M9000 AFT功能实现IPv4网络与IPv6网络互访
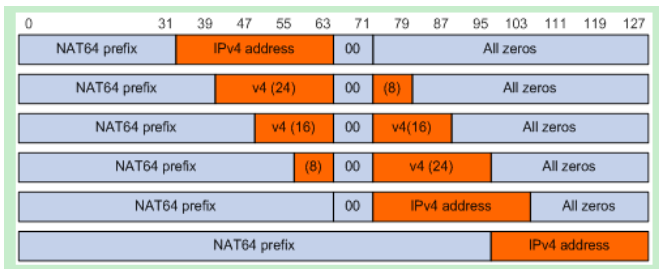
IPv6   AFT   **李政**   2018-06-26 发表

组网及说明

一、AFT简介

IPv4向IPv6过渡阶段，AFT可以实现IPv4网络和IPv6网络的互访。AFT本质与NAT类似，通过将IPv6地址映射为IPv4地址和IPv4地址映射为IPv6地址实现互访。对AFT地址转换方式的理解也可以参考NAT，具体包含以下四种方式：

1、静态模式（1对1）；

2、动态模式（1对多）

3、前缀方式：

nat64前缀；将IPv4地址和IPv6地址相互映射，前缀长度为32、40、48、56、64或96，格式如下：
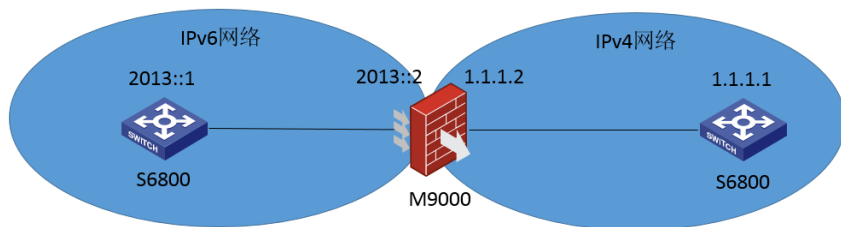

IVI前缀和general前缀：IPv6侧发起访问时，将IPv6地址映射为IPv4地址

4、IPv6内部服务器

　　　IPv6侧发起访问时，实现地址和端口映射

匹配优先级：IPv6内部服务器>静态模式>动态模式>前缀模式

此外AFT还支持FTP、DNS、ICMP差错报文的ALG处理。以SSH为例

二、组网图

在M9000中需要先配置域间策略，放通IPv4和IPv6报文。此处略过，重点关注AFT配置方式

配置步骤

典型配置及验证

1、IPv4客户端通过SSH访问IPv6服务器

1）防火墙配置

```
#
aft prefix-nat64 2013:: 96                        //IPv4地址通过NAT64前缀方式转换为IPv6地址
#
aft v6server protocol tcp 1.1.1.5 22 2013::1 22   //IPV6地址2013::1映射为1.1.1.5 端口号为22
#
interface GigabitEthernet1/5/0/9
 aft enable                                       //端口使能AFT功能
interface GigabitEthernet1/5/0/13
 aft enable
```

2）结果验证：

<S6800-L5>ssh 1.1.1.5

Username: aaa

Press CTRL+C to abort.

Connecting to 1.1.1.5 port 22.

The server is not authenticated. Continue? [Y/N]:y

Do you want to save the server public key? [Y/N]:y

aaa@1.1.1.5's password:

Enter a character ~ and a dot to abort.

<S6800-L1>

<S6800-L1>

在防火墙上查看地址映射信息：

[H3C]dis aft address-mapping

Slot 0 in chassis 1:

Total address-mapping found: 0

Slot 1 in chassis 1:

Total address-mapping found: 0

CPU 1 on slot 2 in chassis 1:

IPv6: **Source IP/port: 2013::101:101/15940**

   Destination IP/port: 2013::1/22

   VPN instance/VLAN ID/VLL ID: -/-/-

   Protocol: TCP(6)

IPv4: **Source IP/port: 1.1.1.1/15940**

   Destination IP/port: 1.1.1.5/22

   VPN instance/VLAN ID/VLL ID: -/-/-

   Protocol: TCP(6)

Total address-mapping found: 1

2、IPv6客户端通过SSH访问IPv4服务器

1）防火墙配置

```
#
aft address-group 0                    //IPv6地址转换为地址族内的地址对外网进行访问
 address 1.1.1.5 1.1.1.7
#
aft prefix-nat64 2013:: 96             //IPv4地址通过NAT64前缀方式转换为IPv6地址
#
aft v6tov4 source acl ipv6 number 2001 address-group 0
#
interface GigabitEthernet1/5/0/9        //接口使能aft功能
 aft enable
interface GigabitEthernet1/5/0/13        //接口使能aft功能
 aft enable
```

2）结果验证：

<S6800-L1>ssh ipv6 2013::1.1.1.1

Username: aaa

Press CTRL+C to abort.

Connecting to 2013::101:101 port 22.

aaa@2013::101:101's password:

Enter a character ~ and a dot to abort.

<S6800-L5>

<S6800-L5>

在防火墙上查看映射关系：

[H3C]dis aft address-mapping

Slot 0 in chassis 1:

Total address-mapping found: 0

Slot 1 in chassis 1:

Total address-mapping found: 0

CPU 1 on slot 2 in chassis 1:

IPv6: **Source IP/port: 2013::1/16330**

    Destination IP/port: 2013::101:101/22

    VPN instance/VLAN ID/VLL ID: -/-/-

    Protocol: TCP(6)

IPv4: **Source IP/port: 1.1.1.6/1035**

    Destination IP/port: 1.1.1.1/22

    VPN instance/VLAN ID/VLL ID: -/-/-

    Protocol: TCP(6)

Total address-mapping found: 1

配置关键点

1、防火墙域间策略需放通IPv6报文；

2、利用NAT64作地址映射通常采用96为地址前缀，如1.1.1.1映射为2013::1.1.1.1