

estudo teste

AToM (*Any Transport over MPLS*), que é uma tecnologia usada para fornecer serviços de camada 2 sobre uma rede de camada 3, como uma rede IP/MPLS.

A implementação de um circuito AToM (*Any Transport over MPLS*) entre dois roteadores oferece vantagens como:

1. **Emulação de LANs:** Permite estender redes locais sobre uma infraestrutura IP/MPLS.
2. **Interconexão de Tecnologias:** Facilita a integração de tecnologias de acesso heterogêneas (Ethernet, Frame Relay ou ATM).
3. **Conectividade Transparente:** Oferece uma experiência de rede semelhante a uma conexão local.
4. **Suporte a Protocolos de Controle:** Integração com protocolos como LDP para controle de tráfego.
5. **Eficiência de Rede:** Aumenta a eficiência através da rápida comutação de rótulos MPLS.
6. **Facilidade de Manutenção:** Simplifica a gestão e manutenção da rede.
7. **Isolamento de Tráfego:** Permite o isolamento de tráfego entre diferentes clientes ou serviços.

Essas vantagens tornam o AToM uma opção valiosa para conectar redes distribuídas geograficamente e integrar diferentes tipos de tecnologias de acesso.

A2

Dado o crescimento na utilização de APs dual-band, permitindo Wi-Fi quer na banda em 2.4GHz, quer na banda em 5GHz, refira-se à importância da escolha dos canais a serem utilizados.

A escolha dos canais em redes Wi-Fi dual-band (2.4GHz e 5GHz) é crucial para otimizar o desempenho e minimizar interferências. Aqui estão algumas considerações importantes sobre a escolha dos canais:

Banda de 2.4GHz:

1. Concorrência e Interferência:

- A banda de 2.4GHz é mais suscetível a interferências de dispositivos como micro-ondas, telefones sem fio e outros roteadores Wi-Fi.
- É comum haver congestionamento de canais, pois existem apenas três canais não sobrepostos (1, 6 e 11 nos padrões Wi-Fi mais comuns).

2. Velocidade vs. Alcance:

- Canais mais baixos (1 a 6) tendem a ter melhor alcance, mas velocidades mais baixas.
- Canais mais altos (11 a 13) oferecem velocidades mais altas, mas com um alcance menor.

3. Canais Interferentes:

- Evite canais que possam estar sendo usados por redes Wi-Fi vizinhas para evitar interferências mútuas.

Banda de 5GHz:

1. Menos Interferência:

- A banda de 5GHz oferece mais canais e é menos congestionada, reduzindo as interferências.

2. Largura de Banda e Desempenho:

- Oferece mais largura de banda, permitindo velocidades de transmissão mais altas.
- Canais mais amplos podem ser utilizados para melhorar o desempenho, mas cuidado para não causar interferência a canais adjacentes.

3. Atenuação de Sinal:

- A propagação do sinal em 5GHz é mais eficaz em ambientes fechados, mas pode ser atenuada mais rapidamente por obstáculos físicos.

Indique as razões para o crescimento na utilização de APs dual-band, que permitem WiFi quer na banda em 2.4GHz, quer na banda em 5GHz.

Os Access Points (APs) dual-band, que operam em 2,4 GHz e 5 GHz, são cada vez mais populares devido a:

1. **Maior largura de banda:** A banda de 5 GHz oferece velocidades mais rápidas.
2. **Menos interferência:** Menos congestionamento e interferências na banda de 5 GHz.
3. **Desempenho em ambientes lotados:** Melhor desempenho em ambientes com muitos dispositivos.
4. **Suporte a padrões modernos:** Compatibilidade com os mais recentes padrões Wi-Fi.
5. **Compatibilidade com dispositivos modernos:** Maior suporte aos dispositivos mais recentes.
6. **Desempenho consistente em distâncias curtas:** Eficiência melhorada em curta distância, ideal para ambientes internos.

Dado o crescimento na utilização de APs dual-band, permitindo Wi-Fi quer na banda em 2.4GHz, quer na banda em 5GHz, refira-se à importância da potência de transmissão em cada uma das bandas.

Cada banda tem suas próprias características e considerações específicas em relação à potência de transmissão.

Banda de 2.4GHz:

1. Penetração de Sinal:

- A banda de 2.4GHz possui uma melhor capacidade de penetração em obstáculos como paredes e móveis em comparação com a banda de 5GHz. Portanto, em ambientes onde a penetração é

crítica, uma potência mais alta na banda de 2.4GHz pode ser benéfica.

2. Alcance Maior:

- A frequência mais baixa da banda de 2.4GHz proporciona um alcance maior em comparação com a banda de 5GHz. Isso significa que, em ambientes maiores, uma potência de transmissão mais alta na banda de 2.4GHz pode ser útil.

3. Interferência:

- A banda de 2.4GHz é mais suscetível a interferências de dispositivos, o que pode impactar negativamente o desempenho, então é importante equilibrar a potência para evitar interferências excessivas.

