

Instituto Politécnico de Lisboa (IPL)

Instituto Superior de Engenharia de Lisboa (ISEL)

Área Departamental de Engenharia da
Eletrónica e Telecomunicações e de Computadores(ADEETC)
LEETC, LEIC, LEIM, LEIRT, MEIC

Redes de Internet (RI) – Trabalho nº 1 (VLANs/STP/RIP)

Inverno de 2018/2019 - Data limite de entrega: **Ver Moodle**

Este trabalho tem como objetivo o aprofundamento dos conhecimentos sobre VLANs e os protocolos STP e RIP.

O trabalho prático é de execução por grupos de até 3 alunos, podendo na aula prática de realização do trabalho, ou parte, existir avaliação do grupo e/ou individual sobre a realização do mesmo e o tema que envolve.

Este trabalho, tal como os seguintes, é considerado pedagogicamente fundamental (“[NORMAS DE AVALIAÇÃO DE CONHECIMENTOS](#)”, Conselho Pedagógico do ISEL, ponto 2.3.1).

É assumido que os alunos sabem utilizar convenientemente os comandos de configuração dos equipamentos, incluindo os de *show* e *debug*, para validar o seu trabalho e resolver os desafios que lhes vão aparecendo.

O docente decidirá conforme os relatórios entregues e as notas individuais se fará, e com que grupos fará, a discussão final dos trabalhos.

O simulador de redes utilizado neste trabalho será o Packet Tracer.

O relatório deve incluir na identificação, para além do número do grupo e dos alunos, os respetivos nomes e o curso. Deve incluir em anexo, os ficheiros de configuração das várias fases do simulador e a justificação das escolhas efetuadas. No ato da entrega do relatório, **não esquecer** que deverá também ser disponibilizado o ficheiro **.pkt**

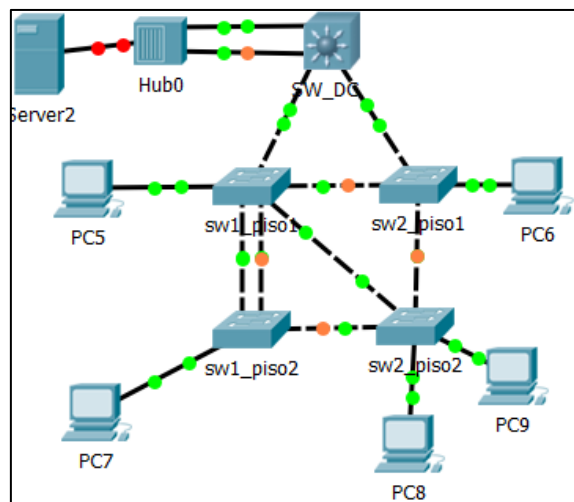
Nota: Ler TODO o enunciado antes de se começar a configurar os equipamentos!

