INSTITUTO POLITÉCNICO DE TOMAR
ESCOLA SUPERIOR DE TECNOLOGIA DE TOMAR

ENGENHARIA INFORMÁTICA

PROJECTO DE REDES

2012 / 2013

Lab 2: Configuração de ACLs

Objectivos:

- □ **Montagem da componente física de uma rede.**
- □ **Configuração de equipamento activo.**
- □ **Definição e configuração de ACLs.**
- □ **Debugging e trobleshooting.**

GRUPO 6

11046 Vasco Marques	11598 Bruno Calças

Topologia da rede:

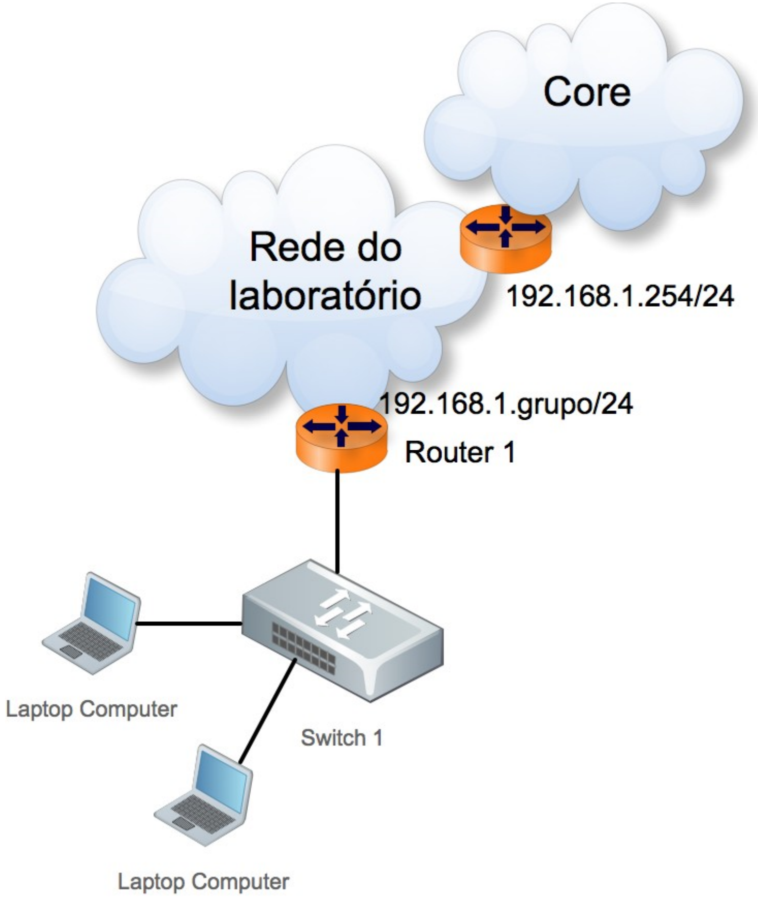


Tabela das VLANs:

VLAN ID	Nome	Portas	Modo	Default Gateway dos membros dessa VLAN
99	**Gestão**	Fa 0/24	tagged	10.99.grupo.254
		Mgmt	NA	
10	**Funcionários**	Fa 0/24	tagged	10.10.grupo.254
		Fa 0/0-12	untagged	
20	**Alunos**	Fa 0/24	tagged	10.20.grupo.254
		Fa 0/13-16	untagged	
30	**guest**	Fa 0/17-20	untagged	NA

Passo 2: Apague as configurações dos routeres.

