

H3C MSR 系列路由器内网用户通过 NAT 地址访问地址重叠的外网典型配置举例(V7)

Copyright © 2014 杭州华三通信技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。本文档中的信息可能变动，恕不另行通知。



目 录

1 简介	1
2 配置前提	1
3 配置举例	1
3.1 组网需求	1
3.2 配置思路	1
3.3 使用版本	2
3.4 配置步骤	2
3.5 验证配置	3
3.6 配置文件	4
4 相关资料	5

1 简介

本文档介绍 MSR 系列路由器内网用户通过 NAT 地址访问地址重叠的外网典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的 MSR 系列路由器，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

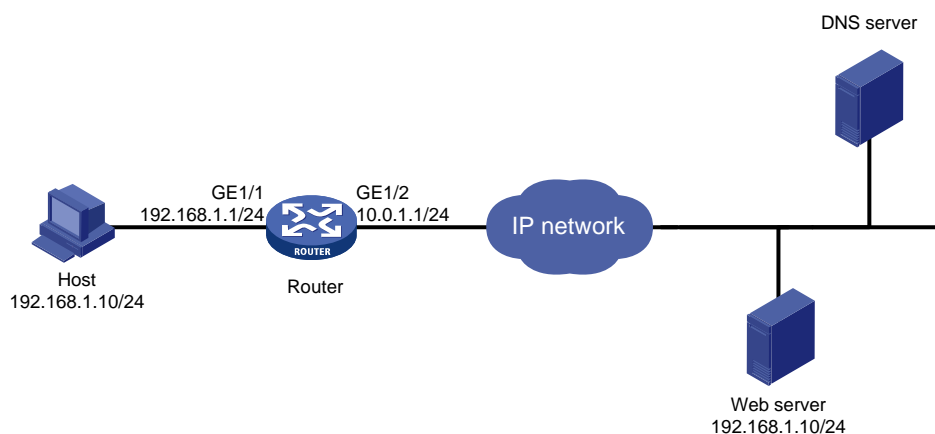
本文档假设您已了解 NAT 特性。

3 配置举例

3.1 组网需求

如 [图 1](#) 所示，Router 作为某公司内网访问外网的网关，内网网段与外网 Web server 所在网段地址重叠。该公司拥有 202.38.1.2 和 202.38.1.3 两个公网地址。现要求 Host 可以通过域名访问外网的 Web server。

图1 内网用户通过 NAT 地址访问地址重叠的外网典型配置组网图



3.2 配置思路

- 由于外网 DNS 服务器回复给内网主机的 Web 服务器地址与内网主机地址重叠，因此 NAT 设备需要将 Web 服务器地址转换为动态分配的一个 NAT 地址。动态地址分配可以通过入方向动态地址转换实现，地址转换需要通过 DNS ALG 功能实现。
- 由于内网主机的地址与外网 Web 服务器的真实地址重叠，因此也需要为内网主机动态分配一个 NAT 地址，可以通过出方向动态地址转换实现。

- 外网 Web 服务器对应的 NAT 地址在 NAT 设备上没有路由，因此需要手工添加静态路由。

3.3 使用版本

本举例是在 R0106 版本上进行配置和验证的。

3.4 配置步骤

配置路由器各接口的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/1
[Router-GigabitEthernet1/1] ip address 192.168.1.1 24
[Router-GigabitEthernet1/1] quit
[Router] interface gigabitethernet 1/2
[Router-GigabitEthernet1/2] ip address 10.0.1.1 24
[Router-GigabitEthernet1/2] quit
```

开启 DNS 协议的 ALG 功能。

```
[Router] nat alg dns
```

配置 ACL 2000，仅允许对 192.168.1.0/24 网段的用户报文进行地址转换。

```
[Router] acl number 2000
[Router-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2000] quit
```

创建地址组 1。

```
[Router] nat address-group 1
```

添加地址组成员 202.38.1.2。

```
[Router-nat-address-group-1] address 202.38.1.2 202.38.1.2
[Router-nat-address-group-1] quit
```

创建地址组 2。