Introdução

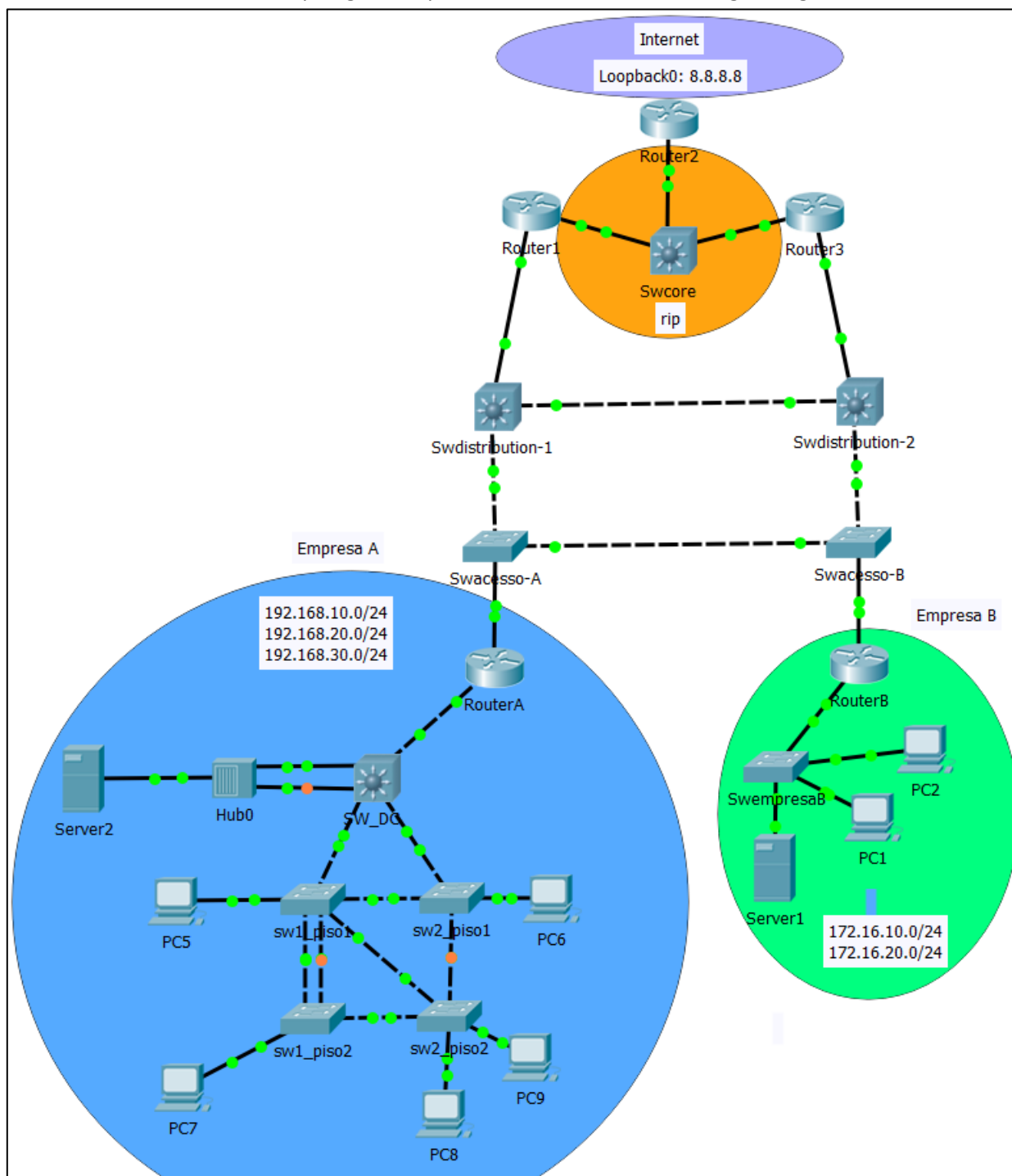
Este trabalho tem como objetivo familiarizar os alunos com a temática das VLANs, com o protocolo de proteção contra *loops* na camada 2 (STP), encaminhamento estático e com o protocolo de encaminhamento dinâmico RIP.

Objetivo

Numa fase inicial, será fornecido um ficheiro de Packet Tracer com a topologia abaixo descrita. Nesta os alunos reforçarão numa primeira fase os seus conhecimentos de Spanning-Tree (STP) e posteriormente sobre VLANs.



Numa segunda fase será pedido para os alunos expandirem a topologia fornecida, passo a passo, aumentando progressivamente a dificuldade. A topologia final pretendida encontra-se na imagem seguinte:



Esta topologia representa a infraestrutura de um *Internet Service Provider* (ISP) que fornece conetividade/trânsito a duas empresas. Este ISP coloca equipamentos nas instalações de cada empresa que servem como um *Network Demarcation Device* (NDD).

O ISP atribuiu diversas redes (blocos de endereços) a cada empresa para uso interno destas. As empresas possuem vários departamentos e como tal necessitam de possuir a sua rede segmentada, o *gateway* de cada rede é sempre o *router* de cada empresa. O ISP utiliza ainda duas redes /30 (P2P em layer3) de interligação entre os seus *routers* e o de cada empresa.

Cada empresa possui uma rota estática *default* a apontar para o *router* do ISP. Este por sua vez, anuncia de forma estática as redes que atribuiu às empresas.

É utilizado o protocolo RIP 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*).

Tarefas

1) Importe o ficheiro com a topologia base e responda às seguintes questões:

- Qual o tipo de Spanning-Tree (STP) ativo?
- Quantas árvores existem?
- Qual a *root bridge* (RB)? Justifique.
- Qual o custo do caminho mais curto até à RB do sw2_piso2?
- Force a RB no SW_DC através da prioridade. Possui alguma porta bloqueada? Justifique.
- Ative o RPVST+, é necessário ativar em todos os *switches*? Justifique.
- Quantas árvores passaram a existir?
- Existem duas ligações entre o sw1_piso1 e o sw1_piso2, uma delas cortada, explique o processo que está na origem do corte num *link* e não do outro.
- Explique de forma detalhada a razão do sw2_piso2 preferir o caminho pelo sw1_piso1. Realize as alterações que achar necessárias para que o caminho preferido seja pelo sw2_piso1.

