ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

# Licenciatura em Engenharia Informática e Multimédia

## Redes de Informação

Ano Letivo 2020/21

**5º Semestre**

## Trabalho 1

**30 novembro**


**Grupo 7:**

Luís Fonseca (A45125)

Miguel Silvestre (A45101)

Duarte Domingues (A45140)

**Docente:** Eng. Vítor Almeida

# Índice de Conteúdos

# Índice de Figuras

# 1. Introdução e Objetivos

Para este primeiro projeto proposto na disciplina de Redes de Informação, pretendia-se uma familiarização com a temática das VLAN (Virtual LAN), com o protocolo de proteção contra loops na camada 2 (STP), encaminhamento estático e com o protocolo de encaminhamento dinâmico RIP.

Começámos por criar a topologia sugerida no enunciado, usando o programa "Cisco Packet Tracer". Esta representa uma infraestrutura simplificada de um Internet Service Provider (ISP), que fornece conectividade a duas empresas (dois clientes), A e B. Este ISP coloca equipamentos nas instalações de cada empresa que servem como um Network Demarcation Device (NDD).

Para dar um pouco mais de contexto, iremos explicar alguns dos dados que nos foram fornecidos, além da topologia.

O ISP atribuiu blocos de endereços IP distintos a cada empresa para uso interno destas. As empresas possuem vários departamentos e, como tal, necessitam de possuir a sua rede segmentada em várias sub-redes, sendo o gateway de cada sub-rede sempre o router de cada empresa. O ISP utiliza ainda duas redes /30 (P2P na camada 3) de interligação entre os seus routers e os de cada empresa. Cada empresa possui uma rota estática default a apontar para o router do ISP. Este, por sua vez, anuncia através de rotas estáticas as redes que atribuiu às empresas. É utilizado o protocolo RIPv2 no core do ISP para os seus routers trocarem informações de rotas. O R2 do ISP possui uma ligação à Internet que é simulada como uma interface virtual (Loopback0). Pretende-se então que com a topologia indicada se consiga implementar a maior redundância possível sem comprometer a eficiência ou necessitar de novos equipamentos.

Posto, isto, todas as questões relativas a esta topologia serão abordadas no presente relatório.

# 2. Tarefa 1 – Pequenas configurações na EmpresaA

Após a implementação da rede no programa, conseguimos responder às várias perguntas da primeira Tarefa.

**a) Use o comando: "no ip domain-lookup". Qual o objetivo deste comando?**

Qualquer palavra inserida num dispositivo que não seja reconhecido como um comando válido é tratado como um nome de host. Esse respetivo dispositivo irá traduzir essa palavra para um endereço IP, para um processo que dura cerca de um minuto. Este comando permite retirar um servidor DNS configurado para um dado router ou switch, usando este comando, é possível evitar este processo. Em baixo pode ser visto uma figura de como foi usado este comando:

```
Switch>exemplo
Translating "exemplo"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer
address

Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console
^Z
Switch#^Z
Switch#example
Translating "example"
% Unknown command or computer name, or unable to find computer
address
```

*Figura 1 - comando no ip domain-lookup usado*

**b) Quais as VLAN por omissão que existem [sh vlan] antes de ser configurada qualquer VLAN em qualquer equipamento?**

Usando este comando, é possível de verificar que, na empresa A, tanto os switches, como os routers apresentam cinco VLANs por omissão. Na figura de baixo é possível de ver o nome das VLANs por omissão.

```
Switch#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- ---------
-------------------------------
1    default                           active    Fa0/1, Fa0/2,
Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6,
Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10,
Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14,
Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18,
Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22,
Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

*Figura 2 - VLANS por omissão*

**c) Qual a tag que as tramas pertencentes à VLAN 1 transportam?**

Olhando para a VLAN 1, é possível de verificar que a tag das tramas é 1, tag essa que corresponde ao id dessa mesma VLAN.

**d) Quais as consequências de passarmos os timers "Max Age" = 20 sec e "Forward Delay" = 15 sec para metade desses valores? Qual é a Root Bridge (RB)? Justifique.**

Antes de responder à pergunta propriamente dita, é necessário saber o significado destes dois conceitos:

**Max Age**: controla o período máximo, que passa antes que uma bridge port guarda as suas informações BPDU de configuração. Este tempo, por omissão, é de 20 segundos, mas pode ser ajustado para um tempo entre 6 e 40 segundos.

**Forward Delay:** é o tempo gasto em ouvir e aprender um estado. Este tempo, por omissão, é igual a 15 segundos, no entanto, pode ser alterado para um valor entre 4 e 30 segundos.

Com isto, concluímos que se passarmos os timers para metade, o tempo para ouvir e aprender um estado é menor (ou seja aprende mais depressa) mas a informação que uma brigde port demora a guardar as suas informações é maior. A root bridge será o switch1_piso2.

**e) Por omissão qual é o tipo de Spanning-Tree (STP) ativo [sh span]?**

Inicialmente todas as Bridges enviam as mensagens BPDU com o seu identificador de Bridge e assumindo-se como Root Bridge. Todas as Bridges recebem as mensagens com os identificadores das outras Bridges e apenas reenviam as mensagens cujo identificador é o menor identificador de todas as Bridges. Ao fim de algum tempo, apenas a Root Bridge está a enviar as mensagens com o seu identificador como Root Bridge, e todas as outras estão a reenviar essas mensagens atualizando os seus campos. Desta forma a Bridge com o menor valor de identificador é eleita como Root Bridge. Isto é, todas as Bridges têm o mesmo valor de prioridade (valor por omissão) e por isso o desempate é feito com base no endereço MAC.

**f) Quantas árvores (spanning trees) existem na topologia implementada?**

Inicialmente, existem 4 árvores (não contando com a VLAN default), visto que só temos 4 VLAN (VLAN0001, VLAN0010, VLAN0020, VLAN0030, VLAN0050, como se observa ao invocar o comando "sh span")

**g) Para a empresa A, construa a tabela de cálculo do custo dos caminhos e de determinação de quais são as portas Root, Designated e Blocking e calcule os respetivos valores. Os resultados a que chegou são coerentes com os que o simulador apresenta?**

| Porta | | PC | RPC | RP | DPC | DP | Blocking |
|---|---|---|---|---|---|---|---|
| SW1_piso1 | Fa0/2 | 19 | 19+19+19=57 | | 19 | X | |
| | Fa0/10 | 19 | - | - | - | - | - |
| | Fa0/20 | 19 | 19+19=38 | | 19 | X | |
| | Fa0/24 | 19 | 19 | | 19 | | X |
| | Gi0/1 | 4 | 19+19+4+4=46 | | 19 | X | |
| | Fa0/23 | 19 | 19 | X | 19 | | |
| SW1_piso2 | Fa0/10 | 19 | 0 | - | | | |
| | Fa0/2 | 19 | 0 | - | 0 | X | |
| | Fa0/24 | 19 | 0 | - | 0 | X | |
| | Fa0/23 | 19 | 0 | - | 0 | X | |
| SW2_piso1 | Fa0/10 | 19 | - | - | - | - | |
| | Fa0/24 | 19 | 19+19=38 | | 19+19=38 | | X |
| | Fa0/2 | 19 | 19+19=38 | | 38 | | X |
| | Gig0/1 | 4 | 19+4+4=27 | X | | | |
| SW2_piso2 | Fa0/11 | 19 | - | - | - | - | |
| | Fa0/20 | 19 | 19+19=38 | | 19 | | X |
| | Fa0/10 | 19 | - | - | - | - | - |
| | Fa0/2 | 19 | 19 | X | 19 | X | |
| | Fa0/24 | 19 | 19+4+4+19=46 | | 19 | X | |
| SW_DC | Gig1/0/1 | 4 | 19+4=23 | X | 19+4=23 | | |
| | Gig1/0/2 | 4 | 19+19+4=42 | | 19+4=23 | | |
| | Gig1/0/3 | 4 | - | - | - | - | - |
| | Gig1/0/4 | 4 | - | - | - | - | - |
| | Gig1/0/5 | 4 | - | - | - | - | - |

**h) Qual o custo do caminho mais curto até ao Router A desde o PC9?**

O custo do caminho mais curto será: 57(19+19+19), e o percurso efetuado é o seguinte:

➔ RA > SW2_piso1 > SW2_piso2 > PC9

**i) Force a root bridge para ser o SW_DC através da prioridade. Possui alguma porta bloqueada?**

Para fazer com que o SW_DC torna-se root bridge foi necessário alterar a sua prioridade, essa prioridade foi alterada para um valor mais baixo, neste caso foi passado para o valor 28670. Na figura abaixo, é possível der ver o comando que foi usado para alterar a prioridade deste switch, tornando assim a root bridge da empresa A

