational efficiency. Managing dual-stack (IPv4 and IPv6) is complex. By creating IPv6-only internal networks and using NAT64/DNS64 for the "last-mile" of connectivity to the IPv4 internet, they simplify their network architecture and reduce dependency on scarce IPv4 addresses.

US Government Use of NAT64/DNS64

The US government's adoption is driven by official mandates to transition to IPv6 to ensure future-proofness, security, and interoperability.

1. The Official Mandate:

· The Office of Management and Budget (OMB) mandates IPv6 adoption for all federal agencies. Key directives include:

· OMB Memorandum M-21-07: Requires that at least 80% of IP-capable assets on federal networks be IPv6-only or operating in dual-stack mode.

· This mandate explicitly encourages the use of IPv6-only networks where feasible, which inherently requires transition technologies like NAT64/DNS64.

2. Agencies Leading the Charge:

· Department of Defense (DoD): The DoD has a strong IPv6 policy and is actively transitioning. NAT64/DNS64 is a critical component for their "IPv6-Only" deployment model in certain secure and new installations, allowing them to maintain connectivity while modernizing.

· National Institute of Standards and Technology (NIST): NIST publishes extensive guidelines and standards for IPv6 deployment. Their publications explicitly cover and recommend NAT64 as a core transition technology.

· General Services Administration (GSA): As the manager of many federal networks and services, the GSA ensures that government-wide internet access points and cloud acquisitions support IPv6, creating the backbone upon which agencies can deploy NAT64/DNS64.

Common Driver for Government: The motivation is compliance, security, and long-term readiness. Adopting IPv6 (and by extension, technologies like NAT64) is seen as a strategic national interest to maintain technological leadership and secure network infrastructure against the exhaustion and limitations of IPv4.

Summary

Sector	Key Users	Primary motivation
US Companies	Google, Microsoft Apple, Meta Amazon	Operation Efficiency Cost Reduction Scalability
US Government	DoD, GSA all Federal Agencies (mandated by OMB)	Compliance, Security future-Proofing Interoperability

In conclusion, the use of NAT64 and DNS64 is a sign of a mature and forward-looking network strategy. It is heavily employed by leading US tech companies to run their own operations and is a mandated part of the US government's plan to modernize its digital infrastructure.

2 - Europe

The adoption of NAT64 and DNS64 in the European Union is widespread, driven by a combination of EU-wide policy, mobile network evolution, and corporate cloud strategy. The approach is more decentralized than in China or under a single US federal mandate, but it is nonetheless deeply embedded.

Here’s a breakdown of the usage within EU companies and government institutions.

EU Companies Using NAT64/DNS64

Leading European telecom operators and cloud-centric companies are the primary drivers, mirroring the global trend.

1. Deutsche Telekom (Germany), Orange (France), Telefónica (Spain), Vodafone (Group, with strong EU presence):

· Usage: This is the most significant and widespread use case. European mobile network operators (MNOs) are heavily deploying NAT64/DNS64 in their 4G/5G networks.

· Reason: The motivation is identical to carriers elsewhere: to efficiently handle the exhaustion of IPv4 addresses and simplify network architecture. They assign IPv6-only addresses to smartphones by default. When a user needs to access an IPv4-only app or website, the carrier's network seamlessly performs the translation using NAT64/DNS64. This is a standard practice across the industry.

2. SAP (Germany):

· Usage: As a global leader in enterprise software and cloud services, SAP almost certainly uses NAT64/DNS64 within its own data center and cloud infrastructure. This allows them to build new, scalable IPv6-only server environments while maintaining connectivity to legacy systems and the broader IPv4 internet.

· Evidence: SAP is a prominent member of the German IPv6 Council and actively promotes IPv6 adoption, which inherently includes knowledge and use of modern transition technologies.

3. Bosch (Germany) & Siemens (Germany):

· Usage: These industrial giants are key players in the Industrial Internet of Things (IIoT) and Industry 4.0. For their massive-scale IoT deployments, using IPv6-only sensors and devices is the only scalable long-term solution. NAT64/DNS64 provides these devices with controlled access to cloud management platforms that may still be on IPv4.

