

## 28. Cisco Viptela SDWAN设计



教主技术进化论 2021

*翻越下一座技术的高峰*



# 目录

1. Cisco Viptela SDWAN
2. Cisco Viptela 架构与组件
3. Cisco Viptela 控制层面
4. Cisco Viptela Edge部署



# 1 Cisco Viptela SDWAN



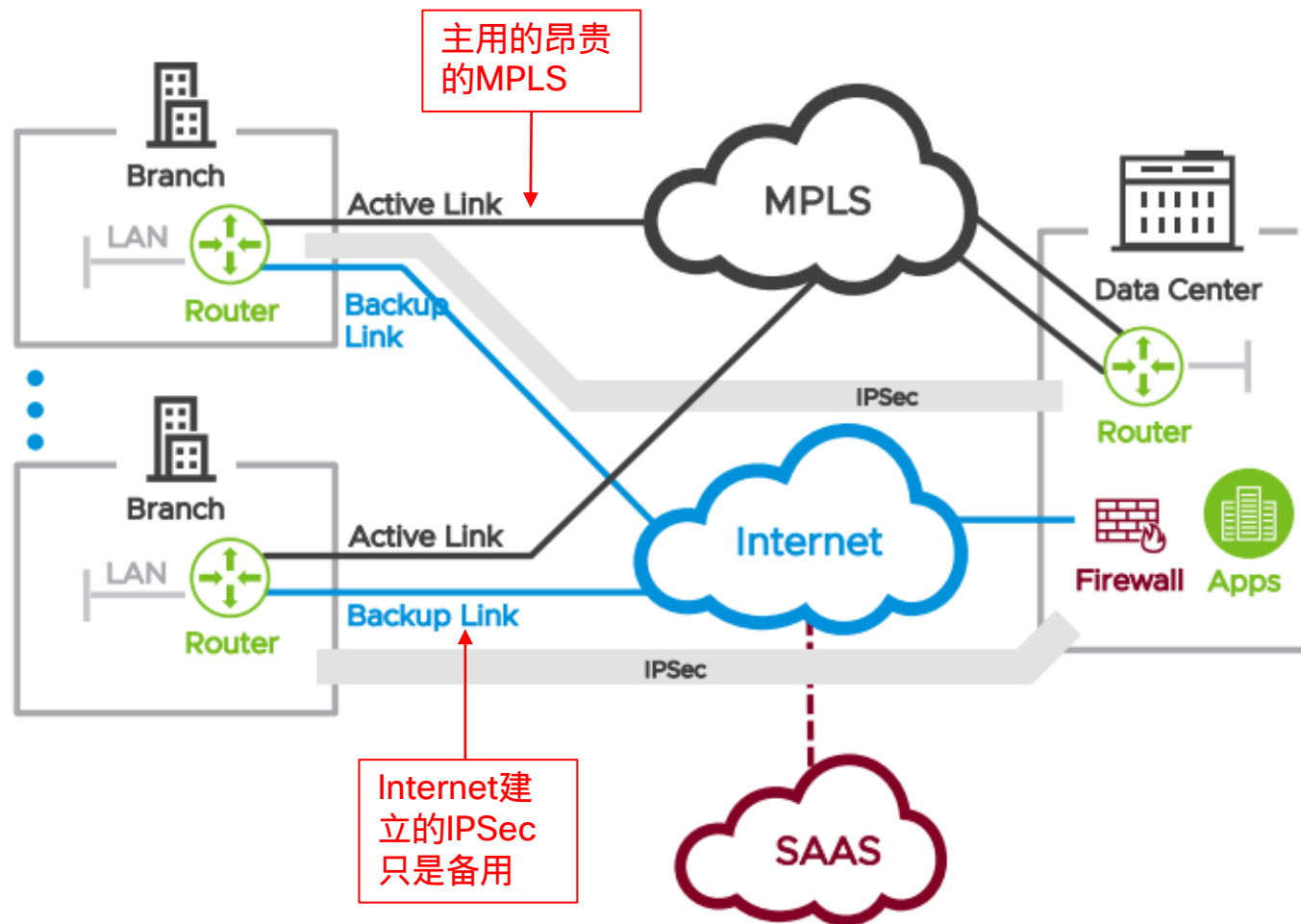
# Cisco 重回领导者





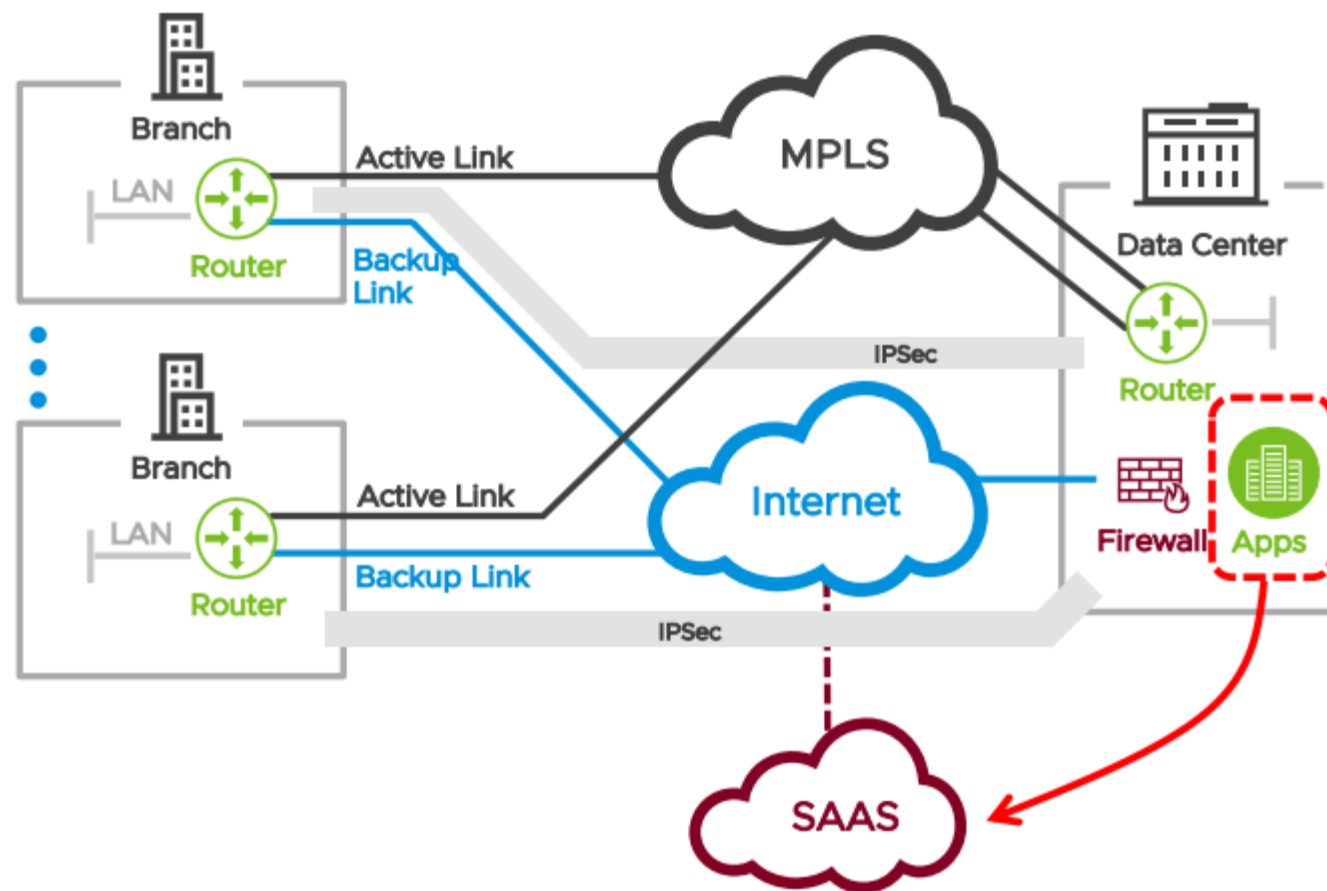
# 当前的企业WAN

效率低下





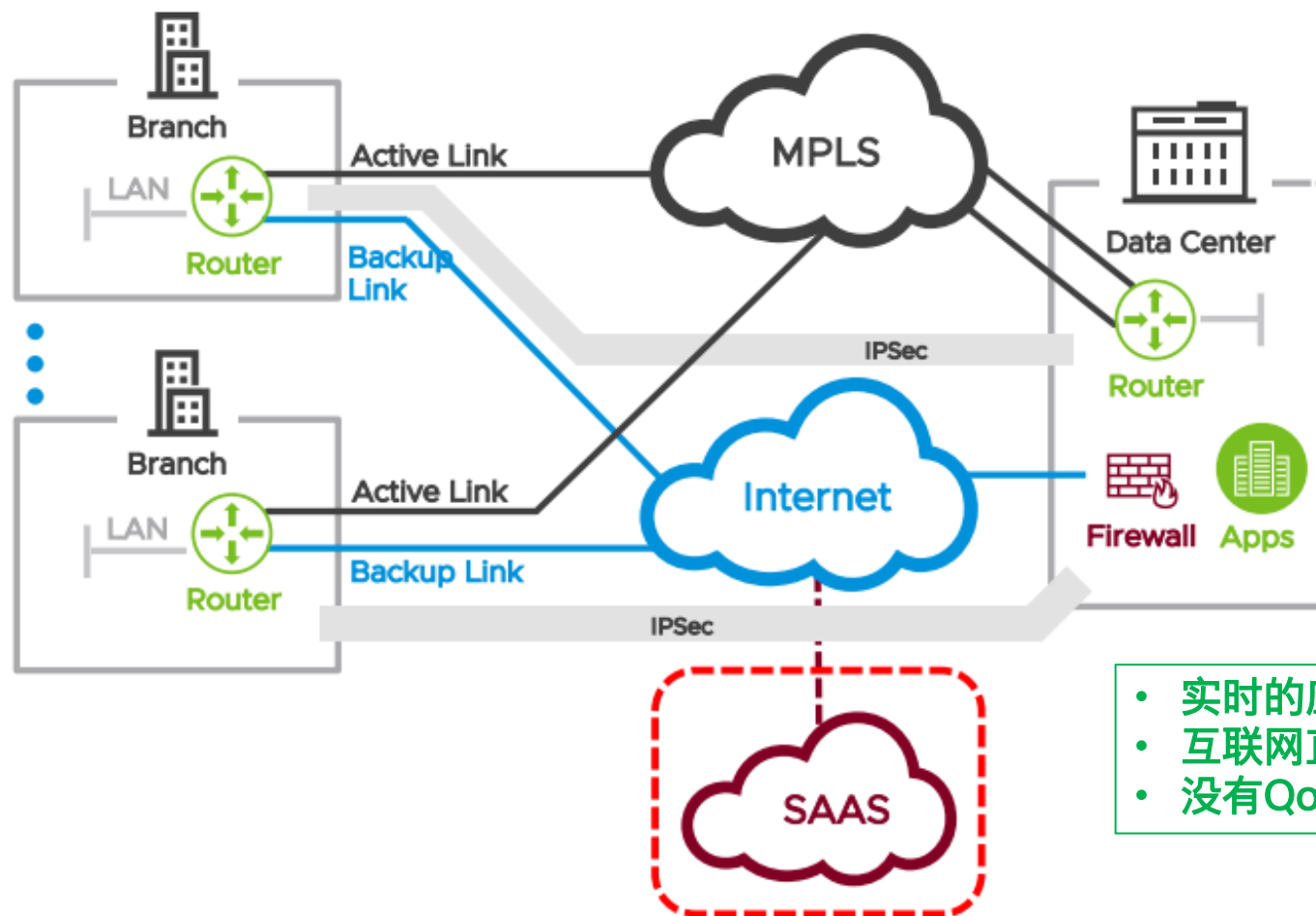
# 当前的企业WAN



- 应用正在逐步的迁移到云
- 数据中心不断被整合



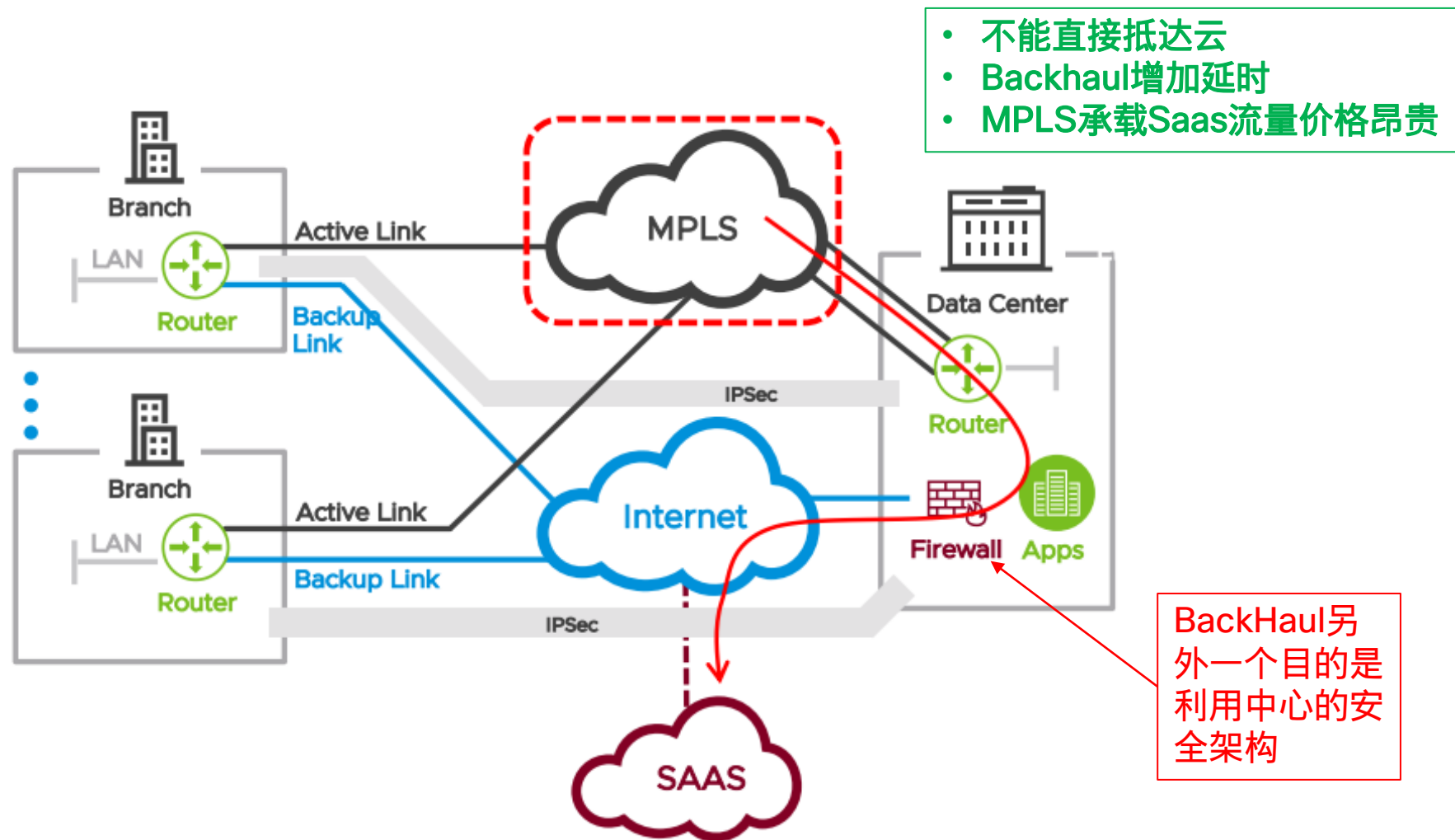
# 当前的企业WAN



- 实时的应用 (例如:VoIP)
- 互联网直接可达
- 没有QoS/SLA



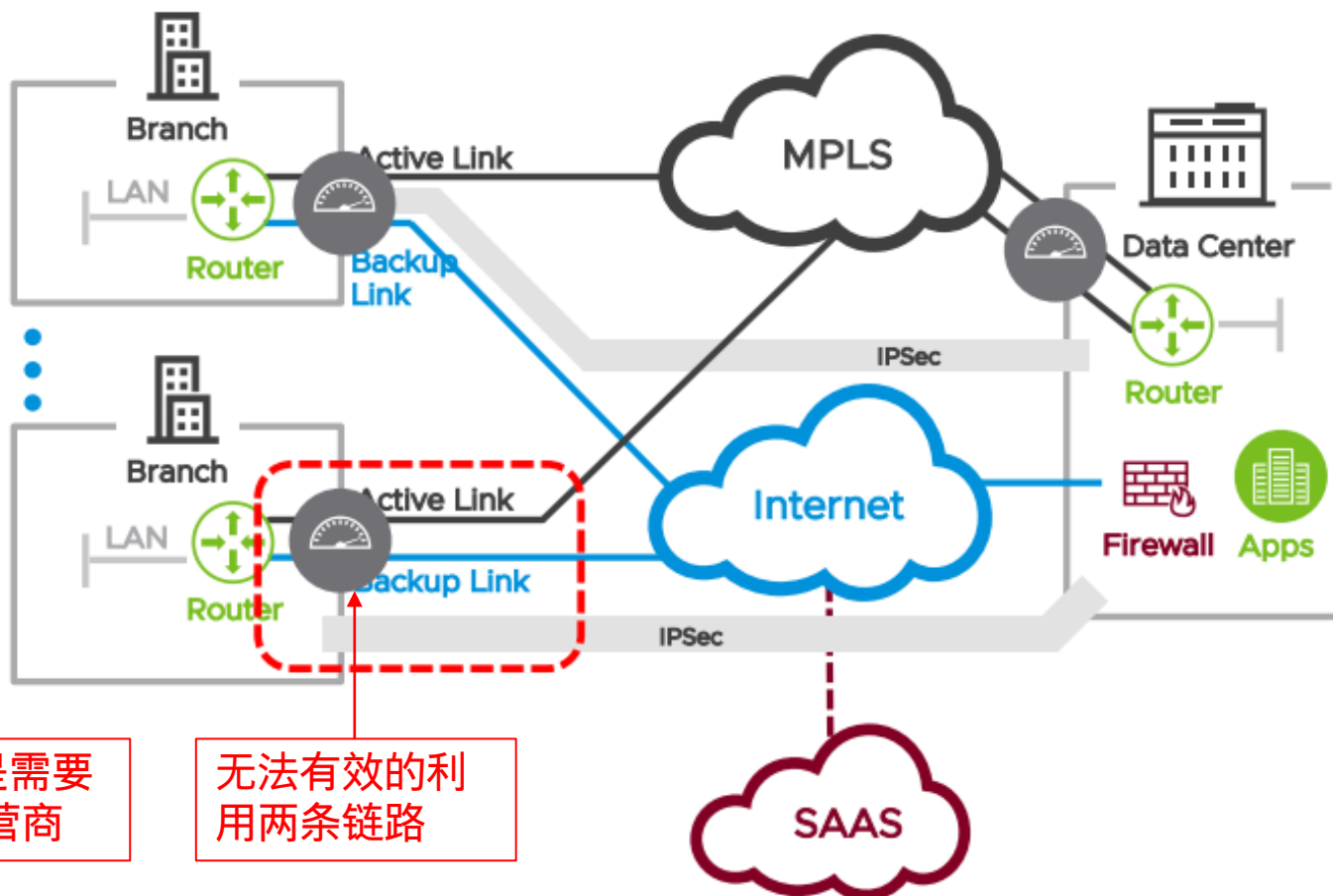
# 当前的企业WAN







# 当前的企业WAN



- MPLS带来费用压力
- 无法实现相同质量的链路冗余
- ISP集中和锁定风险

MPLS总是需要  
用一个运营商

无法有效的利用  
两条链路

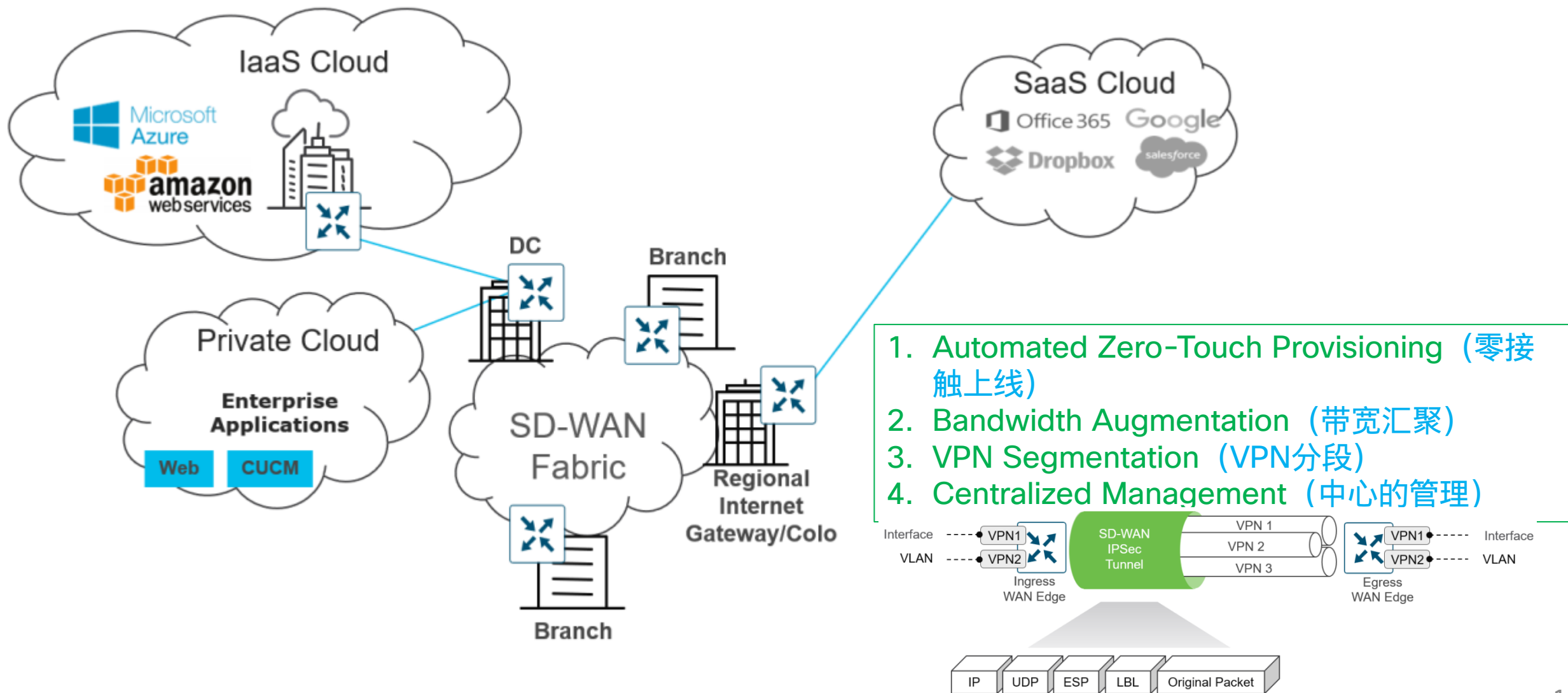


## 四大使用场景

Use Case	Description
Secure Automated WAN <span data-bbox="580 501 945 568">安全自动的广域网</span>	Secure connectivity between remote offices, data centers, and public/private cloud over a transport independent network
Application Performance Optimization <span data-bbox="644 601 937 668">应用性能优化</span>	Improves the application experience for users at remote offices
Secure Direct Internet Access <span data-bbox="708 762 945 829">安全的DIA</span>	Locally offloads Internet traffic at the remote office
