Cisco Community

Community Live event

Personalizando SD-WAN: desatando el poder de las políticas

Eduardo Moisa, Director General de Your Next Hop y Co Fundador de Grupo Infotech, 3x CCIE (#52536)

David Peñaloza Seijas, Lead Network Consulting Engineer, Verizon Enterprise

Octubre 27, 2020

Novedades & Eventos próximos

Ask Me Anything- Sesión del evento

Hasta el Viernes 30 de Octubre, 2020

Con
Eduardo & David

http://bit.ly/foro-sdwan-politicas

Julio Moisa
Director General & Co-Fundador
3xCCIE (#52536)

David Peñaloza
Lead Network Consulting Engineer

Próximo evento – Meet the Authors

CCIE Security y su aplicación práctica en la red actual: Zero Trust

Jueves 19 de
Octubre
11hrs CDT (utc-6)

Con los expertos top
en seguridad

http://bit.ly/MeetAuthors-oct

Califique el contenido de la Comunidad de Cisco en Español

¡Califique “Discusiones, Documentos y Videos!

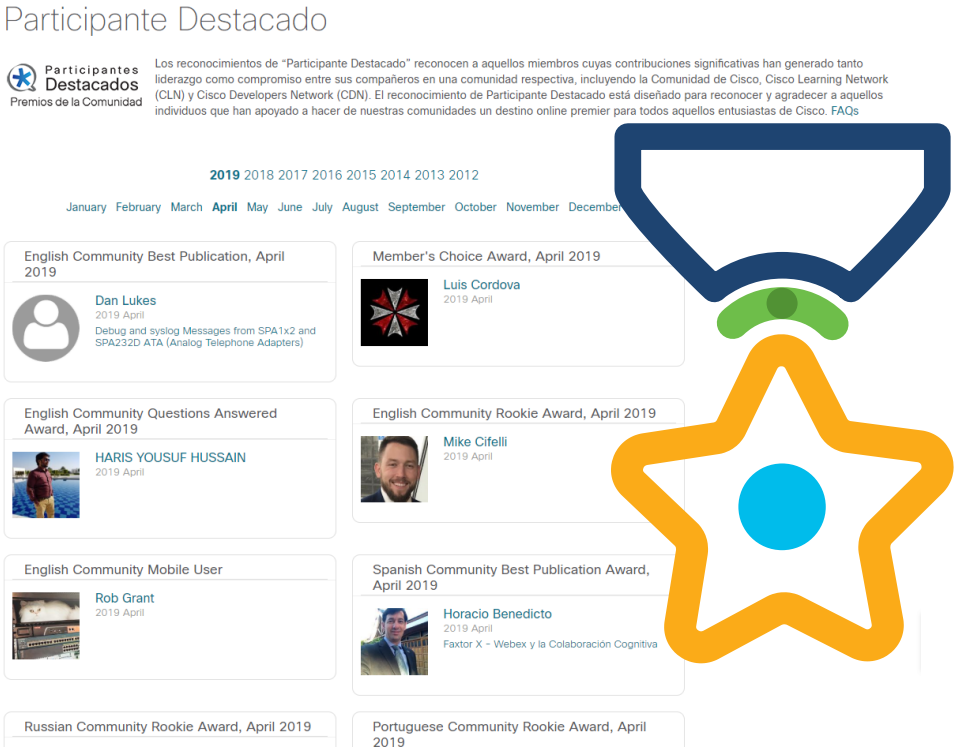
Ayúdenos a identificar el contenido de calidad y a reconocer el esfuerzo de los integrantes de la Comunidad

Reconocimientos en la Comunidad

Participante Destacado

Reconocimiento mensual

Diseñado para reconocer y agradecer a quienes colaboran en la comunidad: publicando contenido o participando en discusiones



Gracias por su asistencia el día de hoy

La presentación incluirá algunas preguntas a la audiencia.
Le invitamos cordialmente a participar activamente en las preguntas que le haremos durante la sesión

¡Resuelva su dudas y comparta opiniones!

Expertos de la Comunidad de Cisco

David Peñaloza
Lead Network Consulting Engineer

Cisco Champion

CISCO DESIGNATED cisco VIP PROGRAM

Julio Moisa
Director General
3x CCIE #52536

¡Gracias por estar con nosotros hoy día!

http://bit.ly/sdwan-slides-oct

¡Haga sus preguntas al Panel de Expertos!

Use el panel de preguntas y (**P&R / Q&A**) para preguntar a los expertos.

Sus preguntas serán respondidas eventualmente

Personalizando SD-WAN: desatando el poder de las políticas

Eduardo Moisa & David Peñaloza

Octubre 27, 2020

Cisco Champion

VIP 2020

AGENDA

1. Introducción a Cisco SD-WAN
2. TLOCs y tipos de rutas
3. Estructura de las políticas de Cisco SD-WAN
4. Empleando *control policies* para modificar la topología del *overlay*
5. Empleando *data policies* para proporcionar una mejor experiencia del usuario
6. Demo

Polling Question 1

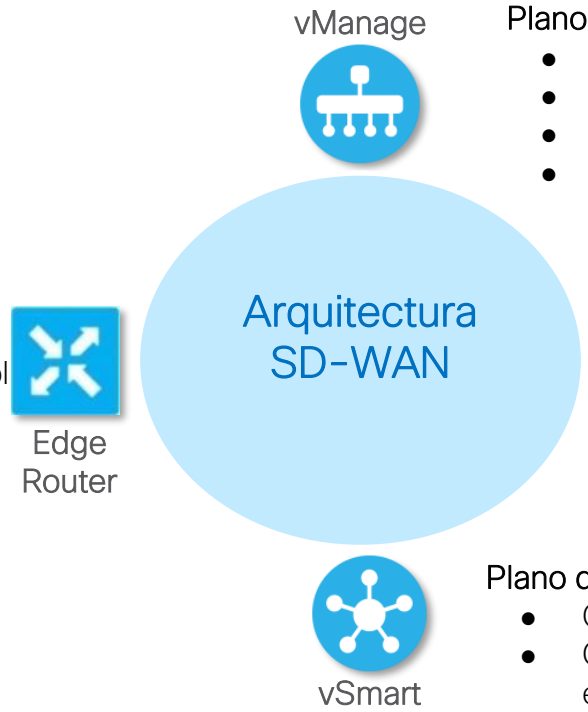
¿Tienes conocimiento sobre las políticas de Cisco SD-WAN?

A. Si

B. No

Introducción a Cisco SD-WAN

Componentes de Cisco SD-WAN



Plano de Administración

- Administración centralizada
- Creación de plantillas y políticas
- Brinda herramientas de tshoot y monitoreo
- Provee interfaces para programabilidad

Plano de Datos

- WAN Edge router
- Asegura el plano de control con otro WAN Edge
- Implementa políticas en el plano de datos.

Plano de Orquestación

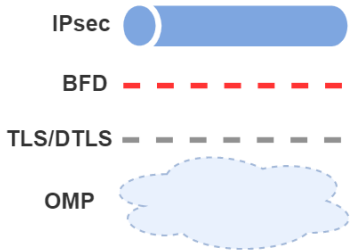
- Primer punto de autenticación
- Servidor STUN
  - Facilita NAT Traversal

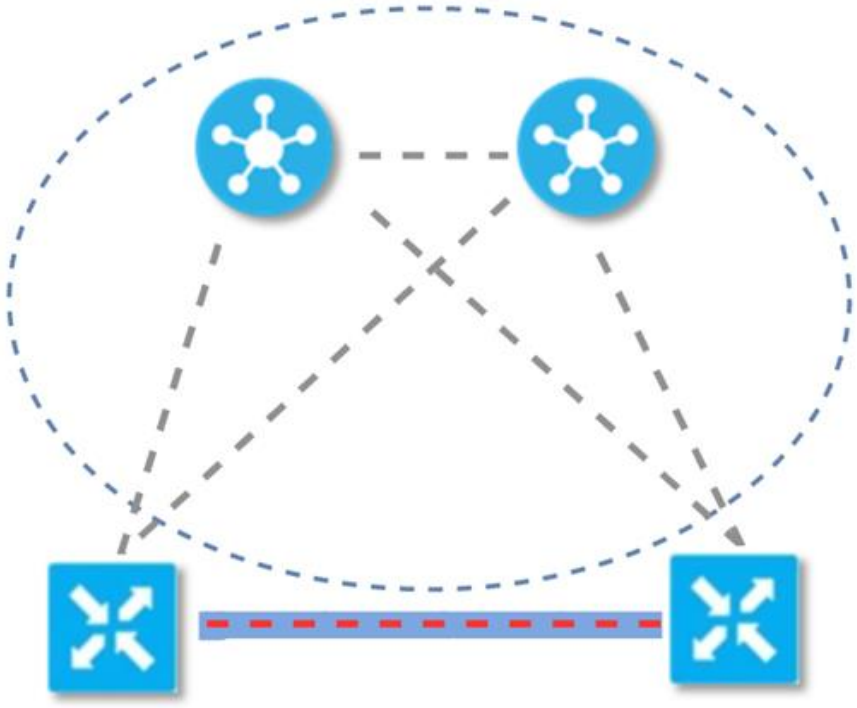
Plano de Control

- Cerebro de la solución
- Controla y administra lo relacionado a enrutamiento y políticas
- Facilita el cifrado de datos entre los WAN Edges
- Utiliza el protocolo OMP para propagar información a los WAN Edges

