

网络组网实验报告

原创

beater_Kirito 于 2019-12-12 10:57:07 发布 5104 收藏 35

文章标签: [计算机网络 组网试验](#)

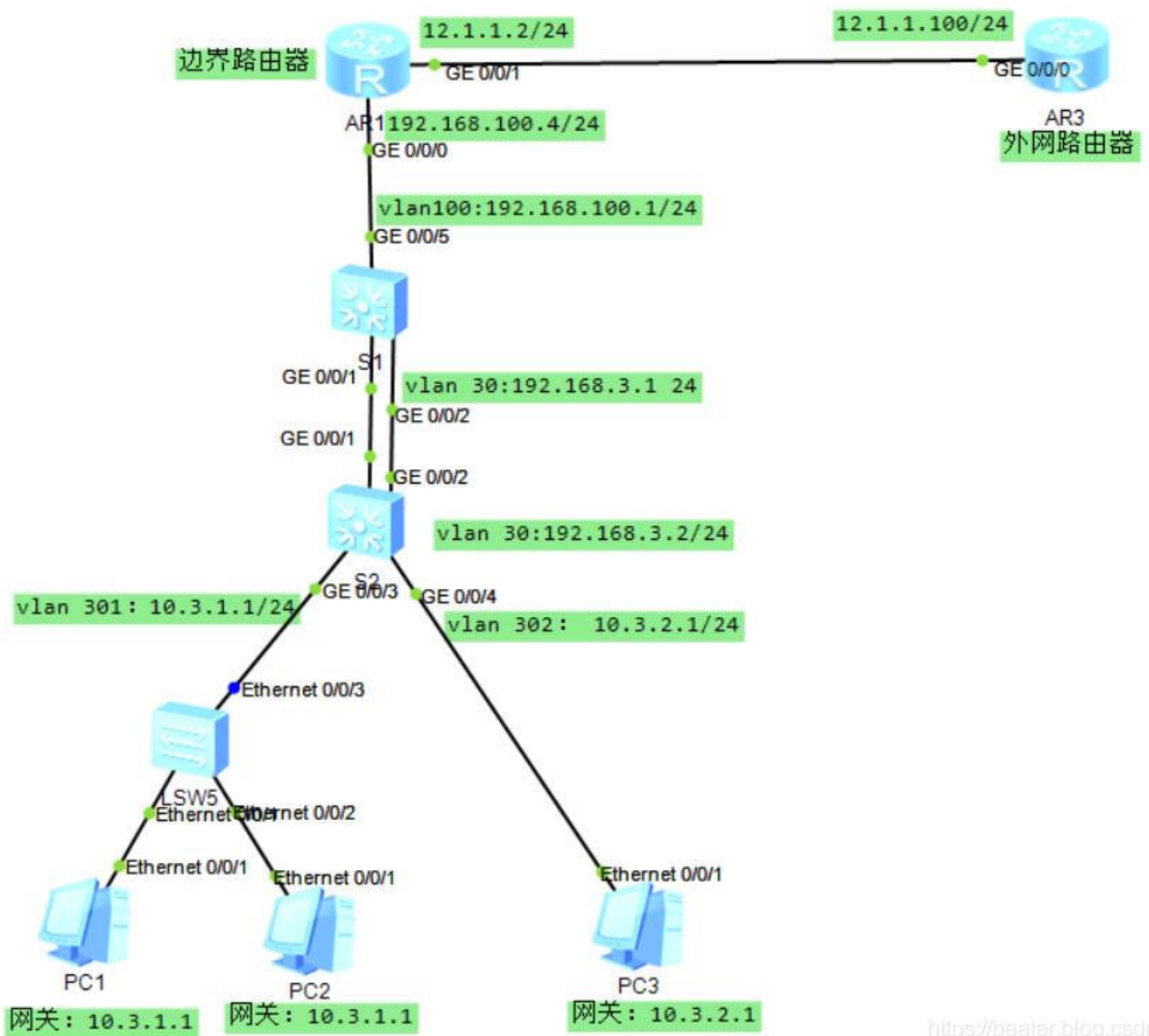
版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_42931810/article/details/103504742

版权

一、网络拓扑构建

1. 网络拓扑图



<https://beater.blog.csdn.net>

图1 网络拓扑图

2. 网络配置过程详解

2.1 配置VLAN

2.1.1 交换机端口类型

Access：Access类型的端口只能属于1个VLAN，一般用于连接计算机的端口；

Trunk：Trunk类型的端口可以允许多个VLAN通过，可以接收和发送多个VLAN的报文，一般用于交换机之间连接的端口；

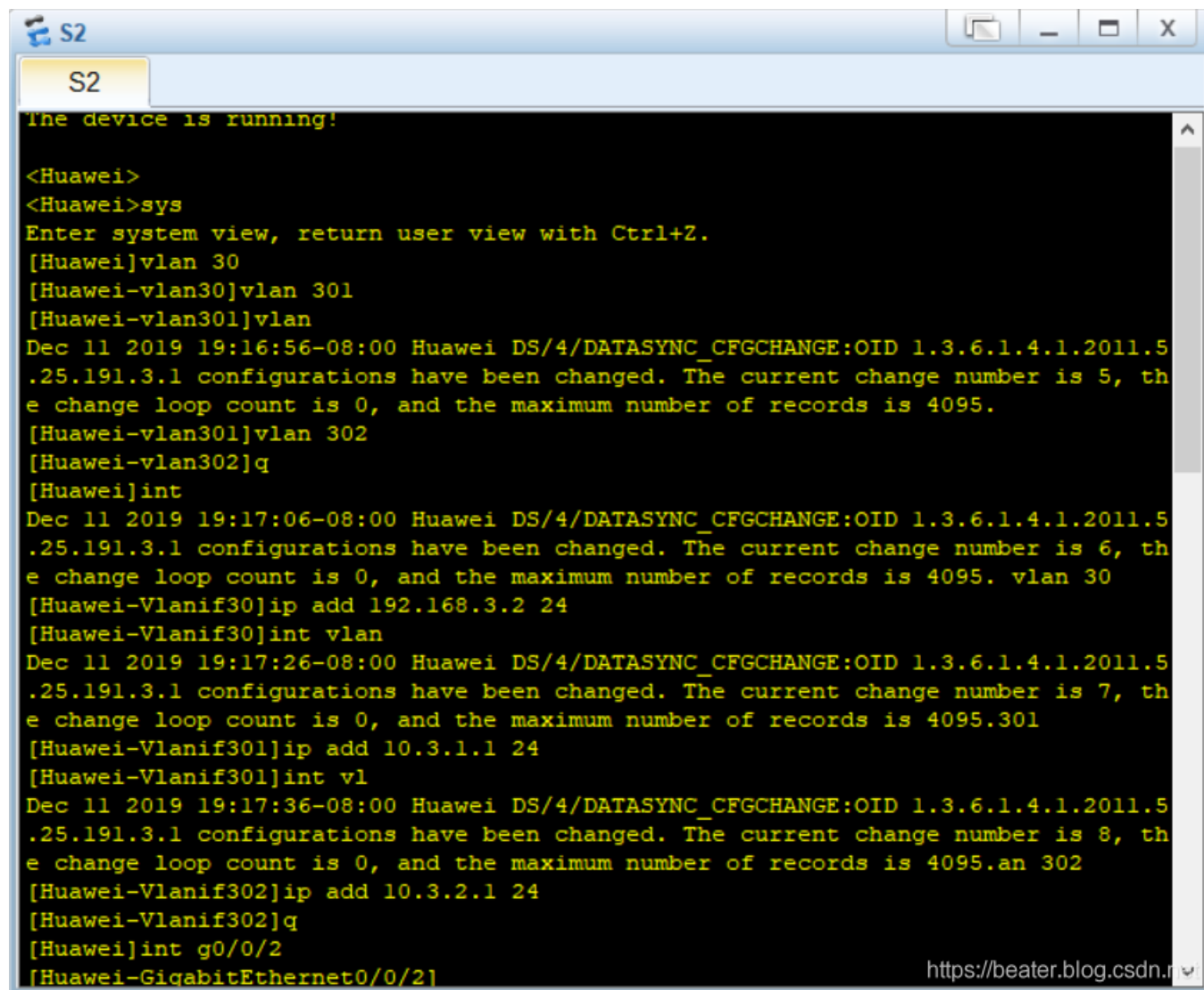
基于上述内容，因此我们需要将与计算机连接的端口设置为Access类型，这里由于而与其他交换机连接时全是不一样VLAN，因此，所有与其他交换机连接的端口均设置为Trunk端口