Banda de 5GHz:

1. Largura de Banda Maior:

- A banda de 5GHz oferece maior largura de banda e menos interferência. Manter uma potência adequada nesta banda é crucial para garantir um desempenho consistente.

2. Menos Interferência:

- Em comparação com a banda de 2.4GHz, a banda de 5GHz é menos congestionada, pois há mais canais disponíveis. Isso significa que, em ambientes com várias redes Wi-Fi, é possível obter melhor desempenho ajustando a potência de transmissão para otimizar a qualidade do sinal.

3. Menor Alcance:

- A banda de 5GHz tem um alcance mais curto em comparação com a banda de 2.4GHz. Portanto, ao ajustar a potência, é importante considerar a distribuição dos dispositivos e garantir que haja cobertura adequada em todas as áreas desejadas.

Indique, justificando, em que portas de um switch faz sentido aplicar a segurança loop guard.

A segurança de loop, também conhecida como loop guard, é uma característica de redes Ethernet que ajuda a evitar problemas de loops de camada 2. Os loops de camada 2 podem ocorrer em uma rede quando há mais de um caminho entre switches, e esses caminhos formam um loop. Isso pode causar tempestades de broadcast, tornando a rede ineficiente e, em casos extremos, levando à indisponibilidade da rede.

A função do loop guard é detectar e evitar a criação de loops de camada 2, desativando automaticamente portas que se tornam suspeitas de fazer parte de um loop. Normalmente, o loop guard é aplicado em portas que podem ser propensas a loops, como aquelas que estão conectadas a outros switches.

Aqui estão algumas sugestões de onde aplicar o loop guard em um switch, justificando cada escolha:

1. **Portas de Uplink (Conexão entre Switches):** É sensato aplicar o loop guard em portas de uplink, especialmente aquelas que conectam switches entre si. Isso ocorre porque os loops geralmente ocorrem quando há múltiplos caminhos entre switches. Se um loop ocorrer nessa conexão, pode se espalhar por toda a rede. Ao aplicar o loop guard nas portas de uplink, você ajuda a garantir que qualquer loop seja rapidamente identificado e a porta seja desativada para evitar danos à rede.
2. **Portas em Redes com Configurações Dinâmicas (STP, RSTP, etc.):** Em redes onde estão sendo utilizados protocolos de spanning tree, como STP (Spanning Tree Protocol) ou RSTP (Rapid Spanning Tree Protocol), faz sentido aplicar loop guard em todas as portas configuradas com esses protocolos. Isso ajuda a complementar as funcionalidades de spanning tree, melhorando a detecção de loops.

EXAME NORMAL 2019

Esboço da resolução

1. VLAN10sede: 100.100.100.0/26 (1-62)
VLAN20sede: 100.100.100.96/27 (97-126)
VLAN30sede: 100.100.100.80/28 (81-94)
VLAN30filial2: 100.100.100.64/28 (65-78)
VLAN99sede: 192.168.1.0/24
R1-R2: 192.168.12.0/24
R2-R3: 192.168.23.0/24
R1-R4: 192.168.14.0/24
2. R1(config)#username R4 password RAS
R1(config)#mpls label range 100 199
R1(config)#interface Loopback0
R1(config-if)#ip address 1.1.1.1 255.255.255.255
R1(config-if)#interface Multilink1
R1(config-if)#ip address 192.168.14.1 255.255.255.0
R1(config-if)#compress mppc
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R1 password RAS
R1(config-if)#ppp multilink
R1(config-if)#ppp multilink group 1
R1(config-if)#interface Ethernet0/0
R1(config-if)#no shutdown
R1(config-if)#interface Ethernet0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#xconnect 3.3.3.3 10 encapsulation mpls
R1(config-subif)#interface Ethernet0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 100.100.100.126 255.255.255.224
R1(config-subif)#interface Ethernet0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#xconnect 3.3.3.3 33 encapsulation mpls
R1(config-subif)#interface Ethernet0/0.99
R1(config-subif)#encapsulation dot1Q 99 native
R1(config-subif)#ip address 192.168.1.11 255.255.255.0
R1(config-subif)#interface Serial2/0
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#interface Serial2/1
R1(config-if)#encapsulation frame-relay

```

R1(config-if)#frame-relay interface-dlci 102 ppp Virtual-Template1
R1(config-if)#no shutdown
R1(config-if)#interface Serial2/2
R1(config-if)#encapsulation frame-relay
R1(config-if)#frame-relay interface-dlci 304 ppp Virtual-Template1
R1(config-if)#no shutdown
R1(config-if)#interface Virtual-Template1
R1(config-if)# ppp multilink
R1(config-if)#ppp multilink group 1
R1(config-if)#router ospf 1
R1(config-router)#mpls ldp autoconfig
R1(config-router)#network 1.1.1.1 0.0.0.0 area 0
R1(config-router)#network 100.100.100.96 0.0.0.31 area 0
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.12.0 0.0.0.255 area 0
R1(config-router)#network 192.168.14.0 0.0.0.255 area 0

