检测工具，发送免费ARP，携带了毒化后的错误的MAC地址覆盖正确的ARP映射。在ARP缓存表机制存在一个缺陷，就是当请求主机收到ARP应答包后，不会去验证自己是否向对方主机发送过ARP请求包，就直接把这个返回包中的IP地址与MAC地址的对应关系保存进ARP缓存表中，如果包含原有相同IP对应关系，原有的则会被替换。

如图49-2所示，攻击者B把A向网关C的请求，毒化A的映射表项到B，同时毒化C（10.1.1.2 b.b.b.b）的表项，所有的流量都转到了B设备。

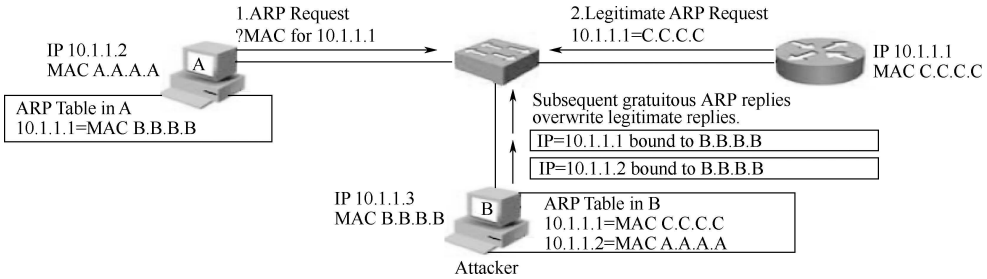

图49-2　ARP毒化攻击示意图

动态ARP检测技术基于DHCP Snooping绑定表（其中包含正确的IP和MAC的映射），丢弃免费ARP，停止ARP毒化和中间人攻击，限制ARP请求，也终止扫描攻击。通常上行接口（如Trunk链路）配置Trust，连接PC接口默认Untrusted。如图49-3所示为实施计划。

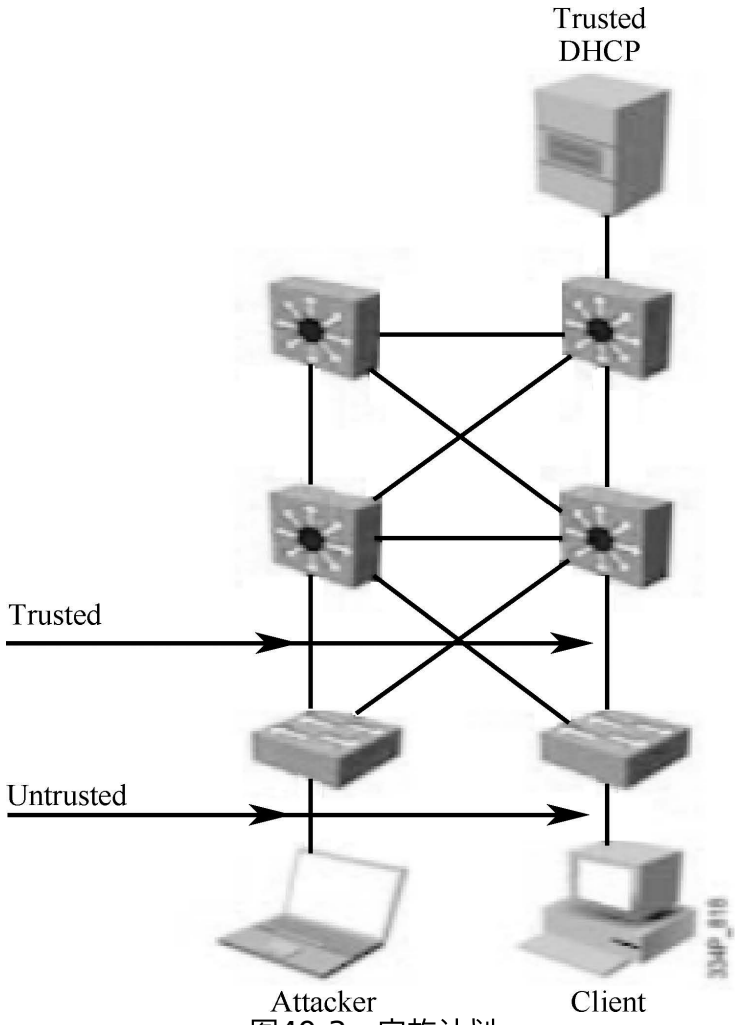

图49-3　实施计划

IP Source Guard也是DHCP Snooping的衍生技术，用于抵御IP地址的欺骗，利用DHCP Snooping的绑定表，跟踪IP到端口的关联，从而抵御IP地址欺骗。

49.2　实验需求及拓扑描述

局域网交换机安全实验拓扑如图49-4所示。

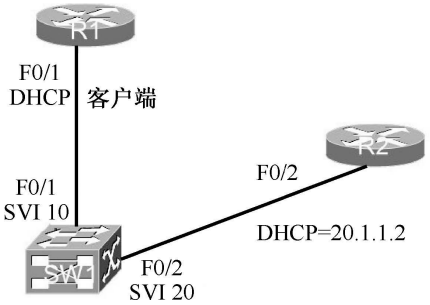

图49-4　局域网交换机安全实验拓扑图

49.3　实验步骤

49.3.1　完成交换机的VLAN创建、划分端口及SVI

```
vlan 10
vlan 20
interface FastEthernet0/1
  switchport access vlan 10
  switchport mode access
 spanning-tree portfas
interface FastEthernet0/2
  switchport access vlan 20
  switchport mode access
 spanning-tree portfast
```

验证：

```
SW1#show vlan id 10

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
10   VLAN0010                          active    Fa0/1,

VLAN  Type   SAID           MTU     Parent  RingNo  BridgeNo  Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
10    enet   100010      1500   -       -       -          -     -       0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

SW1#show vlan id 20

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
```

```
20   VLAN0020                         active    Fa0/2


VLAN  Type   SAID           MTU     Parent  RingNo  BridgeNo  Stp
BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------
- ------ ------
20    enet   100020      1500   -       -       -          -     -
0      0


Remote SPAN VLAN----------------
Disabled


Primary Secondary Type              Ports
------- --------- ----------------- ---------------------------
---------------
```

创建SVI接口：

```
ip routing——不要忘记开启路由功能
interface Vlan10
 ip address 10.1.1.1 249.255.255.0
interface Vlan20
ip address 20.1.1.1 255.255.255.0
```

验证：

```
SW1#show ip route connected
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Vlan10



L       10.1.1.1/32 is directly connected, Vlan10
C       20.1.1.0/24 is directly connected, Vlan20
```

```
L        20.1.1.1/32 is directly connected, Vlan20
```

