目 录

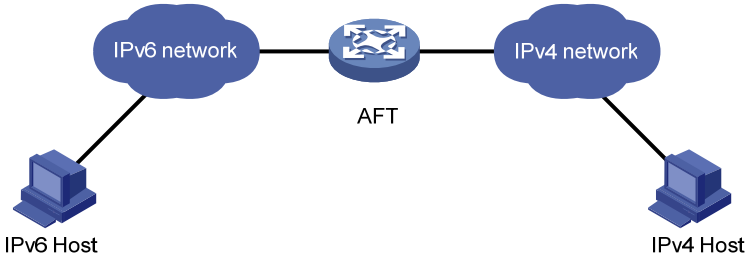
1 AFT

1.1 AFT简介

AFT（Address Family Translation，地址族转换）提供了 IPv4 和 IPv6 地址之间的相互转换功能。在 IPv4 网络完全过渡到 IPv6 网络之前，两个网络之间直接的通信可以通过 AFT 来实现。例如，使用 AFT 可以使 IPv4 网络中的主机直接访问 IPv6 网络中的 FTP 服务器。

如 图 1-1 所示，AFT作用于IPv4 和IPv6 网络边缘设备上，所有的地址转换过程都在该设备上实现，对IPv4 和IPv6 网络内的用户来说是透明的，即用户不必改变目前网络中主机的配置就可实现IPv6 网络与IPv4 网络的通信。

图1-1 AFT 应用场景



1.2 AFT转换方式

AFT 的地址转换分为静态转换、动态转换、前缀转换及 IPv6 内部服务器方式。

1.2.1 静态转换

静态转换方式是指采用手工配置的 IPv6 地址与 IPv4 地址的一一对应关系来实现 IPv6 地址与 IPv4 地址的转换。

1.2.2 动态转换

动态转换方式是指动态地创建 IPv6 地址与 IPv4 地址的对应关系来实现 IPv6 地址与 IPv4 地址的转换。和静态转换方式不同，动态转换方式中 IPv6 和 IPv4 地址之间不存在固定的一一对应关系。

将 IPv6 报文的源 IPv6 地址转换为 IPv4 地址时，动态转换方式分为 NO-PAT 和 PAT 两种模式。

1. NO-PAT模式

NO-PAT（Not Port Address Translation，非端口地址转换）模式下，一个 IPv4 地址同一时间只能对应一个 IPv6 地址进行转换，不能同时被多个 IPv6 地址共用。当使用某 IPv4 地址的 IPv6 网络用户停止访问 IPv4 网络时，AFT 会将其占用的 IPv4 地址释放并分配给其他 IPv6 网络用户使用。

该模式下，AFT 设备只对报文的 IP 地址进行 AFT 转换，同时会建立一个 NO-PAT 表项用于记录 IPv6 地址和 IPv4 地址的映射关系，并不涉及端口转换，可支持所有 IP 协议的报文。

2. PAT模式

PAT（Port Address Translation，端口地址转换）模式下，一个 IPv4 地址可以同时被多个 IPv6 地址共用。该模式下，AFT 设备需要对报文的 IP 地址和传输层端口同时进行转换，且只支持 TCP、UDP 和 ICMPv6（Internet Control Message Protocol for IPv6，IPv6 互联网控制消息协议）查询报文。

PAT 模式的动态转换策略支持对端口块大小进行限制，从而达到限制转换和溯源的目的。可划分的端口号范围为 1024～65535，剩余不足划分的部分则不会进行分配。IPv6 主机首次发起连接时，为该地址分配一个用于转换的 IPv4 地址，以及该 IPv4 地址的一个端口块。后续从该 IPv6 主机发起的连接都使用这个 IPv4 地址和端口块里面的端口进行转换，直到端口块里面的端口用尽。

1.2.3 前缀转换

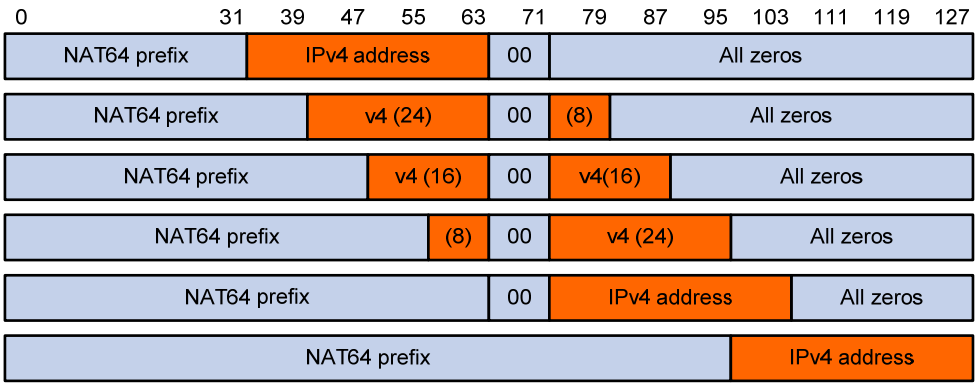
前缀转换包括 NAT64 前缀转换、IVI 前缀转换和 General 前缀转换。

1. NAT64 前缀转换

NAT64 前缀是长度为 32、40、48、56、64 或 96 位的 IPv6 地址前缀，用来构造 IPv4 节点在 IPv6 网络中的地址，以便 IPv4 主机与 IPv6 主机通信。网络中并不存在带有 NAT64 前缀的 IPv6 地址的主机。

如 图 1-2 所示，NAT64 前缀长度不同时，地址转换方法有所不同。其中，NAT64 前缀长度为 32、64 和 96 位时，IPv4 地址作为一个整体添加到IPv6 地址中；NAT64 前缀长度为 40、48 和 56 位时，IPv4 地址被拆分成两部分，分别添加到 64～71 位的前后。

图1-2 对应 IPv4 地址带有 NAT64 前缀的 IPv6 地址格式

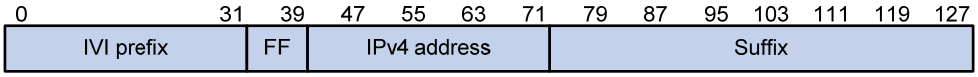


IPv4 侧发起访问时，AFT 利用 NAT64 前缀将报文的源 IPv4 地址转换为 IPv6 地址；IPv6 侧发起访问时，AFT 利用 NAT64 前缀将报文的目的 IPv6 地址转换为 IPv4 地址。

2. IVI前缀转换

IVI前缀是长度为 32 位的IPv6 地址前缀。IVI地址是IPv6 主机实际使用的IPv6 地址，这个IPv6 地址中内嵌了一个IPv4 地址，可以用于与IPv4 主机通信。由IVI前缀构成的IVI地址格式如 图 1-3 所示。

