White Paper

NAT64 Technology: Connecting IPv6 and IPv4 Networks

Last updated: April 2012

Contents

What You Will Learn

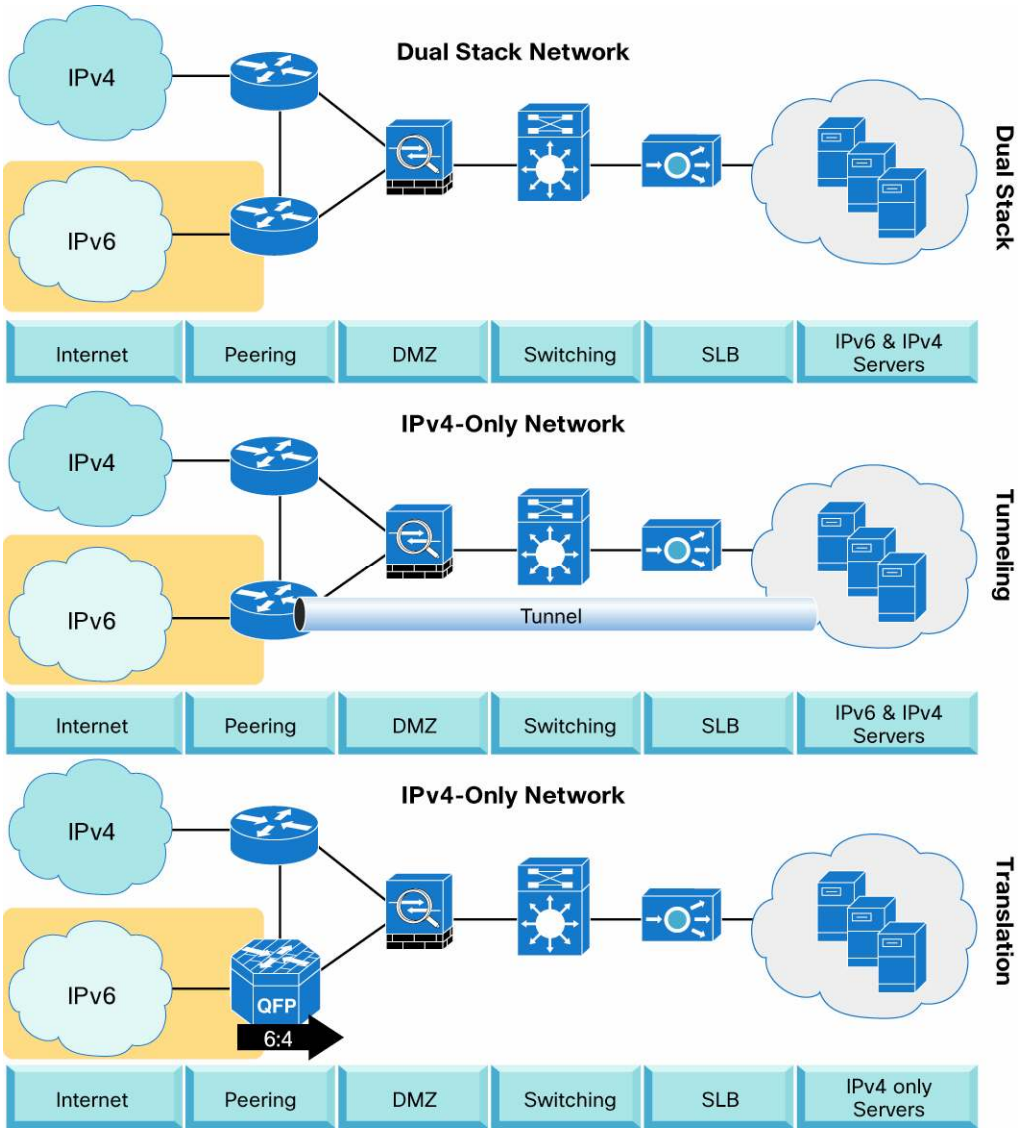
Three main options are available for migration to IPv6 from the existing network infrastructure: dual-stack network, tunneling, and translation. This document briefly discusses each of these options and highlights the advantages of translation and, in particular, stateful translation, over the other two. It provides a technical overview of the translation scenarios documented in RFC 6144.

This document discusses ways to provide a seamless Internet experience to users accessing IPv4 Internet services through completely new (“greenfield”) IPv6-only networks. It also describes how established content providers and content enablers can transparently provide existing or new services to IPv6 Internet users by deploying Network Address Translation IPv6 to IPv4 (NAT64) technology with little or no change in their existing network infrastructure, thus maintaining business continuity.

Available IPv6 Transition Technologies

Figure 1 shows The three options available for migration to IPv6 from the existing network infrastructure: dual-stack network, tunneling, and translation.

Figure 1. Available IPv6 Transition Techniques



Dual-Stack Network

Dual stack is a transition technology in which IPv4 and IPv6 operate in tandem over shared or dedicated links. In a dual-stack network, both IPv4 and IPv6 are fully deployed across the infrastructure, so that configuration and routing protocols handle both IPv4 and IPv6 addressing and adjacencies.

Although dual-stack may appear to be an ideal solution, it presents two major deployment challenges to enterprises and ISPs:

- It requires a current network infrastructure that is capable of deploying IPv6. In many cases, however, the current network may not be ready and may require hardware and software upgrades.
- IPv6 needs to be activated on almost all the network elements. To meet this requirement, the existing network may need to be redesigned, posing business continuity challenges.

Tunneling

Using the tunneling option, organizations build an overlay network that tunnels one protocol over the other by encapsulating IPv6 packets within IPv4 packets and IPv4 packets within IPv6 packets. The advantage of this approach is that the new protocol can work without disturbing the old protocol, thus providing connectivity between users of the new protocol.

Tunneling has two disadvantages, as discussed in RFC 6144:

- Users of the new architecture cannot use the services of the underlying infrastructure.
- Tunneling does not enable users of the new protocol to communicate with users of the old protocol without dual-stack hosts, which negates interoperability.

Translation

Address Family Translation (AFT), or simply translation, facilitates communication between IPv6-only and IPv4-only hosts and networks (whether in a transit, an access, or an edge network) by performing IP header and address translation between the two address families.

AFT is not a long-term support strategy; it is a medium-term coexistence strategy that can be used to facilitate a long-term program of IPv6 transition by both enterprises and ISPs.

Translation offers two major advantages, as discussed in RFC 6144:

- Translation provides a gradual migration to IPv6 by providing seamless Internet experience to greenfiled IPv6-only users, accessing IPv4 Internet services.
- Existing content providers and content enablers can provide services transparently to IPv6 Internet users by using translation technology, with little or no change in the existing network infrastructure, thus maintaining IPv4 business continuity.

Specific protocols such as File Transfer Protocol (FTP) and Session Initiation Protocol (SIP) that embed IP address information within the payload require application-layer gateway (ALG) support for translation.

Scenarios for IPv6/IPv4 Translation

As discussed, AFT offers benefits over the other available IPv6 migration and transition technologies. Figure 2 and Table 1 summarize various scenarios supported by translation. These scenarios are standardized by IETF in RFC 6144.