Multicloud Connectivity <span data-bbox="593 868 810 935">多云链接</span>	Connects remote offices with cloud (SaaS and IaaS) applications over an optimal path and through regional colocation/exchange points where security services can be applied.



# 安全自动的广域网

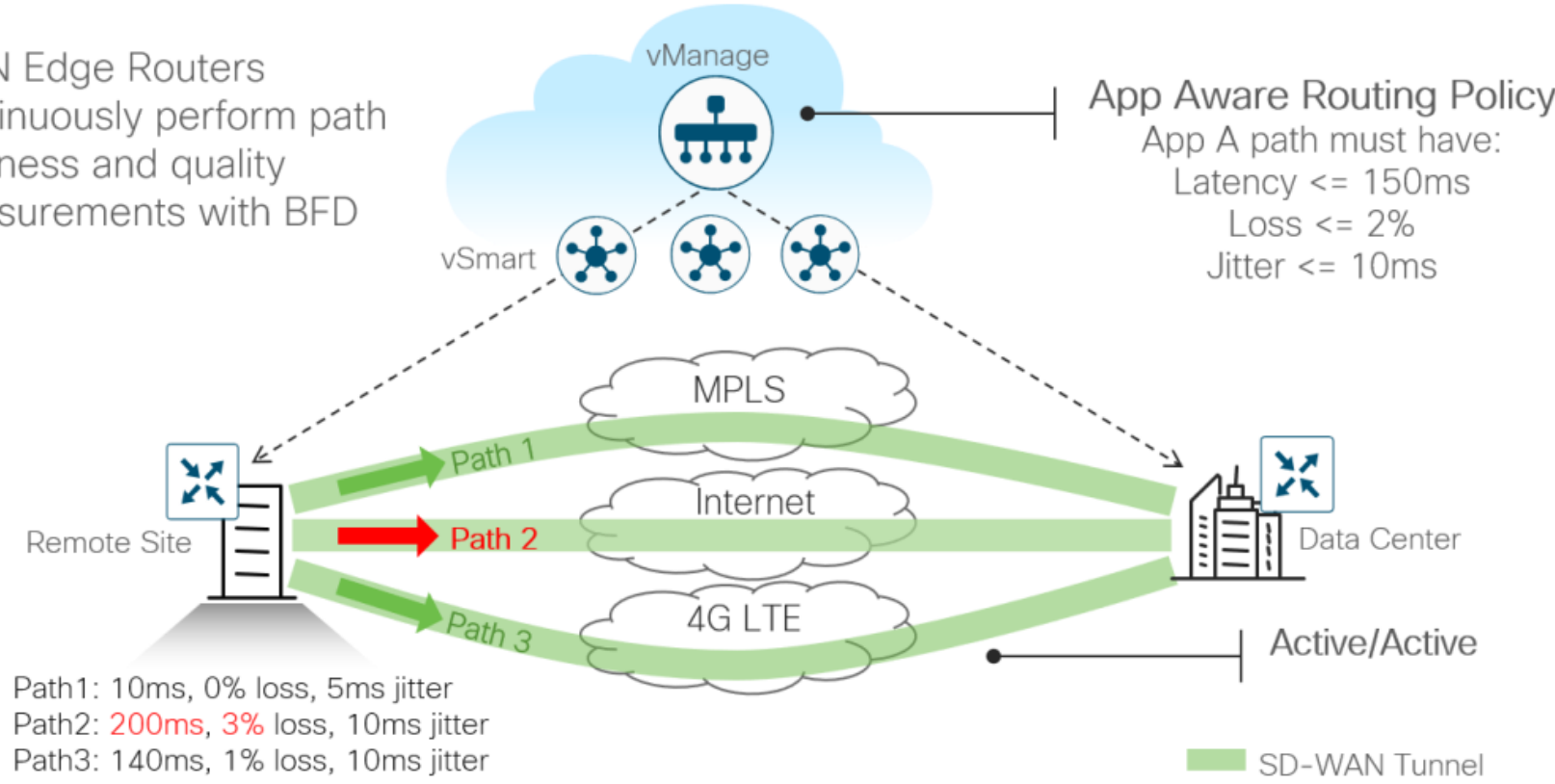


1. Automated Zero-Touch Provisioning (零接触上线)
2. Bandwidth Augmentation (带宽汇聚)
3. VPN Segmentation (VPN分段)
4. Centralized Management (中心的管理)

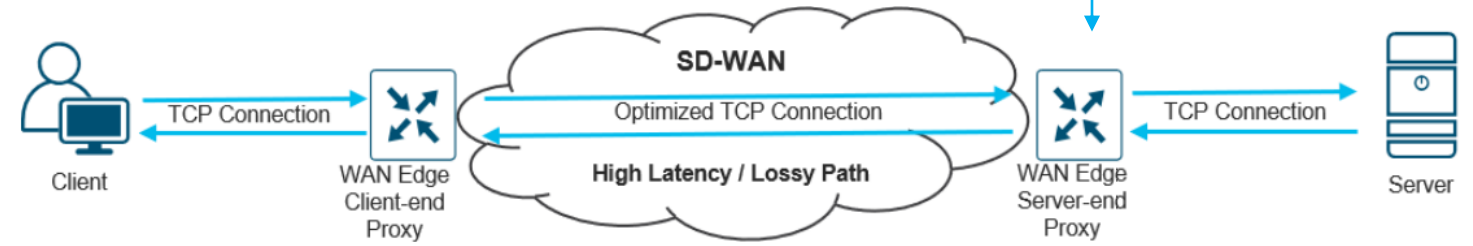


# 应用性能优化

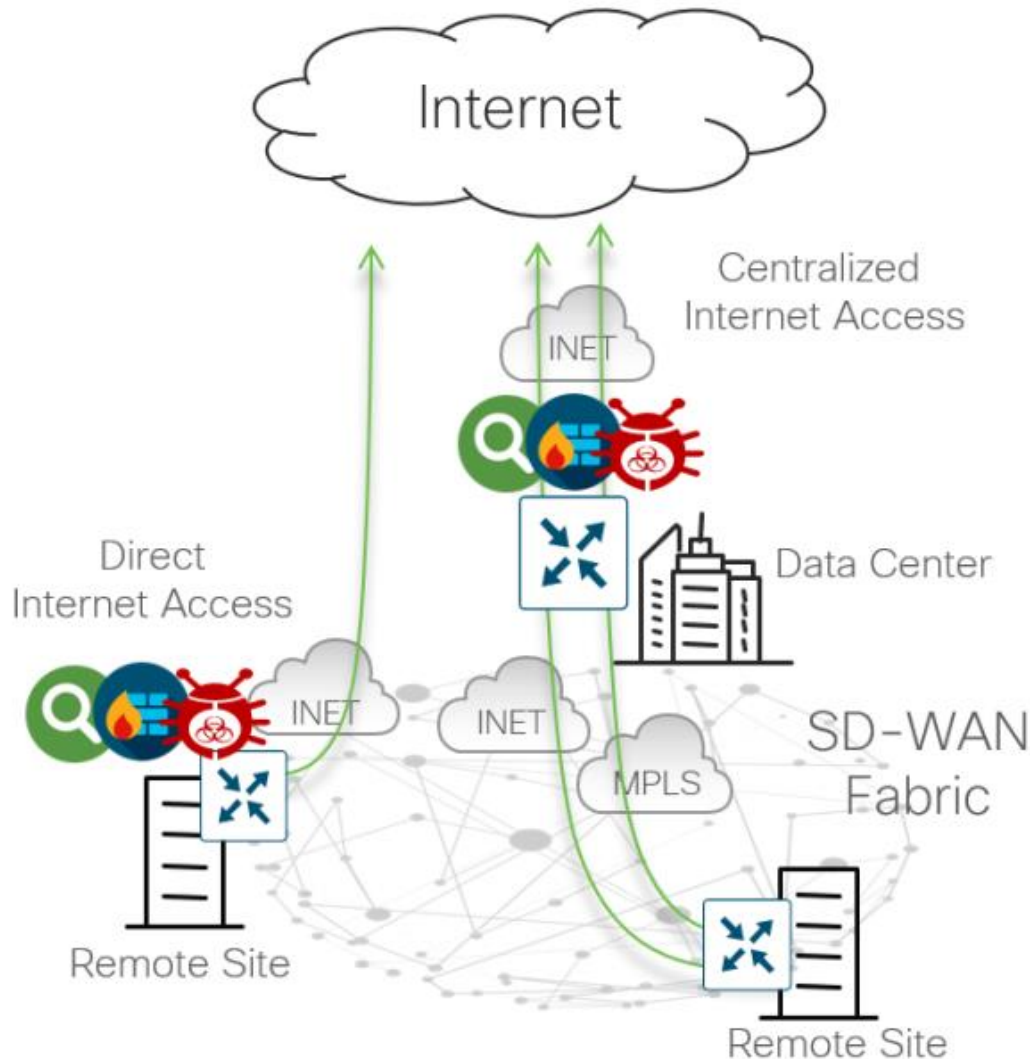
WAN Edge Routers continuously perform path liveliness and quality measurements with BFD



1. Application-Aware Routing (应用感知的路由)
2. Quality of Service (QoS)
3. Forward Error Correction (FEC) and Packet Duplication
4. TCP optimization and Session Persistence (TCP优化和会话持久)



## 安全的DIA



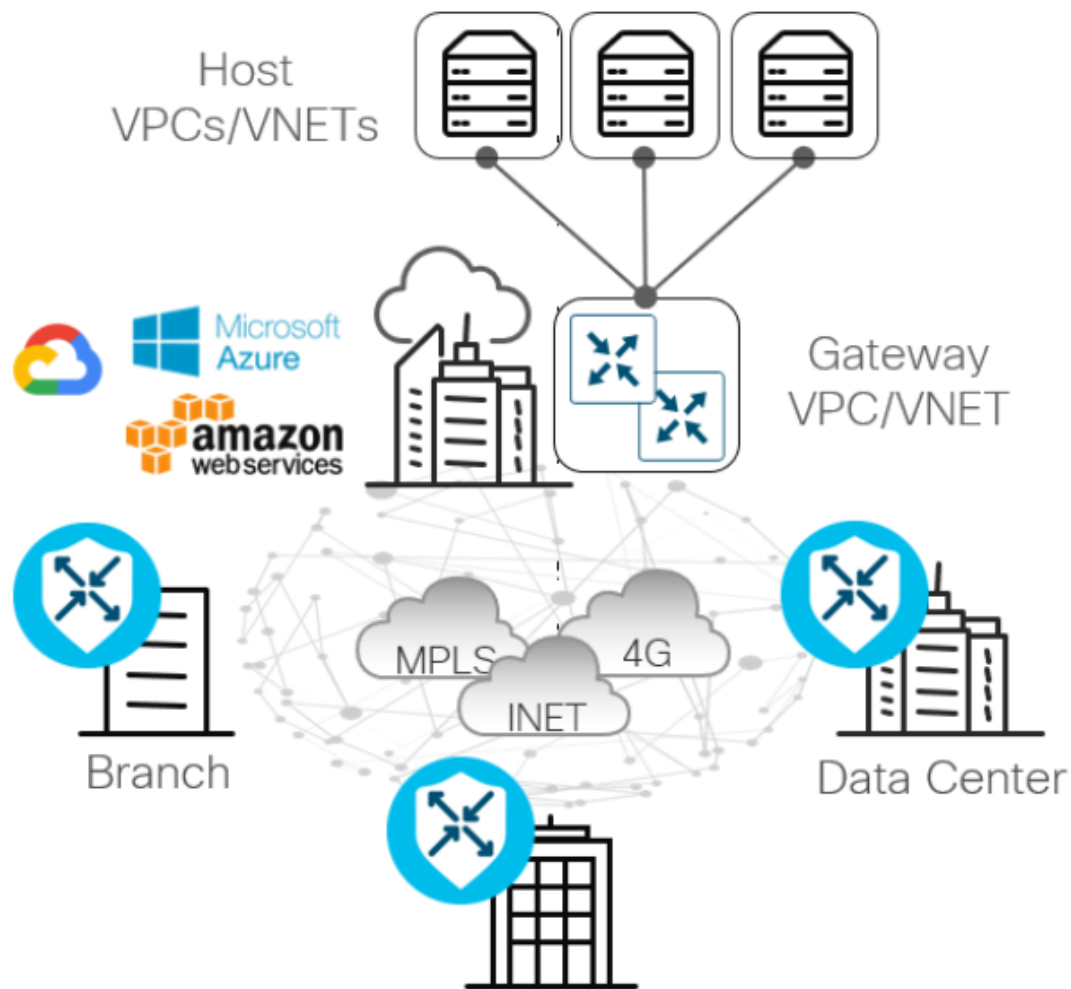
DIA can pose security challenges as remote site traffic needs security against Internet threats. Cisco SD-WAN can help solve this by leveraging the **embedded SD-WAN security features on IOS XE SD-WAN devices** or utilizing a Secure Internet Gateway (SIG), the **Cisco Umbrella Cloud**.