图1-3 IVI 地址格式

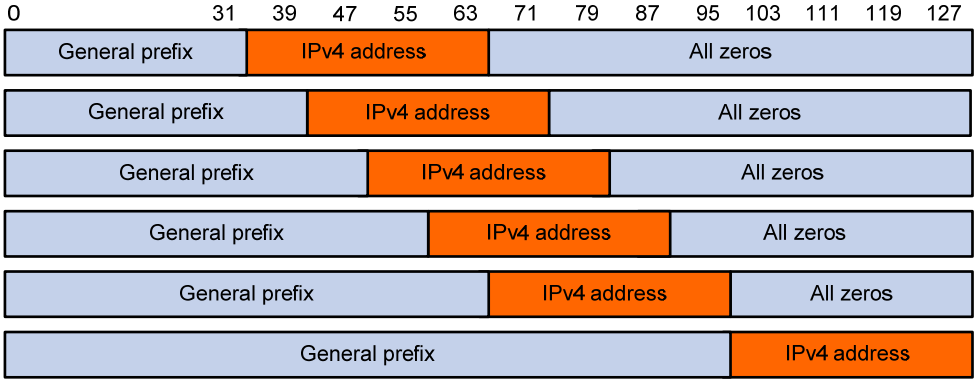


从 IPv6 侧发起访问时，AFT 可以使用 IVI 前缀将报文的源 IPv6 地址转换为 IPv4 地址。

3. General前缀

General前缀与NAT64 前缀类似，都是长度为 32、40、48、56、64 或 96 位的IPv6 地址前缀，用来构造IPv4 节点在IPv6 网络中的地址。如 图 1-4 所示，General前缀与NAT64 前缀的区别在于，General前缀没有 64 到 71 位的 8 位保留位，IPv4 地址作为一个整体添加到IPv6 地址中。

图1-4 对应 IPv4 地址带有 General 前缀的 IPv6 地址格式



从 IPv6 侧发起访问时，AFT 利用 General 前缀将报文的源/目的 IPv6 地址转换为 IPv4 地址。需要注意的是，General 前缀与 NAT64 前缀都不能与设备上的接口地址同网段。

1.2.4 IPv6 内部服务器

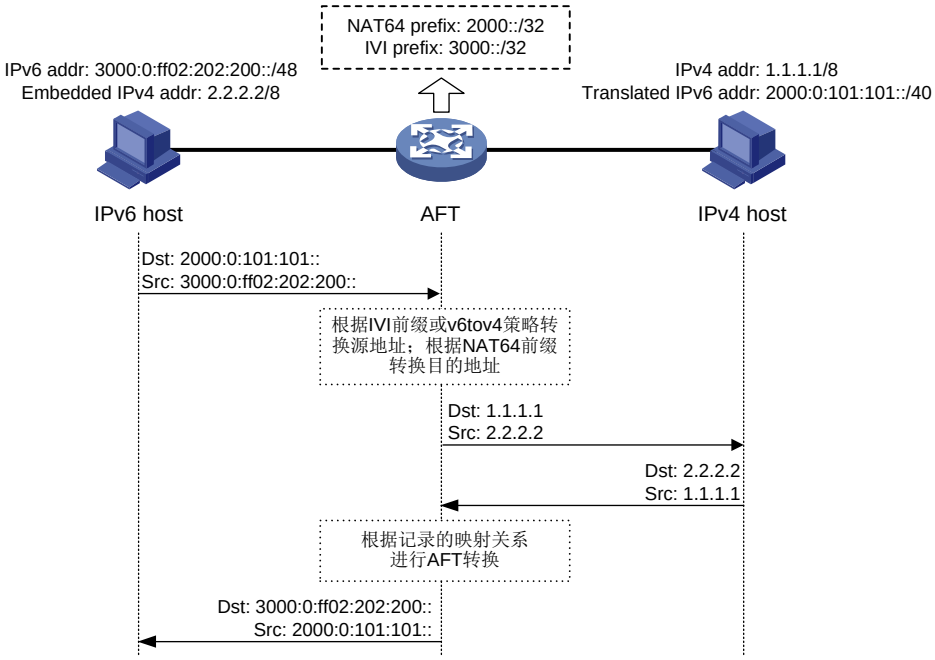
IPv6 内部服务器是指向 IPv4 网络主机提供服务的 IPv6 网络中的服务器。通过配置 IPv6 内部服务器，可以将 IPv6 服务器的地址和端口映射到 IPv4 网络，IPv4 网络中的主机通过访问映射后的 IPv4 地址和端口就可以访问 IPv6 网络中的服务器。

1.3 AFT报文转换过程

IPv6 侧发起访问和 IPv4 侧发起访问的报文转换过程有所不同，下面将分别介绍。

1.3.1 IPv6 侧发起访问

图1-5 IPv6 侧发起访问的 AFT 报文转换过程



如 图 1-5 所示，IPv6 侧发起访问时AFT设备对报文的转换过程为：

(1) 判断是否需要进行 AFT 转换：AFT 设备接收到 IPv6 网络主机（IPv6 host）发送给 IPv4 网络主机（IPv4 host）的报文后，判断该报文是否要转发到 IPv4 网络。如果报文的目的 IPv6 地址能够匹配到 IPv6 目的地址转换策略，则该报文需要转发到 IPv4 网络，需要进行 AFT 转换；如果未匹配到任何一种转换策略，则表示该报文不需要进行 AFT 转换。

(2) 转换报文目的地址：根据 IPv6 目的地址转换策略将报文目的 IPv6 地址转换为 IPv4 地址。

(3) 根据目的地址预查路由：根据转换后的 IPv4 目的地址查找路由表，确定报文的出接口。如果查找失败，则丢弃报文。需要注意的是，预查路由时不会查找策略路由。

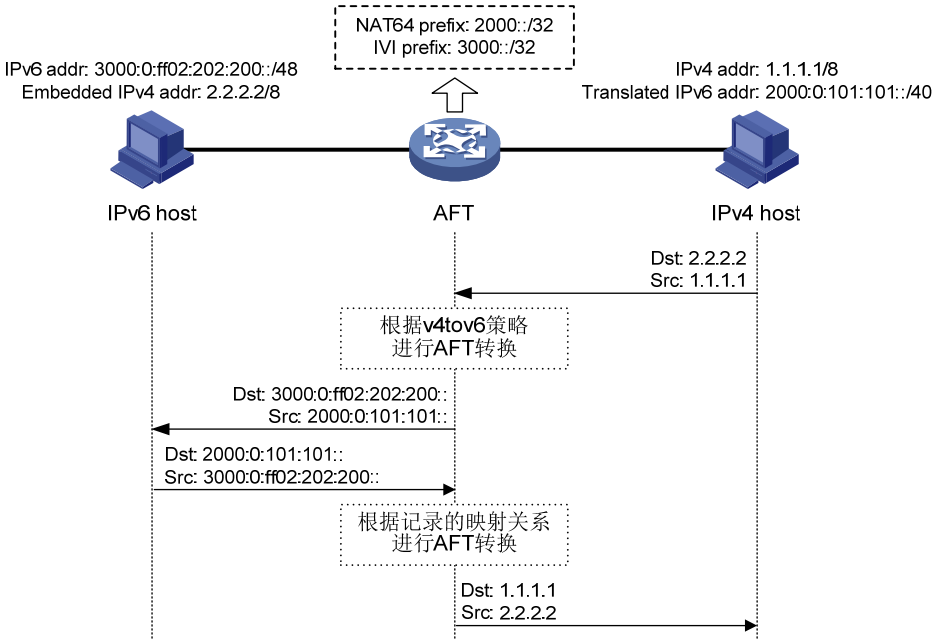
(4) 转换报文源地址：根据 IPv6 源地址转换策略将报文源 IPv6 地址转换为 IPv4 地址。如果未匹配到任何一种转换策略，则报文将被丢弃。

