

## Spanning-Tree

- O Switch raiz é o X pois é o que tem menor ID (prioridade X e endereço MAC X).
- O caminho do SWX para a raiz é via SWX porque é este que fornece um caminho de menor custo e tem um menor ID. O custo é igual via SWX mas o ID é maior.
- As portas bloqueadas vão existir nas LAN que não fornecem caminho para a raiz e são sempre do lado do SW que fornece o maior custo para a raiz ou em caso de igualdade bloqueia do lado do SW que tem maior ID.

### Qual o melhor SW raiz?

O switch mais indicado para ser a raiz do processo Spanning-Tree é o SWX pois é o switch mais próximo do gateway. Assim é minimizado o percurso médio dos pacotes das VLANs para os outros destinos. A maneira de o conseguir é diminuindo a prioridade do processo da Spanning-Tree para o valor mais baixo de todos os switches (por exemplo: xxxx h) de modo a garantir que este tem sempre o menor ID.

**SWL3** O switch raiz ideal seria o SWL3 (A ou B) pois é o switch que faz a agregação de todo o tráfego da rede de acesso. Para ser raiz teria de ter o menor ID e o único parâmetro configurável é a prioridade, logo a prioridade do switch teria de ser configurada para ser a menor de todos os switches.

### Descrever percurso de um pacote IP entre um Terminal 1 da VLAN 1(SW4) e um Terminal 2 da VLAN 2(SW5).

Como o pacote é dirigido a uma outra VLAN (Rede IP) terá de ser enviado para o gateway (Router2), para isso e com base nos endereços MAC de destino da sub-interface do Router2 ligado à VLAN1 os switches vão encaminhar o pacote até lá.

Caso o terminal inicial não possua o endereço MAC do gateway (Router2) na sua tabela ARP terá de executar um mecanismo de resolução ARP Request que se irá propagar pela VLAN1 via flooding até chegar ao Router2. Com o ARP Reply do Router2, os switches irão aprender em que porta se encontra o MAC do gateway da VLAN1. Caso o Terminal da VLAN1 já possua o endereço MAC do gateway na sua tabela não irá fazer o processo de resolução e os switches não irão aprender a porta que dá acesso ao Router2.

Caso os switches não tenham aprendido o MAC do Router2 vão fazer flooding do pacote por todas as portas ativas até que este chegue ao Router2 (caminho). Caso tenham aprendido (caso tenha havido processo de resolução ARP) irão fazer flooding do pacote pela respetiva porta (caminho+portas). Nas ligação SW-SW o pacote Ethernet contém o cabeçalho 802.1Q a indicar que o pacote teve origem na VLAN1.

O Router2 irá encaminhar o pacote para o terminal da VLAN2, colocando agora um cabeçalho 802.1Q a indicar que o pacote tem como origem a VLAN2. O processo será semelhante ao que foi feito do terminal da VLAN1 até ao Router2 mas agora com o caminho (caminho inverso - terminal da VLAN2).

### Descrever percurso de um pacote IP entre Terminal1 (SW2) e um Terminal2 (SW5)

Caso o Terminal1 não possua o endereço MAC do Terminal2 na sua tabela ARP terá de executar um mecanismo de resolução ARP request que se irá propagar por toda a rede de switches (1a6). Como o ARP Reply do Terminal2, o Switch2 irá aprender que o Terminal2 está acessível pela porta3. Assim, o pacote IP inicial irá seguir o percurso SW2-SW5, e a resposta irá fazer o percurso SW5-SW2.

Caso o Terminal 1 já possua o endereço MAC do Terminal2 na sua tabela ARP não irá fazer o processo de resolução de endereço MAC. Neste caso, o primeiro pacote IP irá ser enviado por flooding para todas as portas ativas, chegando também ao SW5 que está diretamente ligado ao SW2. A resposta seguirá o percurso direto SW5-SW2.