IOS XE SD-WAN security features include **Enterprise Application-Aware Firewall, Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), DNS/Web Layer Security, URL Filtering, SSL Proxy, and Advanced Malware Protection (AMP)**. vEdge routers natively support an application-aware firewall. **The Cisco Umbrella Cloud unifies several security features and delivers them as a cloud-based service**

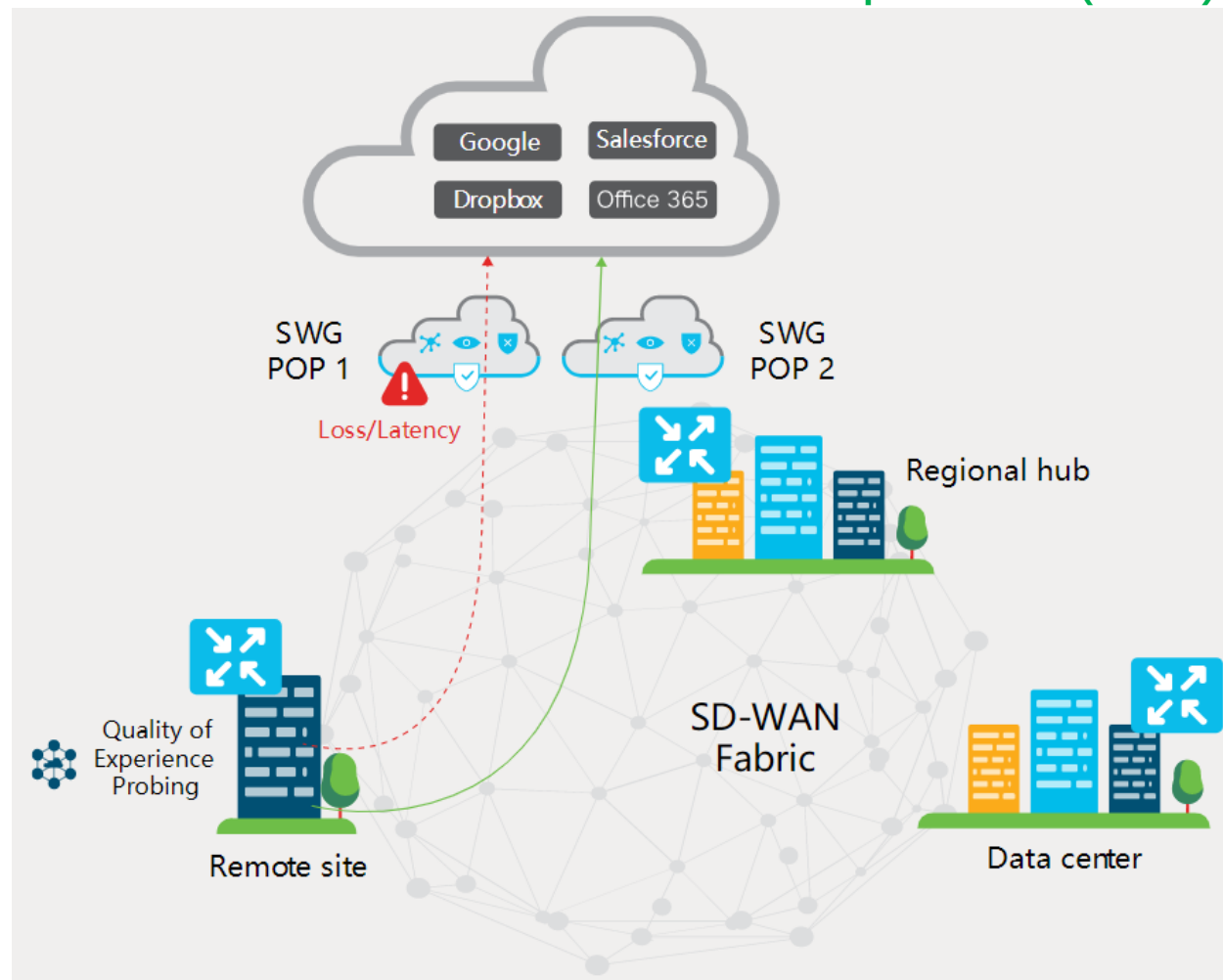


# 多云连接

## Cisco Cloud onRamp for IaaS







## Cisco Cloud onRamp for SaaS(SASE)

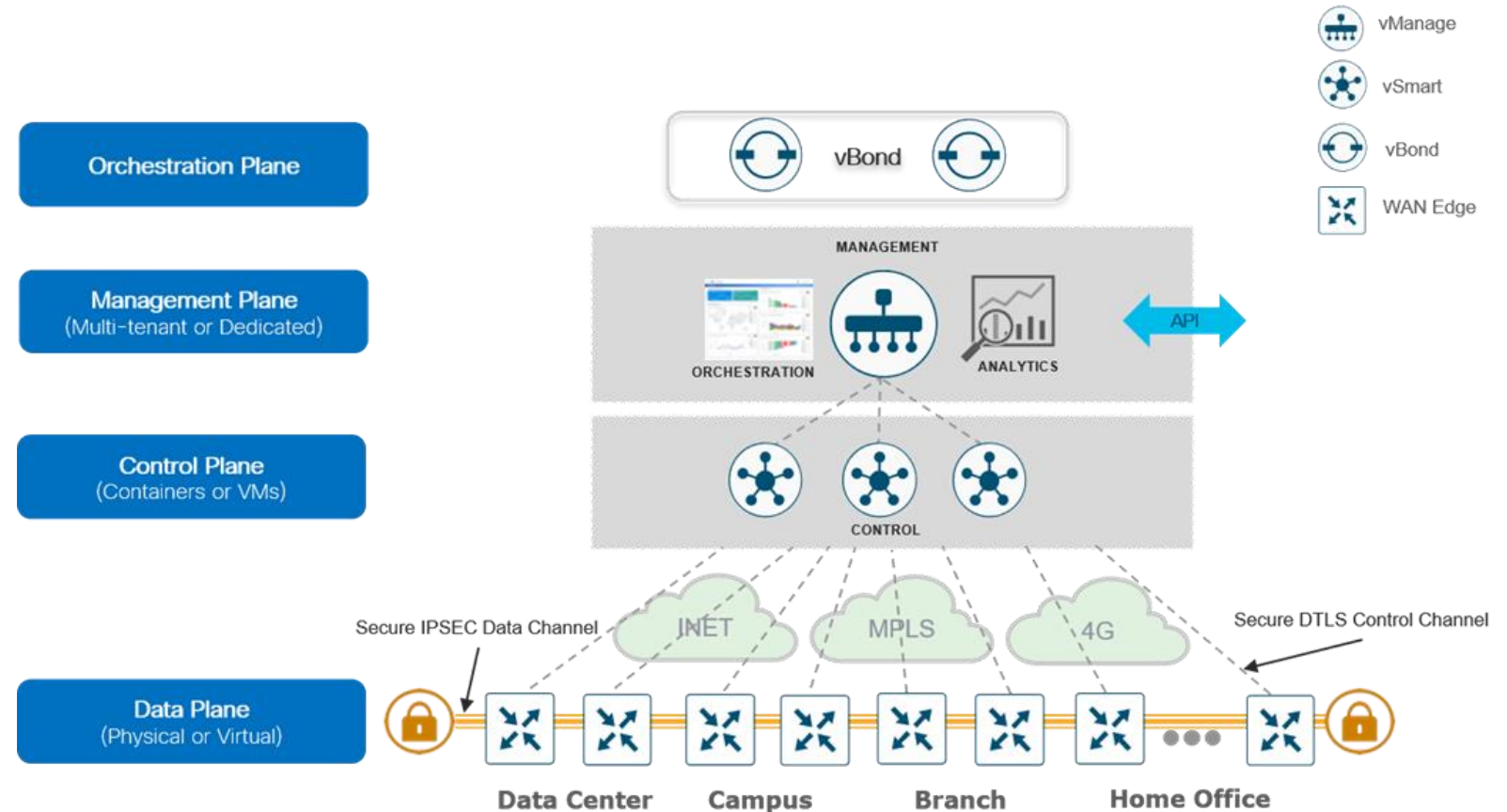




## 2 Cisco Viptela 架构与组件

# 架构与组件

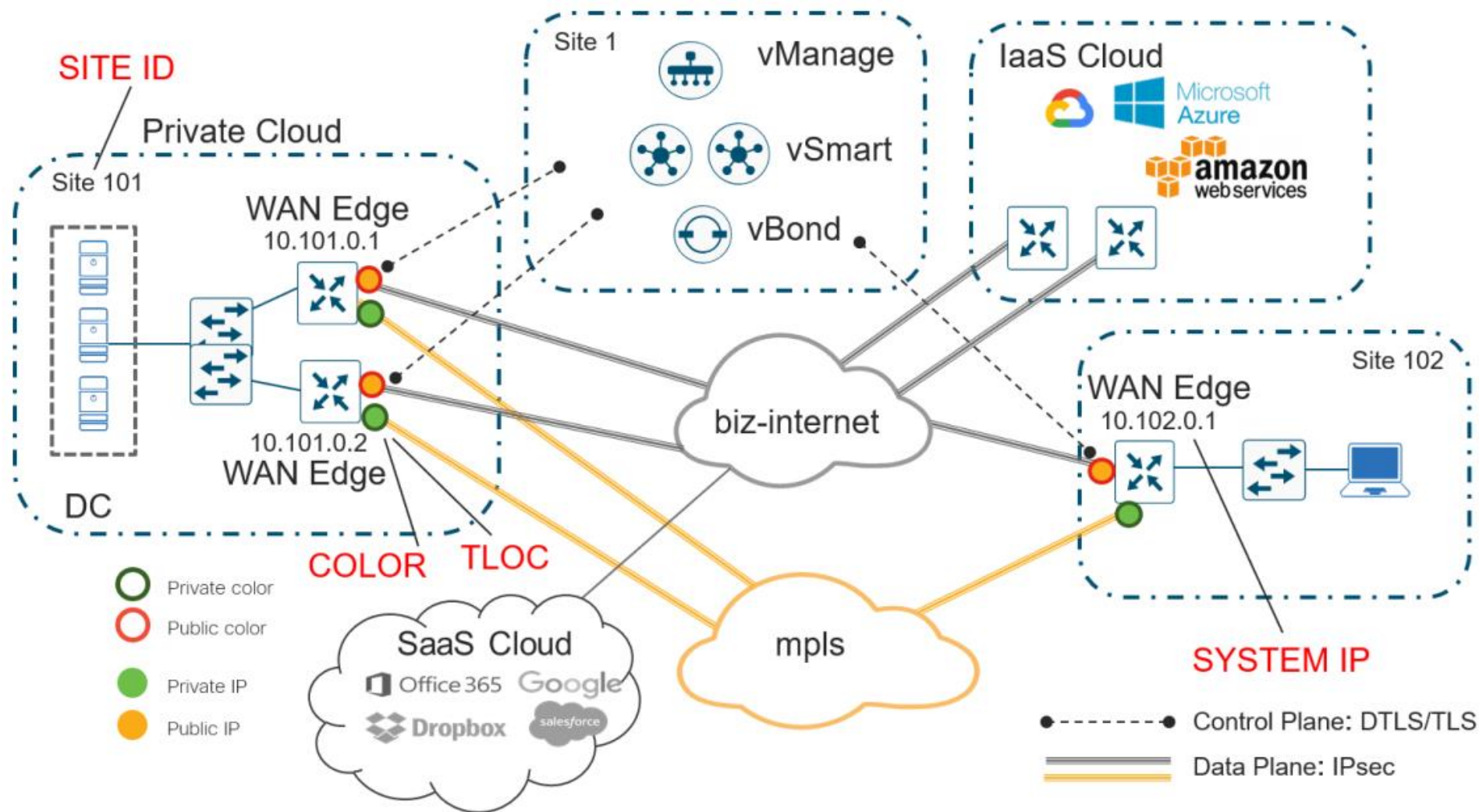
- 
**The orchestration plane** assists in the automatic onboarding of the SD-WAN routers into the SD-WAN overlay.
- 
**The management plane** is responsible for central configuration and monitoring.
- 
**The control plane** builds and maintains the network topology and makes decisions on where traffic flows.
- 
**The data plane** is responsible for forwarding packets based on decisions from the control plane.







# SDWAN拓扑





# 术语

## Site ID:

A site ID is a unique identifier of a site in the SD-WAN overlay network with a numeric value 1 through 4294967295 ( $2^{32}-1$ ) and it **identifies the source location of an advertised prefix**[标识路由的源位置]. This ID must be configured on every WAN Edge device, including the controllers, and must be the same for all WAN Edge devices that reside at the same site. A site could be a data center, a branch office, a campus, or something similar. By default, IPsec tunnels are not formed between WAN Edge routers within the same site which share the same site-id.

## System IP:

A System IP is a persistent, system-level IPv4 address that uniquely identifies the device independently of any interface addresses., **It acts much like a router ID**[类似于router ID] so it doesn't need to be advertised or known by the underlay. It is assigned to the system interface that resides in VPN 0 and is never advertised. A best practice, however, is to assign this system IP address to a loopback interface and advertise it in any service VPN. It can then be used as a source IP address for SNMP and logging, making it easier to correlate network events with vManage information.



# 术语

## Organization Name:

Organization Name is a name that is assigned to the SD-WAN overlay. It is case-sensitive and must match the organization name configured on all the SD-WAN devices in the overlay. **It is used to define the Organization Unit (OU) field to match in the Certificate Authentication process**[证书认证需要匹配OU] when an SD-WAN device is brought into the overlay network.

## TLOC:

A TLOC, or Transport Location, **is the attachment point where a WAN Edge router connects to the WAN transport network**[Edge路由器连接到广域网传输网络的接入点]. A TLOC is uniquely identified and represented by a three-tuple, consisting of system IP address, link color, and encapsulation (Generic Routing Encapsulation [GRE] or IPsec).

## Color:

The color attribute applies to WAN Edge routers or vManage and vSmart controllers and helps to **identify an individual TLOC**[用来标识一个TLOC]; different TLOCs are assigned different color labels. The example SD-WAN topology in figure 10 uses a public color called biz-internet for the Internet transport TLOC and a private color called mpls for the other transport TLOC. You cannot use the same color twice on a single WAN Edge router.



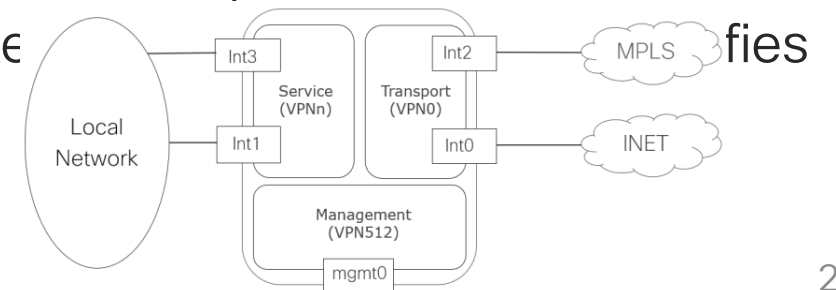
## 术语

### Overlay Management Protocol (OMP):

The OMP routing protocol, which has a structure **similar to BGP****[类似于BGP]**, manages the SD-WAN overlay network. The protocol runs **between vSmart controllers and between vSmart controllers and WAN Edge routers** where control plane information, such as route prefixes, next-hop routes, crypto keys, and policy information, **is exchanged over a secure DTLS or TLS connection**. The vSmart controller acts similar to a BGP route reflector; it receives routes from WAN Edge routers, processes and applies any policy to them, and then advertises the routes to other WAN Edge routers in the overlay network.

### Virtual private networks (VPNs):

In the SD-WAN overlay, virtual private networks (VPNs) provide segmentation, much **like Virtual Routing and Forwarding instances (VRFs)****[类似于VRF]** that many are already familiar with. Each VPN is isolated from one another and each have their own forwarding table. An interface or subinterface is explicitly configured under a single VPN and cannot be part of more than one VPN. Labels are used in OMP route attributes and in the packet to identify the VPN a packet belongs to.

