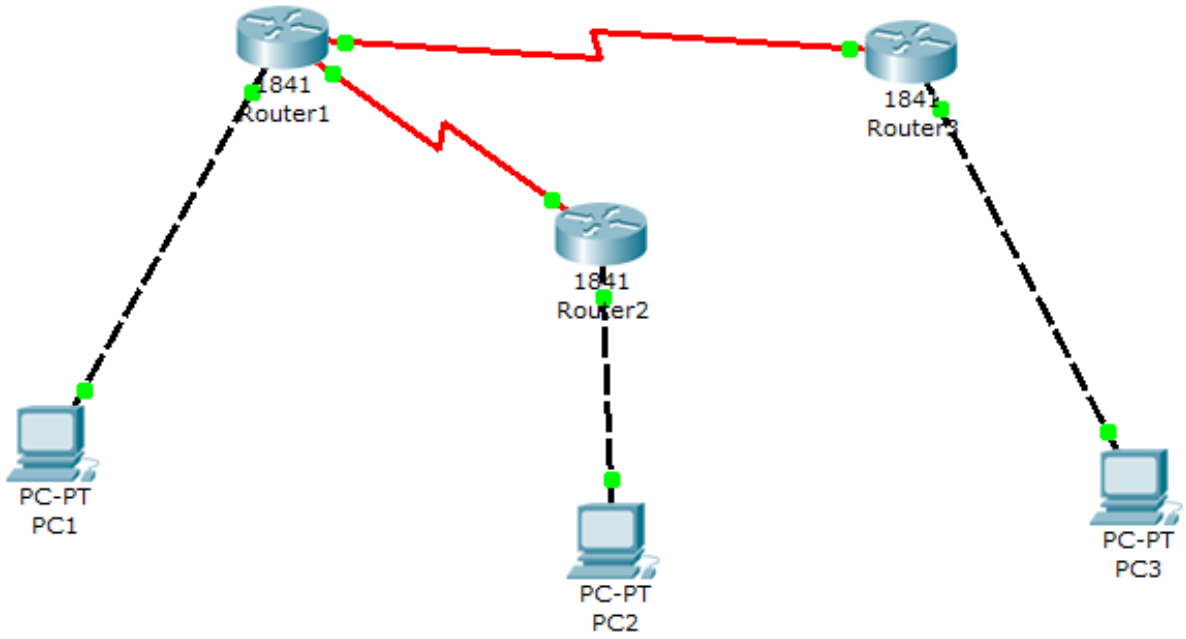
Rotas Estáticas

Nesta aula vamos aprender a ligar redes locais com routers, utilizando comandos do Cisco IOS. As topologias ensaiadas serão conseguidas à custa da ligação back to back (directa) de dois ou mais routers. Este tipo de ligação pode ser efectuado de diferentes formas. Por exemplo, através de portas ethernet com um cabo cruzado ou, então, através de portas série com um cabo DCE/DTE. O exercício seguinte vai utilizar esta segunda forma de ligação.

Exercício

Configure a Internet apresentada no esquema seguinte:



Em que os endereços IP dos PCs e routers são:

PC 1	→	193.136.235.1
PC2	→	196.136.235.1
PC3	→	197.136.235.1
Router1	→	193.136.235.254, 194.136.235.1 e 195.136.235.1
Router2	→	194.136.235.2 e 196.136.235.254
Router3	→	195.136.235.2 e 197.136.235.254

- **Configuração no Router1**

```
Router1>enable
Router1#config terminal
Router1(config)#interface e0/0
Router1(config-if)#ip address 193.136.235.254 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#CTRL Z

Router1#config terminal
Router1(config)#interface serial0/0
Router1(config-if)#ip address 194.136.235.1 255.255.255.0
Router1(config-if)#clock rate 128000[1]
Router1(config-if)#no shutdown
Router1(config-if)#CTRL Z

Router1#config terminal
Router1(config)#interface serial0/1
Router1(config-if)#ip address 195.136.235.1 255.255.255.0
Router1(config-if)#clock rate 128000[3]
Router1(config-if)#no shutdown
Router1(config-if)#CTRL Z

Router1#config terminal
Router1(config)#ip route 196.136.235.0 255.255.255.0 194.136.235.2[2]
Router1(config)#ip route 197.136.235.0 255.255.255.0 195.136.235.2[4]
Router1(config)#CTRL Z
Router1#show ip route
```

- **Configuração no Router2**

```
Router2>enable
Router2#config terminal
Router2(config)#interface e0/0
Router2(config-if)#ip address 196.136.235.254 255.255.255.0
```

[1] O comando **clock** deve ser efectuado no router onde se encontra a ponta do cabo marcada como DCE.
[2] Para retirar esta linha da tabela de encaminhamento usar este mesmo comando, mas começado pela palavra **no** (no ip route…)

```
Router2(config-if)#no shutdown
Router2(config-if)#CTRL Z


Router2#config terminal
Router2(config)#interface serial0/0
Router2(config-if)#ip address 194.136.235.2 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#CTRL Z


Router2#config terminal
Router2(config)#ip route 0.0.0.0 0.0.0.0 194.136.235.1
Router2(config)#CTRL Z
Router2#show ip route
```

- **Configuração no Router3**

```
Router3>enable
Router3#config terminal
Router3(config)#interface e0/0
Router3(config-if)#ip address 197.136.235.254 255.255.255.0
Router3(config-if)#no shutdown
Router3(config-if)#CTRL Z


Router3#config terminal
Router3(config)#interface serial0/0
Router3(config-if)#ip address 195.136.235.2 255.255.255.0
Router3(config-if)#no shutdown
Router3(config-if)#CTRL Z


Router3#config terminal
Router3(config)#ip route 0.0.0.0 0.0.0.0 195.136.235.1
Router3(config)#CTRL Z
Router3#show ip route
```

Finalmente, teste as configurações anteriores com os comandos **ping** e **tracert** (nos PCs) ou **traceroute** (nos routers).

Encaminhamento IPv4

1. Arquitetura hierárquica*;*
2. Arquitetura distribuída;
3. Protocolos de encaminhamento;
4. Encaminhamento extremo a extremo.

Arquitetura hierárquica

- A Internet só considera dois tipos de entidades, *hosts* e *gateways;*

- Havia um sistema central de encaminhamento, denominado **Core**, implementado por **Core Gateways**;

- As CGs eram administradas de forma centralizada e trocavam informação de encaminhamento entre si através do Gateway to Gateway Protocol;

Arquitetura hierárquica

- Fora do Core existiam os Autonomous Systems, ligados ao Core através das **External Gateways***;*

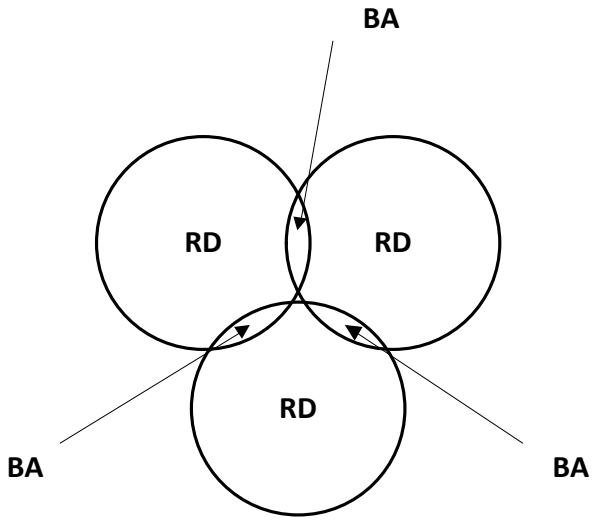
- Estas trocavam informação de encaminhamento entre si e com as Core Gateways através do Exterior Gateway Protocol;

- Com o crescimento da Internet, a carga de processamento e armazenamento, da informação de encaminhamento, nas gateways do Core era enorme, obrigando a abandonar esta arquitetura hierárquica.

Arquitetura distribuída

- Novo modelo de encaminhamento, mais escalável e adaptado às características da Internet*;*

- Contempla apenas Autonomous Systems, denominados Routing Domains, todos de igual importância relativa, ligados pelas border areas:



Arquitetura distribuída

- Os Routing Domains trocam informação de encaminhamento entre si através do Border Gateway Protocol ou do EGP*;*

- Este modelo não depende de um sistema central (Core) para a escolha dos “melhores” caminhos para a informação.

Protocolos de encaminhamento

- **Interior gateway protocols**

  São usados no interior dos sistemas autónomos;

- **Exterior gateway protocols**

  São usados na ligação dos sistemas autónomos uns aos outros.

Protocolos de encaminhamento

- Interiores: Routing Information Protocol, Open Shortest Path First, Enhanced Interior Gateway Routing Protocol;

- Exteriores: Enhanced Interior Gateway Routing Protocol, Border Gateway Protocol.

Protocolos de encaminhamento

- Distance vector: Routing Information Protocol;
- Path vector: Border Gateway Protocol;
- Link state: Open Shortest Path First;
- Híbrido: Enhanced Interior Gateway Routing Protocol.

Protocolos de encaminhamento

- Distance vector: shortest distance;
- Path vector: shortest distance, best path;
- Link state: several metrics, several paths;
- Híbrido: both distance vector and link state.

