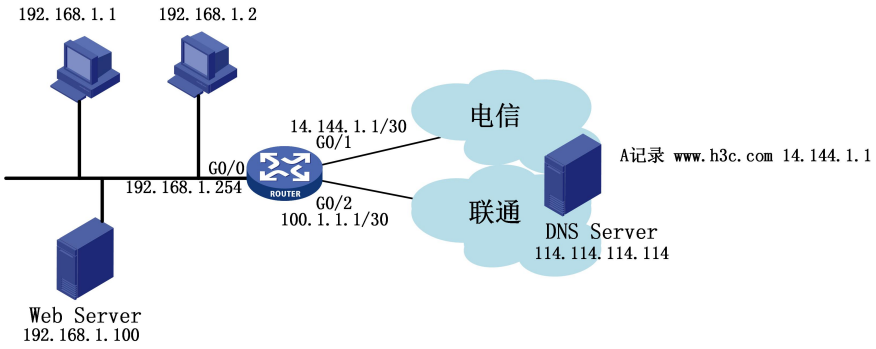
MSR G2系列路由器双出口DNS Mapping典型配置

NAT 吕甲南 2015-12-31 发表

1. 双出口电信G0/1，联通G0/2，个别用户访问互联网通过G0/1接口，剩余用户访问互联网通过G0/2接口

2. 内部服务器提供Web服务，域名为www.h3c.com，对外映射的地址为G0/1的接口地址14.144.1.1，该地址从电信购买

3. 所有内网用户需要使用域名+私网地址的方式访问内部服务器



1. 配置

```
# 配置ACL匹配源地址
acl number 2001
 rule 0 permit source 192.168.1.1 0
 rule 5 permit source 192.168.1.100 0
#配置基于报文源地址的转发策略路由
policy-based-route 1 permit node 1
 if-match acl 2001
 apply next-hop 14.144.1.2
#在内网接口配置转发策略路由
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 192.168.1.254 255.255.255.0
 ip policy-based-route 1
#在电信出接口配置NAT Server对外提供Web服务
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 14.144.1.1 255.255.255.252
 nat outbound
 nat server protocol tcp global 14.144.1.1 80 inside 192.168.1.100 80
#在联通出接口配置NAT Server使内网用户可以使用域名访问内部服务器
interface GigabitEthernet0/2
 port link-mode route
 combo enable copper
 ip address 100.1.1.1 255.255.255.252
 nat outbound
```

