São Paulo Skills SENAI


# Projeto Teste

Gestão de Sistema e Rede TI

Modulo C - Cisco

# Introdução ao projeto de teste

A seguir, há uma lista de seções ou informações que devem ser incluídas em todas as propostas de Projeto de Teste enviadas à WorldSkills.

- Conteúdo, incluindo a lista de todos os documentos, desenhos e fotografias que compõem o Projeto de Teste Introdução/visão geral
- Breve descrição do projeto e das tarefas
- Instruções para o Competidor
- Outros

# Introdução

O conhecimento de tecnologia de rede está se tornando essencial hoje em dia para as pessoas que desejam construir uma carreira de sucesso em qualquer área de engenharia de TI. Esse projeto de teste contém muitos desafios da experiência da vida real,
principalmente integração e terceirização de TI. Se você conseguir concluir este projeto com uma pontuação alta, estará definitivamente pronto para atender à infraestrutura de rede de qualquer empresa com várias filiais.

# Instruções para o Competidor

A competição tem um horário fixo de início e término. Você deve decidir a melhor forma de dividir seu tempo. Leia as instruções com atenção!
Quando o tempo de competição terminar, deixe sua estação em um estado de funcionamento. A avaliação ocorrerá em seu estado atual. Nenhuma reinicialização será feita, nem as máquinas que estiverem desligadas serão ligadas!
Use as informações abaixo para todos os servidores e clientes.

**Use a senha padrão "Skill39" para todos os fins, a menos que lhe seja solicitada uma senha diferente.**

| Software/SO | Nome de usuário | Senha |
|---|---|---|
| VMware ESXi | raiz | P@ssw0rD |
| EVE-NG Web | administrador | véspera |
| EVE-NG VM | raiz | 1234.qwer |
| Servidor Windows | Administrador | 1234.qwer |
| Cliente Windows | Competidor | 1234.qwer |
| Linux | Root/competitor | 1234.qwer |

# Descrição do projeto e das tarefas

Este projeto de teste foi desenvolvido usando uma variedade de tecnologias de rede que devem ser familiares nas trilhas de certificação da Cisco. As tarefas são divididas nas seguintes seções de configuração:

• Configuração básica
• Comutação
• Roteamento
• Serviços
• Segurança
• WAN E VPN

Todas as seções são independentes, mas juntas criam uma infraestrutura de rede muito complexa. Algumas tarefas são bastante simples e diretas; outras podem ser complicadas. Você pode ver que algumas tecnologias devem funcionar em cima de outras tecnologias. Por exemplo, espera-se que o roteamento IPv6 seja executado sobre as VPNs configuradas, que, por sua vez, devem ser executadas sobre o roteamento IPv4, que, por sua vez, deve ser executado sobre o VRF, e assim por diante. É importante entender que, se você não conseguir encontrar uma solução em meio a esses problemas, será necessário um sistema de roteamento IPv4. isso não significa que o restante de seu trabalho não será avaliado. Por exemplo, você pode não configurar o roteamento IPv4 necessário para a VPN devido à capacidade de alcance do IP, mas pode usar rotas estáticas e depois continuar a trabalhar com a configuração da VPN e tudo o que for executado em cima. Você não receberá pontos por IPv4
mas você receberá pontos por tudo o que tornou operacional no topo, desde que o teste funcional seja bem-sucedido.

## Configuração básica

Configure todas as máquinas e equipamentos com o seguinte:

- Configure o nome do host e o endereçamento IP de acordo com a topologia e a tabela de endereçamento de todos os dispositivos.
- Configure o NAT/PAT conforme achar necessário.
- Configure o nome de domínio para "wsc2024.fr" em todos os dispositivos.
- Configure a senha para "skill#39" para o modo privilegiado em todos os equipamentos.
- Configure um banner de pré-login: "Este dispositivo é apenas para pessoal autorizado do domínio $(domain)!" .
- Configure um banner pós-login: "###Acesso concedido. Bem-vindo a $(hostname).###".
- Adicione descrições a todas as interfaces para identificar qual host está conectado: hostname - port
- Desative o CDP somente para as portas não utilizadas em todos os equipamentos.
- Configure o login via autenticação TACACS com failover local usando o fail-user.
- Configure o acesso remoto usando SSHv2 via autenticação TACACS com failover local usando fail-user.
- Crie o usuário local usando o algoritmo de hash PBKDF2.
- Configure o fuso horário do dispositivo como CET +1 em todos os equipamentos.