Figure 2. Scenarios for IPv6/IPv4 Translation

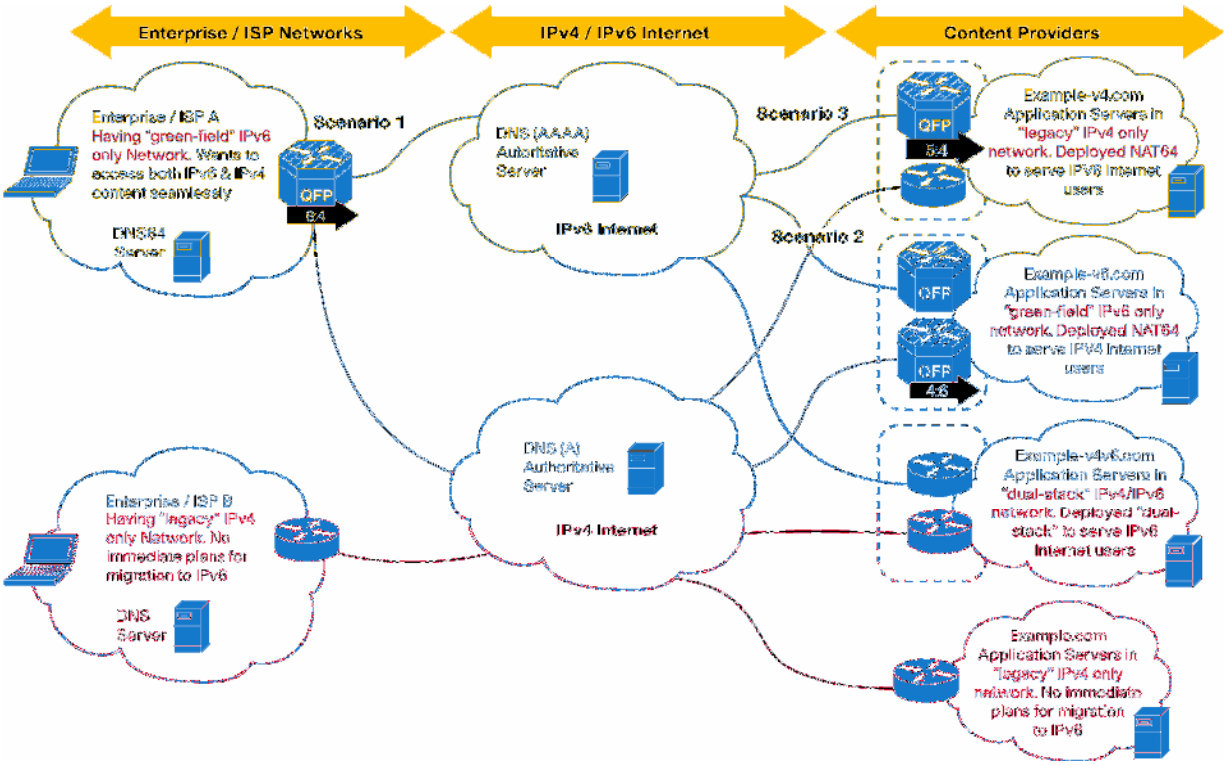


Table 1. Translation Scenarios and Their Applicability

Scenarios for IPv6/IPv4 Translation	Applicability	Example
Scenario 1: An IPv6 network to the IPv4 Internet	• Greenfield IPv6-only network wanting to transparently access both IPv6 and existing IPv4 content • Initiated from IPv6 hosts and network	• ISPs rolling out new services and networks for IPv6-only smartphones (third-generation [3G], Long-Term Evolution [LTE], etc.) handsets • Enterprises deploying IPv6-only network
Scenario 2: The IPv4 Internet to an IPv6 network	• Servers in greenfield IPv6-only network wanting to transparently serve both IPv4 and IPv6 users • Initiated from IPv4 hosts and network	Upcoming or existing content providers rolling out services in IPv6-only environment
Scenario 3: The IPv6 Internet to an IPv4 network	• Servers in existing IPv4-only network wanting to serve IPV6 Internet users • Initiated from IPv6 hosts and network	Existing content providers migrating to IPv6 and thus wanting to offer services to IPv6 Internet users as part of coexistence strategy
Scenario 4: An IPv4 network to the IPv6 Internet	Not a viable case in the near future; this scenario will probably occur only some time after the early stage of the IPv6/IPv4 transition	None
Scenario 5: An IPv6 network to an IPv4 network	Both an IPv4 network and an IPv6 network are within the same organization	Similar to scenario 1, catering to Intranet instead of Internet
Scenario 6: An IPv4 network to an IPv6 network	Same as above	Similar to scenario 2, catering to intranet instead of Internet
Scenario 7: The IPv6 Internet to the IPv4 Internet	Would suffer from poor throughput	None
Scenario 8: The IPv4 Internet to the IPv6 Internet	No viable translation technique to handle unlimited IPv6 address translation	None

Technologies Facilitating IPv6/IPv4 Translation

AFT can be achieved using either of the following two technologies:

- Network Address Translation-Protocol Translation (NAT-PT)
- Network Address Translation 64 (NAT64)

NAT-PT has been deemed deprecated by IETF because of its tight coupling with Domain Name System (DNS) and its general limitations in translation, all of which are documented in RFC 4966. With the deprecation of NAT-PT and the increasing urgency to get moving on IPv6 transition, IETF proposed NAT64 as the viable successor to NAT-PT.

Network Address Translation IPv6 to IPv4, or NAT64, technology facilitates communication between IPv6-only and IPv4-only hosts and networks (whether in a transit, an access, or an edge network). This solution allows both enterprises and ISPs to accelerate IPv6 adoption while simultaneously handling IPv4 address depletion. The DNS64 and NAT64 functions are completely separated, which is essential to the superiority of NAT64 over NAT-PT.

All viable translation scenarios are supported by NAT64, and therefore NAT64 is becoming the most sought translation technology. AFT using NAT64 technology can be achieved by either stateless or stateful means:

- Stateless NAT64, defined in RFC 6145, is a translation mechanism for algorithmically mapping IPv6 addresses to IPv4 addresses, and IPv4 addresses to IPv6 addresses. Like NAT44, it does not maintain any bindings or session state while performing translation, and it supports both IPv6-initiated and IPv4-initiated communications.
- Stateful NAT64, defined in RFC 6146, is a stateful translation mechanism for translating IPv6 addresses to IPv4 addresses, and IPv4 addresses to IPv6 addresses. Like NAT44, it is called stateful because it creates or modifies bindings or session state while performing translation. It supports both IPv6-initiated and IPv4-initiated communications using static or manual mappings.

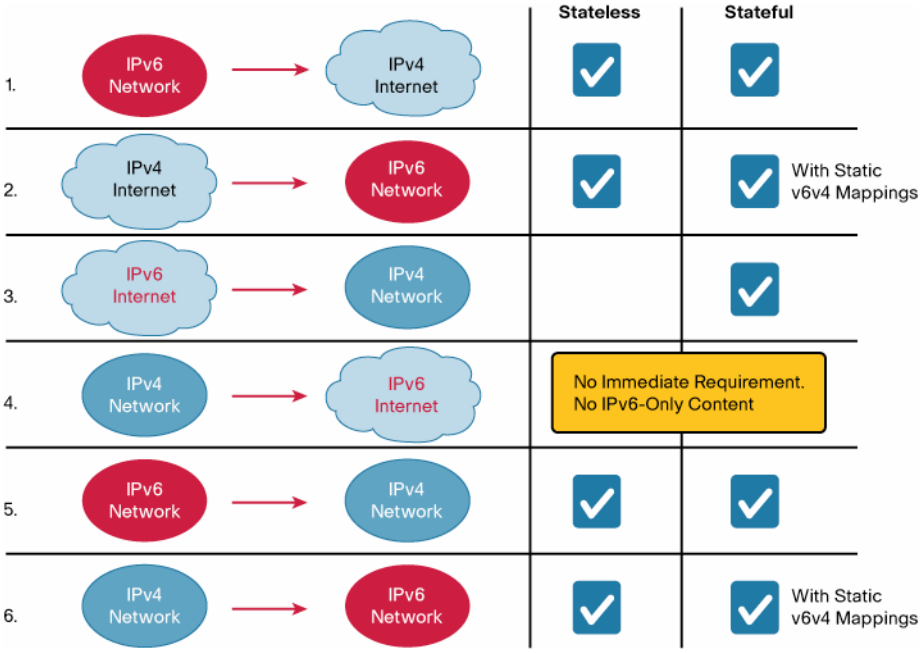
Table 2 and Figure 3 compare stateless and stateful NAT64.

Specific protocols such as FTP and SIP that embed IP address information within the payload require ALG support for AFT.

Table 2. Comparison Between Stateless and Stateful NAT64

Stateless NAT64	Stateful NAT64
1:1 translation, hence applicable for limited number of endpoints	1: N translation, hence no constraint on the number of end points therefore, also applicable for carrier grade NAT (CGN)
No conservation of IPv4 address	Conserves IPv4 address
Helps ensure end-to-end address transparency and scalability	Uses address overloading; hence lacks end-to-end address transparency
No state or bindings created on the translation	State or bindings created on every unique translation
Requires IPv4-translatable IPv6 address assignment (mandatory requirement)	No requirement for the characteristics of IPv6 address assignment
Requires either manual or Domain Host Configuration Protocol Version 6 (DHCPv6)–based address assignment for IPv6 hosts	Capability to choose any mode of IPv6 address assignment: manual, DHCPv6, or stateless address autoconfiguration (SLAAC)

Figure 3. IPv4/IPv6 Translation Scenarios



Reviewing this comparison, it is clear that stateful NAT64 is the preferred choice for AFT.