(5) 转发报文并记录映射关系：报文的源 IPv6 地址和目的 IPv6 地址都转换为 IPv4 地址后，设备按照正常的转发流程将报文转发到 IPv4 网络中的主机。同时，将 IPv6 地址与 IPv4 地址的映射关系保存在设备中。

(6) 根据记录的映射关系转发应答报文：IPv4 网络主机发送给 IPv6 网络主机的应答报文到达 AFT 设备后，设备将根据已保存的映射关系进行相反的转换，从而将报文发送给 IPv6 网络主机。

1.3.2 IPv4 侧发起访问

图1-6 IPv4 侧发起访问的 AFT 报文转换过程



如 图 1-6 所示，IPv4 侧发起访问时AFT设备对报文的转换过程为：

(1) 判断是否需要进行 AFT 转换：AFT 设备接收到 IPv4 网络主机（IPv4 host）发送给 IPv6 网络主机（IPv6 host）的报文后，判断该报文是否要转发到 IPv6 网络。如果报文的目的 IPv4 地址能够匹配到 IPv4 目的地址转换策略，则该报文需要转发到 IPv6 网络，需要进行 AFT 转换。如果未匹配到任何一种转换策略，则表示该报文不需要进行 AFT 地址转换。

(2) 转换报文目的地址：根据 IPv4 目的地址转换策略将报文目的 IPv4 地址转换为 IPv6 地址。

(3) 根据目的地址预查路由：根据转换后的 IPv6 目的地址查找路由表，确定报文的出接口。如果查找失败，则丢弃报文。需要注意的是，预查路由时不会查找策略路由。

(4) 转换报文源地址：根据 IPv4 源地址转换策略将报文源 IPv4 地址转换为 IPv6 地址。如果未匹配到任何一种转换策略，则报文将被丢弃。

(5) 转发报文并记录映射关系：报文的源 IPv4 地址和目的 IPv4 地址都转换为 IPv6 地址后，设备按照正常的转发流程将报文转发到 IPv6 网络中的主机。同时，将 IPv4 地址与 IPv6 地址的映射关系保存在设备中。

(6) 根据记录的映射关系转发应答报文：IPv6 网络主机发送给 IPv4 网络主机的应答报文到达 AFT 设备后，设备将根据已保存的映射关系进行相反的转换，从而将报文发送给 IPv4 网络主机。

1.4 AFT支持ALG

AFT 只对报文头中的 IP 地址和端口信息进行转换，不对应用层数据载荷中的字段进行分析。然而对于一些特殊协议，它们的报文的数据载荷中可能包含 IP 地址或端口信息。例如，FTP 应用由数据连接和控制连接共同完成，而数据连接使用的地址和端口由控制连接报文中的载荷信息决定。这

些载荷信息也必须进行有效的转换，否则可能导致功能问题。ALG（Application Level Gateway，应用层网关）主要完成对应用层报文的处理，利用 ALG 可以完成载荷信息的转换。

目前，AFT 支持对 FTP 报文、DNS 报文和 ICMP 差错报文进行 ALG 处理。

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
MSR810、MSR810-W、MSR810-W-DB、MSR810-LM、MSR810-W-LM、MSR810-10-PoE、MSR810-LM-HK、MSR810-W-LM-HK	支持
MSR810-LMS、MSR810-LUS	不支持
MSR810-LMS-EA、MSR810-LME	支持
MSR2600-6-X1、MSR2600-10-X1	支持
MSR 2630	支持
MSR3600-28、MSR3600-51	支持
MSR3600-28-SI、MSR3600-51-SI	不支持
MSR3600-28-X1、MSR3600-28-X1-DP、MSR3600-51-X1、MSR3600-51-X1-DP	支持
MSR3610-I-DP、MSR3610-IE-DP、MSR3610-IE-ES	支持
MSR3610-X1、MSR3610-X1-DP、MSR3610-X1-DC、MSR3610-X1-DP-DC	支持
MSR 3610、MSR 3620、MSR 3620-DP、MSR 3640、MSR 3660	支持
MSR3610-G、MSR3620-G	支持

型号	描述
MSR810-W-WiNet、MSR810-LM-WiNet	支持
MSR830-4LM-WiNet	支持
MSR830-5BEI-WiNet、MSR830-6EI-WiNet、MSR830-10BEI-WiNet	支持
MSR830-6BHI-WiNet、MSR830-10BHI-WiNet	支持
MSR2600-6-WiNet、MSR2600-10-X1-WiNet	支持
MSR2630-WiNet	支持
MSR3600-28-WiNet	支持
MSR3610-X1-WiNet	支持
MSR3610-WiNet、MSR3620-10-WiNet、MSR3620-DP-WiNet、MSR3620-WiNet、MSR3660-WiNet	支持

型号	说明
MSR2630-XS	支持
MSR3600-28-XS	支持

型号	说明
MSR3610-XS	支持
MSR3620-XS	支持
MSR3610-I-XS	支持
MSR3610-IE-XS	支持

1.5 AFT配置任务简介

AFT 配置任务如下：

(1) 开启AFT功能

(2) 配置 IPv6 侧发起的会话的转换配置

- 配置IPv6 到IPv4 的目的地址转换策略
- 配置IPv6 到IPv4 的源地址转换策略
- （可选）配置AFT转换后IPv4 报文的ToS字段值

(3) 配置 IPv4 侧发起的会话的转换配置

- 配置IPv4 到IPv6 目的地址转换策略
- 配置IPv4 到IPv6 源地址转换策略
- （可选）配置AFT转换后IPv6 报文的Traffic Class字段值

(4) （可选）开启AFT日志功能

1.6 开启AFT功能

1. 配置限制和指导

只有在连接 IPv4 网络和 IPv6 网络的接口上都开启 AFT 功能后，才能实现 IPv4 报文和 IPv6 报文之间的相互转换。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 开启 AFT 功能。

aft enable

缺省情况下，AFT 功能处于关闭状态。

1.7 配置IPv6到IPv4的目的地址转换策略

1. 功能简介

IPv6 目的地址转换策略匹配的优先级从高到低为：

(1) IPv4 到 IPv6 的源地址静态转换策略。

(2) General 前缀。

(3) NAT64 前缀。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 IPv6 到 IPv4 的目的地址转换策略。

- 配置 IPv4 到 IPv6 源地址静态转换策略。

  aft v4tov6 source *ipv4-address* [**vpn-instance** *ipv4-vpn-instance-name*] *ipv6-address* [**vpn-instance** *ipv6-vpn-instance-name*]