2) Segmente a rede com as informações abaixo:

Nº Vlan	Nome	IP do Gateway	Rede	PCs
10	Contabilidade	192.168.10.1	192.168.10.0/24	PC5,PC8
20	Secretariado	192.168.20.1	192.168.20.0/24	PC6,PC7,PC9
30	Informática	192.168.30.1	192.168.30.0/24	Server2
50	Gestão	192.168.50.1	192.168.50.1/24	

- Crie as VLANs com o respetivo nome em todos os *switches*.
 - Configure as portas em modo *access* ou *trunk* dependendo das necessidades. Desligue o protocolo Dynamic Trunking Protocol (DTP) em cada interface que configurar como *access* ou *trunk*.
 - Configure o endereçamento de todos os PCs. Verifique se existe conetividade entre os PCs da mesma VLAN.
- 3) Adicione o RouterA à topologia ligado ao SW_DC. Configurar o RouterA e SW_DC com os seguintes parâmetros de forma a este ficar com as configurações consideradas “*best practises*”:
- Ativar o modelo AAA e definir que a autenticação é local:
RouterN (config)# aaa new-model
RouterN (config)# aaa authentication login default local
 - Configurar um *username* e *secret* bem como proteger o modo de *enable* da forma mais segura possível. (Se não usar *password/secret* de nível 5, garanta que pelo menos o serviço de encriptação de *passwords* está ativo - *service password-encryption*)
Nota: Como usernames e passwords, use sempre “cisco”.
 - Ativar o procolo SSH
RouterN (config)# ip domain name xx.pt
RouterN (config)# crypto key generate rsa
RouterN (config)# ip ssh time-out 60
RouterN (config)# ip ssh version 2
 - Garanta que o *router* não tenta resolver nomes via DNS cada vez que se enganar, desative o DNS *lookup*:

RouterN (config)# no ip domain-lookup

- e) Configure uma mensagem inicial para quem entra no equipamento:

RouterN (config)# banner login ^C

```
--- Router N ---
---
--- UNAUTHORISED ACCESS IS PROHIBITED ---
--- Entradas nao autorizadas sao punidas por lei ---
--- (lei 109/2009 de 15 de Setembro) ---
^C
```

- f) Configure de forma correta as *lines* de consola e *vty*, para garantir que o *router* não interrompe com mensagens de *debug* e outras a introdução de comandos através do CLI (*logging synchronous*); o tempo de uma sessão seja no máximo 30 minutos (*exec-timeout 30 0*); o acesso por *telnet* não é permitido, apenas por SSH (*transport input ssh*); é escolhido o tamanho máximo do *buffer* para os comandos introduzidos na CLI (*history size 256*). Nota importante: Ainda faltava configurar nas *lines vty access-control-lists* que permitissem o acesso a estas apenas a partir de determinadas redes, mas este tipo de conteúdo será lecionado em TAR.

- g) Configurar e ativar as *interfaces* utilizadas. Exemplo: (Tenha em atenção que quando usa *subinterfaces* a interface física não possui configuração de IP)

RouterN(config)# interface Fa0/1

RouterN(config-if)# ip address xxx.yyy.zzz.www mmm.mmm.mmm.mmm

RouterN(config-if)# description [Fa0/1] Link to SWY G1/0/5

RouterN(config-if)# no ip redirects

RouterN(config-if)# no ip directed-broadcast

RouterN(config-if)# no ip proxy-arp

RouterN(config-if)# no shutdown

- h) Salve as configurações no *router*:

RouterN# copy running-config startup-config ou apenas *RouterN# write*

- i) Verifique a conectividade entre PCs entre diferentes VLANs utilizando o *ping*. Caso tenha problemas, faça o *troubleshooting* para verificar se o problema está na *vlan/rede* (possível causa nos *switches/vlans* não criadas/passadas; portas em *access/trunks* ou a própria configuração dos PCs/endereço/máscara do PC/GW)) execute um *ping* ao seu GW ou utilize um *traceroute* para verificar em que “hop” está o problema. Se estiver a tentar “pingar” o PC7 do PC5 e se cada PC possuir conectividade com o seu GW, então o problema estará de certeza no *router*. Pode usar comandos como:

<i>show arp</i>	: Shows the Address Resolution Protocol
<i>show mac-address-table</i>	: Shows the MAC Address Table
<i>traceroute <ip address></i>	: Execute a traceroute to a destination ip
<i>show interface <interface> <number></i>	: Interface status and configuration
<i>show ip interface brief</i>	: Brief summary of IP interface status and configuration

- 4) **(Opcional)** Realize as configurações necessárias para que seja possível aceder por SSH/Gestão ao SW_DC. Teste o acesso.