AFT Using Stateful NAT64

AFT using stateful NAT64 is preferred over the other available IPv6 migration and transition technologies. It facilitates communication using User Datagram Protocol (UDP), Transmission Control Protocol (TCP), or Internet Control Message Protocol (ICMP) between IPv6-only and IPv4-only hosts and networks by performing:

- IP header translation between the two address families using an algorithm defined in RFC 6145 (IP/ICMP Translation Algorithm)
- IP address translation between the two address families using an algorithm defined in RFC 6052 (IPv6 Addressing of IPv4/IPv6 Translators)

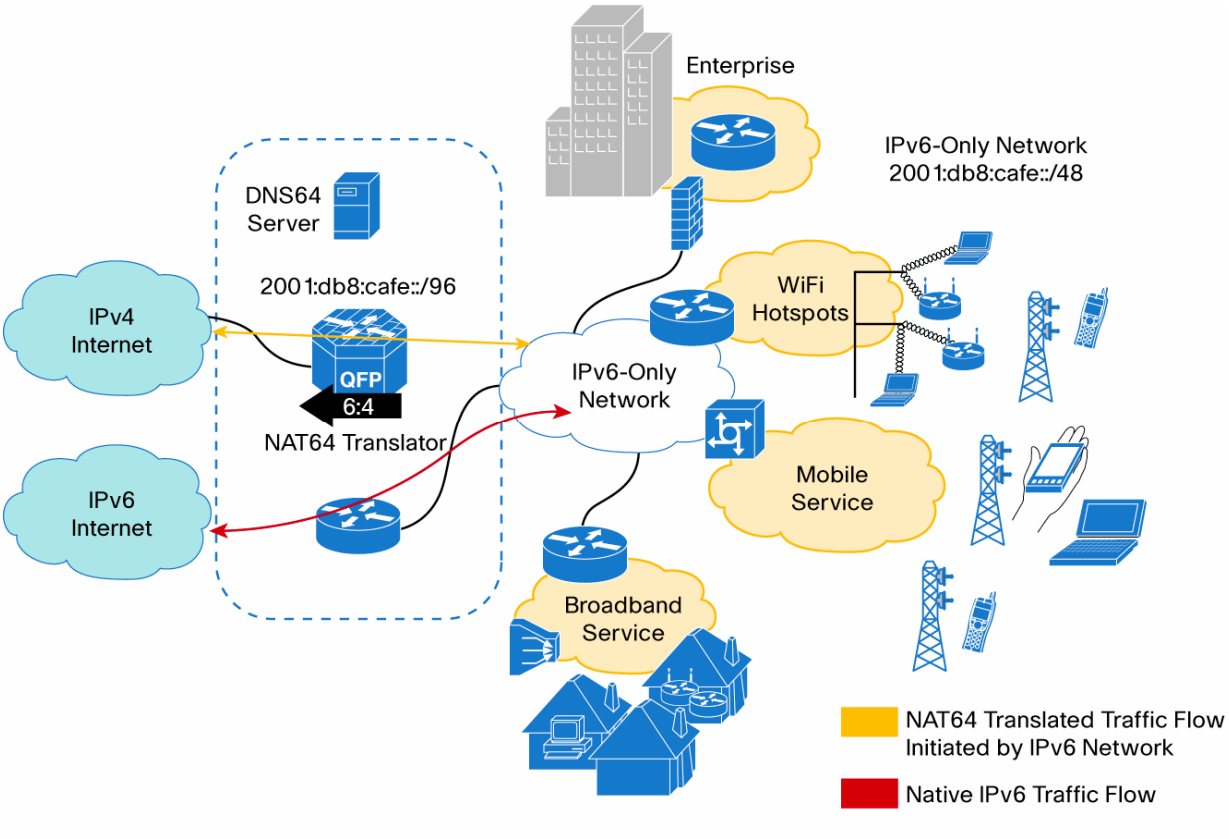
Table 3. Stateful NAT64 Terminology

Terminology	Definition
Well-known prefix (WKP)	The IPv6 prefix 64:ff9b::/96, defined in RFC 6052, used for algorithmic mapping between address families.Prefix 64:ff9b::/96 is not a globally routable prefix and hence must not be used in scenario 3
Network-specific prefix (NSP)	An IPv6 prefix assigned by an organization for use in algorithmic mapping between address families; it is usually carved out of the organization prefix and can be globally routable: for example, 2001:db8:cafe::/96 carved out of organization prefix 2001:db8:cafe::/48
IPv4-converted IPv6 addresses	IPv6 addresses used to represent IPv4 nodes in an IPv6 network: for example, 2001:db8:cafe::c000:0201 using NSP or 64:ff9b::c000:0201 using WKP, both representing 192.0.2.1 (hex c000201)

Providing IPv4 Internet Access to IPv6-Only Networks

Figure 4 shows a typical greenfield IPv6-only network: for example, an enterprise, mobile service operator, broadband service provider, or ISP network. The primary requirement of such a greenfield network deployment is seamless connectivity for IPv6-only hosts to reach both IPv6 and IPv4 Internet and network content.

Figure 4. Greenfield IPv6-Only Network



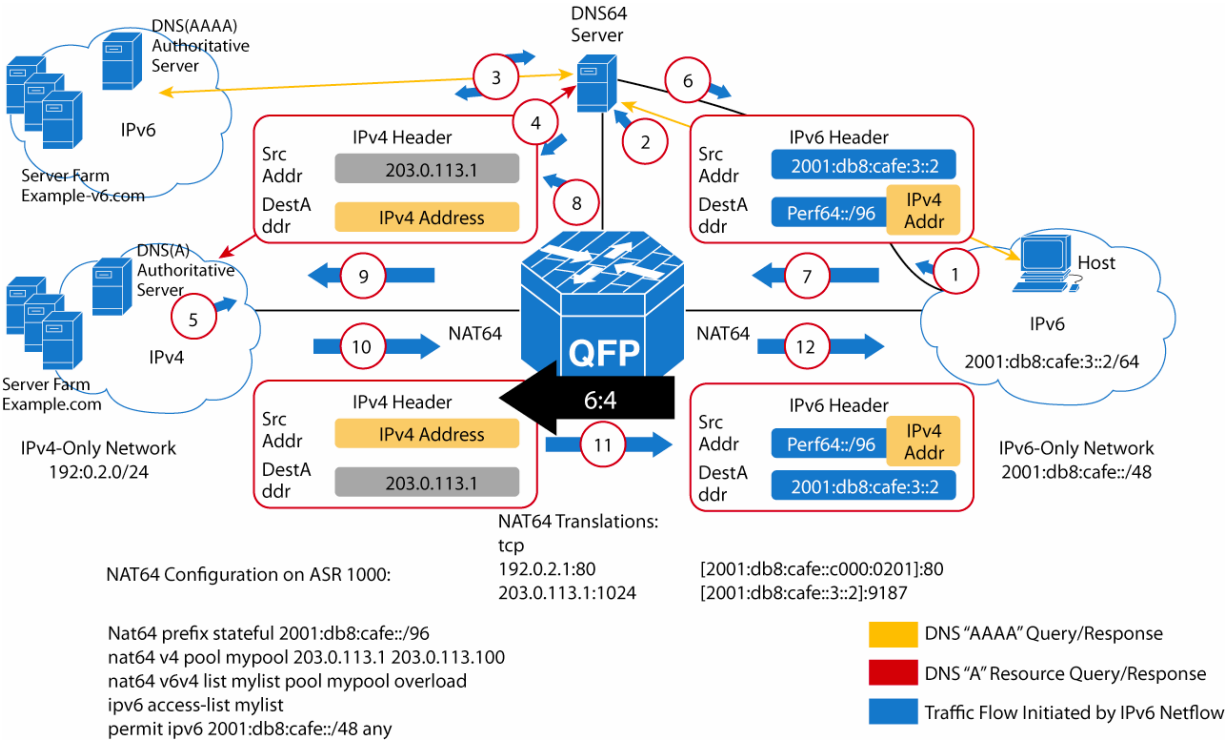
This requirement is identified as scenarios 1 and 5 in RFC 6144 discussed earlier in this document and can be met by using stateful NAT64 technology provided by Cisco® ASR 1000 Series Aggregation Services Routers. With stateful NAT64 on Cisco ASR 1000 Series routers, enterprises and ISPs gain the following benefits:

- A public IPv4 address pool is shared among several IPv6-only hosts, thus conserving IPv4 addresses.
- IPv6-only hosts can access the IPv6 Internet and network using native IPv6 transport.
- IPv6-only hosts pass through stateful NAT64 translation to access the IPv4 Internet and network. Traffic flow is initiated from the IPv6 network to reach IPv4 content.

DNS64, an optional component defined in RFC 6147, when used in conjunction with NAT64, would trick the IPv6 hosts into thinking that the IPv4 destination as an IPv6 address, by synthesizing AAAA (quad A) resource records from A resource records.