## Switching

- Estabeleça uma comunicação de rede sem problemas entre os dispositivos, configurando o posicionamento dos dispositivos de rede e a conectividade da rede com referência à topologia e à tabela de endereçamento.
- Use o protocolo VTP para configurar centralmente as VLANs em uma rede corporativa.
    - Configure DS1 e DS3 como o servidor VTP.
    - Configure os switches DS2, AS1, DS4 e AS2 como cliente VTP.
    - A tabela de VLAN deve conter as seguintes redes:
        - VLAN100 denominada MGT.
        - VLAN200 denominada DATA
        - VLAN300 denominada DATA-REDUNDANCY
        - VLAN400 com o nome NATIVE.
        - VLAN500 denominada SHUTDOWN.
- Configure trunks entre todos os switches usando o protocolo IEEE 802.1q.
    - As portas de switch conectadas aos clientes e ao servidor devem operar sem negociação. Desative o DTP explicitamente.
    - O trunking entre switches no HQ1 deve ser configurado sem o uso de negociação. Desative o DTP explicitamente.
    - Os trunks entre os switchs do HQ2 devem ser negociados por DTP, o switch DS3 deve iniciar o trunk e os switchs DS4 e AS2 devem aguardar que o vizinho inicie a negociação, mas não inicie
      negociação em si.
    - Para todos os trunks, atribua a VLAN nativa 400.
    - Impedir que todas as VLANs não utilizadas, incluindo a VLAN1, sejam encaminhadas por meio de trunks
- Configure a agregação de links entre os switches para HQ1 e HQ2.
    - Grupo de portas:
        - Entre os switches DS1 (Gi0/2) e DS2 (Gi0/3).
        - Entre os switches DS3 (Gi0/2) e DS4 (Gi0/3).
    - O link agregado entre DS1 e DS2 deve ser organizado usando o padrão aberto IEEE 802.3ad protocolo de negociação. O DS1 deve ser configurado no modo ativo e o DS2 no modo passivo.
    - O link agregado entre DS3 e DS4 deve ser organizado usando o protocolo de negociação proprietário da Cisco. O DS3 deve ser definido como Preferred e o DS4 como Automatic.
- Configurar o protocolo spanning tree para HQ1 e HQ2:
    - Usar o protocolo PVST
    - Os switches DS1 e DS3 devem ser o root spanning tree nas VLANs 100, 200, 300 e 400, e, em caso de falha do DS1, o root deve ser os switches DS2 e DS4.
    - Configure as portas cliente dos switches AS1 e AS2 para que, quando forem ligados, entrem imediatamente no estado de encaminhamento sem esperar que o spanning tree seja recalculada.
- Em todos os switches, mova as portas não utilizadas para a VLAN 500.

## Roteamento

- Consulte a "Tabela de endereços" no apêndice para garantir que todos os dispositivos recebam endereços IP apropriados.
- Configure o Router-on-a-stick Inter-VLAN no CR1, CR2, CR3 e CR4 para que o IPv4 e o IPv6 funcionem em conjunto com as VLANs e os protocolos FHRP:
    - Gig0/0.100 e Gig0/3.100 - VLAN MGMT
    - Gig0/0.200 e Gig0/3.200 - VLAN DATA
    - Gig0/0.300 e Gig0/3.300 - VLAN DATA-R
- Configure adequadamente o roteamento dinâmico para todos os dispositivos usando o diagrama de roteamento no apêndice.
- Configure o OSPFV3 para garantir que o roteamento IPv4 e IPv6 entre os dispositivos CR1, CR2, CR3 e CR4 esteja configurado corretamente, de preferência com o método de autenticação mais seguro.
- Configure o roteamento MP-BGP para garantir que o roteamento IPv4 e IPv6 entre os dispositivos ISP1, BR1, BR2, IR1 e IR2 esteja configurado corretamente, de preferência com o método de autenticação mais seguro.
    - Use AS 65001 para ISP, 65002 para IR1, 65003 para IR2, 65004 para BR1 e 65005 para BR2.
- Configurar VRFs no ISP para redes IPv4 e IPv6.
    - O VRF ISP1 deve ser usado para encaminhar para BR1 e IR1.
    - O VRF ISP2 deve ser usado para encaminhar para BR2 e IR2.
- Certifique-se de que a configuração do BGP funcione em conjunto com o VRF ISP1 e ISP2.
- Configure a redistribuição de roteamento entre OSPFv2, OSPFv3 e MP-BGP para IPv4 e IPv6 usando os roteadores IR1 e IR2.

## Serviços

- Configurar a autoridade de certificação no roteador ISP:
    - Inclua o FQDN do roteador ISP nos certificados emitidos.
    - Use o registro automático
    - Emita certificados para todos os dispositivos e serviços necessários.
    - Não use a verificação de revogação
- Configure o NTP com a seguinte configuração:
    - Configure um servidor NTP de nível Stratum 7 no roteador ISP.
        - Os roteadores IR1, IR2, BR1 e BR2 e os switches AS3 e AS4 devem configurar o ISP como servidor NTP.
        - Os dispositivos que usam um roteador ISP como servidor de horário usam a chave 1
        - Certifique-se de realizar a certificação. Use o algoritmo SHA como um hash de cifra.
    - Configure um servidor NTP de nível Stratum 8 no dispositivo CR1.
        - Os roteadores e switches do HQ1 e HQ2 devem ser configurados para sincronizar a hora com esse servidor.
        - Os dispositivos que usam dispositivos CR1 como servidores de horário usam a chave 2 para realizar a autenticação.
        - Use o algoritmo MD5 como hash.
- Configure o DHCP para IPv4 e IPv6 para os clientes HQ1 e HQ2, de preferência usando o DHCPv6 stateless para cliente HQ2-CLI1 e DHCPv6 stateful para o cliente HQ1-CLI1.
    - Essa configuração deve funcionar em conjunto com as redes FHRP.
- Configure o HSRP como o protocolo FHRP para HQ1 para redes IPv4 e IPv6 com dois grupos diferentes (o mesmo número de VLAN IDs) e VIPs de acordo com a tabela de endereçamento, de preferência usando o método de autenticação mais seguro e a melhor configuração de redundância.