Cisco Discovery Protocol

- O CDP é um protocolo de nível 2, que corre nos seguintes equipamentos Cisco:

  - »Routers
  - »Bridges
  - »Access servers
  - »Switches

Cisco Discovery Protocol

- Um equipamento activo com o CDP ligado envia periodicamente actualizações relativas aos seus interfaces de rede para um endereço de multicast bem conhecido (01:00:0C:CC:CC:CC), de modo a dar-se a conhecer aos seus vizinhos na rede.

- Uma vez que se trata de um protocolo de nível 2, as tramas que envia não são encaminhadas de uma rede IP para outra.

Cisco Discovery Protocol

- A utilização do protocolo SNMP com a CDP MIB (CISCO-CDP-MIB) permite a gestão da rede através dos agentes e consola SNMP.

- Numa própria dedicamos particular atenção ao protocolo de gestão de redes TCP/IP denominado Simple Network Management Protocol (SNMP).

Cisco Discovery Protocol

- O CDP encontra-se ligado, por omissão, nos activos Cisco. Para **desligar** o CDP:

```
# conf t
# no cdp run
```

- Para voltar a **ligar** o CDP:

```
# conf t
# cdp run
```

Cisco Discovery Protocol

- Para verificar se o CDP está ligado ou não, usar o comando:

```
Router#show cdp neighbors
Capability Codes: R − Router, T − Trans Bridge, B − Source Route Bridge
S − Switch, H − Host, I − IGMP, r − Repeater
Device ID Local Intrfce Holdtme Capability Platform Port ID
Router#
Router#show cdp
Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled
Router#
```

Cisco Discovery Protocol

- Os comandos anteriores mostram que o CDP está ligado no activo de rede, mas não foram descobertos quaisquer activos nas vizinhanças da rede.

```
Router#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
R2-AGS           Ser 1              129           R        2500      Ser 0
R6-2500          Eth 0              144           R        4000      Eth 0
Router#
```

- No segundo caso, o CDP está ligado e foram descobertos dois routers na rede, denominados R2-AGS e R6-2500.

Cisco Discovery Protocol

- O comando **sh cdp neighbors detail** mostra informação adicional acerca dos activos vizinhos:

```
router#show cdp neighbors detail
-------------------------
Device ID: lab-7206
Entry address(es):
IP address: 172.19.169.83
Platform: cisco 7206VXR, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): FastEthernet0/0/0
Holdtime : 123 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 12.1(2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.
advertisement version: 2
Duplex: half
-------------------------
Device ID: lab-as5300-1
Entry address(es):
IP address: 172.19.169.87
Platform: cisco AS5300, Capabilities: Router
```

Cisco Discovery Protocol

- O comando **sh cdp entry** mostra informação adicional acerca dos activos vizinhos:

```
router#show cdp entry lab-7206
-------------------------
Device ID: lab-7206
Entry address(es):
IP address: 172.19.169.83
Platform: cisco 7206VXR, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): FastEthernet0/0/0
Holdtime : 123 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 12.1(2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.
advertisement version: 2
Duplex: half
```

Cisco Discovery Protocol

- O CDP pode ser desabilitado num dado interface com o comando **no cdp enable**:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface s1
Router(config-if)#no cdp enable
Router(config-if)#^Z
Router#4w5d: %SYS-5-CONFIG_I: Configured from console by console
```

- A informação sobre o interface desabilitado só deixa de ser apresentada pelo comando **show cdp neighbors** quando o temporizador **Holdtime** expira.

Cisco Discovery Protocol

- Não é possível habilitar/desabilitar o CDP num dado interface, a menos que o CDP esteja globalmente activo com o comando **cdp run**.

- Se existirem muitos activos de rede na vizinhança, a activação do CDP pode acarretar o consumo de toda a RAM disponível no activo de rede.

Cisco Discovery Protocol

O CDP é um protocolo proprietário da Cisco, que corre nos seus routers e switches. Nesta aula vamos aprender a configurar, ligar e desligar o CDP nos activos de rede.

1.Caracteristicas

O CDP é um protocolo de nível 2, que corre nos seguintes equipamentos Cisco:

- Routers
- Bridges
- Access servers
- Switches

Um equipamento activo com o CDP ligado envia periodicamente actualizações relativas aos seus interfaces de rede para um endereço de multicast bem conhecido (01:00:0C:CC:CC:CC), de modo a dar-se a conhecer aos seus vizinhos na rede. Uma vez que se trata de um protocolo de nivel 2, as tramas que envia não são encaminhadas de uma rede IP para outra. A utilização do protocolo SNMP com a CDP MIB (CISCO-CDP-MIB) permite a gestão da rede através dos agentes e consola SNMP.

2.Configuração

O CDP encontra-se ligado, por omissão, nos activos Cisco. Para desligar o CDP:

```
# conf t
# no cdp run
```

Para voltar a ligar o CDP:

```
# conf t
# cdp run
```

Para verificar se o CDP está ligado ou não, usar o comando:

```
# show cdp neighbors
```

Por exemplo, o output obtido poderá ser:

```
Router#show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater
Device ID Local Intrfce Holdtme Capability Platform Port ID
Router#
Router#show cdp
Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled
Router#
```

Os comandos anteriores mostram que o CDP está ligado no activo de rede, mas não foram descobertos quaisquer activos nas vizinhanças da rede. Agora, se o output for:

```
Router#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
R2-AGS           Ser 1              129          R        2500      Ser 0
R6-2500          Eth 0              144          R        4000      Eth 0
Router#
```

O CDP está ligado e foram descobertos dois routers na rede, denominados R2-AGS e R6-2500. De facto, o comando **sh cdp neighbors** apresenta a seguinte informação:

- Tipo de equipamento descoberto
- Nome do equipamento
- Número e tipo de interfaces de rede do equipamento
- Número de segundos em que o anúncio da porta é válido
- Tipo do activo
- Número do produto
- Identificação da porta

Os comandos **sh cdp neighbors detail** e **sh cdp entry** mostram informação adicional acerca dos activos vizinhos, incluindo protocolo de nível 2 e respectiva versão.

```
router#show cdp neighbors detail
-------------------------
Device ID: lab-7206
Entry address(es):
IP address: 172.19.169.83
Platform: cisco 7206VXR, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): FastEthernet0/0/0
Holdtime : 123 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 12.1(2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.
advertisement version: 2
Duplex: half
-------------------------
Device ID: lab-as5300-1
Entry address(es):
IP address: 172.19.169.87
Platform: cisco AS5300, Capabilities: Router
```

```
router#show cdp entry lab-7206
-------------------------
Device ID: lab-7206
Entry address(es):
IP address: 172.19.169.83
Platform: cisco 7206VXR, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): FastEthernet0/0/0
Holdtime : 123 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 12.1(2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.
advertisement version: 2
Duplex: half
```

3.Habilitar/desabilitar o CDP num interface

O comando **cdp run** habilita o CDP de forma global, ou seja, em todos os interfaces do activo que são suportados pelo protocolo (excepto interfaces de Frame Relay). O CDP pode ser desabilitado num dado interface com o comando **no cdp enable**. Vejamos como:

```
Router#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
R2-AGS           Ser 1              129          R        2500      Ser 0
R6-2500          Eth 0              144          R        4000      Eth 0
Router#
```

Para desabilitar o CDP no interface Serial 1:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface s1
Router(config-if)#no cdp enable
Router(config-if)#^Z
Router#4w5d: %SYS-5-CONFIG_I: Configured from console by console
```

A informação sobre o interface desabilitado só deixa de ser apresentada pelo comando **show cdp neighbors** quando o temporizador **Holdtime** expira.

Com o comando **show cdp interface** vemos se o CDP se encontra habilitado ou desabilitado interface a interface:

Router#sh cdp int fa0/0

4.Notas finais

Não é possível habilitar/desabilitar o CDP num dado interface, a menos que o CDP esteja globalmente activo com o comando **cdp run**.

Se existirem muitos activos de rede na vizinhança, a activação do CDP pode acarretar o consumo de toda a RAM disponível no activo de rede.

Hot Standby Routing Protocol

- Uma forma de conseguir SLAs muito próximos de 100% consiste em utilizar o HSRP, que oferece redundância de encaminhamento em redes IP.

- Através da partilha de endereços IP e MAC virtuais, dois ou mais routers podem comportar-se como um único router (virtual).

Hot Standby Routing Protocol

- **Virtual IP :** Este endereço IP da subrede local, é atribuido como default gateway a todos os hosts.

- **Virtual MAC address** : O endereço Virtual MAC address é gerado automaticamente pelo HSRP. Os primeiros 24 bits dizem respeito à CISCO (0000.0c). Os 16 bits seguintes são o HSRP ID. Os últimos 8 bits são o group number em hexadecimal. Por exemplo, se o group number for 10 então os últimos 8 bits serão 0a.

Hot Standby Routing Protocol

- Um router é eleito como activo, ou seja, é o único que encaminha os pacotes enviados pelos hosts para o router virtual. Outro router é eleito como passivo (standby).

- Se o activo falhar, o passivo toma o seu lugar na tarefa de encaminhamento de pacotes IP.

Hot Standby Routing Protocol

- Para minimizar o tráfego na rede, apenas os routers activo e passivo trocam mensagens HSRP periódicas entre si.

