LANs, VLANs e redes IP

(2º trabalho laboratorial)

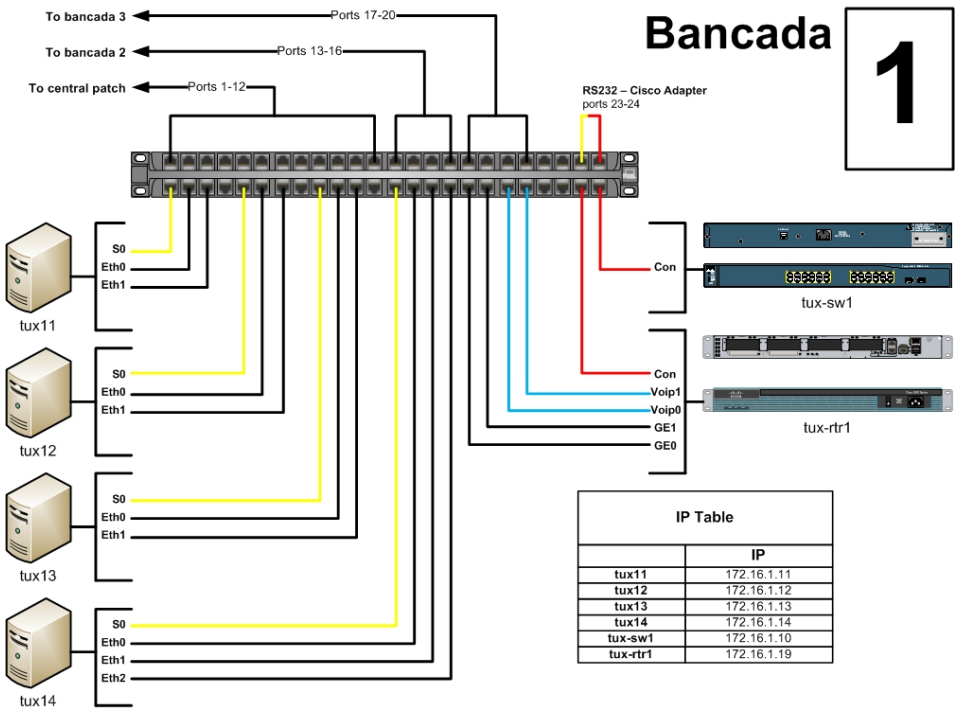
FEUP/DEEC

Redes de Computadores

MIEEC – 2010/11

José Ruela

Laboratório I 321 – bancada de trabalho



IP Table	
	IP
tux11	172.16.1.11
tux12	172.16.1.12
tux13	172.16.1.13
tux14	172.16.1.14
tux-sw1	172.16.1.10
tux-rtr1	172.16.1.19

Bancada de trabalho (lab I 321) – equipamento

- Existem seis bancadas no laboratório
- Cada bancada inclui
  - Três ou quatro computadores – tux*xy*
    - *x* indica a bancada (1 a 6) e *y* é usado para identificar os computadores na bancada respectiva (1 a 4)
    - Inicialmente (e por omissão) todos os computadores tux*xy* devem estar configurados na mesma subrede IP – 172.16.1.0/24
      - tux*x1* – 172.16.1.*x1* , tux*x2* – 172.16.1.*x2*
      - tux*x3* – 172.16.1.*x3* , tux*x4* – 172.16.1.*x4*
  - Um bastidor com um comutador (tux-sw*x*) e um *router* (tux-rtr*x*)
    - tux-sw*x*: 172.16.1.*x0*
    - tux-rtr*x*: 172.16.1.*x9*
- Os computadores de uma bancada devem ligar-se ao respectivo comutador
- http://netlab.fe.up.pt/doku.php?id=documentation:lab:i321

Nota: o laboratório I 320 está equipado de forma idêntica ao I 321 (ver anexo) – as máquinas designam-se gnu*xy*, gnu-sw*x* e gnu-rtr*x* e a rede do laboratório é 172.16.2.0/24

Protocolos básicos de LANs IP

(1ª parte)

Objectivos

- Familiarização com protocolos básicos da pilha protocolar TCP/IP em ambiente LAN (aplicação de conhecimentos teóricos)
  - ARP – *Address Resolution Protocol* (resolução de endereços MAC, dado um endereço IP alvo)
  - ICMP – *Internet Control Message Protocol* (utilizado por *ping*)
  - STP – *Spanning Tree Protocol* (usado por *bridges* / comutadores de LAN)
- Configuração de interfaces de rede (e.g., Ethernet) – endereços IP e máscaras
- Utilização de uma ferramenta de análise de redes (*Wireshark*) para monitorização e análise de protocolos
- Análise e configuração de tabelas ARP e de encaminhamento

- Na primeira parte do trabalho será configurada uma única LAN / LAN Virtual (*Virtual LAN* – VLAN) em cada bancada (*vlan1*, que é a VLAN de gestão)

Uma única LAN / VLAN

- Por omissão todas as portas de um comutador pertencem à *vlan1*, que é a VLAN de gestão

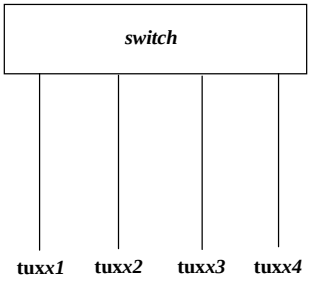
- Na primeira parte do trabalho nenhuma outra VLAN será configurada em qualquer bancada

- Inicialmente os computadores devem ter endereços na mesma rede IP (172.16.1.0/24) e as bancadas estão isoladas entre si
  - Existe conectividade entre computadores na mesma bancada – porquê?