- 配置 General 前缀。

  aft prefix-general *prefix-general prefix-length*

- 配置 NAT64 前缀。

  aft prefix-nat64 *prefix-nat64 prefix-length*

1.8 配置IPv6到IPv4的源地址转换策略

1. 功能简介

IPv6 源地址转换策略匹配的优先级从高到低为：

(1) IPv6 到 IPv4 的源地址静态转换策略。

(2) General 前缀。

(3) IVI 前缀。

(4) IPv6 到 IPv4 的源地址动态转换策略。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) （可选）配置 AFT 地址组。

a. 创建一个 AFT 地址组，并进入 AFT 地址组视图。

aft address-group *group-id*

在配置 IPv6 到 IPv4 源地址动态转换策略前，根据实际情况选配。

b. 添加地址组成员。

address *start-address end-address*

可通过多次执行本命令添加多个地址组成员。

当前地址组成员的 IP 地址段不能与该地址组中或者其它地址组中已有成员的 IP 地址段重叠。

c. 退回系统视图。

quit

仅 IPv6 到 IPv4 源地址动态转换策略支持本配置。

(3) 配置 IPv6 到 IPv4 的源地址转换策略。

- 配置 IPv6 到 IPv4 源地址静态转换策略。

  aft v6tov4 source *ipv6-address* [**vpn-instance** *ipv6-vpn-instance-name*] *ipv4-address* [**vpn-instance** *ipv4-vpn-instance-name*]

- 配置 IPv6 到 IPv4 源地址动态转换策略。

  aft v6tov4 source { **acl ipv6** { **name** *ipv6-acl-name* | **number** *ipv6-acl-number* } | **prefix-nat64** *prefix-nat64 prefix-length* [**vpn-instance** *ipv6-vpn-instance-name*] } { **address-group** *group-id* [**no-pat** | **port-block-size** *blocksize*] | **interface** *interface-type interface-number* } [**vpn-instance** *ipv4-vpn-instance-name*]

- 配置 General 前缀。

  aft prefix-general *prefix-general prefix-length*

- 配置 IVI 前缀。

  aft prefix-ivi *prefix-ivi*

1.9 配置IPv4到IPv6目的地址转换策略

1.9.1 功能简介

IPv4 目的地址转换策略的匹配优先级从高到低为：

(1) IPv6 内部服务器。

(2) IPv6 到 IPv4 的源地址静态转换策略。

(3) IPv4 到 IPv6 的目的地址动态转换策略。

1.9.2 配置IPv6 内部服务器

(1) 进入系统视图。

system-view

(2) 配置 IPv6 侧服务器对应的 IPv4 地址及端口。

aft v6server protocol *protocol-type ipv4-destination-address ipv4-port-number* [**vpn-instance** *ipv4-vpn-instance-name*] *ipv6-destination-address ipv6-port-number* [**vpn-instance** *ipv6-vpn-instance-name*]

1.9.3 配置IPv6 到IPv4 的源地址静态转换策略

(1) 进入系统视图。

system-view

(2) 配置 IPv6 到 IPv4 源地址静态转换策略。

aft v6tov4 source *ipv6-address* [**vpn-instance** *ipv6-vpn-instance-name*] *ipv4-address* [**vpn-instance** *ipv4-vpn-instance-name*]

1.9.4 配置IPv4 到IPv6 的目的地址动态转换策略。

(1) 进入系统视图。

system-view

(2) 配置 IVI 前缀或 General 前缀。请选择其中一项进行配置。

- 配置 IVI 前缀。

  aft prefix-ivi *prefix-ivi*

- 配置 General 前缀。

  aft prefix-general *prefix-general prefix-length*

(3) 配置 IPv4 到 IPv6 目的地址动态转换策略。

aft v4tov6 destination acl { **name** *ipv4-acl-name* **prefix-ivi** *prefix-ivi* [**vpn-instance** *ipv6-vpn-instance-name*] | **number** *ipv4-acl-number* { **prefix-general** *prefix-general prefix-length* | **prefix-ivi** *prefix-ivi* [**vpn-instance** *ipv6-vpn-instance-name*] } }

引用 IVI 前缀或 General 前缀之前，需要先进行 IVI 前缀或 General 前缀的配置，转换策略才能生效。

1.10 配置IPv4到IPv6源地址转换策略

1.10.1 功能简介

IPv4 源地址转换策略的匹配优先级从高到低为：

(1) IPv4 到 IPv6 的源地址静态转换策略。

(2) IPv4 到 IPv6 的源地址动态转换策略。

(3) NAT64 前缀。

1.10.2 配置IPv4 到IPv6 的源地址静态转换策略

(1) 进入系统视图。

system-view

(2) 配置 IPv4 到 IPv6 源地址静态转换策略。

aft v4tov6 source *ipv4-address* [**vpn-instance** *ipv4-vpn-instance-name*] *ipv6-address* [**vpn-instance** *ipv6-vpn-instance-name*]

1.10.3 配置IPv4 到IPv6 的源地址动态转换策略

(1) 进入系统视图。

system-view

(2) 配置 NAT64 前缀或 General 前缀。请选择其中一项进行配置。

- 配置 NAT64 前缀。

  aft prefix-nat64 *prefix-nat64 prefix-length*

- 配置 General 前缀。

  aft prefix-general *prefix-general prefix-length*

(3) 配置 IPv4 到 IPv6 源地址动态转换策略。

aft v4tov6 source acl { **name** *ipv4-acl-name* **prefix-nat64** *prefix-nat64 prefix-length* [**vpn-instance** *ipv6-vpn-instance-name*] | **number** *ipv4-acl-number* { **prefix-general** *prefix-general prefix-length* | **prefix-nat64** *prefix-nat64 prefix-length* [**vpn-instance** *ipv6-vpn-instance-name*] } }

引用 NAT64 前缀或 General 前缀之前，需要先进行 NAT64 前缀或 General 前缀的配置，转换策略才能生效。

1.10.4 配置NAT64 前缀

(1) 进入系统视图。

system-view

(2) 配置 NAT64 前缀。

aft prefix-nat64 *prefix-nat64 prefix-length*

1.11 配置AFT转换后IPv4报文的ToS字段值

1. 功能简介

用户可以设置在进行 AFT 转换后，IPv4 报文中 ToS 字段的取值：

- 为 0：表示将转换后报文的服务优先级降为最低。
- 与转换前对应的 ToS 字段取值相同：表示保持原有的服务优先级。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 IPv6 报文转换为 IPv4 报文后，IPv4 报文的 ToS 字段值为 0。

aft turn-off tos

缺省情况下，当 IPv6 报文转换为 IPv4 报文后，IPv4 报文中的 ToS 字段与转换前的 IPv6 报文的 Traffic Class 字段值相同。

1.12 配置AFT转换后IPv6报文的Traffic Class字段值

1. 功能简介

用户可以设置在 AFT 转换后，IPv6 报文中 Traffic Class 字段的取值：

- 为 0：表示将转换后报文的服务优先级降为最低。
- 与转换前对应的 Traffic Class 字段取值相同：表示保持原有的服务优先级。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 IPv4 报文转换为 IPv6 报文后，IPv6 报文的 Traffic Class 字段值为 0。

aft turn-off traffic-class

缺省情况下，当 IPv4 报文转换为 IPv6 报文后，IPv6 报文中的 Traffic Class 字段与转换前的 IPv4 报文的 ToS 字段值相同。

1.13 开启AFT日志功能

1. 功能简介

为了满足网络管理员安全审计的需要，可以开启 AFT 日志功能，以便对 AFT 连接（AFT 连接是指报文经过设备时，源或目的地址进行过 AFT 转换的连接）信息进行记录。在以下情况下会触发记录 AFT 日志：