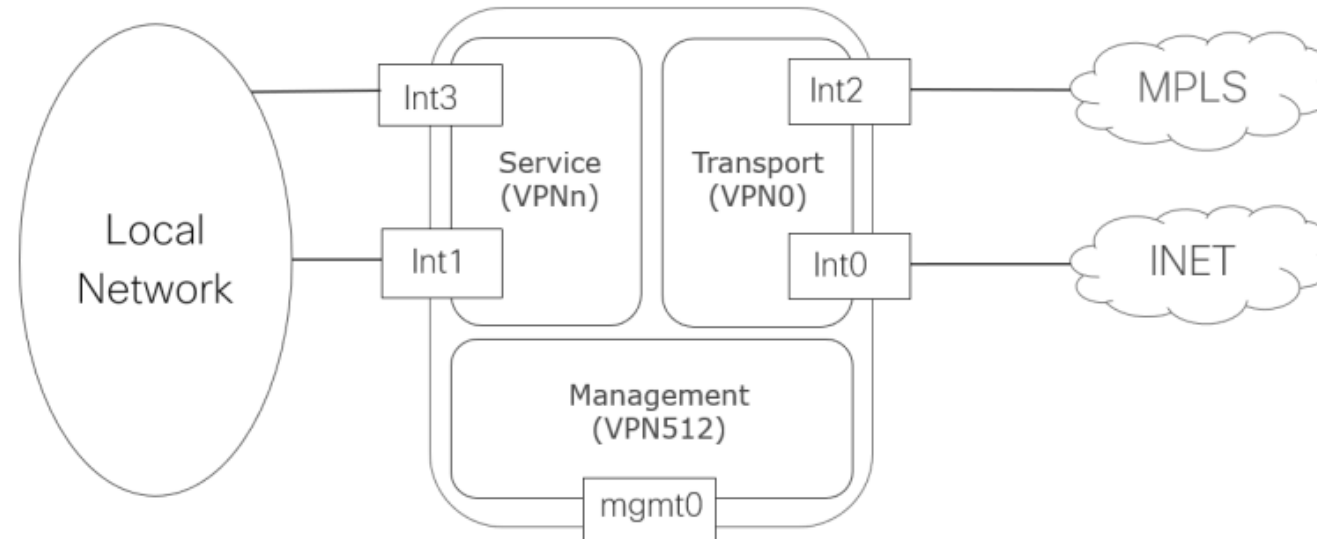


VPN 0 == 全局路由表

VPN 512 == 管理VRF



## 双向重分布



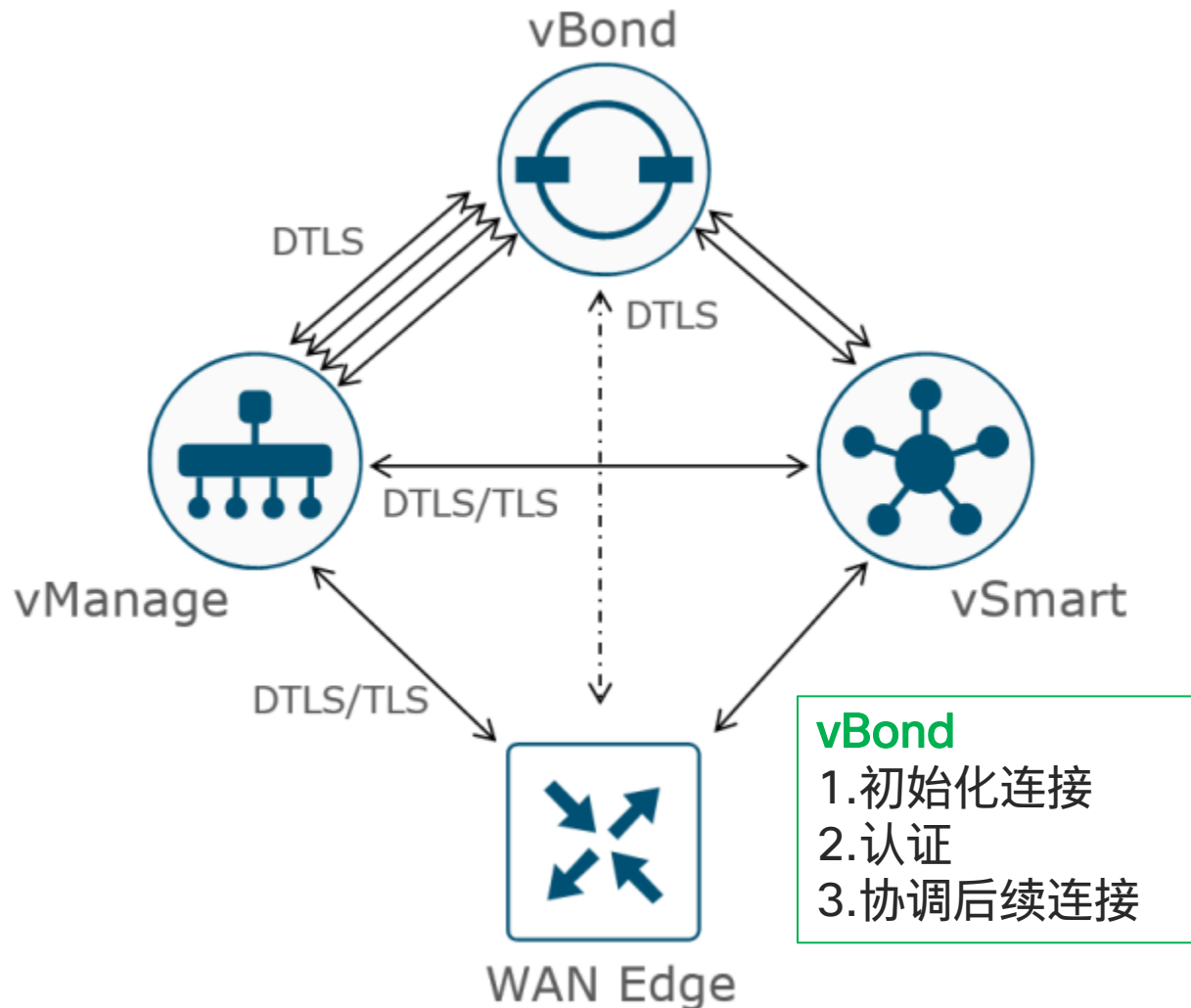
In addition to the default VPNs that are already defined, one or more service-side VPNs need to be created that contain interfaces that connect to the local-site network and carry user data traffic. **It is recommended to select service VPNs in the range of 1-511**, but higher values can be chosen as long as they do not overlap with default and reserved VPNs. **Service VPNs can be enabled for features such as OSPF or BGP, Virtual Router Redundancy Protocol (VRRP), QoS, traffic shaping, or policing**[Service VPN可以激活OSPF,BGP等等特性]. User traffic can be directed over the IPsec tunnels to other sites by redistributing OMP routes received from the vSmart controllers at the site into the service-side VPN routing protocol[OMP路由到Service VPN路由]. In turn, routes from the local site can be advertised to other sites by advertising the service VPN routes into the OMP routing protocol, which is sent to the vSmart controllers and redistributed to the other WAN Edge routers in the



# 3 Cisco Viptela 控制层面



## 控制层面连接

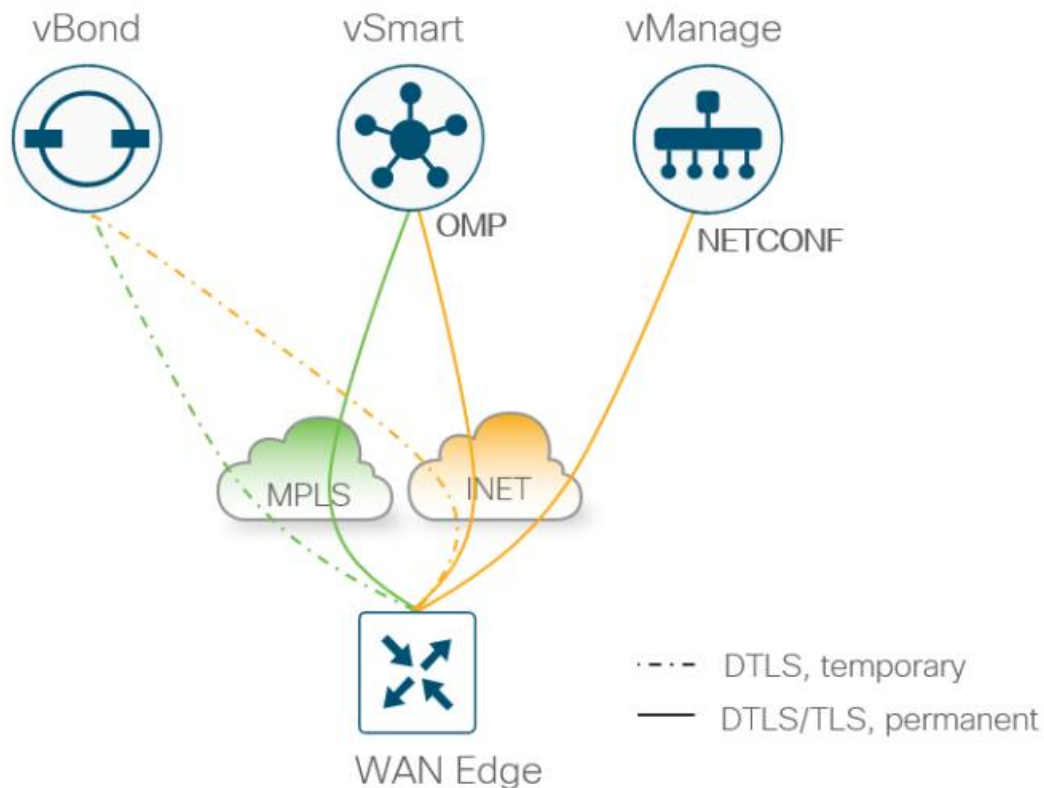


Cisco SD-WAN vManage and vSmart controllers initially contact and authenticate to the vBond controller, forming persistent DTLS connections, and then subsequently establish and maintain persistent DTLS/TLS connections with each other. WAN Edge devices onboard in a similar manner, but drop the transient vBond connection and maintain DTLS/TLS connections with the vManage and vSmart controllers

vManage与vSmart初始化联系vBond，然后形成持久DTLS连接，紧接着vManage和vSmart之间建立和维护DTLS/TLS连接。Edge也是先联系vBond，只是后续会丢掉与vBond的连接，并与vManage和vSmart建立和维护DTLS/TLS连接



## 控制层面连接摘要

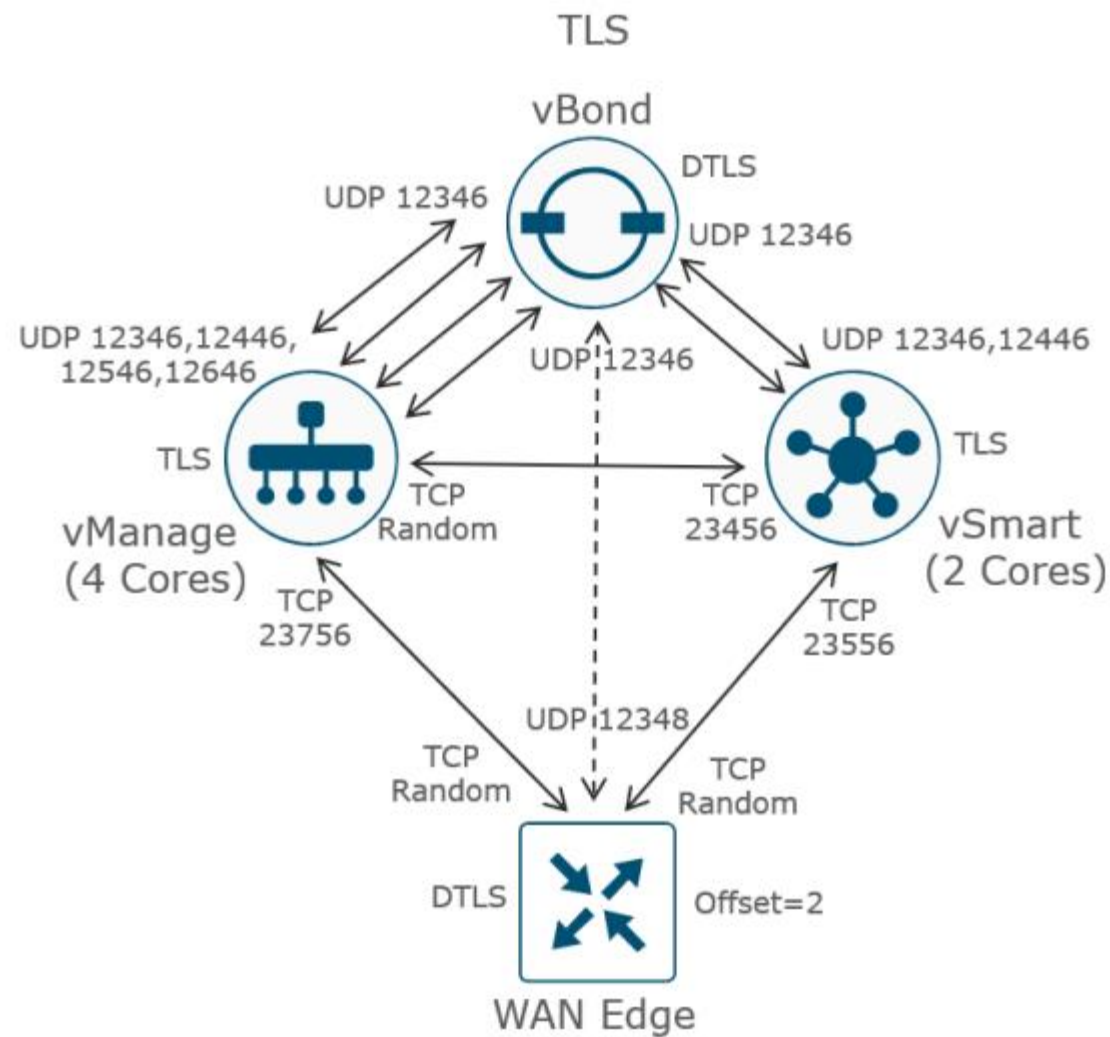
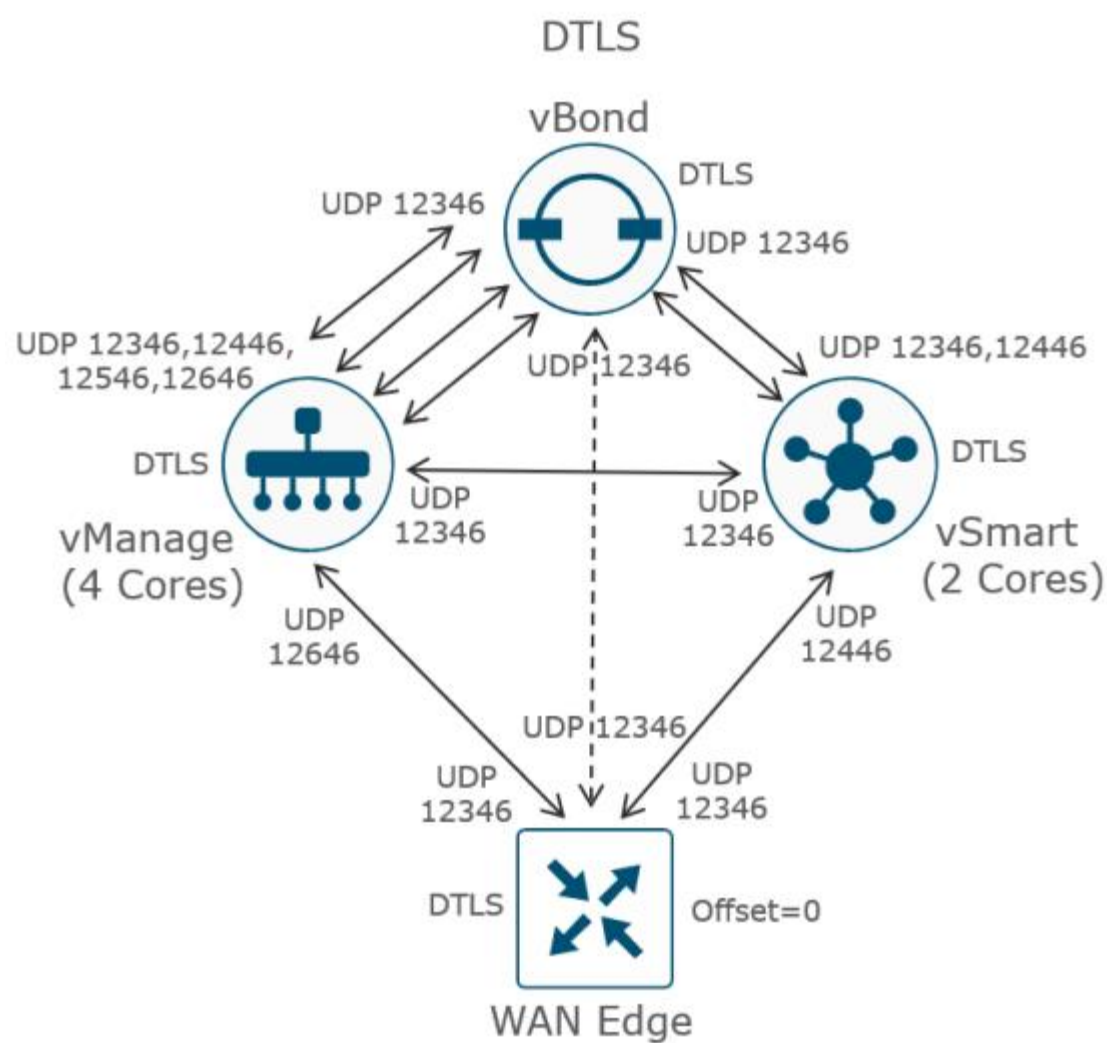


- Permanent DTLS connections between **each vSmart core** (up to 8) and each vBond orchestrator
- Permanent DTLS connections between **each vManage core** (up to 8) and each vBond orchestrator
- **A permanent TLS or DTLS connection** between each vManage and each vSmart controller
- **Full mesh of TLS or DTLS connections** between vSmart controllers (1 connection between each pair)
- **Full mesh of TLS or DTLS connections** between **vManage cluster** instances (1 connection between each pair)\*
- **Temporary DTLS connection** between each WAN Edge and one vBond – one connection on each transport
- Permanent TLS or DTLS connection between each WAN Edge and one vManage instance – **only one connection over one transport is chosen**
- Permanent TLS or DTLS connections between each WAN Edge and two vSmart controllers by default – **connections to each over each transport**[**每一个介质, 每一个vSmart一个连接**]\*\*