49.3.2 完成DHCP的基本配置

R2为DHCP服务器，配置如下：

```
interface FastEthernet0/0
 ip address 20.1.1.2 255.255.255.0
ip dhcp excluded-address 10.1.1.1
ip dhcp pool Ender
network 10.1.1.0 255.255.255.0
 default-router 10.1.1.1
```

R1充当DHCP客户端：

```
interface FastEthernet0/0
 ip address dhcp
```

此时DHCP服务器无法获得来自R1的报文，因为没有DHCP中继代理，同时即使得到来自R1的Discovery报文也无法回复Offer报文，因为R2没有去往10.1.1.0/24的路由。

所以我们要在SW1下做中继代理，在R2书写静态路由。

```
SW1：
interface Vlan10
```

```
  ip address 10.1.1.1 255.255.255.0
ip helper-address 20.1.1.2——启用DHCP代理，指向DHCP服务器地址
R2：
ip route 10.1.1.0 255.255.255.0 20.1.1.1——R2配置静态路由，可以返回数据包到10.1.1.0/24网段
```

验证：

```
R2#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

49.3.3 在交换机上完成DHCP Snooping

首先在VLAN10下开启DHCP Snooping服务。

```
ip dhcp snooping——全局开启Snooping
ip dhcp snooping vlan 10——针对VLAN10开启Snooping
interface FastEthernet0/1
  switchport access vlan 10
  switchport mode access
```

```
 spanning-tree portfast
  ip dhcp snooping limit rate 30——该接口直连客户端，所以默认是Untrust，我们限制DHCP客户端（如果是恶意的客户端）每秒的最高发包频率为30，默认没有限制
```

验证：

```
SW1#show ip dhcp snooping
Switch DHCP snooping is enabled——已经使能
DHCP snooping is configured on following VLANs:
10——在VLAN 10下使能
DHCP snooping is operational on following VLANs:
10
Smartlog is configured on following VLANs:
none
Smartlog is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled——默认情况下，DHCP的Option 82已经开启
   circuit-id default format: vlan-mod-port
   remote-id: 0026.997b.3b80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following
```

```
Interfaces:

Interface                   Trusted    Allow option    Rate
limit (pps)
-----------------------    -------    ------------    ---------
-------
FastEthernet0/1            no         no              30
  Custom circuit-ids:
SW1#show ip dhcp snooping binding——绑定表已经形成，F0/1接口在VLAN10
中对应的MAC地址得到了10.1.1.2的地址，这张表非常重要
MacAddress               IpAddress            Lease(sec)   Type
VLAN  Interface
------------------   ---------------   ----------   -------------
----  --------------------
00:26:CB:72:1F:04   10.1.1.2         83268       dhcp-snooping
10    FastEthernet0/1
Total number of bindings: 1
```

DHCP服务器的情况：

```
R2#show ip dhcp binding




Bindings from all pools not associated with VRF:
IP address          Client-ID/               Lease expiration
Type
```

```
                    Hardware address/
                    User name
10.1.1.2              0063.6973.636f.2d30.    Feb 16 2001 05:33
AM    Automatic
                    3032.355e.6362.3732.
                    2e31.6630.342d.4661.
                    302f.30
```

在VLAN20也开启DHCP Snooping：

```
SW1(config)#ip dhcp snooping vlan 20
```

关闭R1的F0/0接口释放地址：

```
R1(config)#interface f0/0
R1(config-if)#shutdown
R2#clear ip dhcp binding *
R2#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address           Client-ID/               Lease expiration
Type
                    Hardware address/
                    User name
```

然后开启R1的接口，尝试重新获得地址。

R2开启debug ip dhcp server packet，会发现并无报文发过来。这是因为我们在VLAN 20开启了Snooping，但是却没有Trust连接DHCP服务器的接口。同样的道理，如果存在多个交换机，存在Trunk，我们应该在这些接口配置Trust：

```
interface FastEthernet0/2
  switchport access vlan 20
  switchport mode access
 spanning-tree portfast
ip dhcp snooping trust——配置Trust接口
```

验证：

```
SW1#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20
DHCP snooping is operational on following VLANs:
10,20
Smartlog is configured on following VLANs:
none
Smartlog is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
```

```
   remote-id: 0026.997b.3b80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP  snooping  trust/rate  is  configured  on  the  following
Interfaces:

Interface                    Trusted     Allow option     Rate
limit (pps)
-----------------------    -------    ------------    ---------
-------
FastEthernet0/1            no         no              30
  Custom circuit-ids:
FastEthernet0/2            yes        yes             unlimited
——该接口为一个信任接口
  Custom circuit-ids:
R2#show ip dhcp binding——R1重新获得10.1.1.3的地址
Bindings from all pools not associated with VRF:
IP address           Client-ID/               Lease expiration
Type
                    Hardware address/
                    User name
10.1.1.3             0063.6973.636f.2d30.     Feb 16 2001 06:31
AM    Automatic
                    3032.362e.6362.3732.
                    2e31.6630.342d.4661.
                    302f.30
```

测试：

```
R1#ping 20.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.1.1.2, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max =
1/1/4 ms
```

49.3.4 实现DAI（动态ARP监测）技术

SW1配置：

```
ip arp inspection vlan 10,20——针对VLAN10和VLAN20开启DAI
interface FastEthernet0/2
  switchport access vlan 20
  switchport mode access
  ip arp inspection trust
 spanning-tree portfast
  ip dhcp snooping trust——上行接口是可信任端口，其他默认为Untrust
```

此时不允许客户端随便修改MAC地址（或者换不同设备，因为不同设备有不同的MAC地址），我们反其道而行之用于验证：

```
R1(config-if)#interface FastEthernet0/0
R1(config-if)# mac-address 0001.0001.0001
```

查看SW1：

```
SW1#
*Mar  1 07:19:24.077: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid
ARPs (Req) on Fa0/1, vlan
  10.([0001.0001.0001/10.1.1.3/0026.997b.3bc5/10.1.1.1/07:19:23
UTC Mon Mar 1 1993])
*Mar  1 07:19:24.077: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid
ARPs (Res) on Fa0/1, vlan
  10.([0001.0001.0001/10.1.1.3/ffff.ffff.ffff/10.1.1.3/07:19:23
UTC Mon Mar 1 1993])
```

动态ARP监测功能生效，拒绝了无效的ARP请求：

```
R1#ping 20.1.1.2—此时无法到达目标地址（前边验证时没问题）

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.1.1.2, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
R1#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type
Interface
```