Cisco SD-WAN - Overlay

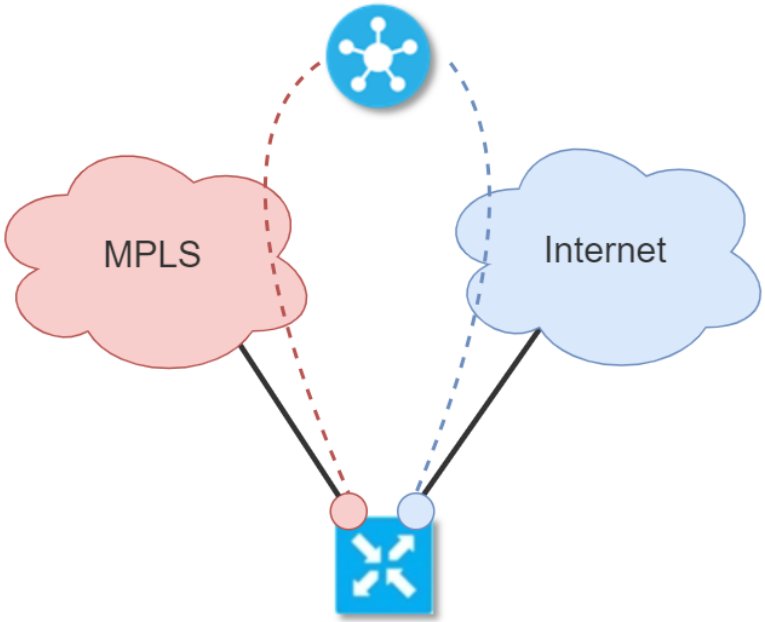
- Plano de Datos entre WAN Edges unicamente
- Plano de control entre WAN Edges y vSmart unicamente





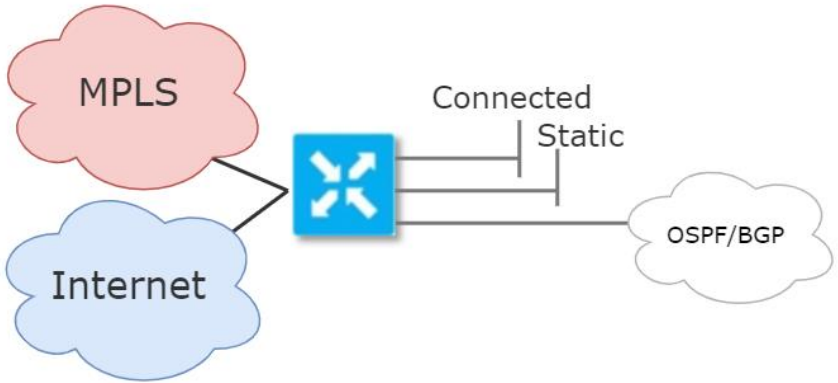
TLOCs

- Rutas asociadando la ubicación fisica y la red - un *next hop*!
- Anunciadas/publicadas a vSmart a traves de OMP.
  - Atributos más reconocidos:
    - Site-ID
    - Encap-SPI
    - Encap-Authentication
    - Encap-Encryption
    - Public IP
    - Public Port
    - Private IP
    - Private Port
    - BFD-Status
    - Tag
    - Weight



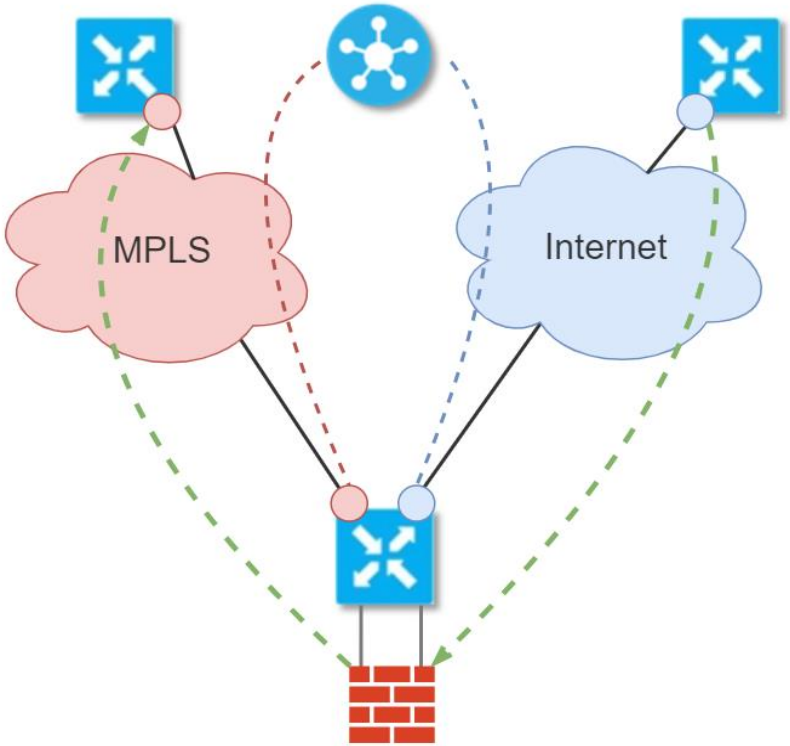
vRoutes

- Tambien conocidas como rutas OMP
- Rutas generadas por los WAN Edges
- Anunciadas/Publicadas a vSmart
- Atributos más resaltantes:
  - TLOC
  - Site-ID
  - Label
  - Tag
  - Preference
  - Originator System IP
  - Origin Protocol
  - Origin Metric
  - AS PATH



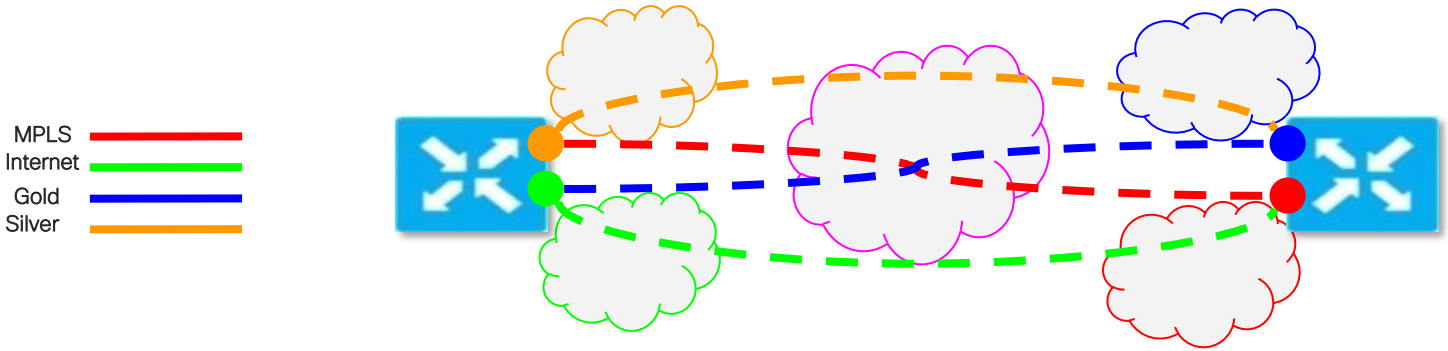
Rutas de servicio

- Relacionadas a servicios aplicados en los WAN Edges
- Anunciadas a vSmart
  - Atributos más impotantes:
    - VPN-ID
    - Service-ID
    - Label
    - Originator System IP
    - TLOC



Colores – ¡no solo una etiqueta!

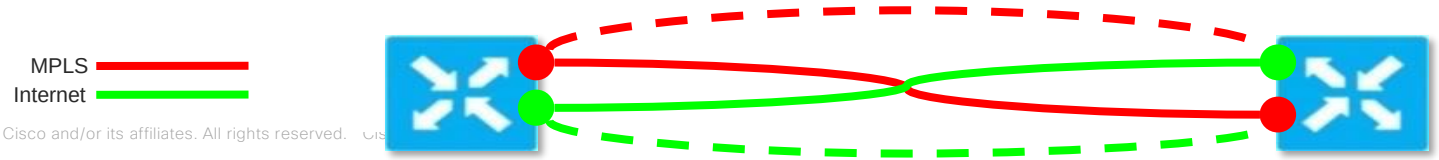
- Identifica el medio de transporte
- Determina la conexión establecida del tunel del WAN Edge
  - Direcciones públicas o privadas son basadas en el color del TLOC
- Atributo utilizado en las políticas para diferenciar y agrupar medios de transporte



Colores – ¡no solo una etiqueta!

FULL MESH

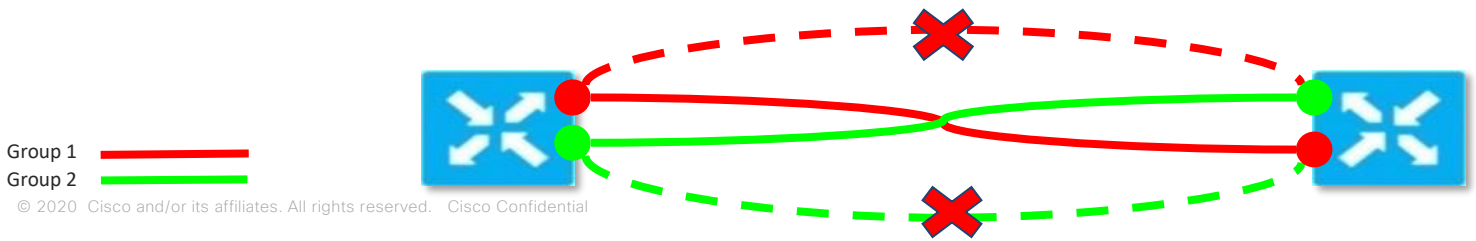
- *Unrestricted*
  - Por defecto, las sesiones BFD se intentarán establecer desde y hacia todos los medios de transporte – todos los colores
  - Requiere que haya conectividad en *underlay*
    - ¿Puede el TLOC de Biz-Internet llegar a MPLS? ¿Ha sido anunciado?
- *Restricted*
  - Sesiones BFD únicamente podrán establecerse entre el mismo color.
  - Ej. BIZ Internet únicamente podrá establecer sesiones con WAN Edge utilizando BIZ Internet y no con otro color como MPLS, Silver, LTE, etc.
    - ¿Necesitas minimizar la cantidad de sesiones? ¿Estás considerando redundancia?



Colores – ¡no solo una etiqueta!