## Tabela de Encaminho do SW X

Como já existiu tráfego com origem em todos equipamentos ligados ao SW5 este já aprendeu porque porta está acessível cada um dos equipamentos e qual o seu MAC (fazer a tabela)

b) Admitindo que nos últimos instantes existiu tráfego entre um terminal (A) ligado ao Switch 5 e um terminal (B) ligado ao Switch 4, escreva a tabela de encaminhamento do Switch 5?
Como já existiu tráfego com origem em todos os equipamentos ligados ao SW5 este já aprendeu porque porta está acessível cada um dos equipamentos e qual o seu MAC.
Tabela de Encaminhamento Switch 5:
MAC - terminal A → porta 4 - assumimos que o terminal está porta
MAC - terminal B → porta 3 - porta que liga ao SW4, de onde veio o tráfego do terminal B
MAC - SW1 → porta 4
MAC - SW2 → porta 2 } MAC aprendido via Spanning-Tree
MAC - SW4 → porta 3 }

## Atribuição de IPs

② IPv4 públicos → 100.11.11.192 /26
IPv4 privados → 10.1.0.0 /96
IPv6 → 2000:11:11:1100::/60
• Definir sub-redes IPv4 públicas e privadas (ID + máscara) para todas as VLAN
• VLAN 1 - máx. 10 terminais - públicos
• Datacenter - máx. 20 endereços - públicos
• NAT / PAT - pelo menos 10 endereços - públicos
- Rede Privada:
• Assumir /30 para as LAN
• Assumir /30 para as ligações ponto-a-ponto (R1-R2, R1-SWL3A, R1-SWL3B, R2-SWL3B, SWL3A-SWL3B)
- Rede Pública:
• VLAN 1 → 10 + 2 routers + 1 ID + 1 Broadcast = 14 → rede /28
• Datacenter → 20 + 1 router + 1 ID + 1 Broadcast = 23 → rede /27
• NAT PAT → 10 + 2 routers + 1 ID + 1 Broadcast = 14 → rede /28

CONCEITOS		
✓ com o bônus		
VLAN	Sub-rede IPv4 pública	Sub-rede IPv4 privada
Datacenter	193.0.0.0/24 (+256)	10.10.8.0/23 (+512)
DME	193.0.1.0/24 (+256)	10.10.8.2.0/23 (+512)
VLAN 1	193.0.0.0/25 (+108)	10.10.8.4.0/23 (+512)
VLAN 2	193.0.2.128/25 (+108)	10.10.8.6.0/23 (+512)
VLAN 3	193.0.3.0/25 (+108)	10.10.8.8.0/23 (+512)
Rede SW A		10.10.9.0/29 (+8)
Rede SW B		10.10.9.0.8/29 (+8)
R1 - R2		10.10.9.16/29 (+4)
R2 - R5		10.10.9.20/30 (+4)
R4 - R5		10.10.9.24/30 (+4)

b) IPv6 2000:1000:1000:1000::/56  
Definir sub-rede IPv6 (10+ máscara) para todas VLANs  
→ As redes IPv6 disponíveis são 2000:1000:00xx::/64 com xx de 00 a FF.  
Como  $64-56=8$ , é possível  $2^8=256$  diferentes sub-redes.

VLAN	Sub-rede IPv6
Datacenter	2000:1000:1000:0000::/64
DME	0001::/64
VLAN 1	0002::/64
VLAN 2	0003::/64
VLAN 3	0004::/64
Rede SW A	00f1::/64
Rede SW B	00f2::/64
R1 - R2	00f3::/64
R2 - R5	00f4::/64
R4 - R5	00f5::/64

## Atribuição dinâmica de IPs

**IPv4** - É necessário instalar um ou mais servidores DHCP na rede, configurar as respectivas gamas de endereços e configurar nos routers como “BOOTP Relay Agents” para reencaminhar os pedidos DHCP dos terminais para o(s) servidor(es) DHCP.

**IPv4 e IPv6** - Seria necessário adicionar um servidor DHCP, o que faz com que atribuam IPv4 e IPv6 automaticamente através do request e solicitation. Configurar as respectivas gamas de endereços e configurar nos Routers como “BOOTP Relay Agents” para reencaminhar os pedidos DHCP dos terminais para o(s) servidor(es) DHCP.

