RS – Resumos das práticas

P01

ifconfig → comando para configurar uma interface de rede

route → mostra / manipula a tabela de roteamento IP
route -n → mostra endereços numéricos, sem tentar resolver os nomes simbólicos das máquinas

cat *etc*/resolv.conf → contem a listagem dos servidores de DNS (nameserver) e o comando cat lista o conteúdo do ficheiro

Para saber o endereço IP através dos nomes das máquinas/servidores basta fazer >> host (domain name):

host www.ua.pt →
"www.ua.pt has address 193.136.173.58"
DNS (Domain Name System) Lookup

Contudo, dá para fazer o inverso com o mesmo comando:

host 193.136.173.58 →
"58.173.136.193.in-addr.arpa domain name pointer www.ua.pt."
Reverse DNS Lookup

Para acessar a um site através do browser, basta inserir o nome do servidor (ex: www.ua.pt). No entanto, também podemos introduzir o respetivo endereço de IP na barra de pesquisa para poder entrar no website.

```
ricardo@ricardo-Legion-Y540-15IRH-PG0:~$ ping www.ua.pt
PING lvs-ng.ua.pt (193.136.173.58) 56(84) bytes of data.
64 bytes from lvs-ng.ua.pt (193.136.173.58): icmp_seq=1 ttl=52 time=15.2 ms
64 bytes from lvs-ng.ua.pt (193.136.173.58): icmp_seq=2 ttl=52 time=16.1 ms
64 bytes from lvs-ng.ua.pt (193.136.173.58): icmp_seq=3 ttl=52 time=14.9 ms
64 bytes from lvs-ng.ua.pt (193.136.173.58): icmp_seq=4 ttl=52 time=14.9 ms
64 bytes from lvs-ng.ua.pt (193.136.173.58): icmp_seq=5 ttl=52 time=18.3 ms
^C
--- lvs-ng.ua.pt ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 14.904/15.909/18.358/1.314 ms
```

icmp_seq → número do ICMP
ttl → "time to leave": número de salto entre máquinas que os pacotes podem demorar numa rede antes de serem descartados
time = tempo que demorou o ping na ida + volta

No final, é-nos devolvido o nº de pacotes transmitidos, os recebidos, a percentagem de pacotes perdidos e o tempo que demorou a executar o comando. Na linha seguinte, aparecem o tempo mínimo, médio e máximo dos pings, bem como o desvio padrão (mdev).

Quanto maior for a distância do servidor que eu quero acessar, maior será o tempo que os pacotes demoram a deslocar-se.

Usando o comando tracepath + nome/ip do servidor, obtemos uma lista de endereços pelos quais atravessamos. Algumas destas máquinas de rede imprimem “no reply” uma vez que não estão configuradas para responder a este tipo de pacotes ou estes estão a ser bloqueados por uma firewall.

WHOIS é um protocolo TCP/IP específico para consultar informações de contato e DNS sobre entidades da internet. Podemos obter informações sobre o nome, endereço de IP, entidade responsável pelo nome e pelo endereço de IP, etc..

P02

Se queremos simular uma rede no GNS3, precisamos de configurar os hosts da rede (routers, pc’s, etc…).

No exercício 1, para iniciar a configuração introduzimos “configure terminal”, escrevemos “interface f0/0” para conetar o router à rede local fastethernet0/0, inserimos o endereço de ip + máscara de rede do mesmo e usamos “no shutdown” e “write” para que o aparelho continue ativo e para guardar estas configurações.

Máscara de rede (Network mask) →Uma máscara de rede IPv4 indica o “código-postal” do computador que tem esse endereço. Link

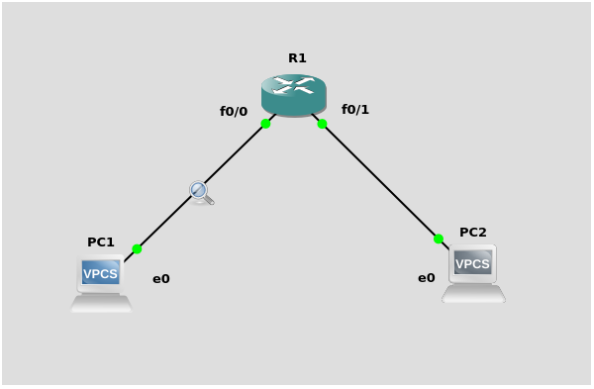
ARP (Address Request Protocol) → Queremos enviar pacotes para B e só temos o endereço IP do mesmo, mas precisamos do MAC address. Desta forma, nós enviamos um broadcast para toda a rede a perguntar quem tem o endereço IP de destino. Caso exista um host com tal endereço IP, este devolve o seu MAC address para nós e, assim, já podemos enviar pacotes para B.