4. European Cloud Providers (e.g., OVHcloud in France, Deutsche Telekom's T-Systems):

· Usage: Like their American and Chinese counterparts, these providers offer NAT64/DNS64 as a service to customers who deploy IPv6-only virtual machines and containers, enabling them to reach the IPv4 internet.

EU Government and Public Sector Use

The deployment is driven by a top-down EU policy framework, though implementation varies by member state.

1. The European Commission:

· Role: The Commission sets the strategic direction. Its "European IPv6 Deployment Strategy" and the supporting EU Cyber Security Act encourage and sometimes mandate the adoption of IPv6 across member states' public administrations and critical infrastructure.

· Directive: While not mandating a specific technology like NAT64, the push for IPv6 readiness and the economic efficiency of IPv6-only networks makes NAT64/DNS64 a logical and recommended choice.

2. National Government Networks (e.g., Germany, France, Netherlands):

· Usage: Technologically advanced member states are actively integrating IPv6 into their government networks. For example:

· Germany's Federal Office for Information Security (BSI) provides detailed technical guidelines for IPv6 deployment, which include specifications for transition mechanisms like NAT64.

· The Dutch and French governments have had public IPv6 action plans for years.

· Implementation: As these governments modernize their internal networks and data centers, they are increasingly building new segments as IPv6-only and using NAT64/DNS64 for connectivity to legacy IPv4-based internal systems and the public IPv4 internet. This is a common strategy for reducing complexity and cost.

3. The GÉANT Network (The Pan-European Data Network for Research and Education):

· Who: The European counterpart to China's CERNET2.

· Usage: GÉANT and its associated National Research and Education Networks (NRENs) across Europe are global leaders in IPv6 deployment. They actively run IPv6-only pilot networks and testbeds for their users (universities, research institutes). In these environments, NAT64/DNS64 is an essential service that allows researchers to access the entire internet.

4. ENISA (The European Union Agency for Cybersecurity):

· Role: ENISA promotes IPv6 as a fundamental element of future-proof and secure internet infrastructure. Their reports and guidelines acknowledge and describe the

role of transition technologies, providing the justification for their use across the public and private sectors.

Summary

Sector	Key Users	Primary motivation
EU Companies	**Mobile Networ Operators DT, Orange, etc..** **Industrial IoT (Bosch, Siemens)** **Cloud/Software (SAP)**	Network Efficiency **IoT Scalability** **Data Center Modernization** Cost Reduction
EU Governments & Public	**Driven by EC Strategy** **Implemented by national Governments (DE, FR,..)** **Research Networks (GÉANT)**	**Policy Compliance,** **Operational Efficiency,** **Fostering Innovation,** **Maintaining Technological Competitiveness**

In conclusion, the use of NAT64 and DNS64 in the EU is mature and strategic. It is the backbone of modern mobile internet connectivity for hundreds of millions of users and a key enabler for the next generation of industrial and governmental digital infrastructure, all supported by a coherent, if federated, policy framework.

3 - China

The deployment of NAT64 and DNS64 in China is a critical component of the national strategy to lead in IPv6 adoption and build a "network powerhouse". While specific internal implementations are often not publicly detailed, we can identify key players and sectors based on public policy, industry trends, and technical evidence.

Here’s a breakdown of which Chinese companies and government entities are using or driving the adoption of NAT64 and DNS64.

Chinese Companies Using NAT64/DNS64

Leading Chinese tech giants, particularly in cloud computing, content delivery, and telecommunications, are the primary drivers.

1. Alibaba Cloud (Aliyun) & Tencent Cloud:

· Usage: As China's leading cloud providers, they offer NAT64/DNS64 as a core service to their customers. This allows businesses renting IPv6-only virtual private clouds (VPCs) or containers to seamlessly access the wider IPv4 internet and services.

· Evidence: Their product documentation includes guides on configuring IPv6 and enabling connectivity for IPv6-only instances, which inherently relies on translation technologies like NAT64.

2. Huawei:

· Usage: Huawei is a major enabler and user. They integrate NAT64/DNS64 capabilities directly into their networking equipment (routers, switches, firewalls) and carrier-grade solutions.