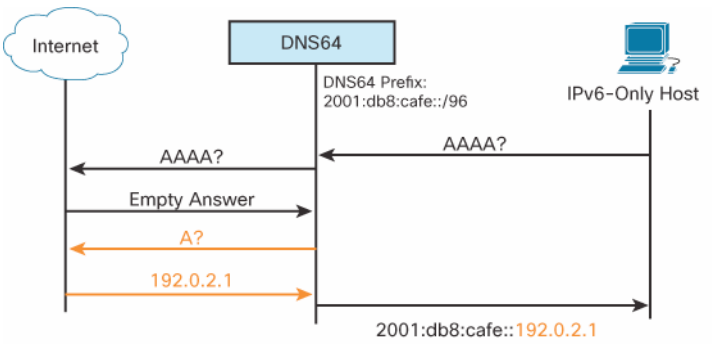
Figure 5 summarizes the steps required for NAT64 translation on a Cisco ASR 1000 Series router running stateful NAT64 when a greenfield IPv6-only network accesses services offered by example.com, residing in an existing IPv4 Internet and network.

Figure 5. Cisco ASR 1000 Series Router Translating IPv6 Traffic to IPv4 and IPv4 Traffic to IPv6



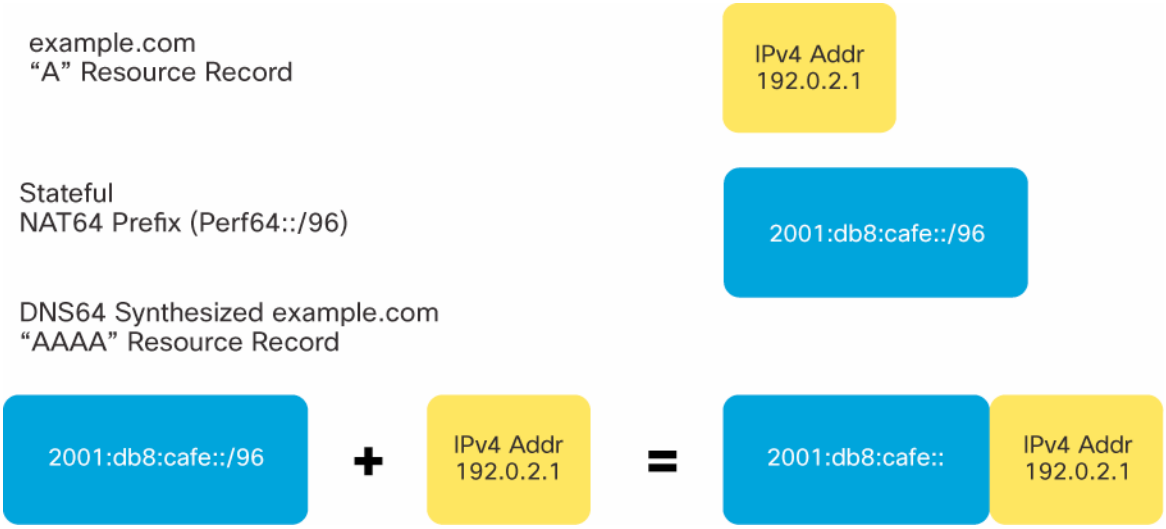
1. The IPv6-only host performs as DNS lookup by triggering a DNS query (AAAA: example.com) to access a service from example.com.
2. The DNS64 server receives a DNS AAAA query for resolving example.com.
3. DNS64 triggers an AAAA query to the DNS AAAA authoritative server for the domain being queried. However, because the server has only an A record for example.com, an empty AAAA response is returned (Figure 6).

Figure 6. DNS64 Operation



4. On receiving the empty answer in the response to the AAAA request, DNS64 triggers an A query (A: example.com) to the DNS A authoritative server.
5. DNS64 receives a DNS A record for the service being queried (A: example.com—192.0.2.1).
6. DNS64 synthesizes the AAAA record by prefixing it with the NAT64 prefix, which may be the WKP or an NSP, as described in Table 3 (Figure 7).

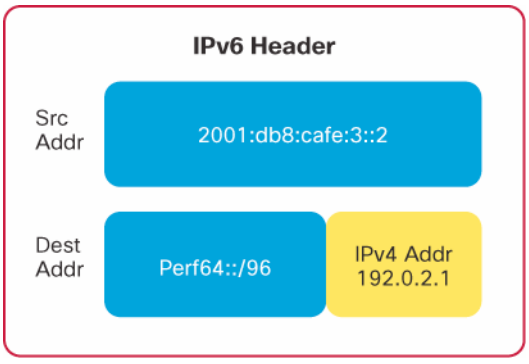
Figure 7. DNS64 Synthesizing an A Record into an AAAA Record



7. The IPv6-only host connects to the service hosted by example.com using the IPv6 address received in the AAAA DNS response. The synthesized AAAA record is transparent to the host, and it appears as if example.com services are accessible over the IPv6 Internet and network (Figure 8):
   - DNS64 AAAA response to example.com: 2001:db8:cafe::c000:0201
   - IPv6 source address: 2001:db8:cafe:3::2
   - IPv6 destination address: 2001:db8:cafe::c000:0201

Note: 192.0.2.1 is represented as c0000201 in hexadecimal format.

Figure 8. IP Source and Destination Address Used by IPv6-Only Host



8. Cisco ASR 1000 Series router running NAT64 receives the IPv6 packet sent by the host on the NAT64-enabled interface and performs the following tasks:

a. Since the router is configured with 2001:db8:cafe::/96 as the stateful NAT64 prefix, it tries to match the first 96 bits of the destination IPv6 address.

b. Packets are forwarded untranslated using IPv6 routing if the IPv6 destination address does not match the configured stateful NAT64 prefix.

c. If the destination address matches the stateful NAT64 prefix, the IPv6 packet undergoes NAT64 translation (Figure 9):

i. The IPv6 header is translated into an IPv4 header.

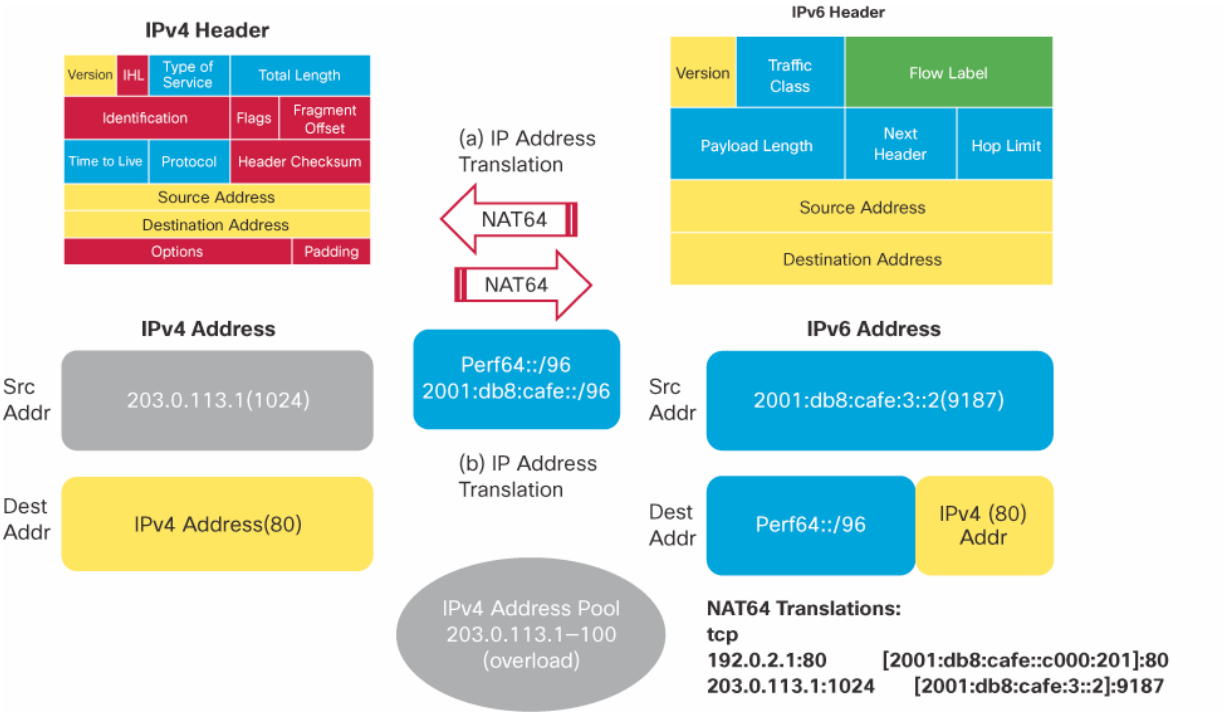
ii. The IPv6 destination address is translated into an IPv4 address by removing the IPv6 stateful NAT64 prefix.

iii. The IPv6 source address is translated into an IPv4 address by using the configured IPv4 address pool. Depending on the NAT64 configuration, either 1:1 address translation or IPv4 address overloading is performed.

iv. Stateful NAT64 IP address translation states are created for both the source and destination IP addresses. States are created when the translation is performed for the first time; thereafter, a state is maintained until the traffic stops and the state maintenance timer expires. Subsequent IPv6 packets are translated using the NAT64 translation state created at this step.