```



3. SW1(config)#ip routing

```

SW1(config-if)#interface Loopback0
SW1(config-if)#ip address 5.5.5.5 255.255.255.255
SW1(config-if)#interface range Ethernet0/0 - 2
SW1(config-if-range)#switchport trunk encapsulation dot1q
SW1(config-if-range)#switchport trunk native vlan 99
SW1(config-if-range)#switchport mode trunk
SW1(config-if-range)#interface Ethernet2/0
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
SW1(config-if)#interface Ethernet2/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#interface Vlan10
SW1(config-if)#ip address 100.100.100.62 255.255.255.192
SW1(config-if)#no shutdown
SW1(config-if)#interface Vlan30
SW1(config-if)#ip address 100.100.100.94 255.255.255.240
SW1(config-if)#no shutdown
SW1(config-if)#interface Vlan99
SW1(config-if)#ip address 192.168.1.1 255.255.255.0
SW1(config-if)#no shutdown

```

```
SW1(config-if)#router ospf 1
SW1(config-router)#network 5.5.5.5 0.0.0.0 area 0
SW1(config-router)#network 100.100.100.0 0.0.0.63 area 0
SW1(config-router)#network 100.100.100.80 0.0.0.15 area 0
SW1(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

4. Dado que um circuito AToM transporta quadros nível 2 sobre uma rede MPLS, as interfaces nos extremos do circuito não têm endereçamento IP. Desta forma, o encaminhamento da VLAN 20 teria que passar de R1 para SW1, permitindo existir mais um circuito AToM a partir de R1.
5. Root Bridge: SW5, porque apresenta a prioridade mais baixa (16384).
Portas bloqueadas:
 - a. SW3.E0/1, SW3.E0/2
As portas adjacentes dos segmentos destas interfaces fazem parte de bridges com identificadores (prioridade+mac) inferiores.
 - b. SW1.E0/1, SW1.E0/2
As portas adjacentes dos segmentos destas interfaces têm custos inferiores para a root bridge.
 - c. SW4.E0/0
Como SW5 é root, todas as portas são designated. Como só pode haver uma designated port por segmento, esta porta terá que bloquear porque não é root port.
6. Os comandos estabelecem a segurança na porta SW1.E2/0, definindo o primeiro endereço aprendido nessa porta como seguro. Assumindo a configuração por omissão (switchport port-security maximum 1), qualquer outro endereço irá ser considerado como quebra de segurança.
7. PC4-VLAN10
 (sem marcação)
 SW2
 (com marcação VID=10)


SW5

 (com marcação VID=10)

SW4

 (com marcação VID=10)

SW1

 (sem marcação)

SW4

 (sem marcação)

SW5

 (sem marcação)

SW2

 (sem marcação)

R1

 (com marcação DLCI=102 ou DLCI=304)

FR1

 (com marcação DLCI=201 ou DLCI=403)

R4

 (com marcação VID=30)

SW7

 (sem marcação)

PC8-VLAN30

6 de 6

8. Link Origem Destino Labels MPLS

R1-R2 PC2-VLAN20 (100.100.100.97) PC9-VLAN30 (100.100.100.83)
203+301

R1-R2 PC9-VLAN30 (100.100.100.83) PC2-VLAN20 (100.100.100.97) 101

R2-R3 PC1-VLAN10 (100.100.100.1) PC7-VLAN10 (100.100.100.3) 300

R2-R3 PC7-VLAN10 (100.100.100.3) PC1-VLAN10 (100.100.100.1) 200+100

9. A monitorização de tráfego faz-se recorrendo aos protocolos SPAN e RSPAN, que

permitem a monitorização de portas, respetivamente, locais e remotas. Para isso, os routers poderiam ser substituídos por switch-routers, por forma a poder utilizar estes protocolos. Exemplo de uma sessão SPAN, porta monitorizada SR.f0/5, porta observadora SR.f0/6:

```
SR(config)#monitor session 1 source int f0/5 both
SR(config)#monitor session 1 destination int f0/6 encapsulation replicate
```

10. Atualmente, o acesso Wi-Fi é realizado por dispositivos alimentados por bateria, o que impede que sejam utilizadas grandes potências de transmissão. Pela mesma razão, muitos destes dispositivos são utilizados junto ao corpo humano, o que se traduz numa preocupação crescente com dispositivos de baixa

radiação. Por outro lado, em ambientes urbanos de grande densidade populacional, aumentos nas potências de transmissão potenciam débitos inferiores devido ao aumento das interferências pelos APs vizinhos. Desta forma, a utilização de APs dual-band, nas bandas em 2.4GHz e 5GHz, permitirá que clientes próximos possam utilizar a banda dos 5GHz, por ser menos propensa a interferências ao mesmo tempo que disponibiliza um número maior de

canais não-sobrepostos. Pelo contrário, dada a propagação na banda dos 2.4GHz

ser superior, em especial na presença de obstáculos, torna-se a escolha ideal em situações de baixa concentração de APs para clientes distantes.