· Evidence: Their technical whitepapers and configuration guides for "IPv6 Transition" explicitly detail how to deploy stateful NAT64 and DNS64 on their platforms. Furthermore, they likely use it within their own extensive corporate network.

3. China's Three Major Telecom Operators:

· Who: China Mobile, China Telecom, and China Unicom.

· Usage: This is one of the most significant areas of deployment. The carriers are using NAT64/DNS64 in their mobile networks (4G/5G).

· Context: To conserve IPv4 addresses and simplify network architecture, many mobile carriers worldwide assign IPv6-only addresses to smartphones by default. When a user on such a network needs to access an IPv4-only website or app, the carrier's network performs the translation seamlessly using NAT64/DNS64. This provides a native IPv6 experience while maintaining full backward compatibility.

4. Baidu, Tencent, & ByteDance:

· Usage: Similar to their US counterparts, these internet giants use NAT64/DNS64 internally within their data centers. This allows them to build new server clusters as IPv6-only, which is more efficient and scalable than managing dual-stack. It's a standard practice for modern, large-scale data center operations.

Chinese Government and Public Sector Use

The driving force behind this adoption is a top-down, national strategic policy.

1. Central Cyberspace Affairs Commission / Cyberspace Administration of China (CAC):

· Role: The top-level body setting the strategic direction. While they don't implement the technology directly, they issue the policies and action plans that make NAT64/DNS64 deployment mandatory for government and commercial entities.

2. Ministry of Industry and Information Technology (MIIT):

· Role: This is the key implementing ministry. MIIT has launched multiple "IPv6 Deployment Special Action" plans that set aggressive targets for IPv6 traffic, user penetration, and network readiness.

· Directive: Their policies explicitly encourage moving beyond dual-stack to IPv6-only in many scenarios, which logically requires the deployment of transition technologies like NAT64/DNS64 across all sectors.

3. Government Networks and "Government Online Projects":

· Usage: As per the national mandate, all government websites and online services have been required to support IPv6. While many currently operate in dual-stack mode, the strategic direction is toward more efficient IPv6-native infrastructure. NAT64/DNS64 is a key technology enabling this transition for internal government networks that need to access legacy IPv4 systems.

4. The Education and Research Sector (CERNET2):

· Who: The China Education and Research Network 2.

· Usage: As previously discussed, CERNET2 is a canonical example. As the world's first large-scale pure IPv6 backbone, it relies entirely on transition technologies like NAT64/DNS64 to allow its researchers and students to access the global IPv4 internet.

Summary

Sector	Key Users	Primary motivation
Chinese Companies	Telecom Operators (Mobile, Telecom, Unicom Cloud Providers (Alibaba, Tencent) Tech Giants (Huawei, Baidu)	Efficiency, Scalability, Compliance with National Policy, Ena
China Governments & Public	Driven by MIIT and CAC mandates; implemented across government networks . and public sectors like education (CERNET) education (CERNET)	Chinese Government National Strate; Building a "Network Powerhouse," Fut Infrastructure

In conclusion, the use of NAT64 and DNS64 in China is widespread and strategic. It is not merely a technical workaround but a fundamental component of the country's plan to build a next-generation, scalable, and sovereign internet infrastructure. The deployment is most advanced in the mobile carrier networks, cloud computing services, and the education and research sector.

4 – Japan

The adoption of NAT64 and DNS64 in Japan follows a similar pattern to other technologically advanced regions, driven by mobile carrier needs, government IT modernization, and the strategic goals of leading tech companies.

Here's a breakdown of the key Japanese companies and government entities using or promoting NAT64/DNS64.

Japanese Companies Using NAT64/DNS64

The deployment is most prominent in the telecommunications and internet services sectors.