Hay un límite en el número de sesiones BFD

- *TLOC Groups*
  - Pemite agrupar varios colores
  - Sesiones BFD solo serán establecidas entre miembros del mismo grupo
    - Objetivo final: reducir el uso de recursos, solo establecer sesiones necesarias
      - *Trade-off:* Optimalidad vs escalabilidad
  - Similar al despliegue de tipo **restricted**, pero mas amplio
    - El lugar feliz entre ambos extremos
  - Los grupos pueden estar compuestos de que cualquier lista de colores que defina el administrador
    - Ejemplos:
      - Private1 and Private2
      - Biz-Internet and Public Internet



Cisco SD-WAN policy framework

Políticas

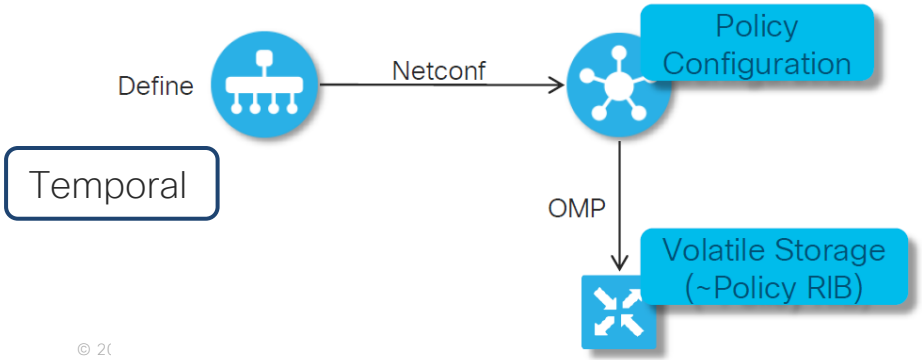
¿Dónde aplicamos las políticas?

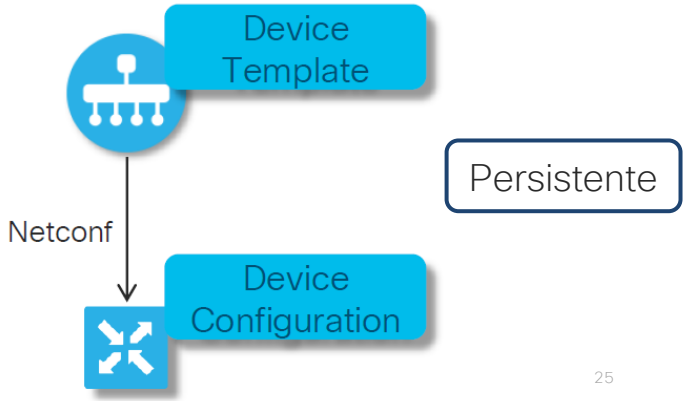
- Plano de control
  - Cualquier modificación que afecte el enrutamiento
    - Ej *Peerings, routing protocols, prefix filtering/tagging/announcement, VPN membership*
- Plano de datos
  - Cualquier modificación que afecte como fluyen servicios, aplicaciones o datos.
    - Ej. Marcado de tráfico, *Application Aware Routing* (AAR)

Políticas (cont.)

Las políticas pueden ser desplegadas de dos maneras:

- *Centralized*
  - Aplicado desde vManage hacia vSmart a través de una transacción NETCONF y finalmente publicadas a los WAN Edge.
- *Localized*
  - Aplicado desde el vManage hacia los WAN Edge directamente, considerado como persistente.





Políticas (cont.)

¿Cuáles son las diferencias entre estos metodos? ¿Qué modifican?

- *Centralized Control policy*
  - Ej *Peerings, routing protocols, prefix filtering/tagging/announcement, VPN membership*
- *Localized Control Policy*
  - Ej *Peerings* en OSPF and BGP

- *Centralized Data policy*
  - Ej *Packet marking*, *application pinning*, *Application Aware Routing* (AAR)
- *Localized Data Policy*
  - Ej QoS, ACLs bajo interfaces.

Políticas (cont.)

Políticas del plano de control:

Nos permiten manipular el enrutamiento de manera global o puntual.

Algunos servicios posibles:

- *Service Chaining*
- *Traffic Engineering*
- *Extranet VPNs*
- Topologías de VPN
- Conectar planos de datos discontinuos

Políticas del plano de datos:

Contrarias a las políticas de control, las políticas en plano de datos se encuentran mas enfocadas a las VPNs de servicios y como podemos manipular los datos a traves de ellas.

Algunas de las funciones:

- *Application Pinning*
- NAT/DIA
- *Classification, Policing and Marking*
- ACLs

Políticas (cont.)

Procesadas de Arriba hacia Abajo

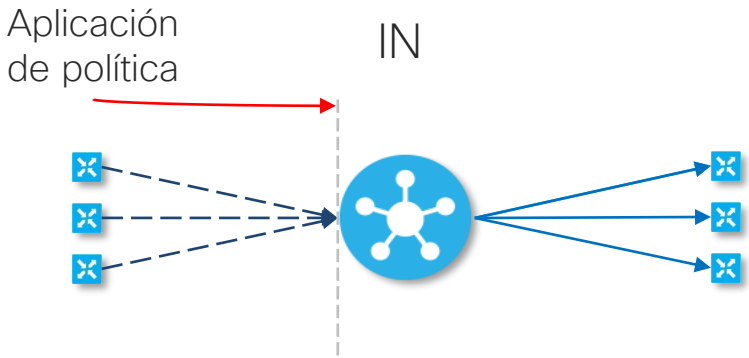
Pasos a seguir para crear una política

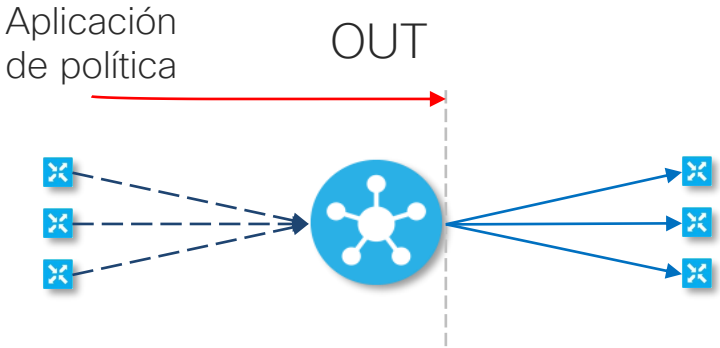
El orden es importante

Atributos

1. Creación de lista de interés
   - Ej. Application, site, TLOC, color, prefix, SLA class, VPN
2. Decidir el tipo de política a crear
   - *Control* o *Data policy*
3. Definir la secuencia
4. Definir parametros de clasificación (*match*) – en que se basara la política?
   - Ej. Ruta, TLOC, aplicación, prefijo origen/destino, protocolo
5. Definir una acción
   - *Set*
     - Ej. TLOC, preference, tag, TLOC list, service, DSCP
   - *Accept* o *reject*
6. Aplicar la Política y especificar dirección (si es necesario)
   - *IN* y/o *OUT*

Políticas (cont.)





Actualizacion de enrutamiento aplicada sin política aplicada

Actualización de enrutamiento aplicado con política aplicada

Consideraciones:

- Las políticas son aplicadas desde el punto de vista de vSmart
- Una política centralizada está compuesta de un subgrupo de políticas:
  - Data
    - Cflowd
    - App-route
  - Control
    - *VPN membership/affiliation*
- Sólo se puede aplicar una política de cada tipo por lista de sitio (site-id). Un site-id es el elemento mínimo requerido para aplicar una política.
- Se puede tener diferentes políticas de control por dirección.

Sin dirección
Por VPN

Estructura de una política de Control

```
control-policy <name>
  sequence <n>
    match tloc
      carrier <carrier>
      color <color>
      color-list <name>
      domain-id <domain-id> -Not Supported
      group-id <group-id>
      omp-tag <tag>
      originator <system-ip>
      preference <preference>
      site-id <site-id>
      site-list<name>
      tloc<tloc>
      tloc-list <name>
    !
    action accept
      set
        omp-tag <tag>
        preference <preference>
      !
    !
  !
default-action accept
!
```

```
control-policy <name>
  sequence <n>
   match route
    color <color>
    color-list <name>
    ipv6-prefix-list <name>
    omp-tag <tag>
    origin <protocol>
    originator <system-ip>
    preference <preference>
    prefix-list <name>
    site-id <site-id>
    site-list<name>
    tloc<tloc>
    tloc-list <name>
    vpn<vpn-id>
    vpn-list <name>
   !
  action accept
   export-to <vpn> | vpn-list
   set
    omp-tag <tag>
    preference <preference>
    service <service-type>
    tloc<tloc>
    tloc-action <action>
    tloc-list<name>
   !
  !
 !
 default-action accept
!
```


Source: Cisco Live BRKRST-2791

Polling Question 2

Si necesitas modificar la topología de la red, ¿qué tipo de política usarías?