```
SW5(config)#interface Ethernet0/0
SW5(config-if)#spanning-tree cost 99
SW5(config)#interface Ethernet0/1
SW5(config-if)#spanning-tree cost 101
SW4(config)#interface Ethernet0/3
SW4(config-if)#spanning-tree port-priority 64
```

Q-in-Q

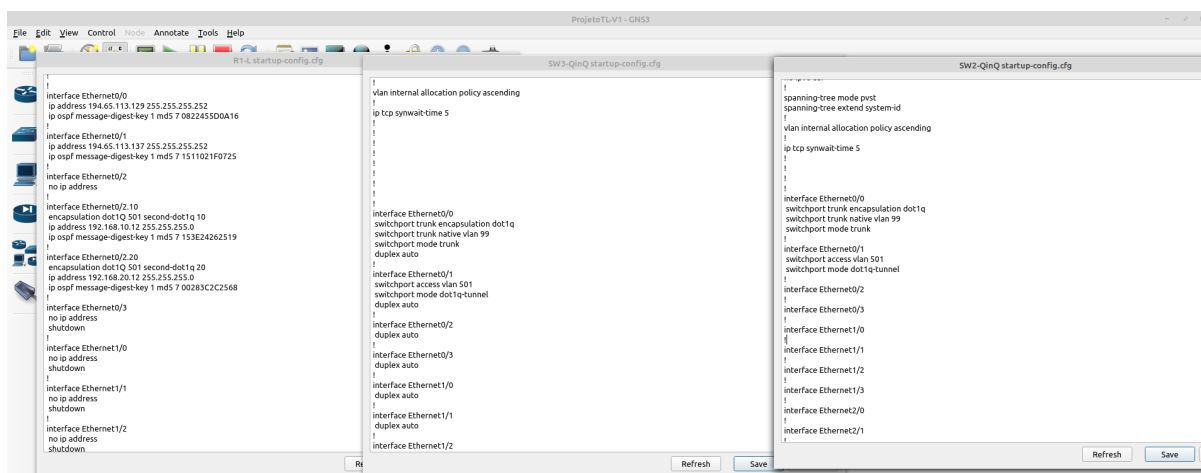
A ligação R5-R6 ser suportada em QinQ tem as seguintes vantagens e inconvenientes:

- **Vantagens:**

- Permite transportar múltiplas VLANs sobre uma única ligação Ethernet, sem conflitos de identificadores de VLAN.
- Simplifica a configuração e a gestão da rede, pois não é necessário definir subinterfaces ou túneis para cada VLAN.
- Aumenta a segurança e a privacidade dos dados, pois as VLANs são encapsuladas com uma tag adicional que as identifica como pertencentes a um determinado cliente ou serviço.

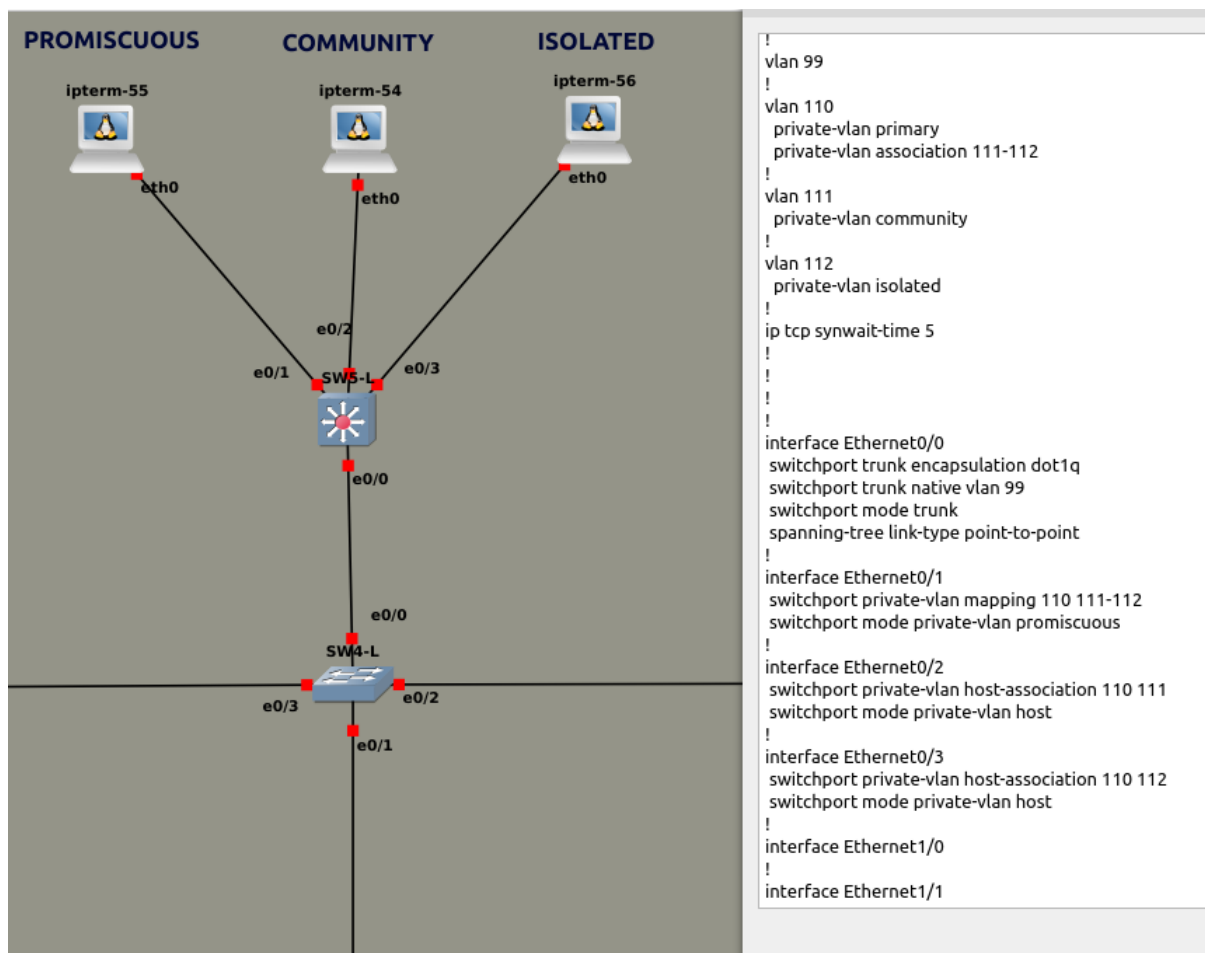
- **Inconvenientes:**

- Aumenta o tamanho dos quadros Ethernet, o que pode causar problemas de fragmentação ou MTU mismatch.
- Requer equipamentos compatíveis com QinQ nas extremidades da ligação, o que pode limitar a interoperabilidade ou aumentar os custos.
- Reduz a visibilidade e o controlo sobre as VLANs transportadas, pois as tags internas não são visíveis para os equipamentos intermediários.



PVLAN