1. Major Mobile Network Operators (MNOs):
· Who: NTT Docomo, KDDI (au), SoftBank, and Rakuten Mobile.

· Usage: This is the most widespread and critical use case. Japanese mobile carriers, like their global counterparts, are heavily deploying NAT64/DNS64 in their 4G LTE and 5G networks.
· Reason: To efficiently manage IPv4 address exhaustion and simplify their network architecture. They increasingly assign IPv6-only addresses to smartphones by default. When a user on such a network needs to access an IPv4-only service, the carrier's network seamlessly handles the translation using NAT64/DNS64. This is a standard and essential practice for modern mobile internet infrastructure in Japan.
2. Rakuten Mobile:
· Special Note: As a newer, cloud-native mobile network operator, Rakuten Mobile has been particularly vocal about building a modern, software-defined network. A key part of this architecture is leveraging IPv6 from the ground up, which inherently relies on transition technologies like NAT64/DNS64 for backward compatibility.
3. Leading Internet and E-commerce Companies:
· Who: Yahoo Japan (now part of Z Holdings) and LINE (also part of Z Holdings).
· Usage: These companies operate massive-scale online platforms and data centers. To ensure scalability and manageability, they are building new server clusters as IPv6-only. NAT64/DNS64 is used within their infrastructure to allow these IPv6-only servers to communicate with legacy internal systems or external services that are still on IPv4.
4. Cloud and IT Services Providers:
· Who: Sakura Internet, GMO Internet, and the cloud divisions of NTT Communications (e.g., NTT PC Communications).
· Usage: These providers offer NAT64/DNS64 as a configurable service to their customers. This allows businesses renting cloud servers or VPSs to deploy IPv6-only instances while maintaining outbound connectivity to the IPv4 internet.

Japanese Government Use of NAT64/DNS64

The Japanese government has a clear, top-down strategy for IPv6 adoption, which logically includes the use of transition technologies.

1. The IT Strategic Headquarters and Ministry of Internal Affairs and Communications (MIC):
· Role: These are the central bodies driving Japan's digital transformation. The MIC has been promoting IPv6 for over a decade through its "IPv6 Action Plan" and later the "Road to IPv6" initiative.
· Policy: The government's goal is to make Japan a leading "advanced ICT nation." A core part of this is mandating IPv6 support for all government procurement and encouraging its adoption in the private sector. While they may not mandate NAT64 specifically, their push for IPv6-only and dual-stack networks in government systems creates the direct need for it.
2. Government Agencies and Local Municipalities:
· Usage: As per the national strategy, all central government ministries and local

governments are required to make their websites and online services accessible via IPv6. For their internal networks (e.g., new office networks, IoT sensor deployments for smart cities), adopting IPv6-only segments is a cost-effective and future-proof strategy. In these cases, NAT64/DNS64 is the essential technology that allows government employees and systems to access the vast remaining IPv4 internet and legacy internal applications.

3. National Research and Education Network:

· Who: SINET (Science Information Network)

· Usage: Similar to CERNET2 in China or GÉANT in Europe, Japan's SINET provides a high-speed academic backbone. It has been a long-time pioneer of IPv6. Research institutes and universities connected to SINET often run IPv6-only experimental networks for research, where NAT64/DNS64 is a critical service for providing full internet access.

Summary

Sector	Key Users	Primary motivation
Japanese Companies	Mobile Operators (NTT Docomo, KDDI, SoftBank, Rakuten) Internet Giants (Yahoo Japan/LINE)	Mobile Network Efficiency Data Center Scalability Cloud Service Offerings
Japan Government	Driven by MIC policy; implemented across government networks . and local government IT systems and research networks (SINET)	National ICT Strategy, Procurement Compliance Operational Modernization, Future-Pr

In conclusion, Japan is a robust and mature market for NAT64/DNS64 deployment. Its use is fundamental to the operation of modern mobile data services used by millions and is a key enabling technology for the continued modernization of both corporate and public-sector IT infrastructure in line with national strategic goals.

5 – Saudi Arabia

The adoption of NAT64 and DNS64 in Saudi Arabia is a key part of the Kingdom's broader digital transformation strategy, Saudi Vision 2030. The drive to modernize infrastructure, including the transition to IPv6, is strong and creates a direct need for these transition technologies.

Here's a breakdown of the key Saudi companies and government entities that are using or driving the adoption of NAT64 and DNS64.

Saudi Companies Using NAT64/DNS64

The deployment is most critical within the telecommunications sector, which is the backbone of the digital economy.