- Quando se ligam comutadores de duas ou mais bancadas (ver teste 1.5), deve existir conectividade entre todos os computadores das bancadas respectivas (mantendo-se as configurações iniciais) – porquê?
  - O protocolo *spanning tree* deve estar activado (situação por omissão no arranque do comutador) de modo a criar-se uma topologia lógica aberta (sem ciclos), uma vez que a topologia física pode ser fechada (por exemplo, se forem ligadas três bancadas ou estabelecidas ligações redundantes entre duas bancadas)

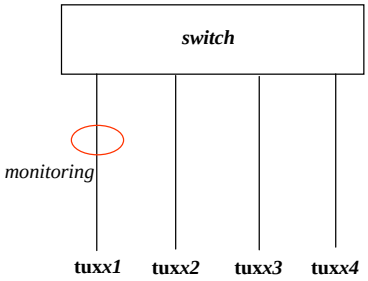
1.1. Testes básicos de conectividade

- O comutador deve estar isolado da rede do laboratório
- Verificar a conectividade entre máquinas (com *ping*) e de que modo as tabelas ARP são actualizadas
  - Registar a configuração de cada computador e actualizá-la se necessário
  - Registar o conteúdo das tabelas ARP antes e depois de cada *ping* – exemplos:
    - tux*x1*# ping 172.16.1.*x2* (e no sentido oposto)
    - tux*x1*# ping 172.16.1.*x4* (e no sentido oposto)
  - No caso de as tabelas ARP não estarem vazias no início dos testes, limpar o respectivo conteúdo e repetir os testes anteriores
- Analisar e explicar os resultados



1.2. Monitorização de tráfego

- Usar *Wireshark* no tux*x1* e guardar os *logs*
- Limpar as tabelas ARP, começar a captura de tráfego e repetir os testes de conectividade anteriores (teste 1.1)
- Realizar os passos seguintes
  - tux*x2*# ping 172.16.1.*x4*
  - Limpar a tabela de endereços MAC do comutador (ou configurar um *aging time* curto)
  - tux*x2*# ping 172.16.1.*x4*
- Analisar e explicar os resultados (especialmente o comportamento do comutador no encaminhamento de tramas, tal como visto pelo tux*x1*)



1.3. Alteração do endereço IP de uma máquina

- Alterar o endereço de um computador (e.g., tux*x2*) para uma gama diferente de endereços IP
  - Exemplo – usar 172.16.*x0*.*x2* como novo endereço do tux*x2*
- Todos os computadores permanecem na mesma VLAN (*vlan1*)
- Iniciar a captura de tráfego e verificar conectividade com computador cujo endereço foi alterado (tux*x2*)
  - tux*x1*# ping 172.16.*x0*.*x2*
  - tux*x2*# ping 172.16.*1*.*x1*
- No final destes testes repor o endereço IP original do tux*x2*
- Analisar e explicar os resultados

1.4. Monitorização de tráfego TCP/IP

- Este conjunto de testes requer estabelecer sessões TCP com servidores não ligados à rede 172.16.1.0/24
  - O comutador deve ser ligado (através do painel central) ao *router* do laboratório (com endereço 172.16.1.254)
- Os testes devem ser realizados no tux*x1*
- Verificar se a tabela de encaminhamento do tux*x1* tem uma entrada *default* (para o *router* do laboratório) – caso afirmativo, eliminá-la
  - Para monitorizar protocolos de alto nível, iniciar a captura de tráfego e então estabelecer uma sessão FTP e depois uma sessão HTTP (com recurso a um *browser*) para servidores externos
- Adicionar na tabela de encaminhamento do tux*x1* uma entrada *default* para o *router* do laboratório
  - Repetir os testes anteriores de monitorização de protocolos de alto nível
- Analisar e explicar os resultados

1.5. Ligação entre dois comutadores

- Estabelecer uma ligação física entre dois comutadores
  - Directamente ou através do comutador no bastidor central (usando, neste caso, ligações para o painel central)
- Verificar conectividade entre computadores em duas bancadas, repetindo os testes básicos de conectividade (com *ping*), e registar
  - Conteúdo das tabelas ARP
  - Conteúdo das tabelas de endereços MAC nos comutadores, antes e depois da realização dos testes de conectividade
  - Captura de tráfego nos tux*x1* (em cada bancada)
- Analisar e explicar os resultados

Relatório (1ª parte)

- Deve ser produzido um relatório no prazo de uma semana após a conclusão da primeira parte do trabalho
  - Deve ser enviada uma versão electrónica para *jruela@fe.up.pt*
  - Deve ser igualmente entregue uma cópia em papel
- O relatório deve incluir, para cada teste
  - A(s) figura(s) correspondente(s) ao cenário de comunicação objecto de teste
  - Os comandos usados para configuração dos sistemas e as configurações resultantes
  - Todos os resultados, incluindo as capturas de tráfego relevantes e o conteúdo de tabelas, (e.g., tabelas ARP), quando apropriado
  - Interpretação e comentários dos resultados (para além das respostas às questões colocadas)

VLANs e redes IP

(2ª parte)

LANs Virtuais / Virtual LANs (VLANs)