```
Switch(config)#sp
Switch(config)#spanning-tree vlan 1
Switch(config)#spanning-tree vlan 1 p
Switch(config)#spanning-tree vlan 1 priority 28670
% Bridge Priority must be in increments of 4096.
% Allowed values are:
  0     4096  8192  12288 16384 20480 24576 28672
  32768 36864 40960 45056 49152 53248 57344 61440
Switch(config)#
Switch(config)#
Switch(config)#spanning-tree vlan 1 priority 20480
Switch(config)#end
```

*Figura 3 - comando usado para alterar a prioridade deste switch*

Não contém portas bloqueadas, apenas Designated. Através do comando “show spanning-tree”, conseguimos analisar o estado das portas em todas as VLAN existentes.

**j) Na literatura sobre spanning tree encontra-se frequentemente a afirmação de que todas as portas de um root switch/bridge são portas Designated. Comente tendo em consideração o SW_DC.**

Assumindo que o SW_DC é a root bridge, todas as portas, seguindo o protocolo STP iram ser todas designated. Uma porta que sendo designated é uma porta com o menor custo até à root bridge. Sendo que uma porta em estado root, não pode ser designated

**k) Ative o modo per-Vlan rapid spanning tree. Verifique se é necessário ativá-lo em todos os switches?**

Não será necessário ativá-lo em todos os switches, apenas na raiz, que enviará mensagens de mudança de topologia para os restantes switches. Neste caso, sabemos que a raiz é o multilayer switch (SW_DC), que se localiza no centro da topologia da rede da empresa A. Efetuámos então o seguinte comando:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#sp
Switch(config)#spanning-tree mode
Switch(config)#spanning-tree mode r
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#end
```

*Figura 4 - comando de ativação do Per-VLAN spanning tree*

**l) Quantas árvores passaram a existir?**

Através do comando “show spanning-tree” conseguimos observar as várias VLAN existentes. São as mesmas de antes, 4 VLAN (mais 1, que é a pôr default: VLAN 0001)

**m) Existem duas ligações entre o sw1_piso1 e o sw1_piso2, uma delas bloqueada. Altere a configuração de maneira a desbloquear a ligação bloqueada e a desbloquear outra.**

Foi o usado o comando "shutdown" que permitiu desligar a ligação entre o Switch1_Piso1 e o Switch1_Piso2(switches usados para o teste deste comando). Na figura abaixo, pode ser visto o comando a ser usado:

```
Switch(config-if)#int fa0/23
Switch(config-if)#shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23,
changed state to down

Switch(config-if)#
Switch(config-if)#int fa0/24
Switch(config-if)#no shutdown
```

*Figura 5 - Bloqueio de ligação entre Switches*

Como se pretendia, ao bloquear esta ligação, a outra para o mesmo caminho desbloqueou-se.

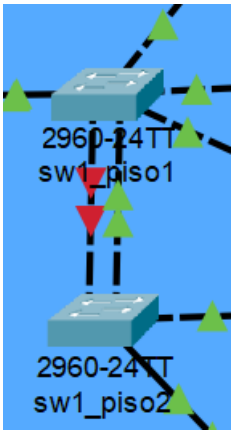


*Figura 6 - Nova ligação entre o Switch1_piso1 e Switch1_piso2*

**n) Explique de forma detalhada a razão do sw2_piso2 escolher o caminho por omissão em detrimento de outro possível. Realize as alterações que considerar necessárias para que o caminho preferido seja outro que não o escolhido (por omissão).**

O caminho por omissão do Switch2_piso2 permite-lhe chegar aos restantes Switches com menos ligações intermédias, isto é, pelo caminho mais curto, de forma generalizada. Alterámos então este caminho por omissão, bloqueando-o, como foi efetuado na alínea prévia (interface Fa0/4 shutdown). Deste modo, a topologia mudou, desbloqueando um dos restantes segmentos.

o) **Considere a seguinte afirmação: "Com o SW_DC como root bridge, a substituição do Hub0 por um switch, interligado entre o sw1_piso1 e o SW_DC, iria melhor a conetividade entre o PC5 e o Server2 pois o caminho ficava mais curto.". Indique, justificando, se a mesma é falsa ou verdadeira atendendo a que todas as ligações ao switch novo funcionam a 100 Mbps.**

Esta afirmação é falsa, visto que o Hub apenas permite fazer o transporte e a ligação das BPDUs, qualquer que seja a sua velocidade de transmissão.