端口GigabitEthernet0/0/3连接接入层交换机，配置为VLAN 301，默认网关为10.3.1.1/24

端口GigabitEthernet0/0/4连接接PC 3，配置为VLAN 302，默认网关为10.3.2.1/24

端口GigabitEthernet0/0/1和GigabitEthernet0/0/2连接核心层交换机，配置为VLAN 30，默认网关为192.168.3.1/24

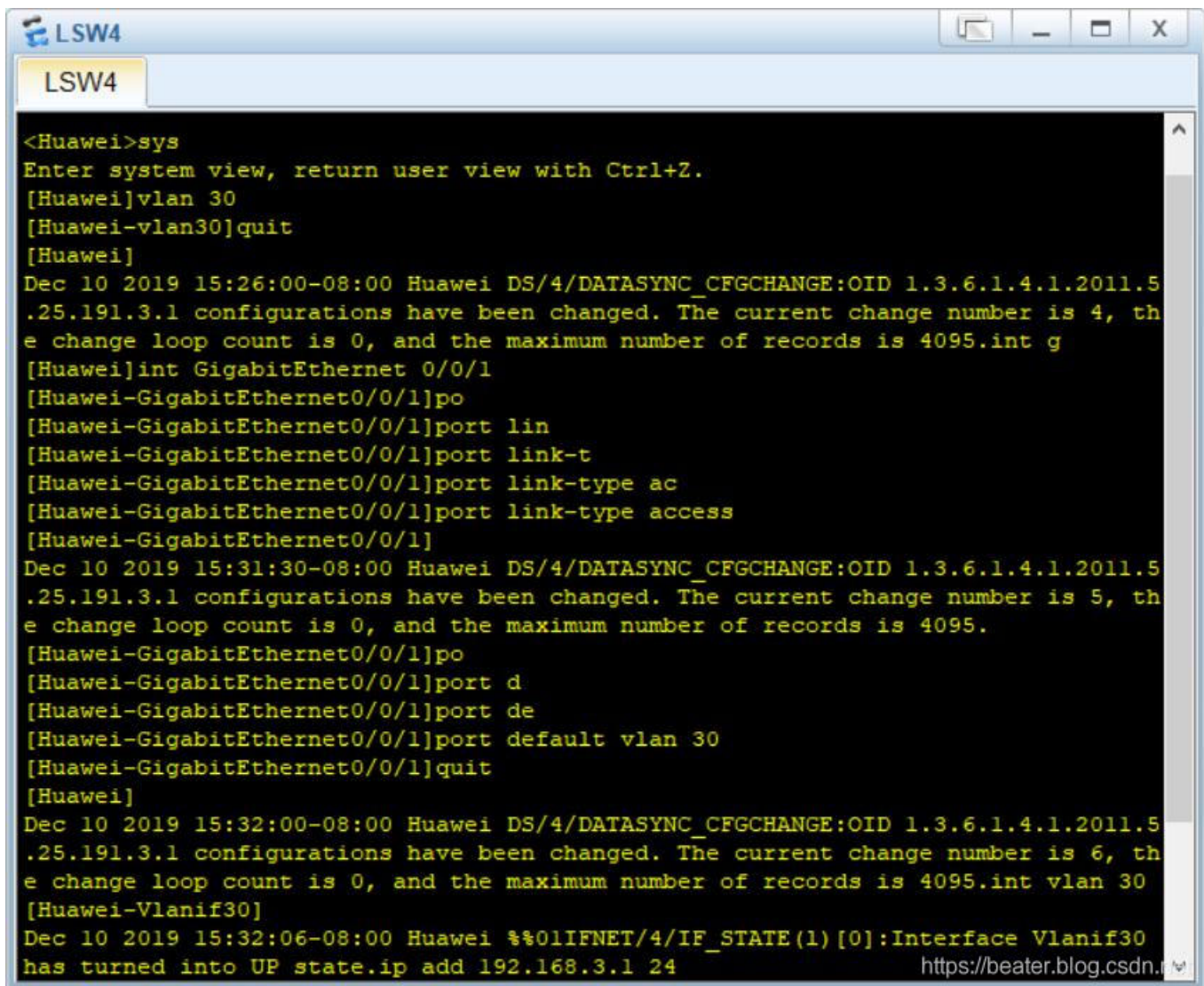
核心层交换机与汇聚层交换机使用链路备份



```
S2
S2
The device is running!
<Huawei>
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]vlan 30
[Huawei-vlan30]vlan 301
[Huawei-vlan301]vlan
Dec 11 2019 19:16:56-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 5, th
e change loop count is 0, and the maximum number of records is 4095.
[Huawei-vlan301]vlan 302
[Huawei-vlan302]q
[Huawei]int
Dec 11 2019 19:17:06-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 6, th
e change loop count is 0, and the maximum number of records is 4095. vlan 30
[Huawei-Vlanif30]ip add 192.168.3.2 24
[Huawei-Vlanif30]int vlan
Dec 11 2019 19:17:26-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 7, th
e change loop count is 0, and the maximum number of records is 4095.301
[Huawei-Vlanif301]ip add 10.3.1.1 24
[Huawei-Vlanif301]int vl
Dec 11 2019 19:17:36-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 8, th
e change loop count is 0, and the maximum number of records is 4095.an 302
[Huawei-Vlanif302]ip add 10.3.2.1 24
[Huawei-Vlanif302]q
[Huawei]int g0/0/2
[Huawei-GigabitEthernet0/0/2]
```

<https://beater.blog.csdn.net>

图2 汇聚层交换机VLAN配置



```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]vlan 30
[Huawei-vlan30]quit
[Huawei]
Dec 10 2019 15:26:00-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 4, th
e change loop count is 0, and the maximum number of records is 4095.int g
[Huawei]int GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1]po
[Huawei-GigabitEthernet0/0/1]port lin
[Huawei-GigabitEthernet0/0/1]port link-t
[Huawei-GigabitEthernet0/0/1]port link-type ac
[Huawei-GigabitEthernet0/0/1]port link-type access
[Huawei-GigabitEthernet0/0/1]
Dec 10 2019 15:31:30-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 5, th
e change loop count is 0, and the maximum number of records is 4095.
[Huawei-GigabitEthernet0/0/1]po
[Huawei-GigabitEthernet0/0/1]port d
[Huawei-GigabitEthernet0/0/1]port de
[Huawei-GigabitEthernet0/0/1]port default vlan 30
[Huawei-GigabitEthernet0/0/1]quit
[Huawei]
Dec 10 2019 15:32:00-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 6, th
e change loop count is 0, and the maximum number of records is 4095.int vlan 30
[Huawei-Vlanif30]
Dec 10 2019 15:32:06-08:00 Huawei %01IFNET/4/IF_STATE(1)[0]:Interface Vlanif30
has turned into UP state.ip add 192.168.3.1 24
https://beater.blog.csdn.net
```