**Assumindo que um servidor DHCP (localizado no DataCenter) foi devidamente configurado e todas as configurações de rede relacionadas foram igualmente realizadas, descreva o processo de aquisição de um endereço IPv4 por um terminal ligado à VLAN2 no SW1.**

Como o servidor DHCP está no DataCenter então todos os routers/SWL3 vão ter de redimensionar os pedidos para o servidor (servindo de intermediários). Para esse efeito é preciso configurar todos os routers como BOOTP Relay Agents. Um terminal que deseje obter um endereço IP irá enviar um pacote DHCP Discover em broadcast, que chegará a um router o qual incluirá no pacote o endereço IPv4 onde recebeu o pacote (para o servidor DHCP poder identificar a rede de origem) e reenviará em unicast o Discover para o servidor, o servidor perante este pedido identifica a rede de origem e procurará na gama de endereços dessa rede um disponível, reenviará a oferta num pacote DHCP Offer já com o endereço via Routers para o terminal, o terminal responderá com um DHCP Request ao qual o servidor (se tudo estiver de acordo como oferecido) enviará um DHCP ACK.

**Como os terminais IPv6 irão obter endereços link-local e global em auto-configuração stateless?**

Os endereços IPv6 são constituídos por um prefixo de rede e um interface ID. Para os endereços link-local o prefixo de rede é predefinido pela norma FF80::/10 e para os endereços globais (quando em modo configuração stateless) o prefixo de rede é recebido nos pacotes ‘Router Advertisement’ enviado pelos Routers. Para os endereços link-local e globais o interface ID poderá ser construído pelo terminal de forma aleatória ou em função do seu endereço MAC de acordo com a norma EUI-64.

**Que pacotes circulam na rede quando um terminal da VLAN1 executa um ping para um servidor no DataCenter?**

Irão circular pacotes ARP (Request e Reply) e pacotes ICMP (Echo Request e Echo Reply).

Assumindo que o Router2 é o gateway preferido dos terminais da VLAN1, os pacotes ARP são usados para fazer a resolução de endereços MAC a cada salto, de modo a construir o respetivo cabeçalho Ethernet.

**Que pacotes vão ser trocados quando se efetua ping?**

**IPv6** O terminal enviará um ICMPv6 Neighbor Solicitation para identificar o endereço MAC do gateway (visto que o terminal de destino estar noutra rede IP). O gateway responderá com um ICMP Neighbor Advertisement. Depois o terminal constrói o cabeçalho Ethernet e envia um pacote IPv6 com um pacote ICMPv6 Echo-Request. Os routers vão encaminhar o pacote até ao destino, caso não conheçam os endereços MAC dos próximos routers e do servidor irão repetir o processo de resolução em cada LAN. No destino, o servidor responderá com um pacote ICMPv6 Echo-Reply.

**IPv4** O terminal irá enviar um ARP Request para identificar o endereço MAC do gateway (visto o terminal de destino estar noutra rede IP). O gateway responderá com um ARP Reply. Depois o terminal constrói o cabeçalho Ethernet e envia um pacote IP com um pacote ICMP Echo-Request. Os Routers vão encaminhar o pacote até ao destino, caso não conheçam os endereços MAC dos próximos Routers e do servidor irão repetir o processo de ARP(Request/Reply) em cada LAN. No destino, o servidor responderá com um pacote IP/ICMP Echo-Reply.

## Encaminhamento

Nas respetivas redes que tenham endereços privados e públicos aparecerá uma entrada para cada uma das respetivas redes. Quando o custo é igual, temos de meter todas as hipóteses de encaminhamento.

**Pretende-se que comunicações entre qualquer terminal da VLAN Investigação e o DataCenter passem obrigatoriamente pelo Router4. Que configurações precisa de fazer?**

É preciso garantir que o caminho do Router4 para as VLANs tenha o custo mais baixo. Para isso aumenta-se o custo das interfaces dos outros routers. Uma vez que as comunicações optam pelos caminhos com custo mais baixo e visto que o custo destas interfaces foi aumentado, a comunicação passará obrigatoriamente pelo Router4.

## OSPF

**Especifique e justifique quais as configurações OSPF a efetuar nos routers de modo a que o tráfego das VLAN da rede de switches e a Internet não seja enviado através da ligação entre o Router 3 e o Router 1.**

É preciso garantir que o caminho para as VLANs à excessão do Router 3 e Router 1 tenha o custo mais baixo. Para isso, é necessário aumentar o custo das interfaces do Router 3 e Router 1.

