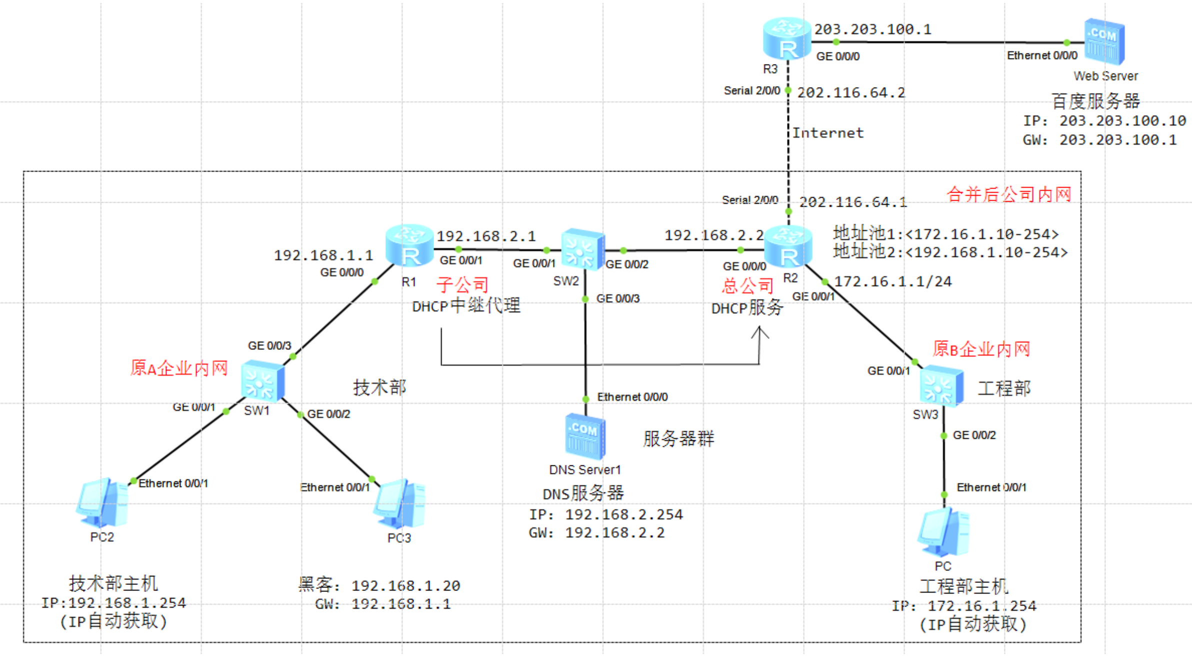
DNS欺骗劫持与防御策略

环境拓扑



基本配置

接口IP与默认路由配置

R1

```
<Huawei>sys
[Huawei]sys R1
[R1]undo info en
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]ip add 192.168.1.1 24
[R1-GigabitEthernet0/0/0]q
[R1]int g0/0/1
[R1-GigabitEthernet0/0/1]ip add 192.168.2.1 24
[R1-GigabitEthernet0/0/1]q
[R1]rip 1
[R1-rip-1]version 2
[R1-rip-1]network 192.168.1.0
[R1-rip-1]network 192.168.2.0
[R1-rip-1]q
[R1]ip route-static 0.0.0.0 0.0.0.0 192.168.2.2
```

R2

```
<Huawei>sys
[Huawei]sys R2
[R2]undo info en
[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]ip add 192.168.2.2 24
[R2-GigabitEthernet0/0/0]q
[R2]int g0/0/1
```

```
[R2-GigabitEthernet0/0/1]ip add 172.16.1.1 24
[R2-GigabitEthernet0/0/1]q
[R2]int s2/0/0
[R2-Serial2/0/0]ip add 202.116.64.1 2
[R2-Serial2/0/0]q
[R2]rip 1
[R2-rip-1]version 2
[R2-rip-1]network 192.168.2.0
[R2-rip-1]network 192.16.0.0
[R2-rip-1]q
[R2]ip route-static 0.0.0.0 0.0.0.0 serial 2/0/0
```

R3

```
<Huawei>sys
[Huawei]sys R3
[R3]undo info en
[R3]int s2/0/0
[R3-Serial2/0/0]ip add 202.116.64.2 24
[R3-Serial2/0/0]q
[R3]int g0/0/0
[R3-GigabitEthernet0/0/0]ip add 203.203.100.1 24
[R3-GigabitEthernet0/0/0]q
[R3]
```