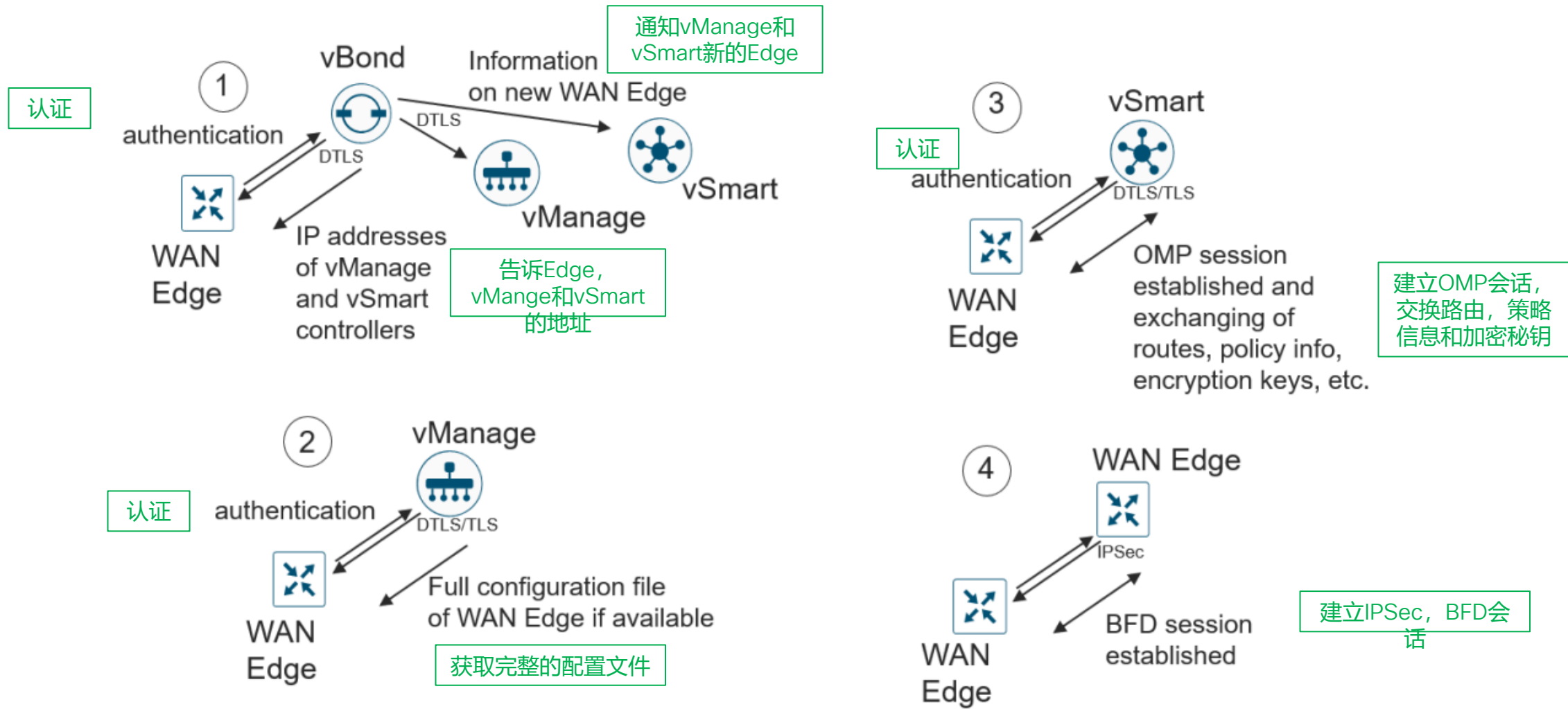


# 控制层面端口号详情



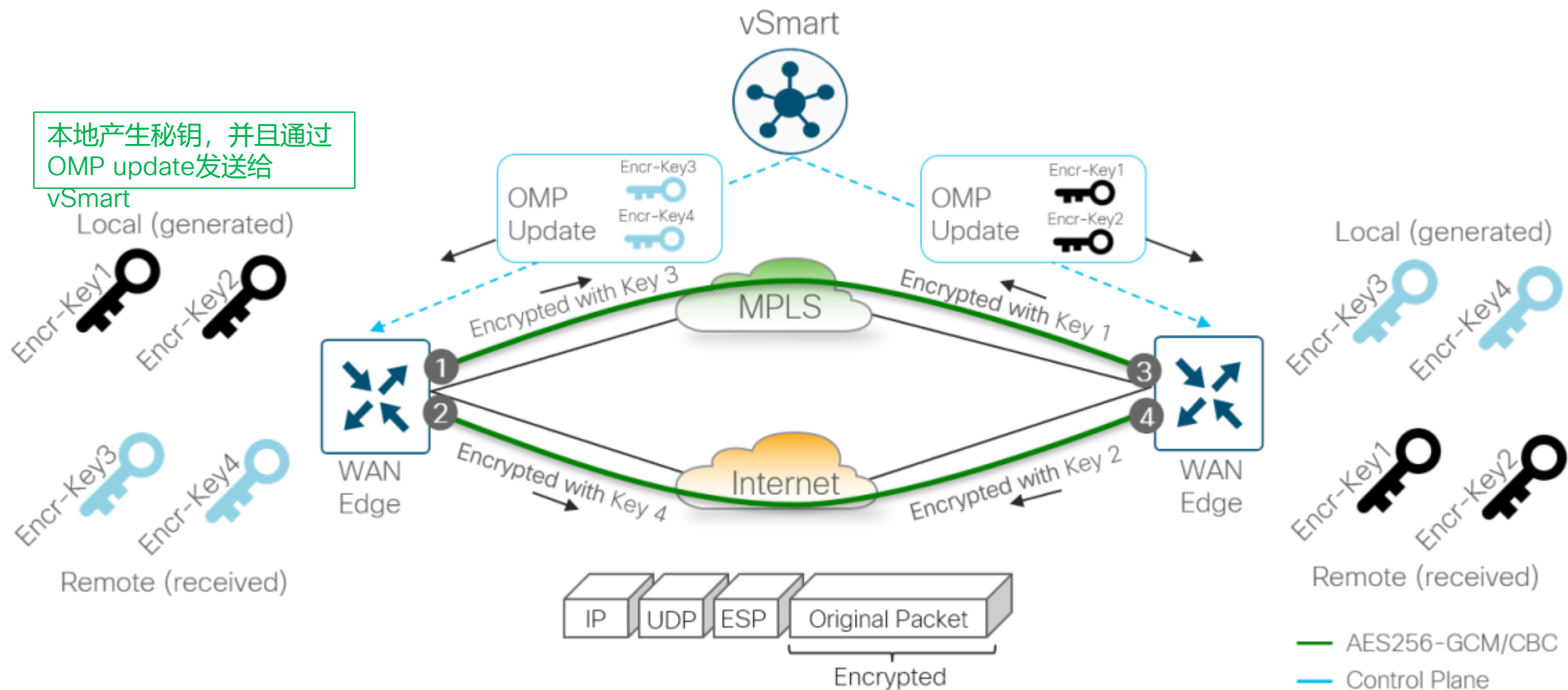


# WAN Edge上线



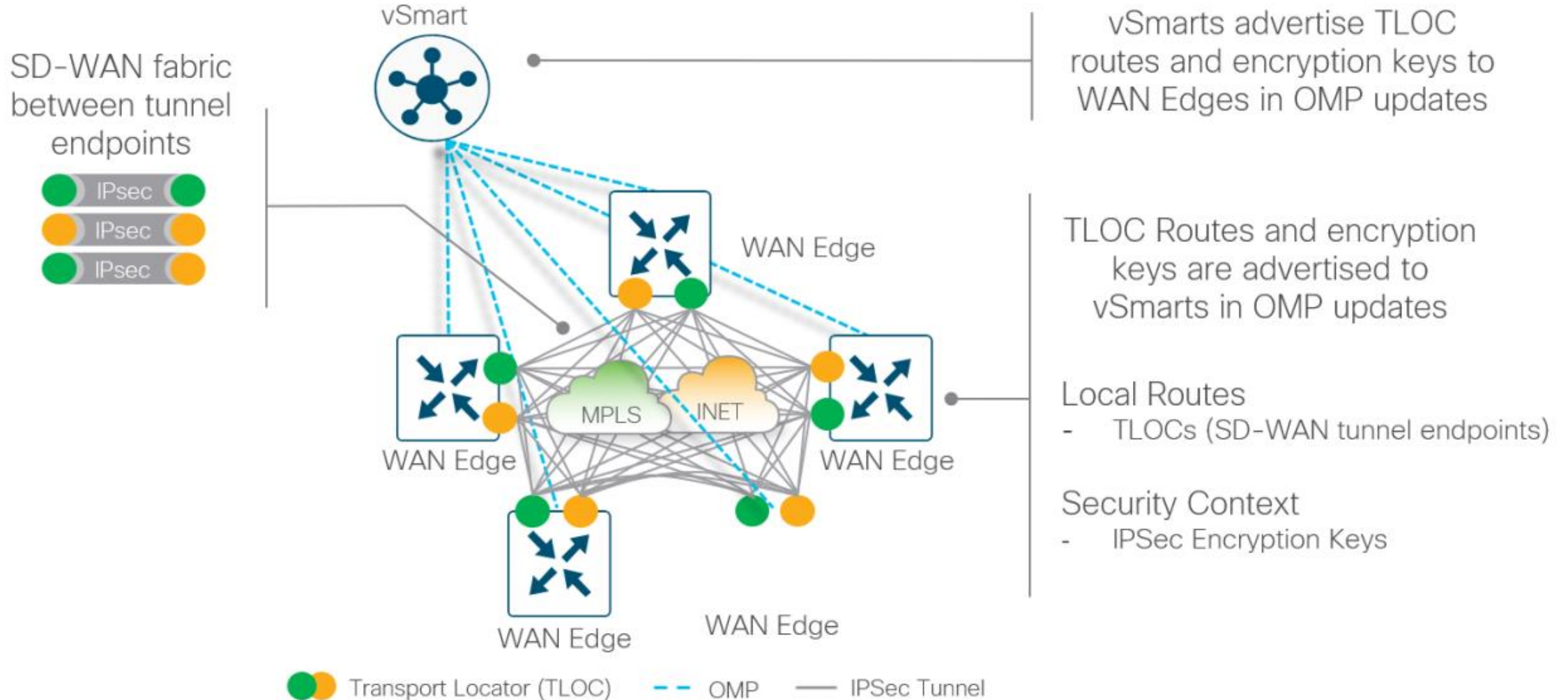


# 数据层面加密密钥



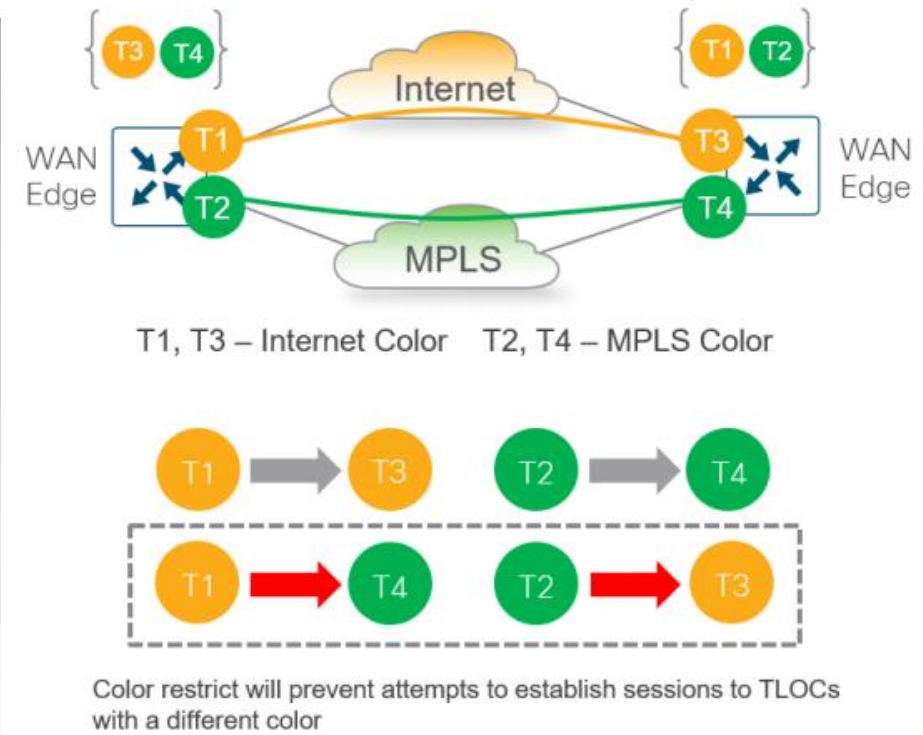
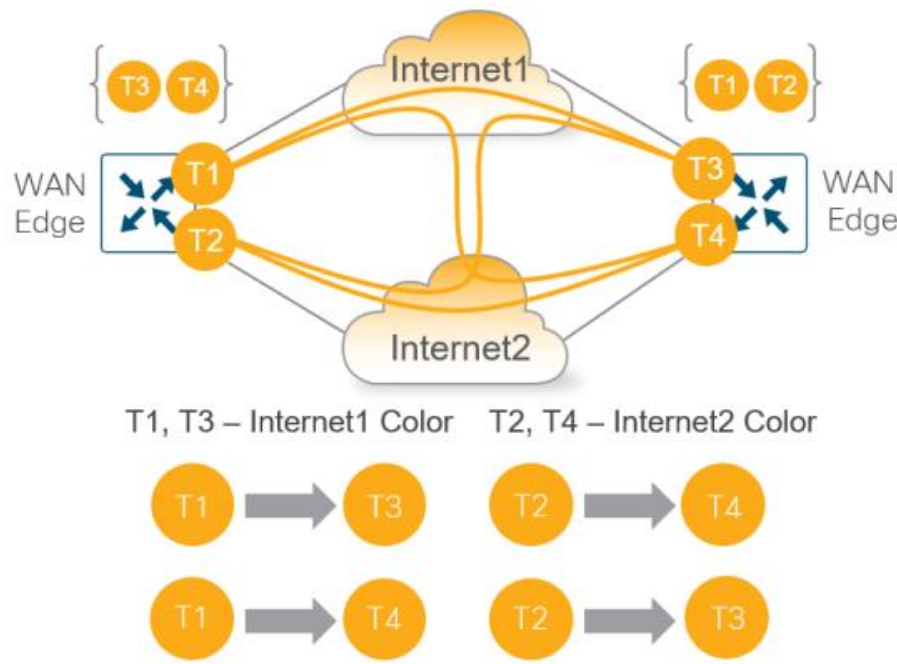


# vSmart与Edge通告的内容





# vSmart与Edge通告的内容

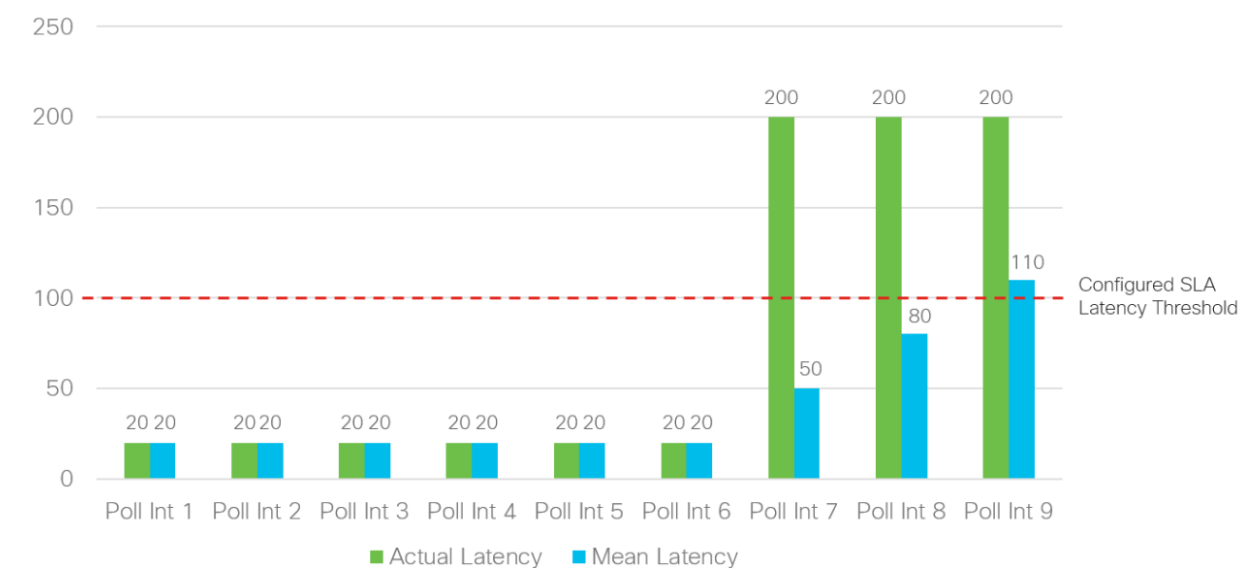
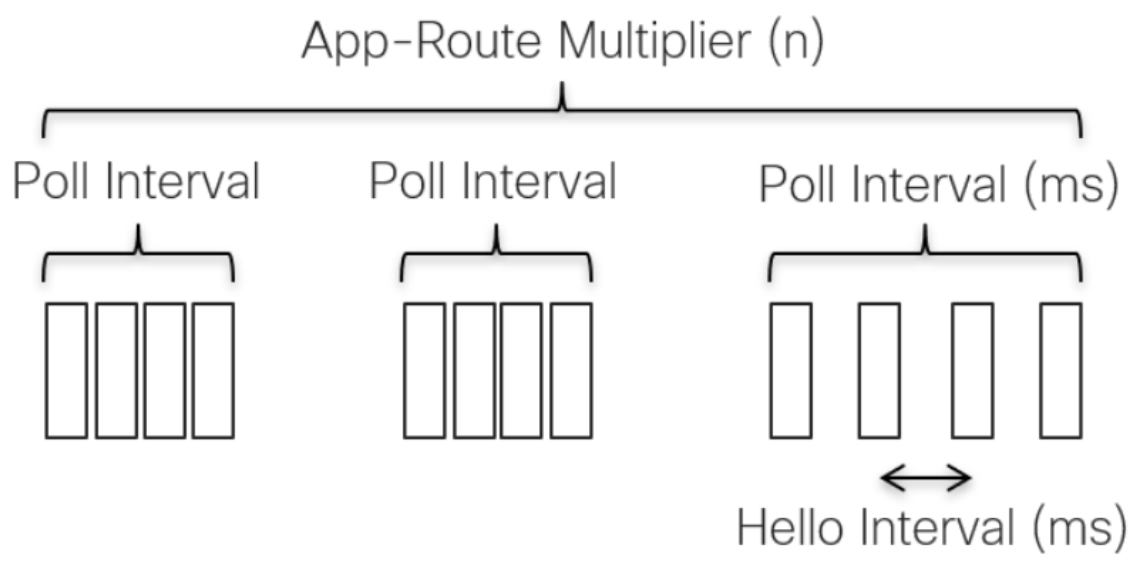


By default, WAN Edge routers **attempt to connect to every TLOC over each WAN transport**, including TLOCs that belong to other transports marked with different colors. This is helpful when you have different Internet transports at different locations, for example, that should communicate directly with each other. To prevent this behavior, there is a **restrict keyword** that can be specified along with the color of the tunnel. **This prevents attempts to establish BFD sessions to TLOCs with different color**. This is commonly used on private transports to prevent forming sessions with public transports



# 路径质量

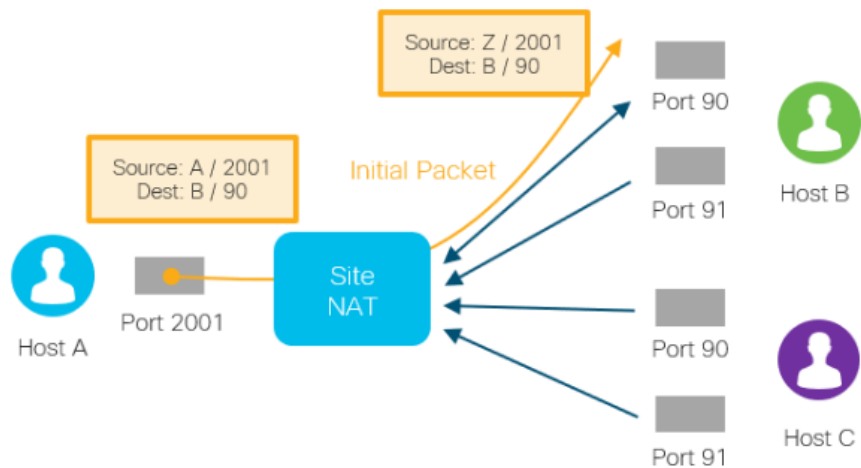
For measurements, the WAN Edge router collects packet loss, latency, and jitter information for every BFD hello packet. This information is collected over the **poll-interval period, which is 10 minutes by default**, and then the average of each statistic is calculated over this poll-interval time. A multiplier is then used to specify how many poll-interval averages should be reviewed against the SLA criteria. **By default, the multiplier is 6, so 6 x 10-minute poll-interval averages for loss, latency, and jitter are reviewed and compared against the SLA thresholds before an out-of-threshold decision is made.**