- AFT 端口块新建。
- AFT 端口块删除。
- AFT 流创建，即 AFT 会话创建时输出日志。
- AFT 流删除，即 AFT 会话释放时输出日志。

生成的日志信息将被发送到设备的信息中心，通过设置信息中心的参数，决定日志信息的输出规则（即是否允许输出以及输出方向）。有关信息中心参数的配置请参见“网络管理和监控配置指导”中的“信息中心”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 AFT 日志功能。

aft log enable

缺省情况下，AFT 日志功能处于关闭状态。

配置本命令后，将记录 AFT 端口块新建和 AFT 端口块删除的日志信息。

(3) （可选）开启 AFT 流创建或流删除的日志功能。

- 开启 AFT 流创建的日志功能。

  aft log flow-begin

  缺省情况下，AFT 新建流的日志功能处于关闭状态。

  如需记录 AFT 会话创建时的日志信息，则需要配置本命令。只有配置 **aft log enable** 命令之后，本命令才能生效。

- 开启 AFT 流删除的日志功能。

  aft log flow-end

  缺省情况下，AFT 删除流的日志功能处于关闭状态。

  如需记录 AFT 会话释放时的日志信息，则需要配置本命令。只有配置 **aft log enable** 命令之后，本命令才能生效。

1.14 AFT显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 AFT 配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以删除 AFT 会话或统计信息。

表1-1 AFT 显示和维护

操作	命令
显示AFT配置信息	**display aft configuration**
显示地址组信息	**display aft address-group** [*group-id*]
显示AFT地址映射信息	（独立运行模式） **display aft address-mapping** （IRF模式） **display aft address-mapping** [**slot** *slot-number*]
显示AFT NO-PAT表项信息	（独立运行模式） **display aft no-pat** （IRF模式） **display aft no-pat** [**slot** *slot-number*]
显示AFT端口块映射表项信息	（独立运行模式） **display aft port-block** （IRF模式） **display aft port-block** [**slot** *slot-number*]
显示AFT会话	（独立运行模式） **display aft session ipv4** [{ **source-ip** *source-ip-address* | **destination-ip** *destination-ip-address* } * [**vpn-instance** *ipv4-vpn-instance-name*]] [**verbose**] **display aft session ipv6** [{ **source-ip** *source-ipv6-address* | **destination-ip** *destination-ipv6-address* } * [**vpn-instance** *ipv6-vpn-instance-name*]] [**verbose**] （IRF模式） **display aft session ipv4** [{ **source-ip** *source-ip-address* | **destination-ip** *destination-ip-address* } * [**vpn-instance** *ipv4-vpn-instance-name*]] [**slot** *slot-number*] [**verbose**] **display aft session ipv6** [{ **source-ip** *source-ipv6-address* | **destination-ip** *destination-ipv6-address* } * [**vpn-instance** *ipv6-vpn-instance-name*]] [**slot** *slot-number*] [**verbose**]
显示AFT统计信息	（独立运行模式） **display aft statistics** （IRF模式） **display aft statistics** [**slot** *slot-number*]

操作	命令
删除AFT会话	（独立运行模式） **reset aft session** （IRF模式） **reset aft session** [**slot** *slot-number*]
删除AFT统计信息	（独立运行模式） **reset aft statistics** （IRF模式） **reset aft statistics** [**slot** *slot-number*]

1.15 AFT典型配置举例

1.15.1 IPv6 网络访问IPv4 Internet配置举例

1. 组网需求

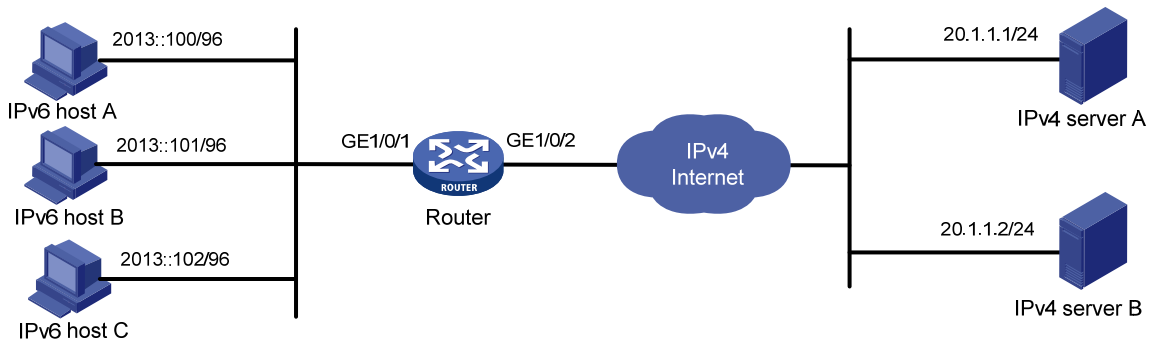
某公司将网络升级到了 IPv6，但是仍然希望内网 2013::/96 网段的用户可以访问 IPv4 Internet，其它网段的用户不能访问 IPv4 Internet。该公司访问 IPv4 Internet 使用的 IPv4 地址为 10.1.1.1、10.1.1.2 和 10.1.1.3。

为满足上述需求，本例中实现方式如下：

- 使用 NAT64 前缀与 IPv4 网络中的主机地址组合成为 IPv6 地址，此 IPv6 地址将与 IPv4 Internet 内的主机建立相应的映射关系，IPv6 网络中的主机访问该 IPv6 地址即可实现对 IPv4 Internet 的访问。报文到达 Router 后，设备将根据 NAT64 前缀将该目的 IPv6 地址转换为对应的 IPv4 地址。
- 使用 IPv6 到 IPv4 源地址动态转换策略将 IPv6 网络到 IPv4 网络报文的源地址转换为 IPv4 地址 10.1.1.1、10.1.1.2 或 10.1.1.3。

2. 组网图

图1-7 IPv6 网络访问 IPv4 Internet 配置组网图



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

配置地址组 0 包含三个 IPv4 地址 10.1.1.1、10.1.1.2 和 10.1.1.3。

```
<Router> system-view
[Router] aft address-group 0
[Router-aft-address-group-0] address 10.1.1.1 10.1.1.3
[Router-aft-address-group-0] quit
```

配置 IPv6 ACL 2000，该 ACL 用来匹配源 IPv6 地址属于 2013::/96 网段的报文。

```
[Router] acl ipv6 basic 2000
[Router-acl-ipv6-basic-2000] rule permit source 2013:: 96
[Router-acl-ipv6-basic-2000] rule deny
[Router-acl-ipv6-basic-2000] quit
```

配置 IPv6 到 IPv4 的源地址动态转换策略，将匹配 ACL 2000 的 IPv6 报文源地址转换为地址组 0 中的地址，即将 2013::/96 网段内主机所发送报文的源 IPv6 地址转换为 IPv4 地址 10.1.1.1、10.1.1.2 或 10.1.1.3。

```
[Router] aft v6tov4 source acl ipv6 number 2000 address-group 0
```