```
Internet  10.1.1.1                0   Incomplete      ARPA——去往网关的MAC地址无效
Internet  10.1.1.3                    -    0001.0001.0001  ARPA   FastEthernet0/0
```

当然我们是有补救措施的，可以通过手动添加放行没有在DHCP Snooping绑定表中的地址：

```
SW1(config)#arp access-list Ender
SW1(config-arp-nacl)#permit ip host 10.1.1.3 mac host 1.1.1——书写ARP的ACL放行10.1.1.3对应的MAC地址
SW1(config)#ip arp inspection filter Ender vlan 10 static——应用ARP的ACL，可选的增加log，此处无增加
SW1#show arp  access-list
ARP access list Ender
permit ip host 10.1.1.3 mac host 0001.0001.0001
R1#ping 20.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.1.1.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
R1#show arp
```

```
Protocol  Address          Age (min)  Hardware Addr   Type
Interface
Internet  10.1.1.1               0   0026.997b.3bc5  ARPA
FastEthernet0/0



Internet  10.1.1.3               -   0001.0001.0001  ARPA
FastEthernet0/0
```

49.3.5 IP源保护技术、跟踪IP到端口的关联、抵御IP地址欺骗攻击

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
  ip verify source——开启源保护技术，如果接口下的IP地址和绑定表中的地址不匹配则可以关闭接口，同时可以和端口安全结合使用
```

修改R1地址：

```
R1(config-if)#ip address 10.1.1.100 255.255.255.0
```

查看SW1：

```
*Mar  1 07:34:13.261: %SW_DAI-4-ACL_DENY: 1 Invalid ARPs (Res) on Fa0/1, vlan 10.([0001.0001.
 0001/10.1.1.100/ffff.ffff.ffff/10.1.1.100/07:34:13 UTC Mon Mar 1 1993])——此时交换机监测到VLAN10下的F0/1端口的到达的报文的源IP与绑定表不同，则拒绝ARP广播
R1#ping 20.1.1.2——无法ping通对端地址

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.1.1.2, timeout is 2 seconds:
.....
R1#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.100             -   0001.0001.0001  ARPA   FastEthernet0/0
```

当然我们还是有额外手段放行特殊情况下的手工修改IP的情况：

```
SW1(config)#ip source binding 0001.0001.0001 vlan 10 10.1.1.100 interface Fa0/1——该接口的MAC1.1.1对应的IP为10.1.1.100，注意此时绑定表可能已经改变，效果可能不明显。此时可能还需要修改ARP Access-list
SW1(config)#arp access-list Ender
SW1(config-arp-nacl)#permit ip host 10.1.1.100 mac host 1.1.1
```

测试：

```
R1#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max =
1/2/4 ms
```

实验完成。

下面给出SW1的综合配置：

```
hostname SW1
ip routing
ip arp inspection vlan 10,20
ip arp inspection filter Ender vlan    10 static
!
ip dhcp snooping vlan 10,20
ip dhcp snooping
!
vlan 10
!
vlan 20
!
```

```
interface FastEthernet0/1
  switchport access vlan 10
  switchport mode access
 spanning-tree portfast
  ip verify source port-security
  ip dhcp snooping limit rate 30
!
interface FastEthernet0/2
  switchport access vlan 20
  switchport mode access
  ip arp inspection trust
 spanning-tree portfast
 ip dhcp snooping trust
!
!
interface Vlan10
 ip address 10.1.1.1 255.255.255.0
 ip helper-address 20.1.1.2
!
interface Vlan20
 ip address 20.1.1.1 255.255.255.0


!
ip source binding 0001.0001.0001 vlan 10 10.1.1.100 interface
Fa0/1
!
arp access-list Ender
```

```
permit ip host 10.1.1.3 mac host 0001.0001.0001
permit ip host 10.1.1.4 mac host 0001.0001.0001
permit ip host 10.1.1.100 mac host 0001.0001.0001
```

实验完成。

第50章
uRPF-单播逆向路径转发

本章要点

- **单播逆向路径转发基础**
- **实验需求及拓扑描述**
- **uRPF实验步骤**

50.1　单播逆向路径转发基础

单播逆向路径转发的英文全称为Unicast Reverse Path Forwarding。

网络管理员可以使用uRPF来帮助限制恶意流量（防范DoS或者DDoS攻击），uRPF的安全特性在路由器使能之后，用于验证到达的入方向流量报文是否进行转发，和组播技术中的RPF检查有类似之处。针对一个数据流，路由器会对它进行监测，如果源地址是无效的（是否存在于路由表是一个要点）那么将丢弃该报文。uRPF有3种工作模式：严格模式、松散模式和VRF模式（虚拟路由转发模式，用于MPLS VPN或者VRF的场景）。需要注意的是，并不是所有设备都支持这3种模式。

严格模式（strict mode）：从某个接口收到的报文，路由器返回该报文时，将用该接口作为出接口，即严格模式将严格检查数据流中源地址是否和去往该源的FIB表的出接口一致，如果不一致将丢弃报文，否则根据FIB表中数据包的目的地来转发该报文。但是严格的uRPF在异步路由的情况下将错误地丢弃报文，如图50-1所示，当Router A上记录的到Router B的路径为1，Router B上记录的到Router A的路径为2，如果在Router A上配置了uRPF，则会将Router B从路径2到来的报文丢弃，所以引入了松散模式。

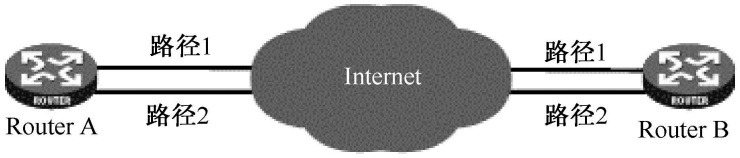

图50-1　uRPF示意图

松散模式（loose mode）：仅检查报文的源地址是否在FIB表中存在，而不再检查报文的入接口与FIB表是否匹配。这种更为“友好开放”的算法，使得部署在ISP-ISP端的uRPF既可以有效地阻止DDoS攻击，又可以避免错误地拦截合法用户的报文。

uRPF允许通过使用默认路由来通过检查；另外一个报文中源地址路由指向null0时（即路由表中存在该源的路由），该路由不能通过监测，将被丢弃；ACL的使用可以允许特定的、额外的源地址，即使没通过uRPF的监测也可以进行转发。

通常运营商之间采用松散模式，企业边缘采用严格模式，本节不涉及VRF模式。

注意： 在思科设备上，FIB表即运行了CEF之后形成的邻接表、路由表等一系列特性的转发表，所以运行uRPF之前一定要使能CEF。

50.2　实验需求及拓扑描述

本实验采用如图50-2所示的实验拓扑图。IP地址说明，每个设备有一个32位的环回口，如R1的环回口为11.1.1.1/32；直连地址说明，如R2上连接R3的地址为23.1.1.2/24，以此类推。

