

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**

[1. Introdução e Objetivos 5](#_Toc57487405)

[2. Tarefa 1 – Pequenas configurações na EmpresaA 6](#_Toc57487406)

[3. Tarefa 2 – Configurações fixas para a EmpresaA 11](#_Toc57487407)

[4. Tarefa 2 – Configurações no Router A 15](#_Toc57487408)

[5. Tarefa 4 – Configurações da Empresa B 18](#_Toc57487409)

[6. Tarefa 5 – Topologia ISP 21](#_Toc57487410)

[7. Tarefa 6 – Roteamento Estático 26](#_Toc57487411)

[8. Tarefa 7 – Rip e conetividade à Internet 28](#_Toc57487412)

[9. Conclusões 30](#_Toc57487413)

[10. Bibliografia 31](#_Toc57487414)

**Índice de Figuras**

[Figura 1 - comando no ip domain-lookup usado 6](#_Toc57487276)

[Figura 2 - VLANS por omissão 6](file:///C:\Users\luisc\Desktop\Faculdade\Disciplinas\RI\Trabalhos\20_21\Tp1\RI_TP1_GRUPO7.docx#_Toc57487277)

[Figura 3 - comando usado para alterar a prioridade deste switch 9](#_Toc57487278)

[Figura 4 - comando de ativação do Per-VLAN spanning tree 9](#_Toc57487279)

[Figura 5 - Bloqueio de ligação entre Switches 10](#_Toc57487280)

[Figura 6 - Nova ligação entre o Switch1\_piso1 e Switch1\_piso2 10](file:///C:\Users\luisc\Desktop\Faculdade\Disciplinas\RI\Trabalhos\20_21\Tp1\RI_TP1_GRUPO7.docx#_Toc57487281)

[Figura 7 - cálculo do parâmetro X 11](#_Toc57487282)

[Figura 8 - comandos da criação das vlans 12](#_Toc57487283)

[Figura 9 - Novas VLANs criadas 12](#_Toc57487284)

[Figura 10 - porta configurada como trunk 12](file:///C:\Users\luisc\Desktop\Faculdade\Disciplinas\RI\Trabalhos\20_21\Tp1\RI_TP1_GRUPO7.docx#_Toc57487285)

[Figura 11 - porta configurada como access 12](file:///C:\Users\luisc\Desktop\Faculdade\Disciplinas\RI\Trabalhos\20_21\Tp1\RI_TP1_GRUPO7.docx#_Toc57487286)

[Figura 12 - Verificação da desativação do DTP nas interfaces 13](#_Toc57487287)

[Figura 13 - Definição do Gateway,IP e máscara para o PC5 13](#_Toc57487288)

[Figura 14 - Ping do PC7 para o PC9 14](#_Toc57487289)

[Figura 15 - Ping do PC5 para o PC8 14](#_Toc57487290)

[Figura 16 - Subnets para as VLAN no Router A 15](#_Toc57487291)

[Figura 17 VLAN em modo trunk numa interface 16](#_Toc57487292)

[Figura 18 - Desativação do DNS lookup 17](#_Toc57487293)

[Figura 19 - Mensagem inicial de entrada no equipamento 17](#_Toc57487294)

[Figura 20 - ping PC5 para o PC7 17](#_Toc57487295)

[Figura 21 - Portas em modo de acesso para as VLAN da Empresa B 18](#_Toc57487296)

[Figura 22 - Porta trunked para as VLANs da Empresa B 19](#_Toc57487297)

[Figura 23 - Pings entre os PCs da Empresa B 19](#_Toc57487298)

[Figura 24 - Distribuição de interfaces trunk ou access 21](#_Toc57487299)

[Figura 25 - ping do Router 1 para o Router A 22](#_Toc57487300)

[Figura 26 - - ping do Router B para o Router 2 22](#_Toc57487301)

[Figura 27 - Ativação de RPVST+ 23](#_Toc57487302)

[Figura 28 - Definição das prioridades das Root Bridges 23](#_Toc57487303)

[Figura 29 - VLANs existentes 24](#_Toc57487304)

[Figura 30 - Sumário das VLAN ativas 25](#_Toc57487305)

[Figura 31 - Endereços conhecidos por cada router 27](#_Toc57487306)

[Figura 32 - Ping e traceroute do Server2 para a Internet 28](#_Toc57487307)

