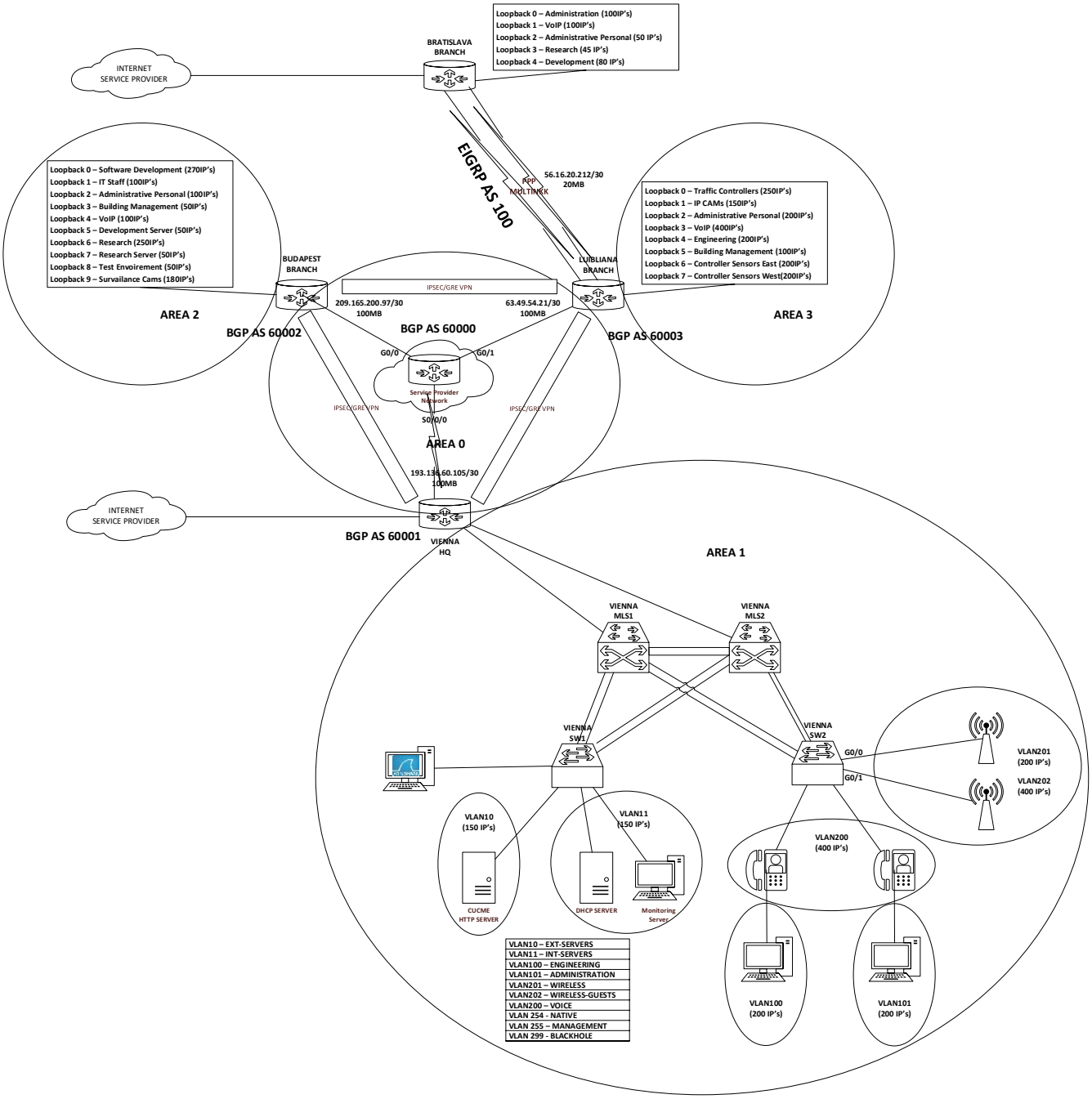
Topologia:



Nota: Garanta que o *router* utilizado para **Vienna** é um **c2911.**

Esquema de Endereçamento:

1. A proposta de endereçamento deve estar contida na gama 172.19.0.0/18
2. A proposta de endereçamento IPv6 deve estar contida na gama 1000::/58, devendo ser utilizado 64 bits para identificar as máquinas