# 3. Tarefa 2 – Configurações fixas para a EmpresaA

Antes de passar para a execução desta tarefa, foi necessário saber informação acerca dos diferentes parâmetros desta tarefa. Os parâmetros foram os seguintes:

- ➔ N_Grupo: corresponde ao número do grupo associado;
- ➔ X: obtido pela fórmula dada pelo enunciado;

Para o cálculo do parâmetro X, foi usado o website wolframalpha, o link deste website pode ser encontrado na página referente à bibliografia. Na figura seguinte, pode ser visto o cálculo deste parâmetro:

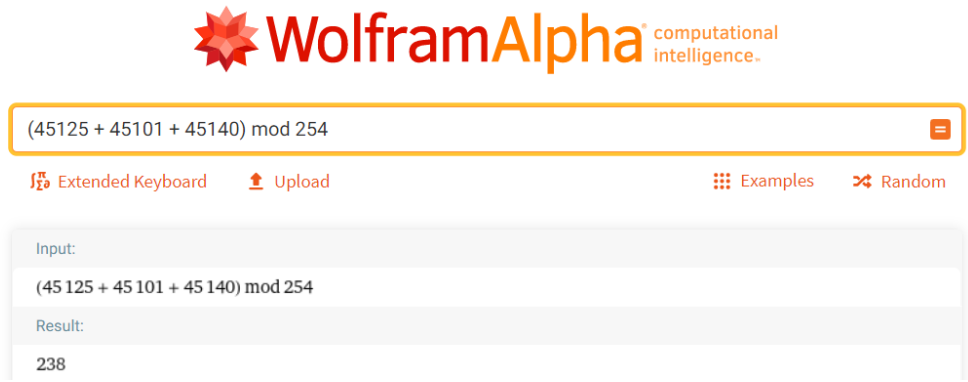


*Figura 7 - cálculo do parâmetro X*

Seguidamente, segmentámos a topologia da Empresa A, utilizando VLAN para ficar de acordo as regras abaixo:

| Nº VLAN | Nome | IP do Gateway | Rede | PC´s |
|---|---|---|---|---|
| **80** | Contabilidade | 192.168.238.0 | 192.168.238.0/24 | PC7, PC9 |
| **90** | Secretariado | 192.168.239.0 | 192.168.239.0/24 | PC5, PC8 |
| **100** | Informática | 192.168.240.0 | 192.168.240.0/25 | Server2 |
| **105** | Gestão de rede | 192.168.240.128 | 192.168.240.129/25 | PC6 |

Pretendia-se então a implementação no simulador da topologia indicada e o resultado dos testes que comprovassem a correta implementação da mesma.

De acordo a tabela acima, implementámos as VLAN em cada switch. Abaixo figura o exemplo para a configuração da VLAN 80 no switch2_piso1 (as restantes VLAN seguem as mesmas instruções).

```
Switch(config)#vlan 80
Switch(config-vlan)#name Contabilidade
Switch(config-vlan)#vlan 90
Switch(config-vlan)#name Secretariado
Switch(config-vlan)#vlan 100
Switch(config-vlan)#name Informatica
Switch(config-vlan)#vlan 135
Switch(config-vlan)#name GestaoDeRede
Switch(config-vlan)#exit
```

*Figura 8 - comandos da criação das vlans*

Após estarem definidos os nomes de todas as VLAN, invocámos um “do show vlan br” para as observar

```
sw1_piso1(config)#do sh vlan br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/21, Fa0/22, Fa0/23, Gig0/2
80   Contabilidade                     active
90   Secretariado                      active    Fa0/10
100  Informatica                       active
105  gestao_da_rede                    active
```

*Figura 9 - Novas VLANs criadas*

Por fim, configurámos as portas em modo access ou trunk. Falando no sw1_piso1, para a vlan 90uma das portas tem de estar em modo access. Contudo, as restantes interfaces que ligam às VLAN, devem estar em modo trunk, pois entre switches as ligações serão sempre deste tipo, trunk. Efetuamos o comando seguinte em todas estas interfaces que nos interessavam:

```
interface FastEthernet0/10
 switchport access vlan 90
 switchport mode access
 switchport nonegotiate
!
```

*Figura 11 - porta configurada como access*

```
interface FastEthernet0/9
 switchport trunk native vlan 105
 switchport trunk allowed vlan 80-105
 switchport mode trunk
 switchport nonegotiate
```

*Figura 10 - porta configurada como trunk*

É de notar que o comando “switchport nonegotiate” foi usado para desligar protocolo Dynamic Trunking Protocol (DTP) em cada interface configurada como access ou trunk. Todas as portas foram configuradas com DTP. Para comprovar que em todos os switches este protocolo foi desligado foi usado o comando “show dtp”, e o resultado pode ser visto na figura em baixo:

```
sw1_pisol#sh dtp
Global DTP information
    Sending DTP Hello packets every 30 seconds
    Dynamic Trunk timeout is 300 seconds
    0 interfaces using DTP
```

*Figura 12 - Verificação da desativação do DTP nas  interfaces*

Agora, tendo em conta os dados na primeira tabela, configurámos IPs para cada PC. O algoritmo é o mesmo para todos, apenas se alteram os endereços, de forma que iremos exemplificar uma vez, no caso do PC5. Este PC pertence à VLAN 90, com Gateway de 192.168.239.1 /24.

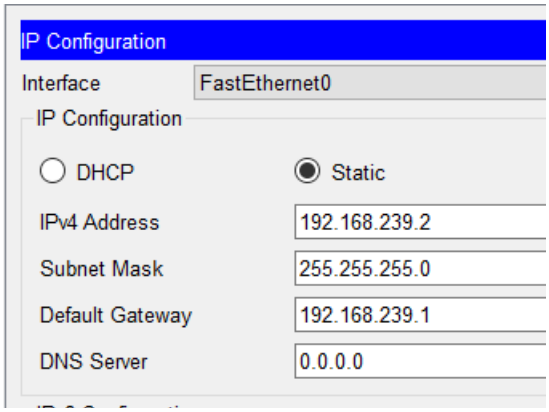


*Figura 13 - Definição do Gateway,IP e máscara para o PC5*

Para lhe adicionar um endereço IP, servimo-nos do comando “(config-if)# **ip add 192.168.239.2 255.255.255.0**”, sendo que é esta a máscara para “/24”. Nos restantes PCs efetuámos o mesmo comando, seguindo a linha de endereços devidos para a respetiva rede.
Em suma, expomos a seguinte tabela com os endereços IP que atribuímos:

| PC | Endereço IP | Gateway |
|---|---|---|
| **PC5** | 192.168.239.2 | 192.168.238.1 |
| **PC6** | 192.168.240.130 | 192.168.240.129 |
| **PC7** | 192.168.238.2 | 192.168.238.1 |
| **PC8** | 192.168.239.3 | 192.168.239.1 |
| **PC9** | 192.168.238.3 | 192.168.238.1 |