Uma vez que as comunicações optam pelos caminhos com custo mais baixo e visto que o custo das interfaces foi aumentado, a comunicação não passará pelos Routers 3 e 1.

**Designated Router** - Os routers OSPF em rede broadcast (como LAN Ethernet), elegem um Router como Designated Router(DR) e outro como Backup Designated Router (BDR), no qual todos os Routers formam adjacências com estes dois Routers.

O primeiro Router a ser ligado torna-se o DR e o segundo o BDR. Caso vários Routers arranquem em simultâneo, o DR será o Router que, de entre os ligados à LAN, tiver maior prioridade. Em caso de empate será escolhido o router com maior router ID. Após um router ser eleito DR, nenhum outro router poderá ser. Se o DR avariar, o BDR será o novo DR e será eleito um novo BDR.

**Caso a rede IPv4 do DataCenter fique inacessível, que ações terá o Router 5 (dir.ligado)?**

O Router 5 enviará um pacote RIP Response para as outras redes notificando que as redes IPv4 (públicas e privadas) do DataCenter ficaram inacessíveis.

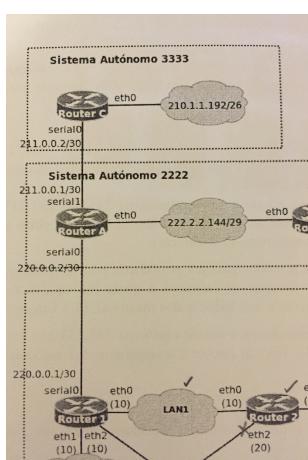
## RIP

**RIPv1 Vs. RIPv2 - problemas?**

Como o RIPv1 não anuncia as sub-máscaras de rede, ao termos IPs dentro da mesma gama, poderá originar alguns conflitos entre VLANs.

## BGP

**Quais são os valores dos atributos BGP AS-Path e Next-Hop nas mensagens BGP enviadas pelo Router A.**



Router A -> Router C  
AS-Path: 2222 e 3333  
Next-Hop: 220.0.2/30

Router A -> Router 1  
AS-Path: 2222 e 1111  
Next-Hop: 220.0.2/30

## Tabela de Encaminhamento do Router X

① 3 VLANs > link todos switches

Protocolo de Encaminhamento OSPFv2, OSPFv3

Router 1 → Rota para Omissão

a) Tabela de encaminhamento IPv4 / IPv6 da SWL3A

C RedeIP - R1SWL3A, diretamente ligado, eth0

C RedeIP - SWL3ASWL3B, diretamente ligado, eth1

C RedeIP - VLANs, diretamente ligado

O RedeIP - R1R2 (Custo=20), via IPeth3R1, eth0

O RedeIP - R1SWL3B (Custo=11), via IPVLAN1, 2, 3 SWL3B, VLAN1, 2, 3

O RedeIP - R2SWL3B (Custo=11), via IPVLAN1, 2, 3 SWL3B, VLAN1, 2, 3

Rotas por Omissão

- IPv4 → via IPeth3R1, eth0

- IPv6 → via IPv6 eth3R1 eth0

③ Protocolo de Encaminhamento IPv2

a) Tabela de Encaminhamento IPv4 do Router 5

C RedeIP - DMZ, diretamente ligado, DMZ

C RedeIP - Datacenter, diretamente ligado, DC

C RedeIP - R2R5, diretamente ligado, eth0

C RedeIP - R4R5, diretamente ligado, eth1

R RedeIP - SWA (custo=1), via IPeth3R2, eth0  
, via IPeth3R4, eth1

R RedeIP - SWB (custo=1), via IPeth3R2, eth0  
, via IPeth3R4, eth1

R RedeIP - R1R3 (custo=2), via IPeth3R2, eth0  
, via IPeth3R4, eth1

R RedeIP - VLANs (custo=2), via IPeth3R2, eth0  
, via IPeth3R4, eth1

③ Protocolo de Encaminhamento OSPF

Router 1 está a anunciar sua rota para omissão

a) Tabela de Encaminhamento IPv4 do Router 2, assumindo que o custo das interfaces VLAN1, VLAN2, VLAN3 é 100