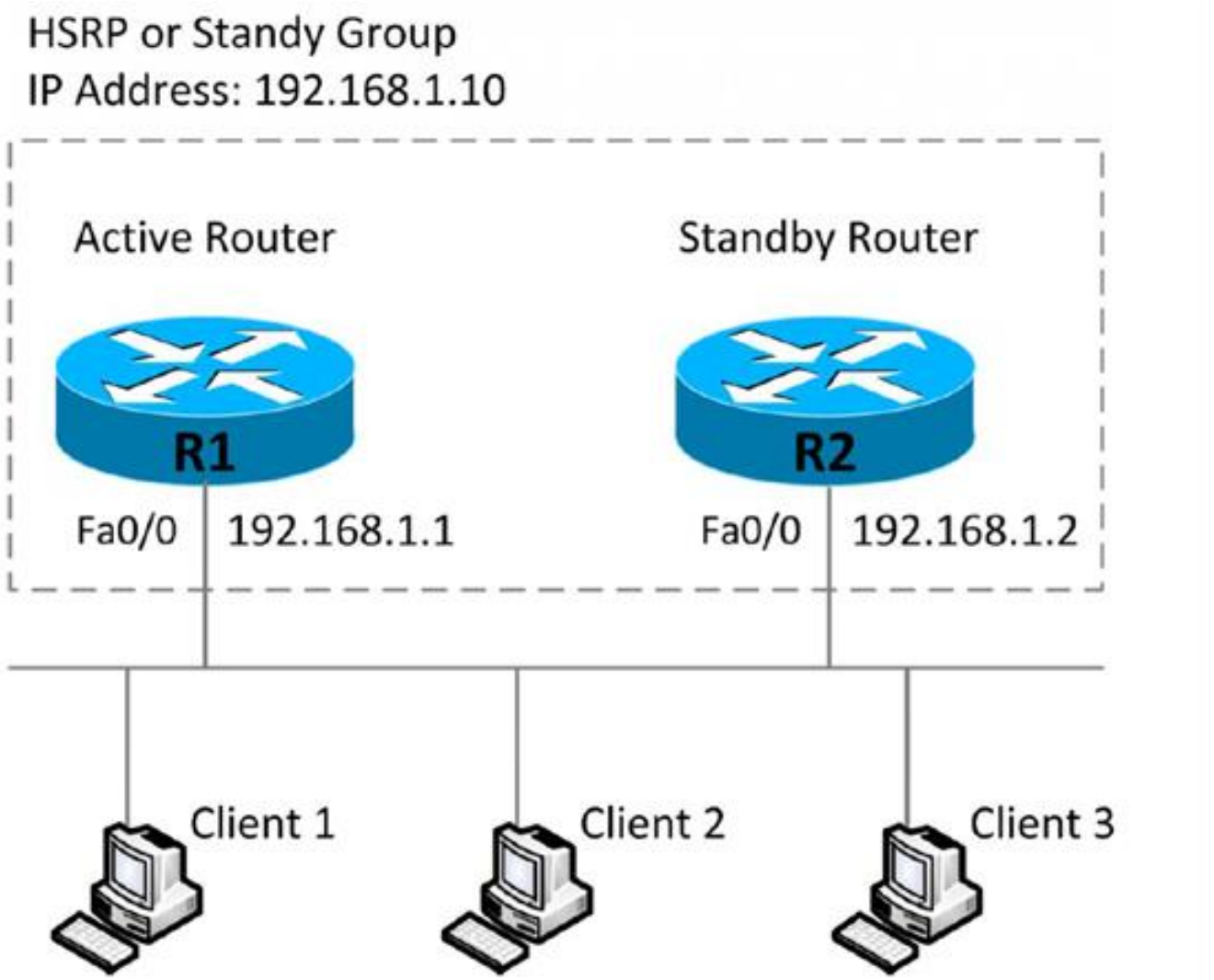
- Se o router passivo falhar ou passar a activo, é eleito um novo router passivo a partir do standby group.

Hot Standby Routing Protocol

- Numa LAN podem existir múltiplos standby groups, inclusivamente com routers a pertencer a mais de um grupo.

- Nesta situação, o router mantém variáveis de estado e temporizadores separados para cada grupo a que pertence.

Hot Standby Routing Protocol



Hot Standby Routing Protocol

- O router R1 encontra-se configurado com uma prioridade de 110, que é superior á prioridade por omissão (100). O router R2 encontra-se configurado com a prioridade 100.

- Os interfaces Ethernet dos routers R1 e R2 são configurados com os endereços 192.168.1.1 e 192.168.1.2.

Hot Standby Routing Protocol

- O endereço IP atribuído ao HSRP group 10 é 192.168.1.10, que está configurado nos dois membros do grupo, através do comando **standby ip**.

- O qualificador **preempt** permite ao router de maior prioridade tornar-se o router activo de forma imediata.

- A prioridade é determinada pelo valor configurado e pelo endereço IP. Em ambos os casos, a maior prioridade é atribuída ao valor mais elevado (O IP de R2 tem maior prioridade que o IP de R1).

Hot Standby Routing Protocol

R1:

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#standby version 2
R1(config-if)#standby 10 preempt
R1(config-if)#standby 10 priority 110
R1(config-if)#standby 10 ip 192.168.1.10
R1(config-if)#end
R1#
```

Hot Standby Routing Protocol

R2:

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface FastEthernet0/0
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#standby version 2
R2(config-if)#standby 10 preempt
R2(config-if)#standby 10 priority 100
R2(config-if)#standby 10 ip 192.168.1.10
R2(config-if)#end
R2#
```

Hot Standby Routing Protocol

```
R1#show standby
FastEthernet0/0 – Group 10 (version 2)
State is Active
5 state changes, last state change 00:08:23
Virtual IP address is 192.168.1.10
Active virtual MAC address is 0000.0c9f.f00a
Local virtual MAC address is 0000.0c9f.f00a (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.948 secs
Preemption enabled
Active router is local
Standby router is 192.168.1.2, priority 100 (expires in 9.412 sec)
Priority 110 (configured 110)
Group name is "hsrp-Fa0/0-10" (default)
```

Hot Standby Routing Protocol

```
R2#show standby
FastEthernet0/0 – Group 10 (version 2)
State is Standby
7 state changes, last state change 00:00:12
Virtual IP address is 192.168.1.10
Active virtual MAC address is 0000.0c9f.f00a
Local virtual MAC address is 0000.0c9f.f00a (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.756 secs
Preemption enabled
Active router is 192.168.1.1, priority 110 (expires in 8.760 sec)
MAC address is c200.09ac.0000
Standby router is local
Priority 100 (default 100)
Group name is "hsrp-Fa0/0-10" (default)
```

Hot Standby Routing Protocol

Uma forma de conseguir SLAs muito próximos de 100% consiste em utilizar o HSRP, que oferece redundância de encaminhamento em redes IP. Através da partilha de endereços IP e MAC, dois ou mais routers podem comportar-se como um único router virtual.

- **Virtual IP :** Este endereço IP da subrede local, é atribuido como default gateway a todos os hosts.

- **Virtual MAC address** : O endereço Virtual MAC address é gerado automaticamente pelo HSRP. Os primeiros 24 bits dizem respeito à CISCO (0000.0c). Os 16 bits seguintes são o HSRP ID. Os últimos 8 bits são o group number em hexadecimal. Por exemplo, se o group number for 10 então os últimos 8 bits serão 0a.

Independentemente do número de membros do standby group, só um router é eleito como activo, ou seja, é o único que encaminha os pacotes enviados pelos hosts para o router virtual. Outro router é eleito como passivo (standby).

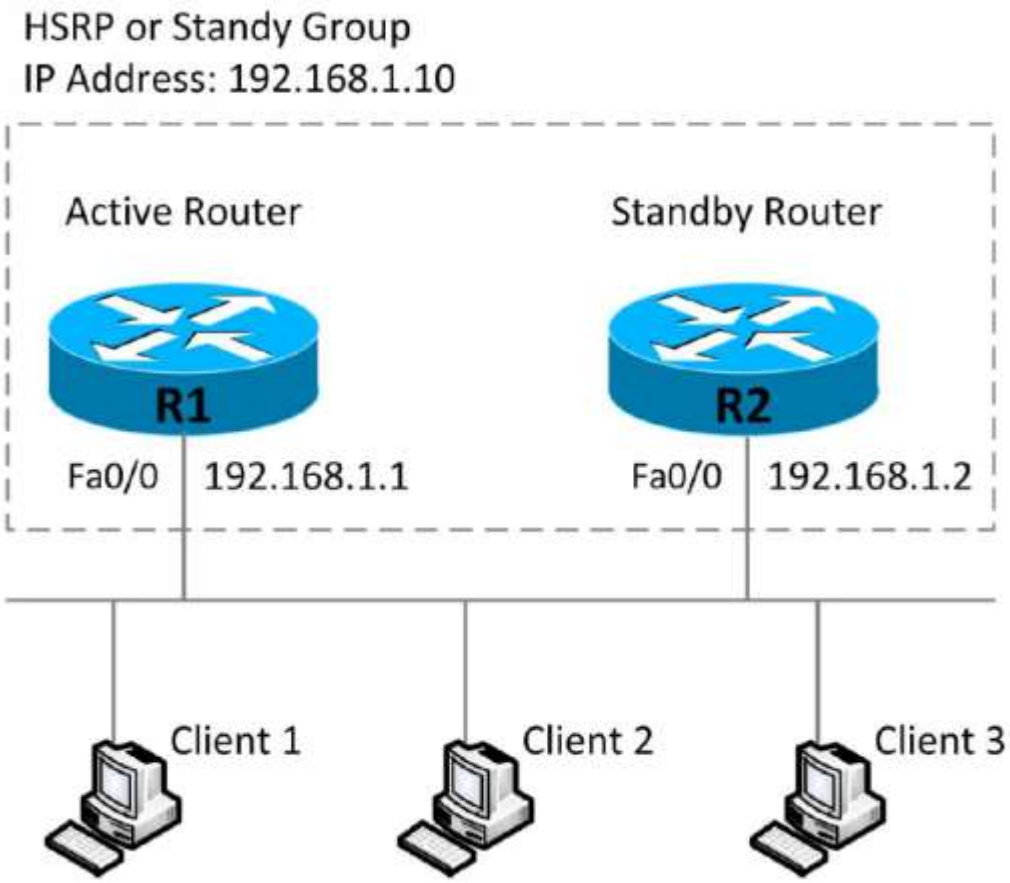
Se o activo falhar, o passivo toma o seu lugar na tarefa de encaminhamento de pacotes IP. Para minimizar o tráfego na rede, apenas os routers activo e passivo trocam mensagens HSRP periódicas entre si.