nat server protocol tcp global 14.144.1.1 80 inside 192.168.1.100 80

#

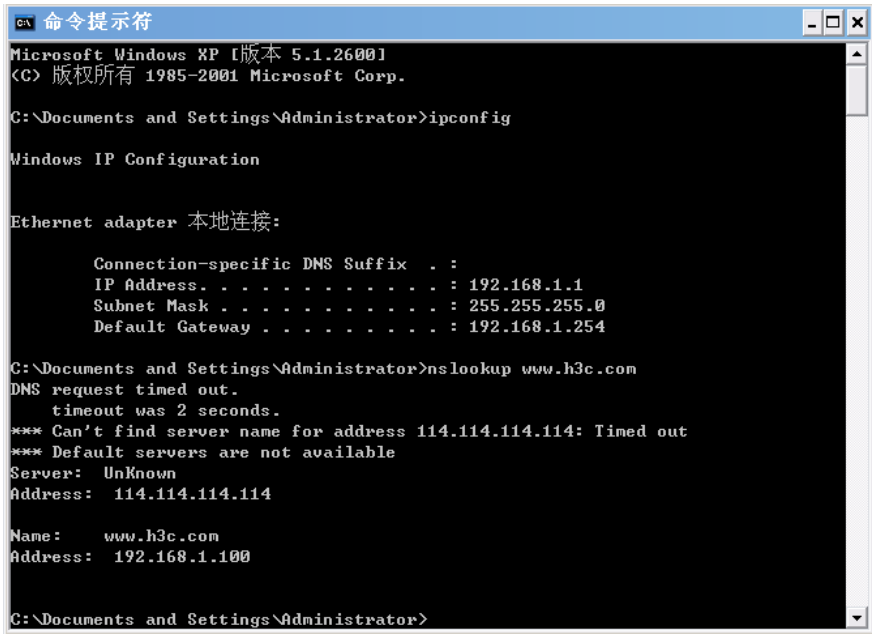
ip route-static 0.0.0.0 0 100.1.1.2

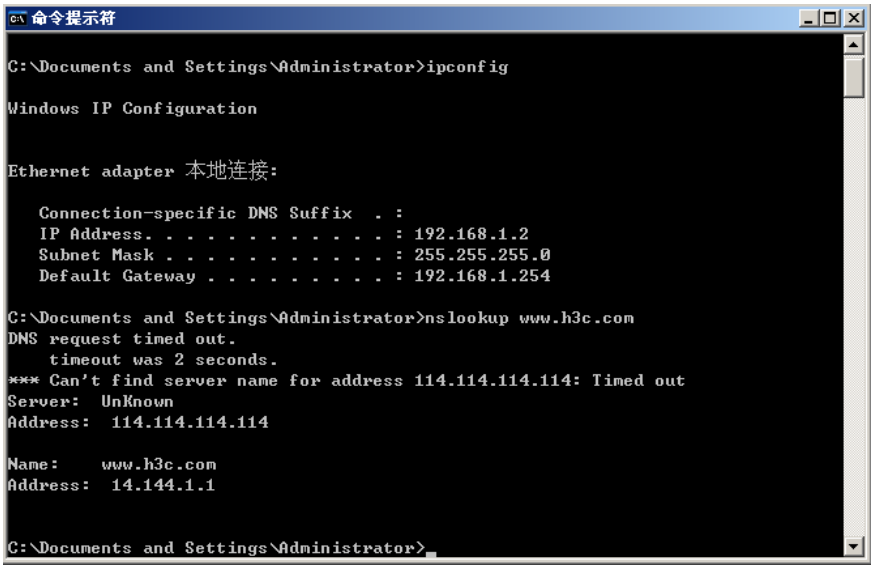
#配置域名到内部服务器的映射

nat dns-map domain www.h3c.com protocol tcp ip 14.144.1.1 port 80

2. 测试

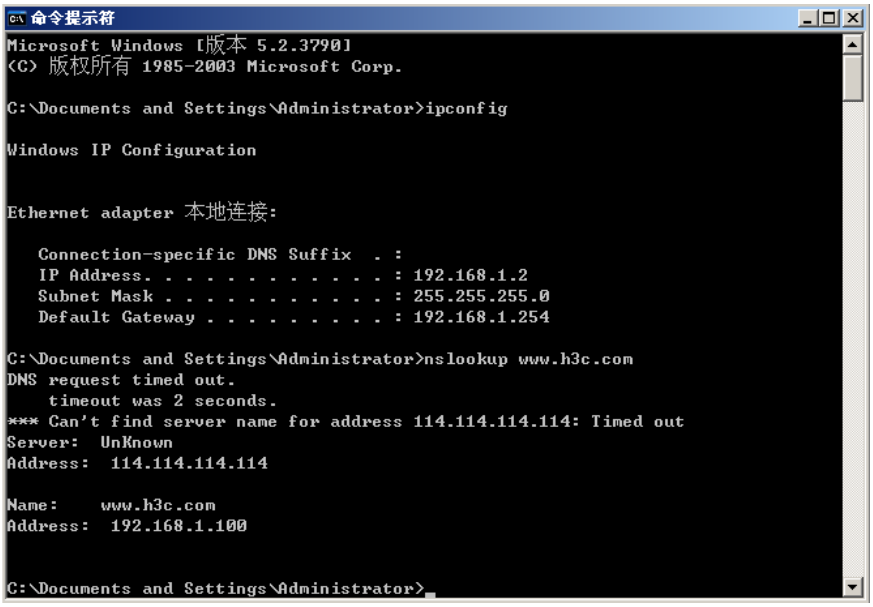
2.1 在G0/2接口配置 undo nat server protocol tcp global 14.144.1.1 80





从测试结果可以看到，从未配置NAT Server的G0/2接口发出的DNS查询，DNS回应Web服务器的地址是映射的公网地址，并没有转换成私网地址

2.2在G0/2接口配置nat server protocol tcp global 14.144.1.1 80 inside 192.168.1.100 80



从测试结果可以看到，从配置NAT Server的G0/2发出的DNS查询，DNS回应Web服务器的地址已经转换成私网地址

2.3显示NAT内部服务器的信息

display nat server

NAT internal server information:

Totally 2 internal servers.

Interface: GigabitEthernet0/1

Protocol: 6(TCP)

Global IP/port: 14.144.1.1/80

Local IP/port : 192.168.1.100/80

Config status : Active

Interface: GigabitEthernet0/2

Protocol: 6(TCP)

Global IP/port: 14.144.1.1/80

Local IP/port : 192.168.1.100/80

Config status : Active

2.4显示NAT DNS mapping配置信息。

display nat dns-map

NAT DNS mapping information:

Totally 1 NAT DNS mappings.

Domain name : www.h3c.com

Global IP : 14.144.1.1

Global port : 80

Protocol : TCP(6)

Config status: Active

2.5 通过debug，查看DNS ALG的过程

terminal monitor

The current terminal is enabled to display logs.

terminal debugging

The current terminal is enabled to display debugging logs.

debugging nat alg all

*Nov 28 11:04:19:554 2015 H3C NAT/7/ALG:

EVENT: (GigabitEthernet0/2) The payload of DNS packet with domain www.h3c.com will be translated.