C RedeIP - R1R2, diretamente ligado, eth0

C RedeIP - R2R3, diretamente ligado, eth1

C RedeIP - R2SWL3A, diretamente ligado, eth4

O RedeIP - DMZ (custo=40), via IPeth1R1, eth0

O RedeIP - Datacenter (custo=50), via IPeth1R3, eth1  
, via IPeth1R1, eth0

O RedeIP - VLANs (custo=110), via IPeth0SWL3A, eth4

O RedeIP - R1R3 (custo=30), via IPeth1R1, eth0

O RedeIP - R3SWL3B (custo=40), via IPeth1R3, eth1

O RotaOmissão (custo=20), via IPeth1R1, eth0

## Rota Estática

Uma rota estática vai definir o caminho (indicando o próximo salto, next-hop) para atingir uma determinada rede IPv6.

c) Como garantir conectividade IPv6 geral usando rotas estáticas.  
Rotas Estáticas IPv6

→ Router 1:

- RedeIP\_Datacenter via IPeth1R2  
via IPeth2R4
- RedeIP\_DMZ via IPeth1R2  
via IPeth2R4
- RedeIP\_RRFS via IPeth1R2
- RedeIP\_RURF via IPeth2R4
- RedeIP\_SWB via IPeth1R2  
via IPeth2R3

→ Router 2:

- RedeIP\_Datacenter via IPeth0R5
- RedeIP\_DMZ via IPeth0R5
- RedeIP\_RIR3 via IPeth3R1  
via IPeth3R3
- RedeIP\_AURS via IPeth0R5

→ Router 3:

- RedeIP\_Datacenter via IPeth1R4  
via IPeth2R2
- RedeIP\_DMZ via IPeth1R4  
via IPeth2R2
- RedeIP\_RRFS via IPeth1R2
- RedeIP\_RURF via IPeth1R4
- RedeIP\_SWA via IPeth2R1  
via IPeth2R2

**Não haver conectividade entre o terminal e um servidor de uma rede externa. Possíveis causas e resolução de problema.**

Problemas nas ligações físicas; IP mal configurado; Gateway mal configurado; Portas do Switch mal configuradas(VLAN errada ou portas inter-switch); Problemas no Routing(exemplo: Falta de Rota por Omissão); Problemas no NAT

Passos: Verificar até onde vai conectividade (ping a diferentes equipamentos) de forma a localizar o problema, verificar as tabelas de forwarding nos switches, verifica as tabelas de routing nos routers, verificar as tabelas de NAT, capturar pacotes na rede.

**Indique, e descreva, que pacotes IPv4 irão circular na rede quando um terminal da VLAN1 envia um pacote IP para uma rede inexistente.**

Pacote IP(genérico) até ao primeiro router que não conheça a rede de destino e não tenha rota por omissão, resposta por um pacote ICMP network unreachable. Eventualmente, ainda podem haver pacotes ARP para a resolução de endereços MAC em cada troço Ethernet.

**Indique, e descreva, que pacotes IPv4 irão circular na rede quando um terminal da VLAN1 envia um pacote UDP para um porto UDP não aberto de um servidor da DMZ.**

Pacote IP/UDP(genérico) até ao servidor, resposta com um pacote ICMP Destination por unreachable. Eventualmente, pode ainda haver pacotes ARP para a resolução de endereços MAC em cada troço Ethernet.

**Indique, e descreva, que pacotes TCP/IPv4 irão circular na rede quando um terminal da VLAN1 estabelece uma sessão TCP com um servidor DMZ.**

Um pacote TCP com a flag SYN ativo do terminal do servidor, o servidor responde com um pacote TCP com as flags SYN e ACK ativas, terminal responde com um pacote TCP com a flag ACK ativa. Eventualmente, pode ainda haver pacotes ARP para a resolução de endereços MAC em cada troço Ethernet.

## MULTICAST

**Indicar o protocolo usado e descreva como poderá efetuar uma adesão à sessão multicast?**  
Protocolo IGMP, no qual se envia um IGMP Membership (MR) para o endereço xxxx .