1. Major Telecom Operators:
· Who: stc (Saudi Telecom Company), Mobily, and Zain KSA.
· Usage: This is the most significant and widespread use case. Saudi mobile carriers are deploying NAT64/DNS64 in their 4G/5G core networks.
· Reason: The primary drivers are IPv4 address exhaustion and network simplification. By assigning IPv6-only addresses to smartphones and IoT devices by default, carriers can efficiently scale their networks. When a user on such a network needs to access an IPv4-only app or website (e.g., a legacy service), the carrier's network seamlessly performs the translation using NAT64/DNS64. This is a global best practice that Saudi operators have adopted.
2. Cloud and Data Center Providers:
· Who: stc cloud, Mobily Cloud, and major local data center operators.
· Usage: As part of their service offerings, these providers enable NAT64/DNS64 for customers who deploy IPv6-only cloud instances or private clouds. This allows businesses to build modern, scalable applications on IPv6 while maintaining outbound connectivity to the wider IPv4 internet.
3. Large Enterprises in Banking and Industry:
· Usage: Leading Saudi banks, petrochemical companies (e.g., Saudi Aramco's internal IT initiatives), and other large corporations are modernizing their internal networks. As they deploy new IPv6-only segments for corporate Wi-Fi, IoT sensor networks, or new data centers, they will use NAT64/DNS64 gateways to ensure connectivity to legacy IPv4-based internal systems and the internet.

Saudi Government Use of NAT64/DNS64

The Saudi government's push is part of a centralized, strategic effort to become a leading digital hub.

1. The Communications, Space & Technology Commission (CST):
· Role: This is the primary regulator and driver. The CST has launched a National IPv6 Program with a clear roadmap to transition the country from IPv4 to IPv6.
· Directive: The program mandates IPv6 adoption for all telecom operators and encourages its implementation across government entities. This top-down policy creates the essential environment where technologies like NAT64/DNS64 become necessary for a smooth transition.
2. The Saudi Digital Government:
· Who: The Yesser E-Government Program and individual ministries.
· Usage: As per the national directive, all government websites and digital services are required to be accessible via IPv6. For their internal networks—such as new smart city initiatives (e.g., NEOM), IoT deployments for utilities, or modernized office networks—adopting IPv6-only architectures is a forward-looking strategy. In these scenarios, NAT64/DNS64 is the critical component that allows government systems and employees to access the entire internet, including IPv4 resources.
3. National Cybersecurity Authority (NCA):
· Role: The NCA has a vested interest in how new network technologies are deployed securely. The structured and managed approach of NAT64 (as opposed to unmanaged tunnels) provides a more secure and auditable path for transition, which aligns with the NCA's mission to strengthen the Kingdom's cybersecurity posture.
4. Major Public Projects (e.g., NEOM, Red Sea Global):
· Usage: These "giga-projects" are being built from the ground up with cutting-edge technology. It is a core principle to implement IPv6-by-default for all their digital infrastructure, from utilities to citizen services. In such greenfield environments, NAT64/DNS64 will be the standard method for these next-generation cities to interact with the existing IPv4 internet.

Summary

Sector	Key Users	Primary motivation
Saudi Companies	Saudi Companies Telecom Operators (stc, Mobily, Zain) Cloud Providers Large Enterprises Mobile Network	Scalability IPv4 Exhaustion Cloud Service Modernization
SaudiGovernment	Driven by CST & National IPv6 Program implemented across digital	Saudi Vision 2030 National Digital Transforma Regulatory Compliance,

In conclusion, Saudi Arabia's adoption of NAT64 and DNS64 is strategic and policy-driven. It is fundamental to the operations of its modern mobile networks and is a key enabling technology for the Kingdom's ambitious goals to build a leading, resilient, and future-proof digital economy.

Annex

A – NAT 64

NAT64 is a key internet technology that allows devices on an IPv6-only network to communicate with servers and services on the traditional IPv4 internet.

In simple terms, it's a translator between the "new" internet language (IPv6) and the "old" one (IPv4).

The Core Problem NAT64 Solves

The internet is running out of unique IPv4 addresses (like 192.0.2.1). The long-term solution is IPv6, which has a virtually unlimited supply of addresses (like 2001:db8::1).