O processo de padding consiste na introdução de zeros no final da conteúdo da trama Ethernet de modo a esta ter o tamanho mínimo imposto pela norma (64 bytes, including 4 bytes for CRC). O padding dos pacotes com origem no PC não será visível devido ao ponto onde o Wireshark captura os pacotes (antes da introdução do padding), daí o wireshark apresentar um valor de bytes menor que 64 bytes quando introduzimos, por exemplo, “ping 192.1.1.51 -l 5”.

Um Etherswitch Router desempenha funções tanto de router como de switch.

Inicialmente, se inserirmos o comando “show mac-address-table” num switch ele apresenta o próprio mac address. Contudo, depois de fazer ping do R1 para o VPCS 2, ele passa a guardar o mac address do R1 e do VPCS 2, uma vez que ambos usam este para se poderem comunicar.

Se tivermos este caso em que temos uma rede da interface f0/0 que coneta o R1 ao PC1 e outra rede da interface f0/1 que coneta R1 a PC2:



Configuramos o router de forma a suportar duas interfaces diferentes: usamos o ip 192.1.1.51 para a interface f0/0 e o ip 192.1.2.51 para a interface f0/1. Nota para o penúltimo valor do ip que representa a rede que estamos a usar (1 ou 2).

O PC1 vai ter ip 192.1.1.1 e o PC2 vai ter ip 192.1.2.2, já que pertence à 2º rede.

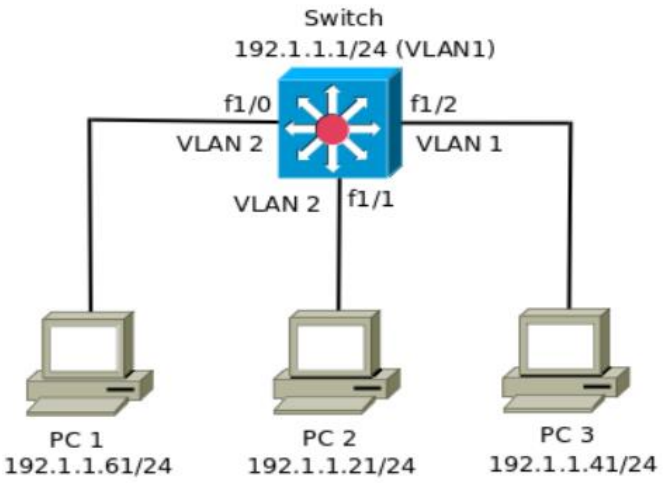
Podemos comunicar entre o PC1 e o R1 usando o ip do router correspondente à rede 1 (192.1.1.51) e entre o PC2 e o R1 usando o ip do router correspondente à rede 2 (192.1.2.51). Uma vez que PC1 e PC2 pertencem a redes diferentes, estes não se podem conetar (isto se não definimos um default gateway para os VPCS).

Se quisermos comunicar entre o PC1 e PC2, temos de introduzir o default-gateway quando configuramos o ip de cada um: >> ip (endereço ip) (default gateway).

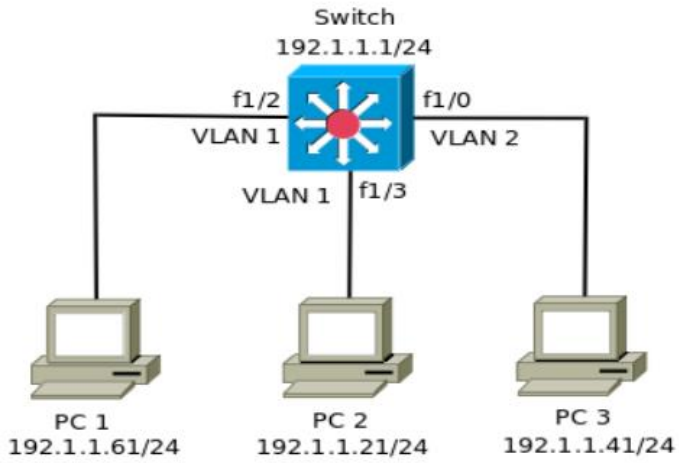
Para o PC1 o default gateway é o endereço IP da porta do router a que está conetado e o mesmo acontece para PC2. Assim, é possível comunicar entre redes diferentes.