```
vlan 99
!
vlan 110
private-vlan primary
private-vlan association 111-112
!
vlan 111
private-vlan community
!
vlan 112
private-vlan isolated
!
ip tcp synwait-time 5
!
!
!
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport trunk native vlan 99
switchport mode trunk
spanning-tree link-type point-to-point
!
interface Ethernet0/1
switchport private-vlan mapping 110 111-112
switchport mode private-vlan promiscuous
!
interface Ethernet0/2
switchport private-vlan host-association 110 111
switchport mode private-vlan host
!
interface Ethernet0/3
switchport private-vlan host-association 110 112
switchport mode private-vlan host
!
```



Ao configurar o switch SW6 com o comando `vtp mode client` :

1. O switch atua como cliente VTP.
2. Recebe informações de VLAN do servidor VTP.
3. Não pode adicionar, remover ou modificar VLANs localmente.
4. Não propaga suas próprias informações de VLAN para outros switches.

Ao aplicar `vtp mode server` no switch SW6:

1. O switch opera como um servidor VTP.
2. Ele pode adicionar, modificar ou remover VLANs.

3. Propaga essas alterações para outros switches VTP na mesma área.
4. Mantém consistência de informações de VLAN usando uma revisão de VTP.
5. Gere globalmente as VLANs na rede VTP.

Ao usar `vtp mode transparent` no switch SW6:

1. Opera em modo VTP transparente.
2. Encaminha anúncios VTP, mas não modifica localmente VLANs com base neles.
3. Preserva VLANs localmente configuradas.
4. Mantém uma revisão de VTP própria.
5. Permite controle local independente sobre VLANs, sem afetar outros switches VTP.

Ao configurar `spanning-tree guard root` na interface GigabitEthernet0/0 do switch SW2:

1. Ativa o Root Guard na interface;
2. Impede que a interface se torne a raiz da Spanning-Tree;
3. Protege contra ataques de spoofing;
4. Mantém a integridade da topologia da Spanning-Tree.

Além disso, protege contra BPDUs de switches vizinhos que indicam uma raiz mais preferível, evitando alterações indesejadas na topologia e fornecendo segurança contra manipulação da raiz.

Quais as razões para se utilizar a inibição da difusão periódica do SSID de uma rede WiFi?

A inibição da difusão periódica do SSID (Service Set Identifier) numa rede Wi-Fi, também conhecida como "SSID broadcasting", pode ser utilizada por algumas razões específicas, embora tenha algumas desvantagens. Aqui estão algumas razões comuns para desativar a difusão do SSID:

1. Redução de Visibilidade:

- Ocultar o SSID pode reduzir a visibilidade da rede para utilizadores casuais, tornando-a menos óbvia ao explorar redes disponíveis.

2. Segurança Básica:

- Alguns administradores de rede acreditam que ocultar o SSID fornece uma camada mínima de segurança básica, uma vez que torna a rede menos visível para utilizadores não autorizados.

3. Prevenção de Conexões Indesejadas:

- Ao ocultar o SSID, é possível evitar que dispositivos se conectem automaticamente à rede, a menos que o SSID correto seja conhecido e configurado manualmente.

4. Desafio Adicional para Invasores:

- Ocultar o SSID pode adicionar uma camada mínima de complexidade para invasores, uma vez que eles precisarão descobrir o SSID antes de tentar aceder à rede.

8. Qual a grande diferença de operação entre a atual norma WiFi 6 e a futura norma WiFi 7?

A grande diferença de operação entre a atual norma Wi-Fi 6 e a futura norma Wi-Fi 7 é a velocidade e a capacidade de transmissão. A norma Wi-Fi 7 promete velocidades ainda mais rápidas, com taxas de transferência de dados de vários gigabits por segundo. Além disso, a norma Wi-Fi 7 também deve oferecer uma maior capacidade de conexão simultânea, permitindo que mais dispositivos se conectem à rede sem comprometer o desempenho.

1. `SW4(config)#interface Ethernet0/3` : Este comando entra no modo de configuração para a interface Ethernet0/3.
2. `SW4(config-if)#spanning-tree port-priority 64` : Este comando define a prioridade da porta STP para a interface especificada como 64. A prioridade da porta STP é um valor que determina a prioridade de uma porta na seleção da porta raiz. Um valor mais baixo indica uma prioridade mais alta. Neste caso, a prioridade está definida como 64.

Lembre-se de que o STP é um protocolo usado para prevenir loops em redes Ethernet, selecionando dinamicamente uma ponte raiz e criando uma topologia sem loops. A prioridade da porta é um dos fatores considerados no processo de seleção da porta raiz. A prioridade padrão da porta é 128, então definir como 64 torna essa porta mais propensa a ser selecionada como a porta raiz, assumindo que outros fatores sejam iguais.

O comando "`spanning-tree bpduguard enable`" ativa o BPDU Guard. Esse recurso protege contra loops na rede, desativando automaticamente a interface se detectar Bridge Protocol Data Units (BPDUs) não autorizadas. Isso evita problemas de loop causados por dispositivos não autorizados e ajuda a manter a estabilidade da rede. O administrador deve intervir para resolver a situação, identificar a causa e, se necessário, reativar a interface manualmente. Essa configuração é útil em interfaces de acesso para prevenir conexões não autorizadas que poderiam afetar a topologia da rede.

1. **Refira-se aos efeitos decorrentes da aplicação dos seguintes comandos no switch SW6:**

`SW6(config)#interface Ethernet 2/0`

`SW6(config-if)#switchport port-security`

`SW6(config-if)#switchport port-security violation shutdown`

`SW6(config-if)#switchport port-security maximum 1`

`SW6(config-if)#switchport port-security mac-address sticky`