A. *Control Policy*

B. *Data Policy*

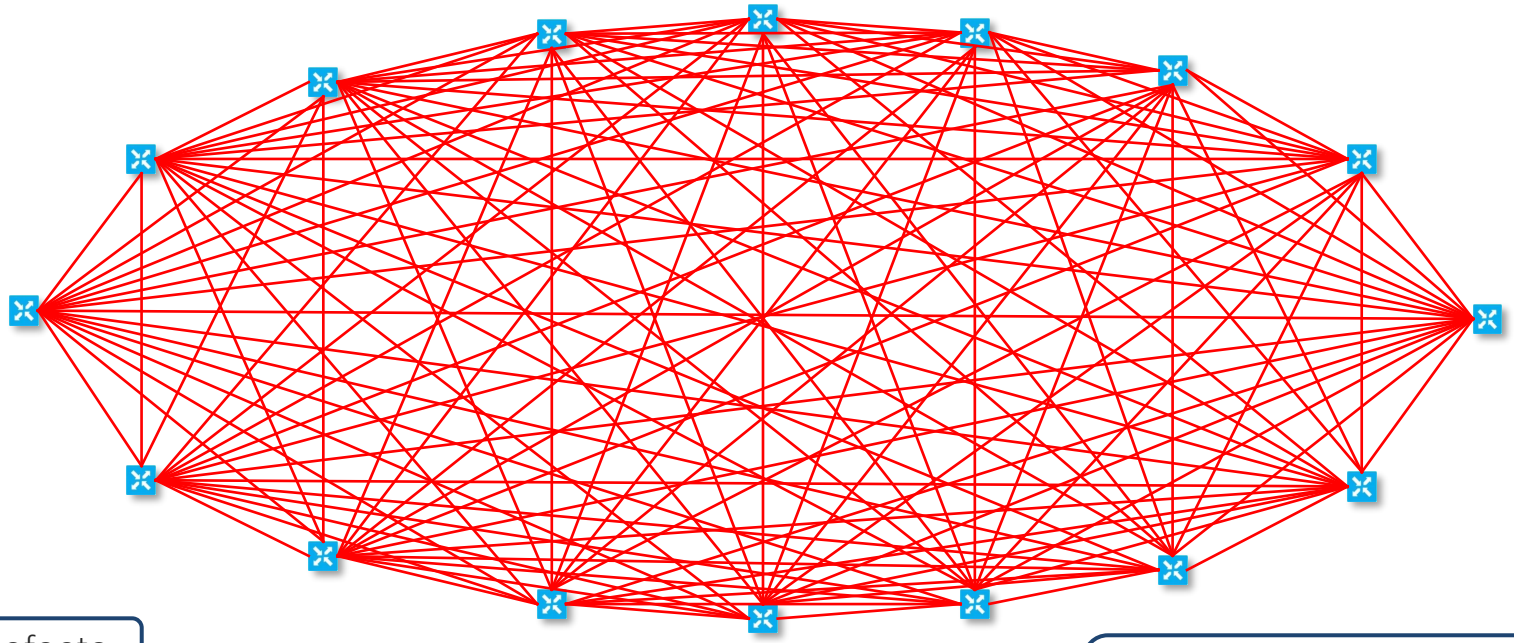
Empleando control policies para modificar la topología del overlay

Full Mesh

Optimalidad

Mayor Costo

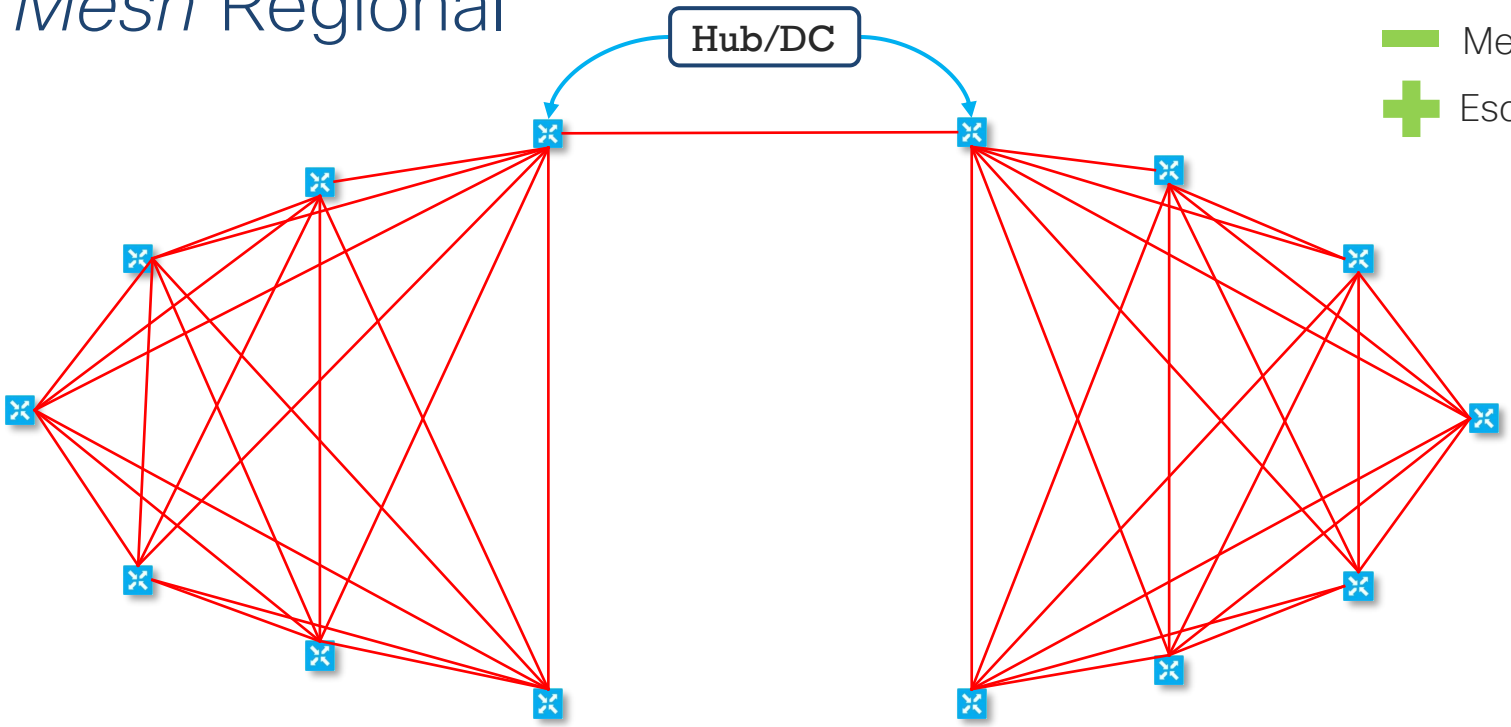
Escalabilidad



Por defecto

Cada modelo de Edge router tiene un numero límite de túneles

Full Mesh Regional



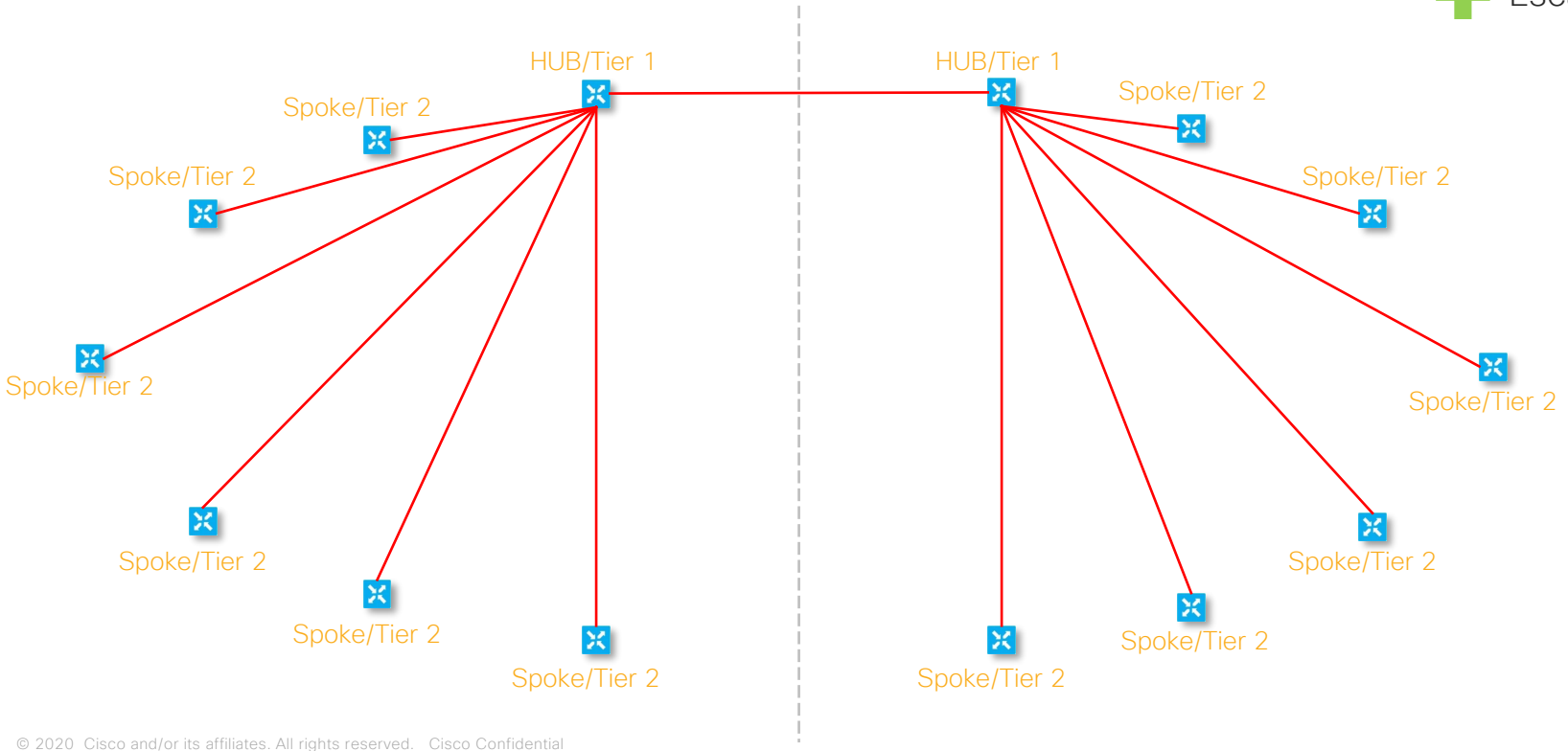
Optimalidad

Menor Costo

Escalabilidad

- ¿Necesitas *full mesh* entre regiones?
- ¿Cuántos medios de transporte tienes?
- ¿Qué tan importante es optimización vs escalabilidad?
- ¿Dónde se encuentran hospedados tus servicios y aplicaciones?