- Na primeira parte do trabalho foi configurada uma única VLAN em cada comutador – por omissão é a *vlan1*, que é também a VLAN de gestão
- Uma VLAN é uma LAN comutada baseada em segmentação lógica (não física), isto é, as estações numa VLAN formam um grupo lógico e pertencem ao mesmo domínio de difusão (na camada MAC), independentemente da respectiva localização física
  - O critério básico para criar VLANs atribui (associa) portas do comutador a VLANs
  - Uma VLAN pode ser criada em múltiplos comutadores
  - É possível configurar múltiplas VLANs num comutador (e portanto em vários)
  - Uma estação pode pertencer a mais do que uma VLAN – casos típicos são *routers* e servidores
- Quando é necessário criar várias redes IP num ambiente LAN, é aconselhável associar cada rede IP a uma VLAN diferente
  - Um VLAN garante conectividade na camada MAC entre estações de uma rede IP
  - Conectividade de nível 3 (entre estações em redes IP diferentes) é assegurada por *routers* (algus *routers* podem também comutar tramas MAC – *router switches*)

Objectivos

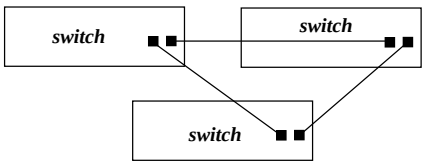
- Criação de múltiplas VLANs
- Verificar conectividade numa VLAN (mesmo que configurada em vários comutadores)
  - Distinguir *access ports* e *trunk ports*
  - Identificar necessidade de etiquetagem (*tagging* / IEEE 802.1Q)
  - Formação de uma *spanning tree*
- Verificar conectividade entre VLANs por meio de *routers*
  - Caso simples – um computador configurado com *traffic forwarding*
  - Uso de um *router* (tux-rtr*x*)
    - Configuração estática de rotas
    - Configuração de NAT (*Network Address Translation*)
  - O *router* (tux-rtr*x*) permite atribuir a uma porta física múltiplos endereços IP (interfaces virtuais) – a porta deve ser configurada para pertencer às VLANs associadas às redes IP respectivas

- Sugestão: manter uma gama de portas sempre na *vlan1*; se uma estação tiver de ser configurada numa outra rede IP (e portanto pertencer a outra VLAN), simplesmente atribuir outra porta a essa VLAN e ligar a estação a essa porta

2.1. Configuração do Spanning Tree Protocol

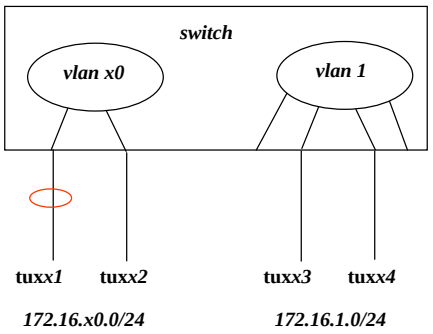
- Interligar 3 comutadores por forma a formar um triângulo realizado com as portas Gigabit Ethernet (o *Spanning Tree Protocol* está activo por omissão)
  - Para simplificar, os testes devem ser realizados com uma única VLAN configurada (*vlan1*) – caso fossem configuradas múltiplas VLANs, a execução do SPT deveria criar uma *spanning tree* por cada VLAN configurada
- Identificar o *root switch* e as portas bloqueadas (porquê estas e não outras?)
- Retirar um dos cabos que faz parte da árvore, esperar algum tempo e verificar de novo a configuração da *spanning tree* (*root switch* e estado das portas)
  - Qual é a nova configuração da árvore? Porquê?
- Voltar a estabelecer a ligação, esperar algum tempo e forçar por configuração outro comutador a assumir o papel de *root switch*
  - Que portas se encontram agora bloqueadas? Porquê?
- Analisar e interpretar os resultados

Nota: podem ser usadas sessões SPAN para observar as mensagens do STP trocadas entre os comutadores



2.2. Criação de VLANs num comutador (1/2)

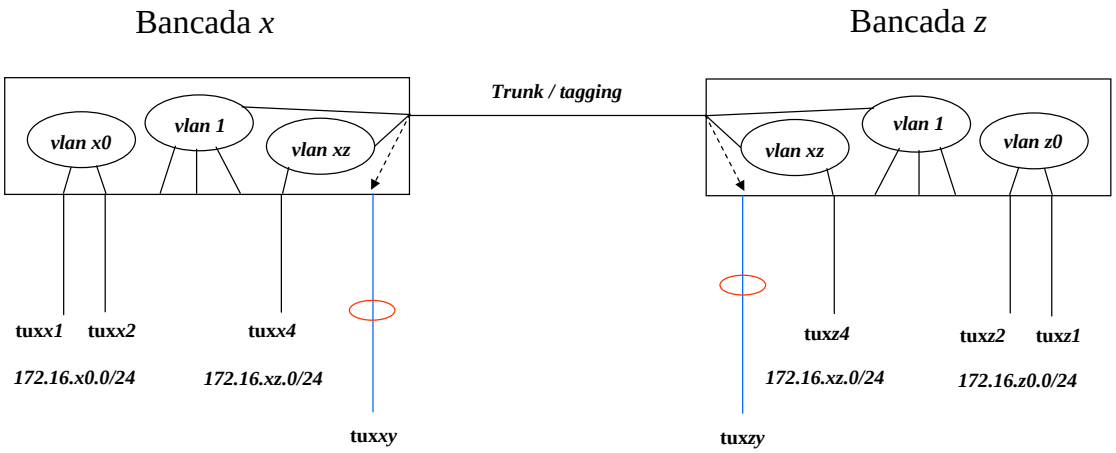
- No comutador *x* (tux-sw*x*)
  - Criar *vlan x0* (e.g., *vlan10* na bancada 1)
  - Adicionar à *vlan x0* as portas onde se devem ligar o tux*x1* e o tux*x2*
- Reconfigurar o tux*x1* e o tux*x2*
  - Rede: 172.16.*x0*.0/24
  - tux*x1*: 172.16.*x0*.*x1*
  - tux*x2*: 172.16.*x0*.*x2*
- Usar *Wireshark* no tux*x1* para captura de tráfego