- Configure o GLBP como o protocolo FHRP para HQ2 para redes IPv4 e IPv6 com dois grupos diferentes (o mesmo número de VLAN IDs) e VIPs de acordo com a tabela de endereçamento, de preferência usando o método de autenticação mais seguro e a melhor configuração de redundância.
- Use o HQ1-SVR1 como servidor TACACS+ (pré-configurado) para dispositivos IPv4 e IPv6 que desejam usar os serviços AAA. Adicione a seguinte conta de autenticação tacacs-user.

## Segurança

- Configure o Port Security nos switches AS1 e AS2 para os clientes.
    - Nos links associados aos dispositivos HQ1-CLI1 e HQ2-CLI1
- Configure o DHCP snooping nos switches AS1 e AS2. Restringir os serviços de DHCP nos dispositivos, permitir somente para redes VLANs DATA e DATA-REDUNDANCY. Use a memória flash como local de armazenamento do banco de dados.
- Configure a inspeção dinâmica de ARP nos switches AS1 e AS2.
    - Nas VLANs DATA e DATA-REDUNDANCT, os dispositivos de rede validam os endereços MAC com base no banco de dados DHCP snooping.
- Configure o intervalo de desativação de erros para 3 minutos e ative a recuperação automática para inspeção de ARP, BPDU Guard e violações do Port Security.
- Habilite o acesso SSHv2 aos dispositivos por meio da autenticação TACACS com failover local usando o fail-user.
- Os dispositivos de site HQ e BR devem executar a autenticação TACACS+ ou a autenticação local ao entrar no modo privilegiado. Os clientes HQ devem se comunicar com o TACACS+ via IPv6 e os clientes BR via IPv4. Adicione uma conta "fail-user" como uma conta local.

## WAN E VPN

- Configure uma VPN Hub-and-Spoke usando o dispositivo ISP como roteador Hub e os dispositivos IR1, IR2, BR1, BR2 como roteadores spoke, de preferência em uma configuração FlexVPN com o roteador hub usando uma interface VTI dinâmica e os roteadores de spoke usando uma interface VTI estática.
- Proteja o tráfego VPN do Hub e do Spoke com IPSec, de preferência usando o protocolo VPN e o método de autenticação mais seguros disponíveis.
- Certifique-se de que o túnel FlexVPN seja o caminho preferencial para o tráfego entre as redes BR1 e BR2.
- Configure o roteamento MP-BGP e o VRF no ISP para que funcionem corretamente com a configuração do FlexVPN, a fim de garantir um roteamento estável e eficiente no ambiente FlexVPN.
- Configure uma DMVPN que suporte totalmente o tráfego IPv4 e IPv6, de preferência em uma configuração Dual Hub Single Cloud para garantir redundância e roteamento otimizado.
    - Use os roteadores CR1 e CR3 como Hubs. Use os roteadores CR2 e CR4 como spokes.
- Proteja o tráfego DMVPN com IPSec, de preferência usando o protocolo VPN e o método de autenticação mais seguros disponíveis.
- Certifique-se de que o túnel DMVPN seja o caminho preferencial para o tráfego entre as redes HQ1 e HQ2.
- Configure o roteamento OSPFv2 e OSPFv3 para funcionar corretamente com o tipo de rede DMVPN a fim de garantir um roteamento estável e eficiente no ambiente DMVPN.

## Apêndice - Tabela de endereçamento

| Roteador CR1 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| GigabitEthernet0/0.100 | 192.168.100.2/24 | 2001:DB8:100::2/64 |
| GigabitEthernet0/0.200 | 192.168.11.2/24 | 2001:DB8:11::2/64 |
| GigabitEthernet0/1 | 201.68.128.2/24 | 2001:DB8:128::2/64 |
| GigabitEthernet0/2 | 201.68.1.1/30 | 2001:DB8:1::1/64 |
| GigabitEthernet0/3.300 | 192.168.13.2/24 | 2001:DB8:13::2/64 |
| GigabitEthernet0/4 | 201.68.3.1/30 | 2001:DB8:3::1/64 |
| VIP 0 | 192.168.100.1/24 | 2001:DB8:100::1/64 |
| VIP 1 | 192.168.11.1/24 | 2001:DB8:11::1/64 |
| VIP 2 | 192.168.13.1/24 | 2001:DB8:13::1/64 |
| Túnel0 | 10.0.0.1/24 | 2001:DB8:1:100::1/64 |

| Roteador CR2 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| GigabitEthernet0/0.100 | 192.168.100.3/24 | 2001:DB8:100::3/64 |
| GigabitEthernet0/0.200 | 192.168.11.3/24 | 2001:DB8:11::3/64 |
| GigabitEthernet0/1 | 201.68.129.2/24 | 2001:DB8:129::3/64 |
| GigabitEthernet0/2 | 201.68.1.2/30 | 2001:DB8:1::2/64 |
| GigabitEthernet0/3.300 | 192.168.13.3/24 | 2001:DB8:13::3/64 |
| GigabitEthernet0/4 | 201.68.4.1/30 | 2001:DB8:4::1/64 |
| VIP 0 | 192.168.100.1/24 | 2001:DB8:100::1/64 |
| VIP 1 | 192.168.11.1/24 | 2001:DB8:11::1/64 |
| VIP 2 | 192.168.13.1/24 | 2001:DB8:13::1/64 |
| Túnel0 | 10.0.0.2/24 | 2001:DB8:1:100::2/64 |