Se o router passivo falhar ou passar a activo, é eleito um novo router passivo a partir do standby group.

Numa LAN podem existir múltiplos standby groups, inclusivamente com routers a pertencer a mais de um grupo. Nesta situação, o router mantém variáveis de estado e temporizadores separados para cada grupo a que pertence.

1.Configuração

A figura da página seguinte esquematiza a topologia básica HSRP, com dois routers formando um standby group.



O router R1 encontra-se configurado com uma prioridade de 110, que é superior á prioridade por omissão (100). O router R2 encontra-se configurado com a prioridade 100. Os interfaces Ethernet dos routers R1 e R2 estão configurados com os endereços 192.168.1.1 e 192.168.1.2 respectivamente. O endereço IP atribuído ao HSRP group 10 é 192.168.1.10, que está configurado nos dois membros do grupo, através do comando **standby ip**.

R1:

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#standby version 2
R1(config-if)#standby 10 preempt
R1(config-if)#standby 10 priority 110
R1(config-if)#standby 10 ip 192.168.1.10
R1(config-if)#end
R1#
```

R2:

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface FastEthernet0/0
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#standby version 2
R2(config-if)#standby 10 preempt
R2(config-if)#standby 10 priority 100
R2(config-if)#standby 10 ip 192.168.1.10
R2(config-if)#end
R2#
```

O qualificador **preempt** permite ao router de maior prioridade tornar-se o router activo de forma imediata. A prioridade é determinada pelo valor configurado e pelo endereço IP. Em ambos os casos, a maior prioridade é atribuída ao valor mais elevado. O IP de R2 tem maior prioridade que o IP de R1.

Para verificar a configuração efectuada usa-se o comando **show standby**. R1 é o router activo.

```
R1#show standby
FastEthernet0/0 – Group 10 (version 2)
State is Active
5 state changes, last state change 00:08:23
Virtual IP address is 192.168.1.10
Active virtual MAC address is 0000.0c9f.f00a
Local virtual MAC address is 0000.0c9f.f00a (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.948 secs
Preemption enabled
Active router is local
Standby router is 192.168.1.2, priority 100 (expires in 9.412 sec)
Priority 110 (configured 110)
Group name is “hsrp-Fa0/0-10″ (default)
```

O resultado do comando show standby em R2 indica que se trata do standby router.

```
R2#show standby
FastEthernet0/0 – Group 10 (version 2)
State is Standby
7 state changes, last state change 00:00:12
Virtual IP address is 192.168.1.10
Active virtual MAC address is 0000.0c9f.f00a
Local virtual MAC address is 0000.0c9f.f00a (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.756 secs
Preemption enabled
Active router is 192.168.1.1, priority 110 (expires in 8.760 sec)
MAC address is c200.09ac.0000
Standby router is local
Priority 100 (default 100)
Group name is “hsrp-Fa0/0-10″ (default)
```

Virtual Local Area Networks

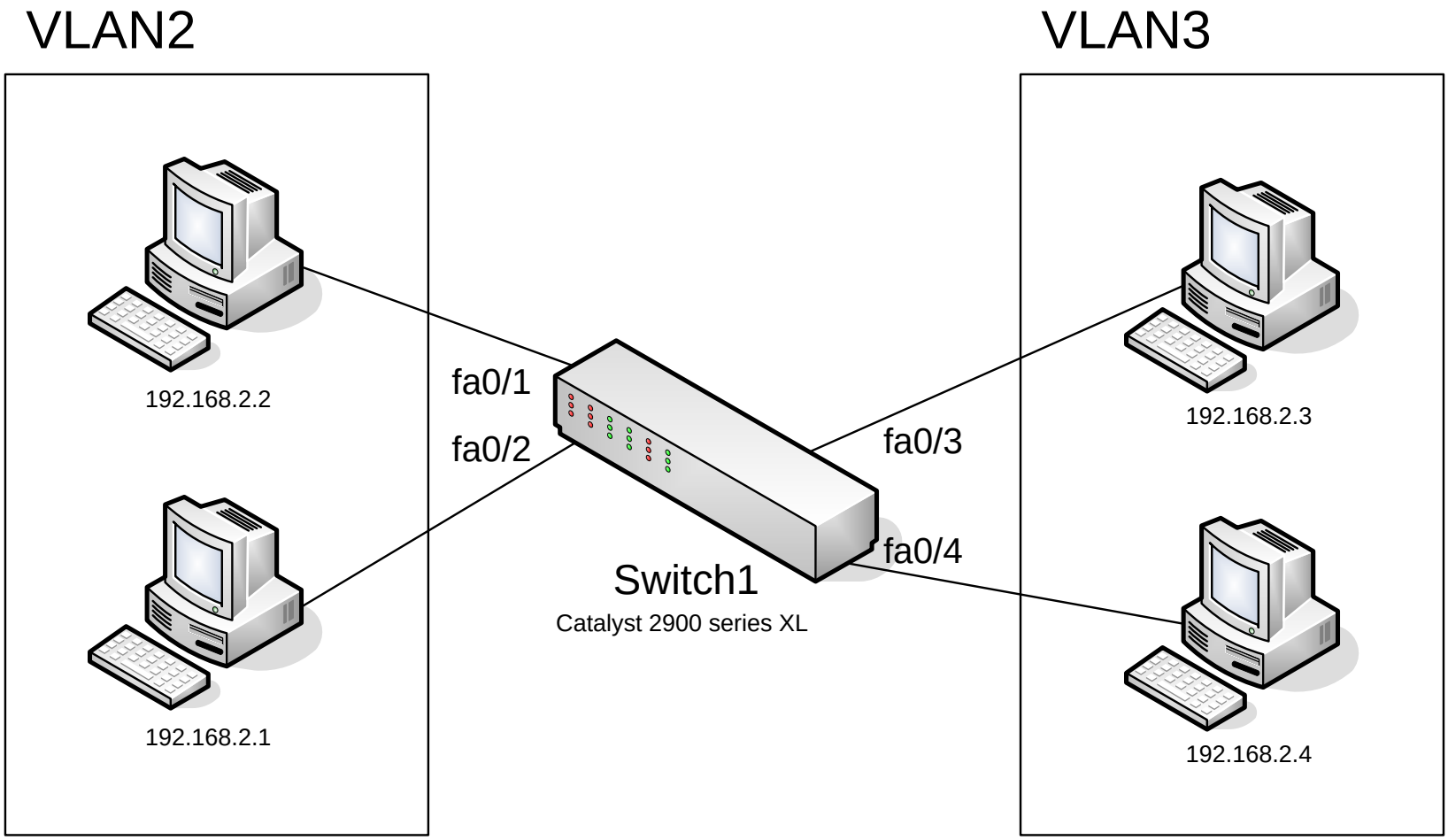
- Separação lógica de uma LAN física em múltiplas sub-redes virtuais, em que cada uma constitui o seu próprio domínio de broadcast de nível 2.

- Só a nível 3 poderemos ter comunicação entre VLANs diferentes.

Virtual Local Area Networks

- As VLANs são criadas com objectivos de âmbito administrativo e/ou desempenho.
- No primeiro caso, pretende-se limitar ou compartimentar logo a nível 2 o tráfego destinado aos utilizadores finais.
- No segundo caso, pretende-se poupança da largura de banda disponível.

Virtual Local Area Networks



Virtual Local Area Networks

- Com a criação de VLANs num switch, a principal diferença verifica-se na forma como os broadcasts e multicasts de N2, vão passar a ser processadas.

- Quando não existem VLANs configuradas, broadcasts e multicasts são propagados para todas as portas (flooding).

Virtual Local Area Networks

- VLANs num switch implicam a segmentação do domínio de broadcast de N2 em tantos subdomínios quantas as VLANs configuradas, não existindo tráfego de nível 2 entre VLANs.

- Pelas razões anteriores, tivemos de usar o comando **dhcp helper** (nos routers).