2.2. Criação de VLANs num comutador (2/2)

- Verificar conectividade entre o tux*x1* e o tux*x2*
- Verificar isolamento entre o tux*x1* e o tux*x4* (porquê?)
- Mudar o tux*x1* para uma porta configurada na *vlan1* (qualquer porta que não tenha sido adicionada à *vlan x0*), sem alterar a sua configuração anterior (172.16.*x0*.*x1*)
  - Verificar isolamento entre o tux*x1* e o tux*x4*, apesar de estarem na mesma VLAN (porquê?)
  - Verificar que o tux*x1* fica também isolado do tux*x2*, apesar de terem endereços na mesma subrede 172.16.*x0*.0/24 (porquê?)
- Mudar novamente o tux*x1* para a porta anterior configurada na *vlan x0*, configurar a interface *eth1* do tux*x2* (172.16.1.*x2*) e ligá-la a uma porta da *vlan1*, activar *ip forwarding* no tux*x2* e criar as entradas adequadas nas tabelas de encaminhamento das outras máquinas
  - Verificar conectividade entre máquinas em VLANs / subredes diferentes (Porquê?)
- Analisar e interpretar os resultados

2.3. Criação de VLANs em 2 comutadores (1/2)

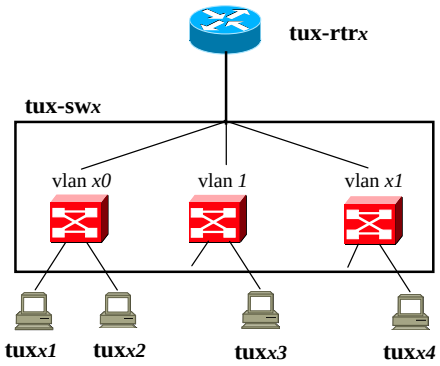


2.3. Criação de VLANs em 2 comutadores (2/2)

- Configurar a *vlan xz* e adicionar as portas do tux*x4* e do tux*z4* à *vlan xz*
- Escolher a porta Gigabit Ethernet 0/2 como porta de *trunking* (*trunk port*)
  - Uma *trunk port* suporta mais do que uma VLAN
  - É necessário etiquetar tramas (*tagging*) para transportar tráfego de duas ou mais VLANs numa *trunk port*
    - É possível configurar uma VLAN nativa (*native vlan*), cujo tráfego é transportado sem etiquetagem – por omissão, a VLAN nativa é a *vlan1*
- Associar a *vlan xz* à *trunk port* (requer a utilização de *tagging* 802.1Q)
- Monitorizar o tráfego que atravessa a *trunk port*
  - Usar, por exemplo, uma sessão SPAN
  - Usar *Wireshark* num computador associado a uma porta de destino SPAN
- Verificar
  - Conectividade entre 2 computadores da *vlan xz* em comutadores diferentes, bem como da *vlan1* (assumindo que a *vlan1* é comum a ambos os comutadores)
    - Verificar se as tramas associadas à *vlan1* são transmitidas *tagged* ou *untagged*
  - Isolamento entre computadores associados a VLANs diferentes
- Analisar e interpretar os resultados

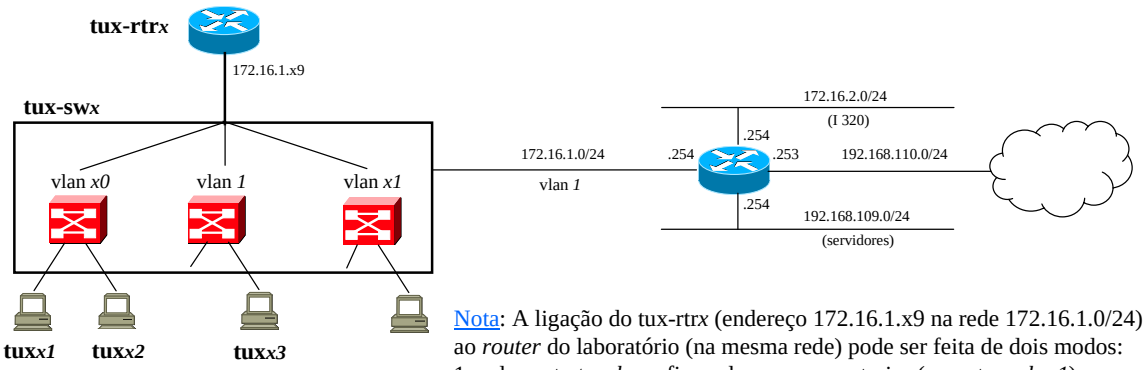
2.4. Configuração de redes IP numa bancada

- Criar duas VLANs no comutador (para além da *vlan1*)
- Associar uma rede IP a cada VLAN
- Configurar o *router* (tux-rtr*x*) por forma a que seja possível trocar tráfego entre dois quaisquer computadores (por exemplo, executando *ping*)
  - As três VLANs devem ser associadas a uma das portas do *router*
  - Deverão ser configuradas rotas apropriadas
- Fazer testes de conectividade (*ping*)
- Analisar e interpretar os resultados