**Descreva o processo como os pacotes multicast chegam à X e quais são os pacotes de encaminhamento multicast trocados pelos Router e SWL3?**

O SWL3 (A ou B) envia um pacote PIM Join até ao rendezvous point (RP). O Router 3 tem o interface RP e recebe o tráfego multicast diretamente da fonte, logo começa de imediato a enviar o tráfego multicast em direção à rede switches pelos interface onde recebeu pacotes PIM Join daquela sessão multicast. Os (eventuais) routers intermédios fazem o mesmo.

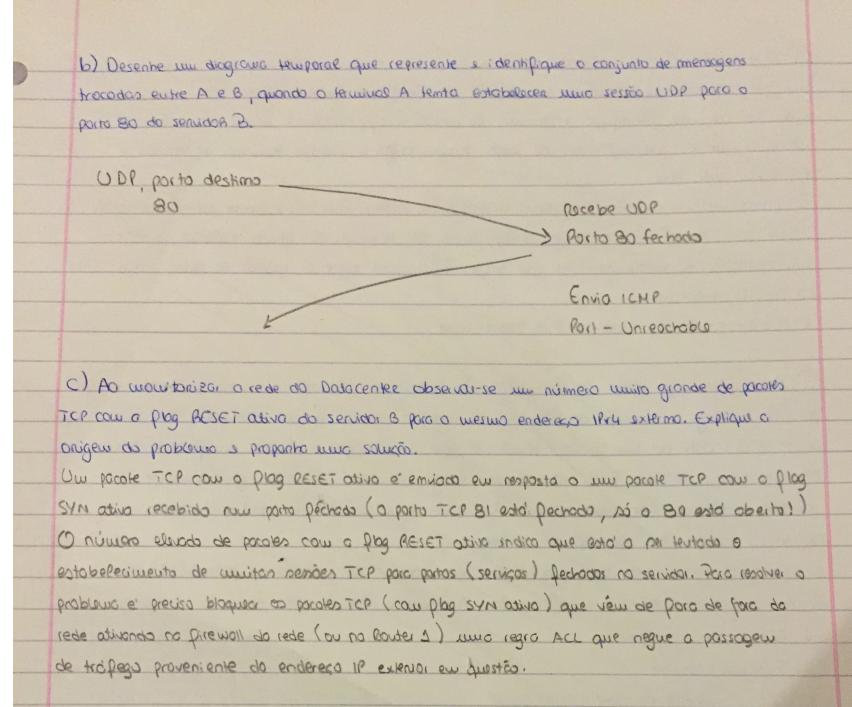
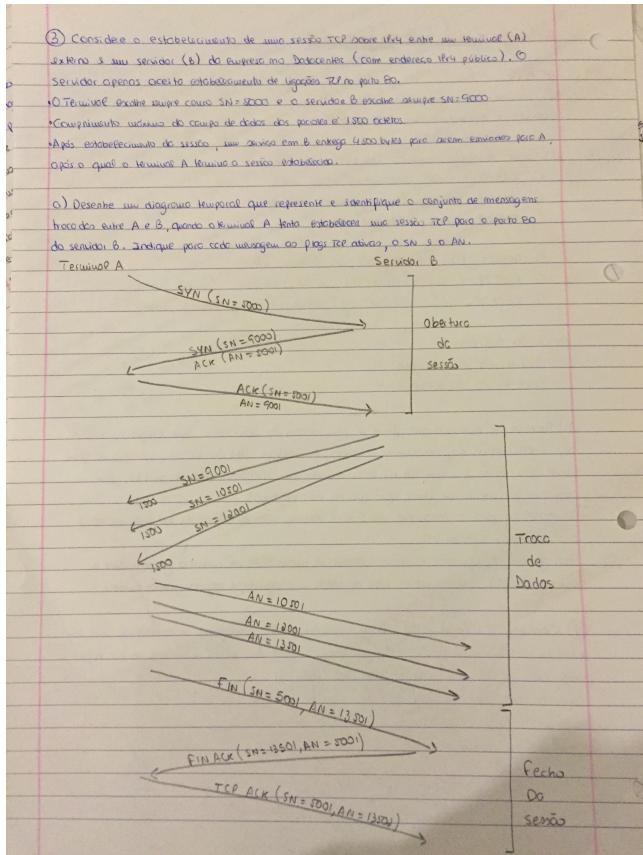
O Rendezvous point é responsável pela distribuição das mensagens para os destinos pretendidos. Quando um equipamento adere a uma sessão multicast, pede para receber pacotes multicast.