路由器R2 Rasy-IP 配置

```
[R2]acl 2000
[R2-acl-basic-2000]rule permit source 192.168.1.0 0.0.0.255
[R2-acl-basic-2000]rule permit source 192.168.2.0 0.0.0.255
[R2-acl-basic-2000]rule permit source 172.16.1.0 0.0.0.255
[R2-acl-basic-2000]q
[R2]int s2/0/0
[R2-Serial2/0/0]nat outbound 2000
[R2-Serial2/0/0]q
[R2]
```

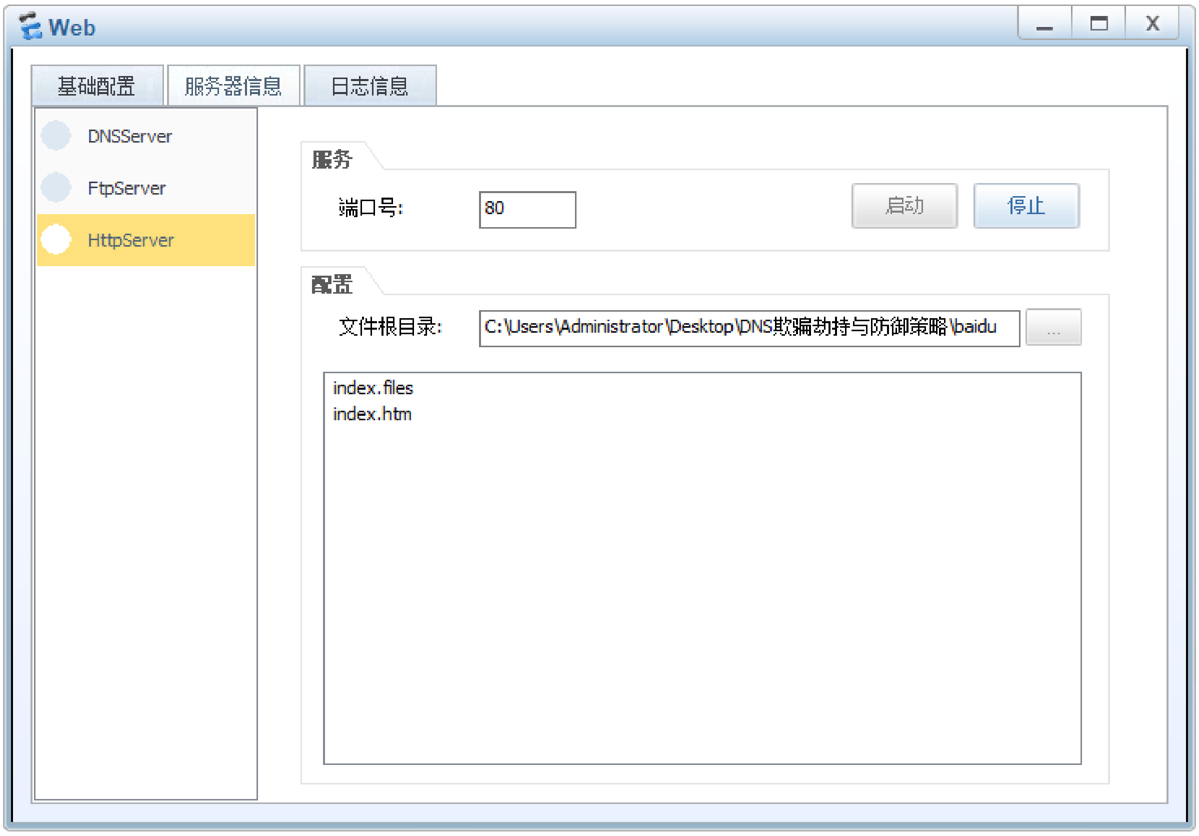
配置R2路由器DHCP服务 给技术部和工程部主机分配IP地址

```
[R2]dhcp enable
[R2]ip pool jishu
[R2-ip-pool-jishu]network 192.168.1.0 mask 24
[R2-ip-pool-jishu]gateway-list 192.168.1.1
[R2-ip-pool-jishu]dns-list 192.168.2.254
[R2-ip-pool-jishu]excluded-ip-address 192.168.1.2 192.168.1.9
[R2-ip-pool-jishu]q

[R2]ip pool gongcheng
[R2-ip-pool-gongcheng]network 172.16.1.0 mask 24
[R2-ip-pool-gongcheng]gateway-list 172.16.1.1
[R2-ip-pool-gongcheng]dns-list 192.168.2.254
[R2-ip-pool-gongcheng]excluded-ip-address 172.16.1.2 172.16.1.9
[R2-ip-pool-gongcheng]q