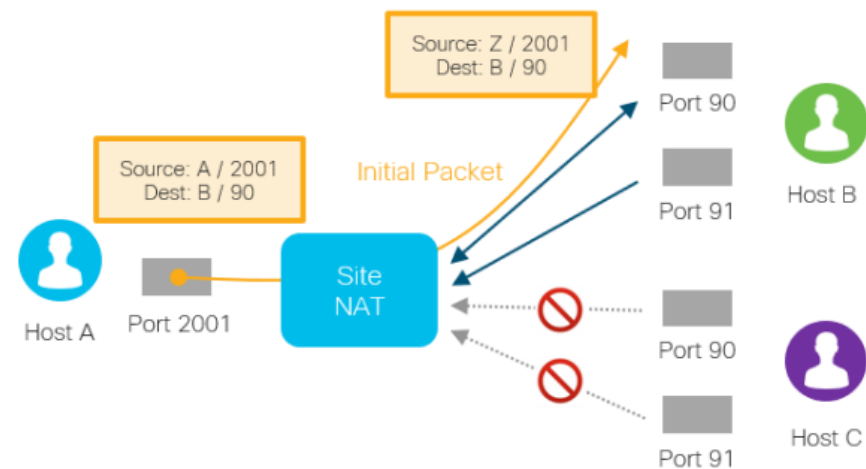


# NAT类型

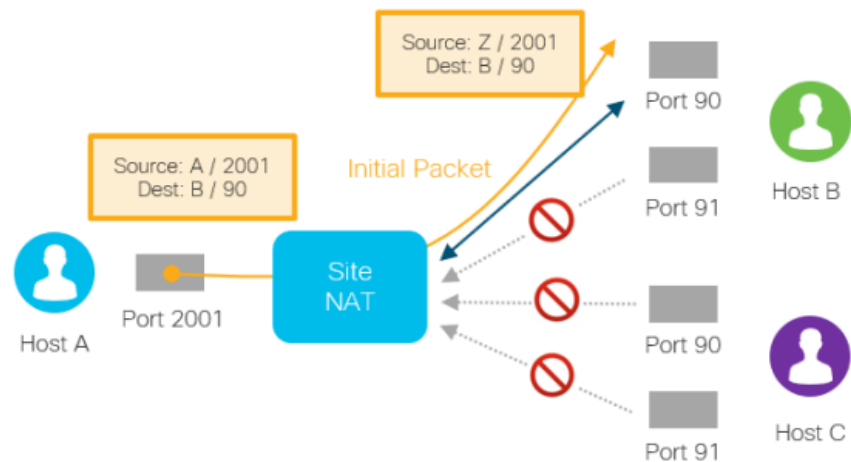
### Full-Cone



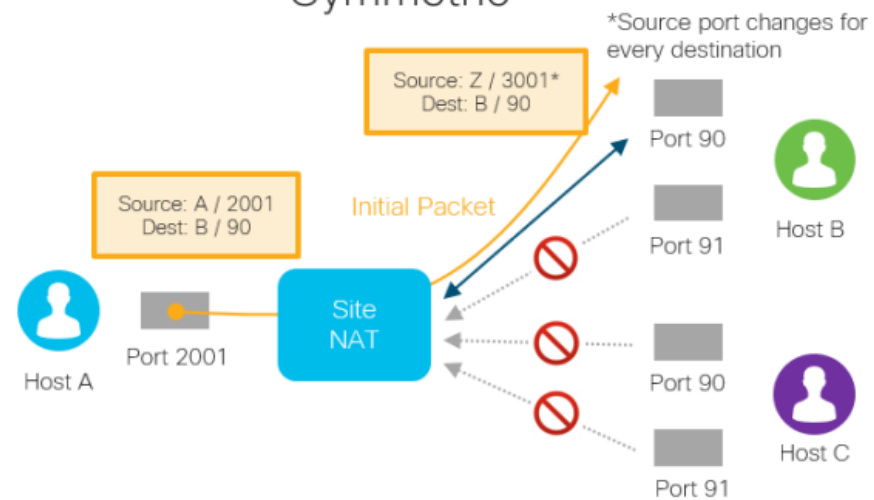
### Restricted-Cone NAT



### Port-Restricted-Cone NAT



### Symmetric





## 两个Edge之间的NAT类型

WAN Edge A	WAN Edge B	IPSec Tunnel Status	
Public IP (No NAT)	Public IP (No NAT)		
Full Cone	Full Cone		
Full Cone	Port/Address Restricted		
Port/Address Restricted	Port/Address Restricted		
Public	Symmetric		
Full Cone	Symmetric		
Symmetric	Port/Address Restricted		
Symmetric	Symmetric		

Direct IPSec Tunnel

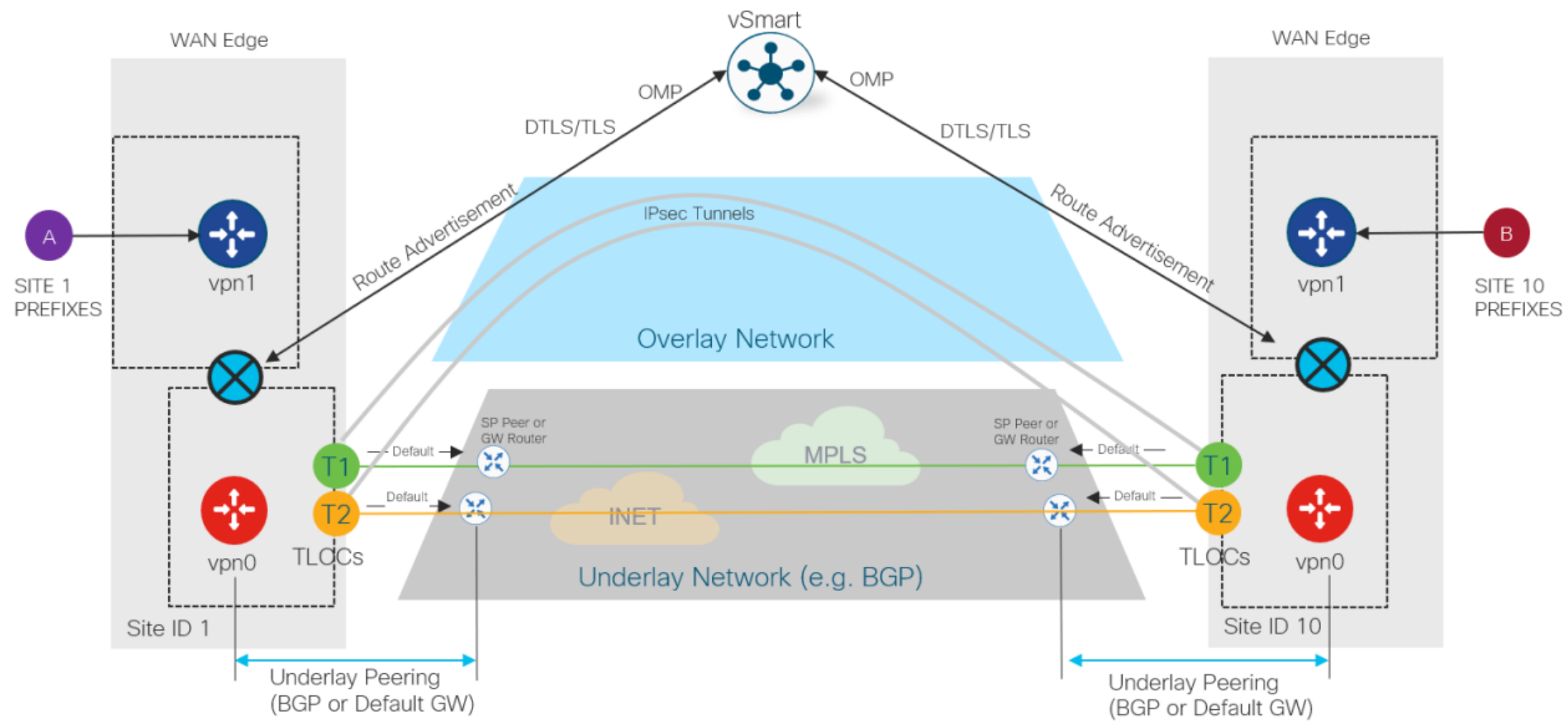
No Direct IPSec Tunnel (traffic traverses hub)

Mostly Encountered



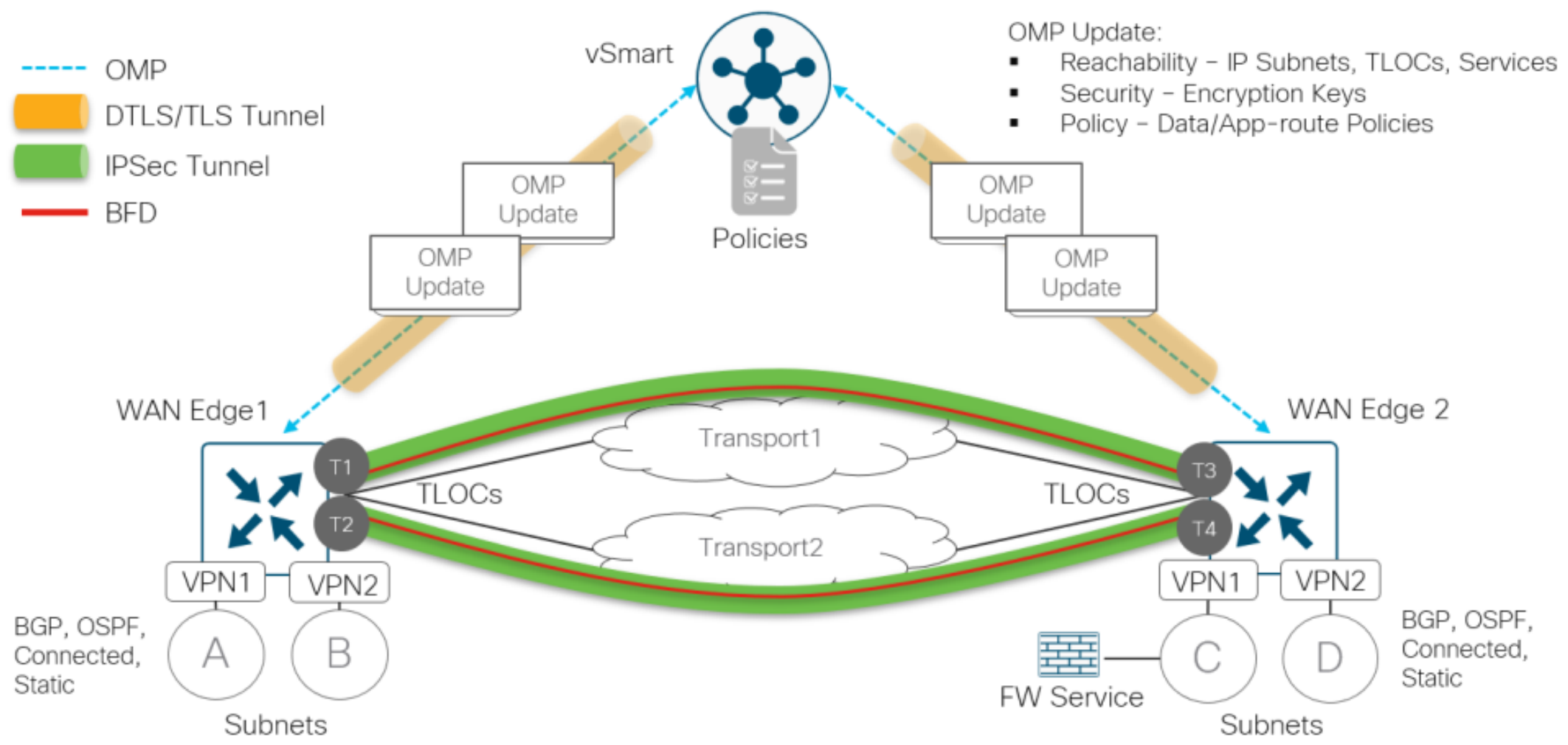


# Underlay vs overlay routing



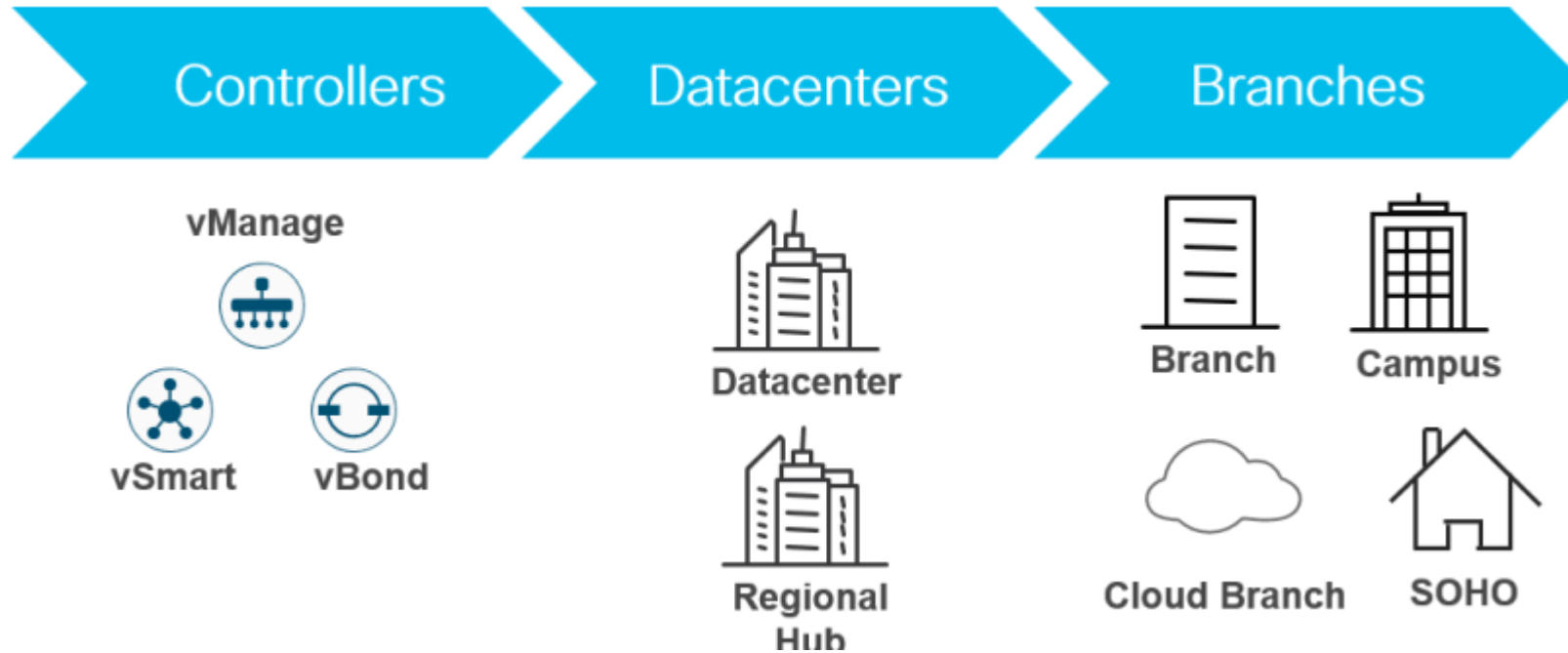


# OMP操作





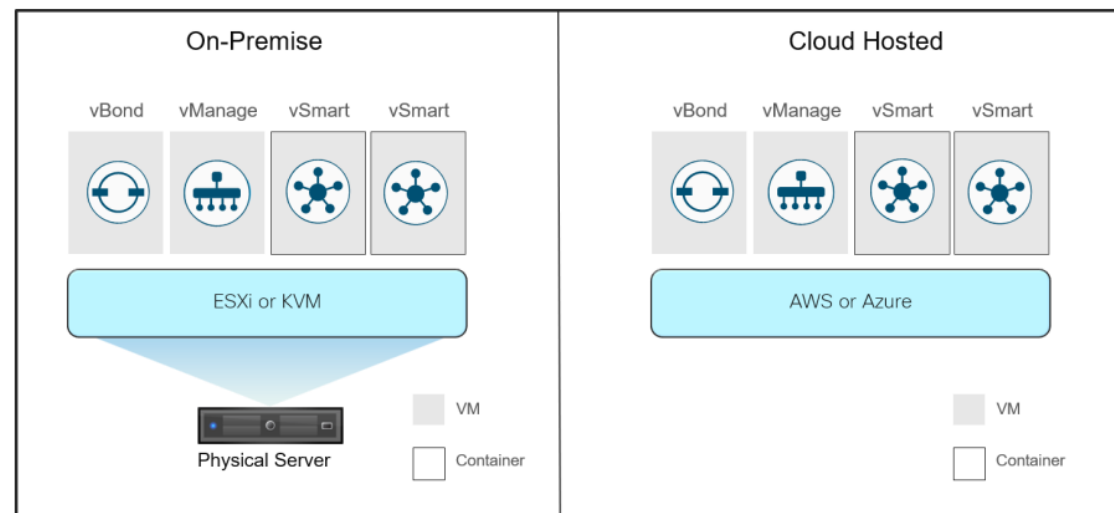
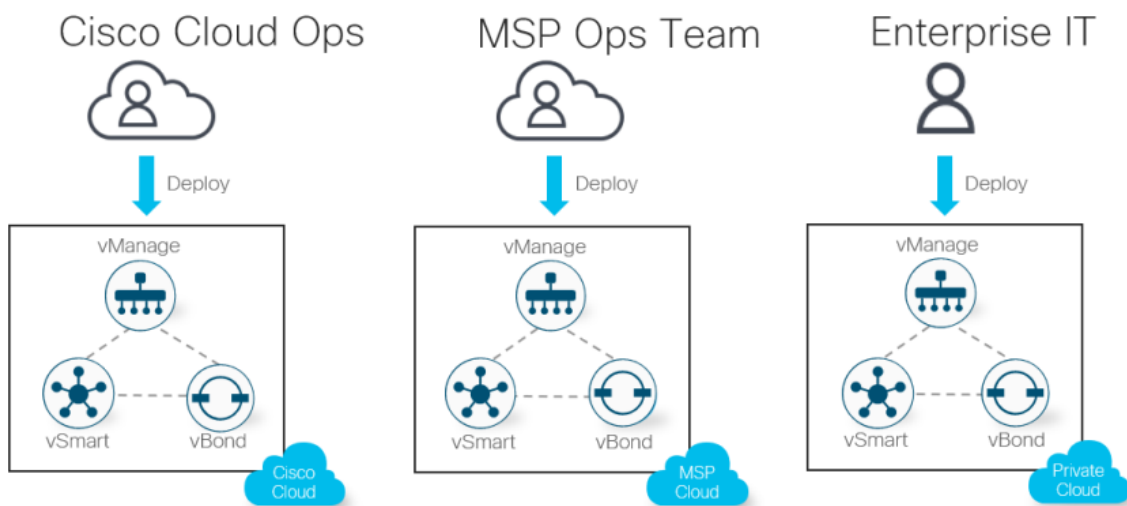
# 控制器部署顺序



In any SD-WAN deployment, the controllers are deployed and configured first[先控制器], followed by the main hub or data center sites[再Hub和DC], and lastly, the remote sites[最后Edge]. As each site is deployed, the control plane is established first, automatically followed by the data plane. It is recommended that hub sites are used to route between SD-WAN and non-SD-WAN sites[hub站点用来在SDWAN与非SDWAN之间进行路由] as the sites are being migrated to SD-WAN