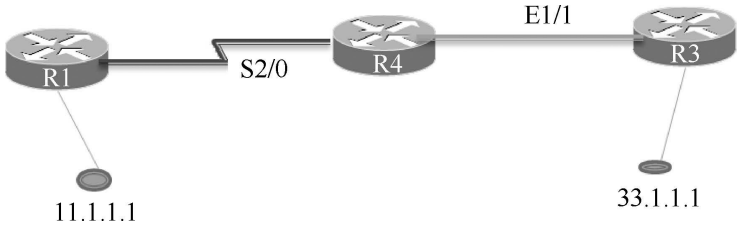

图50-2　uRPF实验拓扑图，R4模拟运营商网络

本实验中R4采用的IOS版本为Version 15.0（1）M3，其他设备为正常的12.4的IOS。

50.3　uRPF实验步骤

50.3.1　完成基本网络配置

R3完成默认路由，下一跳为R4：

```
interface Loopback0
  ip address 33.1.1.1 255.255.255.255
!
interface Ethernet1/1
  ip address 34.1.1.3 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 34.1.1.4
```

R1和R4运行eBGP，R4通告34.1.1.0的直连网段到BGP，R1通告环回口0的11.1.1.1到BGP，没有通告环回口1的1.1.1.1到BGP。

R1的配置：

```
interface Loopback0
  ip address 11.1.1.1 255.255.255.255
!
```

```
interface Serial2/0
  ip address 14.1.1.1 255.255.255.0
  serial restart-delay 0
 no dce-terminal-timing-enable
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
  network 11.1.1.1 mask 255.255.255.255
  neighbor 14.1.1.4 remote-as 200
 no auto-summary
```

R4的配置：

```
interface Ethernet1/1
  ip address 34.1.1.4 255.255.255.0
 duplex half
 !
interface Serial2/0
  ip address 14.1.1.4 255.255.255.0
  serial restart-delay 0
 !
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 network 34.1.1.0 mask 255.255.255.0
```

```
 neighbor 14.1.1.1 remote-as 100
no auto-summary
```

验证路由的情况：

```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 -
IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-
user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 34.1.1.4 to network 0.0.0.0

     34.0.0.0/24 is subnetted, 1 subnets
C       34.1.1.0 is directly connected, Ethernet1/1
     33.0.0.0/32 is subnetted, 1 subnets
C       33.1.1.1 is directly connected, Loopback0
S*   0.0.0.0/0 [1/0] via 34.1.1.4

R4#show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

     11.0.0.0/32 is subnetted, 1 subnets
B       11.1.1.1 [20/0] via 14.1.1.1, 00:14:57
     14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       14.1.1.0/24 is directly connected, Serial2/0
L       14.1.1.4/32 is directly connected, Serial2/0
     34.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       34.1.1.0/24 is directly connected, Ethernet1/1
L       34.1.1.4/32 is directly connected, Ethernet1/1

R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 -
IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-
user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     34.0.0.0/24 is subnetted, 1 subnets
B       34.1.1.0 [20/0] via 14.1.1.4, 00:15:14
     11.0.0.0/32 is subnetted, 1 subnets
C       11.1.1.1 is directly connected, Loopback0
     14.0.0.0/24 is subnetted, 1 subnets
C       14.1.1.0 is directly connected, Serial2/0
```

R3和R4都有R1环回口0的路由，而且R1和R4都有34.1.1.3的路由，所以数据包的情况如下：

```
R3#ping 11.1.1.1

Type escape sequence to abort.
Sending  5,  100-byte  ICMP  Echos  to  11.1.1.1,  timeout  is  2
```

```
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
16/44/68 ms
```

但是由于环回口1的路由没有通告，所以数据包的情况如下：

```
R3#ping  11.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.1.1.1, timeout is 2
seconds:
Packet sent with a source address of 33.1.1.1
.....
Success rate is 0 percent (0/5)
```

以上就是我们的基本环境，站在R4的角度，R1的环回口0（11.1.1.1）是一个正常路由；R3的环回口0（33.1.1.1）是非正常路由（路由表中不存在）。

50.3.2 配置严格的uRPF

在R4的E1/1接口进行配置：

```
interface Ethernet1/1
  ip address 34.1.1.4 255.255.255.0
```

```
 ip verify unicast source reachable-via rx——rx代表严格的uRPF检查
```

验证：

```
R3#ping    11.1.1.1 source loopback 0

Type escape sequence to abort.
Sending  5,  100-byte  ICMP  Echos  to  11.1.1.1,  timeout  is  2
seconds:
Packet sent with a source address of 33.1.1.1
.....
Success rate is 0 percent (0/5)
R4#show ip interface ethernet 1/1
Ethernet1/1 is up, line protocol is up
 ------------------------------------省略-----------------------
---------------
IP verify source reachable-via RX——RX代表严格模式的uRPF
   5 verification drops——有5个报文因为不符合规则而被丢弃
   0 suppressed verification drops
   0 verification drop-rate
```

分析： 因为R3上有默认路由指向R4，而R4通过BGP得到11.1.1.1的路由，正常情况下R4会路由去往11.1.1.1的数据，但是如果配置了uRPF的严格模式，即在路由表中查找源（33.1.1.1）的路由，而且必须和去往该路由（33.1.1.1）的下一跳（E1/1）吻合才能转发该数据，否则丢弃数据。

现在的场景，R4上没有去往33.1.1.1的路由，所以丢弃了报文，R4的路由表如下：

```
R4#  show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
         D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
         o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

      11.0.0.0/32 is subnetted, 1 subnets
B        11.1.1.1 [20/0] via 14.1.1.1, 02:51:45
      14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        14.1.1.0/24 is directly connected, Serial2/0
L        14.1.1.4/32 is directly connected, Serial2/0
```

```
      34.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        34.1.1.0/24 is directly connected, Ethernet1/1
L        34.1.1.4/32 is directly connected, Ethernet1/1
```

50.3.3　通过默认路由完成源的严格uRPF配置

我们先做一个反例，在R4上默认路由指向R1：

```
R4(config)#ip route 0.0.0.0 0.0.0.0 14.1.1.1
R4(config)#int ethernet1/1
R4(config-if)# ip verify unicast source reachable-via rx allow-default——加上default关键字，即如果路由表中存在默认路由，而且源符合该默认路由的出接口，则进行转发
```