Regional hub & spoke (2 tier)



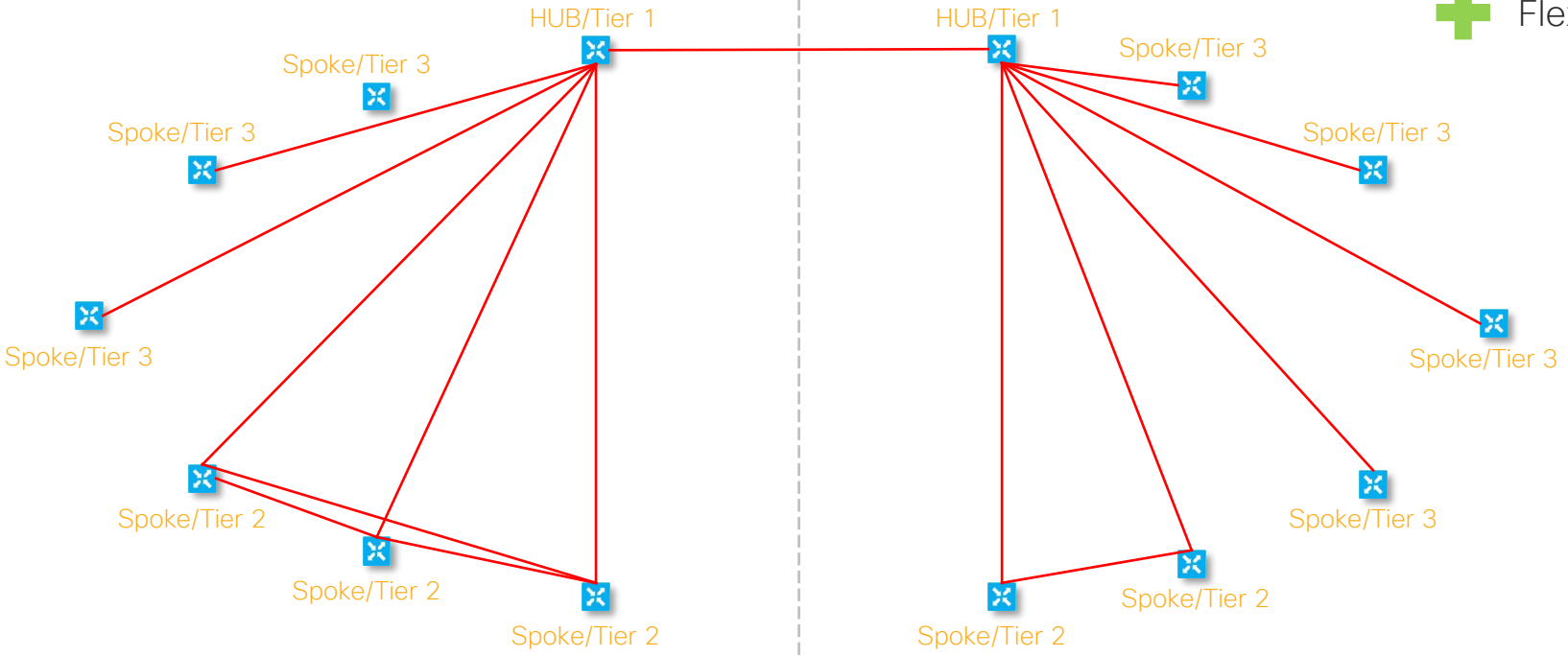
Regional Hub/Spoke (3 Tier)

Optimalidad

Menor Costo

Escalabilidad

Flexibilidad

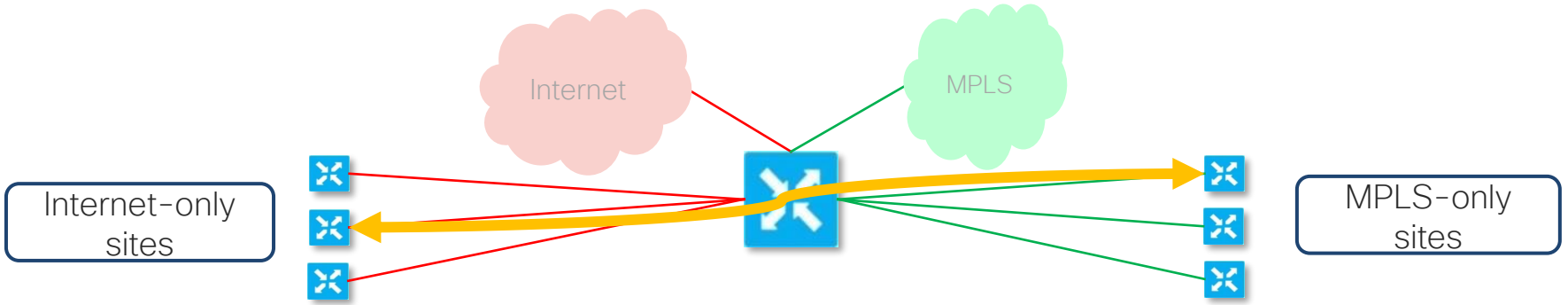


Conectando planos de datos discontinuos

Cuando algunos sitios poseen solo un tipo de transporte y los mismos no son compatibles, una política puede ser instalada para conectar estos medios de transporte a través un sitio conectado a ambos transportes. Ej. *Dual homed*.

La comunicación se realizará a través del hub. Tan pronto como el TLOC remoto sea valido.

- Los túneles del plano de datos serán formados entre los WAN Edge *routers* a través del HUB.



Empleando data policies para proporcionar una mejor experiencia del usuario

Políticas de plano de datos (*Data Policies*)

Contrarias a las políticas de control, las políticas en plano de datos operan a lo ancho de las VPNs, sin interfaces especificas. Diferentes políticas pueden ser aplicadas a diferentes VPNs.

- Aplicadas en el vSmart, publicadas y ejecutadas en los WAN Edge

Algunos posibles servicios son:

- Application Pinning
- NAT/DIA
- Classification, Policing and Marking

Estructura de una política de Datos

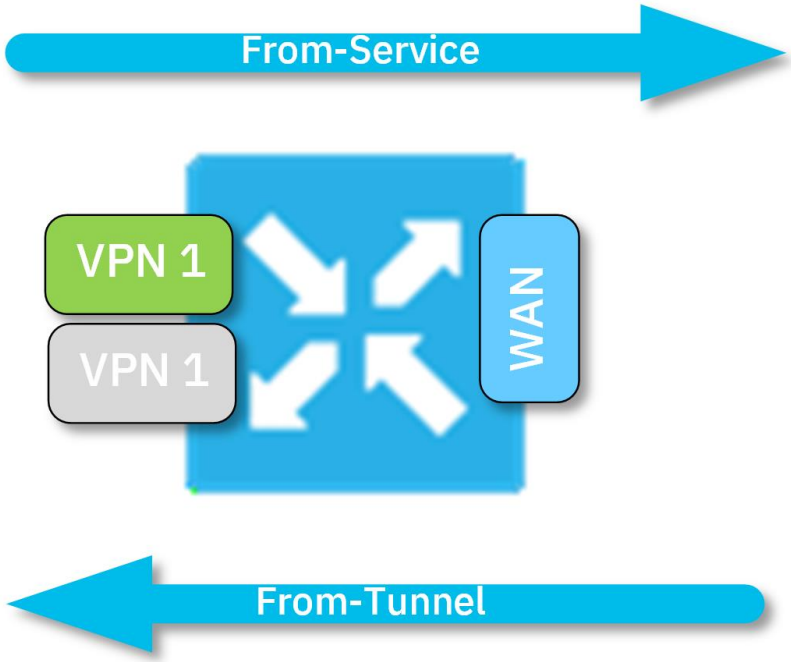
```
data-policy <name>
 vpn-list <name>
  sequence <n>
   match
    app-list <name>
    destination-data-ipv6-prefix-list <name>
    destination-data-prefix—list <name>
    destination-ip<ip-address>
    destination-ipv6 <ipv6-address>
    destination-port <port>
    dnsrequest | response
    dnsapp-list <name>
    dscp<dscp>
    packet-length <length>
    plp<plp>
    protocol <protocol>
    source-data-ipv6-prefix-list <name>
    source-data-ip-prefix-list <name>
    source-ip<ip-address>
    source-ipv6 <ipv6-address>
    source-port <port>
    tcp-syn
   !
  !
```

```
  action
    accept
     set
      dscp<dscp>
      forwarding-class <name>
      local-tloc<tloc>
      local-tloc-list <list>
      next-hop <ip-address>
      next-hop-ipv6 <ipv6-address>
      policer <name>
      service <name>
      tloc<tloc>
      tloc-list <name>
      vpn<vpn-id>
     cflowd
     count <counter>
     drop
     log
     loss-protect-fec-always
     loss-protect-fec-adaptive
     loss-protect-packet-dup
     nat-pool <nat-pool>
     natuse-vpn<vpn-id>
     redirect dns
     tcp-optimization
    !
   !
  !
 !
!
default-action accept
```