| Roteador CR3 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| GigabitEthernet0/0.100 | 192.168.200.2/24 | 2001:DB8:200::2/64 |
| GigabitEthernet0/0.200 | 192.168.12.2/24 | 2001:DB8:12::2/64 |
| GigabitEthernet0/1 | 201.68.130.2/24 | 2001:DB8:130::2/64 |
| GigabitEthernet0/2 | 201.68.2.1/30 | 2001:DB8:2::1/64 |
| GigabitEthernet0/3.300 | 192.168.14.2/24 | 2001:DB8:14::2/64 |
| GigabitEthernet0/4 | 201.68.4.2/30 | 2001:DB8:4::2/64 |
| VIP 0 | 192.168.200.1/24 | 2001:DB8:200::1/64 |
| VIP 1 | 192.168.12.1/24 | 2001:DB8:12::1/64 |
| VIP 2 | 192.168.14.1/24 | 2001:DB8:14::1/64 |
| Túnel0 | 10.0.0.3/24 | 2001:DB8:1:100::3/64 |

| Roteador CR4 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| GigabitEthernet0/0.100 | 192.168.200.3/24 | 2001:DB8:200::3/64 |
| GigabitEthernet0/0.200 | 192.168.12.3/24 | 2001:DB8:12::3/64 |
| GigabitEthernet0/1 | 201.68.131.2/24 | 2001:DB8:131::2/64 |
| GigabitEthernet0/2 | 201.68.2.2/30 | 2001:DB8:2::2/64 |
| GigabitEthernet0/3.300 | 192.168.14.3/24 | 2001:DB8:14::3/64 |
| GigabitEthernet0/4 | 201.68.3.2/30 | 2001:DB8:3::2/64 |
| VIP 0 | 192.168.200.1/24 | 2001:DB8:200::1/64 |
| VIP 1 | 192.168.12.1/24 | 2001:DB8:12::1/64 |
| VIP 2 | 192.168.14.1/24 | 2001:DB8:14::1/64 |
| Túnel0 | 10.0.0.4/24 | 2001:DB8:1:100::4/64 |

| Roteador ISP | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| Loopback0 | 10.1.200.1/24 | 2001:DB8:200::1/64 |
| Loopback1 | 192.168.255.1/32 | 2001:db8:255::1/128 |
| Loopback2 | 192.168.254.1/32 | 2001:db8:254::1/128 |
| Modelo virtual1 | Loopback0 | Loopback0 |
| GigabitEthernet0/0 | 203.0.113.1/30 | 2001:DB8:201::1/64 |
| GigabitEthernet0/1 | 203.0.113.5/30 | 2001:DB8:202::1/64 |
| GigabitEthernet0/2 | 203.0.113.9/30 | 2001:DB8:203::1/64 |
| GigabitEthernet0/3 | 203.0.113.13/30 | 2001:DB8:204::1/64 |

| Roteador BR1 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| GigabitEthernet0/0 | 192.168.31.1/24 | 2001:DB8:31::1/64 |
| GigabitEthernet0/1 | 203.0.113.2/30 | 2001:DB8:201::2/64 |
| Túnel0 | 10.1.200.2/24 | 2001:DB8:1:200::2/64 |

| Roteador BR2 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| GigabitEthernet0/0 | 192.168.41.1/24 | 2001:DB8:41::1/64 |
| GigabitEthernet0/1 | 203.0.113.6/30 | 2001:DB8:202::2/64 |
| Túnel0 | 10.1.200.3/24 | 2001:DB8:1:200::3/64 |

| Roteador IR1 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| GigabitEthernet0/0 | 203.0.113.10/30 | 2001:DB8:203::2/64 |
| GigabitEthernet0/1 | 201.68.128.1/24 | 2001:DB8:128::1/64 |
| GigabitEthernet0/2 | 201.68.129.1/24 | 2001:DB8:129::1/64 |
| Túnel0 | 10.1.200.4/24 | 2001:DB8:1:200::4/64 |

| Roteador IR2 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| GigabitEthernet0/0 | 203.0.113.14/30 | 2001:DB8:204::2/64 |
| GigabitEthernet0/1 | 201.68.130.1/24 | 2001:DB8:130::1/64 |
| GigabitEthernet0/2 | 201.68.131.1/24 | 2001:DB8:131::1/64 |
| Túnel0 | 10.1.200.5/24 | 2001:DB8:1:200::5/64 |

| Chave DS1 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| VLAN MGMT | 192.168.100.11/24 | 2001:DB8:100::B/64 |

| Chave DS2 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| VLAN MGMT | 192.168.100.12/24 | 2001:DB8:100::C/64 |

| Chave DS3 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| VLAN MGMT | 192.168.200.13/24 | 2001:DB8:200::D/64 |

| Chave DS4 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| VLAN MGMT | 192.168.200.14/24 | 2001:DB8:200::E/64 |

| Switch AS1 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| VLAN MGMT | 192.168.100.15/24 | 2001:DB8:100::F/64 |

| Switch AS2 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| VLAN MGMT | 192.168.200.16/24 | 2001:DB8:200::10/64 |

| Switch AS3 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| VLAN MGMT | 192.168.31.254/24 | 2001:DB8:31::fffe/64 |

| Switch AS4 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| VLAN MGMT | 192.168.41.254/24 | 2001:DB8:41::fffe/64 |

| HQ1-SVR1 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| Ethernet | 192.168.11.10/24 | 2001:DB8:11:A/64 |