配置 NAT64 前缀为 2012::/96，报文的目的地址根据该 NAT64 前缀转换为 IPv4 地址。

```
[Router] aft prefix-nat64 2012:: 96
```

在 IPv6 侧接口 GigabitEthernet1/0/1 开启 AFT 功能。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] aft enable
[Router-GigabitEthernet1/0/1] quit
```

在 IPv4 侧接口 GigabitEthernet1/0/2 开启 AFT 功能。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] aft enable
[Router-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，检查 IPv6 Host 与 IPv4 Server 的连通性。以 IPv6 host A ping IPv4 server A 为例：

```
D:\>ping 2012::20.1.1.1
Pinging 2012::20.1.1.1 with 32 bytes of data:
Reply from 2012::20.1.1.1: time=3ms
Reply from 2012::20.1.1.1: time=3ms
Reply from 2012::20.1.1.1: time=3ms
Reply from 2012::20.1.1.1: time=3ms
```

通过查看 AFT 会话，可以看到创建了一个 IPv6 会话和 IPv4 会话，分别对应转换前和转换后的报文。

```
[Router] display aft session ipv6 verbose
Initiator:
  Source      IP/port: 2013::100/0
  Destination IP/port: 2012::1401:0101/32768
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/1
Responder:
  Source      IP/port: 2012::1401:0101/0
  Destination IP/port: 2013::100/33024
  VPN instance/VLAN ID/Inline ID: -/-/-
```

```
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/2
State: ICMPV6_REPLY
Application: OTHER
Start time: 2014-03-13 08:52:59  TTL: 23s
Initiator->Responder:            4 packets        320 bytes
Responder->Initiator:            4 packets        320 bytes

Total sessions found: 1

[Router] display aft session ipv4 verbose
Initiator:
  Source      IP/port: 10.1.1.1/1025
  Destination IP/port: 20.1.1.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
Responder:
  Source      IP/port: 20.1.1.1/1025
  Destination IP/port: 10.1.1.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
State: ICMP_REPLY
Application: OTHER
Start time: 2014-03-13 08:52:59  TTL: 27s
Initiator->Responder:            4 packets        240 bytes
Responder->Initiator:            4 packets        240 bytes

Total sessions found: 1
```

1.15.2 IPv4 Internet访问IPv6 网络内部服务器配置举例

1. 组网需求

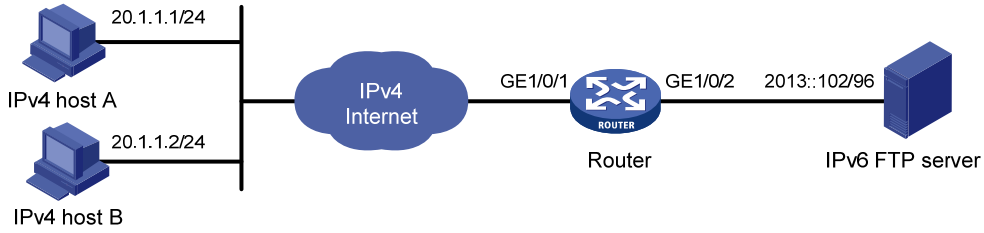
某公司将网络升级到了 IPv6，此时 Internet 仍然是 IPv4 网络。该公司希望内部的 FTP 服务器能够继续为 IPv4 Internet 的用户提供服务。该公司拥有的 IPv4 地址为 10.1.1.1。

为满足上述要求，本例实现方式如下：

- 使用 IPv6 侧服务器配置将 IPv6 内部服务器的地址及端口映射为 IPv4 地址及端口，Router 收到来自 IPv4 Internet 的报文后，根据该配置策略将报文 IPv4 目的地址转换为 IPv6 地址；
- 使用 NAT64 前缀将报文源 IPv4 地址转换为 IPv6 地址。

2. 组网图

图1-8 IPv4 Internet 访问 IPv6 网络内部服务器配置组网图



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

配置 IPv6 侧服务器对应的 IPv4 地址及端口号。IPv4 网络内用户通过访问该 IPv4 地址及端口即可访问 IPv6 服务器。

```
<Router> system-view
[Router] aft v6server protocol tcp 10.1.1.1 21 2013::102 21
```

报文的源地址将根据配置的 NAT64 前缀转换为 IPv6 地址。

```
[Router] aft prefix-nat64 2012:: 96
```

在 IPv4 侧接口 GigabitEthernet1/0/1 开启 AFT。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] aft enable
[Router-GigabitEthernet1/0/1] quit
```

在 IPv6 侧接口 GigabitEthernet1/0/2 开启 AFT。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] aft enable
[Router-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，IPv4 Host 可以通过 FTP 协议访问 IPv6 FTP Server。

通过查看 AFT 会话，可以看到创建了一个 IPv4 会话和 IPv6 会话，分别对应转换前和转换后的报文。

```
[Router] display aft session ipv4 verbose
Initiator:
  Source      IP/port: 20.1.1.1/11025
  Destination IP/port: 10.1.1.1/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
Responder:
  Source      IP/port: 10.1.1.1/21
  Destination IP/port: 20.1.1.1/11025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
```

```
  Inbound interface: GigabitEthernet1/0/2
State: TCP_ESTABLISHED
Application: FTP
Start time: 2014-03-13 09:07:30  TTL: 3577s
Initiator->Responder:            3 packets        124 bytes
Responder->Initiator:            2 packets        108 bytes

Total sessions found: 1

[Router] display aft session ipv6 verbose
Initiator:
  Source      IP/port: 2012::1401:0101/1029
  Destination IP/port: 2013::102/21
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
Responder:
  Source      IP/port: 2013::102/21
  Destination IP/port: 2012::1401:0101/1029
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
State: TCP_ESTABLISHED
Application: FTP
Start time: 2014-03-13 09:07:30  TTL: 3582s
Initiator->Responder:            3 packets        184 bytes
Responder->Initiator:            2 packets        148 bytes

Total sessions found: 1
```

1.15.3 IPv4 网络和IPv6 网络互访配置举例

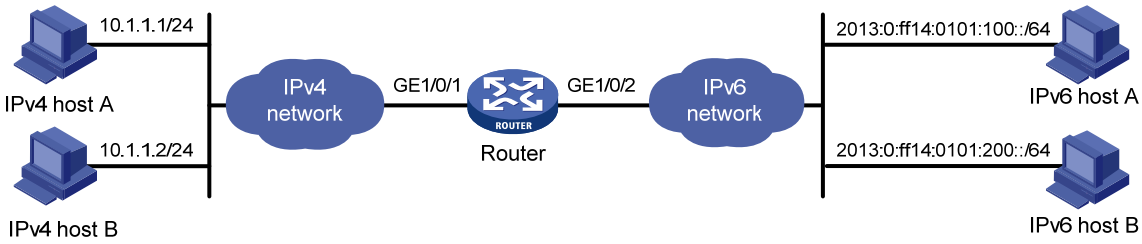
1. 组网需求

某公司内部同时部署了 IPv4 网络和 IPv6 网络，并且希望 IPv4 网络和 IPv6 网络能够互相访问。为满足上述需求，本例中使用如下方式实现：

- 为 IPv6 网络分配一个 IVI 前缀和 IPv4 网段，IPv6 网络中所有 IPv6 主机的地址均配置为由 IVI 前缀和 IPv4 网段中地址组合而成的 IPv6 地址。
- 为 IPv4 网络分配一个 NAT64 前缀，IPv4 网络主动访问 IPv6 网络时，IPv4 源地址使用 NAT64 前缀转换为 IPv6 地址；IPv6 网络主动访问 IPv4 网络时，目的地址使用 NAT64 前缀和 IPv4 地址组合成的 IPv6 地址。