```

```
[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]dhcp select global
[R2-GigabitEthernet0/0/0]q
[R2]
```

```
[R1]dhcp enable
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]dhcp select relay
[R1-GigabitEthernet0/0/0]dhcp relay server-ip 192.168.2.2
[R1-GigabitEthernet0/0/0]q
[R1]
```

配置百度服务器HttpServer

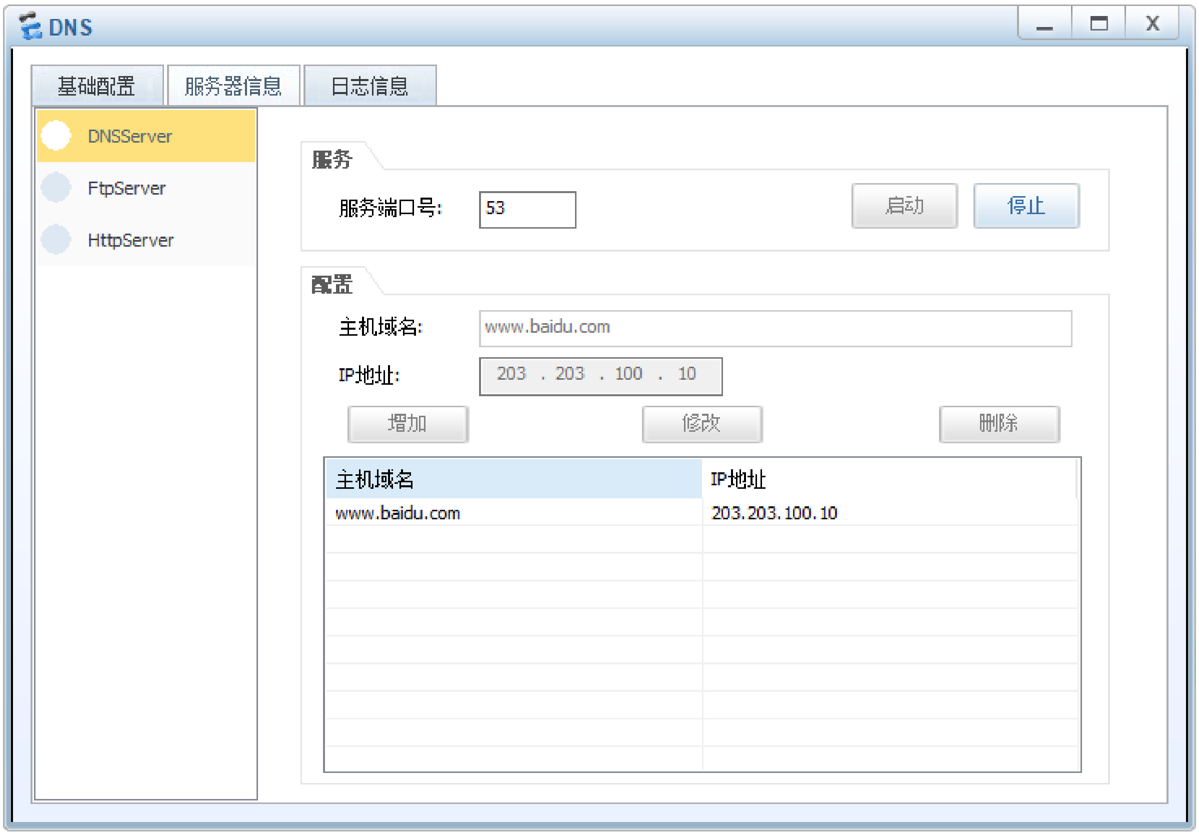


端口号: 80

文件根目录: C:\Users\Administrator\Desktop\DNS欺骗劫持与防御策略\baidu

index.files
index.htm

配置DNS Server



服务端口号: 53

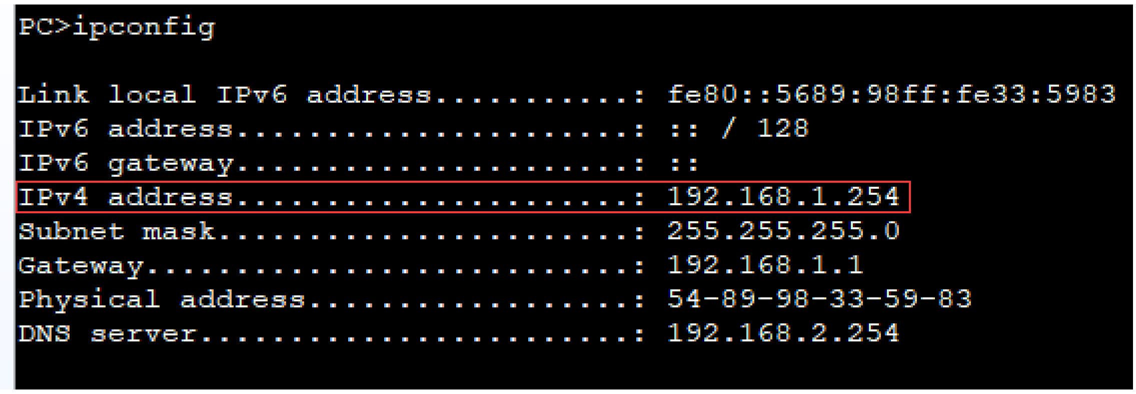
主机域名: www.baidu.com