As organizations build new networks, it's often easier and more efficient to make them IPv6-only. But a huge part of the internet still uses only IPv4. The problem is: an IPv6-only device cannot natively talk to an IPv4-only server.

NAT64 solves this by acting as a bridge.

How NAT64 Works (The Step-by-Step Process)

NAT64 almost always works with a companion technology called DNS64. You can't

have one without the other for this purpose. Here's the process:

Let's imagine you're on an IPv6-only smartphone and you want to visit www.example.com, which is an IPv4-only website.

1. DNS Query: Your phone asks the DNS64 server for the address of www.example.com.
2. Address Lookup: The DNS64 server checks for an IPv6 address (a AAAA record) for the website. It finds none.
3. Address Synthesis: The DNS64 server then checks for the IPv4 address (an A record) and finds 93.184.216.34. It now synthesizes a fake IPv6 address by embedding this IPv4 address into a special IPv6 prefix reserved for NAT64 (e.g., 64:ff9b::/96).
· Result: It gives your phone the synthesized IPv6 address: 64:ff9b::5db8:d822.
4. Routing: Your phone, thinking it's talking to an IPv6 server, sends the data packet to this synthesized address. The network is designed to route all traffic for this special prefix directly to the NAT64 gateway.
5. Translation (The "NAT" part): The NAT64 gateway receives the IPv6 packet. It performs the crucial translation:
· It extracts the embedded IPv4 address (93.184.216.34) from the IPv6 packet.
· It translates the entire packet header from IPv6 to IPv4.
· It also replaces the source address (your phone's IPv6 address) with its own public IPv4 address, so the website has an IPv4 address to reply to.
6. Communication: The NAT64 gateway sends the new IPv4 packet to www.example.com. The website responds to the NAT64 gateway's IPv4 address.
7. Reverse Translation: The NAT64 gateway receives the returning IPv4 packet, looks up its state table to see which IPv6 device it belongs to, and translates the packet back to IPv6, sending it to your phone.

The entire process is seamless. Your IPv6-only phone successfully communicated with an IPv4-only website without you or the phone ever knowing a translation occurred.

A Key Feature: Stateful NAT64

The "Stateful" part is crucial. The NAT64 gateway must keep a state table (a session table) that remembers every active connection. It tracks:

· Which internal IPv6 device made a request.
· Which external IPv4 address it was trying to reach.
· Which source port was used.

This state table allows it to correctly route the returning IPv4 responses back to the correct IPv6 device.

Why is NAT64 So Important?

Scenario	Role of NAT64
Mobile Networks (4G/5G)	Your smartphone is often given only an IPv6 address. NAT64/DNS64 is what lets y case. NAT64/DNS64 is what lets and websites seamlessly.
Corporate & Cloud Networks	Companies building can make them IPv6 and use NAT64 to
IoT (Internet of Things)	massive deployments of sensor using IPv6-only is for simplicity and use NAT64 to reach legacy IPv4 systems or the internet.

NAT64 vs. Other Technologies

· Dual-Stack: The device has both an IPv4 and an IPv6 address. This is the ideal but complex and doesn't solve IPv4 address exhaustion.
· NAT64/DNS64: The device has only an IPv6 address. It's a cleaner, more modern solution for new networks, relying on translation for IPv4 access.

Summary

NAT64 is a network address translation protocol that, together with DNS64, enables IPv6-only clients to contact IPv4 servers by translating IPv6 packets into IPv4 packets and vice versa. It is a fundamental technology for the ongoing transition from the old IPv4 internet to the new, scalable IPv6 internet.

B – DNS 64

Building on the explanation of NAT64, DNS64 is the essential companion technology that makes it all work. If NAT64 is the "translator," then DNS64 is the "bilingual directory assistant."

DNS64 is a DNS server mechanism that synthesizes AAAA records (IPv6 addresses)

for hosts that only have A records (IPv4 addresses).

In simple terms: Its job is to create a "fake" IPv6 address for an IPv4-only server, so that an IPv6-only device can try to connect to it.

The Core Problem DNS64 Solves

An IPv6-only device is programmed to ask for IPv6 addresses. If a server only has an IPv4 address, the IPv6-only device has no native way to find it or connect to it. DNS64 tricks the device into thinking the IPv4 server is actually an IPv6 server, which allows the connection to be handed off to the NAT64 gateway for translation.