3. Deve ser possível realizar sumarização de endereços em todas as localizações (Bratislava, Liubliana, Budapest e Vienna), com o objetivo de simplificar as tabelas de *routing*
4. Preencher uma Tabela de Endereçamento Rede semelhante ao Anexo I (deverá ser entregue na apresentação do trabalho)
5. Preencher uma Tabela de Interfaces semelhante ao Anexo II (deverá ser entregue na apresentação do trabalho)

Configurações:

1. Montar a topologia física
2. Configurar em todos os equipamentos ativos de rede os seguintes parâmetros:
   a. Nome dos equipamentos;
   b. Um utilizador com privilégios de administrador (privilege 15) e com o username cisco e a password class
   c. Restringir o acesso à consola apenas ao utilizador criado anteriormente;
   d. Restringir o acesso ao terminal virtual (VTY) apenas pelo protocolo SSH e ao utilizador criado anteriormente;
   e. Construir tabelas de hosts, utilizando apenas os endereços dos interfaces que interligam os routers e os endereços de gestão dos switchs;
   f. Configurar um banner com a seguinte message of the day "Acesso Restrito a Utilizadores Autorizados" apenas nos routers;
   g. Configurar um banner de login com a seguinte mensagem "Efetue um backup de segurança antes de efetuar alterações";
   h. Garante que todas as passwords armazenadas nos equipamentos estão encriptadas.
3. Configurar os interfaces:
   a. Aplicar os endereços IPv4/IPv6, mascaras/prefixos e descrições de acordo com os dados preenchidos na tabela requisitada anteriormente;
   b. Configurar o bandwidth de acordo com o apresentado na topologia.
   c. Os interfaces que se encontram conectados à Internet deverão receber as configurações de rede IPv4 dinamicamente, e devem ser configurados com o endereço IPv6 2001::/64 estaticamente.
   d. A ligação entre Liubliana e Bratislava é realizada através de uma conexão PPP Multilink com as seguintes carecteristicas
      i. Autenticação CHAP
      ii. Compression Predictor
      iii. Quality 80%;
   e. Configurar as ligações dos MLS-Vienna ao router Vienna como routed e atribuir o endereços especificados.
   f. Configurar os SVI nos switches MLSx-Vienna garantindo:
      i. Resiliência através da configuração de HSRP com as seguintes parametrizações:
         1. O MLS1-Vienna é o gateway active pelas VLANs 10, 11 e 255 e o standby das VLANs 100, 101, 200, 201 e 202;
         2. O MLS2-Vienna é o gateway active pelas VLANs 100, 101, 200, 201 e 202 e o standby das VLANs 10, 11 e 255;
         3. Aos gateways virtuais das diferentes VLANs deverá ser atribuído o último endereço disponível na gama onde se encontram.
   g. Todos os links entre os switchs de Vienna devem ser configurados como etherchannels L2.

Antes de avançar verifique a conectividade ponto a ponto de todos os links.

4. Depois de analisar a tabela de routing de Vienna e de Bratislava (garantir que o interface ligado a Internet já recebeu as configurações de rede), torne a rota default permanente configurando uma rota estática default.
   a. Verifique a conetividades destes equipamentos à Internet.
5. Configurar o protocolo de routing BGP em Vienna, Liubliana e Budapest apenas para estabelecer vizinhança com o Service Provider, utilizando os AS indicados.
6. Configurar os túneis GRE e protege-los com IPSEC utilizando os seguintes parâmetros:
   a. Autenticação: PSK
      i. Vienna-Liubliana - ViLiu12345
      ii. Vienna-Budapest - ViBuda12345
      iii. Budapest-Liubliana – BudaLiu12345
   b. Encriptação: 3DES
   c. Integridade: SHA
   d. Diffie-Hellman: 5
   e. Implementação de segurança: ESP
   f. Utilize redes /30 dentro da gama de endereçamento 10.0.0.0/24 cada um dos túneis.

Antes de avançar verifique a conectividade ponto a ponto de todos os túneis.