IP地址: 203 . 203 . 100 . 10

主机域名	IP地址
www.baidu.com	203.203.100.10

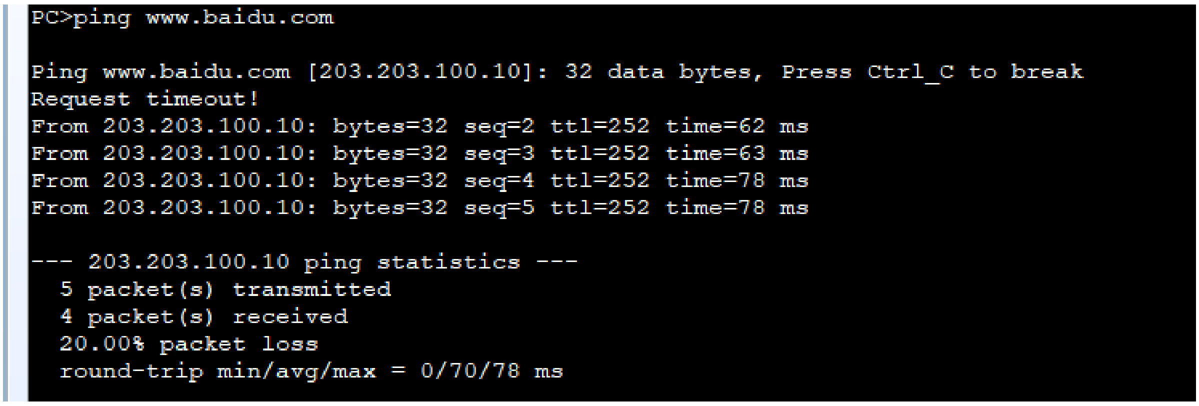
基本配置验证

技术部主机PC2 ping DNS服务器server1



```
PC>ipconfig

Link local IPv6 address...........: fe80::5689:98ff:fe33:5983
IPv6 address......................: :: / 128
IPv6 gateway......................: ::
IPv4 address......................: 192.168.1.254
Subnet mask.......................: 255.255.255.0
Gateway...........................: 192.168.1.1
Physical address..................: 54-89-98-33-59-83
DNS server........................: 192.168.2.254
```