2. 组网图

图1-9 IPv4 网络和 IPv6 网络互访配置组网图



3. 配置步骤

按照组网图配置各接口的 IP 地址，其中 IPv6 网络中的主机使用的 IPv6 地址根据 IVI 前缀 2013::/32 和 20.1.1.0/24 组合而成。具体配置过程略。

配置 ACL 2000 用来过滤需要访问 IPv6 网络的用户，同时匹配该 ACL 2000 的报文的目的地址将会根据配置的 IVI 前缀转换为 IPv6 地址。此处所有 IPv4 网络用户均需要访问 IPv6 网络。

```
<Router> system-view
[Router] acl basic 2000
[Router-acl-ipv4-basic-2000] rule permit
[Router-acl-ipv4-basic-2000] quit
```

配置 NAT64 前缀，用于进行 IPv4 到 IPv6 的源地址转换和 IPv6 到 IPv4 的目的地址转换。

```
[Router] aft prefix-nat64 2012:: 96
```

配置 IVI 前缀，用于进行 IPv6 到 IPv4 源地址转换，且在 IPv4 到 IPv6 动态目的地址转换策略中引用该前缀。

```
[Router] aft prefix-ivi 2013::
```

配置 IPv4 到 IPv6 动态目的地址转换策略，IPv4 到 IPv6 报文的目的 IPv4 地址转换为 IPv6 地址。

```
[Router] aft v4tov6 destination acl number 2000 prefix-ivi 2013::
```

在 IPv4 侧接口 GigabitEthernet1/0/1 开启 AFT。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] aft enable
[Router-GigabitEthernet1/0/1] quit
```

在 IPv6 侧接口 GigabitEthernet1/0/2 开启 AFT。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] aft enable
[Router-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，IPv4 host 与 IPv6 host 可以互通。以 IPv6 host A ping IPv4 host A 为例：

```
D:\>ping 2012::a01:0101
Pinging 2012::a01:0101 with 32 bytes of data:
Reply from 2012::a01:0101: time=3ms
Reply from 2012::a01:0101: time=3ms
Reply from 2012::a01:0101: time=3ms
Reply from 2012::a01:0101: time=3ms
```

通过查看 AFT 会话，可以看到创建了一个 IPv6 会话和 IPv4 会话，分别对应转换前和转换后的报文。显示内容如下：

```
[Router] display aft session ipv6 verbose
Initiator:
  Source      IP/port: 2013:0:FF14:0101:0100::/0
  Destination IP/port: 2012::0a01:0101/32768
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/2
Responder:
  Source      IP/port: 2012::0a01:0101/0
  Destination IP/port: 2013:0:FF14:0101:0100::/33024
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/1
State: ICMPV6_REPLY
Application: OTHER
Start time: 2014-03-13 08:52:59  TTL: 23s
Initiator->Responder:            4 packets        320 bytes
Responder->Initiator:            4 packets        320 bytes

Total sessions found: 1

[Router] display aft session ipv4 verbose
Initiator:
  Source      IP/port: 20.1.1.1/1025
  Destination IP/port: 10.1.1.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
Responder:
  Source      IP/port: 10.1.1.1/1025
  Destination IP/port: 20.1.1.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
State: ICMP_REPLY
Application: OTHER
Start time: 2014-03-13 08:52:59  TTL: 27s
Initiator->Responder:            4 packets        240 bytes
Responder->Initiator:            4 packets        240 bytes

Total sessions found: 1
```

1.15.4 IPv4 网络访问IPv6 Internet中的服务器配置举例

1. 组网需求

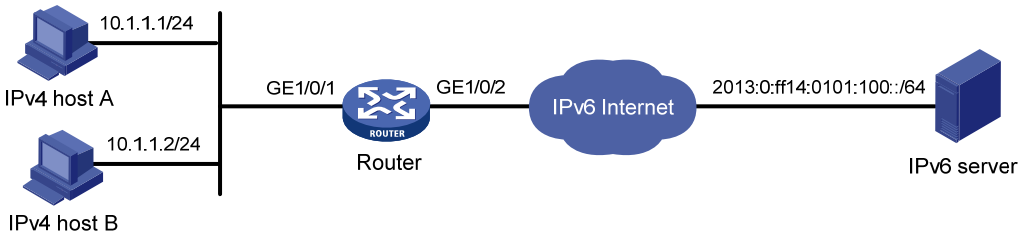
Internet 已经升级到了 IPv6，但是某公司内部网络仍然是 IPv4 网络。而该公司内部网络的 10.1.1.0/24 网段的用户仍需要访问 IPv6 Internet 中的服务器，其他用户不能访问。

为满足上述要求，本例中使用如下方式实现：

- 使用 IPv4 到 IPv6 源地址动态地址转换策略，将 IPv4 报文的源地址转换为 IPv6 地址。
- 通过 IPv6 到 IPv4 的源地址静态转换策略为 IPv6 Internet 上服务器的 IPv6 地址指定一个对应的 IPv4 地址，Router 收到发往该 IPv4 地址的报文时将其转换为对应的 IPv6 地址。

2. 组网图

图1-10 IPv4 网络访问 IPv6 Internet 中的服务器配置组网图



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

配置 ACL 2000，仅允许 IPv4 网络中 10.1.1.0/24 网段的用户可以访问 IPv6 Internet。

```
<Router> system-view
[Router] acl basic 2000
[Router-acl-ipv4-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Router-acl-ipv4-basic-2000] rule deny
[Router-acl-ipv4-basic-2000] quit
```

配置 NAT64 前缀，此前缀将在 IPv4 到 IPv6 源地址动态转换策略中被调用，将报文的源地址转换为 IPv6 地址。

```
[Router] aft prefix-nat64 2012:: 96
```

配置 IPv4 到 IPv6 源地址动态转换策略，将匹配 ACL 2000 报文的源地址根据 NAT64 前缀转换为 IPv6 地址。

```
[Router] aft v4tov6 source acl number 2000 prefix-nat64 2012:: 96
```

配置 IPv6 到 IPv4 的源地址静态转换策略，用于将报文的目的地址转换为 IPv6 地址。

```
[Router] aft v6tov4 source 2013:0:ff14:0101:100:: 20.1.1.1
```

在 IPv4 侧接口 GigabitEthernet1/0/1 开启 AFT。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] aft enable
[Router-GigabitEthernet1/0/1] quit
```

在 IPv6 侧接口 GigabitEthernet1/0/2 开启 AFT。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] aft enable
[Router-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，检查 IPv4 host 与 IPv6 server 的连通性。以 IPv4 host A ping IPv6 server 为例：

```
D:\>ping 20.1.1.1
Pinging 20.1.1.1 with 32 bytes of data:
Reply from 20.1.1.1: bytes=32 time=14ms TTL=63
Reply from 20.1.1.1: bytes=32 time=1ms TTL=63
Reply from 20.1.1.1: bytes=32 time=1ms TTL=63
Reply from 20.1.1.1: bytes=32 time=1ms TTL=63
```