7. Configurar OSPF v2/v3 como o protocolo de routing dinâmico, garantindo que todas as localizações conseguem alcançar todos os destinos. O protocolo deverá redistribuir a rota default desde o HQ e as rotas EIGRP AS 100 desde Liubliana. As rotas redistribuídas devem atualizar a métrica ao longo da rede OSPF.
8. Todas as ligações OSPF dentro da área 0 devem ser autenticadas com message-digest e as mensagens de hello devem ser enviadas no dobro do período default.
9. Configurar EIGRP para o AS 100 redistribuindo a rota default e todas as rotas OSPF. Garantir que o EIGRP funciona como um protocolos classless anunciando as rotas sem sumarização automática.
10. O protocolo EIGRP deve utilizar mensagens autenticadas.
11. Configurar sumarização manual em Bratislava para o protocolo EIGRP e no OSPF em todos os ABRs.
12. Impedir que updades de routing sejam transmitidos em todos os interface que não necessitem deles.
13. A ligação entre Budapest e Liubliana deve ser apenas utilizada como backup, garantindo que todo o trafego passa por Vienna, enquanto os links estiverem ativos, e que em caso de disrupção de conectividade e trafego circula por Liubliana ou Budapest até alcançar Vienna. Pode recorrer a encaminhamento estático, ou á alteração das métricas do OSPF.
14. A ligação entre Vienna-HQ e o MLS1 deve ser utilizada como primária e a ligação entre Vienna-HQ e o MLS2 deve ser utilizada como backup.

Antes de avançar verifique se as tabelas de routing receberam os updates esperados e se existe conectividade entre todos os pontos.

15. Configurar nos switchs de Vienna as seguintes VLAN:
   a. VLAN 10 nome External_Servers
   b. VLAN 11 nome Internal_Serers
   c. VLAN 200 nome Voice
   d. VLAN 100 nome Engineering

e. VLAN 101 nome Administration
f. VLAN 255 nome Management
g. VLAN 254 nome Native
h. VLAN 299 nome BlackHole
i. VLAN 201 nome Wireless
j. VLAN 202 nome Wireless-Guest

16. Configurar os interfaces dos switchs SWx-Vienna, respetivos a VLAN Management, possibilitando desta forma a administração remota dos mesmos.
17. Configurar o default gateway dos switchs SWx-Vienna para o endereço virtual do HSRP configurado para a VLAN Management.
18. Desactivar o DTP (Dynamic Trunking Protocol) em todos os interfaces dos switchs.
19. Configurar os trunks em todos os Port-Channels:
    a. VLAN nativa 254;
    b. Negar a passagem da VLAN BlackHole.
20. Configurar os interfaces dos switch como acesso de acordo com o seguinte esquema:
    a. SW1-Vienna
        i. Interface FastEthernet 0/5 ao 0/14:
            1. Acesso à VLAN10;
            2. Permite apenas um mac-address por porta;
            3. Aprende dinamicamente os mac-address;
            4. Em caso de violação o interface deve desligar-se.
        ii. ii. Interface FastEthernet 0/15 ao 0/26:
            1. Acesso à VLAN11;
            2. Permite apenas um mac-address por porta;
            3. Aprende dinamicamente os mac-address;
            4. Em caso de violação o interface deve desligar-se.
        iii. Os restantes interface que não estejam a ser utilizados devem ser desativadas e colocadas na VLAN 299
    b. b. SW2-Vienna
        i. Interface FastEthernet 0/5 ao 0/14:
            1. Acesso à VLAN100;
            2. VLAN de voz VLAN200
            3. Permite apenas três mac-address por porta;
            4. Aprende dinamicamente os mac-address;
            5. Em caso de violação o interface deve apenas negar o acesso.
        ii. Interface FastEthernet 0/15 ao 0/24:
            1. Acesso à VLAN101;
            2. VLAN de voz VLAN200
            3. Permite apenas três mac-address por porta;
            4. Aprende dinamicamente os mac-address;
            5. Em caso de violação o interface deve apenas negar o acesso.
        iii. Interfaces G0/1 e G0/2:
            1. Configurar como trunk
            2. VLAN Nativa 254
            3. Permitir a passagem apenas das VLAN 201, 202, 254, 255
21. Configurar todas as portas de acesso do switch para não permitir mais do que 10 pedidos de DHCP por segundo.