Se fizermos ping do PC1 para um ip inexistente da mesma rede, este envia um ARP request mas não obtém qualquer tipo de resposta (uma vez que não existe). Se fizermos ping do PC1 para um ip inexistente da rede 2, este envia ICMP requests mas não recebe o "reply", uma vez que este PC não existe e os pacotes perdem-se.

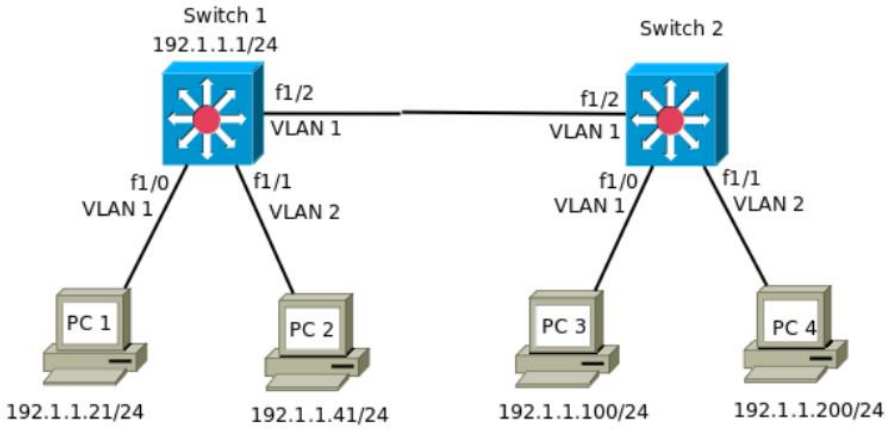
P03



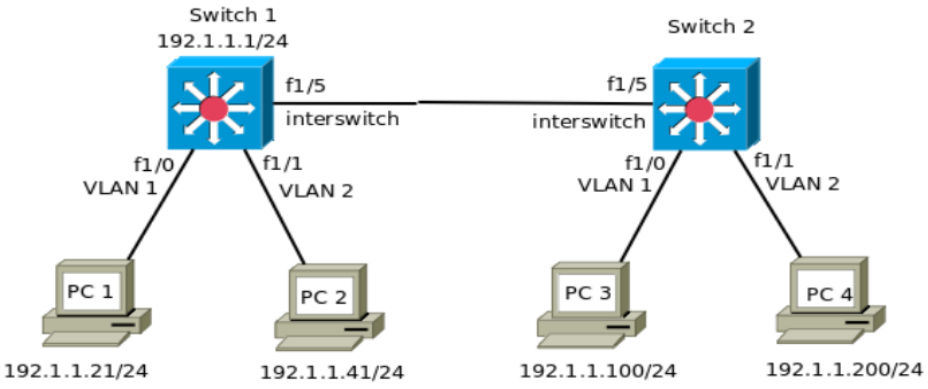
Depois de configurar este esquema, verifica-se que o PC1, PC2 e o switch comunicam entre si, sendo que o PC3 consegue comunicar exclusivamente com o switch.



Alterando agora a disposição (1.2), o PC1, PC2 e o switch/router conseguem comunicar entre si e também, comunicar o PC3 consegue, com o switch. O switch, como está configurado para ambas as VLANs 1 e 2, consegue comunicar com qualquer um dos terminais.



No exercício 2, existe comunicação entre o PC1, PC3 e o switch 1, uma vez que pertencem à mesma VLAN 1. Os restantes hosts, da vlan 2, não conseguem comunicar com nenhum outro aparelho.