How DNS64 Works (Step-by-Step)

Let's use the same example: You are on an IPv6-only smartphone and want to visit www.example.com, which is an IPv4-only website.

Without DNS64 (What would happen):

1. Your phone asks a normal DNS server: "What is the IPv6 address (AAAA record) of www.example.com?"
2. The DNS server replies: "It doesn't have one."
3. Your phone gives up. You cannot reach the website.

With DNS64 (What actually happens):

1. DNS Query: Your phone is configured to use a DNS64 server. It sends a query: "What is the IPv6 address (AAAA record) of www.example.com?"
2. Dual Record Lookup: The DNS64 server performs two checks:
· First, it looks for a real IPv6 address (a AAAA record) for the website.
· If it finds one, it returns that genuine address immediately. Your phone connects natively over IPv6. This is the ideal case.
· If it finds no AAAA record, it then looks for an IPv4 address (an A record).
3. Address Synthesis (The "Magic" Step): Let's say the DNS64 server finds the IPv4 address 93.184.216.34.
· It takes this IPv4 address and embeds it into a special, pre-defined IPv6 prefix. This prefix is reserved for use with the NAT64 gateway (a common one is 64:ff9b::/96).
· Result: It creates a synthesized IPv6 address like 64:ff9b::5db8:d822.
· 64:ff9b:: is the well-known prefix.

· 5db8:d822 is the hexadecimal representation of 93.184.216.34.
4. DNS Response: The DNS64 server returns this synthesized AAAA record to your IPv6-only phone.
5. Initiating Connection: Your phone, believing it has a valid IPv6 address for the website, sends a connection request to 64:ff9b::5db8:d822.
6. Hand-off to NAT64: The network routes all traffic for the 64:ff9b::/96 prefix directly to the NAT64 gateway. The NAT64 gateway then takes over, extracts the embedded IPv4 address, translates the packet, and handles the communication as previously described.

A Key Feature: The Well-Known Prefix

The DNS64 server and the NAT64 gateway must be configured to use the same IPv6 prefix. This is what ensures that the packets destined for the synthesized address are automatically sent to the NAT64 gateway for translation. The most common one is 64:ff9b::/96.

Why is DNS64 So Important?

· Seamless User Experience: The entire process is invisible to the end-user and requires no changes to the applications on the IPv6-only device. The device doesn't even know it's talking to an IPv4 server.
· Enables IPv6-Only Deployment: It is the critical enabler that allows mobile carriers and enterprises to deploy pure IPv6 networks today, while the rest of the internet is still transitioning.
· Efficiency: It's a much cleaner and more scalable solution than older transition technologies like tunneling.

DNS64 and NAT64: An Inseparable Pair

To summarize their relationship:

Technology	Role	Analogy
DNS64	The Directory Assistant	You ask for someone's phone number. The assistant finds their old landline nu and gives you a special switchboard number (synthesized IPv6) to call in
NAT64	The Switch	You call the special number. he operator answers, translates your call and connects you to the actual landline, relaying the conversation back and fo

board
Operator

Conclusion

DNS64 is a DNS server that creates synthetic IPv6 addresses for IPv4-only destinations, thereby enabling IPv6-only clients to initiate communication with them via a NAT64 gateway.

Without DNS64, an IPv6-only device would never even attempt to contact an IPv4 server. With it, the entire internet—both IPv6 and IPv4—becomes accessible from a modern, simplified, IPv6-only network.

C – 464XLAT

464XLAT is an advanced and clever IPv6 transition technology that solves a very specific, but critical, problem that plain NAT64/DNS64 cannot handle.

Let's break it down.

The Core Problem 464XLAT Solves

Basic NAT64/DNS64 has a major limitation: It only works if the IPv6-only client initiates the connection.

This fails in several important scenarios:

1. Applications with Embedded IP Addresses: Some applications, especially older ones like VoIP, online games, or peer-to-peer apps, hardcode IPv4 addresses instead of using DNS hostnames.
2. IPv4 Literal Addresses: If you type an IPv4 address (like 192.0.2.1) directly into your browser, DNS64 is completely bypassed.
3. NAT Traversal Techniques: Some applications use complex methods to discover their own public IP address or establish direct connections with peers. These methods often fail in a pure NAT64 environment.