```
SW6(config-if)#end  
SW6#copy run start
```

Os comandos fornecidos configuram a interface Ethernet 2/0 do switch SW6 com recursos de segurança de porta. Aqui estão os efeitos decorrentes desses comandos:

1. Configuração da Interface:

- `SW6(config)#interface Ethernet 2/0` : Move o prompt de configuração para a interface Ethernet 2/0.

2. Ativação do Port Security:

- `SW6(config-if)#switchport port-security` : Ativa o recurso de segurança de porta na interface Ethernet 2/0.

3. Ação em Violation (Violação):

- `SW6(config-if)#switchport port-security violation shutdown` : Define a ação a ser tomada em caso de violação como "shutdown", desativando a interface em caso de violação de segurança de porta.

4. Número Máximo de Endereços MAC Permitidos:

- `SW6(config-if)#switchport port-security maximum 1` : Especifica que apenas um endereço MAC é permitido na interface. Qualquer tentativa de conectar mais de um dispositivo resultará em uma violação.

5. Aprendizado Automático de Endereços MAC:

- `SW6(config-if)#switchport port-security mac-address sticky` : Ativa o aprendizado automático de endereços MAC (sticky learning), onde o primeiro endereço MAC que é visto na interface é considerado seguro e adicionado à tabela de endereços MAC.

Porque é imprudente reduzir (muito) a periodicidade de transmissão dos quadros beacon de uma rede WiFi?

Reduzir muito a periodicidade dos quadros Beacon em uma rede Wi-Fi pode causar problemas como:

1. **Consumo excessivo de bateria em dispositivos móveis**, uma vez que exige que os dispositivos façam *scans* com mais frequência.
2. **Atrasos na descoberta de redes Wi-Fi por dispositivos e na associação a uma rede específica**, podendo levar a uma experiência de utilização mais lenta e menos eficiente.
3. **Problemas em redes de voz e vídeo**, aumentando a latência e prejudicando a qualidade.
4. **Maior probabilidade de colisões**, podendo levar a congestionamento da rede.
5. **Impacto na capacidade da rede**: Reduz o tempo disponível para a transmissão de dados efetivos.

Qual a grande diferença entre as normas WiFi 6 e WiFi 6E?

A principal diferença entre as normas Wi-Fi 6 (também conhecido como 802.11ax) e Wi-Fi 6E está relacionada ao espectro de frequência que cada uma utiliza:

1. Wi-Fi 6 (802.11ax):

- O Wi-Fi 6 opera principalmente nas faixas de frequência de 2,4 GHz e 5 GHz, que já eram utilizadas por padrões anteriores do Wi-Fi.

2. Wi-Fi 6E:

- O Wi-Fi 6E, por sua vez, estende o espectro de frequência disponível para incluir a faixa de 6 GHz. Isso proporciona mais canais disponíveis, reduzindo a interferência e melhorando a largura de banda disponível para dispositivos Wi-Fi.

Em resumo, a adição da faixa de 6 GHz é a característica distintiva do Wi-Fi 6E em relação ao Wi-Fi 6 padrão. Essa expansão de espectro oferece mais capacidade para comunicação sem fio,

permitindo um desempenho aprimorado e uma melhor experiência para os utilizadores, especialmente em ambientes com muitos dispositivos conectados. O Wi-Fi 6E é uma extensão do Wi-Fi 6, aproveitando a nova faixa de frequência para melhorar a eficiência e a qualidade da conexão Wi-Fi.

Em Wi-Fi, quais as razões para a inibição da difusão periódica dos SSID nos quadros beacon não ser considerada, por si só, um mecanismo de segurança?

Desativar a difusão do SSID nos quadros beacon em redes Wi-Fi não é considerado um mecanismo de segurança eficaz por várias razões:

1. **Descoberta possível:** O SSID ainda pode ser descoberto por meio de monitoramento passivo ou quando dispositivos se reconectam.
2. **Sniffing e descryptografia passiva:** Ferramentas de *sniffing* podem capturar quadros de gestão, expondo informações sobre a rede, como o SSID.
3. **Aumento da complexidade:** Desativar a difusão do SSID pode complicar a gestão da rede e afetar a experiência do utilizador.
4. **Falta de proteção contra ataques avançados:** Ataques de desautenticação podem revelar a rede, mesmo com a difusão do SSID desativada.

EXAME NORMAL 2018

R1(config)#username R4 password RAS
R1(config)#mpls label range 100 199