[Figura 33 - Ping do Server 2 para o Server1 **Erro! Marcador não definido.**](#_Toc57487308)

# 

# 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.

# Tarefa 1 – Pequenas configurações na EmpresaA

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

##### 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:

##### 

Figura 1 - comando no ip domain-lookup usado

##### 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.

##### 

Figura 2 - VLANS por omissão

##### 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.

##### 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.

##### 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.

##### 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”)

##### 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 | - | - | - | - | - |

1. **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

1. **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

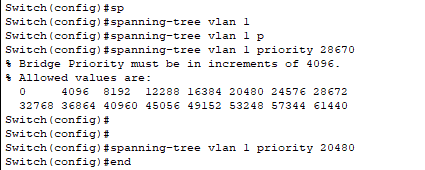


Figura 3 - comando usado para alterar a prioridade deste switch

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

1. **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

1. **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:

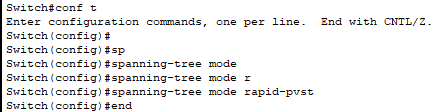


Figura 4 - comando de ativação do Per-VLAN spanning tree

1. **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)

1. **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:

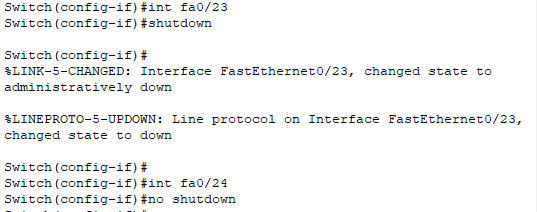
****

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

1. **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.

1. **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.

# 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:

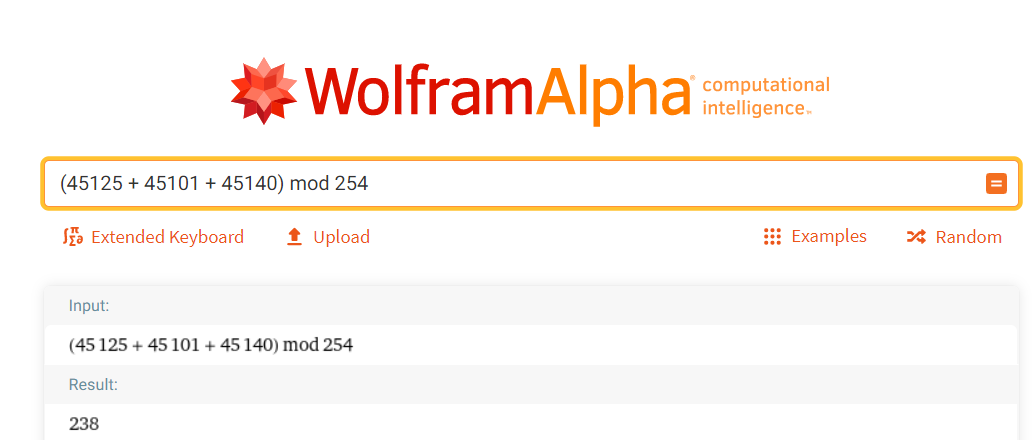


Figura 7 - cálculo do parâmetro X

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).

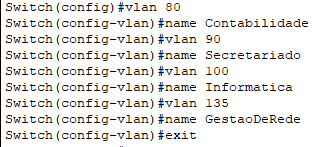


Figura 8 - comandos da criação das vlans

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

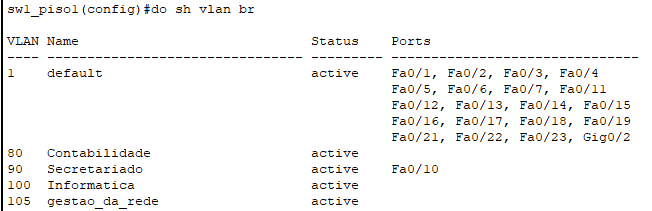


Figura 9 - Novas VLANs criadas

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:

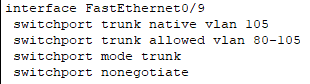


Figura 10 - porta configurada como trunk

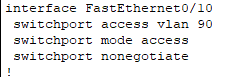


Figura 11 - porta configurada como access

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:

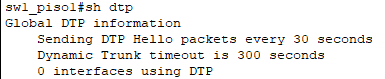


Figura 12 - Verificação da desativação do DTP nas interfaces

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.