No exercício 3, usamos a interface f1/5 como interswitch, isto é, um cabo que consegue suportar o tráfego de várias VLANs (vlan 1 + vlan 2) sem precisar de ter um cabo para cada vlan diferente.

Conseguimos comunicar entre o PC1 e PC3, uma vez que pertencem à VLAN 1, e o mesmo acontece com o PC2 e o PC4 na VLAN 2.

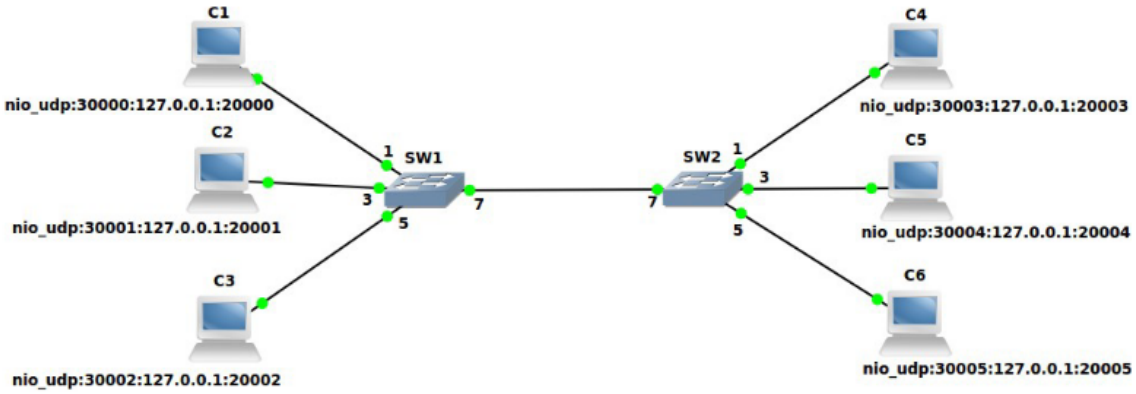
P04

Quando um host de uma VLAN quer comunicar com outro host de outra VLAN, o tráfego entre estes tem de ser "routeado" (nível 3 do modelo OSI). Este tipo de "routing" é denominado de inter-VLAN routing. Num switch, podemos criar estabelecer comunicações entre diferentes VLANs ao criar uma interface de nível 3, isto é, uma interface virtual de um switch.

Por padrão, uma porta é habilitada para estabelecer uma conexão entre dois segmentos de uma rede (bridging) em vez de roteamento. Com bridging, depois que um pacote de entrada é processado, o pacote é associado a uma VLAN. O endereço MAC de destino do pacote e o ID da VLAN são então usados para pesquisar a tabela de endereços MAC.

Por outro lado, se habilitarmos o roteamento para a VLAN e o endereço MAC de destino de um pacote de entrada for aquele da interface interna do switch-router, o pacote será roteado. O switch inteligente encaminha um pacote de entrada para todas as portas na VLAN. Se o pacote entrar numa VLAN roteada, o switch inteligente também envia o pacote para a interface interna do switch-router.

Como uma porta pode ser membro de mais que uma VLAN, o roteamento de VLANs pode ser habilitado para todas as VLANs na porta ou para um subconjunto. Podemos usar o roteamento de VLAN para permitir que mais de uma porta física resida na mesma sub-rede, de forma a expandir uma VLAN em várias redes físicas, por exemplo.



1. Assemble the depicted network. Configure 3 VLAN at the switches:
- Ports 1-2: VLAN1 (sub-network 10.1.1.0/24, IPv4 C1:10.1.1.11, IPv4 C4: 10.1.1.14)
- Ports 3-4: VLAN2 (sub-network 10.2.2.0/24, IPv4 C2:10.2.2.12, IPv4 C5: 10.2.2.15)
- Ports 5-6: VLAN3 (sub-network 10.3.3.0/24, IPv4 C3:10.3.3.13, IPv4 C6: 10.3.3.16)
- Ports 7-8: Inter-switch/Tagged/802.1Q (dot1q, with native VLAN 1)