# 3.1 Teste de conetividade

Verificámos se existe conectividade entre os equipamentos na mesma VLAN e entre VLANs distintas. Abaixo observam-se as mensagens de “echo request” e “echo reply”, bem-sucedidas entre alguns dos computadores.

```
C:\>ping 192.168.238.3

Pinging 192.168.238.3 with 32 bytes of data:

Reply from 192.168.238.3: bytes=32 time=1ms TTL=128
Reply from 192.168.238.3: bytes=32 time=11ms TTL=128
Reply from 192.168.238.3: bytes=32 time<1ms TTL=128
Reply from 192.168.238.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.238.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

*Figura 14 - Ping do PC7 para o PC9*

```
C:\>ping 192.168.239.2

Pinging 192.168.239.2 with 32 bytes of data:

Reply from 192.168.239.2: bytes=32 time=2ms TTL=128
Reply from 192.168.239.2: bytes=32 time=4ms TTL=128
Reply from 192.168.239.2: bytes=32 time=4ms TTL=128
Reply from 192.168.239.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.239.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 2ms
```

*Figura 15 - Ping do PC5 para o PC8*

# 4. Tarefa 2 – Configurações no Router A

Adicionámos ao SW_DC o RouterA, seguindo a linha de "router-in-a-stick", com as seguintes regras:

- ✓ Da rede da Contabilidade não se deve poder comunicar com nenhuma outra rede/VLAN interna ou externa;
- ✓ Da rede do Secretariado deve-se poder comunicar com a VLAN da Informática (Sugestão: Se no exterior esta rede não for "conhecida", os outros routers não enviarão tráfego para ela através do router A);
- ✓ Da rede da Informática deve ser possível comunicar com a VLAN do Secretariado e para fora da Empresa A;
- ✓ Os equipamentos na rede Gestão da empresa A devem poder comunicar todos entre si (Nota: Todos os equipamentos da empresa devem poder ser acedidos a partir do PC6 de maneira a poder ser realizada gestão remota).

Ora, para começar, tivemos de garantir que todos os computadores conseguiam conectar a todos os computadores. Numa primeira fase, realizados vários testes "ping" entre dispositivos, quisemos garantir que todos comunicavam, de facto, entre si. Isto só seria possível através do router A, pois é ele que permite a ligação entre os vários dispositivos, que reenvia os pacotes pelos segmentos, vindos de todo o lado dentro da rede da empresa A. Tivemos então de garantir que o router A tinha subnets virtuais associadas a cada uma das VLAN (80,90,100 e 105). Para isto, efetuámos os seguintes comandos:

- ✓ Interface xxx
- ✓ Interface xxx.nºVLAN
- ✓ Encapsulation dot1q nºVLAN
- ✓ Ip address xxx

Depois de criadas todas as subnets numa interface do router, foi necessário ir a cada PC e alterar o seu Gateway para ser o ip da sua subnet (note-se que todos os PCs de uma mesma VLAN devem ter o mesmo Gateway). Exemplificando, para a VLAN 80, executámos os seguintes comandos no router A:

- ✓ Interface fa0/1
- ✓ Interface fa0/1.80
- ✓ Encapsulation dot1q 80
- ✓ Ip address 192.168.238.0

Seguidamente, figuram todas as 4 subnets configuradas no routerA.

```
RouterA#sh ip int b
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        10.20.7.2       YES manual up                    up
FastEthernet0/1        unassigned      YES NVRAM  up                    up
FastEthernet0/1.80     192.168.238.1   YES manual up                    up
FastEthernet0/1.90     192.168.239.1   YES manual up                    up
FastEthernet0/1.100    192.168.240.1   YES manual up                    up
FastEthernet0/1.105    192.168.240.129 YES manual up                    up
```

*Figura 16 - Subnets para as VLAN no Router A*

De forma a garantir as especificações primeiramente referidas neste capítulo, focámo-nos no multilayer switch, que serve como um “ponto de encontro” de todas as redes para o router A. Tendo cada dispositivo a comunicar com os restantes, falta-nos então restringir a chegada de algumas VLAN ao router. Por fim, deixámos apenas como trunk, neste switch, as VLAN 90 e 100 (Secretariado e Informática, respetivamente), na interface Gig 1/0/5. Abaixo figuram as tais VLAN em modo trunk nesta interface.

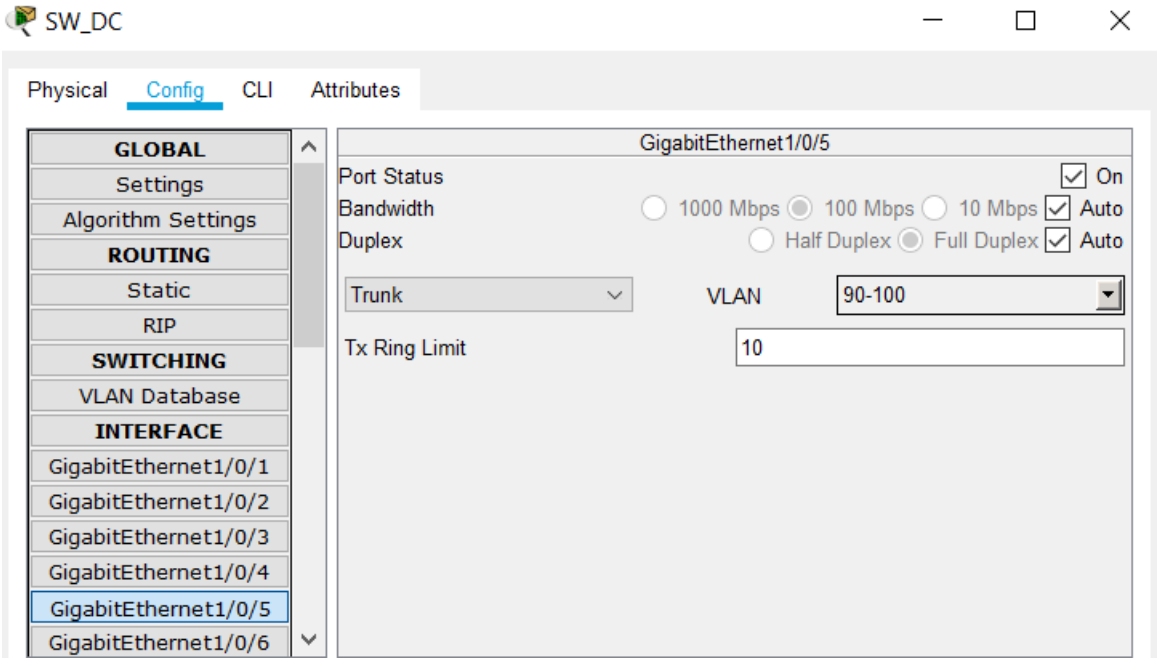


*Figura 17 VLAN em modo trunk numa interface*

## 4.1 Outros comandos úteis

Para nos poupar algum tempo, garantimos também que o router não tenta resolver nomes via DNS cada vez que se enganar. Aliás, efetuamos este comando em todos os routers.