NAT64 Translations:
tcp
192.0.2.1:80 [2001:db8:cafe::c000:0201]:80
203.0.113.1:1024 [2001:db8:cafe:3::2]:9187

Figure 9. NAT64 Translation



9. After NAT64 translation, the translated IPv4 packet is forwarded by the usual IPv4 route lookup.

10. The IPv4 server hosting service offered by domain example.com replies to the NAT64-enabled IPv4 interface on the Cisco ASR 1000 Series router.
11. The Cisco ASR 1000 Series router running NAT64 receives the IPv4 packet sent by the IPv4 server on the NAT64-enabled interface and performs the following tasks:

    a. It performs a lookup and tries to determine whether a NAT64 translation state exists for the IPv4 destination address.

    b. If a translation state does not exist, it discards the IPv4 packet.

    c. If a translation state exists, the router performs following steps:

    i. The IPv4 header is translated into an IPv6 header.

    ii. The IPv4 source address is translated into an IPv6 source address by adding the IPv6 stateful NAT64 prefix.

    iii. The IPv4 destination address is translated into an IPv6 address by using the existing NAT64 translation state.
12. After translation, the IPv6 packets are forwarded using normal IPv6 route lookup.

Thus, seamless communication is established between an IPv6-only host and an IPv4-only server using stateful NAT64 translation at the IPv6 network boundary or edge.

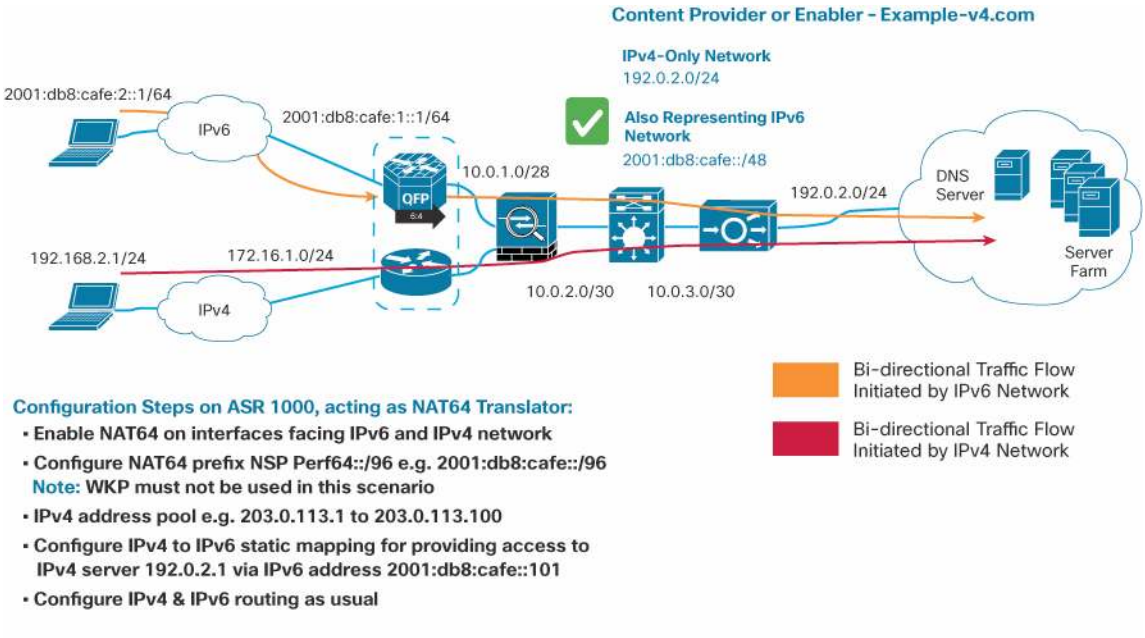
Providing Services to the IPv6 Internet from Existing IPv4 Networks

Figure 10 shows a typical existing IPv4 content provider network: application, e-commerce, social networking, etc. or content enabler network: managed hosting service providers, cloud service providers, etc The primary requirement for an existing IPv4 content provider or content enabler is that they provide services transparently to IPv6 Internet users, with little or no change in the existing network infrastructure, thus maintaining existing business continuity.

This requirement is identified as scenario 3 in RFC 6144 discussed earlier in this document and can be met by using stateful NAT64 technology provided by Cisco ASR 1000 Series routers. With stateful NAT64 on the Cisco ASR 1000 Series, existing content providers or enablers gain the following benefits:

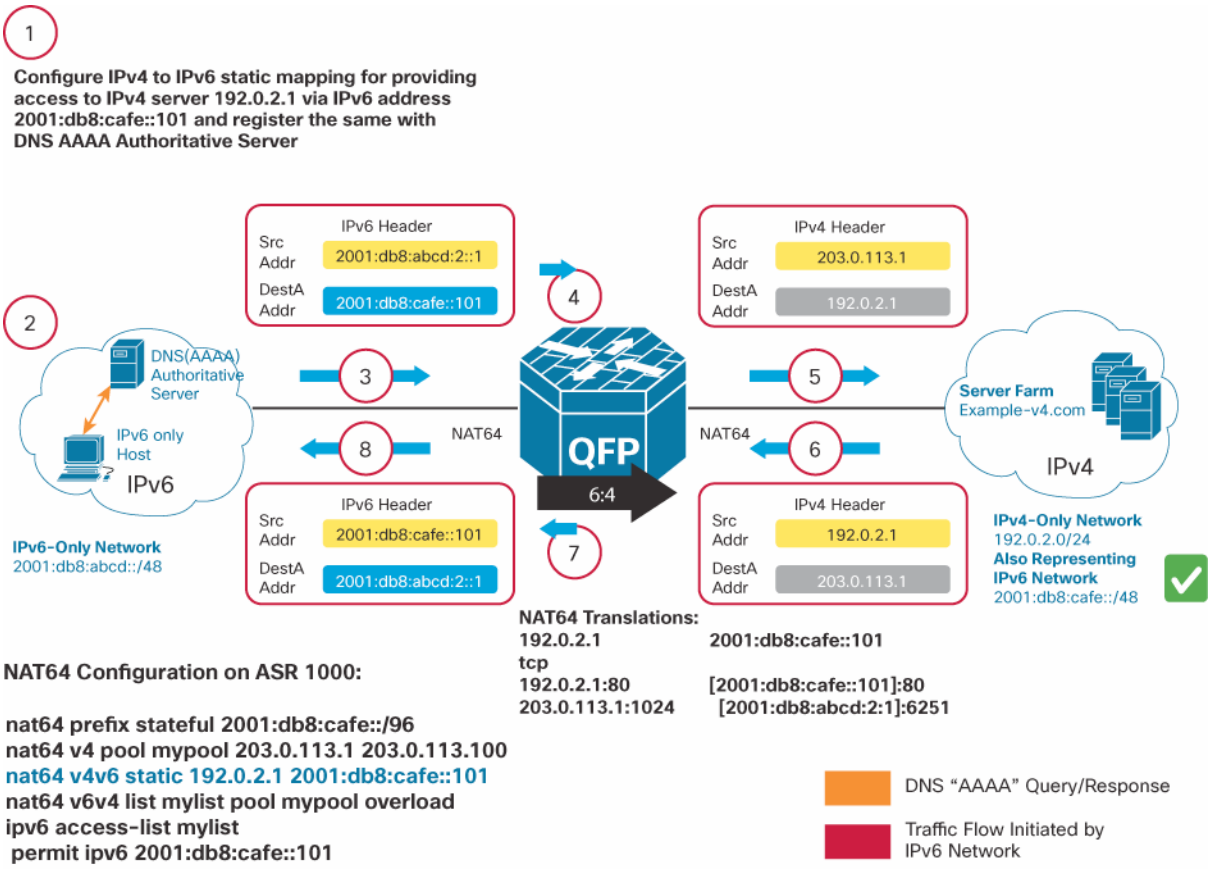
- Nothing changes for the content provider's existing customers. For them, business continuity remains as usual over the IPv4 Internet.
- In addition, the content provider can provide services transparently to new IPv6-only users connected through the IPv6 Internet.
- The content provider can provide services over the IPv6 Internet with little or no change in the existing network infrastructure.
- IPv6-only hosts can access IPv4-only content transparently over native IPv6 by using stateful NAT64 translation at the content provider's edge network.