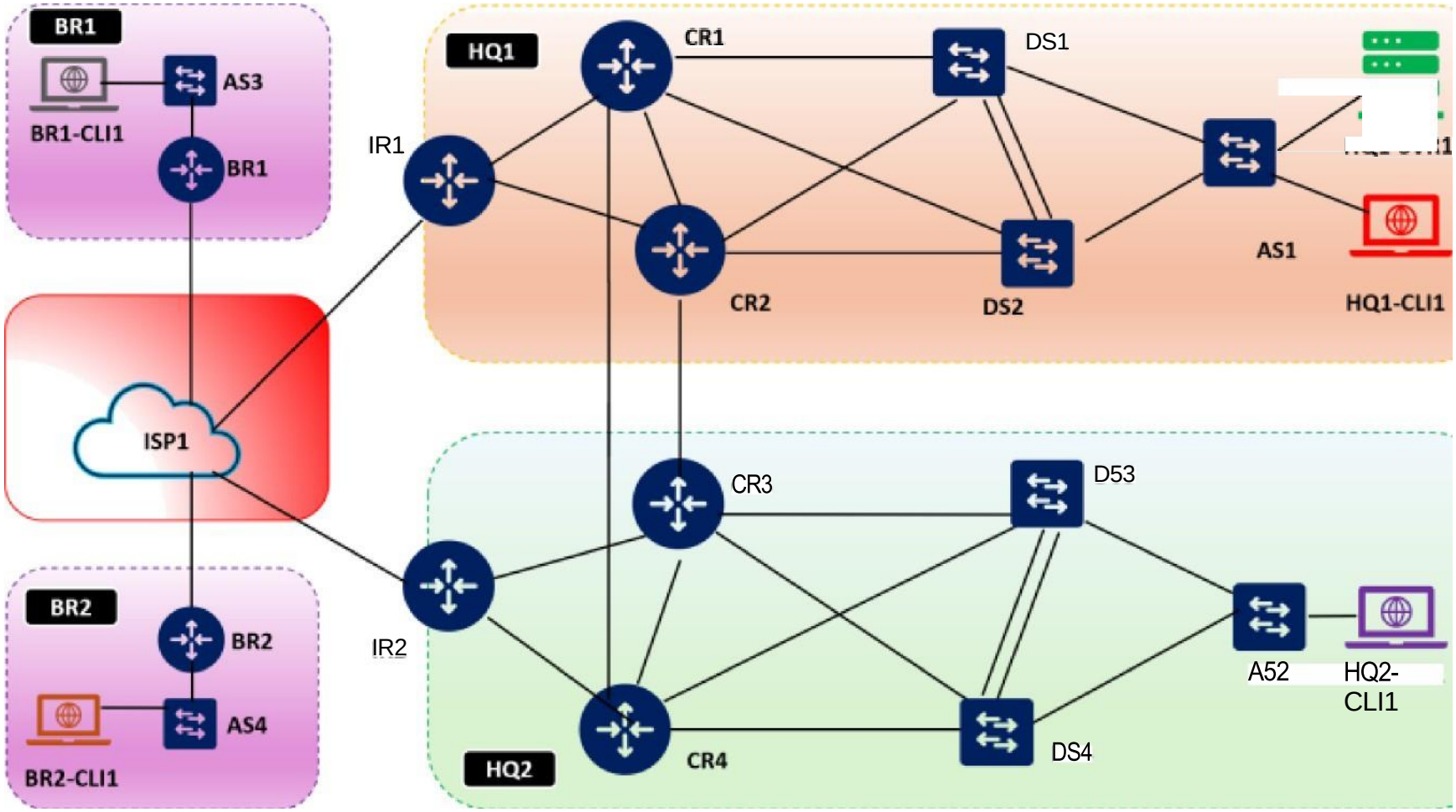
| HQ1-CLI1 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| Ethernet | DHCPv4 - VIP2 GW | DHCPv6 com estado - VIP2 GW |

| HQ2-CLI1 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| Ethernet | DHCPv4 - VIP1 GW | DHCPv6 sem estado - VIP 1 GW |