```

R1(config)#interface Loopback0
R1(config-if)#ip address 1.1.1.1 255.255.255.255
R1(config-if)#interface Ethernet0/0
R1(config-if)#no shutdown
R1(config-if)#interface Ethernet0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 100.100.100.62 255.255.255.192
R1(config-subif)#interface Ethernet0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 100.100.100.126 255.255.255.248
R1(config-subif)#interface Ethernet0/0.99
R1(config-subif)#encapsulation dot1Q 99 native
R1(config-subif)#ip address 192.168.1.11 255.255.255.0
R1(config-subif)#interface Ethernet0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#xconnect 3.3.3.3 33 encapsulation mpls
R1(config-subif)#interface Serial2/0
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#interface Serial2/1
R1(config-if)#encapsulation frame-relay
R1(config-if)#no shutdown
R1(config-if)#interface Serial2/1.102 multipoint
R1(config-subif)#frame-relay interface-dlci 102 ppp Virtual-
Template1
R1(config-subif)#interface Virtual-Template1
R1(config-if)#ip address 192.168.14.1 255.255.255.0
R1(config-if)#ip tcp header-compression
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R1 password RAS
R1(config-if)#router ospf 1
R1(config-router)#mpls ldp autoconfig
R1(config-router)#network 1.1.1.1 0.0.0.0 area 0
R1(config-router)#network 100.100.100.0 0.0.0.63 area 0
R1(config-router)#network 100.100.100.120 0.0.0.7 area 0
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.12.0 0.0.0.255 area 0
R1(config-router)#network 192.168.14.0 0.0.0.255 area 0

```