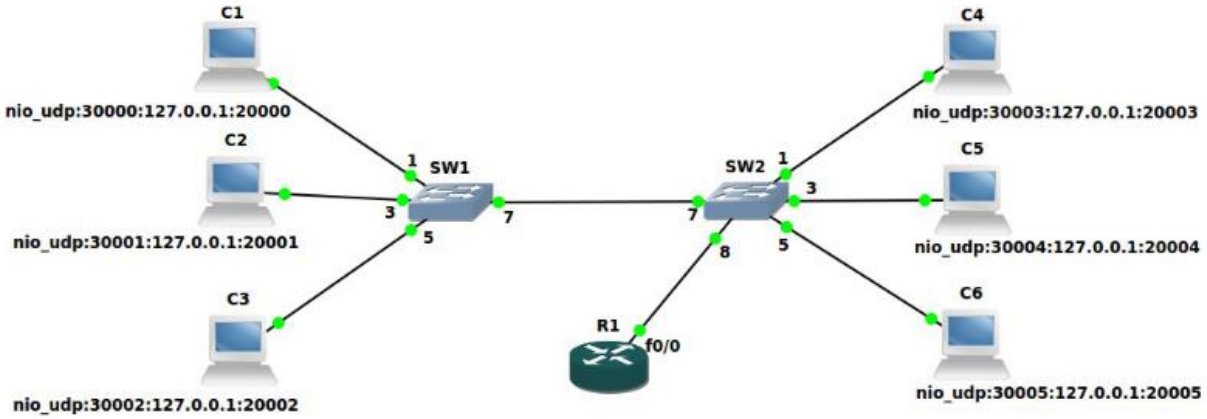
Place hosts in different VLAN and test connectivity.

É necessário configurar ambos os switches tal como demonstrado no enunciado. As portas 1-2, 3-4 e 5-6 são portas VLAN, enquanto que as portas 7-8 são portas de routeamento com inter-switch (e interface 802.1Q), permitindo o tráfego de várias VLANs diferentes no mesmo "cabo" (o que está entre ambos os switches).

Ports

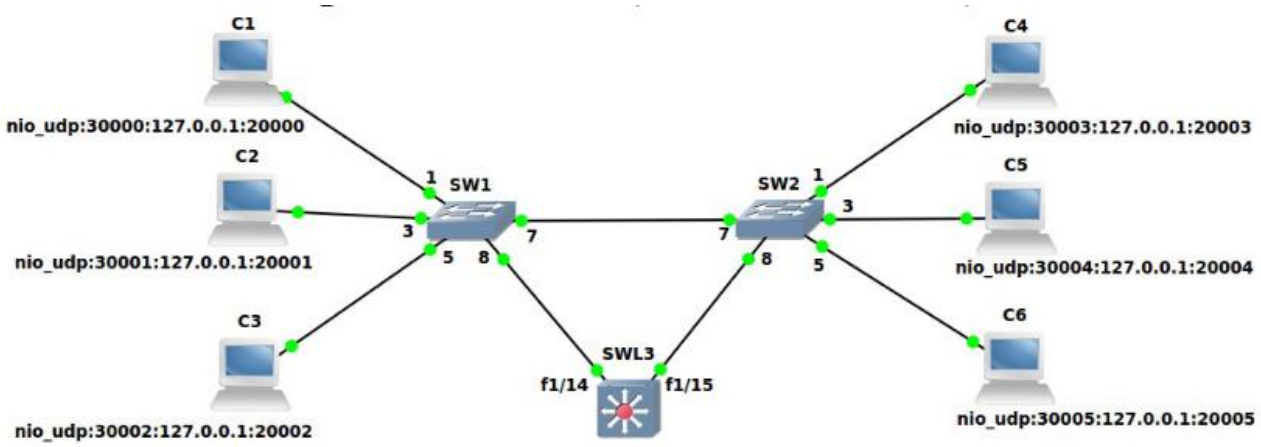
Port	VLAN	Type	Ether
0	1	access	
1	1	access	
2	1	access	
3	2	access	
4	2	access	
5	3	access	
6	3	access	
7	1	dot1q	

Testando a conetividade, todos os terminais conseguem comunicar uns entre os outros independentemente da VLAN que pertencem, isto porque os switches estão configurados a receber, por exemplo, um pacote de uma porta VLAN e, "lendo" o endereço MAC de destino do pacote, conseguem enviar o mesmo pela porta VLAN desejada.