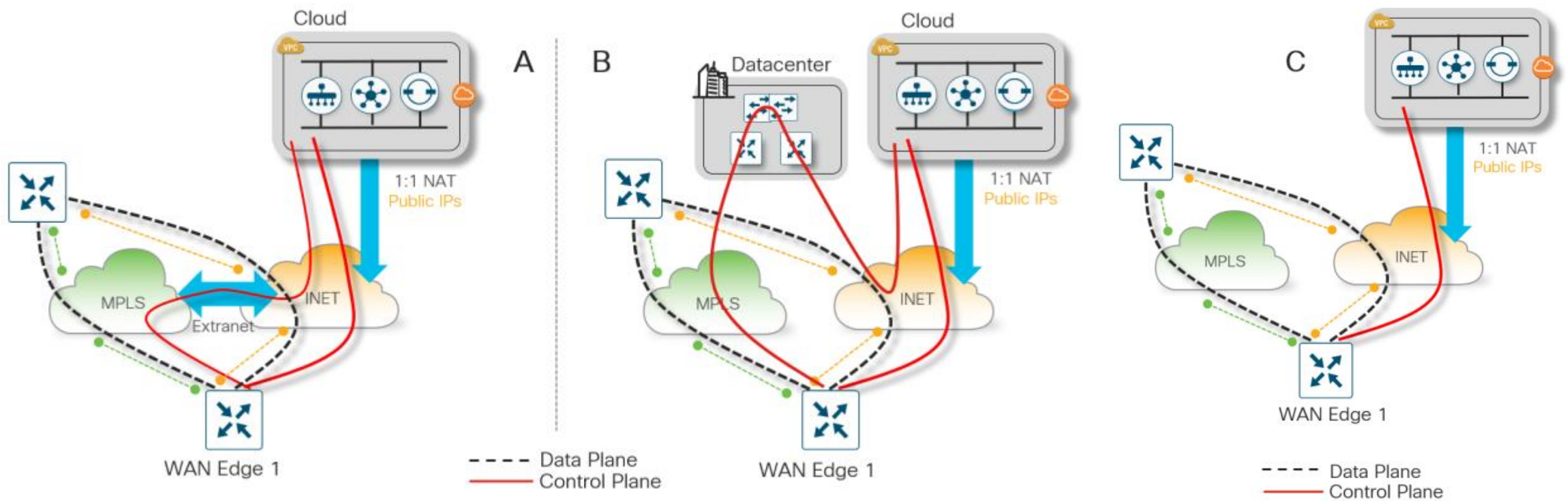


# 灵活的控制面部署选项



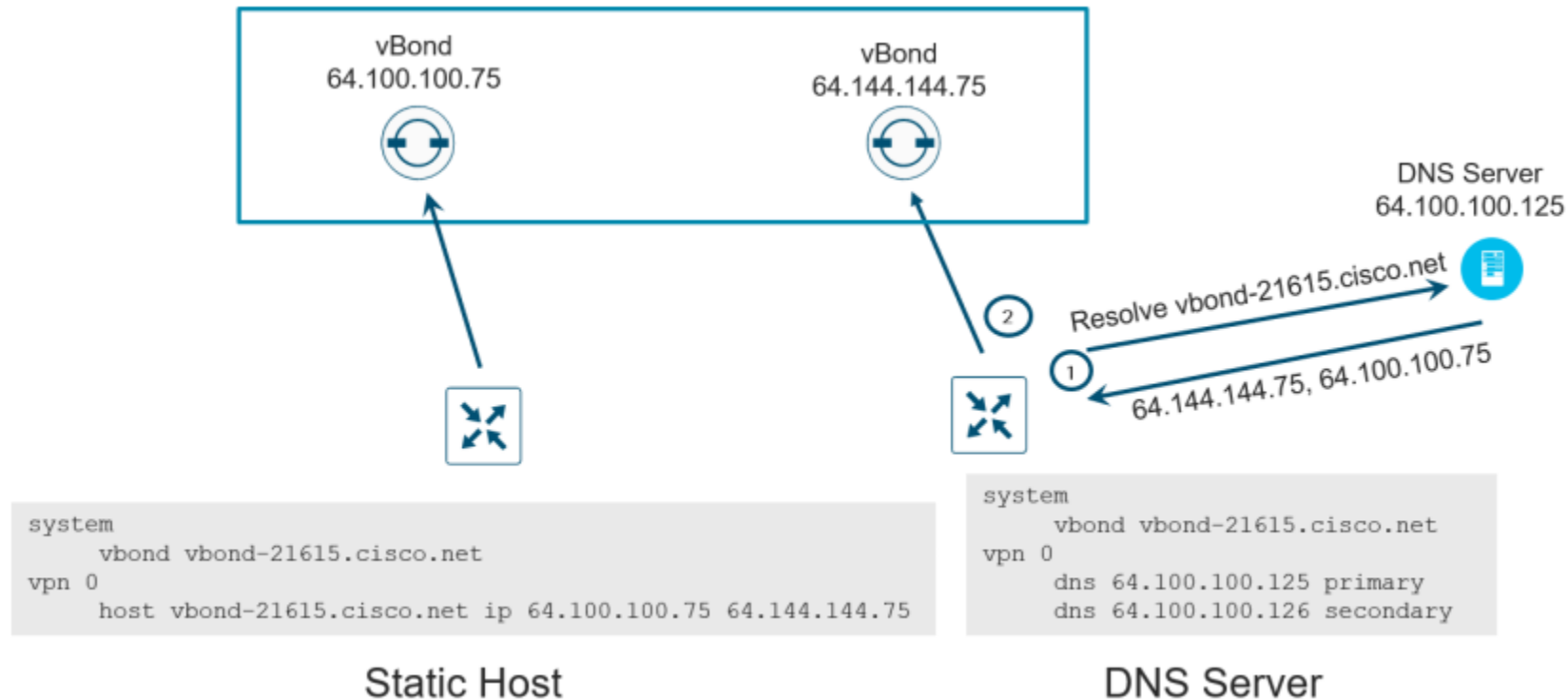


# 控制与数据层面连接选项





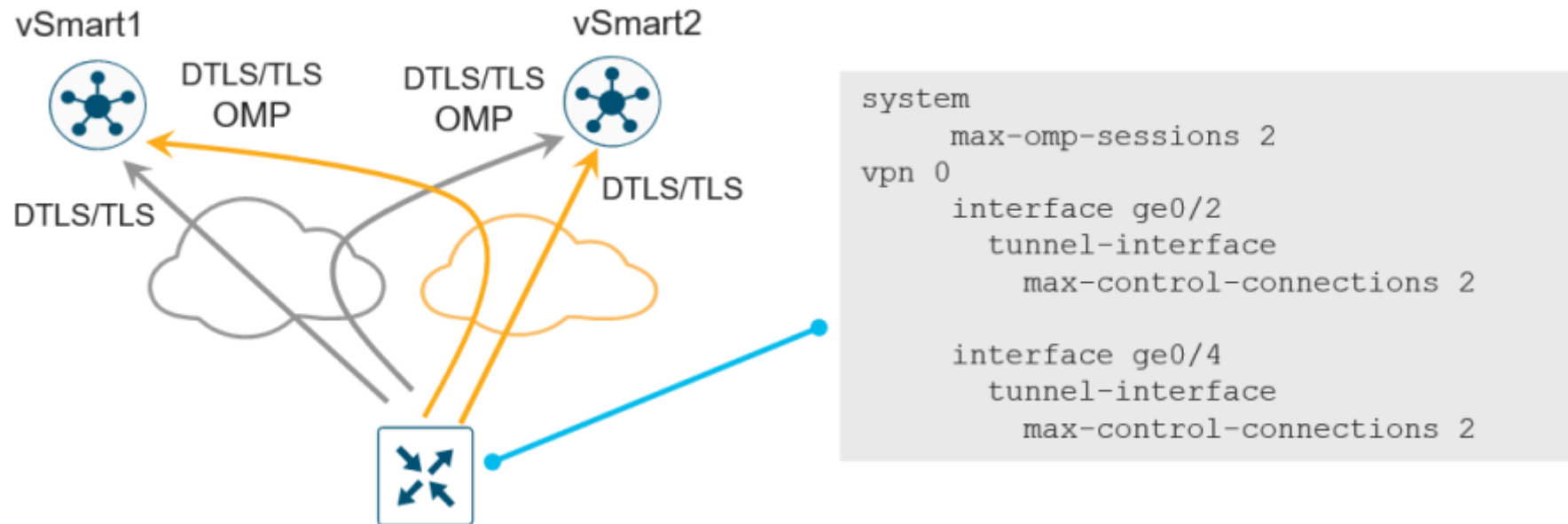
## vBond冗余



In the Domain Name Server (DNS), **multiple IP addresses are associated with the FQDN of the vBond**[vBound域名关联多个IP]. Typically, all vBond IP addresses are passed back to the DNS querier, and each IP address is tried in succession until a successful connection is formed. The **starting point index into the DNS list is determined by a hash function**[使用Hush计算开始点]. If a DNS server is unavailable, static host statements can be configured on the WAN Edge as an alternative.[DNS不可用, 才使用静态配置]



## vSmart冗余

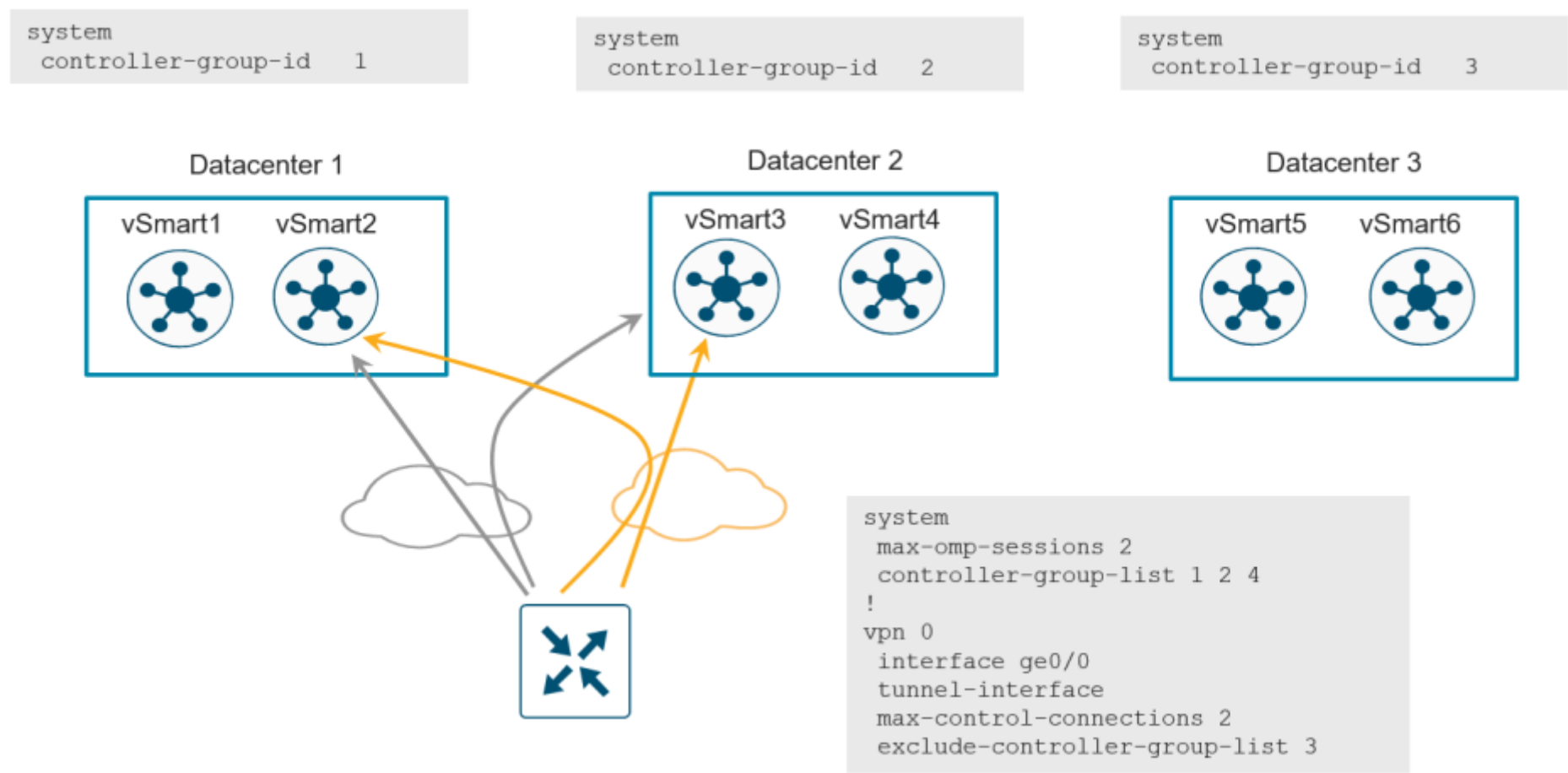


By default, a WAN Edge router will connect **to two vSmart controllers over each transport**. If one of the vSmart controllers fails, the other vSmart controller seamlessly takes over handling the control plane of the network

You can control the number of vSmart connections a WAN router makes with vSmart controllers over each TLOC with the **max-control-connections** command under each interface tunnel in VPN 0. **The default setting is two**. In addition, there is a **max-omp-sessions** command under the system configuration that can also be adjusted. **Its default configuration is also two**. Note that **any number of connections made to the same vSmart controller is considered part of the same OMP session**[**去往一个vSmart的多个conn只算一个session**]. When there are more vSmart controllers in the network than the WAN Edge max-control-connections allow, the WAN Edge router<sup>39</sup>



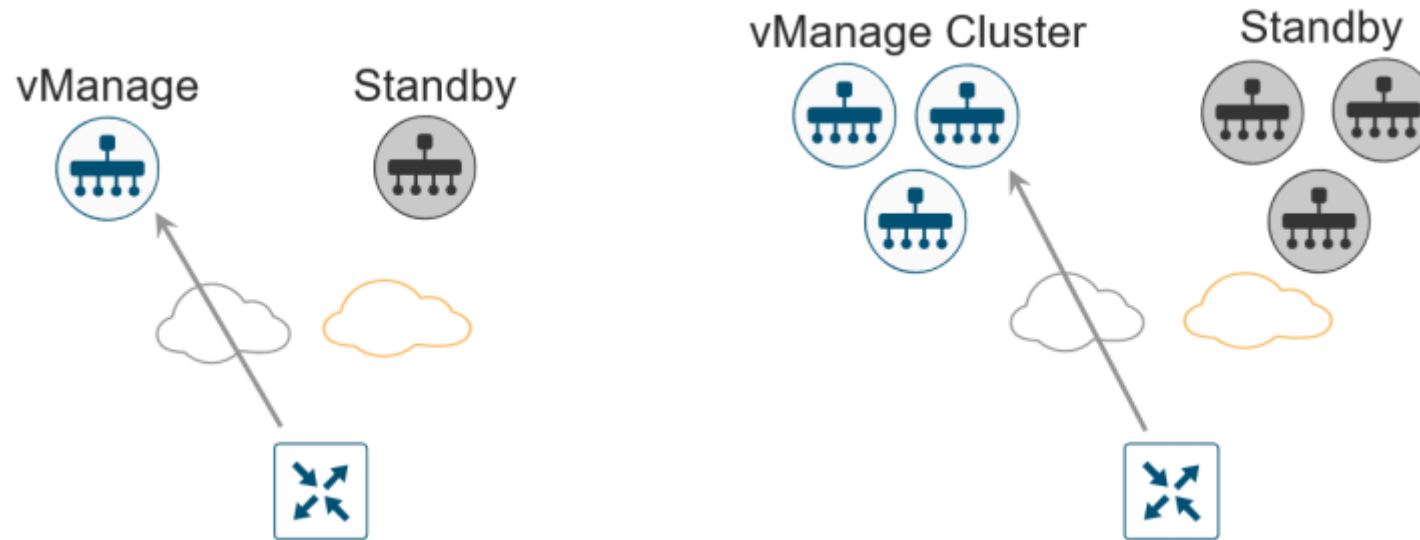
# vSmart亲和







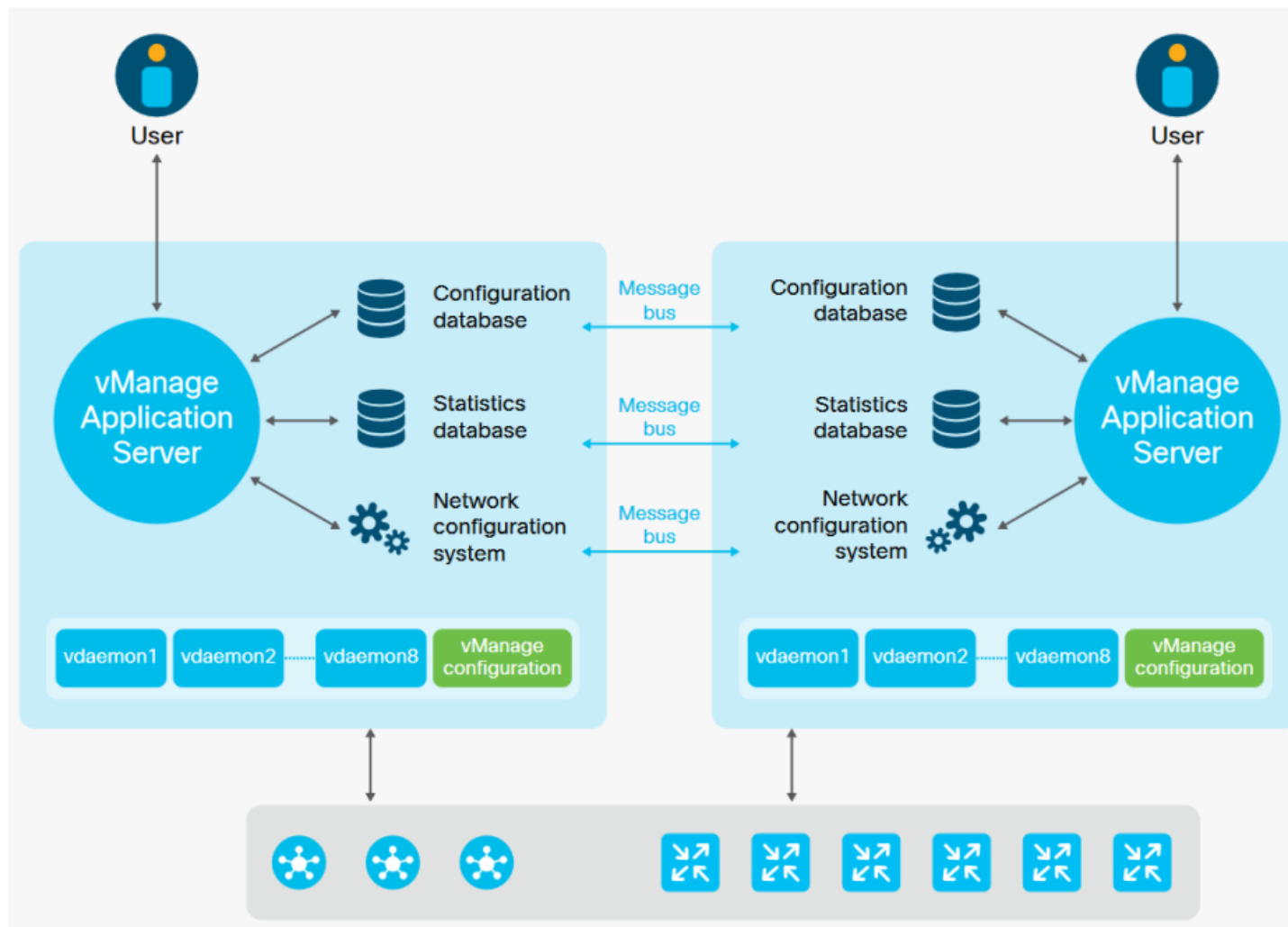
## vManage冗余



WAN Edge routers **connect to vManage over one of the transports**. You can control which transport is used with the `vmanage-connection-preference <number>` command under the tunnel interface on a WAN Edge. To prefer a specific tunnel interface to use to connect to vManage, **use a higher preference value**. Try to use the highest bandwidth link for the vManage connection and avoid cellular interfaces if possible. A zero value indicates that tunnel interface should never connect to vManage. At least one tunnel interface must have a nonzero value.