为了方便验证，可以在R1上开启debug ip icmp命令。

为了方便观察，Ethernet 1/1接口下的配置都会是先去掉然后再配置上去的，即验证之前都是如下情况：

```
R4#show ip interface ethernet 1/1
  IP verify source reachable-via RX, allow default
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
```

验证：

```
R3#ping  11.1.1.1 source loopback 0


Type escape sequence to abort.
Sending  5,  100-byte  ICMP  Echos  to  11.1.1.1,  timeout  is  2
seconds:
Packet sent with a source address of 33.1.1.1
.....
Success rate is 0 percent (0/5)
R4#show ip interface ethernet 1/1
IP verify source reachable-via RX, allow default——default代表可
以通过默认路由通过监测
   5 verification drops——5个报文被丢弃
   0 suppressed verification drops
   0 verification drop-rate
```

此时R1也没有任何相应。

分析：为什么会出现默认路由，但是报文依旧被丢弃的情况？因为源（33.1.1.1）虽然符合默认路由的条件，但是数据（源自33.1.1.1）的入接口（34.1.1.4）却不是默认路由的出接口（14.1.1.4）。

```
R4#    show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
  Known via "static", distance 1, metric 0, candidate default
```

```
path
  Routing Descriptor Blocks:
  * 14.1.1.1
           Route metric is 0, traffic share count is 1
```

下面我们进行正确的通过默认路由完成严格uRPF的检查：

```
R4(config)#no  ip route 0.0.0.0 0.0.0.0 14.1.1.1
R4(config)#ip route 0.0.0.0 0.0.0.0 34.1.1.3——数据源（33.1.1.1）的入接口符合路由去往33.1.1.1的出接口
```

验证：

```
R3#ping    11.1.1.1 source loopback 0

Type escape sequence to abort.
Sending  5,  100-byte  ICMP  Echos  to  11.1.1.1,  timeout  is  2 seconds:
Packet sent with a source address of 33.1.1.1
.....
Success rate is 0 percent (0/5)
R4#show ip interface ethernet 1/1
    IP verify source reachable-via RX, allow default
5 verification drops——依旧是之前的5个被丢弃的报文
   0 suppressed verification drops
   0 verification drop-rate
```

R1已经有debug消息：

```
R1#
*Mar     1 03:28:07.899: ICMP: echo reply sent, src 11.1.1.1,
dst 33.1.1.1
R1#
*Mar     1 03:28:09.891: ICMP: echo reply sent, src 11.1.1.1,
dst 33.1.1.1
R1#
*Mar     1 03:28:11.899: ICMP: echo reply sent, src 11.1.1.1,
dst 33.1.1.1
R1#
*Mar     1 03:28:13.935: ICMP: echo reply sent, src 11.1.1.1,
dst 33.1.1.1
R1#
*Mar     1 03:28:15.887: ICMP: echo reply sent, src 11.1.1.1,
dst 33.1.1.1
```

50.3.4　通过ACL旁路严格的uRPF

在某些特殊场景下，来自某些源的数据虽然没有路由，但是依旧需要转发该数据，此时需要用ACL来旁路这些数据：

```
R4(config)#no ip route 0.0.0.0 0.0.0.0 34.1.1.3——去掉之前的默认路
由
!
```

```
R4(config)#ip access-list extended 100
R4(config-ext-nacl)#permit ip host 33.1.1.1 host 11.1.1.1——匹配允许的源即33.1.1.1的数据
!
R4(config)# interface Ethernet1/1
R4(config-if)#no ip verify unicast source reachable-via rx allow-default——去掉之前的配置
R4(config-if)#ip verify unicast source reachable-via rx 100——调用ACL 100来旁路该ACL允许的流量
```

验证：

```
R3#ping    11.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 33.1.1.1
.....
Success rate is 0 percent (0/5)
R4#show ip interface ethernet 1/1
    IP verify source reachable-via RX, ACL 100——采用严格uRPF，但是旁路了ACL100的流量
   0 verification drops——没有报文被丢弃
   5 suppressed verification drops——5个报文被抑制，没有丢弃
   0 verification drop-rate
R4#show access-lists
```

```
Extended IP access list 100
10 permit ip host 33.1.1.1 host 11.1.1.1 (5 matches)  ——有报文匹配，当然也可以在该ACL后加log关键字，以产生系统日志
```

R1有报文到达：

```
R1#
*Mar     1 03:43:14.995: ICMP: echo reply sent, src 11.1.1.1, dst 33.1.1.1
R1#
*Mar     1 03:43:16.975: ICMP: echo reply sent, src 11.1.1.1, dst 33.1.1.1
R1#
*Mar     1 03:43:18.956: ICMP: echo reply sent, src 11.1.1.1, dst 33.1.1.1
R1#
*Mar     1 03:43:20.987: ICMP: echo reply sent, src 11.1.1.1, dst 33.1.1.1
R1#
*Mar     1 03:43:22.971: ICMP: echo reply sent, src 11.1.1.1, dst 33.1.1.1
```

50.3.5　配置松散的uRPF

松散的uRPF，即只要路由表中存在源的路由即可，无须严格检查路由的出接口是否吻合源流量的入接口。

在R4的E1/1口配置松散的uRPF：

```
R4(config-if)#ip verify unicast source reachable-via any ?
<1-199>          IP access list (standard or extended)
<1300-2699>      IP expanded access list (standard or extended)
  allow-default     Allow default route to match when checking
source address——通过默认路由完成监测
      allow-self-ping      Allow router to ping itself (opens
vulnerability in
                   verification)——允许设备本身发起的ping监测
R4(config-if)#ip verify unicast source reachable-via any——any代
表松散的uRPF
!
R4(config)#ip route 33.1.1.1 255.255.255.255 14.1.1.1——为了完成松
散的uRPF监测，需要在路由表中存在源（33.1.1.1）的路由，当然该路由的下一跳
完全错误（正确的下一跳为34.1.1.4）
```

验证：

```
R3#ping    11.1.1.1 source loopback 0 repeat 2

Type escape sequence to abort.
Sending  2,  100-byte  ICMP  Echos  to  11.1.1.1,  timeout  is  2
seconds:
Packet sent with a source address of 33.1.1.1
..
Success rate is 0 percent (0/2)
```

```
R4#show ip interface serial 2/0
    IP verify source reachable-via ANY——开启了松散的uRPF监测
   0 verification drops——没有报文被丢弃
   2 suppressed verification drops——2个报文通过了验证，没有被丢弃
   0 verification drop-rate
```

R1已经有报文到达：

```
R1#
*Mar     1 04:11:35.242: ICMP: echo reply sent, src 11.1.1.1,
dst 33.1.1.1
R1#
*Mar     1 04:11:37.234: ICMP: echo reply sent, src 11.1.1.1,
dst 33.1.1.1
```