Figure 10. Providing Existing Services to the IPv6 Internet



Example-v4.com is an established content provider, offering existing IPv4 services to users over the IPv6 Internet. Figure 11 summarizes the steps required for NAT64 translation on a Cisco ASR 1000 Series router running stateful NAT64.

Figure 11. Cisco ASR 1000 Series Router Translating IPv6 Traffic to IPv4 and IPv4 Traffic to IPv6



1. Configure IPv4 to IPv6 static mapping to provide access to IPv4 server 192.0.2.1 through IPv6 address 2001:db8:cafe::101. Also register IPv6 address 2001:db8:cafe::101 as a DNS AAAA resource record—for example-v4.com—with the DNS AAAA authoritative server.

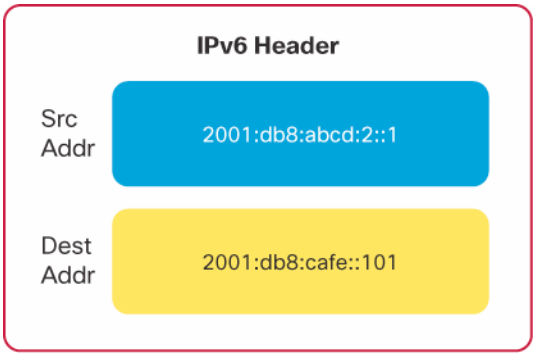
   The following NAT64 translation state is created after static IPv4-to-IPv6 mapping is configured: nat64 v4v6 static 192.0.2.1 2001:db8:cafe::101. Thus, IPv4 address 192.0.2.1 would statically disguise IPv6 address 2001:db8:cafe::101.

   NAT64 Translations:
   192.0.2.1 2001:db8:cafe::101

2. The IPv6-only host triggers a DNS query (AAAA: example-v4.com) to its DNS authoritative server to access a service. The DNS authoritative server responds with an AAAA response for the domain example-v4.com.

3. The IPv6-only host connects to the service hosted by example-v4.com using the IPv6 address received in the AAAA DNS response (Figure 12).

Figure 12. IP Source and Destination Address Used by IPv6-Only Host



4. The Cisco ASR 1000 Series router running NAT64 receives the IPv6 packet sent by the host on the NAT64-enabled interface and performs the following tasks (Figure 13):

   a. The IPv6 access list should be configured allowing only the desired IPv6 packets for which static IPv6-to-IPv4 translation is preconfigured:

   permit ipv6 any host 2001:db8:cafe::101

   b. Since the router is configured with 2001:db8:cafe::/96 as the stateful NAT64 prefix, it tries to match the first 96 bits of the destination IPv6 address.

   c. Packets are dropped if the IPv6 destination address does not match the configured stateful NAT64 prefix.

   d. If the destination address matches the stateful NAT64 prefix, the IPv6 packet undergoes NAT64 translation using the static NAT64 translation created in step 1.

   e. The IPv6 header is translated into an IPv4 header.

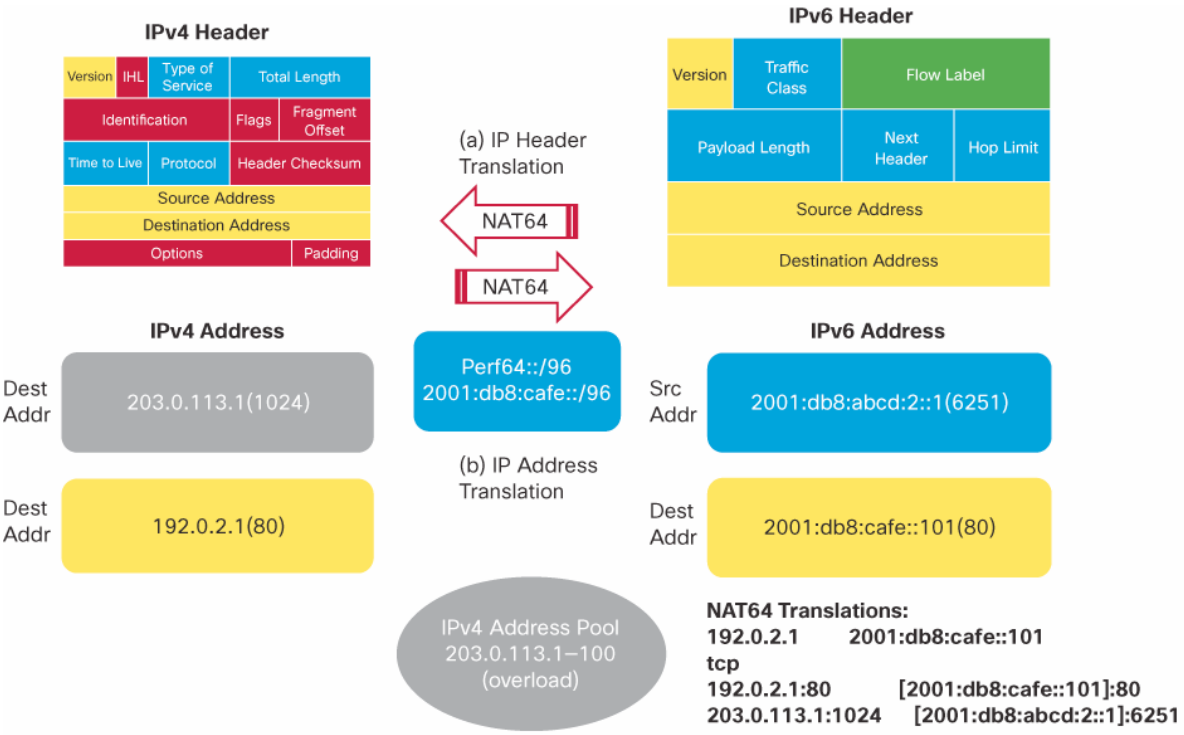
   f. The IPv6 destination address is translated into an IPv4 address using the existing NAT64 translation state.

   g. The IPv6 source address is translated into an IPv4 address by using the configured IPv4 address pool. Depending on the NAT64 configuration, either 1:1 address translation or IPv4 address overloading is performed.

   h. States are created when the translation is performed for the first time; thereafter, a state is maintained until the traffic stops and the state maintenance timer expires. Subsequent IPv6 packets are translated using the NAT64 translation state created in this step.

   NAT64 Translations:
   192.0.2.1 2001:db8:cafe::101
   tcp
   192.0.2.1:80 [2001:db8:cafe::101]:80
   203.0.113.1:1024 [2001:db8:abcd2::1]:6251

Figure 13. NAT64 Translation



5. After NAT64 translation, the translated IPv4 packet is forwarded by the usual IPv4 route lookup to its destination, example-v4.com IPv4 content server.
6. The IPv4 server hosting service offered by domain example-v4.com replies to the NAT64-enabled IPv4 interface on the Cisco ASR 1000 Series router.
7. The Cisco ASR 1000 Series router running NAT64 receives the IPv4 packet sent by the IPv4 server on the NAT64-enabled interface and performs the following tasks:

    a. It performs a lookup and tries to determine whether a NAT64 translation state exists for the IPv4 destination address.

    b. NAT64 discards the IPv4 packet if a translation state does not exist.

    c. If a translation state exists, the router performs following steps:

        i. The IPv4 header is translated into an IPv6 header.

        ii. The IPv4 source address is translated into an IPv6 source address using the existing NAT64 translation state.

        iii. The IPv4 destination address is translated into an IPv6 address using the existing NAT64 translation state.
8. After translation, the IPv6 packets are forwarded using normal IPv6 route lookup.

Thus, transparent communication is established between an IPv6-only host and IPv4-only server using stateful NAT64 translation at the content provider's edge.