图3 核心交换机Vlan配置

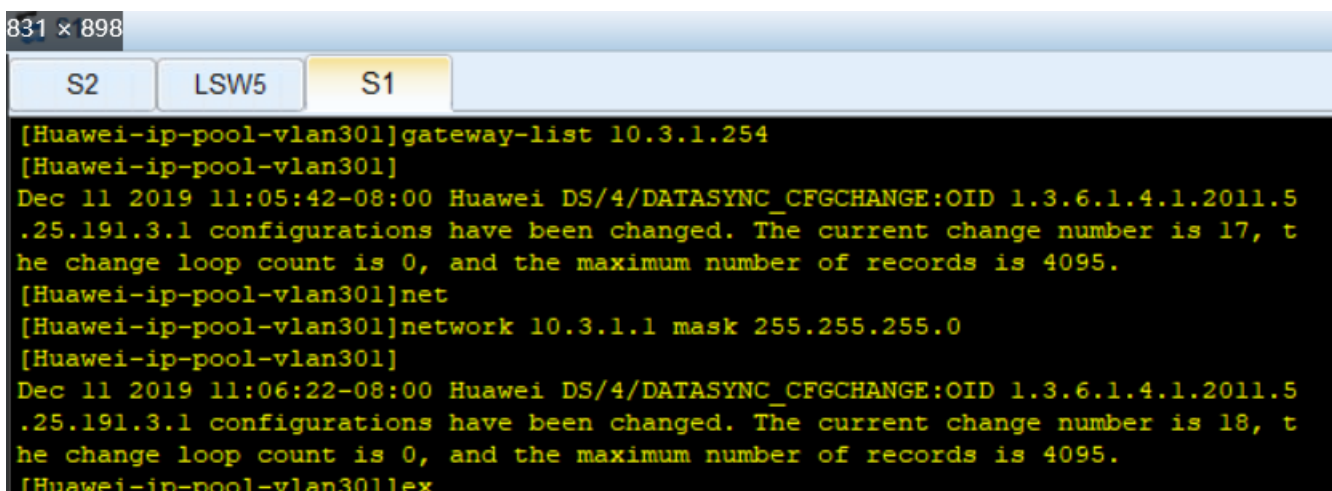
2.配置DHCP地址池

在各交换机上打开DHCP功能，并在各个VLAN中配置地址池。

在VLAN301中配置地址池为10.3.1.2-10.3.1.12

在VLAN302中配置地址池为10.3.2.2-10.3.2.12

在VLAN30中配置地址池为192.168.3.2-192.168.3.12



```
831 x 898
S2 LSW5 S1
[Huawei-ip-pool-vlan301]gateway-list 10.3.1.254
[Huawei-ip-pool-vlan301]
Dec 11 2019 11:05:42-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 17, t
he change loop count is 0, and the maximum number of records is 4095.
[Huawei-ip-pool-vlan301]net
[Huawei-ip-pool-vlan301]network 10.3.1.1 mask 255.255.255.0
[Huawei-ip-pool-vlan301]
Dec 11 2019 11:06:22-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 18, t
he change loop count is 0, and the maximum number of records is 4095.
[Huawei-ip-pool-vlan301]ex
```

```

[Huawei-ip-pool-vlan301]excluded-ip-address 10.3.1.2 10.3.1.12
[Huawei-ip-pool-vlan301]
Dec 11 2019 11:07:02-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 19, t
he change loop count is 0, and the maximum number of records is 4095.
[Huawei-ip-pool-vlan301]q
[Huawei]int vlan 301
[Huawei-Vlanif301]d
[Huawei-Vlanif301]dhcp sr
[Huawei-Vlanif301]dhcp se
[Huawei-Vlanif301]dhcp select g
[Huawei-Vlanif301]dhcp select global
Error: Please enable DHCP in the global view first.
[Huawei-Vlanif301]q
[Huawei]ip p
[Huawei]ip po
[Huawei]ip poo
[Huawei]ip pool vlan301
[Huawei-ip-pool-vlan301]ne
[Huawei-ip-pool-vlan301]netw
[Huawei-ip-pool-vlan301]network 10.3.1.0 mas
[Huawei-ip-pool-vlan301]network 10.3.1.0 mask 255.255.255.0
Error:Please delete the network section first.
[Huawei-ip-pool-vlan301]undo net
[Huawei-ip-pool-vlan301]undo network
[Huawei-ip-pool-vlan301]network 10.3.1.0 mask 255.255.255.0
Dec 11 2019 11:09:02-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 20, t
he change loop count is 0, and the maximum number of records is 4095.
[Huawei-ip-pool-vlan301]
[Huawei-ip-pool-vlan301]q
[Huawei]int vla
Dec 11 2019 11:09:12-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 21, t
he change loop count is 0, and the maximum number of records is 4095.n 301
[Huawei-Vlanif301]dh
[Huawei-Vlanif301]dhcp se
[Huawei-Vlanif301]dhcp select gl
[Huawei-Vlanif301]dhcp select global
Error: Please enable DHCP in the global view first.
[Huawei-Vlanif301]q
[Huawei]dhc
[Huawei]dhcp en
Info: The operation may take a few seconds. Please wait for a moment.done.
[Huawei]
Dec 11 2019 11:09:52-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 22, t
he change loop count is 0, and the maximum number of records is 4095.
[Huawei]d
[Huawei]dhcp se
[Huawei]dhcp sel
[Huawei]int vlan 301
[Huawei-Vlanif301]dh
[Huawei-Vlanif301]dhcp se
[Huawei-Vlanif301]dhcp select g
[Huawei-Vlanif301]dhcp select global
[Huawei-Vlanif301]
Dec 11 2019 11:10:22-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 23, t
he change loop count is 0, and the maximum number of records is 4095.
[Huawei-Vlanif301]q
[Huawei]ip p
[Huawei]ip pool vlan 302