```
RouterA(config)#no ip domain-lookup
RouterA(config)#
RouterA(config)#
RouterA(config)#end
RouterA#
```

*Figura 18 - Desativação do DNS lookup*

Seguidamente, configurámos uma mensagem inicial para quem entra no equipamento, é boa prática fazê-lo, para o caso de ocorrerem acessos indevidos.

```
RouterA(config)#banner login ^C
Enter TEXT message.  End with the character '^'.
--- Router A---
--- ------------------------------------------- ---
--- UNAUTHORISED ACCESS IS PROHIBITED ---
--- Entradas nao autorizadas sao punidas por lei ---
--- (lei 109/2009 de 15 de Setembro) ---
^C
```

*Figura 19 - Mensagem inicial de entrada no equipamento*

## 4.2 Teste de conetividade

Para confirmar que os requisitos acima foram cumpridos, abaixo observam-se as mensagens de echo request e echo reply entre os vários computadores.

```
C:\>ping 192.168.239.2

Pinging 192.168.239.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.239.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

*Figura 20 - ping PC5 para o PC7*

Através dos anteriores pings sem sucesso, conseguimos entender que as restrições requeridas para a comunicação entre VLANS (ou, neste caso, a não comunicação) foram bem cumpridas. Por exemplo, o PC5 e o PC7 não devem comunicar com nenhuma outra. Os pings bem-sucedidos já foram colocados anteriormente no relatório (por exemplo, o PC7 da VLAN de Contabilidade, deve conseguir comunicar com os restantes).

# 5. Tarefa 4 – Configurações da Empresa B

Implementámos então a topologia da Empresa B, sabendo que o ISP forneceu a esta duas redes blocos de endereços IPv4/24, mas que, para efeitos de racionamento de endereçamento, a Empresa B utiliza apenas a primeira /27 de cada bloco. Temos a seguinte informação em mãos:

| Nº VLAN | Nome | IP do Gateway | Rede | PC´s |
|---|---|---|---|---|
| **20** | Servidores | 172.32.7.30 | 172.32.7.0/27 | Server1 |
| **40** | Engenharia | 172.32.8.30 | 172.32.8.0/27 | PC1,PC2 |

A Empresa B possui 1 switch, e nele efetuámos exatamente os mesmos comandos utilizados para a Empresa A. Por exemplo, de forma a permitir a VLAN 20 nele, elaborámos:

- ✓ (config)# vlan 20
- ✓ (config-vlan)# name Servidores
- ✓ (config-if)# exit

Configurámos as 3 interfaces de acesso direto aos PCs da LAN 40 e ao servidor da VLAN 20, no modo de "acesso", pois estas interfaces apenas receberão pacotes de uma mesma VLAN. Não seria necessário usar portas trunked. Por outras palavras, as interfaces Fa0/11 e Fa0/12 estão no modo de acesso apenas para a VLAN 40, enquanto a interface Fa0/10 fica no modo de acesso para a VLAN 20, exclusivamente. Se for necessário várias VLAN comunicarem através de um mesmo segmento, aí a porta do switch deverá ser trunked, contudo, por agora, não é o caso.

```
interface FastEthernet0/11
 switchport access vlan 40
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/12
 switchport access vlan 40
 switchport mode access
 switchport nonegotiate
```

*Figura 21 - Portas em modo de acesso para as VLAN da Empresa B*

Neste switch, haverá uma interface trunk (aqui será a Fa0/1), obviamente, para permitir que pacotes vindos das duas VLAN possam passar por um mesmo segmento, na direção do router. Seguidamente, figura esta configuração