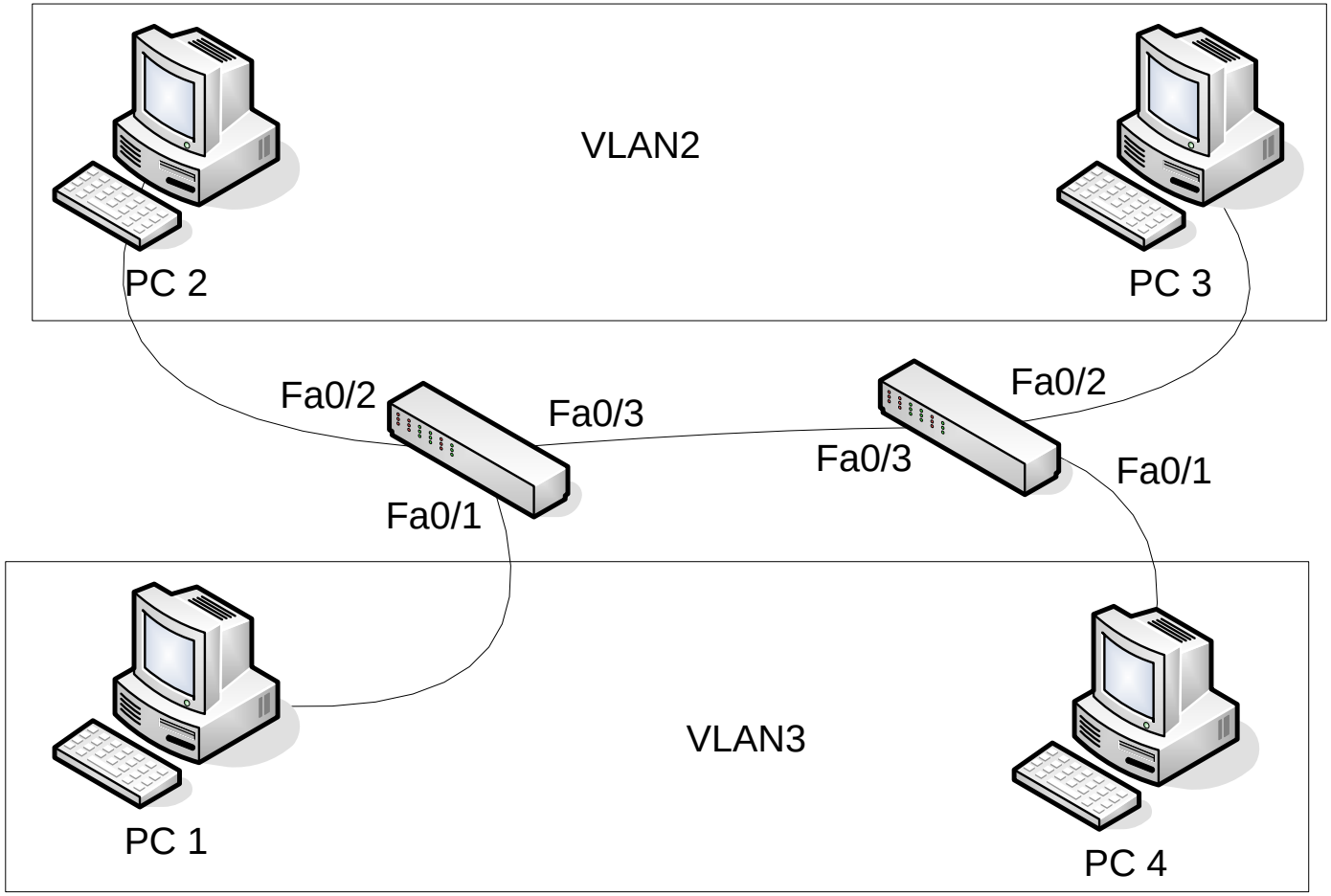
Tipos de portas

- Podem ser configuradas em Access Mode ou Trunk Mode.

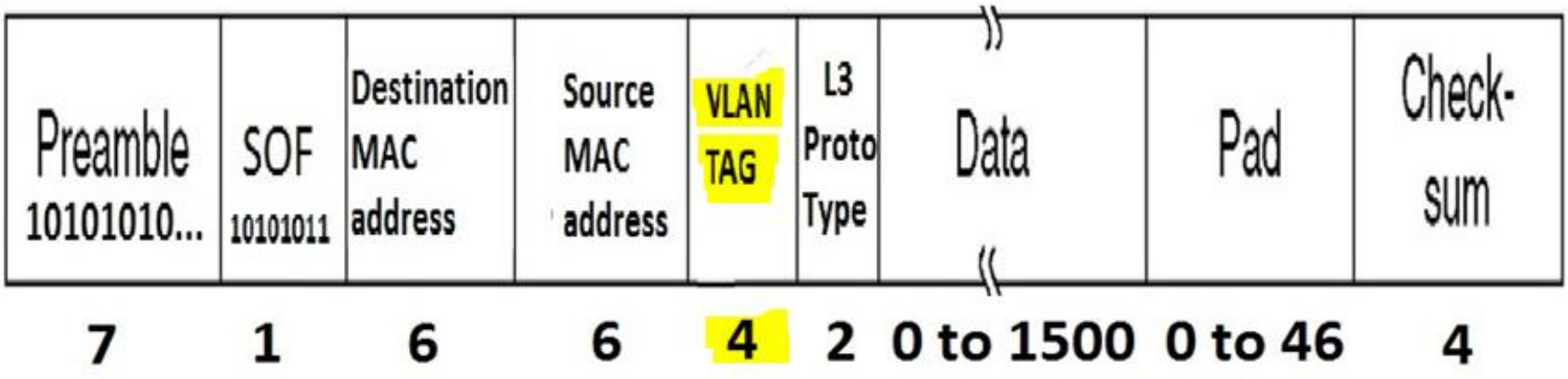
- Nas portas em access mode circulam tramas pertencentes a uma só VLAN.

- Nas portas em trunk mode circulam tramas pertencentes a várias VLANs.

Tipos de portas



Tagging



- O campo VLAN TAG contem o ID e prioridade da VLAN.

Operações básicas de um switch

- Recebe tramas numa porta, determina a(s) porta(s) de saída, com base no endereço MAC de destino e transmite a trama para essa(s) porta(s).

- São três as operações básicas de um switch: Address learning, Frame forwarding e Address Ageing.

Address learning

- Construção dinâmica da tabela ARL (address resolution logic).

- Inicialmente a tabela encontra-se vazia e o switch vai preenchendo a mesma com base na análise das tramas que o atravessam.

- A cada registo que cria na ARL associa um time stamp constituído pelo instante no tempo em que a trama foi recebida.

Frame forwarding

- Esta tarefa é efectuada depois de o switch ter actualizado os registos da ARL.

- Se o endereço MAC destino se encontra na porta em que a trama foi recebida, o switch não executa qualquer acção.

- Se não encontra nenhum registo com o endereço MAC de destino, repete a trama para todas as portas do switch (flooding).

Address Ageing

- Descarte das entradas desactualizadas na tabela ARL, para facilitar a detecção de mudanças dos hosts de uma porta para outra.

- Existe um processo a correr em background que periodicamente verifica o campo time stamp de cada registo da ARL e remove os registos desactualizados.