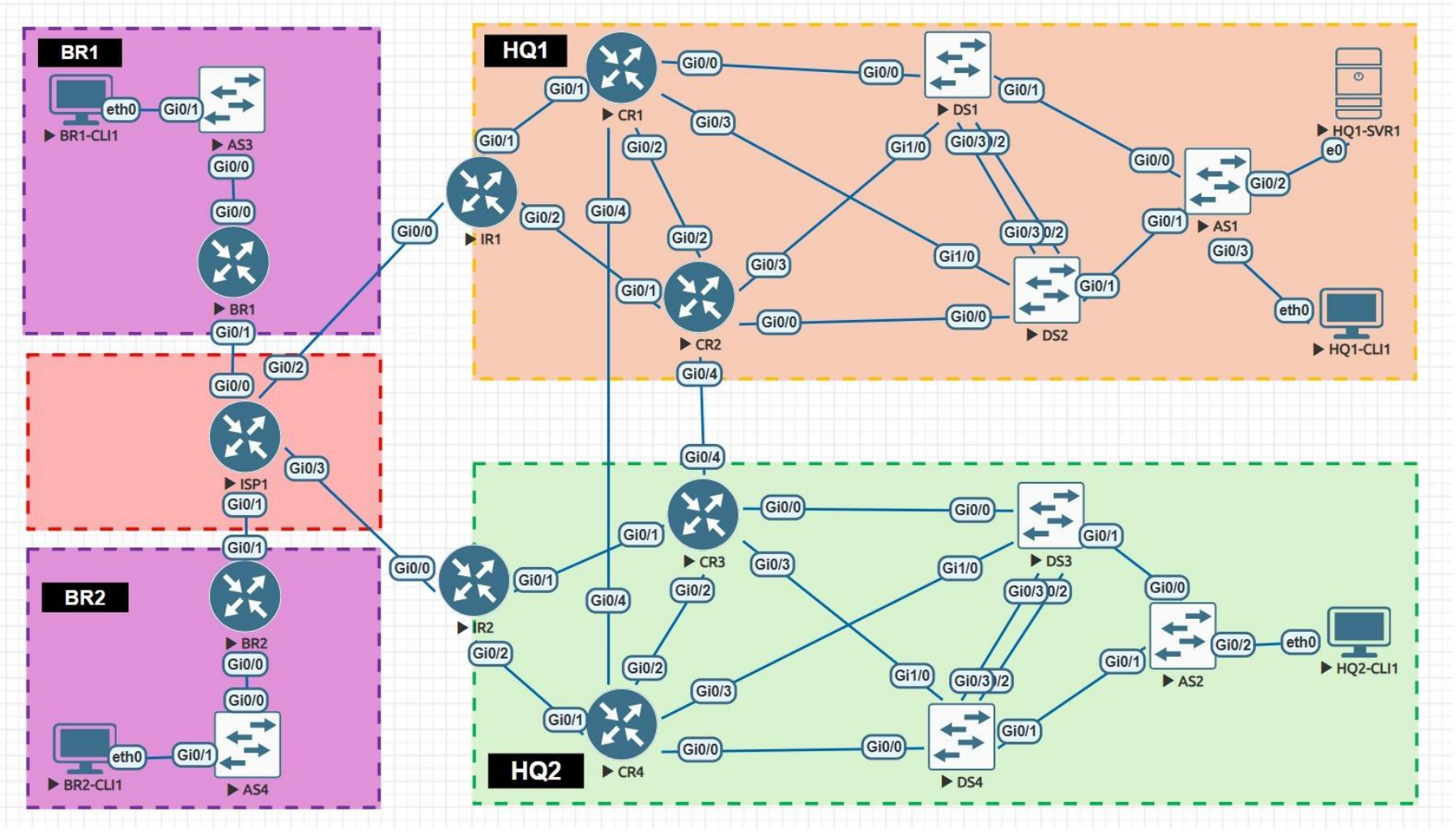
| BR1-CLI1 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| Ethernet | 192.168.31.10/24 | 2001:DB8:31::A/64 |

| BR2-CLI1 | | |
|---|---|---|
| **Interface** | **Endereço IPv4** | **Endereço IPv6** |
| Ethernet | 192.168.41.10/24 | 2001:DB8:41::A/64 |