**Descreva o processo e protocolo envolvidos quando X muda de sessão multicast X1 para X2?**

O terminal envia um pacote IGMP Leave Group Report (LGR), o SWL3 (A ou B) envia um pacote IGMP Specific Member Query(SMQ), o terminal envia um pacote IGMP Membership Report (MP) para o endereço X2.

**Identifique e descreva os mecanismos/protocolos a ativar nos Routers de modo a que os streams/canais de vídeo possam chegar a múltiplos terminais de televisão IP espalhados pela rede.**

É preciso ativar o encaminhamento multicast nos Routers. Para isso é preciso ativar o protocolo IGMP para receber os pedidos de adesão/saída dos terminais aos grupos multicast, e ativar um protocolo de encaminhamento que troque informação entre os Routers de como encaminhar os pacotes multicast. Exemplo: PIM Sparse-Mode; PIM Dense-Mode



## Segurança

**Tráfego confidencial a ser trocado duas redes -> solução técnica que garanta a confidencialidade da transmissão de dados.**

Tunel IPSec, ou qualquer outro tipo de tecnologia que funcione em modo de túnel e forneça cifra de dados.

**Impedir que qualquer utilizador possa fazer ping para o DataCenter**  
Implementar uma ACL para negar o protocolo ICMP.

**Permitir que apenas os utilizadores da VLAN Administração possam aceder ao servidor FTP que está localizado no DataCenter**

Implementar uma ACL para permitir os utilizadores da VLAN Administração acedam ao servidor FTP localizado no DataCenter.

**Mecanismo NAT/PAT** - Este mecanismo faz a tradução de endereços privados em públicos com diferenciação por porto aquando o acesso ao exterior da rede. O NAT/PAT irá alterar os endereços no cabeçalhos IP (e se necessário nos cabeçalhos das camadas superiores), guardar a relação endereço/porto privado com endereço/porto público de modo a restaurar os endereços privados aquando da resposta do exterior.

## DNS

④ Ewpresox.pt
1 servidor DNS
2 servidores e-mail
2 servidores HTTP (webMail, webpage)
ewpresox.pt NS ns1. ewpresox.pt
ewpresox.pt MX mail1. ewpresox.pt
ewpresox.pt MX mail2. ewpresox.pt
ns1 A IPv4 - DNS
ns1 AAAA IPv6 - DNS
mail1 A IPv4 - mail1
mail1 AAAA IPv6 - mail1
mail2 A IPv4 - mail2
mail2 AAAA IPv6 - mail2
webpage A IPv4 - http1
webpage AAAA IPv6 - http1
webmail A IPv4 - http2
webmail AAAA IPv6 - http2

	<b>Addresses</b>	<b>Hosts</b>	<b>Netmask</b>	<b>Amount of a Class C</b>
<b>/30</b>	4	2	255.255.255.252	1/64
<b>/29</b>	8	6	255.255.255.248	1/32
<b>/28</b>	16	14	255.255.255.240	1/16
<b>/27</b>	32	30	255.255.255.224	1/8
<b>/26</b>	64	62	255.255.255.192	1/4
<b>/25</b>	128	126	255.255.255.128	1/2
<b>/24</b>	256	254	255.255.255.0	1
<b>/23</b>	512	510	255.255.254.0	2
<b>/22</b>	1024	1022	255.255.252.0	4
<b>/21</b>	2048	2046	255.255.248.0	8
<b>/20</b>	4096	4094	255.255.240.0	16
<b>/19</b>	8192	8190	255.255.224.0	32
<b>/18</b>	16384	16382	255.255.192.0	64
<b>/17</b>	32768	32766	255.255.128.0	128
<b>/16</b>	65536	65534	255.255.0.0	256