In all these cases, the IPv6-only device has an IPv4 address it wants to talk to, but no synthesized IPv6 address to send the traffic to. The connection simply fails.

464XLAT fixes this by enabling the client itself to initiate communication with an IPv4-only destination, even without DNS.

How 464XLAT Works: The "Two-Step Translation"

The name "464XLAT" reveals exactly how it works:

- **4: The original protocol is IPv4.**
- **64: It's translated to IPv6 for transport across the network.**
- **XLAT: It's translated again (the "X" stands for "trans").**
- **Result: 4 -> 6 -> 4 translation.**

It involves two translation points:

1. CLAT (Customer-side Translator): This is a small, simple function on the client device itself (e.g., your smartphone or router).
2. PLAT (Provider-side Translator): This is the traditional NAT64 gateway located in the ISP's or mobile carrier's network.

Here is the step-by-step process:

Scenario: You are on an IPv6-only mobile network. You use an app that has an IPv4 address (192.0.2.55) hardcoded in it.

Step 1: First Translation (4 to 6) by the CLAT

1. The app on your phone generates a packet destined for the IPv4 address 192.0.2.55.
2. The CLAT on your phone intercepts this IPv4 packet.
3. It embeds the IPv4 destination into a special IPv6 prefix (the same one used by the carrier's NAT64/DNS64 system, e.g., 64:ff9b::/96), creating a synthesized IPv6 address: 64:ff9b::c000:237 (where c000:237 is 192.0.2.55 in hex).
4. The CLAT also translates the source address (your phone's IPv6 address) and sends the new IPv6 packet into the network.

Step 2: Transport Across the Core Network

- **The IPv6 packet travels seamlessly across the carrier's IPv6-only network.**

Step 3: Second Translation (6 to 4) by the PLAT

1. The packet, destined for 64:ff9b::c000:237, arrives at the carrier's PLAT (NAT64 gateway).
2. The PLAT performs the standard NAT64 function: it extracts the embedded IPv4

address (192.0.2.55), translates the packet back to IPv4, and sends it out to the public IPv4 internet.

The return path simply follows these steps in reverse.

The "Magic" and Key Benefit

The brilliance of 464XLAT is that it makes the entire internet—including IPv4-only services and applications that use literal IP addresses—seamlessly accessible from an IPv6-only device.

· For normal web browsing (using domain names), the system uses the efficient NAT64/DNS64 path.
· For apps using IPv4 literals or embedded IPs, the system uses the 464XLAT path.

The user is completely unaware of which path is being used. Everything "just works."

A Simple Analogy

· NAT64/DNS64: Like a company's main switchboard. You ask the operator (DNS64) for a person's name, and they connect you (NAT64).
· 464XLAT: Like having a direct extension from your desk that also connects to the same switchboard. If you already know the person's old internal extension number (IPv4 literal), you can dial it directly from your phone, and your phone's built-in system (CLAT) will route it through the switchboard (PLAT) to reach the outside world.

Why is 464XLAT So Important?

Scenario	Role of 464XLAT
Mobile Networks (4G/5G)	Critical. It's the technology that allows your smartphone to run millions of legacy a games and VoIP apps) without any changes, even when you are on an IPv6-only cellular co
Gaming Consoles & IoT Devices	Devices Ensures devices and apps that use hardcoded IPs for connectivity or upda

Enterprise Networks	Allows a company to deploy an IPv6-only corporate Wi-Fi network while ensuring al function.

Summary

464XLAT is an IPv6 transition mechanism that provides full IPv4 connectivity to IPv6-only clients by performing a two-step translation: first on the client device (CLAT) from IPv4 to IPv6, and then in the network (PLAT) from IPv6 back to IPv4.

It is the key technology that makes large-scale, user-friendly IPv6-only networking a practical reality today, by ensuring complete backward compatibility with the entire IPv4 internet.

Call for submission of your Country IPv6-Only Deployment in the enteprise and governments to latif.ladid@ipv6forum.com