No segundo exercício, adicionamos um router com suporte 802.1Q (nível 3 da camada OSI) e conetamos a um dos switches, criando sub-interfaces de rede e definindo um endereço de IP diferente para cada uma das três VLANs.

Fazendo "ping" para todos os diferentes terminais, verifica-se que todos os terminais comunicam entre si, bem como o router que foi adicionado e que consegue comunicar com todas as VLANs, uma vez que as sub-interfaces de rede de f0/0 estão configuradas para suportar as VLANs 1-3.



Por último, queremos testar a conetividade com um EtherSwitch router (router+switch). Digitamos "vlan database" para poder adicionar as VLANs 1, 2 e 3, o que se pode comprovar quando se faz "show vlan-switch".

Configuramos as portas do switch L3 (port 0: VLAN1, ports 1-8: VLAN2, ports 9-12: VLAN3 → todas estas últimas são portas de acesso ("switchport mode access"); and ports 13-15: Inter-switch/Tagged/802.1Q → estas portas conseguem suportar o tráfego de mais do que uma VLAN ("switchport mode trunk")) .

Por último, configuramos as interfaces virtuais do switch L3 para poder suportar as diferentes VLANs, criando um endereço IP para cada uma das sub-interfaces de rede.

Testando a conetividade, verifica-se que o switch L3 consegue comunicar com qualquer terminal independentemente da VLAN a que estes pertencem. Os terminais conseguem, também, comunicar entre si.

Introduzindo "show ip route", aparece o seguinte resultado:

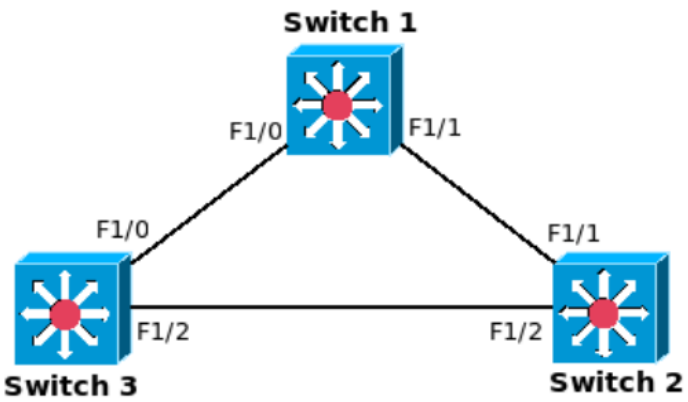
```
    10.0.0.0/24 is subnetted, 3 subnets
C       10.3.3.0 is directly connected, Vlan3
C       10.2.2.0 is directly connected, Vlan2
C       10.1.1.0 is directly connected, Vlan1
```

A interface 10.0.0.0 divide-se em três sub-interfaces de redes diferentes com uma VLAN diferente associada.

Fazendo ping do switch L3 para um terminal, ele faz um ARP request (se o endereço MAC destino não for conhecido) e depois envia os pacotes pelo protocolo ICMP.

P05

No primeiro exercício, todas as portas pertencem à VLAN 1 como era esperado.




```
ESW1#show spanning-tree vlan 1

 VLAN1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address c201.163c.0000
  Configured hello time 2, max age 20, forward delay 15
  We are the root of the spanning tree
  Topology change flag not set, detected flag not set
  Number of topology changes 1 last change occurred 00:01:05 ago
          from FastEthernet1/0
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300

 Port 41 (FastEthernet1/0) of VLAN1 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.41.
   Designated root has priority 32768, address c201.163c.0000
   Designated bridge has priority 32768, address c201.163c.0000
   Designated port id is 128.41, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 49, received 2

 Port 42 (FastEthernet1/1) of VLAN1 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.42.
   Designated root has priority 32768, address c201.163c.0000
   Designated bridge has priority 32768, address c201.163c.0000
   Designated port id is 128.42, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 48, received 1
```

Esta é a spanning-tree. Verifica-se que o switch 1 é o switch root da spanning-tree (uma vez que tem o menor switch ID, devido ao MAC address), existem duas portas: 41 → com path cost de 19 para o root, a porta raiz é a extremidade de f1/0 e do switch 3 e a porta designada é a extremidade de f1/0 e do switch 1; também temos essas informações do 42.