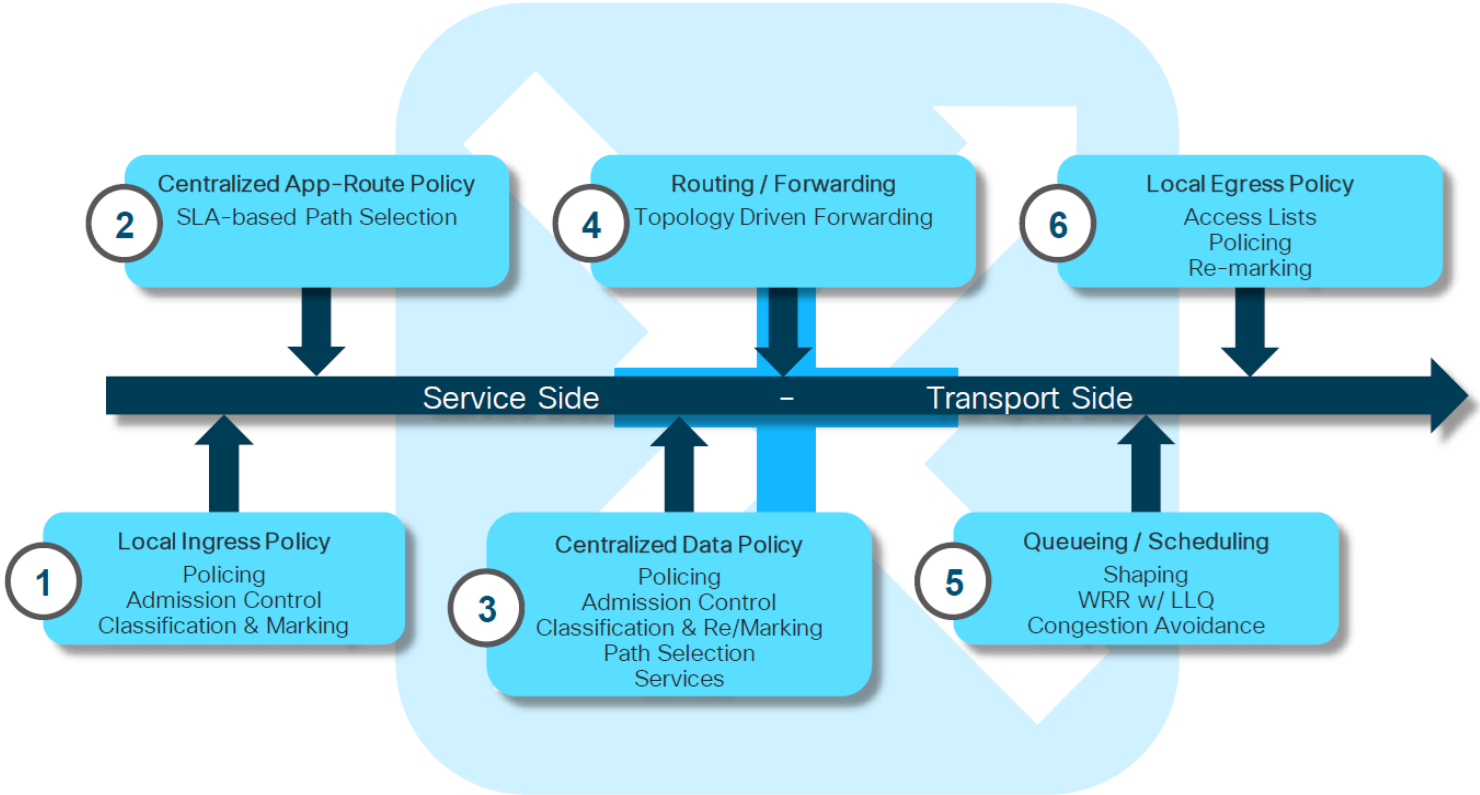

Source: Cisco Live BRKRST-2791

Aplicación de políticas de datos

- Pueden ser aplicados de 3 maneras:
  - *From-Service* (Upstream)
  - *From-Tunnel* (Downstream)
  - *All* (Ambos *Upstream y Downstream*)
- Diferentes políticas pueden ser aplicadas en distintas direcciones.
- El metodo de uso más común es *Upstream*



Orden de Operaciones



Source: [Cisco Live BRKRST-2791]

Polling Question 3

¿Cuál polÍtica deberÍas usar para configurar *Application Pinning* en Cisco SD-WAN?

A. *Control policy*

B. *Data Policy*

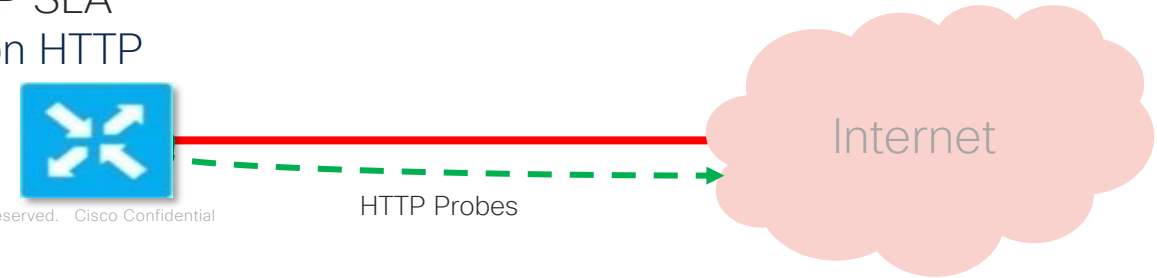
Dedicated Internet Access (DIA)

DIA puede ser implementado en diferentes maneras segun la configuración de los WAN Edge:

- *Localized*
  - Basado en la tabla de enrutamiento de la VPN 0
- *Centralized*
  - Via Política de datos – Tomando ventaja de varias interfaces de Internet y el balanceo de carga.

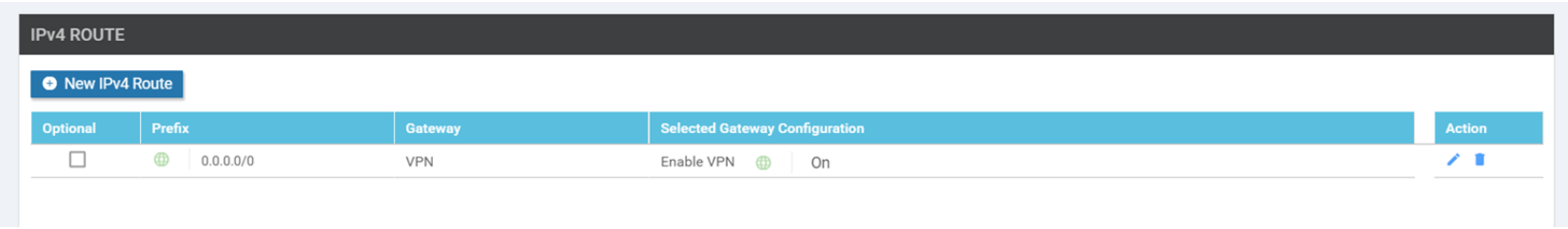
T*racking* puede ser configurado para verificar el funcionamiento de un servicio en Internet. Y asi garantizar disponibilidad en la conexion a Internet más alla del primer salto.

- Similar a IP SLA
- Probes son HTTP



DIA – Trafico hacia Internet en VPN 0

- Ruta estatica en la VPN de servicio hacia VPN 0
- NAT habilitado en los transportes hacia Internet en VPN 0
- Sin clasificar o discriminar trafico en particular (*no matching*)
- La carga de tráfico es compartida por los transportes disponibles
- Puede usar *tracker* para evitar la perdida de trafico debido a *blackholing*



DIA utilizando política de datos

- Más granular que rutas en la VPN de servicio
  - *Matching* en prefijos y *puertos*
- Solo manipulando tráfico web.
  - Podría identificar, por ejemplo, O365 y otras aplicaciones en la nube
- Se puede especificar el medio de transporte de salida.

```
data-policy DIA
  vpn-list VPN-10
    sequence 1
     match
      destination-data-prefix-list
INTERNAL-NETWORKS
     !
     action accept
     !
    !
    sequence 11
     match
      destination-port 80 443
      source-ip 0.0.0.0/0
     !
     action accept
      nat use-vpn 0
```

DIA con *Service Chaining*

- Redirecciona tráfico a servicio local
  - En el ejemplo: GRE tunnel
  - Haciendo uso de Umbrella SIG o zScaler
- Túneles GRE o IPSec son configurados localmente

```
policy
 data-policy Web_Firewall
  vpn-list vpn_all
   sequence 10
    match protocol 6
    match destination-port 80 443
    !
    action accept
     set
      service FW local
     !
    !
   !
   default-action accept
```

Application Aware Routing (AAR)

Por defecto un WAN Edge usara los transportes disponibles, donde el tráfico se distribuirá entre ellos.

- En pocas palabras: **PBR con esteroides**
  - Permite coincidir multiples valores dentro de paquetes IP, entre estos valores tenemos: Source and destination IP addresses
    - Puertos de origen y destino.
    - Protocolos de transporte (capa 4)
    - Marcado de paquetes DSCP
    - Aplicaciones – usando DPI

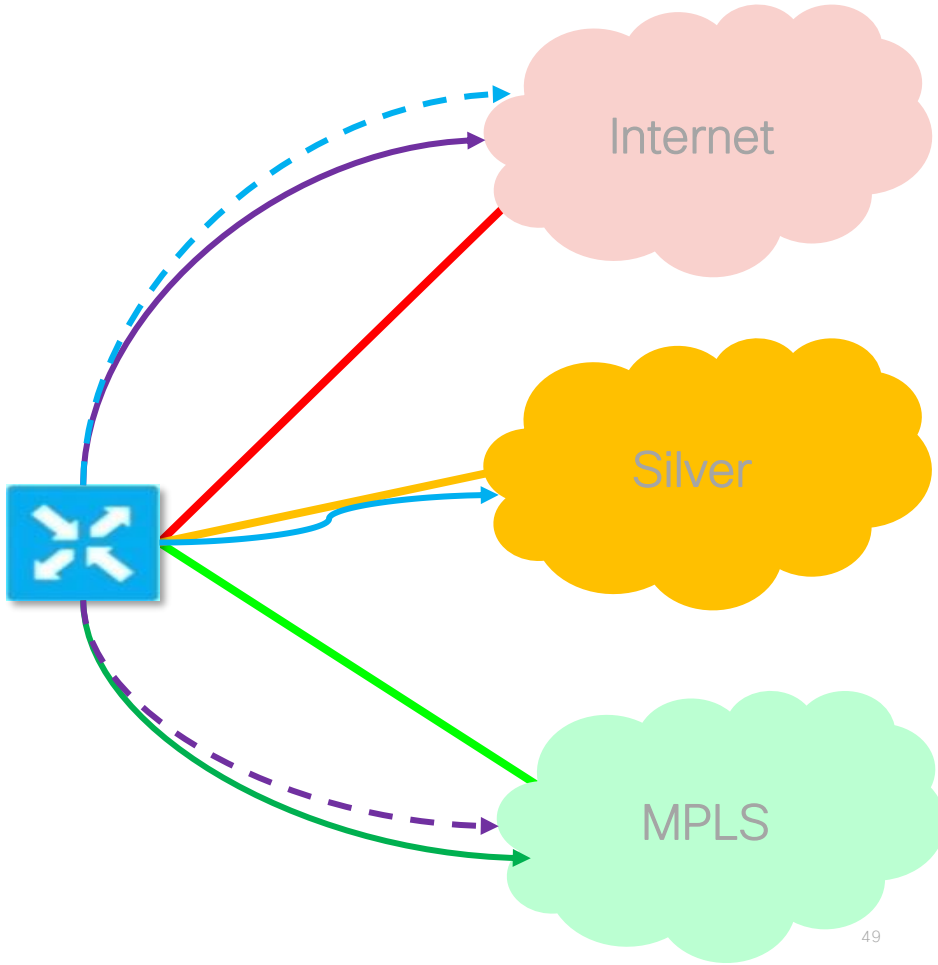
Hay un límite en el numero de flujos por modelo.