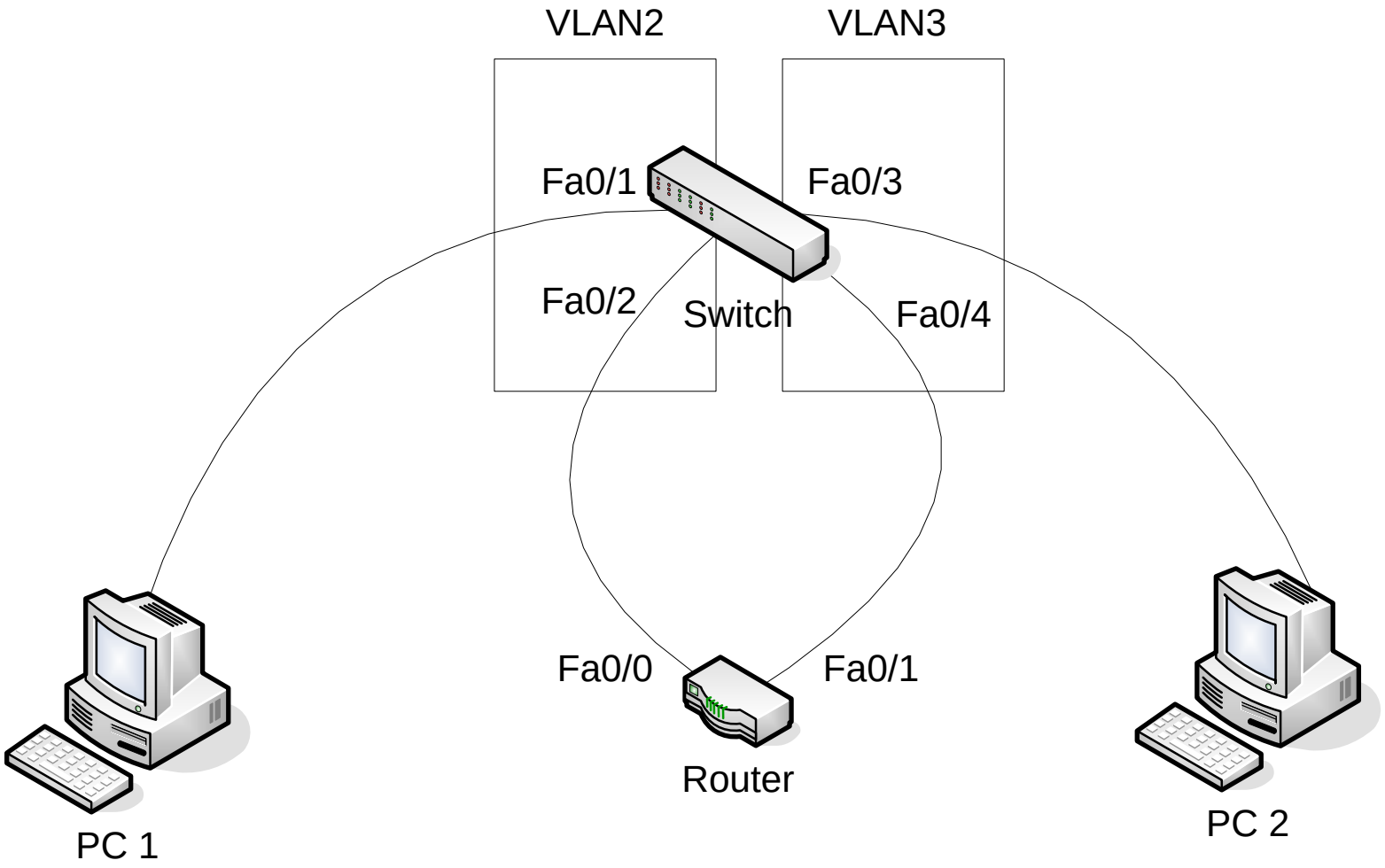
Identificação das VLANs

- **Port based:** Cada porta do switch encontra-se configurada com um dado VLAN ID.

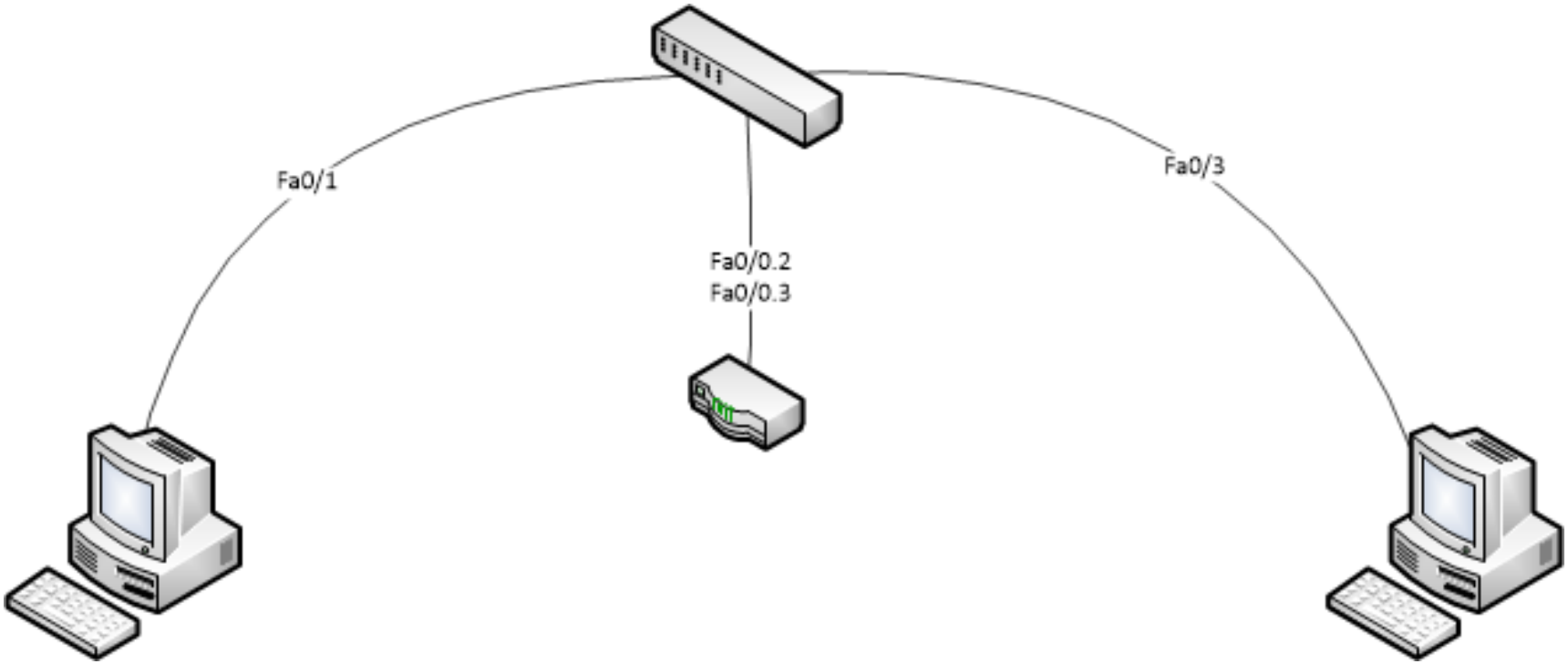
- **MAC based:** O switch é configurado com pares (endereço MAC; VLAN ID).

- **IP based:** O switch é configurado com pares (sub-rede IP; VLAN ID).

Encaminhamento entre VLANs



Sub-interfaces



VLAN Trunking Protocol

- Protocolo proprietário da Cisco que permite disseminar a configuração das VLANs de uma rede, automaticamente por todos os seus switches.

- Utiliza as ligações de trunking para optimizar o tráfego de rede entre switches.

Virtual Local Area Networks

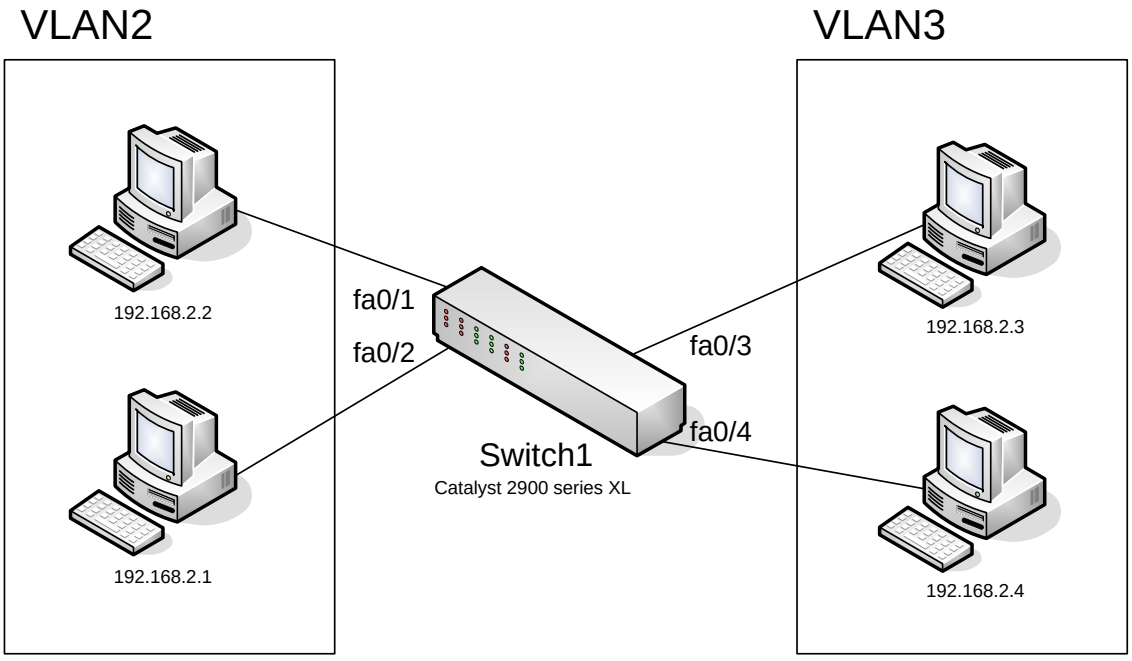
Uma VLAN, tal como o nome indica, consiste numa separação lógica de uma LAN física em múltiplas sub-redes virtuais, em que cada uma constitui o seu próprio domínio de broadcast de nível 2. Só a nível 3 poderemos ter comunicação entre VLANs diferentes.

As VLANs são criadas, fundamentalmente, com objectivos de âmbito administrativo e/ou desempenho. No primeiro caso, pretende-se limitar ou compartimentar logo a nível 2 o tráfego destinado aos utilizadores finais, levando a cada grupo apenas a informação de que necessita. No segundo caso, pretende-se poupança da largura de banda disponível, com vista a garantir um QoS (Quality of Service) mínimo para determinado tipo de aplicações.

Um exemplo típico consiste na utilização de telefones VoIP na rede local, em que os pacotes relativos a telefonia fluem numa VLAN criada especificamente para o efeito (e muitas vezes por isso denominada Voice VLAN).

1.Exemplo

Na figura seguinte esquematiza-se uma LAN física, materializada pelo Switch1, subdividida logicamente na VLAN2 e VLAN3. As portas fa0/1 e fa0/2 pertencem á VLAN2 e as portas fa0/3 e fa0/4 pertencem á VLAN3.