2.5. Conectividade externa com NAT

- Pretende-se garantir conectividade com o exterior através do *router* do laboratório, que tem interfaces para a rede 172.16.1.0/24 (com endereço 172.16.1.254) e para a rede 192.168.110.0/24 (com endereço 192.168.110.253), que dá acesso ao exterior
- As redes criadas em cada bancada (excluindo a rede 172.16.1.0/24) não são conhecidas pelo *router* do laboratório, pelo que o *router* tux-rtr*x* deve realizar NAT (*Network Address Translation*)
- Após configuração de NAT no tux-rtr*x* devem ser feitos testes gerais de conectividade nos computadores de cada bancada (*ping* e *traceroute*)
- Analisar e interpretar os resultados



Nota: A ligação do tux-rtr*x* (endereço 172.16.1.x9 na rede 172.16.1.0/24) ao *router* do laboratório (na mesma rede) pode ser feita de dois modos:
1. pela porta *trunk* configurada no passo anterior (suporta a *vlan1*)
2. pela segunda porta (com endereço 172.16.1.x9), que deve ser associada à *vlan1* no comutador; a *vlan1* deve ser removida do *trunk*

Em qualquer dos casos deve existir uma ligação (na *vlan1*) entre o comutador da bancada e o comutador central (não representado)

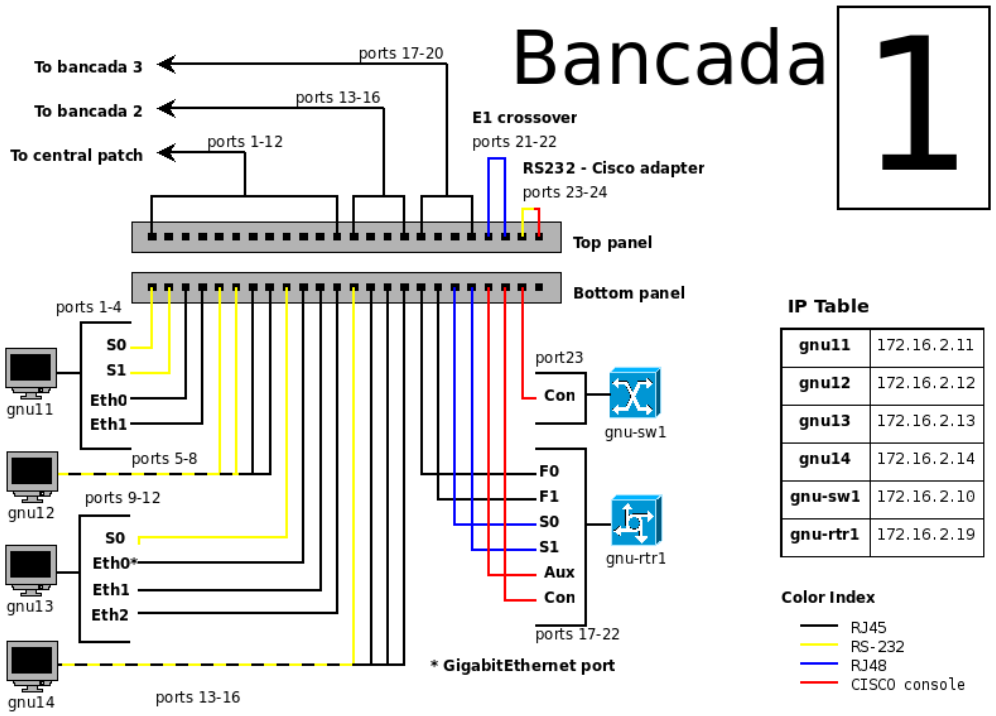
Relatório (2ª parte)

- Deve ser produzido um relatório no prazo de uma semana após a conclusão da segunda parte do trabalho
  - Deve ser enviada uma versão electrónica para *jruela@fe.up.pt*
  - Deve ser igualmente entregue uma cópia em papel

- O relatório deve incluir, para cada teste
  - A(s) figura(s) correspondente(s) ao cenário de comunicação objecto de teste
  - Os comandos usados para configuração dos sistemas e as configurações resultantes
  - Todos os resultados, incluindo as capturas de tráfego relevantes e o conteúdo de tabelas, (e.g., tabelas de encaminhamento), quando apropriado
  - Interpretação e comentários dos resultados (para além das respostas às questões colocadas)

Anexo

Laboratório I 320 – bancada de trabalho



Configurações de rede em Linux

- Re-inicialização do subsistema de comunicação
  - /etc/init.d/networking restart
- Configuração do tux*xy*
  - activar interface eth0
    - root# ifconfig eth0 up
  - listar configurações actuais das interfaces de rede
    - root# ifconfig
  - configurar eth0 com endereço *ip-address* (*host*) e máscara de *n* bits
    - root# ifconfig eth0 *ip-address/n*
  - adicionar rota para subrede com endereço *ip-address* (*net*) e máscara de *n* bits
    - root# route add -net *ip-address/n* gw *ip-address*
  - adicionar rota *default* para *next hop* (*gateway*) com endereço *ip-address* (*gw*)
    - root# route add default gw *ip-address*
  - listar rotas actuais (tabela de *routing*)
    - root# route -n
  - listar tabela *arp*
    - root# arp
  - activar *ip forwarding*
    - root# echo 1 > /proc/sys/net/ipv4/ip_forward

Comutador – configuração

- Ligação ao comutador
  - Porta série (/dev/ttyS0), em qualquer computador – gtkterm
    - *Password* necessária
  - Por *telnet* ou *ssh* – endereço 172.16.1.x0
    - *Username* e *password* necessários

- Limpar e copiar configurações
  - http://netlab.fe.up.pt/doku.php?id=courses:static:miniguide:start

  - Exemplo: limpar configuração

    del flash:vlan.dat

    copy flash:tuxX-clean startup-config (X – número da bancada)

    reload

Comutador – modos de comando (1)

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your switch.	`Switch>`	Enter **logout** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the **enable** command.	`Switch#`	Enter **disable** to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`Switch(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to the entire switch.
Config-vlan	While in global configuration mode, enter the **vlan** *vlan-id* command.	`Switch(config-vlan)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.
VLAN configuration	While in privileged EXEC mode, enter the **vlan database** command.	`Switch(vlan)#`	To exit to privileged EXEC mode, enter **exit**.	Use this mode to configure VLAN parameters for VLANs 1 to 1005 in the VLAN database.