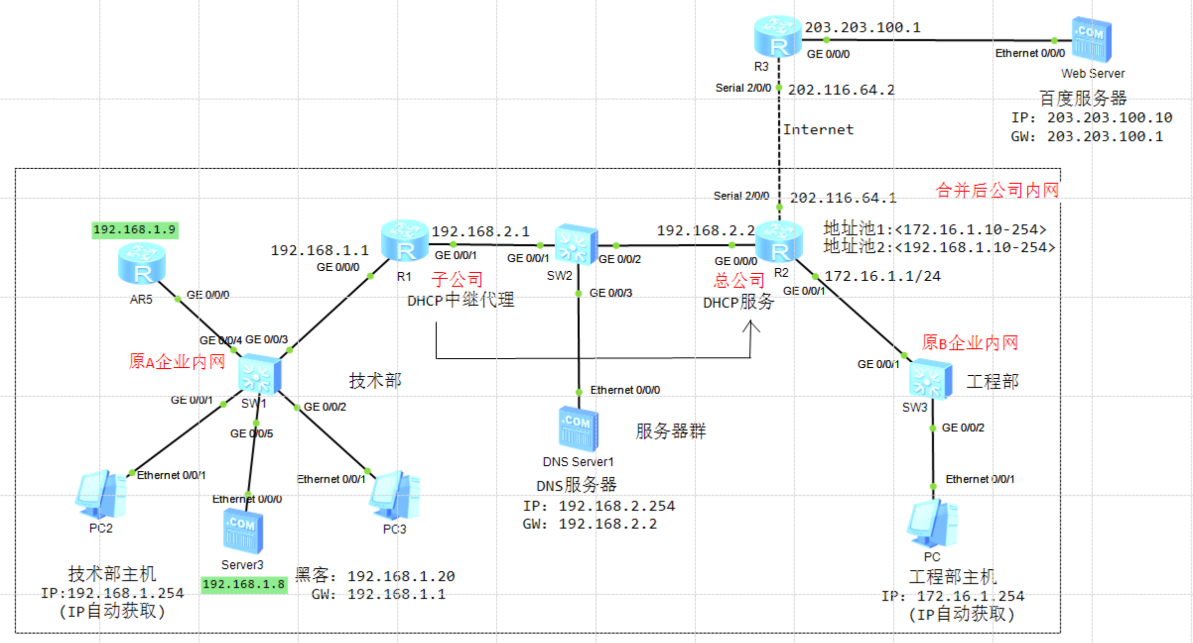
技术部主机PC2 ping baidu.com



```
PC>ping www.baidu.com

Ping www.baidu.com [203.203.100.10]: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 203.203.100.10: bytes=32 seq=2 ttl=252 time=62 ms
From 203.203.100.10: bytes=32 seq=3 ttl=252 time=63 ms
From 203.203.100.10: bytes=32 seq=4 ttl=252 time=78 ms
From 203.203.100.10: bytes=32 seq=5 ttl=252 time=78 ms

--- 203.203.100.10 ping statistics ---
  5 packet(s) transmitted
  4 packet(s) received
  20.00% packet loss
  round-trip min/avg/max = 0/70/78 ms
```