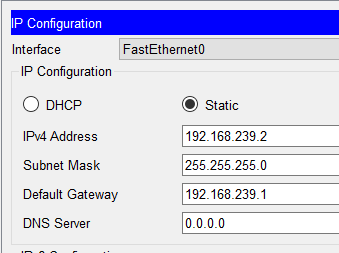


Figura 13 - Definição do Gateway,IP e máscara para o PC5

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.

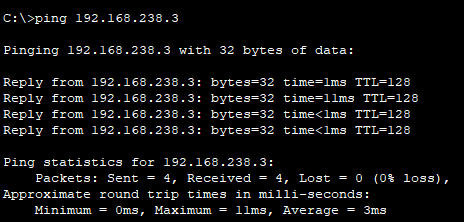


Figura 14 - Ping do PC7 para o PC9

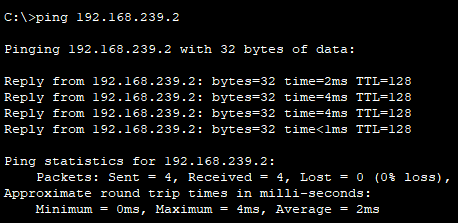


Figura 15 - Ping do PC5 para o PC8

# 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.

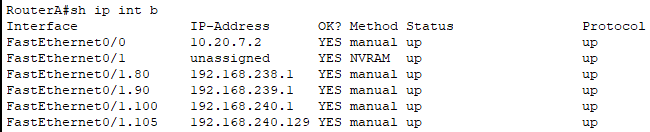


Figura 16 - Subnets para as VLAN no Router A

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.

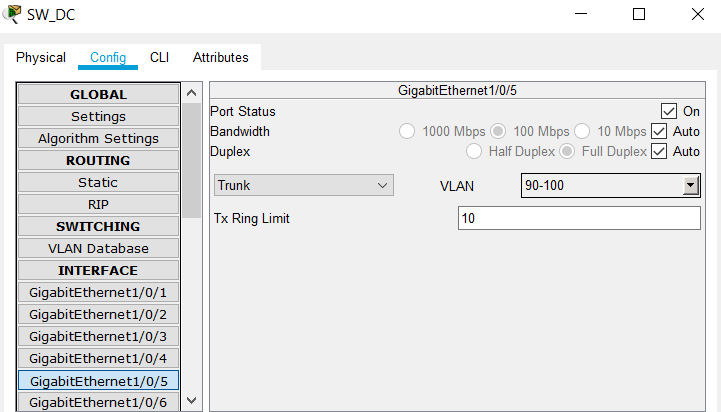


Figura 17 VLAN em modo trunk numa interface

´

**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.

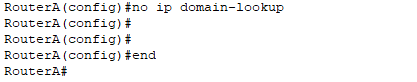


Figura 18 - Desativação do DNS lookup

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

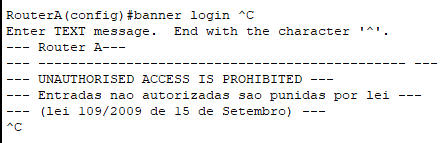


Figura 19 - Mensagem inicial de entrada no equipamento

**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.

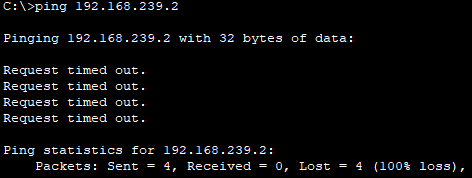


Figura 20 - ping PC5 para o PC7

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).

# 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.

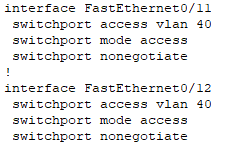


Figura 21 - Portas em modo de acesso para as VLAN da Empresa B

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

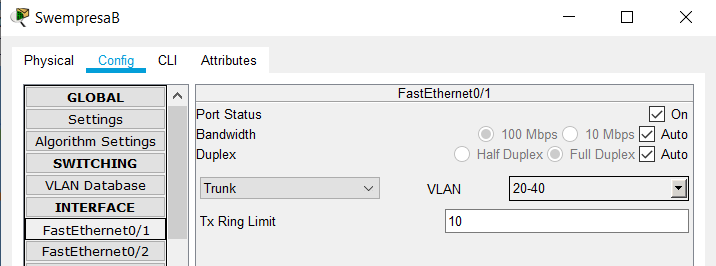
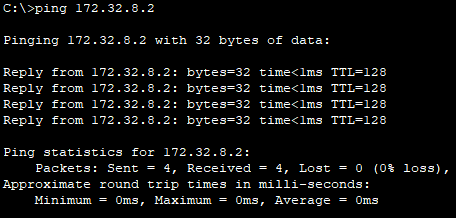