50.3.6　通过ACL旁路松散的uRPF

去掉E1/1口的uRPF配置，去掉去往源（33.1.1.1）的静态路由：

```
R4(config-if)#no ip verify unicast source reachable-via any 100
R4(config)#no ip route 33.1.1.1 255.255.255.255 14.1.1.1
```

在流量的入接口（E1/1）配置：

```
R4(config)#ip access-list extended 100
R4(config-ext-nacl)#10 permit ip host 33.1.1.1 host 11.1.1.1
log——增加log关键字以出现系统日志
!
R4(config-if)#interface ethernet1/1
R4(config-if)#ip verify unicast source reachable-via any 100——
配置松散的uRPF，同时调用ACL 100
```

验证：

```
R3#ping    11.1.1.1 source loopback 0 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 11.1.1.1, timeout is 2
seconds:
Packet sent with a source address of 33.1.1.1
.
Success rate is 0 percent (0/1)
R4#  show access-lists
Extended IP access list 100
    10 permit ip host 33.1.1.1 host 11.1.1.1 log (1 match)  ——
ACL有匹配
R4#
*Dec 24 21:14:21.098: %SEC-6-IPACCESSLOGDP: list 100 permitted
icmp 33.1.1.1 -> 11.1.1.1 (0/0), 1
 packet——log显示，路由了33.1.1.1到11.1.1.1的流量
R4#show ip interface ethernet1/1
```

```
------------------------------------------------------------------
-省略----------------------------------------------------------
  IP verify source reachable-via ANY, ACL 100
   0 verification drops
1 suppressed verification drop —— 一个报文被抑制，没有丢弃
   0 verification drop-rate


R1#
*Mar  1 04:52:30.062: ICMP: echo reply sent, src 11.1.1.1, dst
33.1.1.1
```

其他一些特性的调整：

```
R4(config-if)#ip verify unicast notification threshold 1——接口下每秒钟丢弃一个报文时，发送一个丢弃速率通告，默认值为1000
R4(config-if)#snmp trap ip verify drop-rate——当路由器的uRPF丢包速度超过配置阈值时，发送SNMP的通知报文
R4(config)#ip verify drop-rate notify hold-down 31——全局配置模式下，配置丢弃通告间隔的最小时间为31s，默认值为300s
R4(config)#ip verify drop-rate compute interval 31——全局配置模式下，丢弃率计算的间隔为30s，默认时间为30s
R4(config)#ip verify drop-rate compute window 299——全局配置模式下，丢弃率计算的一个周期为299s，默认时间为300s，此时间需要大于等于interval时间
```

实验完成。

附录A　重点网络词汇

A

ABR，OSPF边界路由器。

ACK，TCP的确认报文。另外，在协议中用于确认的可靠报文，用于确认的更新、查询、回复报文。

Address Family，典型的用于或者BGP协议，比如IPv4单播地址族、IPv6单播地址族用来更新对应的路由更新。

ARP，地址解析协议。RFC826定义，在局域网中一台主机去发现特定的IP地址对应的硬件地址的协议。

Adjacent，邻接，很多时候用于描述为邻居。在OSPF中，到达2-Way状态称之为邻居，之后的状态会到达邻接，用于指定路由器和普通设备之间。

Aggregate Route，路由汇总。Aggregate更多时候用于BGP，即把路由的掩码长度缩短，在可路由的前提下，减少路由条目数。

All OSPF DR Routers，组播组224.0.0.6，用于侦听DR和BDR路由器。

All OSPF Routers，组播组224.0.0.5，用于侦听OSPF路由器。

Alternate Role，一个802.1W快速生成树的端口角色，用于备份根端口。如果根端口出现问题，替换端口向根端口转换。

Area，用于OSPF或者ISIS，一个连续的同一区域成员的设备。通常分为骨干区域和普通区域。

ABR，区域边界路由器，用于连接OSPF骨干区域和普通区域的设备。

ASBR（Autonomous System Boundary Router），从其他OSPF进程或者其他协议引入路由的设备，或者可以产生5类LSA的设备。

B

Backbone，用于连接不同网络区域的区域。在OSPF中，区域0提供骨干区域的功能；在ISIS协议，由连续的Level-2路由器组成。

Backup Role，一个802.1W RSTP端口角色，用于备份相同交换机的指定端口。如果指定端口出现问题，该设备向指定端口切换。

Blocking State，一个802.1D标准生成树的端口状态，该状态不发送、不接收、不学习数据帧，但是会接收BPDU。

BPDUGuard，一个思科特有的特性，在特定模式下收到BPDU就把该接口置于err-disable状态。

Broadcast Subnet，主机位全部为1的地址，如果向该地址发送报文，子网内的主机将得到响应。

C

CEF（Cisco Express Forwarding），思科设备默认的转发方式，通过创建一个预先定义的邻接表和转发信息库快速的优化一个三层转发路径或者一个多层交换机。很多种机制都依赖CEF，比如MPLS等。

CIDR，无类域间路由。RFC1517-1520定义，用于在一个巨大的网络域中通过移除有类地址划分而采取的措施。带来的结果是汇聚或者汇总，在现代网络除了RIPv1之外，其他协议都支持CIDR。

Community Port，私有VLAN技术中，被分配给辅助VLAN，Community VLAN的接口。

Community VLAN，私有VLAN技术中的一类辅助VLAN，同一Community VLAN可以通信，也可以和混杂端口通信。

Control Plane，控制层面。负载创建、更新、交换设备上的控制操作，比如IP路由协议，该控制层面就用于构建IP路由表；另外一个例子是LDP，它用于构建标签转发表。

CST，通用生成树。应用多个VLAN实例到同一个生成树实例的简单生成树。在MST协议中，CST负责互连不同的MST区域，以及提供和非MST实例的互连。

D

Data Planee，数据层面。网络中真正的用于转发数据流的功能层面。一个典型的例子，IP路由表是一个转发表，可以使得路由器在接口真正地去转发数据。

Default route，默认路由，当报文不能匹配到更明细的路由时可以通过查找默认路由来转发数据。

Designed port，指定端口，在生成树中，每个交换网络中负责转发最优的BPDU接口，可以用于转发用户数据。

Dijkstra，另外一个命令称为SPF算法，用于OSPF或者ISIS协议计算数据库得到路由表，由发明者edsger W. Dijkstra命名而来。

Disacarding state，丢弃状态，802.1W的RSTP中不用于转发的状态，等同于802.1D的Disabled、Blocking以及Listen状态。