```

3. SW1(config)#ip routing
SW1(config-if)#interface Loopback0
SW1(config-if)#ip address 5.5.5.5 255.255.255.255
SW1(config-if)#interface range Ethernet0/0 - 2
SW1(config-if-range)#switchport trunk encapsulation dot1q
SW1(config-if-range)#switchport trunk native vlan 99
SW1(config-if-range)#switchport mode trunk
SW1(config-if-range)#interface Ethernet2/0
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
SW1(config-if)#interface Ethernet2/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#interface Vlan30
SW1(config-if)# ip address 100.100.100.94 255.255.255.240
SW1(config-if)#no shutdown
SW1(config-if)#interface Vlan99
SW1(config-if)#ip address 192.168.1.1 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#router ospf 1
SW1(config-router)#network 5.5.5.5 0.0.0.0 area 0
SW1(config-router)#network 100.100.100.80 0.0.0.15 area 0
SW1(config-router)#network 192.168.1.0 0.0.0.255 area 0

```

Indique as vantagens na existência de um circuito AToM entre R1-R3 na VLAN 30.

O circuito AToM permite transportar quadros nível 2 sobre uma rede MPLS. Desta forma, a VLAN 30 da filial 1 corresponde à VLAN 30 da sede, colocando o PC7-VLAN30 "dentro" da sede.

No router R4 deverá optar-se pela utilização de subinterfaces frame-relay? Se sim, de que tipo? Justifique.

Dado que a topologia só apresenta um PVC, a solução mais óbvia passará por ligar directamente a interface física de R4 a este circuito virtual. No entanto, não haverá qualquer entrave à utilização quer de um sub-interface point-to-point, quer de um sub-interface multipoint, sendo necessário identificar o respectivo DLCI a atribuir à sub-interface.

PORTAS BLOQUEADAS - JUSTIFICAÇÃO

Root Bridge: SW4, porque apresenta a prioridade mais baixa (16384).

Portas bloqueadas:

a. SW3.E0/0, SW3.E0/3

As portas adjacentes dos segmentos destas interfaces fazem parte de bridges com identificadores (prioridade+mac) inferiores.

b. SW2.E0/1, SW2.E0/2

As portas adjacentes dos segmentos destas interfaces têm custos inferiores para a root bridge.

c. SW5.E0/0

Como SW4 é root, todas as portas são designated.

Como só pode haver uma designated port por segmento, esta porta terá que bloquear porque não é root port.

Comente sobre a aplicação da protecção *loop guard* nas portas dum switch que tem funções de *root bridge*.

Loop Guard é uma medida de segurança usada para evitar loops em redes Ethernet. Ao aplicá-lo num *switch* que funciona como *root bridge*, focamos em *designated ports* para evitar inconsistências de estado. *Loop Guard* protege contra falhas de BPDUs, colocando a porta em estado inconsistente se deixar de receber essas mensagens. É implementado cautelosamente em ambientes dinâmicos e contribui para a convergência rápida do Spanning Tree, melhorando a estabilidade da rede.

Indique, justificando, em que portas do *switch* SW3 faz sentido aplicar a segurança *loop guard*.

É recomendado usar segurança *loop guard* em todas as portas conectadas a outros switches. Ativar a *loop guard* entre switches ajuda a evitar a propagação de loops na rede. Além disso, em redes onde são usados STP ou RSTP, faz sentido aplicar *loop guard* nas portas que usam esses protocolos, uma vez que ajudam a complementar as funcionalidades do STP, melhorando a deteção de *loops*.

Indique as alterações necessárias na presente topologia para a existência de um circuito AToM entre R1-R3 na VLAN 20.

Dado que um circuito AToM transporta quadros nível 2 sobre uma rede MPLS, as interfaces nos extremos do circuito não têm endereçamento IP. Desta forma, o encaminhamento da VLAN 20 teria que passar de R1 para SW1, permitindo existir mais um circuito AToM a partir de R1.

Refira-se aos efeitos decorrentes da aplicação do seguinte comando no switch-router SW1:

SW1(config)#interface Ethernet2/0

SW1(config-if)#switchport port-security

SW1(config-if)#switchport port-security mac-address sticky

Os comandos estabelecem a segurança na porta SW1.E2/0, definindo o primeiro endereço aprendido nessa porta como seguro. Assumindo a configuração por omissão (switchport port-security maximum 1), qualquer outro endereço irá ser considerado como quebra de segurança.

Indique como poderia monitorizar o tráfego da alínea anterior, i.e., nos links R1-R2 e R2-R3.

A monitorização de tráfego faz-se recorrendo aos protocolos SPAN e RSPAN, que permitem a monitorização de portas, respetivamente, locais e remotas. Para isso, os routers poderiam ser substituídos por switch-routers, por forma a poder utilizar estes protocolos. Exemplo de uma sessão SPAN, porta monitorizada SR.f0/5, porta observadora SR.f0/6:

```
SR(config)#monitor session 1 source int f0/5 both
SR(config)#monitor session 1 destination int f0/6 encapsulation
replicate
```

Indique, justificando, em que portas do switch-router SR1 faz sentido aplicar a segurança BPDU guard.

O BPDU guard é aplicado em portas de switch para evitar loops de camada 2. É geralmente configurado em portas de acesso de utilizador, onde dispositivos finais estão conectados (PCS ou

routers). Também pode ser usado em portas desabilitadas para o STP, onde a presença de BPDUs não é necessária. Evitar a recepção de BPDUs nessas portas ajuda a prevenir loops de camada 2, garantindo a estabilidade da rede. Ao receber um quadro BPDU, numa porta com o BPDU guard ativo, o comportamento típico do BPDU guard é desabilitar imediatamente a porta na qual o quadro BPDU foi recebido. Isso é feito para isolar rapidamente o dispositivo que gerou o BPDU, impedindo a propagação de BPDUs indesejados e evitando a possível criação de loops na rede.

No que concerne ao alcance, como se comporta a recente norma WiFi 6 em comparação com a anterior norma WiFi 5?

No que diz respeito ao alcance, a recente norma WiFi 6 se comporta de forma semelhante à norma WiFi 5 anterior. Ambas as normas têm um alcance semelhante, que depende de fatores como a potência do roteador e a interferência de outros dispositivos.

Apresente uma forma de obter o SSID de uma rede WiFi cuja difusão periódica, nos quadros beacon, tenha sido inibida.

Para obter o SSID de uma rede WiFi cuja difusão nos quadros beacon tenha sido inibida, uma forma é utilizar ferramentas de análise de pacotes, como o Wireshark. Essas ferramentas permitem capturar e analisar o tráfego de rede, incluindo os quadros beacon. Ao examinar os quadros capturados, é possível identificar o SSID da rede oculta.