Providing Services to the IPv4 Internet from IPv6 Networks

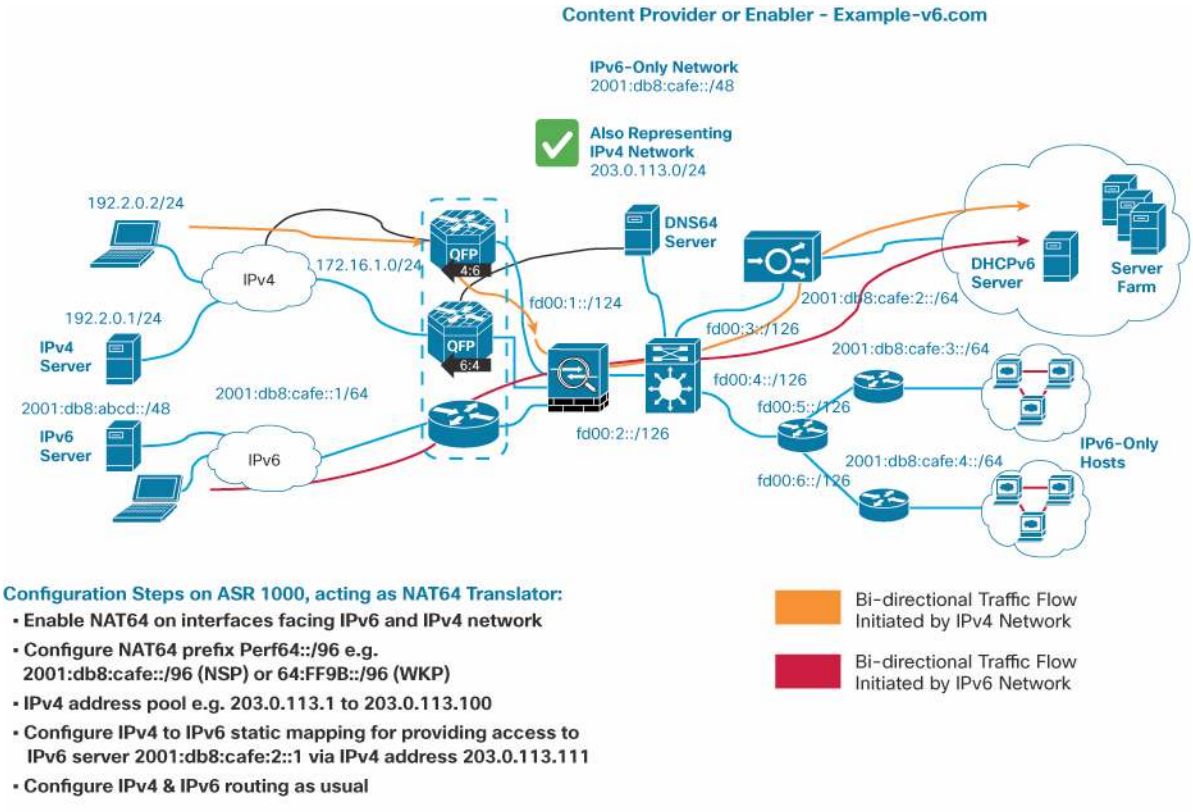
Scenarios 2 and 6 are extensions to scenarios 1 and 5 in RFC 6144 discussed earlier in this document and can be treated as the reverse of scenario 3. Over time, enterprises and ISPs may want to install servers in greenfield IPv6-only networks and thus may want to transparently serve both IPv4 and IPv6 users over the Internet.

Figure 14 shows a typical greenfield IPv6-only enterprise or ISP network that has a server farm. The primary requirement of such a greenfield network deployment is the capability to provide services transparently to both IPv6 and IPv4 users.

This requirement is identified as scenarios 2 and 6 in this document and can be met by using stateful NAT64 technology provided by Cisco ASR 1000 Series routers. With stateful NAT64 on a Cisco ASR 1000 Series router, enterprises and ISPs gain the following benefits:

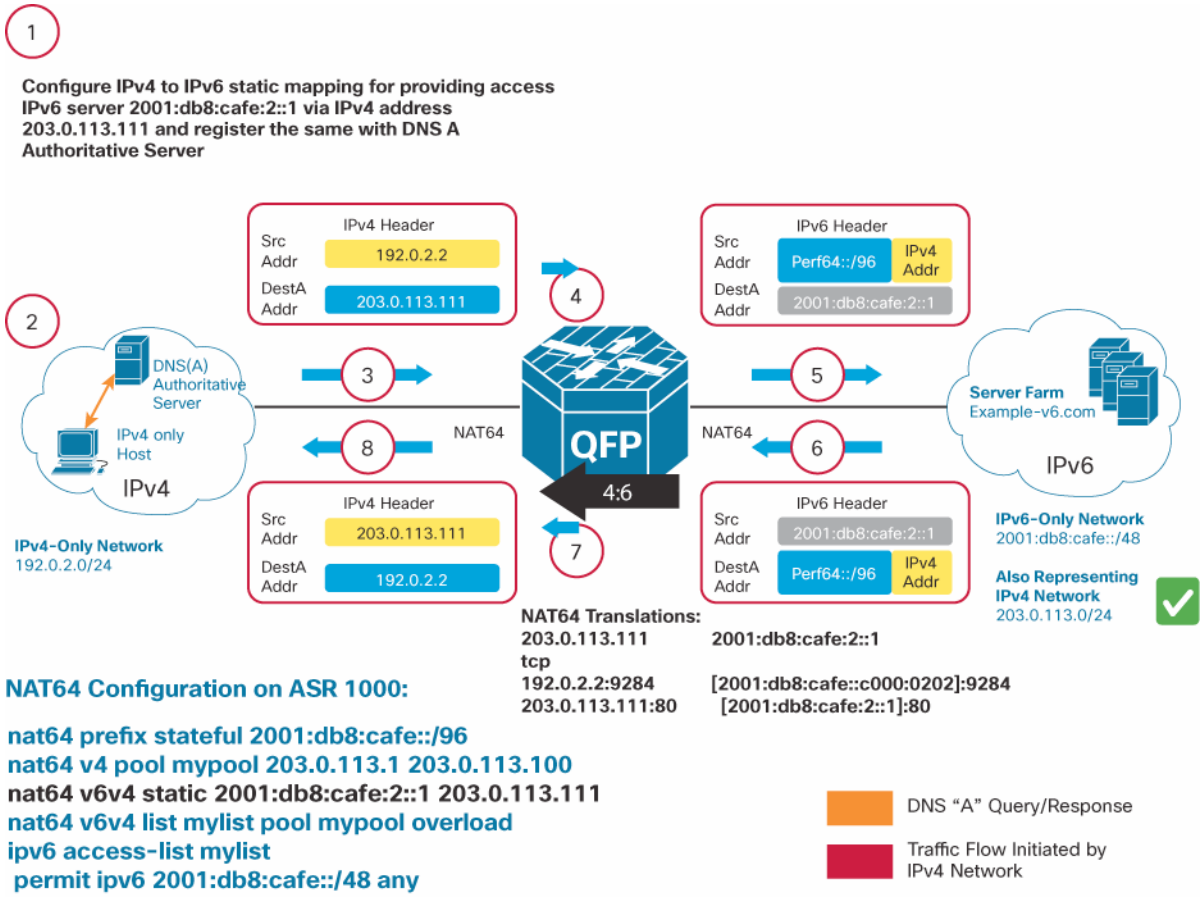
- Nothing changes for the existing users in the IPv6 network; for them, business continuity remains as usual.
- Enterprises and ISPs can provide services to IPv6-only users over the IPv6 Internet and network using native IPv6 transport.
- In addition, they can provide services transparently to IPv4-only users connected through the IPv4 Internet and network.
- IPv4-only hosts can access IPv6-only contents transparently over native IPv4 by using stateful NAT64 translation at the content provider's edge network.

Figure 14. Providing Services to the Existing IPv4 Internet



Example-v6.com is an upcoming content provider offering services to users over the IPv4 Internet as well as the IPv6 Internet. Figure 15 summarizes the steps required for NAT64 translation on a Cisco ASR 1000 Series router running stateful NAT64.

Figure 15. Cisco ASR 1000 Series Router Translating IPv4 Traffic to IPv6 and IPv6 Traffic to IPv4



1. Configure IPv6-to-IPv4 static mapping to provide access to IPv6 server 2001:db8:cafe:2::1 through IPv4 address 203.0.113.111. Also register IPv4 address 203.0.113.111 as a DNS A resource record for example-v6.com with the DNS A authoritative server.

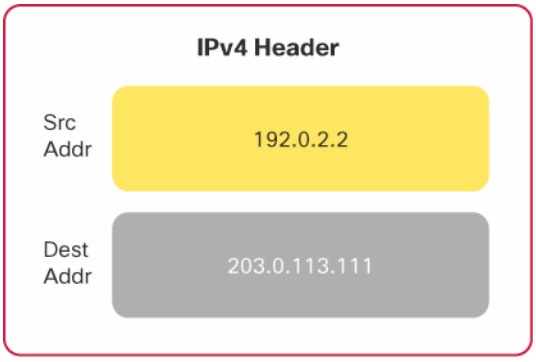
   The following NAT64 translation state is created after static IPv4-to-IPv6 mapping is configured: nat64 v6v4 static 2001:db8:cafe:2::1 203.0.113.111. Thus, IPv6 address 2001:db8:cafe:2::1 statically disguises IPv4 address 203.0.113.111.

   NAT64 Translations:
   203.0.113.111 2001:db8:cafe:2::1

2. The IPv4-only host triggers a DNS query (A: example-v6.com) to its DNS authoritative server to access a service. The DNS authoritative server responds with an A response for domain example-v6.com.

3. The IPv4-only host connects to the service hosted by example-v6.com using the IPv4 address received in the A DNS response (Figure 16).