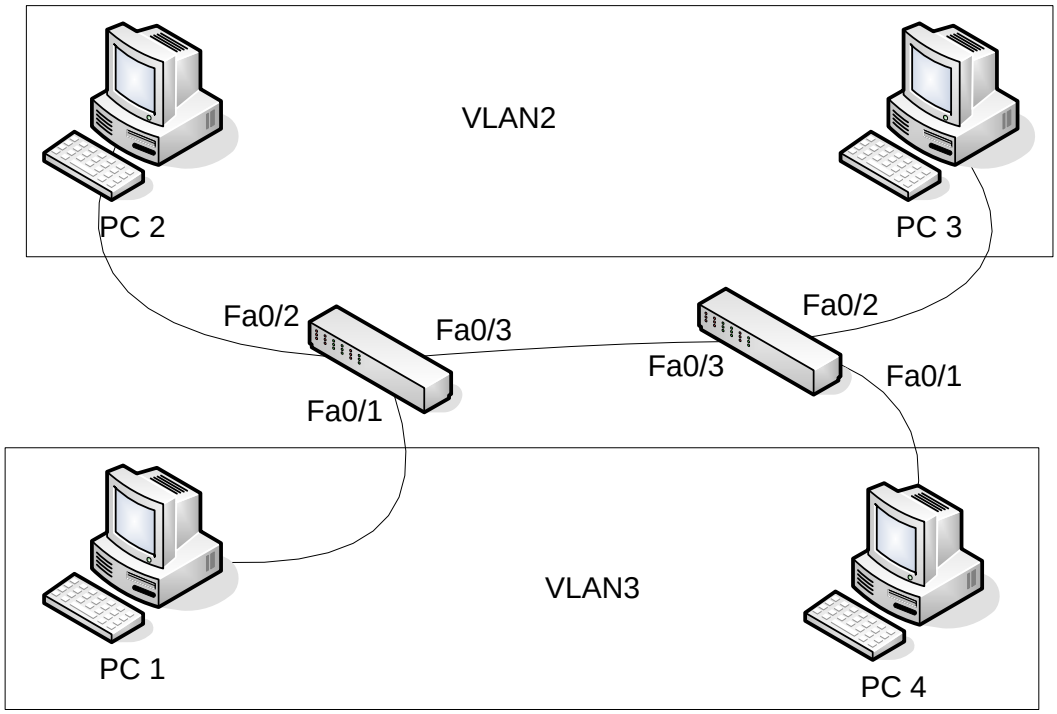
Com a criação das VLANs anteriores no Switch1, a principal diferença verifica-se na forma como os broadcasts de N2 e as tramas de multicast de N2, vão passar a ser processadas pelo switch. Quando não existem VLANs configuradas no switch, ou melhor, quando só existe a VLAN default 1, todas as portas pertencem a esta VLAN1. Como consequência, broadcasts e multicasts são propagados para todas as portas (flooding).

Quando existem outras VLANs configuradas (no exemplo, VLAN2 e VLAN3), o Switch1 vai confinar o flooding dos multicasts e broadcasts apenas aos membros da VLAN onde esses pacotes surgiram. Por outras palavras, a criação de VLANs num switch vai promover a segmentação do domínio de broadcast de N2 em tantos subdomínios quantas as VLANs configuradas, não existindo tráfego de nível 2 entre VLANs.

Pelas razões anteriores, tivemos de usar o comando **dhcp helper** (nos routers) para garantir que os broadcasts dhcp são encaminhados para a VLAN onde se encontra o servidor DHCP.

2.Tipos de portas

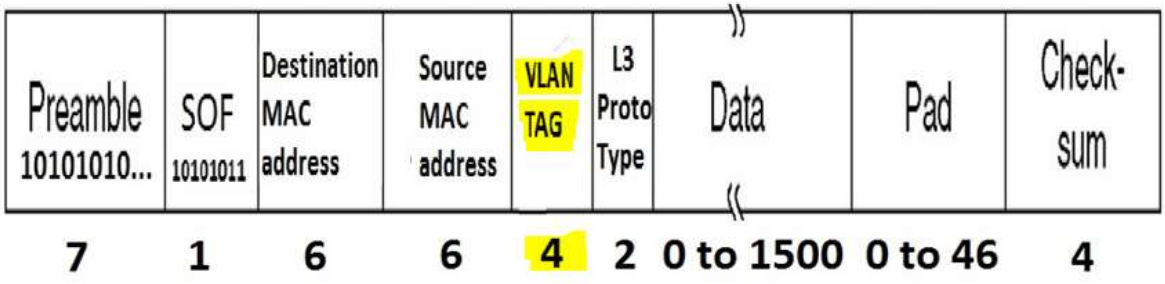
No Switch1 anterior, as portas podem ser configuradas em dois modos de acesso principais: Access Mode ou Trunk Mode. Nas portas em access mode circulam tramas pertencentes a uma só VLAN. Nas portas em trunk mode circulam tramas pertencentes a várias VLANs. Os hosts são, normalmente, ligados a portas configuradas em access mode. Switches, routers, firewalls, são tipicamente ligados a portas em trunk mode. Por exemplo:



As portas fa0/3 nos dois switches deverão encontrar-se configuradas em trunk mode, por forma a deixarem passar tramas pertencentes tanto á VLAN2 como á VLAN3. As portas fa0/1 e fa0/2 deverão estar configuradas em access mode.

3.Tagging

Para que numa ligação em trunk mode, o switch destinatário possa inserir a trama que chega na VLAN correcta, é necessário que estas tragam um campo adicional (no cabeçalho da trama, com 4 bytes de comprimento) com o nome da VLAN a que respeitam. Esta tag é definida no protocolo de trunking normalizado IEEE 802.1Q.



O campo VLAN TAG contem o ID e prioridade da VLAN. A prioridade é usada com o objectivo de garantir QoS a determinadas tramas em prejuízo de outras, no caso de congestão na rede. No switch de destino, o campo VLAN TAG é removido.

4.Operações básicas

Um switch de N2 ou uma bridge encarregam-se de encaminhar tramas dentro de uma LAN. Em termos gerais, recebe tramas numa porta, determina a(s) porta(s) de saída, com base no endereço MAC de destino e transmite a trama para essa(s) porta(s). Desta forma, garante que as tramas são repetidas apenas para as portas necessárias e não para todas (como faz um hub). Nestas condições, são três as operações básicas de um switch:

a)**Address learning**

Construção da tabela ARL (address resolution logic) de forma dinâmica (sem qualquer configuração), baseando-se apenas nos endereços MAC origem das tramas que lhe chegam a qualquer uma das suas portas. Inicialmente a tabela encontra-se vazia e o switch vai preenchendo a mesma com base na análise das tramas que o atravessam. Quando recebe uma trama numa porta, lê o endereço MAC de origem. Se este não existe na ARL, cria um registo para o endereço, na porta por onde a trama entrou. A este registo associa um time stamp constituído pelo instante no tempo em que a trama foi recebida. Se uma nova trama proveniente da mesma origem for recebida na mesma porta, o switch limita-se a actualizar o time stamp do registo.

b)Frame forwarding

Encaminhamento de tramas que chegam para a porta de saída, identificada na tabela ARL pelo(s) respectivo(s) endereço(s) MAC da(s) placa(s) de rede do(s) host(s) ligado(s). Esta tarefa é efectuada depois de o switch ter actualizado os registos da ARL. Para a executar, consulta a ARL para determinar a porta onde se encontra ligado o host que detém o endereço MAC destino presente na trama recebida. Se o endereço MAC destino se encontra na porta em que a trama foi recebida, o switch não executa qualquer acção. Se não encontra nenhum registo com o endereço MAC de destino, repete a trama para todas as portas do switch. Este processo tem o nome de flooding.

c)Address Ageing

Descarte das entradas desactualizadas na tabela ARL, para facilitar a detecção de mudanças dos hosts de uma porta para outra. Existe um processo a correr em background que periodicamente verifica o campo time stamp de cada registo da ARL e remove os registos desactualizados. O valor exacto do time out considerado para o registo varia com a implementação.

Uma vez que os hosts da rede não enviam aos switches tramas com o campo VLAN TAG, tem de existir um método que permita aos switches/routers identificar a VLAN em que se encontra cada uma das suas portas. Isto pode ser efectuado de três maneiras diferentes:

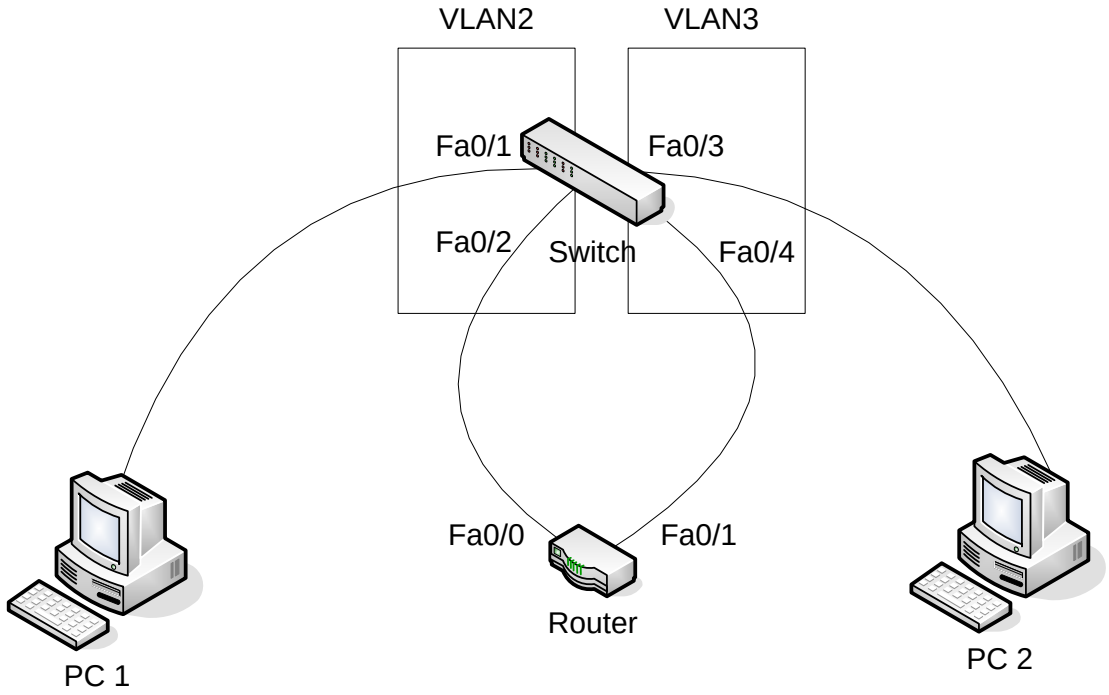
a)Port based
Cada porta do switch encontra-se configurada com um dado VLAN ID. Só em duas situações uma porta pode pertencer a mais de uma VLAN: numa porta de trunking ou numa porta onde VoIP esteja configurado.

b)MAC based
O switch é configurado com pares (endereço MAC; VLAN ID), de tal modo que o switch decide a que VLAN uma trama pertence baseado neste mapeamento e no endereço MAC origem da trama recebida.

c)IP based
O switch é configurado com pares (sub-rede IP; VLAN ID), de tal modo que o switch identifica a VLAN a que a trama recebida pertence, usando o endereço IP presente no cabeçalho do datagrama IP encapsulado na trama.

5.Encaminhamento entre VLANs

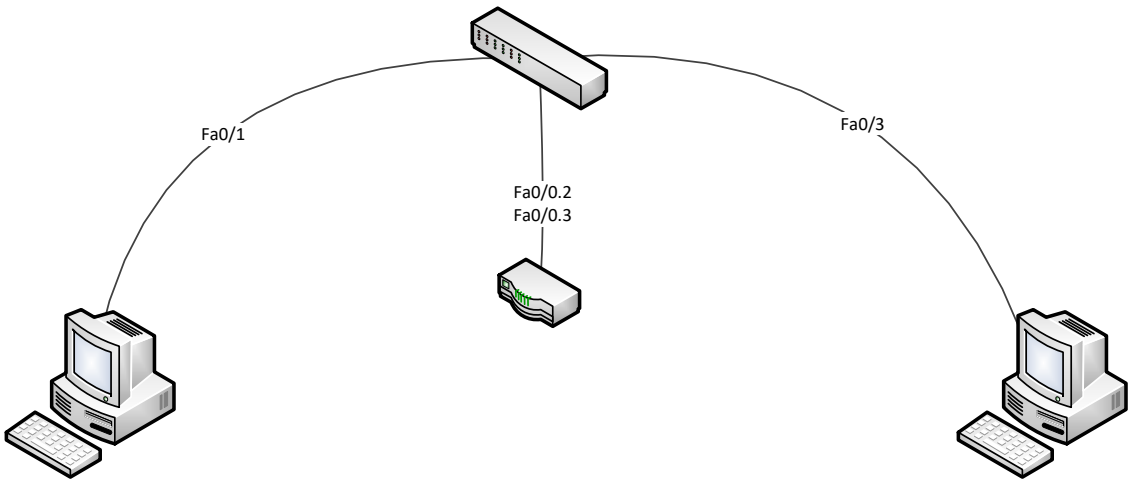
A cada VLAN vai corresponder uma sub-rede IP de N3. Não existindo a possibilidade do switch encaminhar pacotes entre VLANs diferentes, tal função terá de ser desempenhada por um router:



Na LAN anterior temos o tráfego da VLAN2 para a VLAN3 e vice-versa, a ser encaminhado pelo router. Este encontra-se ligado a duas portas no switch, fa0/2 na VLAN2 e fa0/4 na VLAN3. Deve notar-se que o router só encaminha o tráfego de uma VLAN destinado a hosts da outra, filtrando todos os demais datagramas IP.

6.Sub-interfaces

Quando pretendemos ligar um router ou um firewall a uma porta configurada em modo trunking num switch, temos de configurar sub-interfaces no router ou firewall.



A configuração vai variar consoante a implementação do router ou firewall. Nas aulas práticas vamos utilizar a implementação da Cisco.

7.VLAN Trunking Protocol

Trata-se de um protocolo proprietário da Cisco que permite disseminar a configuração das VLANs de uma rede, automaticamente por todos os seus switches. Desta forma não é necessário repetir a configuração das diferentes VLANs em cada um deles.

Utiliza as ligações de trunking para optimizar o tráfego de rede entre switches. Nas aulas práticas vamos efectuar um exemplo de configuração deste protocolo.

Etherchannel

Nesta aula vamos configurar oito interfaces em cada um dos switches centrais (fa0/1 a fa0/8) pertencendo ao channel-group 1. A este grupo vai corresponder o interface Port-channel 1, com uma largura de banda agregada de 800 MB. Os switch centrais são 3560-24PS. Configure ainda dois PCs na rede 10.241.1.0 para teste da ligação:

- **Configuração nos switches centrais** 3560-24PS

  Switch>enable
  Switch#configure terminal
  Switch#int fa0/1
  Switch#channel-group 1 mode on
  Switch#int fa0/2
  Switch#channel-group 1 mode on
  Switch#int fa0/3
  Switch#channel-group 1 mode on
  Switch#int fa0/4
  Switch#channel-group 1 mode on
  Switch#int fa0/5
  Switch#channel-group 1 mode on
  Switch#int fa0/6
  Switch#channel-group 1 mode on
  Switch#int fa0/7
  Switch#channel-group 1 mode on
  Switch#int fa0/8
  Switch#channel-group 1 mode on
  Switch#end

Switch#copy run start
Switch#show etherchannel summary

```
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           -      Fa0/1(P) Fa0/2(P) Fa0/3(P) Fa0/4(P) Fa0/5(P) Fa0
/6(P) Fa0/7(P) Fa0/8(P)
```

Switch# configure terminal
Switch#int port-channel1
Switch#description Etherchannel 800MB
Switch#switchport trunk encap dot1q
Switch#switchport mode trunk
Switch#end
Switch#copy run start

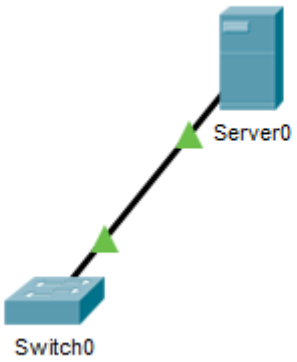
Com o comando **ping** verifique se o port-channel entre os switches deixa passar tráfego.

Switch# configure terminal
Switch#vlan 101
Switch#name VLAN101
Switch#exit
Switch#int fa0/24
Switch#switchport access vlan 101
Switch#end
Switch#copy run start

Com o comando **ping** verifique que os PCs só voltam a trocar mensagens quando a VLAN101 for configurada nos dois switches, o que comprova que o interface Port-channel1 se encontra em modo trunk. Os PCs encontram-se ligados às portas fa0/24 dos respectivos switches.

Servidor TFTP

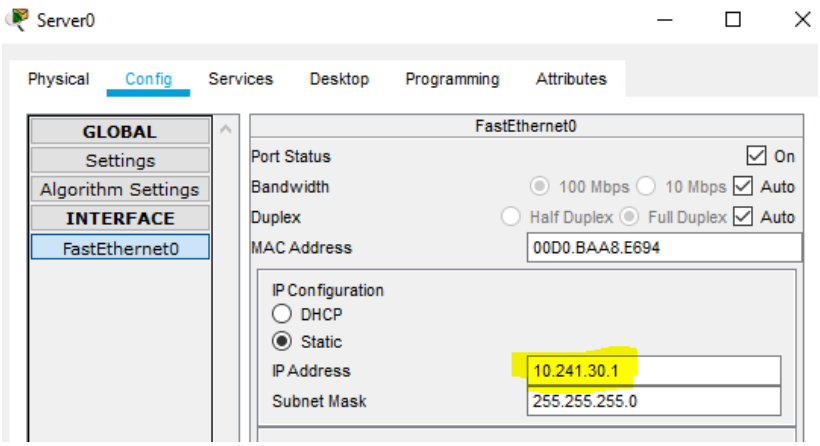
- Criar a seguinte rede local:



- Configuração no Switch0:

#conf t
#vlan 130
#name ADMIN
#exit
#int vlan130
#ip address 10.241.30.2 255.255.255.0
#exit
#int fa0/1
#switchport access vlan 130
#end

- Configuração no Server0:



Efetuar os seguintes comandos no Switch0:

#conf t
#hostname sw1
#end
#copy run tftp
Address or name of remote host [] ? 10.241.30.1
#Destination filename [sw1-confg]?
#
#conf t
#hostname Switch0
#end
#copy tftp run

E, concluido o comando, constatamos que a prompt do IOS passa novamente a ser “sw1#”.