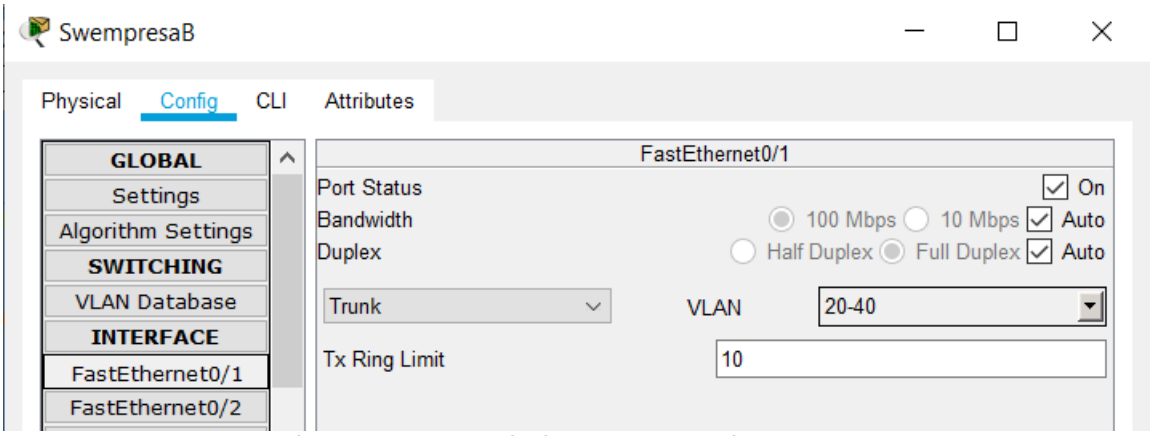


*Figura 22 - Porta trunked para as VLANs da Empresa B*

# 5.1 Testes de Conetividade

Após as configurações nos PCs 1 e 2, efetuamos o ping entre entres, obtendo resposta em ambos os sentidos

```
C:\>ping 172.32.8.2

Pinging 172.32.8.2 with 32 bytes of data:

Reply from 172.32.8.2: bytes=32 time<1ms TTL=128
Reply from 172.32.8.2: bytes=32 time<1ms TTL=128
Reply from 172.32.8.2: bytes=32 time<1ms TTL=128
Reply from 172.32.8.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.32.8.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 172.32.8.3

Pinging 172.32.8.3 with 32 bytes of data:

Reply from 172.32.8.3: bytes=32 time=1ms TTL=128
Reply from 172.32.8.3: bytes=32 time<1ms TTL=128
Reply from 172.32.8.3: bytes=32 time<1ms TTL=128
Reply from 172.32.8.3: bytes=32 time<1ms TTL=128

Ping statistics for 172.32.8.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

*Figura 23 - Pings entre os PCs da Empresa B*

# 6. Tarefa 5 – Topologia ISP

Um ISP (Internet Service Provider) consiste numa organização que fornece serviços de acesso, participação ou utilização da Internet. Na topologia deste trabalho há 2 redes /30 utilizadas por este serviço de conexão à Internet, que interligam os seus routers e o de cada empresa, A e B. As VLAN associadas a estes são:

- VLAN 90 (Empresa A): 10.20.7.0 /30
- VLAN 95 (Empresa B): 10.2.7.4 /30

De forma a implementar esta topologia, tivemos de entender quais seriam as portas a configurar como trunk ou como access. Dentro de uma mesma VLAN (90 ou 95), todas as portas estarão em modo de acesso, excetos aquelas que terão, efetivamente, um segmento de ligação à VLAN oposta. De facto, entre os multilayer switches denominados por "Swdistribution-1" e "Swdistribution-2" existe uma porta trunk, e entre os switches denominados por "Swacesso-A" e "Swacesso-B" existe outra. As restantes encontram-se em modo de acesso, para a mesma VLAN.

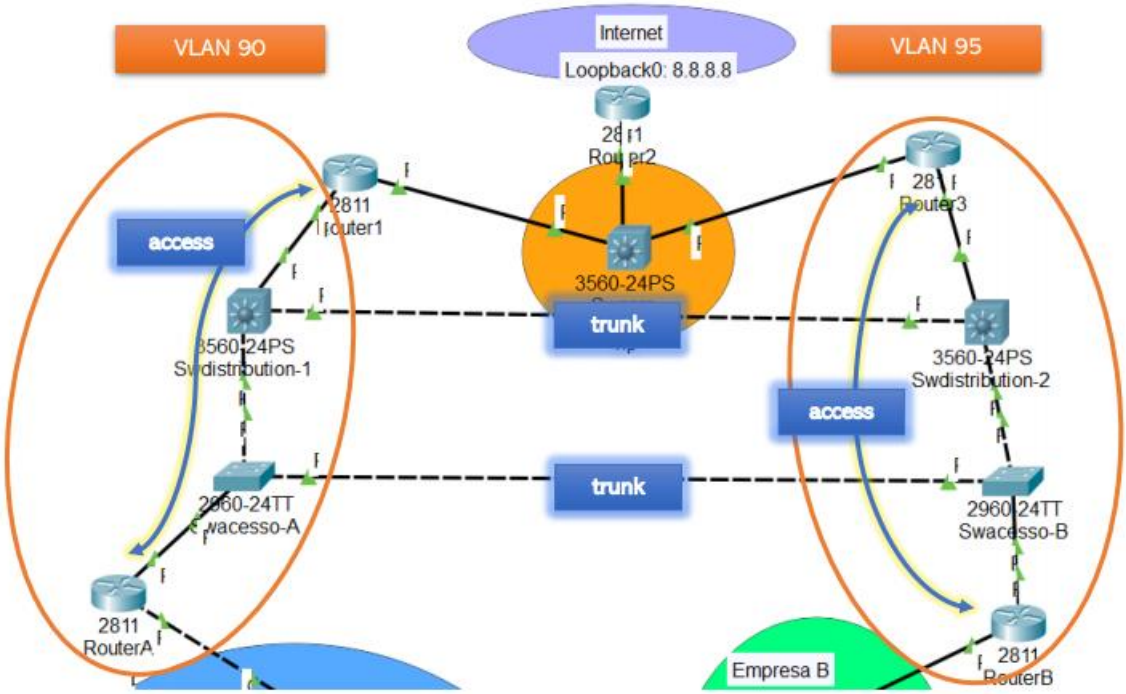


*Figura 24 - Distribuição de interfaces trunk ou access*

Sabendo então quais as portas trunk ou access, seguimos os mesmos comandos já anteriormente explicados para as configurar. Falta-nos então atribuir endereços IP ao Router1, Router3, RouterA e RouterB. Garantimos que os routers do lado do ISP possuíssem os primeiros endereços IP disponíveis na respetiva rede. A seguinte tabela dispõe os endereços atribuídos

| Router | Endereço IP | Máscara |
|---|---|---|
| **A** | 10.20.7.2 | 255.255.255.252 |
| **B** | 10.20.7.6 | 255.255.255.252 |
| **1** | 10.20.7.1 | 255.255.255.252 |
| **3** | 10.20.7.5 | 255.255.255.252 |

De forma a atribuir estes mesmos endereços, utilizámos os seguintes comandos:

- ✓ Router# configure terminal
- ✓ Router(config-if)# ip address [endereço] [máscara]
- ✓ Router(config-if)# exit

## 6.1 Testes de conetividade entre routers

Testámos então a conectividade ponto-a-ponto.