入侵实战

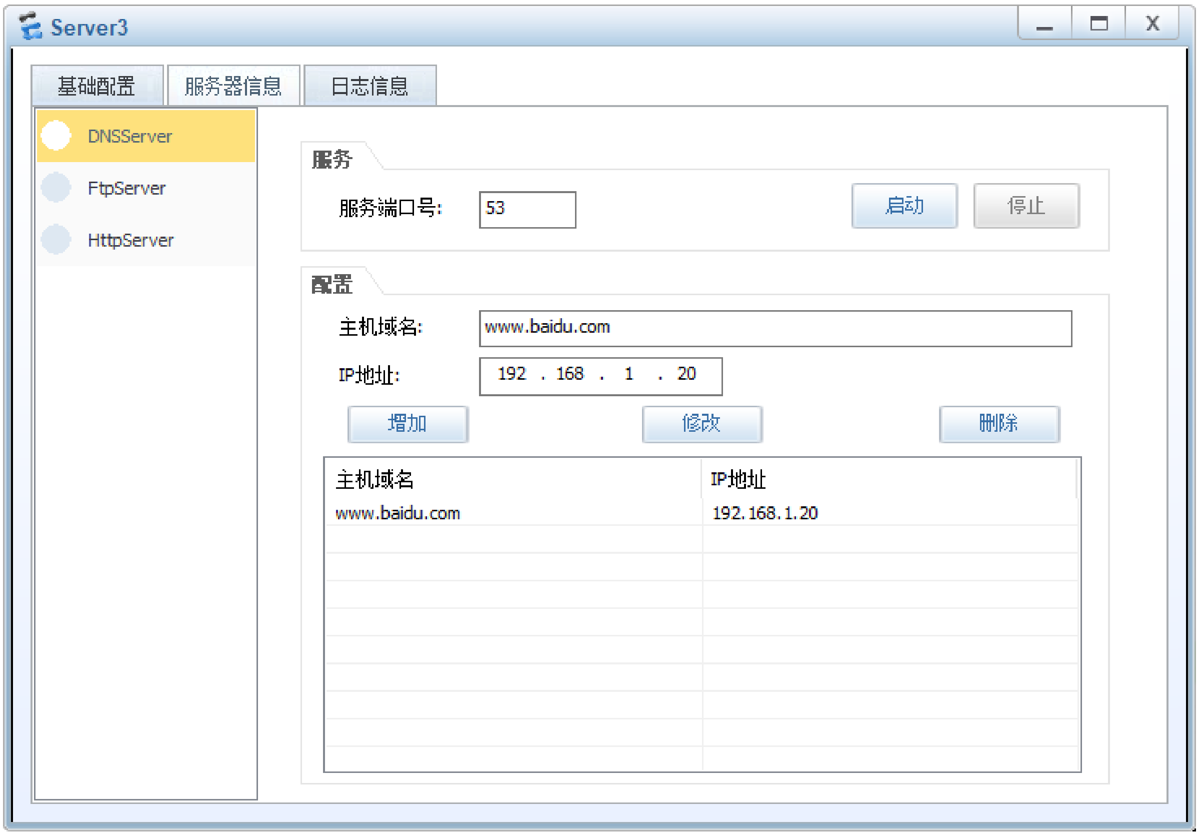
网络拓扑结构图



伪造DHCP服务器R4配置

```
<Huawei>sys
[Huawei]sys R4
[R4]undo info en
[R4]int g0/0/0
[R4-GigabitEthernet0/0/0]ip add 192.168.1.9 24
[R4-GigabitEthernet0/0/0]q
[R4]dhcp enable
[R4]ip pool forget
[R4-ip-pool-forget]network 192.168.1.0 mask 24
[R4-ip-pool-forget]gateway-list 192.168.1.1
[R4-ip-pool-forget]dns-list 192.168.1.8
[R4-ip-pool-forget]q
[R4]int g0/0/0
[R4-GigabitEthernet0/0/0]dhcp select global
[R4-GigabitEthernet0/0/0]q
[R4]
```