22. Configurar ambos os switchs para não permitir DHCP Offers em nenhum interface com a exceção do interface onde se encontra o servidor se DHCP e os interfaces que interligam os switchs.
23. Configurar o router Vienna como master de NTP e todos os restantes equipamentos como slaves.
24. Configuração de Serviços:
    a. O servidor HTTP e o servidor DHCP são simulados por um router com dois interfaces FastEthernet. Cada um destes interfaces simula um interface de um servidor, devendo por isso ser configurado com o endereço IP respetivo da VLAN em que se encontra. Deve ser configurado através de rotas estáticas o default gateway dos servidores simulados.
    b. Configurar uma pool de endereços para as rede Voice, Enginnering, Administration, Wireless e Wireless-Guests cumprindo os requisitos definidos para a cada uma das redes:
        i. Endereço de rede
        ii. Máscara
        iii. *Gateway*
        iv. *DNS Server*: 172.16.208.66, 193.136.60.10 (apenas IPv4)
        v. Lease: 8 dias
        vi. Option 150 (apenas Voice)
    c. Os primeiros 5 e os últimos 5 endereços devem ser excluídos das pools.
    d. Configurar SNMP em todos os equipamentos ativos de redes:
        i. Snmpv2c com a *community string* cisco permitindo apenas leitura.
    e. Configurar um servidor de syslog em todos os equipamentos ativos de redes.
        i. Nível de registos – Informational
        ii. Servidor de logs – IP atribuído ao Monitoring Server.
    f. Configurar netflow em todos os routers:
        i. Version 9
        ii. Netflow colector - IP atribuído ao Monitoring Server
        iii. Ingress e Egress nos interface necessários
    g. Configurar um PC do laboratório como Servidor de Monitorização.
        i. Instalar a aplicação PRTG disponível neste link juntamente com a licença. http://172.16.208.100/Materiais/Files/CCNA4
        ii. Configurar os seguintes sensores no PRTG:
            1. Routers:
                a. Ping
                b. Syslog
                c. SNMP (Interfaces tunnel e GigabitEthernet [Ativas])
                d. Netflow (Interfaces tunnel e GigabitEthernet [Ativas])
            2. Switchs:
                a. Ping
                b. Syslog
                c. SNMP (Interfaces Etherchannel e routed ports)
            3. Access Points:
                a. Ping
                b. Syslog
                c. SNMP (interfaces radio)
            4. Internet:
                a. HTTP (www.google.com)

   h. Cisco Unified Call Manager Express (utilizando o *template* disponível)
      i. IP phone ligado à rede Engineering – extensão 1000
      ii. IP phone ligado à rede Administration – extensão 2000
   i. Configurar um *mirror* do tráfego *inbound* e *outbound* dos interfaces onde se encontram ligados os servidores para o interface onde se encontra ligado o WireShark.
      i. Configurar o WireShark para capturar trafego.

25. Efetuar as configurações necessárias para que todas as redes internas possam chegar a endereços na internet. (apenas IPv4)
26. Configurar NAT estático para permitir o acesso externo ao servidor HTTP. (apenas IPv4)
27. Configurar as seguintes regras de controlo de acesso:
   a. Nenhuma rede, com a exceção da rede IT STAFF (Budapes) e ADMINISTRATION (Vienna), podem comunicar com a rede INT_SERVERS e EXT_SERVERS (Vienna), as restantes redes apenas podem aceder aos serviços indicados por cada servidor.
   b. As redes VoIP não devem comunicar com a Internet.
   c. Com a exceção das diferentes redes Administration e Administrative Personal o acesso a internet apenas pode ser realizado por HTTP HTTPS, estando todos os restantes serviço na Internet bloqueado para os utilizadores que não fazem parte destes grupos.
   d. As redes Research e Development apenas podem comunicar entre elas e com os respetivos servidores independentemente da sua localização, assim como com a Internet. As redes administração podem iniciar comunicações com estas redes mas o contrário deve ser bloqueado.
   e. A rede Test Envoirement apenas pode ser acedida pelas redes Engineering
   f. A rede WIRELESS-GUEST apenas pode aceder a Internet.
   g. Apenas os as redes Management, Administration, os endereços atribuídos ao routers e a endereço do Monitoring Server podem aceder aos equipamentos por SSH
   h. Pedidos SNMP apenas devem ser permitidos ao endereço do Monitoring Server.