```
Router1#ping 10.20.7.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.7.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/15 ms
```

*Figura 25 - ping do Router 1 para o Router A*

```
RouterB#ping 10.20.7.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.7.5, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/8
ms
```

*Figura 26 - - ping do Router B para o Router 2*

## 6.2 Mais configurações

Começámos por ativar uma topologia em RPVST+, indo ao switch raiz e invocando o comando:

```
Swcore(config)#spanning-tree m
Swcore(config)#spanning-tree mode r
Swcore(config)#spanning-tree mode rapid-pvst
Swcore(config)#end
```

*Figura 27 - Ativação de RPVST+*

Agora, tivemos de garantir que o Swdistribution-1 é a Root Bridge primary da VLAN 90 e Root Bridge secondary da VLAN 95. O Swdistribution-2 é a RB primary da VLAN 95 e secondary da VLAN 90. Observemos os comandos que permitem isto:

```
Swdistribution-1(config)#spanning-tree vlan 90 r
Swdistribution-1(config)#spanning-tree vlan 90 root p
Swdistribution-1(config)#spanning-tree vlan 90 root primary
Swdistribution-1(config)#spanning-tree vlan 95 root sec
Swdistribution-1(config)#spanning-tree vlan 95 root secondary
```

```
Swdistribution-2(config)#spanning-tree vlan 95 root primary
Swdistribution-2(config)#spanning-tree vlan 90 root secondary
Swdistribution-2(config)#end
```

*Figura 28 - Definição das prioridades das Root Bridges*

Por fim, de modo a garantir que nos trunks da topologia de switching ISP passam apenas as VLAN necessárias, efetuamos o chamado “prune”. Do router A para o Router 1 só passa a VLAN 90, enquanto que do router B para o Router 3 passa a VLAN 95. Isto é tínhamos feito anteriormente para o router da Empresa B, ou seja, através do comando “switchport vlan access 90” ou “switchport access vlan 95”, garantimos permissão apenas para estas VLANs, no seu respetivo lado.

Uma vantagem do “pruning” consiste em economizar e aumentar a largura de banda disponível, reduzindo tráfego desnecessário, como broadcast, multicast, tráfego desconhecido e pacotes unicast inundados. O pruning bloqueia o trunk de certas redes e permite outras.

Verificámos o número de VLAN presentes na topologia, através do comando “show spanning-tree” num dos swicthes (o switch da VLAN 90). Observe-se que o tipo de STP é “Rapid-STP”.

```
Swdistribution-1#sh sp
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.C961.33DD
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.C961.33DD
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/24           Desg FWD 19        128.24   P2p

VLAN0090
  Spanning tree enabled protocol ieee
  Root ID     Priority    24666
              Address     0001.C961.33DD
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24666  (priority 24576 sys-id-ext 90)
              Address     0001.C961.33DD
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/24           Desg FWD 19        128.24   P2p

VLAN0095
  Spanning tree enabled protocol ieee
  Root ID     Priority    24671
              Address     0060.3E4E.B1E7
              Cost        19
              Port        24(FastEthernet0/24)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28767  (priority 28672 sys-id-ext 95)
              Address     0001.C961.33DD
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
```

*Figura 29 - VLANs existentes*

Observe-se ainda que, nesta parte, temos as VLAN 90 e 95, mais a que vem por default (VLAN 0001).

Através do comando “show spanning-tree summary”, conseguimos observar que além de termos 3 VLAN ativas, há 9 árvores STP ativas (3 para cada VLAN). Quanto a portas bloqueadas, a VLAN por default tem apenas 1, a VLAN 90 não tem nenhuma e a VLAN 95 possui 1 porta bloqueada. As restantes encontram-se no estado “Forwarding”. Este switch encontra-se em “Rapid-STP”.

```
Swdistribution-1#sh spanning-tree summary
Switch is in pvst mode
Root bridge for: default EmpresaA
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                      0         0        0          1          1
VLAN0090                      0         0        0          3          3
VLAN0095                      0         0        0          1          1

---------------------- -------- --------- -------- ---------- ----------
3 vlans                       0         0        0          5          5
```

*Figura 30 - Sumário das VLAN ativas*

As portas que se encontram bloqueadas estão assim devido ao RIP (Routing Information Protocol). Este consiste num padrão para a troca de informações entre gateways e hosts de roteamento. Por outras palavras, o RIP emite mensagens de atualizações de rotas (tabelas de encaminhamento) em intervalos regulares, e quando a topologia muda.

# 7. Tarefa 6 – Roteamento Estático

Neste ponto, configurámos os routers das empresas A e B com rotas estáticas default, assim como os Routers 1 e 3. O objetivo disto é construir manualmente a tabela de encaminhamento e facilitar a entrega de pacotes para um dado destino. De forma a enviar pacotes de rede em rede, se cada router já souber a interface que terá de usar para enviar a um dado destino, a entrega será imediata.

Além disso, as rotas estáticas não são enunciadas na rede, resultado numa maior segurança. Usam também menos largura de banda do que os protocolos de roteamento dinâmico, pois nenhum ciclo de CPU é usado para calcular e comunicar rotas. Também são um modo de criar rotas alternativas, caso ocorram falhas no segmento da rota primária.

As rotas estáticas são úteis para redes de reduzida dimensão, com apenas um caminho para uma rede externa, onde o cenário de rede não é complexo e raramente sofre alterações. O administrador da rede é o responsável pelas rotas que introduz manualmente na tabela de encaminhamento do router, tendo como base o seu conhecimento de toda a infraestrutura da rede de dados. As rotas estáticas têm prioridade sob as rotas que resultam dos protocolos de encaminhamento dinâmico, uma vez que têm uma distância administrativa menor. Visto que as rotas são estáticas, definidas manualmente, estas não se adaptam automaticamente no caso de alterações da rede. Também fornecem segurança em redes maiores para determinados tipos de tráfego ou em links para outras redes que precisam de mais controlo.

Posto isto, é necessário entender que roteamento estático e dinâmico não são mutuamente exclusivos, isto é, a maioria das redes utiliza uma combinação de protocolos de roteamento dinâmico e rotas estáticas. Usámos o seguinte comando para definir, então, os vários caminhos no router:

✓ Router(config)# ip route [endereço origem] [máscara] [endereço destino]

Agora que configurámos endereços estaticamente nos routers, vejamos um exemplo prático: se um PC da Empresa B quiser enviar um pacote para um PC da Empresa A, este passa pelo Router B e percorre os segmentos (não trunked) que estão em modo de acesso para toda a VLAN 95. Da VLAN 95 para a VLAN 90, o pacote passa no multilayer switch central. Deste switch o pacote segue para o Router 1, que agora já sabe, pela sua tabela de encaminhamento configurada com alguns endereços estáticos, que deve enviar o pacote para a interface Fa0/0 do Router A. Aqui, o Router A irá encaminhá-lo para a Empresa A diretamente.

É importante notar que é graças ao RIP que ambas as LANs 90 e 95 conseguem comunicar. O router 2, o central, implementa RIP, através dos seguintes comandos:

- ✓ router rip
- ✓ version 2
- ✓ network 10.0.0.0
- ✓ redistribute static
- ✓ no auto-summary (indica que o protocolo é classless)
- ✓ exit

Portanto, se estivermos numa das empresas, o “next-hop” da rota é o router ao qual o pacote segue, assim que sai do respetivo router da empresa. Saindo da Empresa A (Router A), o “next-hop” é o Router 1, e saindo da empresa B é o Router 3. Através do roteamento estático, estes routers “exteriores” às empresas conhecem as suas rotas, conseguem comunicar e, portanto, toda a rede está interligada.

Invocando o comando “show ip route” nos vários routers, conseguimos observar quais foram os endereços IP colocados estaticamente em cada um.