```


图4 DHCP地址池配置命令

DHCP地址池配置成功后，各PC均得到充当DHCP服务器的交换机分配的IP地址，如下图所示

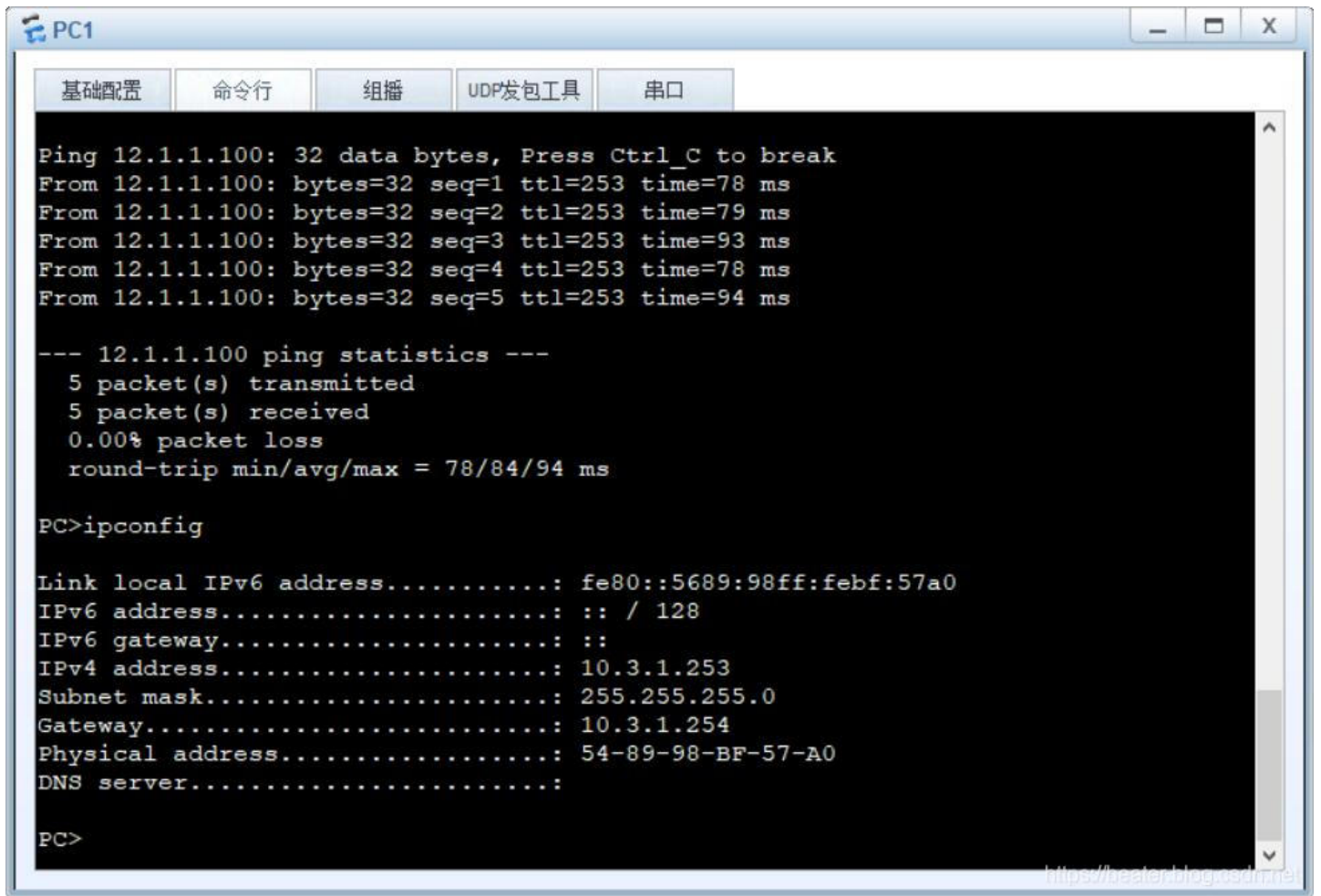


图5 PC1的IP地址分配情况

```
PC2
基础配置 命令行 组播 UDP发包工具 串口

Ping 10.3.1.253: 32 data bytes, Press Ctrl_C to break
From 10.3.1.253: bytes=32 seq=1 ttl=128 time=31 ms
From 10.3.1.253: bytes=32 seq=2 ttl=128 time=31 ms
From 10.3.1.253: bytes=32 seq=3 ttl=128 time=32 ms
From 10.3.1.253: bytes=32 seq=4 ttl=128 time=31 ms
From 10.3.1.253: bytes=32 seq=5 ttl=128 time=31 ms

--- 10.3.1.253 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/31/32 ms

PC>ipconfig

Link local IPv6 address.....: fe80::5689:98ff:feb8:5853
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 10.3.1.252
Subnet mask.....: 255.255.255.0
Gateway.....: 10.3.1.254
Physical address.....: 54-89-98-B8-58-53
DNS server.....:

PC>
```

图6 PC2由DHCP分配的IP地址

3. STP + VRRP配置

由于核心路由器的负荷最重，所以本实验采用两台核心路由器AR1，AR4双机热备份的设计。运行VRRP，AR4作为备份路由器。下图为AR1的配置命令，AR4的配置命令与AR1基本相同。

```
[Huawei]int vlan 301
[Huawei-Vlanif301]
[Huawei-Vlanif301]vrr
[Huawei-Vlanif301]vrrp v
[Huawei-Vlanif301]vrrp vrid 10 v
[Huawei-Vlanif301]vrrp vrid 10 virtual-ip 10.3.1.254
[Huawei-Vlanif301]vrrp vrid 10 virtual-ip
Dec 11 2019 11:30:53-08:00 Huawei %01VRRP/4/STATEWARNINGEXTEND(1)[10]:Virtual R
outer state BACKUP changed to MASTER, because of protocol timer expired. (Interf
ace=Vlanif301, VrId=10, InetType=IP
Dec 11 2019 11:30:53-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 40, t
he change loop count is 0, and the maximum number of records is
[Huawei-Vlanif301]vrrp vrid 10 pr
[Huawei-Vlanif301]vrrp vrid 10 priority 120
[Huawei-Vlanif301]
Dec 11 2019 11:31:03-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
.25.191.3.1 configurations have been changed. The current change number is 41, t
he change loop count is 0, and the maximum number of records is 4095.
```