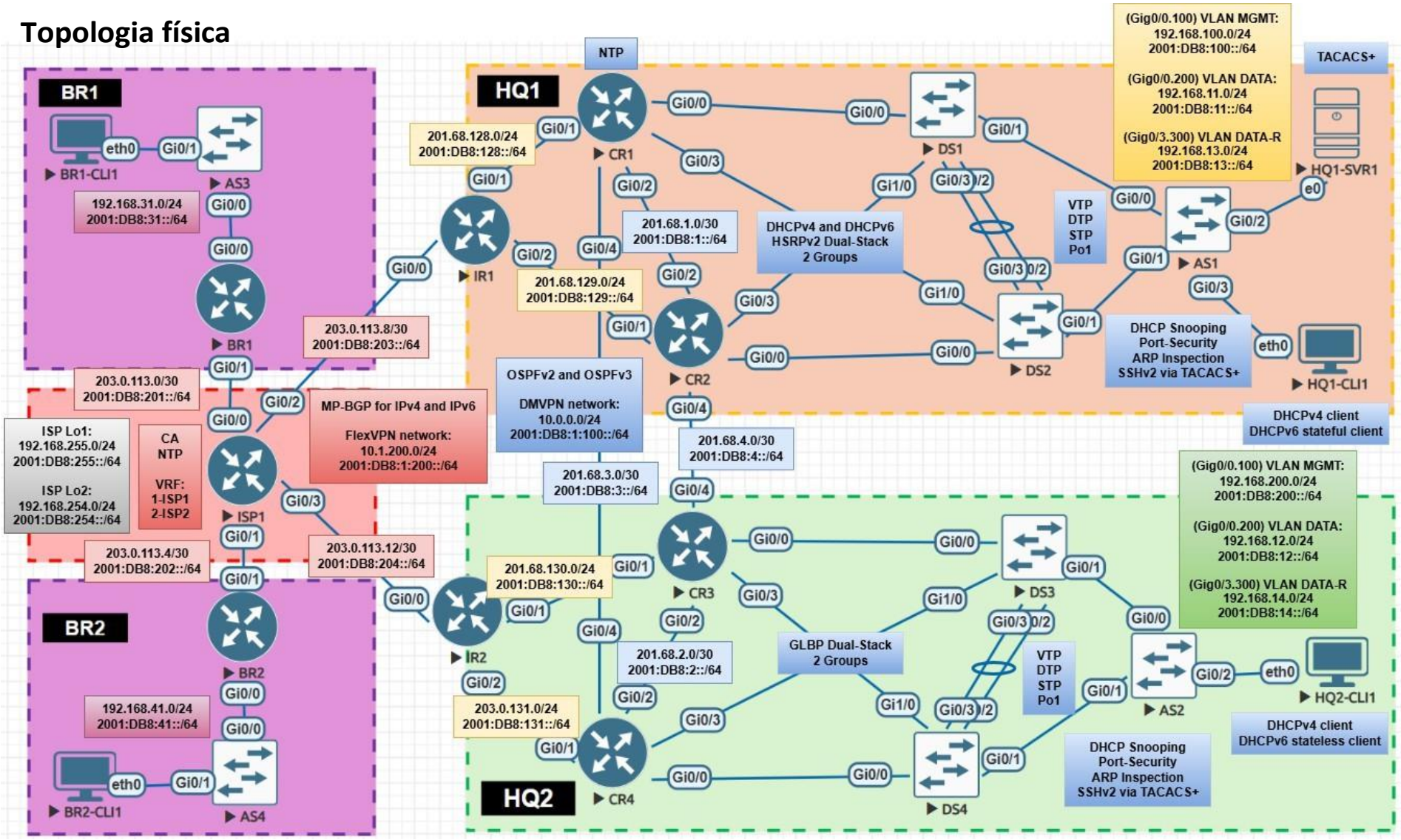
## Topologia geral

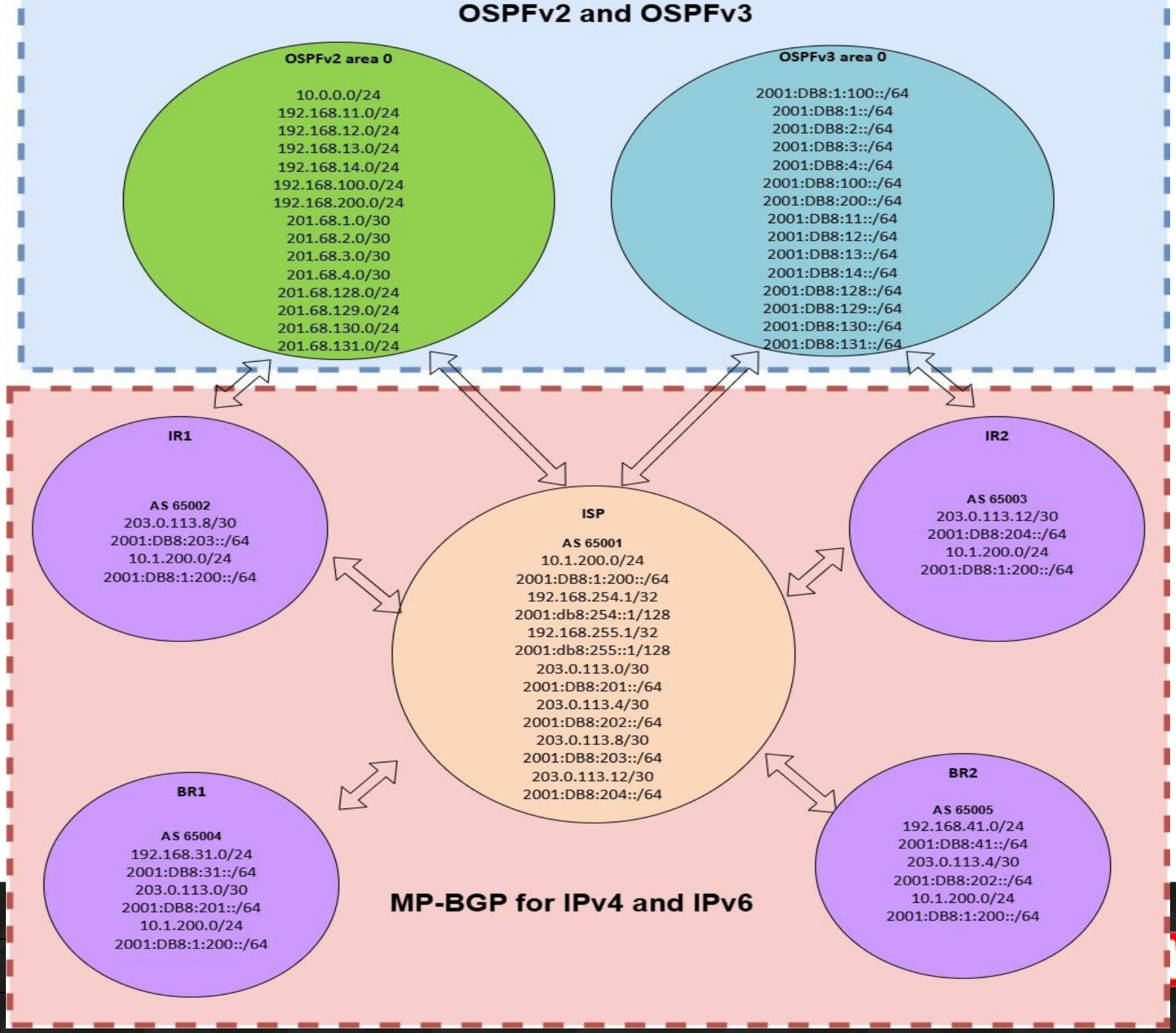


## Topologia geral



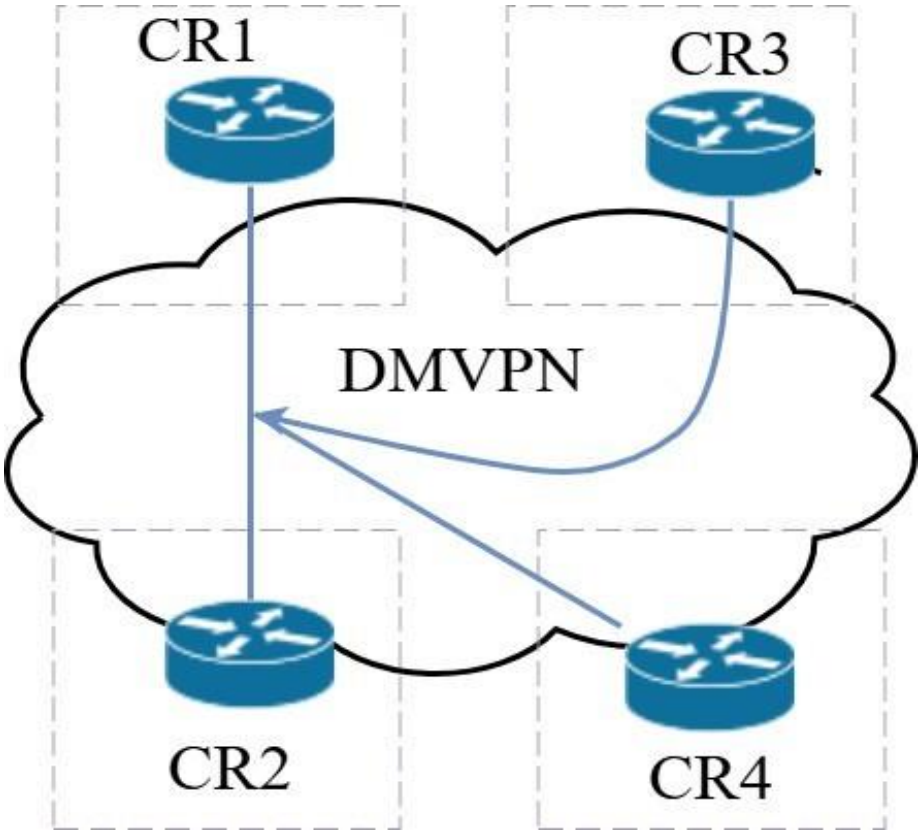
## Topologia física




OSPFv2 and OSPFv3
OSPFv2 area 0
10.0.0.0/24
192.168.11.0/24
192.168.12.0/24
192.168.13.0/24
192.168.14.0/24
192.168.100.0/24
192.168.200.0/24
201.68.1.0/30
201.68.2.0/30
201.68.3.0/30
201.68.4.0/30
201.68.128.0/24
201.68.129.0/24
201.68.130.0/24
201.68.131.0/24
OSPFv3 area 0
2001:DB8:1:100::/64
2001:DB8:1::/64
2001:DB8:2::/64
2001:DB8:3::/64
2001:DB8:4::/64
2001:DB8:100::/64
2001:DB8:200::/64
2001:DB8:11::/64
2001:DB8:12::/64
2001:DB8:13::/64
2001:DB8:14::/64
2001:DB8:128::/64
2001:DB8:129::/64
2001:DB8:130::/64
2001:DB8:131::/64
IR1
AS 65002
203.0.113.8/30
2001:DB8:203::/64
10.1.200.0/24
2001:DB8:1:200::/64
ISP
AS 65001
10.1.200.0/24
2001:DB8:1:200::/64
192.168.254.1/32
2001:db8:254::1/128
192.168.255.1/32
2001:db8:255::1/128
203.0.113.0/30
2001:DB8:201::/64
203.0.113.4/30
2001:DB8:202::/64
203.0.113.8/30
2001:DB8:203::/64
203.0.113.12/30
2001:DB8:204::/64
IR2
AS 65003
203.0.113.12/30
2001:DB8:204::/64
10.1.200.0/24
2001:DB8:1:200::/64
BR1
AS 65004
192.168.31.0/24
2001:DB8:31::/64
203.0.113.0/30
2001:DB8:201::/64
10.1.200.0/24
2001:DB8:1:200::/64
BR2
AS 65005
192.168.41.0/24
2001:DB8:41::/64
203.0.113.4/30
2001:DB8:202::/64
10.1.200.0/24
2001:DB8:1:200::/64
MP-BGP for IPv4 and IPv6

## Diagrama de VPN

## DMVPN Dual Hub Single Cloud



## Cisco FlexVPN Hub-and-Spoke