- Despues de hacer *matching*, los paquetes serán enviados de acuerdo a ciertos criterios.
  - Medio de transporte especifico
    - Ej. Si el enlace a Internet no está disponible, nadie podrá navegar a *Facebook o Youtube.*
  - Conociendo los SLAs (perdida de paquetes, delay, jitter)
    - Ej. Si el enlace de MPLS de un ISP muestra alta latencia, el tráfico sera trasladado de manera automatica a otro enlace menos congestionado.

Application Pinning

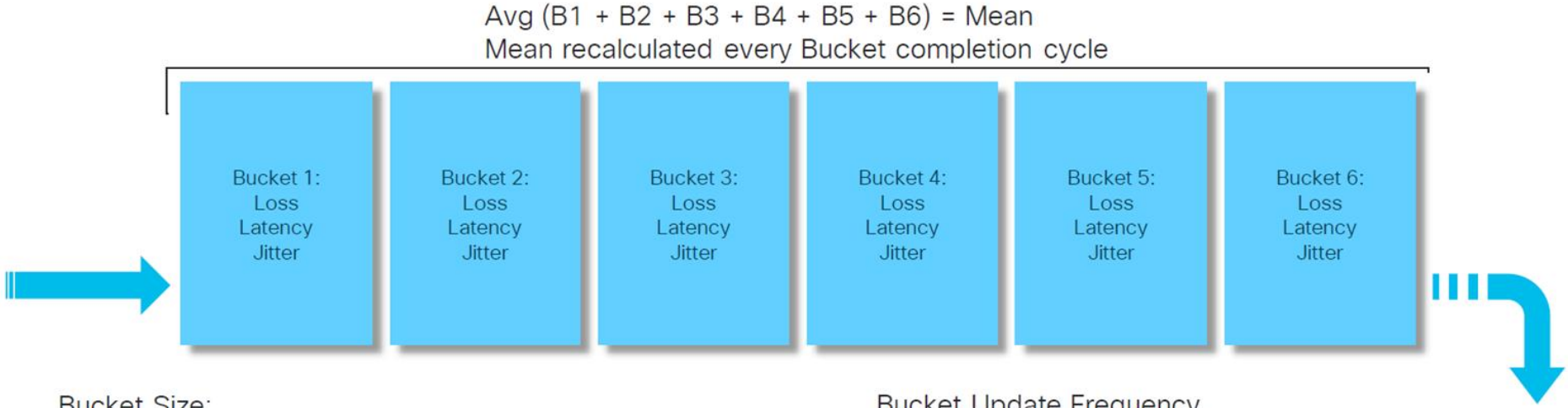
- Si las condiciones de un enlace satisfacen los parametros de un especifico SLA, un enlace de respaldo puede ser utilizado (si esta en modo *loose*)
- Modo *strict*, la aplicacion podría unicamente funcionar sobre un enlace o medio de transporte especifico.

App1 – Primary path
App1 – Backup path
App2 – Primary path
App2 – Backup path
App3 – Primary path



Algoritmo App-Route

No hay fail-over inmediato – estabilidad vs detección de fallas



Bucket Size:

```
bfd
 app-route poll-interval
```
(default 600,000 ms)

# of Buckets:

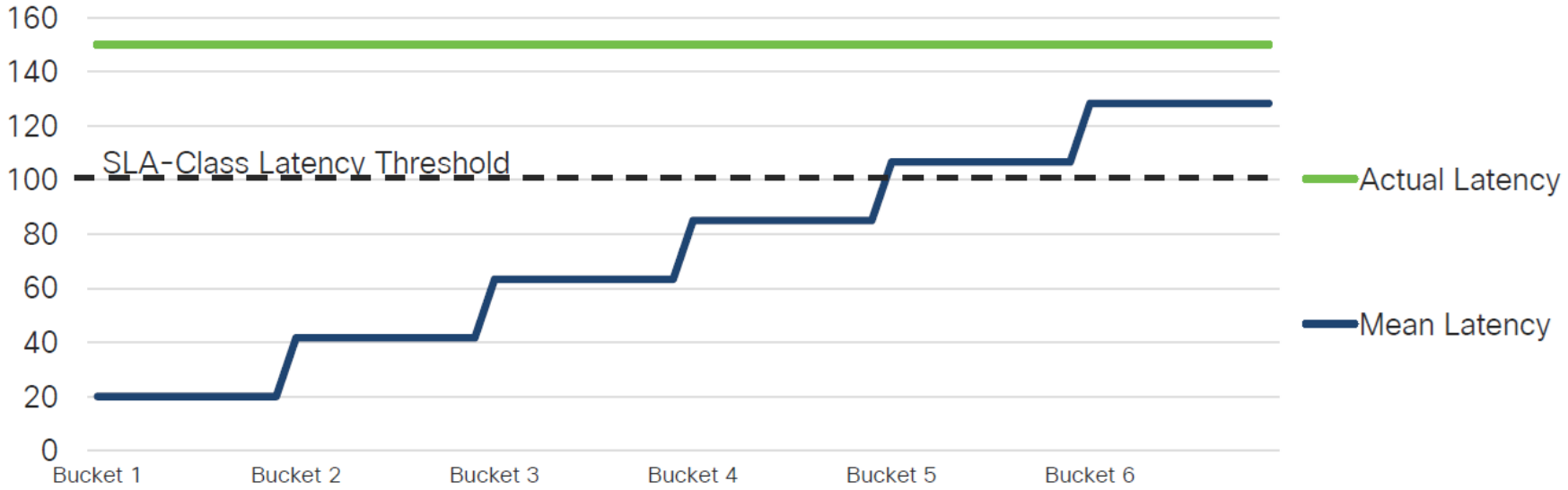
```
bfd
 app-route multiplier
```
(default 6)

Bucket Update Frequency

```
bfd
 hello-interval
```
(default 1000ms)

Source: Cisco Live BRKRST-2791

Convergencia de App-route



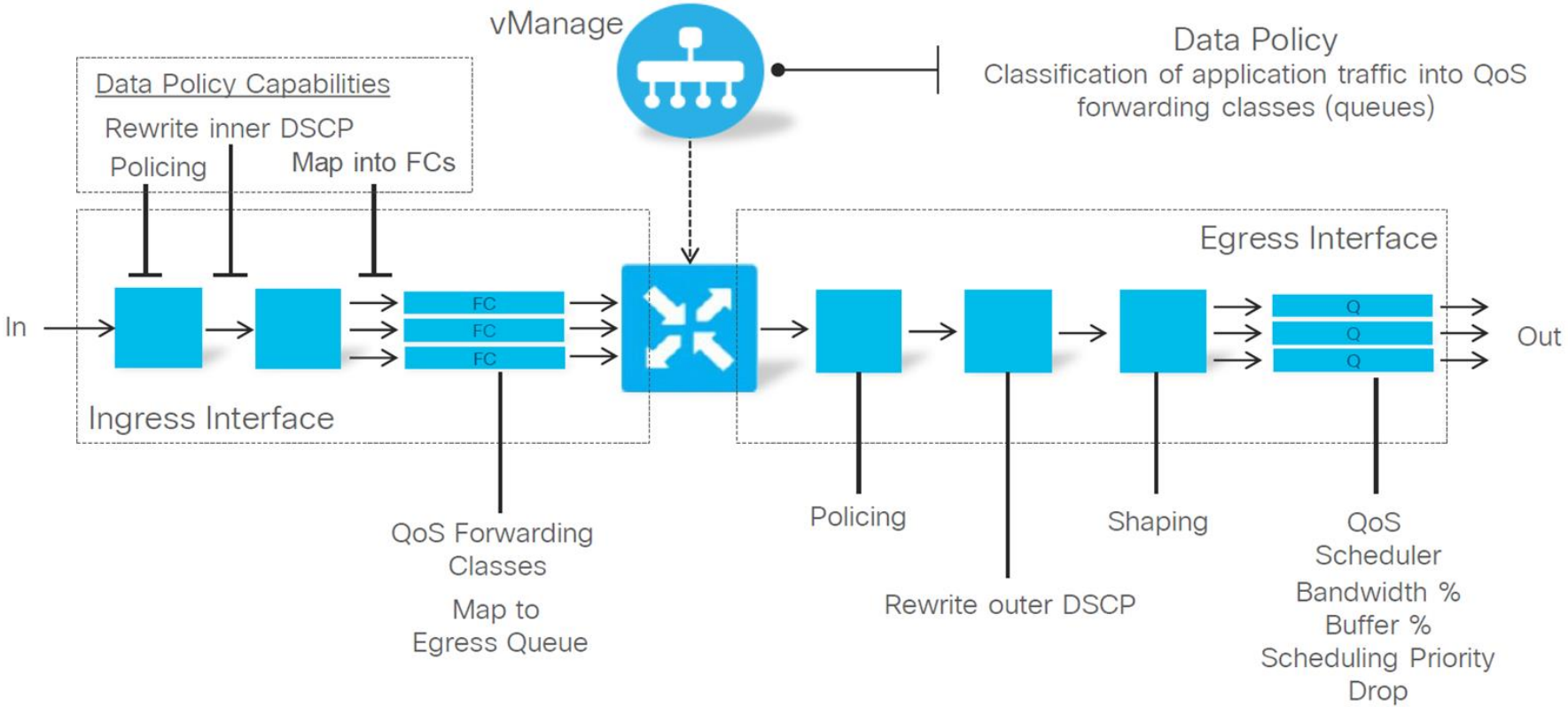
Current Mean Latency is 20ms, when Latency jumps to 150ms as Bucket 1 collection starts

Source: Cisco Live BRKRST-2791

QoS – Calidad de servicio

- Configurado a través de política *localized* (localizada)
- Soporta:
  - Policing
  - Shaping (congestion management)
  - Congestion avoidance (RED) y tail drop
  - Rewrite DSCP

QoS – Calidad de servicio (cont.)