ROUTER:

```
Router>enable
Router#configure terminal
Router(config)#erase startup-config
Router(config)#reload
```

SWITCH:

```
Switch>enable
Switch#erase startup-config
Switch#reload
```

Tarefa 2: Configurações Básicas

Configure o Router de acordo com as orientações seguintes:

1. Atribua um nome a cada router de acordo com a topologia descrita (hostname)

2. Desabilite o DNS lookup.

3. Configure uma password para aceder ao modo Exec Privileged Mode. **(Password=class)**

4. Configure a message-of-the-day banner.

5. Configure uma password para ligações do tipo console. **(Password=class)**

6. Configure uma password para ligações do tipo VTY. **(Password=class)**

ROUTER:

```
Router>enable
Router#configure terminal
Router#hostname Router1
Router1(config)#no ip domain lookup
Router1(config)#enable secret cisco
Router1(config)#line console 0
Router1(config-line)#password class
Router1(config-line)#login
Router1(config-line)#exit
Router1(config)#line vty 0 4
Router1(config-line)#password class
Router1(config-line)#login
Router1(config-line)#exit
Router1(config)#banner motd “Bem Vindo ao Router1”
Router1(config)#exit
```

```
Router1#copy running startup-config
```

SWITCH:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname Switch1
Switch1(config)#enable secret class
Switch1(config)#line console 0
Switch1(config-line)#password class
Switch1(config-line)#login
Switch1(config-line)#exit
Switch1(config)#line vty 0 4
Switch1(config-line)#password class
Switch1(config-line)#login
Switch1(config-line)#exit
Switch1(config-line)#exit
Switch1#copy running startup-config
```

Tarefa 3: Configure as interfaces dos Routers.

Passo 1: Configure as interfaces do router com base na informação da tabela

ROUTER:

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/1
Router1(config-if)#ip address 192.168.6.1 255.255.255.0
Router1(config)#no shutdown
Router1(config)#exit
Router1(config)#interface FastEthernet0/0.10
Router1(config-subif)#encapsulation dot6Q 10
Router1(config-subif)#ip address 10.10.6.254
255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface FastEthernet0/0.20
Router1(config-subif)#encapsulation dot6Q 20
Router1(config-subif)#ip address 10.20.6.254
255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface FastEthernet0/0.30
Router1(config-subif)#encapsulation dot6Q 30
Router1(config-subif)#ip address 10.30.6.254
255.255.255.0
```

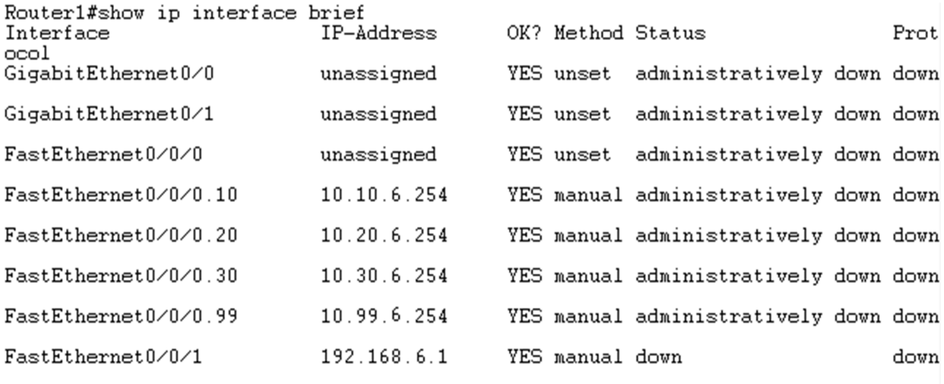
```
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface FastEthernet0/0.99
Router1(config-subif)#encapsulation dot6Q 99
Router1(config-subif)#ip address 10.99.6.254
255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
```

Passo 2: Verifique os endereços atribuídos às interfaces.

Use o comando **show ip interface brief** para verificar as configurações que efectuou no passo anterior.

Guarde as configurações activas na NVRAM.

```
Router#show ip interface brief
```



```
Router1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Prot
ocol
GigabitEthernet0/0         unassigned      YES unset  administratively down down

GigabitEthernet0/1         unassigned      YES unset  administratively down down

FastEthernet0/0/0          unassigned      YES unset  administratively down down

FastEthernet0/0/0.10       10.10.6.254     YES manual administratively down down

FastEthernet0/0/0.20       10.20.6.254     YES manual administratively down down

FastEthernet0/0/0.30       10.30.6.254     YES manual administratively down down

FastEthernet0/0/0.99       10.99.6.254     YES manual administratively down down

FastEthernet0/0/1          192.168.6.1     YES manual down                  down
```

```
Router1#copy running startup-config
```

Passo 3: Configure o servidor DHCP para as redes Funcionário, Aluno e Guest.