图7 VRRP配置命令

4.OSPF配置

```
[Huawei]os
[Huawei]ospf
[Huawei-ospf-1]ar
[Huawei-ospf-1]are
[Huawei-ospf-1]area 0
[Huawei-ospf-1-area-0.0.0.0]net
[Huawei-ospf-1-area-0.0.0.0]network 192.168.100.0 0.0.0.255
[Huawei-ospf-1-area-0.0.0.0]network 192.168.100.0 0.0.0.255
Dec 11 2019 11:38:57-08:00 Huawei %%01OSPF/4/NBR_CHANGE_E(1)[2]:Neighbor changes
event: neighbor status changed. (ProcessId=256, NeighborAddress=1.100.168.192,
NeighborEvent=HelloReceived, NeighborPreviousState=Down, NeighborCurrentState=In
it)
[Huawei-ospf-1-area-0.0.0.0]network 192.168.100.0 0.0.0.255
Dec 11 2019 11:38:57-08:00 Huawei %%01OSPF/4/NBR_CHANGE_E(1)[3]:Neighbor changes
event: neighbor status changed. (ProcessId=256, NeighborAddress=1.100.168.192,
NeighborEvent=2WayReceived, NeighborPreviousState=Init, NeighborCurrentState=2Wa
y)
[Huawei-ospf-1-area-0.0.0.0]network 192.168.100.0 0.0.0.255
Dec 11 2019 11:38:57-08:00 Huawei %%01OSPF/4/NBR_CHANGE_E(1)[4]:Neighbor changes
event: neighbor status changed. (ProcessId=256, NeighborAddress=1.100.168.192,
NeighborEvent=AdjOk?, NeighborPreviousState=2Way, NeighborCurrentState=ExStart)

[Huawei-ospf-1-area-0.0.0.0]network 192.168.100.0 0.0.0.255
Dec 11 2019 11:38:57-08:00 Huawei %%01OSPF/4/NBR_CHANGE_E(1)[5]:Neighbor changes
event: neighbor status changed. (ProcessId=256, NeighborAddress=1.100.168.192,
NeighborEvent=NegotiationDone, NeighborPreviousState=ExStart, NeighborCurrentSta
te=Exchange)
[Huawei-ospf-1-area-0.0.0.0]network 192.168.100.0 0.0.0.255
Dec 11 2019 11:38:57-08:00 Huawei %%01OSPF/4/NBR_CHANGE_E(1)[6]:Neighbor changes
event: neighbor status changed. (ProcessId=256, NeighborAddress=1.100.168.192,
NeighborEvent=ExchangeDone, NeighborPreviousState=Exchange, NeighborCurrentState
=Loading)
[Huawei-ospf-1-area-0.0.0.0]network 192.168.100.0 0.0.0.255
Dec 11 2019 11:38:57-08:00 Huawei %%01OSPF/4/NBR_CHANGE_E(1)[7]:Neighbor changes
event: neighbor status changed. (ProcessId=256, NeighborAddress=1.100.168.192,
NeighborEvent>LoadingDone, NeighborPreviousState>Loading, NeighborCurrentState=F
ull)
[Huawei-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255
[Huawei-ospf-1-area-0.0.0.0]network 10.3.1.0 0.0.0.255
[Huawei-ospf-1-area-0.0.0.0]network 10.3.2.0 0.0.0.255
[Huawei-ospf-1-area-0.0.0.0]q
[Huawei-ospf-1]ip r
[Huawei-ospf-1]q
[Huawei]ip r
[Huawei]ip rp
[Huawei]ip rou
[Huawei]ip route-
[Huawei]ip route-static 0.0.0.0 0.0.0.0 12.1.1.100
[Huawei]o
[Huawei]os
[Huawei]ospf 1
[Huawei-ospf-1]de
[Huawei-ospf-1]default-r
[Huawei-ospf-1]default-route-advertise
[Huawei-ospf-1]q
[Huawei]q
<Huawei>save AR1.cfg
Are you sure to save the configuration to AR1.cfg? (y/n) [n]:t
Error: Input error
<Huawei>y
^
Error: Unrecognized command found at '^' position.
```

```
<Huawei>save AR1.cfg
Are you sure to save the configuration to AR1.cfg? (y/n)[n]:y
It will take several minutes to save configuration file, please wait.....
Configuration file had been saved successfully
```

图8 OSPF配置图

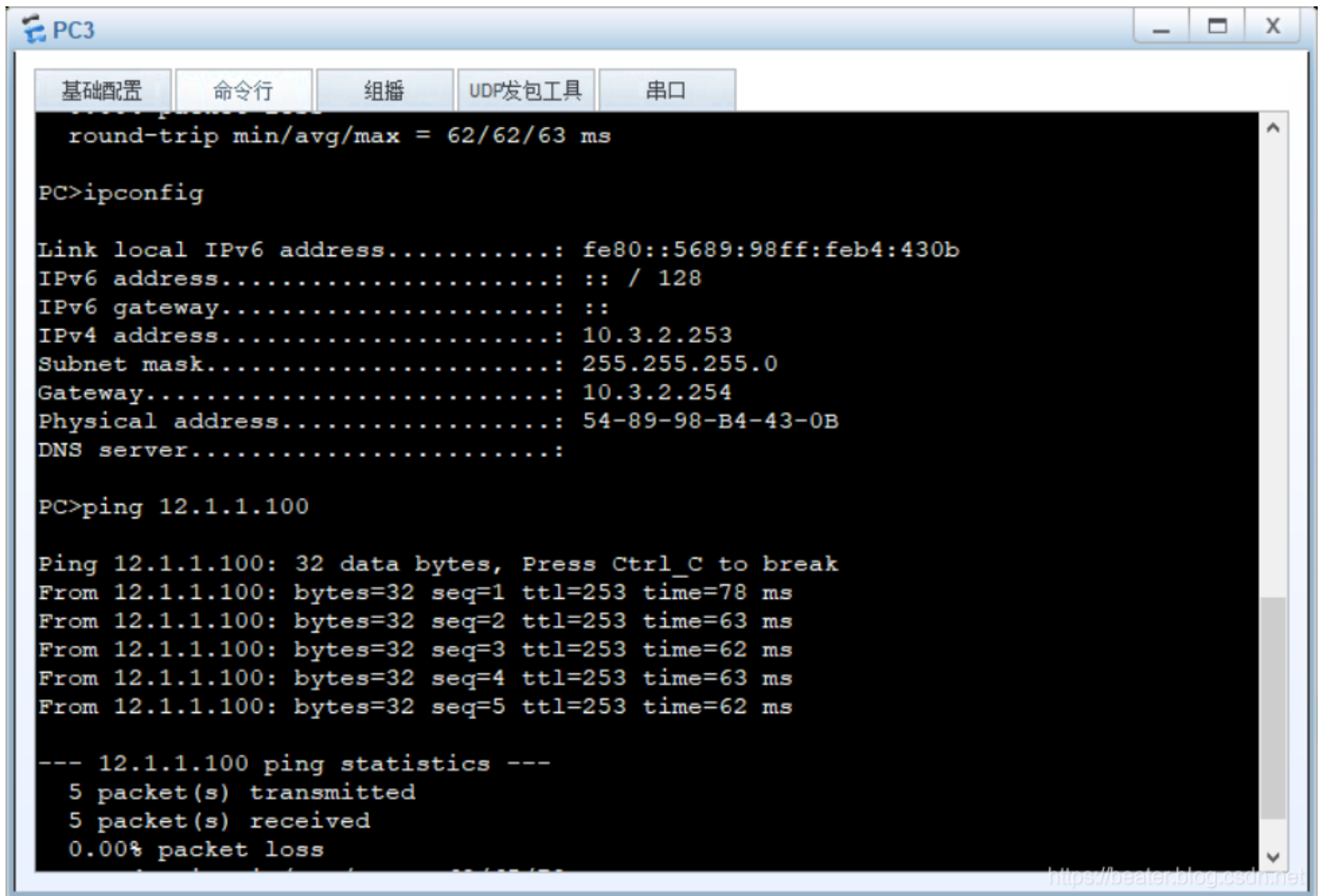
5. NAT配置

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]acl num 2000
[Huawei-acl-basic-2000]ru
[Huawei-acl-basic-2000]rule 0 p
[Huawei-acl-basic-2000]rule 0 permit s
[Huawei-acl-basic-2000]rule 0 permit source 10.3.1.0 0.0.0.255
[Huawei-acl-basic-2000]rule 5 permit source 10.3.2.0 0.0.0.255
[Huawei-acl-basic-2000]rule 10 permit source 192.168.3.0 0.0.0.255
[Huawei-acl-basic-2000]rule 15 permit source 192.168.100.0 0.0.0.255
[Huawei-acl-basic-2000]q
[Huawei]int g0/0/1
[Huawei-GigabitEthernet0/0/1]nat o
[Huawei-GigabitEthernet0/0/1]nat outbound 2000
[Huawei-GigabitEthernet0/0/1]nat s
[Huawei-GigabitEthernet0/0/1]nat sta
[Huawei-GigabitEthernet0/0/1]nat static g
[Huawei-GigabitEthernet0/0/1]nat static global 12.1.1.10 ins
[Huawei-GigabitEthernet0/0/1]
```

图9 NAT配置图

6. 实验结果

如下图10所示，配置后可以ping通外网



The image shows a terminal window titled 'PC3' with a menu bar containing '基础配置', '命令行', '组播', 'UDP发包工具', and '串口'. The terminal output is as follows:

```
round-trip min/avg/max = 62/62/63 ms

PC>ipconfig

Link local IPv6 address.....: fe80::5689:98ff:feb4:430b
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 10.3.2.253
Subnet mask.....: 255.255.255.0
Gateway.....: 10.3.2.254
Physical address.....: 54-89-98-B4-43-0B
DNS server.....:

PC>ping 12.1.1.100

Ping 12.1.1.100: 32 data bytes, Press Ctrl_C to break
From 12.1.1.100: bytes=32 seq=1 ttl=253 time=78 ms
From 12.1.1.100: bytes=32 seq=2 ttl=253 time=63 ms
From 12.1.1.100: bytes=32 seq=3 ttl=253 time=62 ms
From 12.1.1.100: bytes=32 seq=4 ttl=253 time=63 ms
From 12.1.1.100: bytes=32 seq=5 ttl=253 time=62 ms

--- 12.1.1.100 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
```

A URL <https://beatenblog.csdn.net/> is visible in the bottom right corner of the terminal window.

图10 实验结果样式

二、抓包协议分析

这里以PC1的报文为例，抓包开始前先将PC1关闭，开启Wireshark，开始抓包，然后开启PC1，并在PC1上ping 外网，截取该过程中的报文，并对截取的报文进行分析。在报文内容中大致有如下几个协议报文：VRRP协议、OSPF协议、STP、DHCP、ARP协议报文。

2.1 VRRP协议

虚拟路由冗余协议(Virtual Router Redundancy Protocol, 简称VRRP)是由IETF提出的解决局域网中配置静态网关出现单点失效现象的路由协议，1998年已推出正式的RFC2338协议标准。VRRP广泛应用在边缘网络中，它的设计目标是支持特定情况下IP数据流量失败转移不会引起混乱，允许主机使用单路由器，以及及时在实际第一跳路由器使用失败的情形下仍能够维护路由器间的连通性。

下面我们来看RFC中规定的VRRP格式

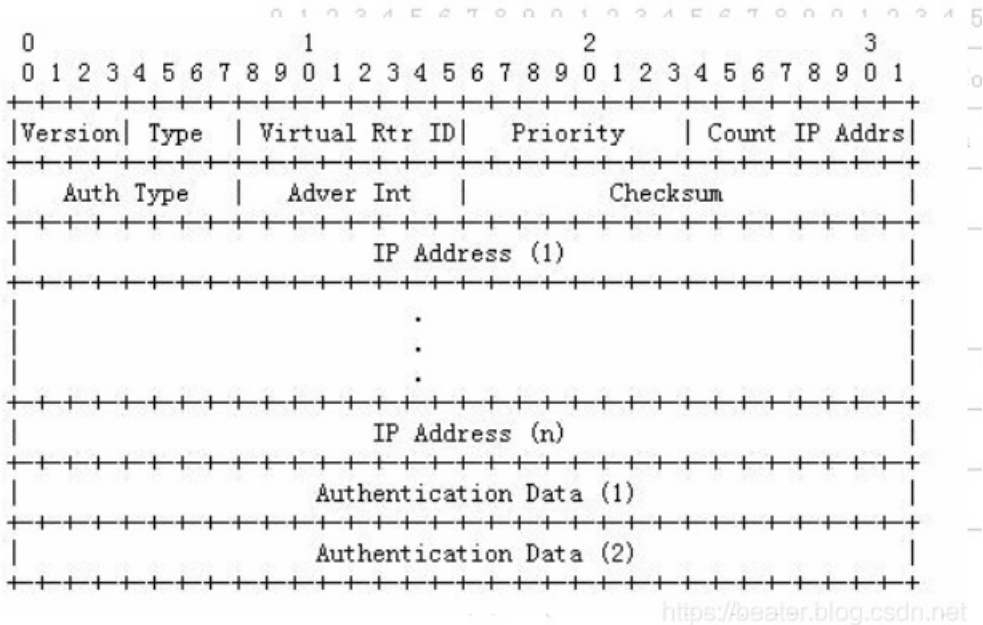


图11 VRRP协议报文格式（摘自RFC 3768）

```

v Virtual Router Redundancy Protocol
  v Version 2, Packet type 1 (Advertisement)
    0010 .... = VRRP protocol version: 2
    .... 0001 = VRRP packet type: Advertisement (1)
  Virtual Rtr ID: 10
  Priority: 120 (Non-default backup priority)
  Addr Count: 1
  Auth Type: No Authentication (0)
  Adver Int: 1
  Checksum: 0x5af2 [correct]
  [Checksum Status: Good]
  IP Address: 10.3.1.254

```

Source: <https://beater.blog.csdn.net>

图12 VRRP协议报文

参照图11的标准报文格式及实际截取的图12报文内容可得知，该报文，VRRP版本为2。

Type: 该字段指明了VRRP报文的类型，RFC3768只定义了一种VRRP报文，那就是VRRP通告报文，该字段总是置为1，若收到的VRRP通告报文拥有非1的类型值，那么会被丢弃。

Addr Count: VRRP通告报文中包含的IP地址数量，这个字段其实就是为一个VRRP虚拟路由器所分配的IP地址的数量。这里由于抓包是对PC1抓取的包因此只有一个IP地址。

Auth Type: 认证类型字段，是一个8位的无符号整数，一个虚拟路由器只能使用一种认证类型，如果Backup路由器收到的通告报文中认证类型字段是未知的或和本地配置的不匹配，那么它将丢弃该数据包。

类型 0 – 无认证，此时下面的Authentication Data字段将会被置为全0，接收到的路由器也会忽略此字段。

Adver Int:此字段规定了Master路由器向外发送VRRP通告报文的时间间隔，以秒为单位，取值范围是[1,255]，若没有人工配置，缺省为1秒。

2.2 OSPF报文

首先，我们先来看看OSPF协议的定义：

OSPF路由协议是一种典型的链路状态（Link-state）的路由协议，一般用于同一个路由域内。在这里，路由域是指一个自治系统（Autonomous System），即AS，它是指一组通过统一的路由政策或路由协议互相交换路由信息的网络。在这个AS中，所有的OSPF路由器都维护一个相同的描述这个AS结构的数据库，该数据库中存放的是路由域中相应链路的状态信息，OSPF路由器正是通过这个数据库计算出其OSPF路由表的。

作为一种链路状态的路由协议，OSPF将链路状态组播数据LSA（Link State Advertisement）传送给在某一区域内的所有路由器，这一点与距离矢量路由协议不同。运行距离矢量路由协议的路由器是将部分或全部的路由表传递给与其相邻的路由器。

在信息交换的安全性上，OSPF规定了路由器之间的任何信息交换在必要时都可以经过认证或鉴别（Authentication），以保证只有可信的路由器之间才能传播选路信息。OSPF支持多种鉴别机制，并且允许各个区域间采用不同的鉴别机制。OSPF对链路状态算法在广播式网络（如以太网）中的应用进行了优化，以尽可能地利用硬件广播能力来传递链路状态报文。通常链路状态算法的拓扑图中的一个结点代表一个路由器。若K个路由器都连接到以太网上，在广播链路状态时，关于这K个路由器的报文将达到K的平方个。为此，OSPF在拓扑结构图允许一个结点代表一个广播网络。每个广播网络上所有路由器发送链路状态报文，报告该网络中的路由器的链路状态。

接下来，还是直接上报文格式吧，如下图13。

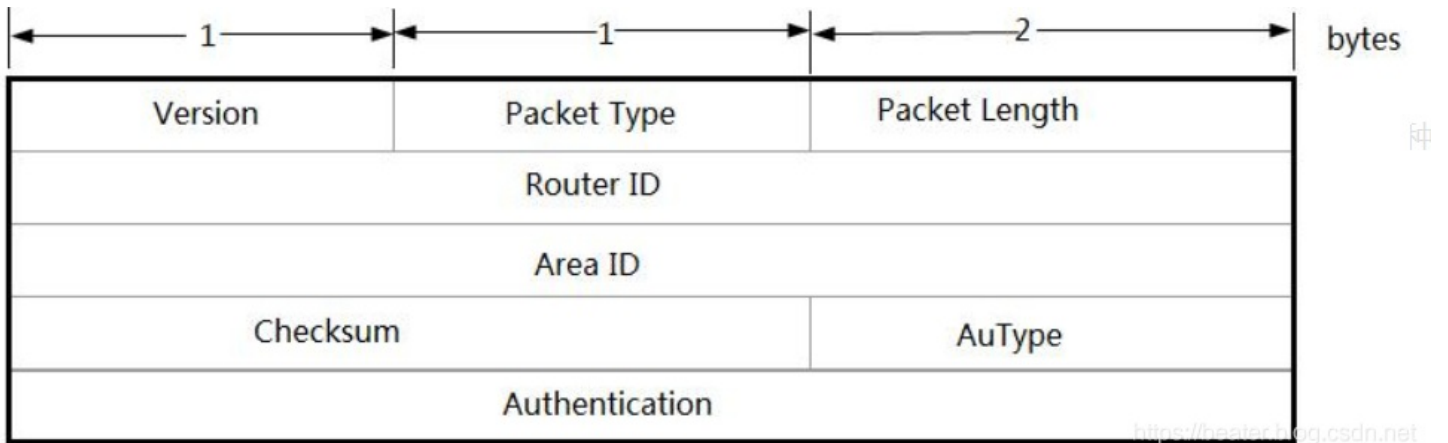


图13 OSPF协议报文格式

接下来我们再来看我们截取的OSPF报文，首先是Hello Packet报文。