```
[Router] nat address-group 2
```

添加地址组成员 202.38.1.3。

```
[Router-nat-address-group-2] address 202.38.1.3 202.38.1.3
[Router-nat-address-group-2] quit
```

在接口 GigabitEthernet1/2 上配置入方向动态地址转换，允许使用地址组 1 中的地址对 DNS 应答报文载荷中的外网地址进行转换，并在转换过程中不使用端口信息，以及允许反向地址转换。

```
[Router] interface gigabitethernet 1/2
[Router-GigabitEthernet1/2] nat inbound 2000 address-group 1 no-pat reversible
```

在接口 GigabitEthernet1/2 上配置出方向动态地址转换，允许使用地址组 2 中的地址对内网访问外网的报文进行源地址转换，并在转换过程中使用端口信息。

```
[Router-GigabitEthernet1/2] nat outbound 2000 address-group 2
[Router-GigabitEthernet1/2] quit
```

配置静态路由，目的地址为外网服务器 NAT 地址 202.38.1.2，出接口为 GigabitEthernet1/2，下一跳地址为 10.0.1.1。

```
[Router] ip route-static 202.38.1.2 32 gigabitethernet 1/2 10.0.1.1
```

3.5 验证配置

以上配置完成后，Host 能够通过域名访问 Web server。在路由器上通过 **display nat all** 命令显示 NAT 配置信息。

```
[Router] display nat all
NAT address group information:
  There are 2 NAT address groups.
  Address group 1:
    Address information:
      Start address      End address
      202.38.1.2         202.38.1.2

  Address group 2:
    Address information:
      Start address      End address
      202.38.1.3         202.38.1.3

NAT inbound information:
  There are 1 NAT inbound rules.
  Interface: GigabitEthernet1/2
    ACL: 2000          Address group: 1      Add route: N
    NO-PAT: Y          Reversible: Y

NAT outbound information:
  There are 1 NAT outbound rules.
  Interface: GigabitEthernet1/2
    ACL: 2000          Address group: 2      Port-preserved: N
    NO-PAT: N          Reversible: N

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled

NAT mapping behavior:
  Mapping mode: Address and Port-Dependent
  ACL          : ---

NAT ALG:
  DNS          : Enabled
  FTP          : Enabled
  H323         : Enabled
  ICMP-ERROR   : Enabled
  ILS          : Enabled
```

```
MGCP      : Enabled
NBT       : Enabled
PPTP      : Enabled
RSH       : Enabled
RTSP      : Enabled
SCCP      : Enabled
SIP       : Enabled
SQLNET    : Enabled
TFTP      : Enabled
XDMCP     : Enabled
```

通过 **display nat session verbose** 命令显示 NAT 会话的详细信息，可以看到 Host 访问 Web server 时生成 NAT 会话信息。

```
[Router] display nat session verbose
Initiator:
  Source      IP/port: 192.168.1.10/1694
  Destination IP/port: 202.38.1.2/8080
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
Responder:
  Source      IP/port: 192.168.1.10/8080
  Destination IP/port: 202.38.1.3/1025
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: HTTP
Start time: 2013-08-15 14:53:29  TTL: 3597s
Interface(in) : GigabitEthernet1/1
Interface(out): GigabitEthernet1/2
Initiator->Responder:          7 packets          308 bytes
Responder->Initiator:          5 packets          312 bytes

Total sessions found: 1
```

3.6 配置文件

```
#
interface GigabitEthernet1/1
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/2
 port link-mode route
 ip address 10.0.1.1 255.255.255.0
 nat inbound 2000 address-group 1 no-pat reversible
 nat outbound 2000 address-group 2
#
 ip route-static 202.38.1.2 32 GigabitEthernet1/2 10.0.1.1
#
```

```
acl number 2000
  rule 0 permit source 192.168.1.0 0.0.0.255
#
nat address-group 1
  address 202.38.1.2 202.38.1.2
#
nat address-group 2
  address 202.38.1.3 202.38.1.3
#
```

4 相关资料

- 《H3C MSR 系列路由器 配置指导(V7)》中的“三层技术-IP 业务配置指导”
- 《H3C MSR 系列路由器 命令参考(V7)》中的“三层技术-IP 业务命令参考”