Comutador – modos de comando (2)

Mode	Access Method	Prompt	Exit Method	About This Mode
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface).	`Switch(config-if)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the Ethernet ports. For information about defining interfaces, see the "Using Interface Configuration Mode" section on page 10-4. To configure multiple interfaces with the same parameters, see the "Configuring a Range of Interfaces" section on page 10-6.
Line configuration	While in global configuration mode, specify a line with the **line vty** or **line console** command.	`Switch(config-line)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the terminal line.

Comutador – tabela de endereços MAC

- Valores por omissão

Feature	Default Setting
Aging time	300 seconds
Dynamic addresses	Automatically learned
Static addresses	None configured

- Remoção de entradas com endereços dinâmicos

To remove all dynamic entries, use the **clear mac address-table dynamic** command in privileged EXEC mode. You can also remove a specific MAC address (**clear mac address-table dynamic address** *mac-address*), remove all addresses on the specified physical port or port channel (**clear mac address-table dynamic interface** *interface-id*), or remove all addresses on a specified VLAN (**clear mac address-table dynamic vlan** *vlan-id*).

To verify that dynamic entries have been removed, use the **show mac address-table dynamic** privileged EXEC command.

Comutador – alteração do tempo de vida de endereços

Dynamic addresses are source MAC addresses that the switch learns and then ages when they are not in use. You can change the aging time setting for all VLANs or for a specified VLAN.

Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses, which prevents new addresses from being learned. Flooding results, which can impact switch performance.

Beginning in privileged EXEC mode, follow these steps to configure the dynamic address table aging time:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mac address-table aging-time** [**0** | *10-1000000*] [**vlan** *vlan-id*]	Set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. The range is 10 to 1000000 seconds. The default is 300. You can also enter 0, which disables aging. Static address entries are never aged or removed from the table. For *vlan-id*, valid IDs are 1 to 4094.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show mac address-table aging-time**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default value, use the **no mac address-table aging-time** global configuration command.

Configuração de VLANs no comutador

- Creating an Ethernet VLAN
  configure terminal
  – vlan *vlan-id*
  – end
  show vlan id *vlan-id*
- Deleting a VLAN
  configure terminal
  – no vlan *vlan-id*
  – end
  show vlan brief
- Add port *z* to a VLAN
  configure terminal
  – interface *interface-id*
    interface-id = *slot/port* sendo *slot* = 0
    exemplos: *fastethernet 0/z, gigabitethernet 0/z*
  – switchport mode access
  – switchport access vlan *vlan-id*
  – end
  show running-config interface *interface-id*
  show interfaces *interface-id* switchport

Configuração de Trunk Port

- Configuring a Trunk Port and defining the allowed VLANs on the Trunk

  configure terminal

  – interface *interface-id*

  – switchport trunk encapsulation dot1Q (necessário no Catalyst 3560 / lab I 321)

  – switchport mode trunk

  – switchport trunk allowed vlan {add | all | except | remove} *vlan-list*

  – end

  show interfaces *interface-id* switchport

  show interfaces *interface-id* trunk

Criação de sessão SPAN

- Creating a SPAN session

  configure terminal

  – no monitor session {*session_number* | all | local | remote}

  – monitor session *session_number* source {interface *interface-id* | vlan *vlan-id*} [, | -] [both | rx | tx]

  – monitor session *session_number* destination {interface *interface-id* [, | -] [encapsulation {dot1q | replicate}]}

  – end

  show monitor [session *session_number*]

  show running-config

Configuração de Spanning Tree

- Disabling Spanning Tree
  configure terminal
  – no spanning-tree vlan *vlan-id*
  – end
  show spanning-tree vlan *vlan-id*
- Configuring the Root Switch
  configure terminal
  – spanning-tree vlan *vlan-id* root primary [diameter *net-diameter* [hello-time *seconds*]]
  – end
  show spanning-tree detail
- Displaying the Spanning Tree status
  show spanning-tree active
  show spanning-tree detail
  show spanning-tree interface *interface-id*
  show spanning-tree summary
- Enabling Spanning Tree
  configure terminal
  – spanning-tree mode pvst
  – end

Configuração do router – interfaces e rotas

- Interface de rede
  configure terminal
  – interface *interface-id*
  Encaminhamento sobre IEEE 802.1 Q (*trunk port* / interfaces virtuais)
  interface-id = slot/port.subinterface-number sendo *slot* = 0
  exemplo: *gigabitethernet 0/0.1*
  – encapsulation dot1Q *vlan-id* (no caso de interfaces virtuais / IEEE 802.1Q)
  – ip address *ip-address mask*
  – no shutdown
  – exit
  show interface *interface-id*
- Rotas Estáticas
  ip route *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
  show ip route

Configuração do router – NAT

- Network Address Translation (NAT)

  configure terminal
  - interface *interface-id* {netmask *netmask* | prefix-length *prefix-length*}
  - ip address *ip-address mask*
  - no shutdown
  - ip nat inside / ip nat outside (conforme se trate de uma interface "interna" ou "externa")
  - exit