```

v Open Shortest Path First
  v OSPF Header
    Version: 2
    Message Type: Hello Packet (1)
    Packet Length: 44
    Source OSPF Router: 10.3.1.1
    Area ID: 0.0.0.0 (Backbone)
    Checksum: 0xe696 [correct]
    Auth Type: Null (0)
    Auth Data (none): 0000000000000000
  v OSPF Hello Packet
    Network Mask: 255.255.255.0
    Hello Interval [sec]: 10
    > Options: 0x02, (E) External Routing
    Router Priority: 1
    Router Dead Interval [sec]: 40
    Designated Router: 10.3.1.1
    Backup Designated Router: 0.0.0.0

```

<https://beater.blog.csdn.net>

图14 OSPF中Hello Packet报文

Message Type :报文类型字段，标识对应报文的类型。OSPF有5种报文，分别是：Hello报文、DD报文、LSR报文、LSU报文、LSAck报文。

Packet Length: 包长度字段，占2个字节。它是指整个报文（包括OSPF报头部分和后面各报文内容部分）的字节长度。由图14可知，该报文长度为44个字节。

Auth Type: 认证类型字段，占2个字节，指定所采用的认证类型，0为不认证，1为进行简单认证，2采用MD5方式认证。

由报文中内容可知，OSPF协议版本为2。本报文类型为Hello Packet。由于本次抓包中没有抓过除了Hello报文以外的部分，因此这里暂不分析其他类型报文。

下面我们来分析Hello报文部分

OSPF协议使用一种称之为Hello的报文来建立和维护相邻邻居路由器之间的链接关系。这个报文很简单的，容量很小，仅用来向邻居路由器证明自己的存在，就像人与人之间的打招呼一样。我们在第8章中已经知道，RIP邻居路由器之间的邻接关系建立都是定期的路由更新报文进行的，通过定期的路由更新来同时向邻居RIP路由器证明自己的存在。显然OSPF的这种Hello报文更简单，可大大减小网络中的报文传输流量。

Hello报文被周期性（默认为10秒）地发向邻居路由器接口发送，如果在设定时间（默认为40秒，通常至少是Hello包发送时间间接4倍）内没有收到对方OSPF路由器发送来的Hello报文，则本地路由器会认为该对方路由器无效。报文内容包括一些定时器设置、DR、BDR以及本路由器已知的邻居路由器。

字段名	长度	功能
Network Mask	4字节	发送Hello报文接口所在的子网掩码
HelloInterval	2字节	指定发送Hello报文的时间间隔，默认为10秒
Options	1字节	可选项，包括E:允许泛洪AS-external-LAS; MC: 允许转发IP组播报文; N/P: 允许处理Type 7 LSA; DC: 允许处理按需链路
Rtr Pri	1字节	指定DR优先级，默认为1。如果设为0，则表示本路由器不参与DR/BDR选举
RouterDeadInterval	4字节	指定路由器失效时间，默认为40秒。如果在此时间内没有收到邻居路由器发来的Hello报文，则认为该邻居路由器已失效
Designated Router	4字节	指定DR的接口IP地址
Backup Designated Router	4字节	指定BDR的接口IP地址
Neighbor	4字节	指定邻居路由器的RID。下面的省略号 (...) 表示可以指定多个邻居路由器RID

图15 Hello Packet报文格式

接下来我们再看看我们抓取的报文中的Hello报文部分。

