ACLSs em equipamentos de comutação - VACL e PACL

Prof.Celso Rabelo M Pinto

Centro Universitário da Cidade

14/12/2013

ACLs em Ambiente de Switches

- ACLS permitem a filtragem de tráfego ingressante ou egresso, baseados em condições específicas
- Normalmente pensamos em ACLs para a filtragem em nível L3
- Podemos pensar também em ACLs atuando em equipamentos L2
- Para isso podemos implementar o conceito de VACL e PACL, sendo a primeira aplicada a uma vlan e a segunda a uma porta

Conceitos Gerais

- VACL prove controle de acesso a pacotesque atravessam uma vlan (modo bridge) ou roteados por uma VLAN (modo roteado)
- Podemos configurar a VACL para controle de tráfego baseado em IP ou MAC
- Se uma VACL for configurada para tipo de pacote, outros pacotes não listados serão negados por padrão

Configuração

- O funcionamento da VACL é semelhante ao funcionamento da técnica ZPF
- É dividida em fases:
- Criação da ACL
- Criação de um mapa de acesso
- Associação do mapa de acesso à vlan

Exemplo

Assume IP-named ACL **net_10** and **any_host** are defined as follows:

```
Router# show ip access-lists net_10
Extended IP access list net_10
    permit ip 10.0.0.0 0.255.255.255 any

Router# show ip access-lists any_host
Standard IP access list any_host
    permit any
```

Exemplo

```
Router(config)# vlan access-map thor 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action forward
Router(config-access-map)# exit
Router(config)# vlan access-map ganymede 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action drop log
Router(config-access-map)# exit
Router(config)# vlan access-map ganymede 20
Router(config-access-map)# match ip address any_host
Router(config-access-map)# action forward
Router(config-access-map)# exit
```

Exemplo

```
Router(config)# vlan filter thor vlan-list 12-16
Router(config)# vlan filter ganymede vlan-list 7-9
```

MAC PBF

- Nesta abordagem é verificado o mac-address para permitir ou não o acesso
- É aplicavel em uma estrutura L3, Router ou Switch

Lista de hosts

```
Router(config)# mac host host_red3 0001.0002.0003
Router(config)# mac host host_blue5 0001.0002.0005
```

ACL

```
Router(config)# mac access-list extended macl_red
Router(config-ext-macl)# permit host host_red host host_blue
Router(config-ext-macl)# exit
Router(config)# mac access-list extended macl_blue
Router(config-ext-macl)# permit host host_blue host host_red
Router(config-ext-macl)# exit
```

Mapa

```
Router(config)# vlan access-map red_to_blue
Router(config-access-map)# match mac address macl_red
Router(config-access-map)# action forward vlan 200 local
Router(config-access-map)# exit
Router(config)# vlan filter red_to_blue vlan-list 100
Router(config)# vlan access-map blue_to_red
Router(config-access-map)# match mac address macl_blue
Router(config-access-map)# action forward vlan 100
Router(config-access-map)# exit
Router(config)# vlan filter blue_to_red vlan-list 200
```

Análise

```
Router(config)# interface vlan 100
Router(config-if)# mac packet-classify
Router(config-if)# exit
Router(config)# interface vlan 200
Router(config-if)# mac packet-classify
Router(config-if)# exit
```

Visão Geral

- A funcionalidade permite o controle de acesso em nível 2 do modelo OSI, em portas em modo acesso ou tronco
- PACL são aplicadas somente em modo de ingresso
- Possui 2 modos: prefer (sobrescrevem outras acls) merge (misturam)

ACL

This example shows how to configure the Extended Named IP ACL simple-ip-acl to permit all TCP traffic and implicitly deny all other IP traffic:

```
Switch(config)# ip access-list extended simple-ip-acl
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# end
```

This example shows how to configure the Extended Named MAC ACL simple-mac-acl to permit source host 000.000.011 to any destination host:

```
Switch(config)# mac access-list extended simple-mac-acl
Switch(config-ext-macl)# permit host 000.000.011 any
Switch(config-ext-macl)# end
```

Modo de Acesso

This example shows how to configure an interface to use prefer port mode:

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# access-group mode prefer port
```

This example shows how to configure an interface to use merge mode:

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# access-group mode merge
```

Aplicação

This example applies the extended named IP ACL simple-ip-acl to interface GigabitEthernet 6/1 ingress traffic:

```
Switch# configure t
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# ip access-group simple-ip-acl in
```

This example applies the extended named MAC ACL simple-mac-acl to interface GigabitEthernet 6/1 ingress traffic:

```
Switch# configure t
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# mac access-group simple-mac-acl in
```

Bibliografia

- http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all$_b$*ook.html*h
*//www.cisco.com/en/US/docs/switches/lan/catalyst*6500/*ios*/12.2*SX*/