```
Gateway of last resort is 10.20.7.1 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 1 subnets
C       10.20.7.0 is directly connected, FastEthernet0/0
C    192.168.238.0/24 is directly connected, FastEthernet0/1.80
C    192.168.239.0/24 is directly connected, FastEthernet0/1.90
     192.168.240.0/25 is subnetted, 2 subnets
C       192.168.240.0 is directly connected, FastEthernet0/1.100
C       192.168.240.128 is directly connected, FastEthernet0/1.105
S*   0.0.0.0/0 [1/0] via 10.20.7.1
```

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.0.0/26 is directly connected, FastEthernet0/0
C       10.20.7.0/30 is directly connected, FastEthernet1/0
     192.168.238.0/30 is subnetted, 1 subnets
S       192.168.238.0 [1/0] via 10.20.7.2
     192.168.239.0/30 is subnetted, 1 subnets
S       192.168.239.0 [1/0] via 10.20.7.2
     192.168.240.0/30 is subnetted, 1 subnets
S       192.168.240.0 [1/0] via 10.20.7.2
```

```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.0.0/26 is directly connected, FastEthernet0/0
C       10.20.7.4/30 is directly connected, FastEthernet1/0
     172.32.0.0/27 is subnetted, 2 subnets
S       172.32.7.0 [1/0] via 10.20.7.6
S       172.32.8.0 [1/0] via 10.20.7.6
```

```
Gateway of last resort is 10.20.7.5 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 1 subnets
C       10.20.7.4 is directly connected, FastEthernet0/0
     172.32.0.0/27 is subnetted, 2 subnets
C       172.32.7.0 is directly connected, FastEthernet0/1.20
C       172.32.8.0 is directly connected, FastEthernet0/1.40
S*   0.0.0.0/0 [1/0] via 10.20.7.5
```

*Figura 31 - Endereços conhecidos por cada router*

Note-se que em cada uma das imagens acima, os endereços escritos a seguir a “S” ou “S*” foram definidos estaticamente.

# 8.Tarefa 7 – Rip e conetividade à Internet

Como já foi mencionado, o RIP consiste num serviço provedor de acesso à Internet. O objetivo neste ponto é garantir conexão entre os PCs das VLAN e a Internet. Adicionámos os equipamentos SWcore e Router2 à topologia e as respetivas ligações ditas no enunciado, atribuindo um IP ao router, através de comandos já analisados. Atribuímos a rede 10.0.0.0 /26 ao core do ISP, configurando as interfaces de cada router. Usámos os comandos:

- ✓ router rip
- ✓ version 2
- ✓ network 10.0.0.0
- ✓ redistribute static
- ✓ no auto-summary (indica que o protocolo é classless)
- ✓ exit

Configurámos a interface loopback0 no Router2 com o IP 8.8.8.8/32, da seguinte forma:

- ✓ Router(config)# interface loopback 0
- ✓ Router(config-if)# ip address 8.8.8.8 255.255.255.255
- ✓ Router(config-ig)# end
- ✓ Router# show interfaces loopback 0 (para confirmar)

Não é necessário colocar a rede 8.8.8.8/32 no RIP, pois os switches só efetuam switching (incluindo o multilayer switch Swcore).
A rota default é propagada através do RIP, do Router2 aos Router1 e 3. Para se alcançar a Internet, deve sempre haver uma rota por default.
De forma a confirmar a realização de todos os requisitos, efetuámos o "traceroute" na interface loopback, no router A.

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time<1ms TTL=253
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253
Reply from 8.8.8.8: bytes=32 time<1ms TTL=253

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.32.7.2

Pinging 172.32.7.2 with 32 bytes of data:

Request timed out.
Reply from 172.32.7.2: bytes=32 time=1ms TTL=124
Reply from 172.32.7.2: bytes=32 time<1ms TTL=124
Reply from 172.32.7.2: bytes=32 time<1ms TTL=124

Ping statistics for 172.32.7.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

*Figura 32 - Ping e traceroute do Server2 para a Internet*

```
Pinging 172.32.7.2 with 32 bytes of data:

Request timed out.
Reply from 172.32.7.2: bytes=32 time=1ms TTL=124
Reply from 172.32.7.2: bytes=32 time<1ms TTL=124
Reply from 172.32.7.2: bytes=32 time<1ms TTL=124

Ping statistics for 172.32.7.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

*Figura 33 - Ping do Server 2 para o Server1*

# 9. Conclusões

Para concluir, apresentamos uma tabela que serve de sumário a todas as configurações nos dispositivos desta topologia trabalhada (computadores, routers e servidores…), contendo endereços IP, máscaras e gateways. Efetivamente, todas as configurações resultaram numa topologia distribuída da seguinte maneira:

Este trabalho permitiu-nos familiarizar com vários comandos para configurações em dispositivos terminais ou não, e construção de uma ou mais redes conectadas. O conceito de VLAN, STP ou RSTP, Telnet, ISP, RIP tornaram-se mais claros e aprendemos a lidar com eles através desta simulação de um cenário real. Pensamos ter ficado mais confortáveis neste tipo de projeto, e solidificámos então as bases com estes conhecimentos um pouco mais avançados para manipular routers, switches, etc.

Fazendo um balanço deste trabalho, pensamos ter conseguido atringir todos os requisitos, tendo comprovado as conexões entre dispositivos com o comando “ping”, assim como a inexistência de conexão entre alguns deles, de acordo as especificações do enunciado. No final, o resultado foi esta rede, com certas VLAN de empresas distintas, que comunicam umas com as outras (se tiverem de comunicar), através de segmentos trunked.

# 10. Bibliografia


- ✓ https://www.omnisecu.com/cisco-certified-network-associate-ccna/how-to-change-spanning-tree-bridge-root-priority-value-and-what-is-extended-system-id.php
- ✓ https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/RPVSpanningTree.html
- ✓ https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10100-priorityvsbw.html
- ✓ https://community.cisco.com/t5/other-network-architecture/howto-save-running-config-file-from-cli/td-p/362191
- ✓ https://pt.wikipedia.org/wiki/Routing_Information_Protocol
- ✓ https://pt.slideshare.net/felipecesarcosta58/protocolo-vtp
- ✓ https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/rip-default-route