DR，Designated Router，指定路由器。在OSPF协议中，是在邻居的2-way状态下选举出来的，用于在子网中泛洪，典型的去创建、泛洪2类LSA；在组播的PIM协议中，负责发送加入、剪枝IGMP信令，或者在第一跳组播路由器位置负责向DR注册。

DRother，在以太子网中，OSPF协议除了DR和BDR之外的角色。

DTP，Dynamic Trunking Protocol，在ISL或者802.1Q中，思科私有的动态协商Trunk协议的方式。

DUAL，Diffusing Update Algorithm，扩散更新算法。eigrp协议中用于计算状态机，得到通告距离等参数的算法。

E

eigrp stube router，eigrp协议中运行了stub命令的设备，一种抑制eigrp查询报文的工具，涵盖的特性和参数较多，比如直连、汇

总等。

External LSA，外部LSA，OSPF协议中引入外部路由时，由ASBR产生的5类LSA，重要信息为标识到达外部路由的度量值、转发地址、路由tag等。

F

Fast switch，快速交换，一种优化的通过三层设备的转发方式，通过一次查找数据流缓存，使得后续报文通过缓存继续转发的方式。

FD，Feasible Distance，可行距离。eigrp协议中，去往特定目的地的拥有最低距离的度量值。

Feasibility condition，可行性条件。eigrp协议中的防环机制，条件为去往目标的次优设备的通告距离小于可行距离。

Feasible successor，可行后继。eigrp协议中，防止环路的充足条件。去往某个特定目标，如果邻居报告的距离小于去往该目标的可行距离，即满足可行性条件。

FIB，Forwarding Information Base，在CEF转发机制中，一个优化的路由信息库，即运行了CEF的路由转发表。

Forward Delay timer，转发时延，生成树协议中侦听状态到学习状态，以及学习状态到转发状态的时延。

Forwarding state，生成树802.1D中发送和接收数据帧的接口。

G

Gateway of last resort，IOS中IP路由表明该路由为默认路由的情况。

GLBP，Gateway Load Balancing Protocol，网关负载均衡协议。思科特有的提供多个虚拟MAC地址的网关备份协议。

Goodbye，eigrp协议中用于一个路由器通知邻居该设备优雅的关闭。

Going active，eigrp协议中标识某条路由进入到了不稳定状态。

H

Hello，一种周期性发送的消息，在多种协议中用于发现、协商、建立和维持邻居的报文，典型的用于eigrp、OSPF、ISIS、PIM、LDP等协议。

Hello interval，发送Hello报文的间隔，不同协议有不同的时间值。

Hello timer，生成树协议中特定的由根设备发送BPDU的间隔，默认为2s。

Hold timer，eigrp协议中决定邻居是否还存在的时间值，通常为Hello间隔的3倍。

HSRP，Hot Standby Router Protocol，思科私有的用于备份网关设备的路由协议，会分发虚拟的IP地址和虚拟MAC地址。

I

I/G bit，Individual/Group bit，以太网中一个MAC地址最小有效位，表明了一个单播地址或者组播地址（地址为二进制的1）。

Inferior BPDU，多个BPDU对比时较差的BPDU，即桥ID较差的BPDU，或者由于优先级较大或者由于MAC地址较大引起。

Instance ID，OSPFv3协议中，相对于OSPFv2额外增加的用于控制邻居关系的字段，默认为实例0，相同实例才能建立OSPFv3邻居。如果有虚链路必须为实例0。

Isolated port，孤立端口，私有VLAN技术中被划分到Isolated VLAN的端口。

Isolated VLAN，私有VLAN技术中的辅助VLAN，它仅仅可以和混杂端口通信。

K

K-value，eigrp协议中，用于计算综合度量值的参数，不同的*K*值将导致不同的度量值（*K* 1控制带宽，*K* 2控制带宽和负载，*K* 3控制时延，*K* 4和*K* 5控制可靠性，*K* 6控制扩展的度量值），K值在邻居两侧不同会引发邻居无法建立。

L

LACP，Link Aggregation Control Protocol，链路聚合控制协议，定义在IEEE802.1AX，用于控制以太通道的链路聚合，通过一定参数去选择接口进入以太通道。

Layer 2 protocol tunneling，用于QinQ协议，允许二层隧道传输，诸如CDP、STP、VTP等通过基于VLAN的二层网络。

Learning state，802.1D协议中的一个状态，不发送、也不接受数据帧，但是可以学习进入的帧中的MAC地址。

Link-state routing protocol，链路状态协议，用SPF算法在LSDB中计算而得到路由的协议，典型为OSPF协议和ISIS协议。

Listening state，侦听状态，802.1D中的一个状态，该状态不发送、不接收帧，也不学习源MAC地址，但是会发送和接收BPDU以决定其在生成树中的角色。

Loop Guard，用于STP中由于单向链路问题引发的环路保护。

LSP（Label Switched Path），在一个MPLS环境中，一个报文通过标签转发通过的路径，该通道由MPLS网络的入口到达出口。

LSA（Link State Advertisement），OSPF数据库中构建和描述拓扑信息。

M

Maxage，一个OSPF的时间值，用于决定在LSA、在LSDB中能够维系的最长时间。

MaxAge timer，生成树中的20s时间，用于存储在端口中的BPDU的超时时间。

MLS，Multilayer Switching，交换机上重要的进程，用于决定除了二层逻辑转发和其他OSI层面的决策。

MST，Multiple Spanning Trees，定位为802.1S，一种折中的、公有的多实例生成树协议，算法采用RSTP的快速算法。

Multicast address，组播地址，用于描述一组接收者的D类地址，范围是224.0.0.0/4，在IPv6范围是FF00::/8。

N

NAT，Network Address Translation，网络地址转换。在RFC1631中定义，通常在IPv4地址族中把私有IP地址转换为公有的IP地址，这样可以减少IPv4公有地址的使用。当然NAT还有更多功能。

Native VLAN，本征VLAN，在802.1Q中不添加802.1Q标记的VLAN，同时当收到不打标记的帧时，将把数据帧转发到本征VLAN。

Network type，OSPF的一个参数，用于决定是否需要选择DR，是否需要静态指定邻居，以及默认的发送Hello的间隔时间。

NSSA，Not-So-Stubby Area，OSPF的一个特殊区域，它不同于末节区域，它可以从本区域的ASBR注入外部路由，但不接受来自主干区域的外部路由。

NTP，Network time protocol，网络时间协议。

O

Offset list，偏移列表，用于RIP和eigrp协议中匹配某些路由，在出或者入方向增加度量值的工具。

Overloading，NAT中端口地址转换的关键字。

P

PAgP，Port Aggregation Protocol，思科私有的用于动态协商以太通道的协议。

Passive，eigrp协议中表明数据库中的状态变成稳定状态的路由。

Poison reverse，毒性反转，距离适量协议中的防环机制，全称为带毒性反转的水平分割。如果某路由通过接口已经不可达，该网络将被显示的通告为不可达。

Policy routing，策略路由，思科IOS路由器的特性，应用一个route-map以决定转发一个报文，典型的基于报文信息转发而非路由表。

Portfast，生成树协议中使得端口状态马上从disable状态到转发状态，不用经历其他的时间。一种快速转发的工具，在标准的802.1D中是一个补丁，在快速生成树和多实例生成树中称为边缘端口。