*Nov 28 11:04:19:554 2015 H3C NAT/7/ALG:

PACKET: (GigabitEthernet0/2-in) DNS RRs was translated:

14.144.1.1 ---> 192.168.1.100

*Nov 28 11:04:31:051 2015 H3C NAT/7/ALG:

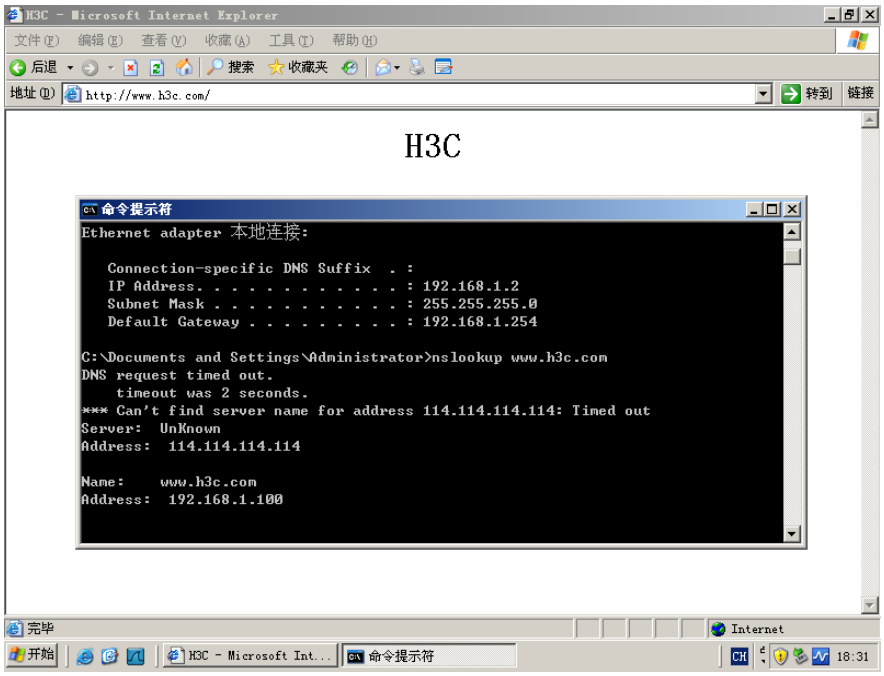
EVENT: (GigabitEthernet0/1) The payload of DNS packet with domain www.h3c.com will be translated.

*Nov 28 11:04:31:051 2015 H3C NAT/7/ALG:

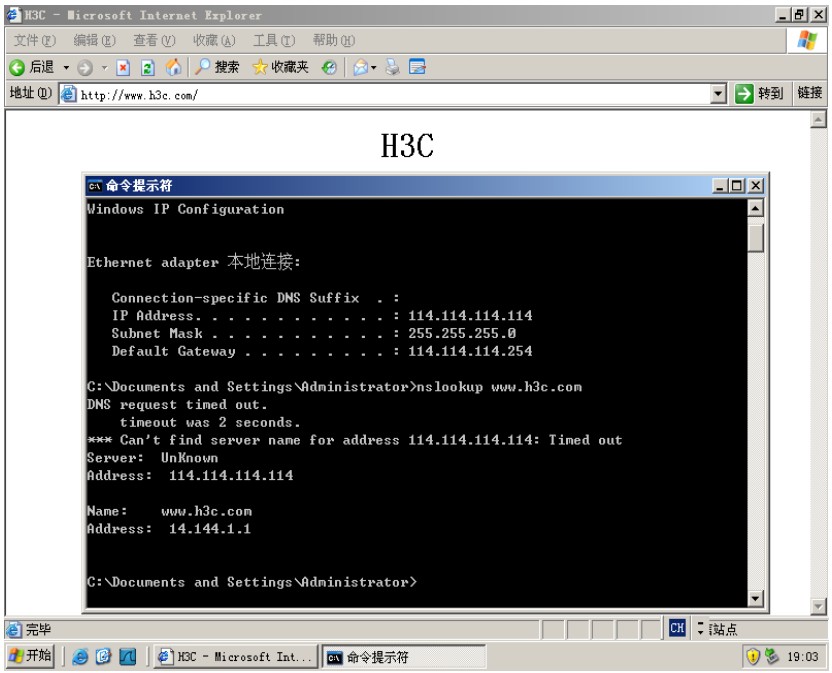
PACKET: (GigabitEthernet0/1-in) DNS RRs was translated:

14.144.1.1 ---> 192.168.1.100

2.6 内网用户使用域名+私网IP访问Web服务器



2.7 外网用户使用域名访问Web服务器



1. NAT的DNS mapping功能需要和内部服务器配合使用
2. 双出口需要配置相同的NAT Server
3. G0/1接口NAT Server的作用是对外提供Web服务，并结合DNS mapping，实现使用内部服务器域名访问同一私网内的内部服务器
4. G0/2接口NAT Server的作用是为了结合DNS mapping，实现使用内部服务器域名访问同一私网内的内部服务器