Nota: O auxilio do seu docente deverá ser mínimo

- 5) Implemente a topologia da EmpresaB, sabendo que o ISP forneceu a esta duas redes /24, mas que para efeitos de racionamento de endereçamento, a EmpresaB utiliza apenas a primeira /27 de cada uma.

Nº Vlan	Nome	IP do Gateway	Rede	PCs
10	Servidores	172.16.10.30	172.16.10.0/27	Server1
20	Engenharia	172.16.20.30	172.16.20.0/27	PC1,PC2

6) Implemente a topologia do ISP:

- a) O ISP utiliza duas redes /30 (P2P em *layer3*) de interligação entre os seus *routers* e o de cada empresa. As redes e respectivas VLANs são:
- i) Vlan 91 (EmpresaA) -> 110.110.1.0/30
 - ii) Vlan 92 (EmpresaB) -> 110.110.1.4/30

Construa os caminhos das VLANs na malha de *switches* (configurando as interfaces em *trunk* ou *access* quando necessário), sabendo que para efeitos de redundância de camada 2, o ISP construiu um circuito entre as duas empresas, logo este é para ser usado.

- b) Atribua o endereçamento ao Router1, Router3, RouterA e RouterB, sabendo que os *routers* do ISP possuem sempre o primeiro endereço disponível da respetiva rede. Teste a conectividade ponto a ponto (R1->RA e R3->RB).

c) Configure no ISP:

- i) O tipo de STP usado no ISP é o RPVST+.
- ii) O Swdistribution-1 é a RB *primary* da *vlan* 91 e RB *secondary* da *vlan* 92.
- iii) O Swdistribution-2 é a RB *primary* da *vlan* 92 e *secondary* da *vlan* 91.
- iv) Face “prune” nos *trunks* da topologia de *switching* do ISP para que apenas passem nos *trunks* as VLANs necessárias/utilizadas. Qual a vantagem/objetivo?
- v) Quantas árvores de STP estão presentes?
- vi) Indique as portas bloqueadas da *vlan* 91 e 92. Justifique o bloqueio nestas portas.

7) Configurar o *routing* estático. No final deste ponto, os PCs da EmpresaA devem conseguir pingar o Router1 e os PCs da EmpresaB devem conseguir pingar o Router3.

- a) Configure nos *routers* das empresas rotas estáticas *default*. Qual o “next-hop” destas rotas? Qual o objetivo?
- b) Neste momento os PCs das empresas já conseguem “pingar” o seu respetivo *router* do ISP? Justifique.
- c) Configure as rotas estáticas que entender necessárias no R1 e R3 para que exista conectividade entre estes e as redes atribuídas a cada empresa. Qual o objetivo desta configuração?

8) Implementação do RIP e conectividade global à Internet: No final deste ponto deve existir conectividade entre os PCs das empresas e das empresas com a Internet.

- a) Adicione os equipamentos Swcore e Router2 à topologia e as respetivas ligações como indica a figura.
- b) Foi atribuída a rede 130.50.0.0/27 ao core do ISP. Configure as *interfaces* de cada *router* tendo presente que o último octeto possui o nº do *router*.
- c) É necessário efetuar alguma configuração do Swcore? Porquê?
- d) Configure o RIP no *core* do ISP com os seguintes objetivos:
 - i) Pretende-se que seja *classless* e que utilize a versão 2.
 - ii) Que forme vizinhos apenas nas *interfaces* viradas para o *core*.
 - iii) Necessita de colocar o R1 e R3 a anunciar para os seus vizinhos que participam no RIP as rotas estáticas que possuam.
 - iv) O R2 propaga automaticamente a rota *default* através do RIP para o R1 e R3.
 - v) Configure a *interface* loopback0 no R2 com o ip 8.8.8.8/32, simulando desta forma a Internet.
 - vi) É necessário colocar a rede 8.8.8.8/32 no RIP? Porquê?
 - vii) O trabalho está completo quando existir conectividade global.

Bibliografia

Documentos de apoio da unidade curricular e material fornecido pelo seu docente