伪造DHCP服务器配置



服务端口号: 53

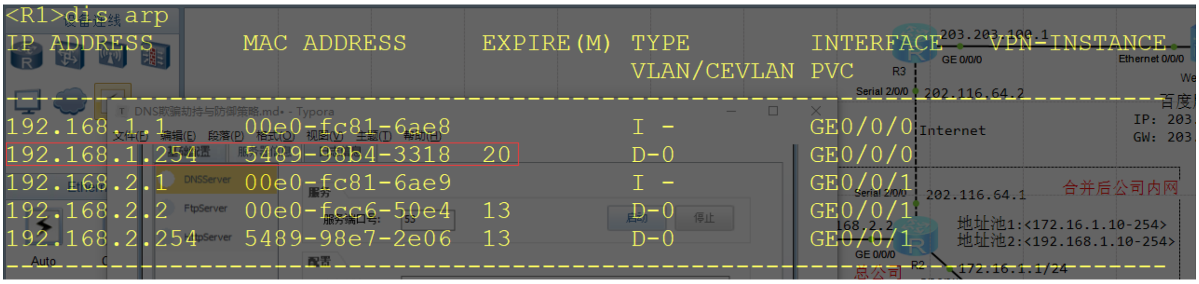
主机域名: www.baidu.com

IP地址: 192 . 168 . 1 . 20

主机域名	IP地址
www.baidu.com	192.168.1.20

arp欺骗

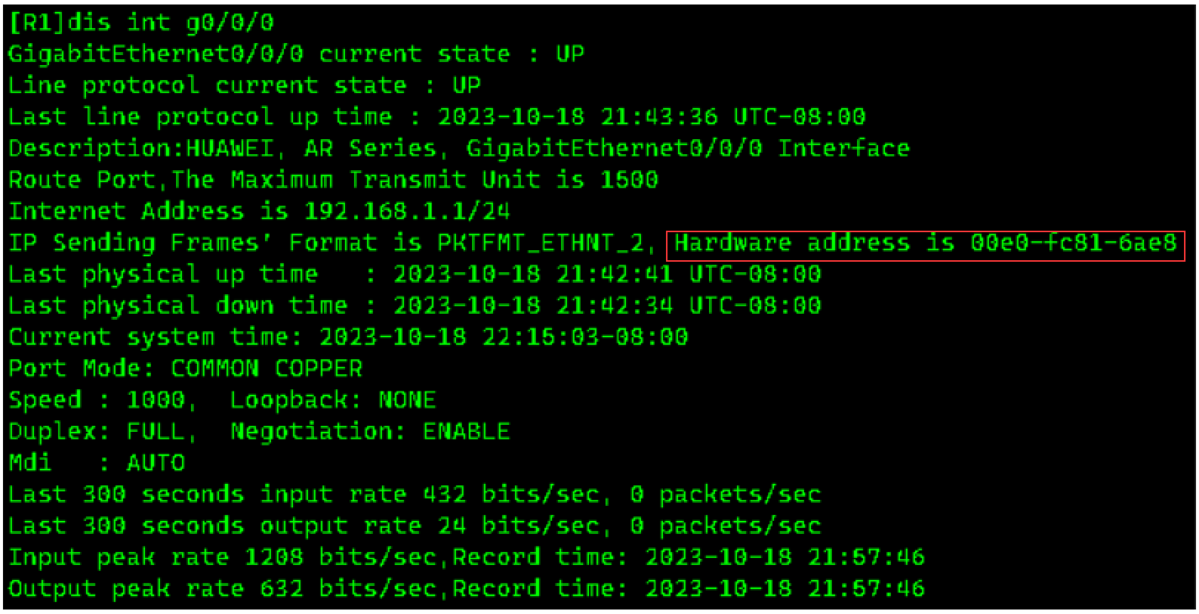
将pc3的IP地址改为pc2的IP地址去ping baidu.com



```
<R1>dis arp
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
------------------------------------------------------------------------------
192.168.1.1     00e0-fc81-6ae8            I -         GE0/0/0
192.168.1.254   5489-98b4-3318  20        D-0         GE0/0/0
192.168.2.1     00e0-fc81-6ae9            I -         GE0/0/1
192.168.2.2     00e0-fcc6-50e4  13        D-0         GE0/0/1
192.168.2.254   5489-98e7-2e06  13        D-0         GE0/0/1
------------------------------------------------------------------------------
```

防御策略

1.查看路由器R1的GE0/0/0接口(网关接口)MAC地址



```
[R1]dis int g0/0/0
GigabitEthernet0/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2023-10-18 21:43:36 UTC-08:00
Description:HUAWEI, AR Series, GigabitEthernet0/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 192.168.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc81-6ae8
Last physical up time   : 2023-10-18 21:42:41 UTC-08:00
Last physical down time : 2023-10-18 21:42:34 UTC-08:00
Current system time: 2023-10-18 22:15:03-08:00
Port Mode: COMMON COPPER
Speed : 1000,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi    : AUTO
Last 300 seconds input rate 432 bits/sec, 0 packets/sec
Last 300 seconds output rate 24 bits/sec, 0 packets/sec
Input peak rate 1208 bits/sec,Record time: 2023-10-18 21:57:46
Output peak rate 632 bits/sec,Record time: 2023-10-18 21:57:46
```

2.在交换机SW1上绑定网关与MAC地址映射关系

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sys SW1
[SW1]undo info en
[SW1]user-bind static ip-address 192.168.1.1 MAC-address 00e0-fc81-6ae8
[SW1]user-bind static ip-address 192.168.1.1 MAC-address 00e0-fc81-6ae8 int g0/0/3 vlan 1
[SW1]vlan 1
[SW1-vlan1]arp anti-attack check user-bind enable
[SW1-vlan1]q
[SW1]
```

任务总结

1.DNS欺骗劫持事件仅发生在局域网内。在IP规划时可通过可变长子网(VLSM)将一个网段划分成多个子网,限制广播域范围以减少此类攻击事件发生

2.DNS欺骗不属于病毒木马,不能通过安装防病毒软件避免此类攻击

3.计算机DNS缓存表不会立刻刷新,需等待一段时长.如需手动刷新,命令为ipconfig /flushdns