Figura 22 - Porta trunked para as VLANs da Empresa B

**5.1 Testes de Conetividade**

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



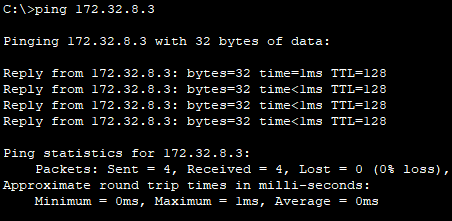


Figura 23 - Pings entre os PCs da Empresa B

# 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.

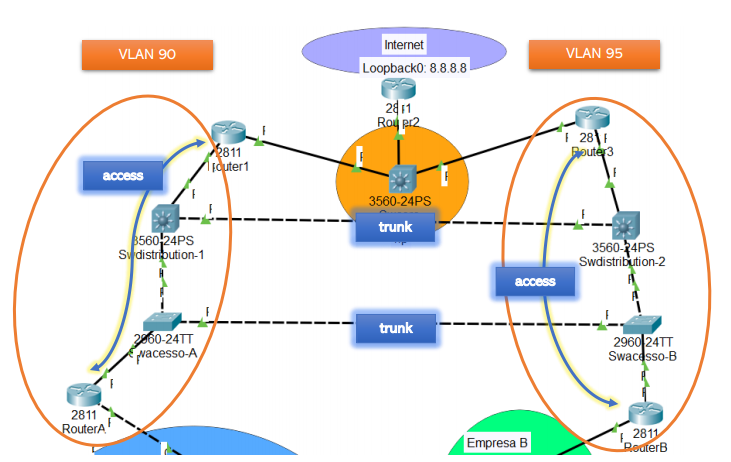


Figura 24 - Distribuição de interfaces trunk ou access

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.

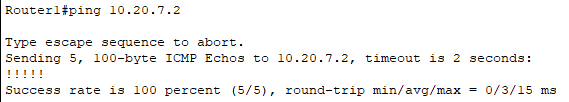


Figura 25 - ping do Router 1 para o Router A

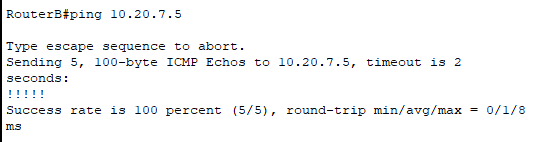


Figura 26 - - ping do Router B para o Router 2

**6.2 Mais configurações**

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

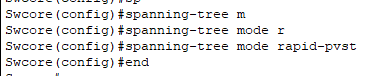


Figura 27 - Ativação de RPVST+

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:

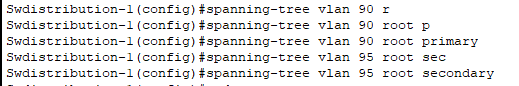




Figura 28 - Definição das prioridades das Root Bridges

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”.

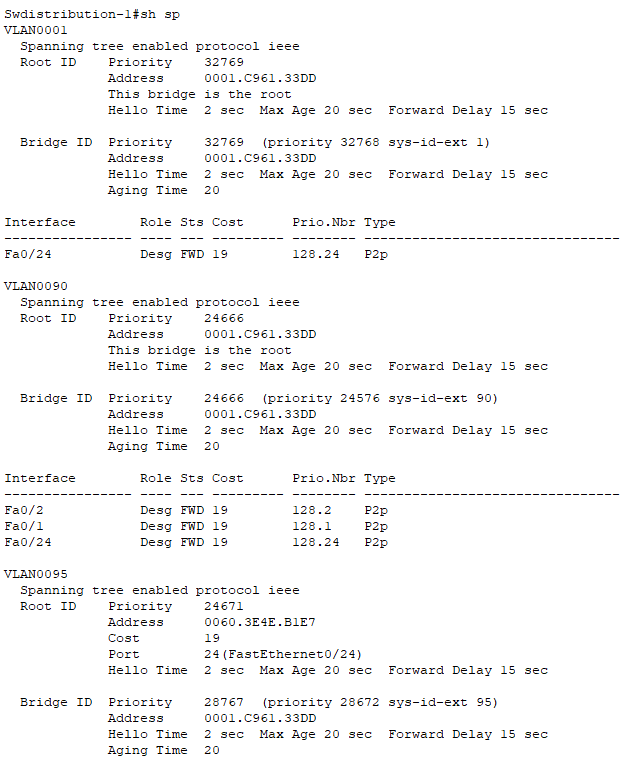


Figura 29 - VLANs existentes

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”.

