Cisco Catalyst WS-C3550 - настройка IP Unnumbered

Опубликовано muff в Чт, 2012-07-26 02:22



Для начала попробуем разобраться, что же такое **IP Unnumbered**, если кто не в курсе. Это разработка **Cisco** для интерфейсов точка-точка (например, **Serial**). При маршрутизации с участием таких интерфейсов нету необходимости "знать" адрес следующего хопа, так как это не широковещательная среда и пакет всегда достигнет своего получателя. Маршрутизатору достаточно знать, за каким интерфейсом "находится" необходимый префикс. Соответственно нету необходимости выделять подсети /30 на интерфейсы, вполне достаточно указать, что обработка пакетов для адресата будет осуществляться с адресом, присвоенному на другой интерфейс, например на **loopback**.

При использовании этой технологии имеем следущие преимущества:

- Не требуется дробить большие сети публичных адресов на мелкие, теряя при этом адреса.
- Возможность ограничения связи между пользователями в сети, исключая варианты с ACL и Port Protected варианты.
- При использовании vlan-per-user и Proxy ARP не требуется Dynamic Arp Inspection и Antispoof ACL.
- Ко всему трафику можно применить единую политику фильтрации в центре сети.

Даный функционал доступен в коммутаторах **Cisco Catalyst 4500/6500**, а также в последних версиях **IOS** для **Catalyst 3550**, **3560**, **3750**, **ME3400**.

Итак, имея в наличии **Cisco Catalyst WS-C3550**, настроим подключение 2 абонентов в разных VLAN с защитой от подделки IP-адресов и ограничением взаимодействия между абонентами.

Отталкиваться будем от того факта, что базовая настройка уже выполнена, маршрутизация настроена.

Итак, для абонентов выделена подсеть **10.3.156.160/27**:

```
# ipcalc 10.3.156.160/27


Address:   10.3.156.160         00001010.00000011.10011100.101 00000Netmask:   255.2
55.255.224 = 27 11111111.11111111.11111111.111 00000Wildcard:  0.0.0.31
00000000.00000000.00000000.000 11111=>Network:   10.3.156.160/27      00001010.00000
011.10011100.101 00000HostMin:   10.3.156.161         00001010.00000011.10011100.101
 00001HostMax:   10.3.156.190         00001010.00000011.10011100.101 11110Broadcast:
 10.3.156.191         00001010.00000011.10011100.101 11111Hosts/Net: 30
       Class A, Private Internet
```

Тоесть, в своем распоряжении имеем 30 IP, один из которых и "повесим" на **loopback** для маршрутизации. Конфигурирование **loopback**-интерфейса:

```
WS-C3550(config)# interface loopback 2
WS-C3550(config-if)# ip address 10.3.156.161 255.255.255.224
WS-C3550(config-if)# no ip redirects
```

Теперь создадим два **VLAN**-интерфейса, включим поддержку **IP Unnumbered**:

```
WS-C3550(config)# vlan 100
WS-C3550(config-vlan)# name vl100
WS-C3550(config-vlan)# exit
WS-C3550(config)# vlan 101
WS-C3550(config-vlan)# name vl101
WS-C3550(config-vlan)# exit
WS-C3550(config)# interface vlan 100
WS-C3550(config-if)# ip unnumbered Loopback 2
Warning: dynamic routing protocols will not work on non-point-to-point interfaces with IP
unnumbered configured.
WS-C3550(config-if)# no ip proxy-arp
WS-C3550(config-if)# interface vlan 101
WS-C3550(config-if)# description Client2
WS-C3550(config-if)# ip unnumbered Loopback 2
Warning: dynamic routing protocols will not work on non-point-to-point interfaces with IP
unnumbered configured.
WS-C3550(config-if)# no ip proxy-arp
```

Теперь подадим созданные **VLAN** на два разных **FastEthernet** интерфейса:

```
WS-C3550(config)# interface FastEthernet 0/1
WS-C3550(config-if)# switchport mode access
WS-C3550(config-if)# switchport access vlan 100
WS-C3550(config-if)# exit
WS-C3550(config)# interface FastEthernet 0/2
WS-C3550(config-if)# switchport mode access
WS-C3550(config-if)# switchport access vlan 101
```

Остался последний штрих - необходимо смаршрутизировать клиентские IP-адреса, поскольку динамическая маршрутизация на **FastEthernet** интерфейсах не работает:

```
WS-C3550(config)# ip route 10.3.156.162 255.255.255.255 vlan 100
WS-C3550(config)# ip route 10.3.156.163 255.255.255.255 vlan 101
```