Source: Cisco Live BRKRST-2791

Política de QoS a través de vManage

CONFIGURATION | POLICIES Localized Policy > Forwarding Class/QoS > View QoS Map Policy

Name: Policy-QoS

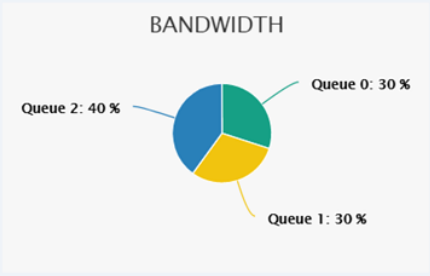
Description: QoS policy

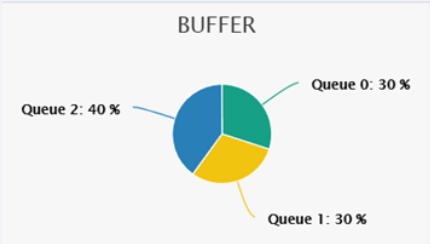
Add Queue

Search Options

Total Rows: 3

Queue	Bandwidth %	Buffer %	Burst	Scheduling Type	Drop Type	Forwarding Class
0	30	30	15000	Low Latency Queuing(LLQ)	Tail	Control
1	30	30	-	Weighted Round Robin(WRR)	Random Early	Citrix
2	40	40	-	Weighted Round Robin(WRR)	Random Early	Bulk





Polling Question 4

Con la experiencia de esta sesión, ¿Crees que puedes usar tu implementación de Cisco SD-WAN más eficientemente?

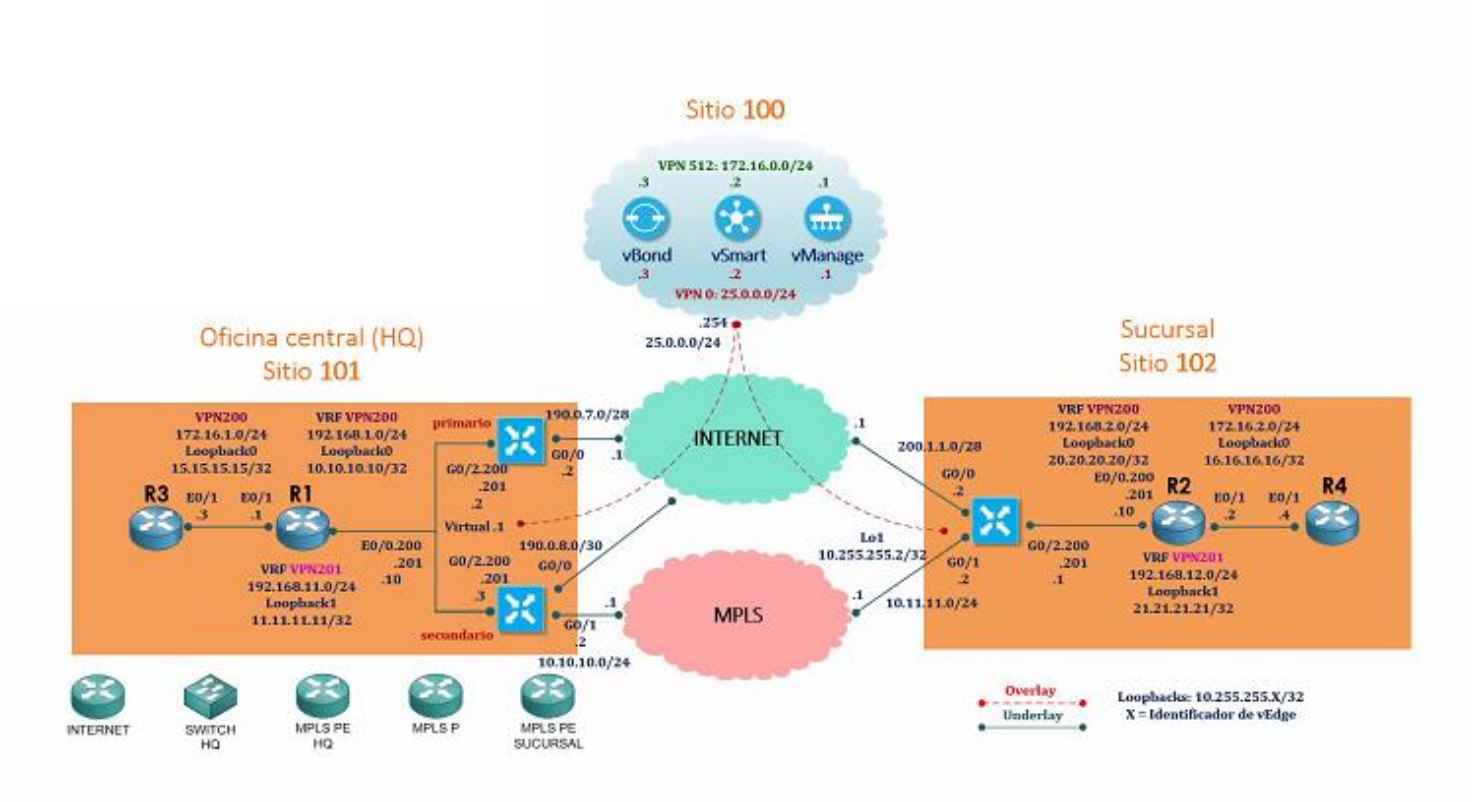
A. Si

B. No

C. No aplica

Demo

Topología



¡Gracias!

Resuelva sus dudas

Utilice el panel de Q&A o P&R para realizar sus preguntas

Ask Me Anything- Sesión del evento

Hasta el Viernes 30 de Octubre, 2020

Con
Eduardo & David

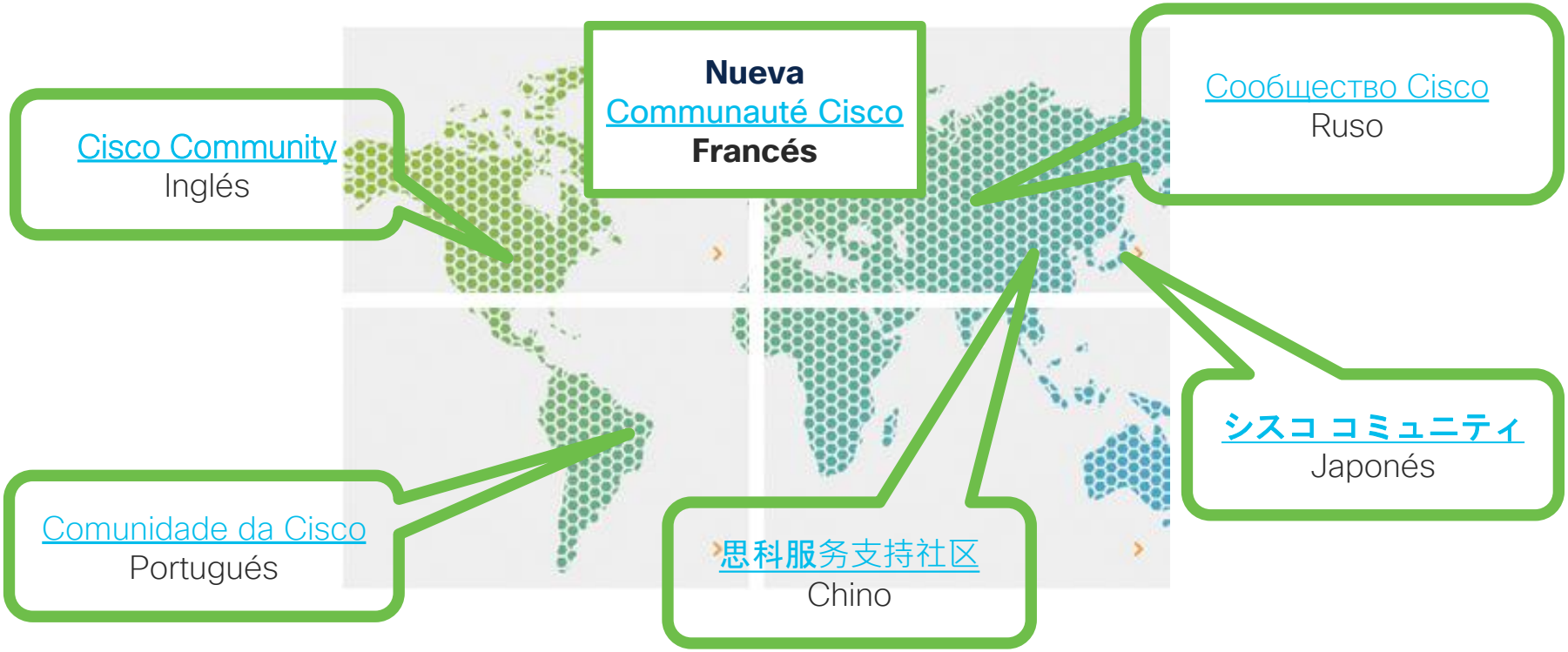
http://bit.ly/foro-sdwan-politicas

Julio Moisa
Director General & Co-Fundador
3xCCIE (#52536)

Luis Celis
Lead Network Consulting Engineer

La Comunidad de soporte tiene otros Idiomas

Si habla Portugués, Japonés, Ruso, Chino o Inglés lo invitamos a participar en otro idioma.



Lo invitamos a nuestros próximos eventos en Redes Sociales

Twitter

- @CiscoTSLatam
- @cisco_spain
- @cisco_support
- @Cisco_LA

Facebook

- Cisco TS- Latam
- Cisco España
- Cisco Latinoamérica
- CiscoCommunity

Lo invitamos a nuestros próximos eventos en Redes Sociales

YouTube

- CiscoLatam
- ciscocommunity

App

- Cisco Technical Support

LinkedIn

- Cisco Community

¡Nos interesa su opinión!

Por favor complete la encuesta,
aparecerá en la pantalla de su buscador

¡Gracias por acompañarnos en el evento, cuídense!


CISCO