ROUTER:

```
Router>enable
Router#configure terminal
Router1(config)#ip dhcp pool vlan99
Router1(dhcp-config)#network 10.10.6.0 255.255.255.0
Router1(dhcp-config)#default-router 10.10.6.254
Router1(dhcp-config)#lease 0 8
Router1(dhcp-config)#exit
Router1(config)#ip dhcp pool vlan20
Router1(dhcp-config)#network 10.20.6.0 255.255.255.0
Router1(dhcp-config)#default-router 10.20.6.254
Router1(dhcp-config)#lease 0 8
Router1(dhcp-config)#exit
Router1(config)#ip dhcp pool vlan30
Router1(dhcp-config)#network 10.30.6.0 255.255.255.0
Router1(dhcp-config)#lease 0 8
Router1(dhcp-config)#exit
```

SWITCH:

```
Switch>configure terminal
Switch1(config)#interface range FastEthernet0/0-12
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
Switch1(config)#interface range FastEthernet0/13-16
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 20
Switch1(config)#interface range FastEthernet0/17-20
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 30
Switch1(config)#inferface FastEthernet 0/24
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#switchport trunk allowed vlan
10,20,99
Switch1(config-if)#end
Switch1(config)#interface vlan 99
Switch1(config-if)#ip address 10.99.6.253 255.255.255.0
Switch1(config-if)#no shutdown
```

Passo 4: Verifique a conectividade entre os dispositivos de cada uma das VLANs e o respectivo default gateway.

Para as diferentes VLANs verificamos que existia conectividade para:

VLAN 10: 10.10.6.254

VLAN 20: 10.20.6.254

Tarefa 4: Configure o OSPF no router

Passo 1: Use o comando **router ospf** para configurar o OSPF em R1.

Nota: A interface exterior pertence à área 0, as interfaces de dentro pertencem à área do Grupo (nº do grupo).

```
Router1#configure terminal
Router1(config)#router ospf 1
Router1(config-router)#network 10.10.6.0 0.0.0.255
area1
Router1(config-router)#network 10.20.6.0 0.0.0.255
area1
Router1(config-router)#network 10.30.6.0 0.0.0.255
area1
Router1(config-router)#network 10.99.6.0 0.0.0.255
area1
Router1(config-router)#network 192.168.6.0 0.0.0.255
area0
```

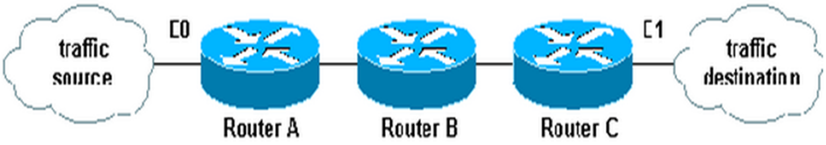
Tarefa 5: Configure ACLs de acordo com os requisitos seguintes.

No sistema Cisco IOS existem três tipos de ACLs:
ACLs Standard – é a lista mais básica consequentemente com menos funcionalidades. Filtrando apenas através do

endereço IP de origem, pois devem ser colocados o mais próximo possível do destino do tráfego.

ACLs Extended – permite filtrar o tráfego através do endereço IP de origem e destino, bem como através de portas e protocolos. Este tipo de ACLs deve ser aplicado o mais próximo possível da origem.

ACLs Named – possui as mesmas características que a ACL extended mas para além disso permite atribuir um nome mais intuitivo para a ACL facilitando a vida do administrador da rede.



O tráfego é considerado ***inbound*** quando vem da rede e entra para o router através de uma das suas interfaces, e é considerado ***outbound*** quando o tráfego sai do router para a rede.

Tarefa 1: Montar a rede.

Passo 1: Ligue os cabos aos equipamentos activos de acordo com a figura anterior.