Academia Cisco ISEP Trabalho Prático
Connecting Networks 6.0

Localization	Description	Network IP Address	Network Mask Prefix
Budapest	Software Development	xxx.xxx.xxx.xxx	/xx
	“”	xxx.xxx.xxx.xxx	/xx
	“”	xxx.xxx.xxx.xxx	/xx
	“”	xxx.xxx.xxx.xxx	/xx
	Free Network Space	xxx.xxx.xxx.xxx	/xx
Budapest	Summarization Address	xxx.xxx.xxx.xxx	/xx
Liubliana	Traffic Controller	xxx.xxx.xxx.xxx	/xx
	“”	xxx.xxx.xxx.xxx	/xx
	“”	xxx.xxx.xxx.xxx	/xx
	“”	xxx.xxx.xxx.xxx	/xx
	Free Network Space	xxx.xxx.xxx.xxx	/xx
Liubliana	Summarization Address	xxx.xxx.xxx.xxx	/xx

Localization	Interface	IP Address	Prefix	Description
Budapest	Serial 0/0/0	xxx.xxx.xxx.xxx	/xx	Software Development
	Serial 0/0/1	xxx.xxx.xxx.xxx	/xx	“”
	LoopBack 0	xxx.xxx.xxx.xxx	/xx	“”
	LoopBack 1	xxx.xxx.xxx.xxx	/xx	“”
	…	xxx.xxx.xxx.xxx	/xx	“”
Liubliana	Serial 0/0/0	xxx.xxx.xxx.xxx	/xx	Traffic Controller
	Serial 0/0/1	xxx.xxx.xxx.xxx	/xx	“”
	LoopBack 0	xxx.xxx.xxx.xxx	/xx	“”
	LoopBack 1	xxx.xxx.xxx.xxx	/xx	“”
	…	xxx.xxx.xxx.xxx	/xx	“”

Cisco | Networking Academy®
Mind Wide Open™

Configuração do Service Provider Router:

```
hostname ISP
!
enable secret 5 $1$Pdb4$c6.xFo5g6EYs4NyCwS615.
!
ip domain name isp.com
ip host Vienna-HQ 193.136.60.105
ip host Liubliana-BR 63.49.54.21
ip host Budapest-BR 209.165.200.97
!
username cisco privilege 15 secret 5 $1$lphz$nMPUxTx/5ocpmMZHvQZia1
!
interface GigabitEthernet0/0
 description Connects to Budapest-BR
 bandwidth 100000
 ip address 209.165.200.98 255.255.255.252
 no shutdown
!
interface GigabitEthernet0/1
 description Connects to Luibliana-BR
 bandwidth 100000
 ip address 63.49.54.22 255.255.255.252
 no shutdown
!
interface Serial0/0/0
 description Connects to Vienna-HQ
 bandwidth 100000
 ip address 193.136.60.106 255.255.255.252
 clock rate 2000000
 no shutdown
!
router bgp 60000
 network 193.136.60.104 mask 255.255.255.252
 network 209.165.200.96 mask 255.255.255.252
 network 63.49.54.20 mask 255.255.255.252
 neighbor 193.136.60.105 remote-as 60001
 neighbor 209.165.200.97 remote-as 60002
 neighbor 63.54.49.21 remote-as 60003
!
alias exec r1 ssh -l cisco Vienna-HQ
alias exec r2 ssh -l cisco Liubliana-BR
alias exec r3 ssh -l cisco Budapest-BR
!
line vty 0 4
 login local
 transport input ssh
!
crypto key generate rsa modulus 1024 exportable
```

Template de configuração túnel GRE/IPSEC:

```
crypto isakmp policy policynumber
 encr encryption_algorithm
 authentication pre-share
 group diffie_hellman_group_number
crypto isakmp key Keystring address peer_public_address
!
crypto ipsec transform-set transform_set_name esp-3des esp-sha-hmac
!
crypto map crypto_map_name sequence_number ipsec-isakmp
 set peer peer_public_address
 set transform-set       transform_set_name
 match address crypto_acl_name
!
interface Tunnel0
 description tunnel_description
 ip address tunnel_address tunnel_mask_address
 tunnel source local_public_address
 tunnel destination remote_public_address
!
interface connect_to_the_public_address
crypto map crypto_map_name
!
ip access-list extended crypto_acl_name
 permit gre host local_public_address host remote_public_address
 deny   ip any any
```