Собственно говоря, на этом настройка **IP Unnumbered** закончена. Чтобы было проще разобраться, вывожу вывод **running-config** на тестовом коммутаторе, с которым точно все работает:

```
WS-C3550# show running-config


Building configuration...

Current configuration : 4713 bytes!version 12.2no service padservice timestamps debu
g datetime msecservice timestamps log datetime msecservice password-encryption!hostn
ame WS-C3550!enable secret 5 $1$SIcl$j00000000000Ea1u26EQE/enable password 7 046E000
000000000000B0B!!!no aaa new-modelauthentication mac-move permitip subnet-zeroip rou
ting!!vtp mode transparent!!crypto pki trustpoint TP-self-signed-3465675776 enrollme
nt selfsigned subject-name cn=IOS-Self-Signed-Certificate-3465675776 revocation-chec
k none rsakeypair TP-self-signed-3465675776!!crypto pki certificate chain TP-self-si
gned-3465675776 certificate self-signed 01  30820241 308201AA A0030201 02020101 300D
0609 2A864886 F70D0101 04050030  31312F30 2D060355 04031326 494F532D 53656C66 2D5369
67 6E65642D 43657274  69666963 6174652D 33343635 36373537 3736301E 170D3933 30333031
 30303031  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```

4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 34363536 37353737 36
30819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100CD2C E845A7D6 8DB2
CD67 00DD83FC BC7DDCA4 AD7858EF DF285DD1 359E6E1D B156002E 34F1083E 2F4C483F F49B00
BA 6E913086 A02031D1 59FCFA74 3B4BF300 AAAA6072 384646CC 27C0B249 76FA34AF 53F87F84
 3F5767DD 82AEF18C E7733D59 E341DACA 840D51AC 39064567 8DFB6775 9FA6E9D0 A2F20BA3 8
1B3E8E1 0D07F262 00000000 00000000 00000000 00000000 00000000 00000000 00000000 000
00000 551D1104 0D300B82 0957532D 43333535 302E301F 0603551D 23041830 16801441 03BE
D924 6B4C66D4 1C24E0F2 8B9E3DC7 BE131630 1D060355 1D0E0416 04144103 BED9246B 4C66D4
1C 24E0F28B 9E3DC7BE 1316300D 06092A86 4886F70D 01010405 00038181 006DF316 E484900A
 05852D2C A47D9513 A7858B13 97E87BB9 8119BDEB 3D15C3B3 769970B1 CDEC2418 D9CAD229 7
7885779 E6357F2E 7369161D FFC98F5E 00000000 00000000 00000000 00000000 00000000 000
00000 00000000 00000000 997B94C9 3F7AEF50 79E1D98B A6EA2091 0806D242 C47A4E8D AB00E
85C 23935C08 9E59E523 41 quitspanning-tree mode pvstspanning-tree etherchannel gua
rd misconfigspanning-tree extend system-id!vlan internal allocation policy ascending
!vlan 3 name Routers_area!vlan 100 name client1!vlan 101 name client2!!!!!!interface
 Loopback2 ip address 10.3.156.161 255.255.255.224 no ip redirects!interface FastEth
ernet0/1 switchport access vlan 100 switchport mode access!interface FastEthernet0/2
 switchport access vlan 101 switchport mode access!interface FastEthernet0/3 switchp
ort mode access!interface FastEthernet0/4 switchport mode access!interface FastEther
net0/5 switchport mode access!interface FastEthernet0/6 switchport mode access!inter
face FastEthernet0/7 switchport mode access!interface FastEthernet0/8 switchport mod
e access!interface FastEthernet0/9 switchport mode access!interface FastEthernet0/10
 switchport mode access!interface FastEthernet0/11 switchport mode access!interface
FastEthernet0/12 switchport mode access!interface FastEthernet0/13 switchport mode a
ccess!interface FastEthernet0/14 switchport mode access!interface FastEthernet0/15 s
witchport mode access!interface FastEthernet0/16 switchport mode access!interface Fa
stEthernet0/17 switchport mode access!interface FastEthernet0/18 switchport mode acc
ess!interface FastEthernet0/19 switchport mode access!interface FastEthernet0/20 swi
tchport mode access!interface FastEthernet0/21 switchport mode access!interface Fast
Ethernet0/22 switchport mode access!interface FastEthernet0/23 switchport mode acces
s!interface FastEthernet0/24 switchport mode access!interface GigabitEthernet0/1 swi
tchport mode trunk!interface GigabitEthernet0/2 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3 switchport mode trunk!interface Vlan1 no ip address
!interface Vlan3 ip address 10.227.206.44 255.255.255.240!interface Vlan100 ip unnum
bered Loopback2 no ip proxy-arp!interface Vlan101 ip unnumbered Loopback2 no ip prox
y-arp!ip default-gateway 10.227.206.33ip classlessip route 0.0.0.0 0.0.0.0 10.227.20
6.33ip route 10.3.156.162 255.255.255.255 Vlan100ip route 10.3.156.163 255.255.255.2
55 Vlan101no ip http serverno ip http secure-server!!ip sla enable reaction-alerts!c
ontrol-plane!!line con 0 password 7 0814400000000000171902 logging synchronous login
line vty 0 4 password 7 0814400000000000171902 loginline vty 5 15 password 7 0814400
000000000171902 login!end

В результате этих настроек пользователи "не видят" друг друга, а имеют доступ только к шлюзу и к сетям, которые находятся за ним. Для включения обмена трафиком между абонентами необходимо на **vlan**-интерфейсах включить функцию **proxy-arp**, которая по умолчанию включена.

Источник (получено *2026-10-30 18:08*):
http://muff.kiev.ua/content/cisco-catalyst-ws-c3550-nastroika-ip-unnumbered