通过查看 AFT 会话，可以看到创建了一个 IPv4 会话和 IPv6 会话，分别对应转换前和转换后的报文。

```
[Router] display aft session ipv4 verbose
Initiator:
  Source      IP/port: 10.1.1.1/1025
  Destination IP/port: 20.1.1.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
Responder:
  Source      IP/port: 20.1.1.1/1025
  Destination IP/port: 10.1.1.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
State: ICMP_REPLY
Application: OTHER
Start time: 2014-03-13 08:52:59  TTL: 27s
Initiator->Responder:            4 packets        240 bytes
Responder->Initiator:            4 packets        240 bytes

Total sessions found: 1

[Router] display aft session ipv6 verbose
Initiator:
  Source      IP/port: 2012::0A01:0101/0
  Destination IP/port: 2013:0:FF14:0101:0100::/32768
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/1
Responder:
  Source      IP/port: 2013:0:FF14:0101:0100::/0
  Destination IP/port: 2012::0A01:0101/33024
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet1/0/2
State: ICMPV6_REPLY
```

```
Application: OTHER
Start time: 2014-03-13 08:52:59  TTL: 23s
Initiator->Responder:            4 packets        320 bytes
Responder->Initiator:            4 packets        320 bytes

Total sessions found: 1
```

1.15.5 IPv6 Internet访问IPv4 网络配置举例

1. 组网需求

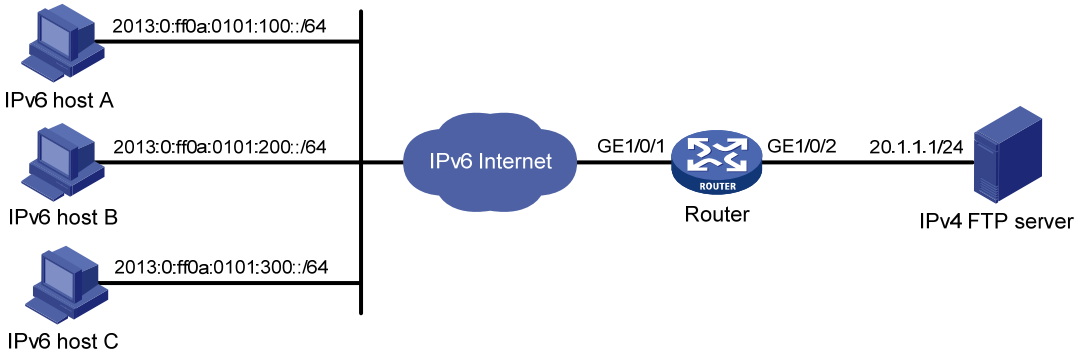
Internet 已经升级到了 IPv6，但是某公司内部网络仍然是 IPv4 网络。而该公司仍希望为 IPv6 Internet 内的用户提供 FTP 服务。该公司访问 IPv6 Internet 使用的 IPv6 地址为 2012::1。

为满足上述要求，实现方式如下：

- 通过 IPv4 到 IPv6 源地址静态转换策略，为 IPv4 网络中的 FTP 服务器地址指定一个对应的 IPv6 地址，IPv6 Internet 中的主机通过访问该 IPv6 地址可以访问 IPv4 网络中的 FTP 服务器。Router 收到发往该 IPv6 地址的报文时将其目的地址转换为对应的 IPv4 地址。
- 通过 IPv6 到 IPv4 源地址动态转换策略，将 IPv6 Internet 发送过来的 IPv6 报文源地址转换为 IPv4 地址 30.1.1.1 和 30.1.1.2。

2. 组网图

图1-11 IPv6 Internet 访问 IPv4 网络配置组网图



3. 配置步骤

按照组网图配置各接口的 IP 地址，具体配置过程略。

配置 IPv4 到 IPv6 源地址静态转换策略，手动指定 IPv4 与 IPv6 地址一一对应的转换关系，此策略可将报文的目的地址转换为对应的 IPv4 地址。

```
<Router> system-view
[Router] aft v4tov6 source 20.1.1.1 2012::1
```

配置地址组 0 包含 2 个 IPv4 地址：30.1.1.1 和 30.1.1.2。

```
[Router] aft address-group 0
[Router-aft-address-group-0] address 30.1.1.1 30.1.1.2
[Router-aft-address-group-0] quit
```

配置 IPv6 ACL 2000，匹配 IPv6 网络到 IPv4 网络的报文。此处允许所有 IPv6 网络内主机访问 IPv4 FTP Server。

```
[Router] acl ipv6 basic 2000
[Router-acl-ipv6-basic-2000] rule permit
[Router-acl-ipv6-basic-2000] quit
```

配置 IPv6 到 IPv4 的源地址动态转换策略，将匹配 ACL 2000 的 IPv6 报文源地址转换为地址组 0 中的 IPv4 地址 30.1.1.2 或 30.1.1.3。

```
[Router] aft v6tov4 source acl ipv6 number 2000 address-group 0
```

在 IPv6 侧接口 GigabitEthernet1/0/1 开启 AFT。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] aft enable
[Router-GigabitEthernet1/0/1] quit
```

在 IPv4 侧接口 GigabitEthernet1/0/2 开启 AFT。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] aft enable
[Router-GigabitEthernet1/0/2] quit
```

4. 验证配置

以上配置完成后，检查 IPv6 host 与 IPv4 FTP server 的连通性。以 IPv6 host A ping IPv4 FTP server 为例：

```
D:\>ping 2012::1
Pinging 2012::1 with 32 bytes of data:
Reply from 2012::1: time=3ms
Reply from 2012::1: time=3ms
Reply from 2012::1: time=3ms
Reply from 2012::1: time=3ms
```

通过查看 AFT 会话，可以看到创建了一个 IPv6 会话和 IPv4 会话，分别对应转换前和转换后的报文。

```
[Router] display aft session ipv6 verbose
Initiator:
  Source      IP/port: 2013:0:FF0A:0101:0100::/1029
  Destination IP/port: 2012::1/21
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
Responder:
  Source      IP/port: 2012::1/21
  Destination IP/port: 2013:0:FF0A:0101:0100::/1029
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
State: TCP_ESTABLISHED
Application: FTP
Start time: 2014-03-13 09:07:30  TTL: 3582s
Initiator->Responder:            3 packets        184 bytes
Responder->Initiator:            2 packets        148 bytes

Total sessions found: 1
```

```
[Router] display aft session ipv4 verbose
Initiator:
  Source      IP/port: 30.1.1.1/11025
  Destination IP/port: 20.1.1.1/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
Responder:
  Source      IP/port: 20.1.1.1/21
  Destination IP/port: 30.1.1.1/11025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
State: TCP_ESTABLISHED
Application: FTP
Start time: 2014-03-13 09:07:30  TTL: 3577s
Initiator->Responder:            3 packets        124 bytes
Responder->Initiator:            2 packets        108 bytes

Total sessions found: 1
```