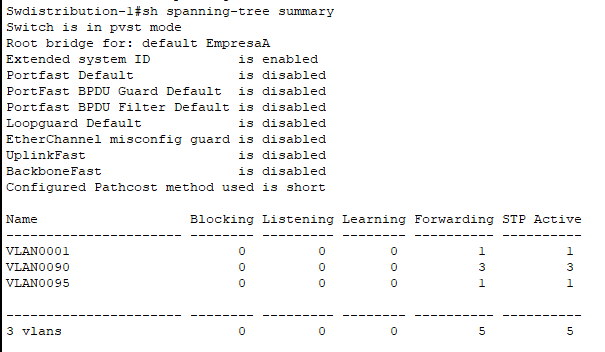


Figura 30 - Sumário das VLAN ativas

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.

# 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]

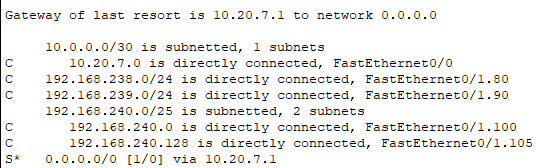
Agora que configurámos endereços estaticamente nos routers, vejamos um exemplo prático: se um PC da Empresa B quiser enviar um pacote para um PC da Empresa A, este passa pelo Router B e percorre os segmentos (não trunked) que estão em modo de acesso para toda a VLAN 95. Da VLAN 95 para a VLAN 90, o pacote 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.

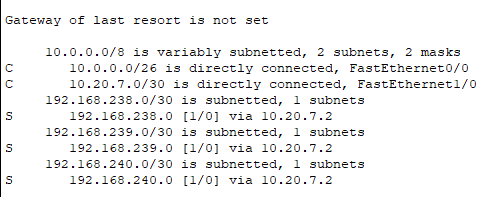
É importante notar que é graças ao RIP que ambas as LANs 90 e 95 conseguem comunicar. O router 2, o central, implementa RIP, através dos seguintes comandos:

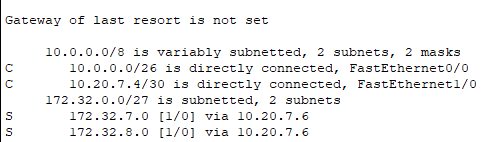
* router rip
* version 2
* network 10.0.0.0
* redistribute static
* no auto-summary (indica que o protocolo é classless)
* exit

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.







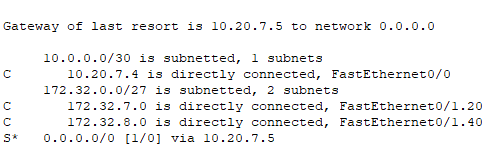


Figura 31 - Endereços conhecidos por cada router

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

# 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.

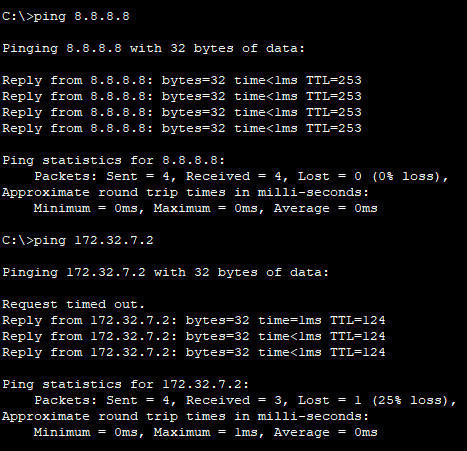


Figura 32 - Ping e traceroute do Server2 para a Internet

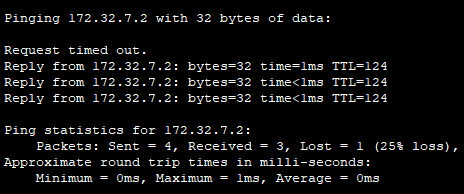


Figura 33 - Ping do Server 2 para o Server1

# 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.

# 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>