Figure 16. IP Source and Destination Address Used by IPv4-Only Host



4. The Cisco ASR 1000 Series router running NAT64 receives the IPv6 packet sent by the host on the NAT64-enabled interface and performs the following tasks:

   a. The IPv4 header is translated into an IPv6 header.

   b. The IPv4 destination address is translated into an IPv6 address using the existing NAT64 translation state.

   c. The IPv4 source address is translated into an IPv6 source address by adding the IPv6 stateful NAT64 prefix.

5. After NAT64 translation, the translated IPv6 packet is forwarded by the usual IPv6 route lookup to its destination, example-v6.com IPv6 content server.

6. The IPv6 server hosting service offered by domain example-v6.com replies to the NAT64-enabled IPv6 interface on the Cisco ASR 1000 Series router.

7. The Cisco ASR 1000 Series router running NAT64 receives the IPv6 packet sent by the IPv6 server on the NAT64-enabled interface and performs the following tasks:

   a. The IPv6 header is translated into an IPv4 header.

   b. The IPv6 source address is translated into an IPv4 address using the existing NAT64 translation state.

   c. The IPv6 destination address is translated into an IPv4 destination address by removing the IPv6 stateful NAT64 prefix.

   NAT64 Translations:
   203.0.113.111 2001:db8:cafe:2::1
   tcp
   192.0.2.2:9284 [2001:db8:cafe::c000:0202]:9284
   203.0.113.111:80 [2001:db8:cafe:2::1]:80

8. After translation, the IPv4 packets are forwarded using normal IPv4 route lookup.

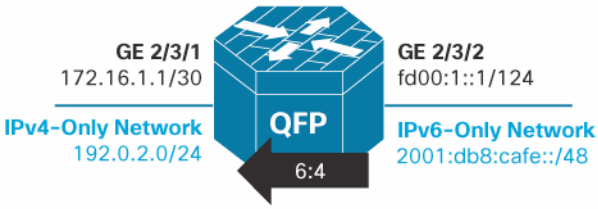
Thus, transparent communication is established between an IPv4-only host and an IPv6-only server using stateful NAT64 translation at the content provider's edge.

Configuration and Troubleshooting

Configuration for Stateful NAT64 Translation

Figure 17 shows the configuration for stateful NAT64 translation.

Figure 17. Configuration for Stateful NAT64 Translation



NAT64 Configuration (*Applicable to scenarios: IPv6 network to IPv4 Internet and IPv4 Internet to IPv6 network*):

```
nat64 prefix stateful 2001:db8:cafe::/96
nat64 v4 pool mypool 203.0.113.1 203.0.113.100
nat64 v6v4 static 2001:db8:cafe:2::1 203.0.113.111
nat64 v6v4 list mylist pool mypool overload
ipv6 access-list mylist
 permit ipv6 2001:db8:cafe::/48 any
```

NAT64 Configuration (*Applicable to scenario: IPv6 Internet to IPv4 Network*):

```
nat64 prefix stateful 2001:db8:cafe::/96
nat64 v4 pool mypool 203.0.113.1 203.0.113.100
nat64 v4v6 static 192.0.2.1 2001:db8:cafe::101
nat64 v6v4 list mylist pool mypool overload
ipv6 access-list mylist
 permit ipv6 any host 2001:db8:cafe::101
```

Interface Configuration:
(*Required in all the NAT64 scenarios*)

```
!
ipv6 unicast-routing
! Enable IPv6 Unicast Routing
interface GigabitEthernet2/3/1
 description Connected to IPv4_Network
 ip address 172.16.1.1 255.255.255.252
 nat64 enable (Enable NAT64 processing on
 this interface)
!
interface GigabitEthernet2/3/2
 description Connected to IPv6_Network
 ipv6 address fd00:1::1/124
 ipv6 enable (Enable IPv6 processing)
 ipv6 rip 1 enable
 nat64 enable (Enable NAT64 processing on
 this interface)
!
router rip
 redistribute static (Optional: Redistribute
 IPv4 static routes into IGP)
 network 172.16.0.0
!
ipv6 router rip 1
 redistribute static (Optional: Redistribute
IPv6 static routes into IGP)
!
```

Verifying NAT64 Translation

The following ICMP NAT64 translations were performed on Cisco ASR 1000 Series router (Figure18):

1. Ping 2001:db8:cafe::0808:0808, representing IPv4 address 8.8.8.8 from IPv6 host 2001:db8:cafe:2::2. This translation is depicted in scenarios 1 and 5 in this document.
2. Ping 2001:db8:cafe::101, representing IPv4 server 192.0.2.1 from IPv6 host 2001:db8:cafe:2::2. This translation is depicted in scenario 3 in this document.
3. Ping 203.0.113.111, representing IPv6 address 2001:db8:cafe:2::1 from IPv4 host 192.0.2.250. This translation is depicted in scenarios 2 and 6 in this document.

Figure 18. Before and After NAT64 Translation

Before NAT64 Translation
(Displaying Static NAT64 Entries Created Through Configuration)

```
ASR1000#show nat64 translations

Proto Original IPv4       Translated IPv4
      Translated IPv6     Original IPv6
------------------------------------------------------------
      203.0.113.111       2001:db8:cafe:2::1
---   192.0.2.1           2001:db8:cafe::101
Total number of translations: 2
ASR1000#
```

After NAT64 Translation
(Displaying Both Dynamically and Statically Created NAT64 Entries)

```
ASR1000#show nat64 translations

Proto Original IPv4       Translated IPv4
      Translated IPv6     Original IPv6
------------------------------------------------------------
      203.0.113.111       2001:db8:cafe:2::1
---   192.0.2.1           2001:db8:cafe::101

icmp  8.8.8.8:2           [2001:db8:cafe::0808:0808]:5321
      203.0.113.1:2       [2001:db8:cafe:2::2]:5321

icmp  192.0.2.1:1         [2001:db8:cafe::101]:1439
      203.0.113.1:1       [2001:db8:cafe:2::2]:1439

icmp  192.0.2.250:14      [2001:db8:cafe::c000:2fa]:14
      203.0.113.111:14    [2001:db8:cafe:2::1]:14
Total number of translations: 5
ASR1000#
```

1
2
3

Products Supporting NAT64

Table 4 lists Cisco products that support NAT64.

Table 4. Cisco Products That Support NAT64

	Cisco ASR 1000 Series	Cisco Carrier Routing System (CRS-1)
Stateless NAT64	Cisco IOS® XE 3.2S	Cisco IOS XR 3.9.3
Stateful NAT64	Cisco IOS XE 3.4S	Cisco IOS XR 4.1.2

Supported Features and RFC Standards

NAT64 supports the features and RFC standards listed in Table 5.

Table 5. Supported Features and RFC Standards

Supported Features	RFC Standards
TCP (HTTP, HTTPS, etc)	RFC 6052 (draft-ietf-behave-address-format)
UDP	RFC 6144 (draft-ietf-behave-v6v4-framework)
ICMP	RFC 6145 (draft-ieft-behave-v6v4-xlate)
FTP64-ALG	RFC 6146 (draft-ietf-behave-v6v4-xlate-stateful)

For More Information

For additional information about Cisco solutions, consult the following resources:

- For more information about IPv6, visit http://www.cisco.com/go/ipv6.
- For additional white papers about IPv6, visit http://www.cisco.com/en/US/products/ps6553/prod_white_papers_list.html.
- For more information about Cisco CRS-1, visit http://www.cisco.com/go/crs.
- For more information about the Cisco ASR 1000 Series, visit http://www.cisco.com/go/asr.
- For more information about Cisco service provider solutions, visit http://www.cisco.com/go/sp.

You can also contact your local Cisco account representative.

You can also consult the relevant RFC standards, listed in Table 6.

Table 6. RFC Standards

RFC	Title
RFC 6052	IPv6 Addressing of IPv4/IPv6 Translators
RFC 6144	Framework for IPv4/IPv6 Translation
RFC 6145	IP/ICMP Translation Algorithm
RFC 6146	Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
RFC 6147	DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers
RFC 4966	Reasons to Move the Network Address Translator—Protocol Translator (NAT-PT) to Historic Status

You may also find the following resources useful:

- IPv4 exhaustion counter: http://inetcore.com/project/ipv4ec/index_en.html
- ARIN: The IANA IPv4 Address Free Pool Is Now Depleted: https://www.arin.net/knowledge/v4-v6.html
- APNIC IPv4 exhaustion: http://www.apnic.net/community/ipv6-program/ipv4-exhaustion
- North American Network Operators' Group: http://www.nanog.org/
- RIPE Network Coordination Centre: http://www.ripe.net/

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-676278-02 04/12