- Não existe conectividade entre os dispositivos das redes Funcionários, Alunos e Guest os dispositivos da rede de gestão.

```
Router1(config)#access-list 110 permit ip 10.10.6.0 0.0.0.255 10.10.6.0 0.0.0.255
Router1(config)#access-list 110 permit ip 10.10.6.0 0.0.0.255 10.20.6.0 0.0.0.255
Router1(config)#access-list 110 permit ip 10.10.6.0 0.0.0.255 10.30.6.0 0.0.0.255
Router1(config)#access-list 110 permit ip 10.20.6.0 0.0.0.255 10.10.6.0 0.0.0.255
Router1(config)#access-list 110 permit ip 10.30.6.0 0.0.0.255 10.10.6.0 0.0.0.255
```

Prosseguiu-se as mesmas configurações para as **VLAN 20** e para a **VLAN 30**, de modo a permitir todo o tráfego entre as VLANS. Para permitir todas as ligações TCP com a origem apartir de uma rede qualquer, para as redes:

10.10.6.0
10.20.6.0
10.30.6.0

Utilizando a regra **established** para o tráfego relacionado com a ligação já estabelecido, isto

```
para que não se crie uma nova ACL para que o
tráfego volte a passar pelo router correctamente.

Router1(config)#access-list 110 permit tcp any
10.10.6.0 0.0.0.255
Router1(config)#access-list 120 permit tcp any
10.20.6.0 0.0.0.255
Router1(config)#access-list 130 permit tcp any
10.30.6.0 0.0.0.255
**Ping 10.99.6.1
```

- Os dispositivos da rede de gestão têm conectividade com os dispositivos de todas as redes.

```
Router1(config)#access-list 110 permit icmp
10.10.6.0 0.0.0.255 any echo-reply
Router1(config)#access-list 120 permit icmp
10.20.6.0 0.0.0.255 any echo-reply
Router1(config)#access-list 130 permit icmp
10.30.6.0 0.0.0.255 any echo-reply
Router1(config)#access-list 100 permit udp any eq
bootpc
Router1(config)#access-list 100 permit udp any eq
bootps
```

- Apenas os dispositivos da rede de gestão podem gerir o router e o switch (snmp, ssh e webview).

```
De acordo com o pedido, apenas foi necessário
permitir ligações tcp e udp de dispositivos da
rede 10.99.6.0 com destino ao router e ao switch.

Router1(config)#access-list 101 permit udp
10.99.6.0 0.0.0.255 host 10.99.6.254 eq 161
Router1(config)#access-list 101 permit tcp
10.99.6.0 0.0.0.255 host 10.99.1.254 eq 22
Router1(config)#access-list 101 permit tcp
10.99.6.0 0.0.0.255 host 10.99.6.254 eq 23

Para permitir as ligações para os protocolos foi
necessário identificar as suas portas snmp(161),
ssh(22) e telnet(23).

Prosseguimos as regras definidas abaixo
apresentadas em cada uma das interfaces, de modo a
que seja permitido/negado todo tráfego na entrada
para o router no modo inbound.

Router1(config)#acces-list 100 deny ip any any

Router1(config)#interface FastEthernet 0/0.10
Router1(config-subif)#ip access-group 110 in
Router1(config-subif)#ip access-group 100 in
```

```
Router1(config-subif)#exit
Router1(config)#interface FastEthernet 0/0.20
Router1(config-subif)#ip access-group 120 in
Router1(config-subif)#ip access-group 100 in
Router1(config-subif)#exit
Router1(config)#interface FastEthernet 0/0.30
Router1(config-subif)#ip access-group 130 in
Router1(config-subif)#ip access-group 100 in
Router1(config-subif)#exit

Na VLAN99, foi permitido todo o tráfego de entrada
e associado a porta FastEthernet0/0.99.
Router1(config)#acces-list 100 deny ip any any

Router1(config)#interface FastEthernet 0/0.99
Router1(config-subif)#ip access-group 199 in
Router1(config-subif)#ip access-group 101 in
Router1(config-subif)#exit
```