Template de configuração CUCME:

```
!Configurações extra a efetuar no router que simula os servidores de dhcp e
!http
!
! Configurar a timezone correta (deve ser efetuado em todos os equipamentos)
clock timezone WET 0 0
clock summer-time WEST recurring last Sun Mar 1:00 last Sun Oct 2:00
!
ip dhcp pool VOICE
 network endereço_rede_voice mascara_rede_voice
 default-router endereço_gateway_voice
 dns-server xxx.xxx.xxx.xxx
 option 150 ip endereço_interface_servidor_http
 lease x
!
telephony-service
 max-ephones 64
 max-dn 128
 ip source-address endereço_interface_servidor_http port 2000
 system message mensagem_do_sistema
 cnf-file location flash:
 load 7912 CP7912080004SCCP080108A.sbin
 create cnf-files
!
ephone-dn  1
 number extensão
```

```
!
ephone-dn  2
 number extensão
!
!
ephone  1
 mac-address mac_address_ipphone1 (MMMM.MMMM.MMMM)
 type 7912
 button  1:1
!
ephone  2
 mac-address mac_address_ipphone2 (MMMM.MMMM.MMMM)
 type 7912
 button  1:2
!
ntp server endereço_ip_ntp_server
end
```

Antes de realizar as configurações deve carregar para a flash o ficheiro **CP7912080004SCCP080108A.sbin** que está disponível para download em http://172.16.208.100/Materiais/Files/CCNA4

Template de configuração Access-Points:

```
hostname ap1
!
dot11 ssid WIRELESS
   vlan 201
   authentication open
   authentication key-management wpa
   mbssid guest-mode
   wpa-psk ascii ciscoclass
!
dot11 ssid WIRELESS-GUESTS
   vlan 202
   authentication open
   authentication key-management wpa
   mbssid guest-mode
   wpa-psk ascii 7 ciscoguest
!
interface Dot11Radio0
 no shutdown
 encryption vlan 201 mode ciphers aes-ccm tkip
 encryption vlan 202 mode ciphers aes-ccm tkip
 ssid WIRELESS
 ssid WIRELESS-GUESTS
 mbssid
!
interface Dot11Radio0.201
 encapsulation dot1Q 201
 bridge-group 201
!
interface Dot11Radio0.202
```

```
 encapsulation dot1Q 202
 bridge-group 202
!
interface Dot11Radio1
 no shutdown
 encryption vlan 201 mode ciphers aes-ccm tkip
 encryption vlan 202 mode ciphers aes-ccm tkip
 ssid WIRELESS
 ssid WIRELESS-GUESTS
 mbssid
!
interface Dot11Radio1.201
 encapsulation dot1Q 201
 bridge-group 201
!
interface Dot11Radio1.202
 encapsulation dot1Q 202
 bridge-group 202
!
interface FastEthernet0
 no shutdown
!
interface FastEthernet0.201
 encapsulation dot1Q 201
 bridge-group 201
!
interface FastEthernet0.202
 encapsulation dot1Q 202
 bridge-group 202
!
interface FastEthernet0.254
 encapsulation dot1Q 254 native
 bridge-group 1
!
interface FastEthernet0.255
 ip address endereço_rede_management mascara_rede
 encapsulation dot1Q 255
 bridge-group 255
!
interface BVI1
 no ip address
!
interface BVI255
 ip address endereço_rede_management mascara_rede
```

Passos para reset de fabrica dos APs:

1. Desloquem a tampa exterior para aceder ao **mode button** que se encontra ao lado da porta de consola
2. Desligue o AP da corrente elétrica.
3. Pressione o **mode button** enquanto liga o AP novamente a corrente elétrica
4. Solte o **mode button** , quando o **LED** da **porta ethernet** ficar **laranja.**

A password de enable default é Cisco.