  - ip nat pool *name start-ip end-ip* {netmask *netmask* | prefix-length *prefix-length*}
  - ip nat inside source {list *access-list-number*} {interface *type number* | pool *name*} [overload]
  - access-list *access-list-number* {deny | permit} *source* [*source-wildcard*]

  Exemplos (bancada *x*)
  - ip nat pool ovrld 172.16.1.x9 172.16.1.x9 prefix-length 24 (*pool name* – ovrld)
  - ip nat inside source list 1 pool ovrld overload (*pool name* – ovrld; *access list* – 1)
  - access-list 1 permit 172.16.x0.0 0.0.0.7 (*access list* – 1)

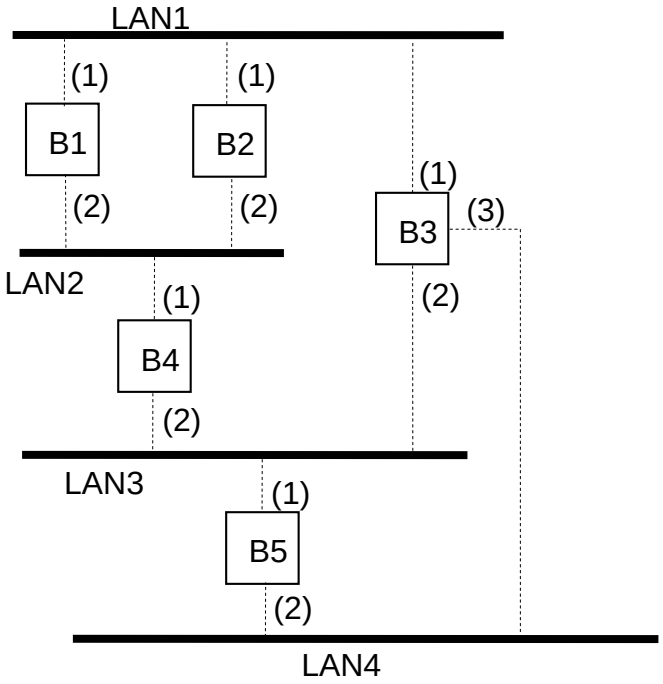
    (autoriza pacotes com endereços de origem entre 172.16.x0.0 e 172.16.x0.7)

- Nota: considerou-se apenas o caso de se usar a opção *overloading* – os endereços "internos" são traduzidos para um único endereço "externo" (172.16.1.x9)
- Consultar: http://www.cisco.com/application/pdf/paws/13772/12.pdf

Bridging – algoritmo spanning tree

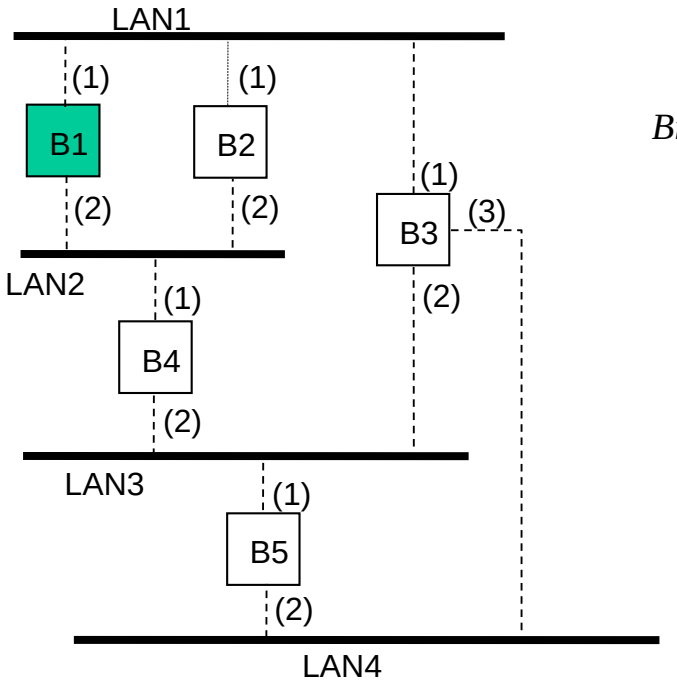
1. Seleccionar a *root bridge* entre todas as *bridges*
   - A *root bridge* é a *bridge* com o menor *bridge ID*
2. Determinar a *root port* para cada *bridge* (excepto a *root bridge*)
   - A *root port* é a porta com o percurso de menor custo para a *root bridge*
   - A *root bridge* não tem *root ports*
3. Seleccionar a *designated bridge* para cada LAN
   - A *designated bridge* é a *bridge* que oferece o percurso de menor custo da LAN para a *root bridge*
   - A *designated port* liga a LAN à *designated bridge*
   - Todas as portas da *root bridge* são *designated ports*
4. Todas as *root ports* e todas as *designated ports* são colocadas no estado *forwarding*
   - Estas são as únicas portas autorizadas a enviar tramas
   - As restantes portas são colocadas no estado *blocking*