- Só é permitido tráfego multicast vindo do exterior se pertencer aos grupos 224.239.0.1-10

```
Router1(config)#access-list 105 permit ip
224.239.0.2 0.0.255.255 any
Router1(config)#access-list 105 permit ip
224.239.0.3 0.0.255.255 any
Router1(config)#access-list 105 permit ip
224.239.0.4 0.0.255.255 any
Router1(config)#access-list 105 permit ip
224.239.0.5 0.0.255.255 any
Router1(config)#access-list 105 permit ip
224.239.0.6 0.0.255.255 any
Router1(config)#access-list 105 permit ip
224.239.0.7 0.0.255.255 any
Router1(config)#access-list 105 permit ip
224.232.0.8 0.0.255.255 any
Router1(config)#access-list 105 permit ip
224.232.0.9 0.0.255.255 any
Router1(config)#access-list 105 permit ip
224.232.0.10 0.0.255.255 any

Router1(config)#access-list 106 permit ip
224.239.0.2 0.0.255.255 any
Router1(config)#access-list 106 permit ip
224.239.0.3 0.0.255.255 any
Router1(config)#access-list 106 permit ip
224.239.0.4 0.0.255.255 any
Router1(config)#access-list 106 permit ip
224.239.0.5 0.0.255.255 any
Router1(config)#access-list 106 permit ip
224.239.0.6 0.0.255.255 any
Router1(config)#access-list 106 permit ip
224.239.0.7 0.0.255.255 any
Router1(config)#access-list 106 permit ip
```

```
224.232.0.8 0.0.255.255 any
Router1(config)#access-list 106 permit ip
224.232.0.9 0.0.255.255 any
Router1(config)#access-list 106 permit ip
224.232.0.10 0.0.255.255 any

Router1(config)#interface FastEthernet 0/1
Router1(config-if)#ip access-group 105 in
Router1(config-if)#ip access-group 106 out
Router1(config-if)#exit
```

- Apenas é suportado o protocolo de encaminhamento OSPF.

```
Router1(config)#access-list 105 permit ospf any
any
```

Anexos

Router:

```
Building configuration...

Current configuration : 2066 bytes
!
! Last configuration change at 20:38:17 UTC Mon Apr 8 2013
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
enable secret cisco
!
no aaa new-model
memory-size iomem 10
!
no ipv6 cef
ip source-route
ip cef
!
!
!
ip dhcp pool vlan99
  network 10.99.6.0 255.255.255.0
  default-router 10.99.6.254
  lease 0 8
!
ip dhcp pool vlan10
  network 10.10.6.0 255.255.255.0
  default-router 10.10.6.254
```

```
   lease 0 8
!
ip dhcp pool vlan20
   network 10.20.6.0 255.255.255.0
   default-router 10.20.6.254
   lease 0 8
!
ip dhcp pool vlan30
   network 10.30.6.0 255.255.255.0
   default-router 10.30.6.254
   lease 0 8
!
!
no ip domain lookup
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1921/K9 sn FCZ1453C28X
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.10.6.254 255.255.255.0
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.20.6.254 255.255.255.0
```

```
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.30.6.254 255.255.255.0
!
interface FastEthernet0/0.99
 encapsulation dot1Q 99
 ip address 10.99.6.254 255.255.255.0
!
interface FastEthernet0/1
 ip address 192.168.1.6 255.255.255.0
 shutdown
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 10.10.6.0 0.0.0.255 area 1
 network 10.20.6.0 0.0.0.255 area 1
 network 10.30.6.0 0.0.0.255 area 1
 network 10.99.6.0 0.0.0.255 area 1
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.6.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
banner motd ^CRouter1^C
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
scheduler allocate 20000 1000
end
```

Switch:

```
Building configuration...

Current configuration : 2421 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname switch1
!
boot-start-marker
boot-end-marker
!
enable secret cisco
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
!
!
!
!
!
!
!
!
!
```

```
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/9
```

```
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 30
 switchport mode access
!
```

```
interface FastEthernet0/19
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 switchport access vlan 99
 switchport trunk allowed vlan 10,20,99
 switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
!
ip http server
ip http secure-server
!
control-plane
!
!
line con 0
line vty 5 15
!
end
```