PPPoE，Point-to-Point Protocol over Ethernet，在以太网之上封装PPP协议，使其增加额外的认证和计费功能。

Prefix suppress，在OSPF中阻止路由前缀在一个传输网络通告。

Priority，在OSPF中，该字段包含在Hello报文中，在选举期内，优先级较大的设备将选为DR，取值范围是0～255，0代表没有能力被选择为DR或者BDR。

Private VLAN，一个思科交换机特性，允许所有端口的主机地址在同一网段，但是可以做到同一网段内的使用辅助VLAN加一隔离，起到节省地址的作用。

Process Switching，一个三层的转发策略，使得三层报文的转发都经过计算，是一种老式的不优化的转发方式。

Promiscuous Port，混杂端口，私有VLAN技术中主VLAN所属的端口，可以和私有VLAN中所有的端口通信。

PVST+，思科特有的生成树，早于IEEE 802.1S和802.1W，每个VLAN一个生成树，而且支持DOT1Q的Trunk封装。

Q

Query，eigrp的查询报文，用于向邻居请求特定的路由，该报文可能会占用较多的资源，查询报文需要收到ACK确认。

R

RD，Route Distinguisher，一个64位的BGP扩展NLRI字段，用于MPLS VPN环境，使得BGP在PE设备之间批量更新时解决可能存在的路由重叠问题。

Remote-VLAN，RSPAN技术中的目标VLAN。

Reply，eigrp的一个报文，用于相应的查询报文，它需要一个确认报文。

RIB，Routing Information Base，一个非优化的路由信息表，服务于运行CEF之后的FIB表。

RID，Router ID，一个32位的用于标识运行特定协议的值，可以用于OSPF、eigrp、BGP以及LDP等。

Root Port，生成树的根端口，在非根交换机上用于接收来自根设备的最优的BPDU。

Route-map，是思科IOS上一个重要的配置工具，逻辑上匹配一组内容，然后设置相应的参数，可以在多处应用，比如重分布、接口等。

Route Reditribution，路由重分布，从其他的路由协议的路由表引入本协议的数据库中，是学习新的路由。

Route Tag，路由标记，路由条目中用于关联一个通用的数值的方式，通常仅仅在外部路由中引用，典型的应用到路由过滤中。

Routed Interface，可路由端口。基于思科IOS的交换机接口，去掉二层特性，配置为一个独享的可以配置IP地址，以及运行路由协议的接口。

RSTP，快速生成树，定义在IEEE 802.1W中，对STP协议的增强，可以快速地进行收敛。

RTO，Retransmission Timeout重传超时时间，eigrp协议中，一个可靠报文开始传输的时间，任何的邻居如果没有影响RTO，那么可靠传输协议就会引发重传，通常RTO基于SRTT的计算，是6倍的SRTT。

RTP，Reliable Transport Protocol，可靠传输协议，用可靠组播和单播传递的协议，用于eigrp。

S

SPAN，Switched Port Analyzer，交换端口分析，一种从交换机端口、VLAN收集流量，然后复制该流量到同一交换机其他端口的技术。

Split horizon，水平分割，一种用于距离适量协议的防环机制，通常从一个接口收到的路由不会再从该接口更新给邻居。

SRTT，Smoothed Round-Trip Time，平滑轮训时间，在eigrp协议中，和邻居之间发送轮询的修改度量的参数，计算公式为

$$srtt = (srtt \times .8) + (rtt \times .2)$$

STP，Spanning Tree Protocol，生成树协议，定义在802.1D中，最基本的生成树诞生于1998年，2004年进行了修正。

Stub Area，末节区域，OSPF协议中不可以引入外部路由的区域，同时该区域的ABR引入默认路由到本区域。

STUB Router，eigrp协议中末节路由器不通告通过eigrp学习到的路由，用于在一定程度上限制查询，其他路由器不会发送查询报文

到末节路由器。

Stuck in active，eigrp中的一条路由出于不稳定状态的时间大于路由器的Active时间的一种状态。

Superior BPDU，更优化的BPDU，选举根桥时，多个BPDU中较优的报文，该报文相比其他报文包含更小的优先级或者MAC地址。

Switched Interface，交换接口，基于思科IOS的交换机被以二层接口对待的接口，相对的为可路由端口工作在三层。

T

TLV，Type-Length-Value，类型长度和值，在单个数据报文中用于存储和传输多种类型的特定格式，通常用于ISIS协议的封装格式。

Totally NSSA Area，完全NSSA区域，在该区域3类和5类LSA被阻止，取而代之的是该区域的ABR注入特殊的默认路由以解决路由问题。

Transit Network，传输网络，两个或者更多个OSPF路由器成为邻居，此时报文可以从一个路由设备传输到另外一个设备。

TTL（Time to Live），IPv4包头中的一个字段，当报文经过一个三层设备时减1。

U

UDLD，UniDirectional Link Detection，单向链路检测。思科私有协议用于去发现由于单向链路引发的问题，通常用于以太网和光线网络的物理层面。

Update，在eigrp中用于更新路由前缀的报文，需要一个ACK确认。

V

Variance，在eigrp中的一个设置的整数，为两个FD的比值取整得到。

Virtual IP Address，虚拟IP，用于VRRP或者HSRP协议中充当网关的地址。

Virtual Link，虚链路，OSPF协议中，把分割的骨干区域或者没有连接到骨干的区域通过虚链路连接起来，是一种临时的措施，同时可以起到优化和备份路由的效果。

VLAN，虚拟的局域网，用于二层交换机，是一个广播子网，一个逻辑的广播域。

VLSM，Variable-Length Subnet Masking，可变长子网掩码，子网划入一个网络，使得网络的主机包含多种不同长度掩码的地址。

VRRP，Virtual Router Redundancy Protocol，在RFC3768中定义，一种公有的网关用于备份协议，会选择一个Master负责相应ARP请求和转发报文，其他设备作为备份。

反侵权盗版声明