```

v OSPF Hello Packet
  Network Mask: 255.255.255.0
  Hello Interval [sec]: 10
  v Options: 0x02, (E) External Routing
    0... .... = DN: Not set
    .0.. .... = O: Not set
    ..0. .... = (DC) Demand Circuits: Not supported
    ...0 .... = (L) LLS Data block: Not Present
    .... 0... = (N) NSSA: Not supported
    .... .0.. = (MC) Multicast: Not capable
    .... ..1. = (E) External Routing: Capable
    .... ...0 = (MT) Multi-Topology Routing: No
  Router Priority: 1
  Router Dead Interval [sec]: 40
  Designated Router: 10.3.1.1
  Backup Designated Router: 0.0.0.0

```

图16 Hello 报文

如图16所示，在Hello报文中展示了我们的子网掩码为24位1，发送时间间隔为10s,路由器失效时间为40s，DR的接口IP地址为10.3.1.1，DR优先级为1。

2.3 DHCP 动态地址分配

DHCP协议的工作过程如下：

- 1.发现阶段：即DHCP客户机寻找DHCP服务器的阶段。DHCP客户机以广播的方式发送DHCP discover 发现信息来寻找DHCP服务器（因为DHCP服务器的IP地址对客户机来说是未知的），即向255.255.255.255发送特定的广播信息，网络上每一台安装了TCP/IP协议的主机都会接收到这种广播信息，但只有DHCP服务器才会作出响应。
- 2.提供阶段：即DHCP服务器提供IP地址的阶段。在网络中收到DHCP discover发现信息的DHCP服务器都会作出响应，它从尚未出租的IP地址中挑选一个分配给DHCP客户机，向DHCP客户机发送一个包含出租的IP地址和其他设置额DHCP offer提供信息。
- 3.选择阶段：DHCP客户机选择某台DHCP服务器提供的IP地址的阶段。如果有多台DHCP服务器向DHCP客户机发来的DHCP offer，客户机只接收第一个收到的DHCP offer，然后它以广播的方式回答一个DHCP request请求信息。该信息中包含它所选定的DHCP服务器请求IP地址的内容。之所以要以广播的方式回答，是为了通知所有的DHCP服务器，它将选择某台DHCP服务器所提供的IP地址。
- 4.确认阶段：即DHCP服务器确认所提供的IP地址的阶段。当DHCP服务器收到DHCP客户机回答的DHCP resquest请求后，它便向DHCP客户机发送一个包含它提供的IP地址和其他设置的DHCP ACK确认信息，告诉DHCP客户机可以使用它所提供的IP地址。然后DHCP客户机便将其TCP/IP协议与网卡绑定，除了DHCP客户机所选择的服务器IP外，其他的DHCP服务器都将收回曾提供的IP地址
- 5.重新登陆：以后DHCP客户机每次登陆网络时，就不需要再发送DHCP discover发现信息了。而是直接发送包含前一次所分配IP地址的DHCP resquest请求。当DHCP服务器收到这一信息后，它会尝试让客户机继续使用原来的IP并回答一个DHCP ACK确认信息，如果此IP地址无法分配个原来的DHCP客户机时（比如IP分配给其他DHCP客户机使用），则DHCP服务器给DHCP客户机回答一个DHCP NACK 否认消息，当原来的DHCP客户机收到此消息后，它就必须重新发送DHCP discover发现信息重新请求新的IP地址。
- 6.更新租约：DHCP服务器向DHCP客户机出租的IP地址一般都由一个租借期限，期满后DHCP服务器会收回出租的IP地址。如果DHCP客户机要延长其IP租约，则必须更新其租约。DHCP客户机启动时和IP租约期限过一半时，DHCP客户机都会自动向DHCP服务器发送其更新租约的信息。

接下里让我们看看我们抓到的DHCP报文

No.	Time	Source	Destination	Protocol	Length	Info
98	61.515000	0.0.0.0	255.255.255.255	DHCP	410	DHCP Discover - Transaction ID 0x78e3
104	63.078000	10.3.1.254	10.3.1.253	DHCP	342	DHCP Offer - Transaction ID 0x78e3
112	65.500000	0.0.0.0	255.255.255.255	DHCP	410	DHCP Request - Transaction ID 0x78e3
113	65.531000	10.3.1.254	10.3.1.253	DHCP	342	DHCP ACK - Transaction ID 0x78e3

图17 DHCP报文总览

如上图可见，由于抓包时间较短，只有发现、提供、选择、确认四个阶段，后两个阶段由于未涉及，因此没有相关报文。

2.3.1 DHCP Discover报文

接下来我们来看看DHCP的发现阶段的报文。


```
Dynamic Host Configuration Protocol (Offer)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x000078e3
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.3.1.253
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: HuaweiTe_bf:57:a0 (54:89:98:bf:57:a0)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (51) IP Address Lease Time
  > Option: (59) Rebinding Time Value
  > Option: (58) Renewal Time Value
  > Option: (54) DHCP Server Identifier (10.3.1.254)
  > Option: (255) End
  Padding: 0000000000000000000000000000000000000000000000000000000000000000
```

<https://beater.blog.csdn.net>

图18 DHCP Offer报文段

DHCP服务器提供了一个可用的IP,在数据包的Your (client) IP Address字段可以看到DHCP服务器提供的可用IP。除此之外，如图中红色矩形框的内容所示，服务器还发送了子网掩码，路由器，DNS，域名，IP地址租用期等信息。

2.3.3 DHCP Request报文段

这个包由于没有太多有效信息，就不再展示。

当Client收到了DHCP Offer包以后（如果有多个可用的DHCP服务器，那么可能会收到多个DHCP Offer包），确认有可以和它交互的DHCP服务器存在，于是Client发送Request数据包，请求分配IP。

此时的源IP和目的IP依然是0.0.0.0和255.255.255.255。

2.3.4 DHCP ACK报文段

服务器用DHCP ACK包对DHCP请求进行响应。


```
Dynamic Host Configuration Protocol (ACK)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x000078e3
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.3.1.253
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: HuaweiTe_bf:57:a0 (54:89:98:bf:57:a0)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  < Option: (53) DHCP Message Type (ACK)
    Length: 1
    DHCP: ACK (5)
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (51) IP Address Lease Time
  > Option: (59) Rebinding Time Value
  > Option: (58) Renewal Time Value
  > Option: (54) DHCP Server Identifier (10.3.1.254)
  > Option: (255) End
```

DHCP的ACK报文段

<https://beater.blog.csdn.net>

图19 DHCP ACK报文段

在数据包中包含以下信息，表示将这些资源信息分配给Client.

Your(client) IP address:分配给Client的可用IP。

后面有许多项option信息，前两项是DHCP服务器发送的消息类型（ACK）和服务器的身份标识，后面几项是：

Subnet Mask:Client端分配到的IP的子网掩码；

Router:路由器

Domain Name Server:DNS,域名服务器

Domain Name:域名

IP Address Lease Time:IP租用期。

2.4 ARP协议

首先我们先来介绍一下ARP协议：地址解析协议，即ARP（Address Resolution Protocol），是根据IP地址获取物理地址的一个TCP/IP协议。主机发送信息时将包含目标IP地址的ARP请求广播到局域网络上的所有主机，并接收返回消息，以此确定目标的物理地址；收到返回消息后将该IP地址和物理地址存入本机ARP缓存中并保留一定时间，下次请求时直接查询ARP缓存以节约资源。地址解析协议是建立在网络中各个主机互相信任的基础上的，局域网络上的主机可以自主发送ARP应答消息，其他主机收到应答报文时不会检测该报文的真实性就会将其记入本机ARP缓存；由此攻击者就可以向某一主机发送伪ARP应答报文，使其发送的信息无法到达预期的主机或到达错误的主机，这就构成了一个ARP欺骗。ARP命令可用于查询本机ARP缓存中IP地址和MAC地址的对应关系、添加或删除静态对应关系等。相关协议有RARP、代理ARP。NDP用于在IPv6中代替地址解析协议。

这里由于没有清空路由表，所以ARP一次询问就直接得到回复。

125 70.468000	HuaweiTe_bf:57:a0	Broadcast	ARP	60 Who has 10.3.1.254? Tell 10.3.1.253
126 70.500000	IETF-VRRP-VRID_0a	HuaweiTe_bf:57:a0	ARP	60 10.3.1.254 is at 00:00:5e:00:01:0a

图20 ARP报文段

2.5 ICMP协议

ICMP协议是一个网络层协议。一个新搭建好的网络，往往需要先进行一个简单的测试，来验证网络是否畅通；但是IP协议并不提供可靠传输。如果丢包了，IP协议并不能通知传输层是否丢包以及丢包的原因。

所以我们就需要一种协议来完成这样的功能—ICMP协议。ICMP协议的功能主要有：

- 1.确认IP包是否成功到达目标地址
- 2.通知在发送过程中IP包被丢弃的原因

127 70.531000	10.3.1.253	12.1.1.100	ICMP	74 Echo (ping) request	id=0xb767, seq=1/256, ttl=128 (reply in 128)
128 70.593000	12.1.1.100	10.3.1.253	ICMP	74 Echo (ping) reply	id=0xb767, seq=1/256, ttl=253 (request in 127)

图21 ICMP报文请求及回应报文

在ICMP中，一组request和reply对应，对应方法为id号相同则说明是一对请求、响应报文。