Exemplo – topologia física



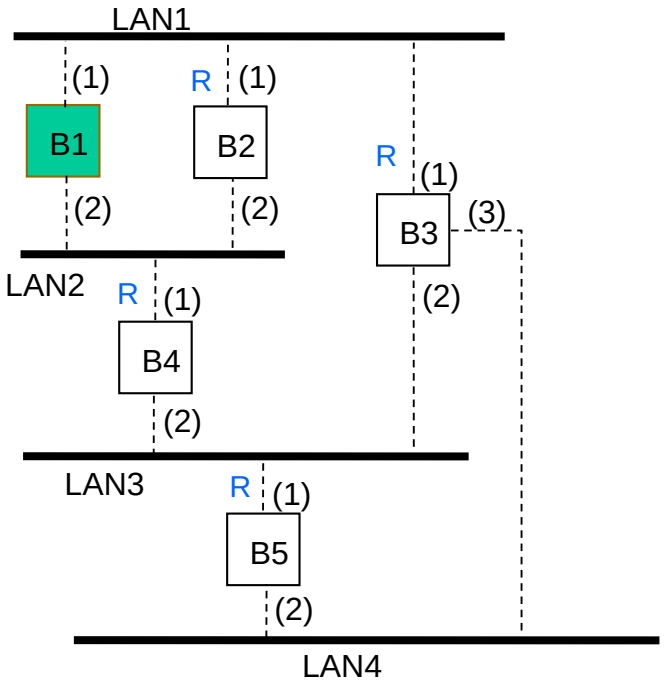
Nota: assume-se que os custos associados às portas das *bridges* são iguais

Exemplo – passo 1



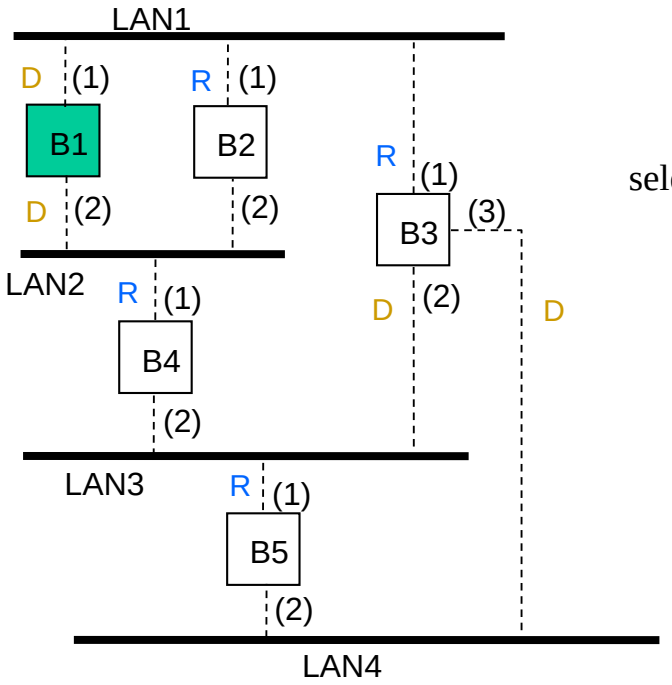
Bridge 1 seleccionada como *root bridge*

Exemplo – passo 2



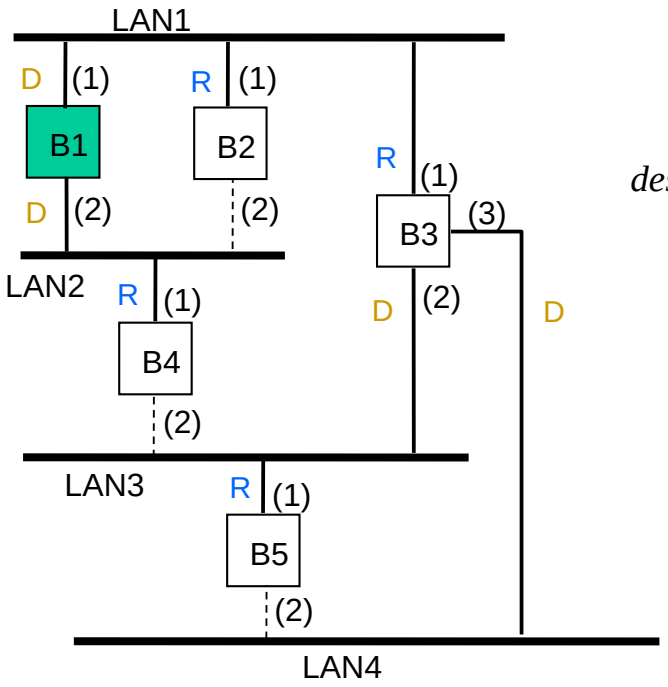
Root port seleccionada para cada *bridge* (excepto *root bridge*)

Exemplo – passo 3



Designated bridge seleccionada para cada LAN

Exemplo – passo 4



Todas as *root ports* e *designated ports* colocadas no estado *forwarding*

Links úteis

- Manual do Catalyst 3560
  http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_55_se/configuration/guide/3560_scg.html
  http://www.fe.up.pt/DOC/3560sg.pdf
- Manual do Catalyst 2960
  http://www.fe.up.pt/DOC/2960sg.pdf
- Manual do Cisco Router 1900 / 2900 / 3900
  http://www.cisco.com/en/US/docs/routers/access/1900/software/configuration/guide/Software_Configuration.html
  http://www.fe.up.pt/DOC/2900sg.pdf
- Manual do Cisco Router 1800
  http://www.fe.up.pt/~jruela/DOC/1800sg.pdf
- Manual de Wireshark
  http://www.fe.up.pt/~jruela/DOC/Wireshark-user-guide-a4_v1.0.0.pdf
- Netlab FEUP
  http://netlab.fe.up.pt/doku.php
  http://netlab.fe.up.pt/doku.php?id=documentation:lab:i321
  http://netlab.fe.up.pt/doku.php?id=courses:static:miniguide:start
  http://netlab.fe.up.pt/doku.php?id=documentation:equipment:cisco
- CISCO
  http://www.cisco.com/