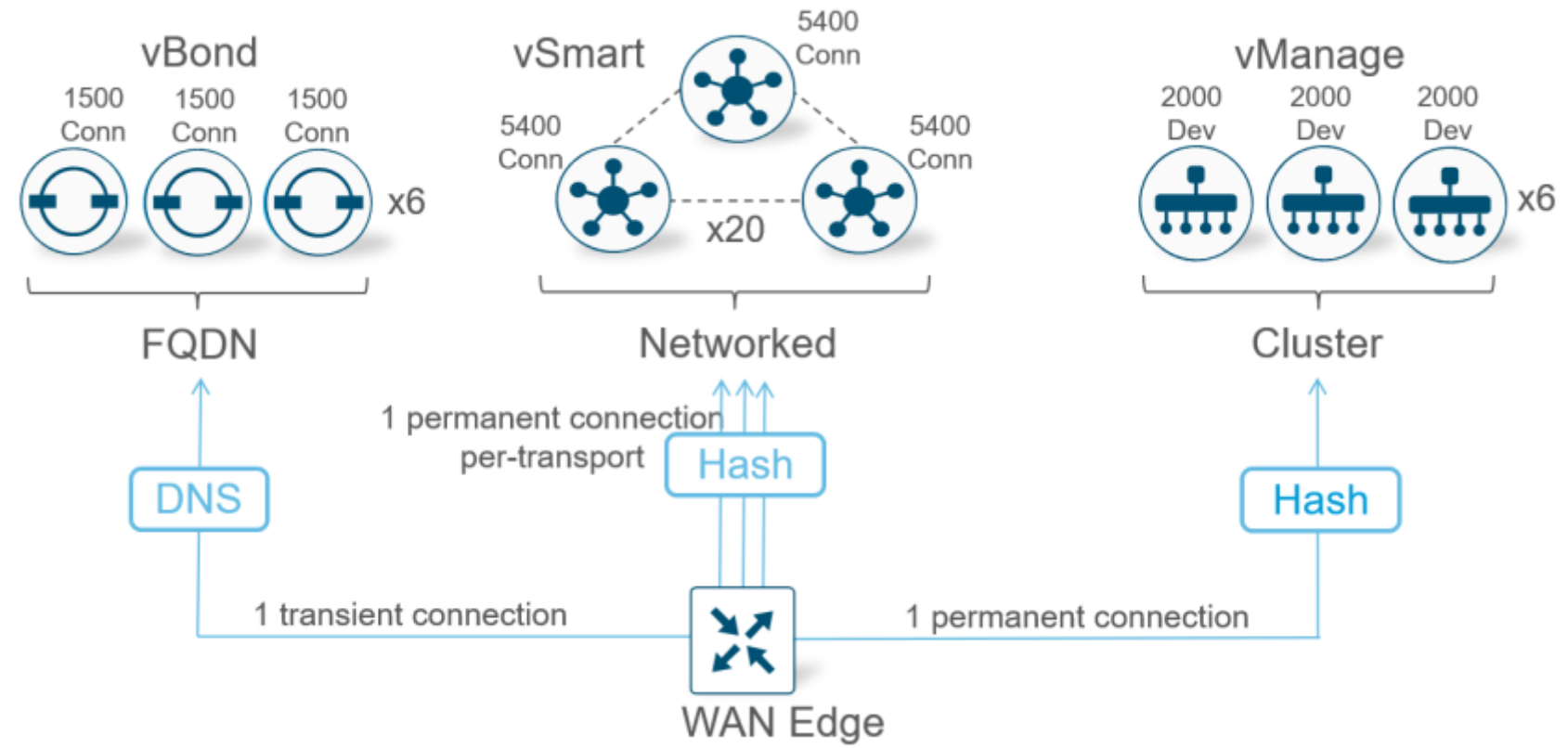


# vManage集群组件





# 控制器高可用性与扩展性



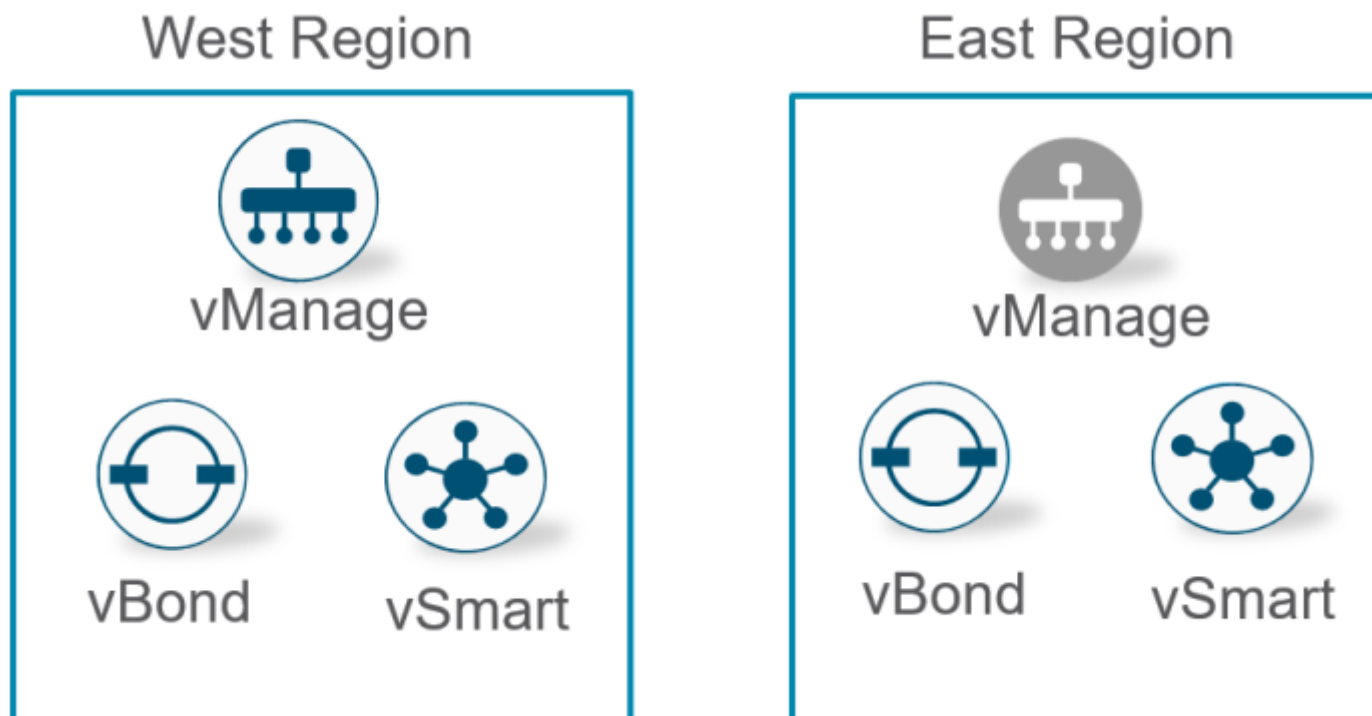


# Number of controllers needed to support WAN Edge devices

Number of WAN Edges	Number of vBonds	Number of vSmarts	Number of vManages (Active)
<=2000	1	1	1
<=4000	2	2	3
<=6000	3	3	4*
<=8000	4	4	5
<=10000	5	5	6

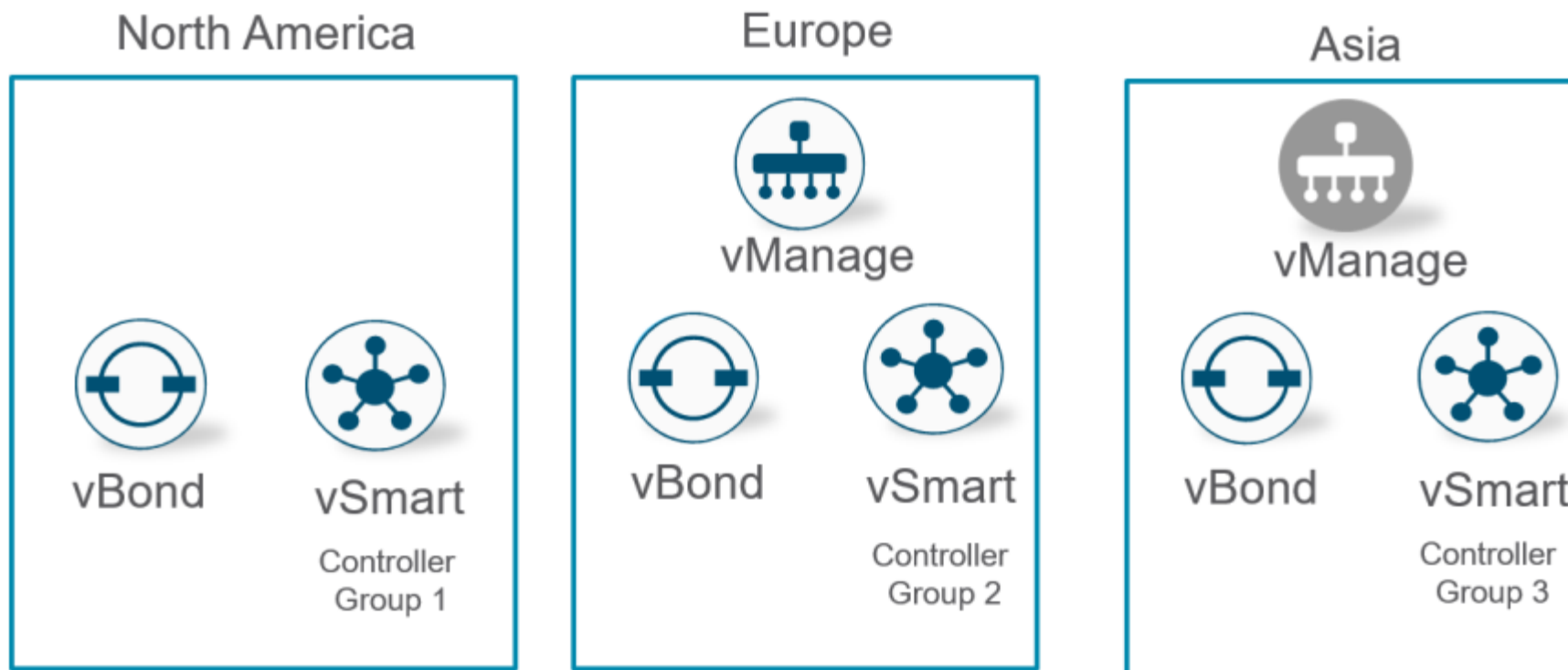


# 控制器部署案例一



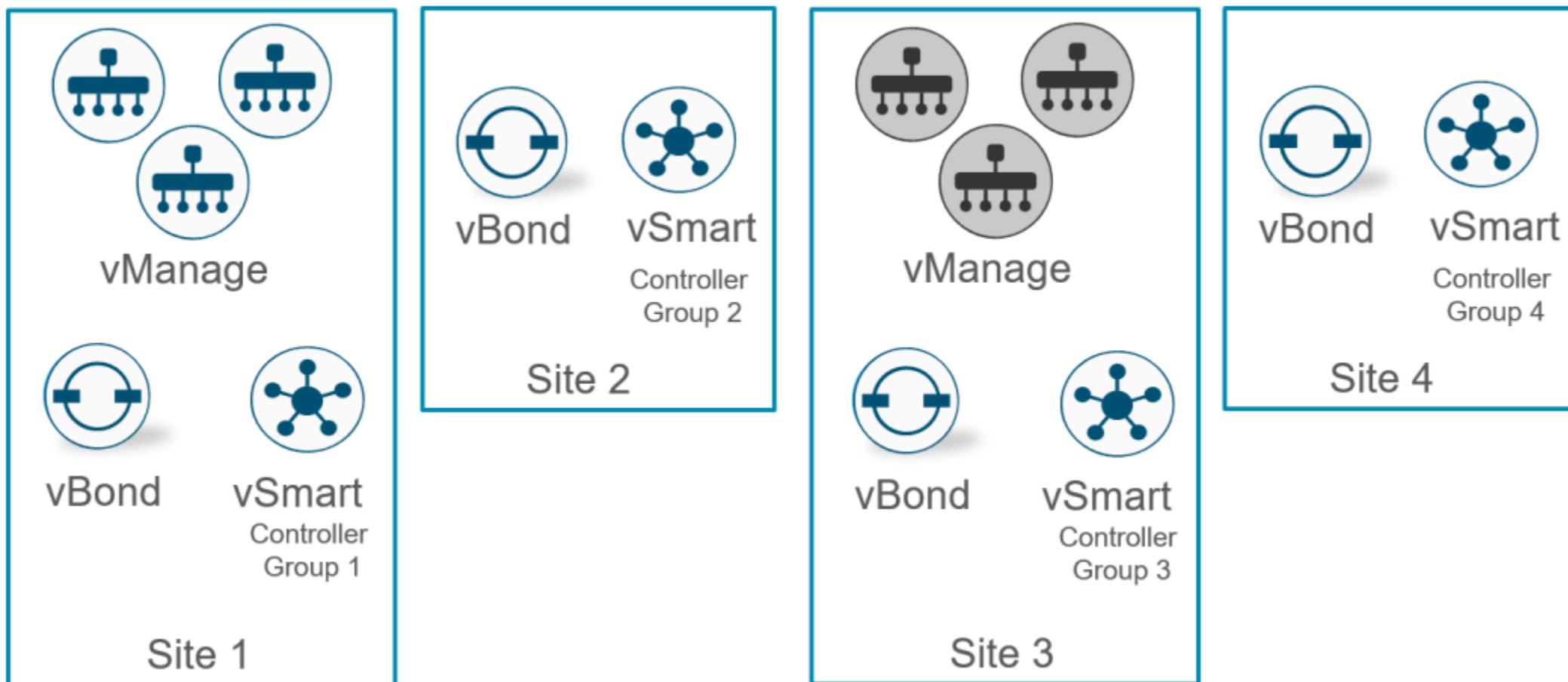


## 控制器部署案例二





# 控制器部署案例三



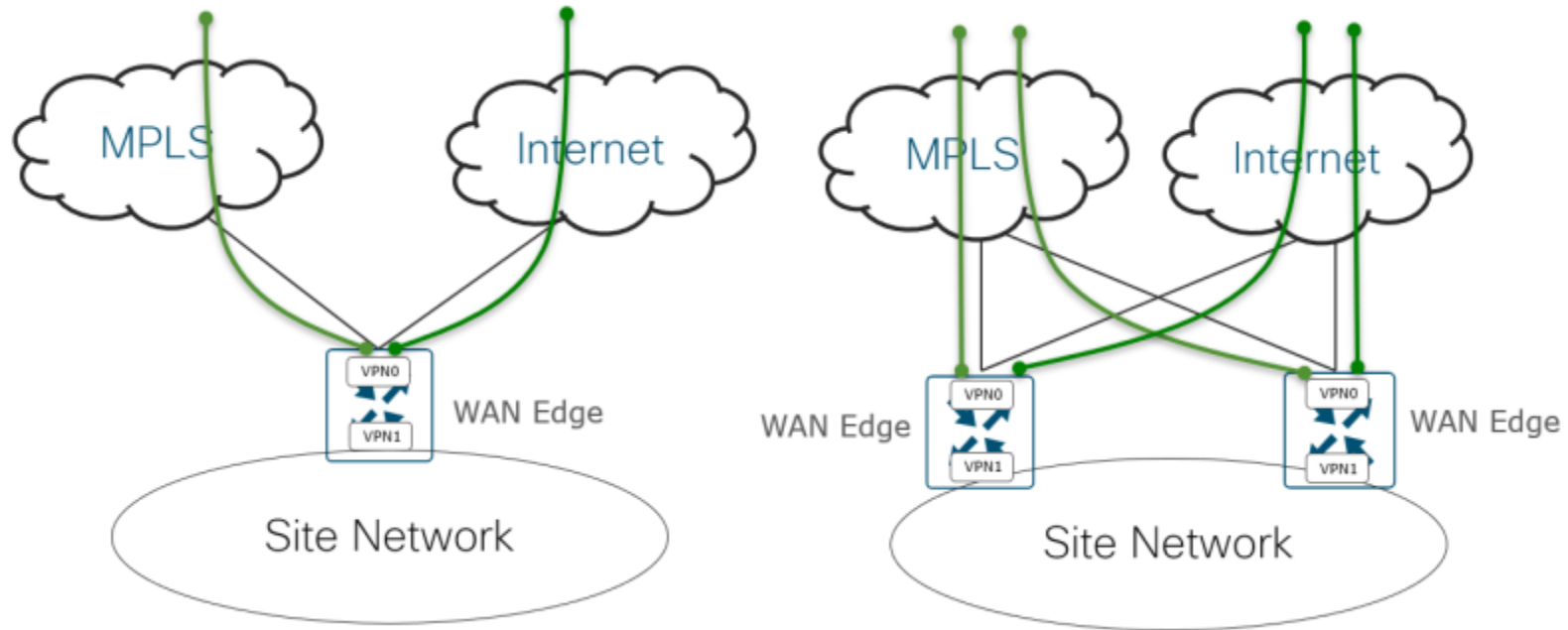


# 4 Cisco Viptela Edge部署



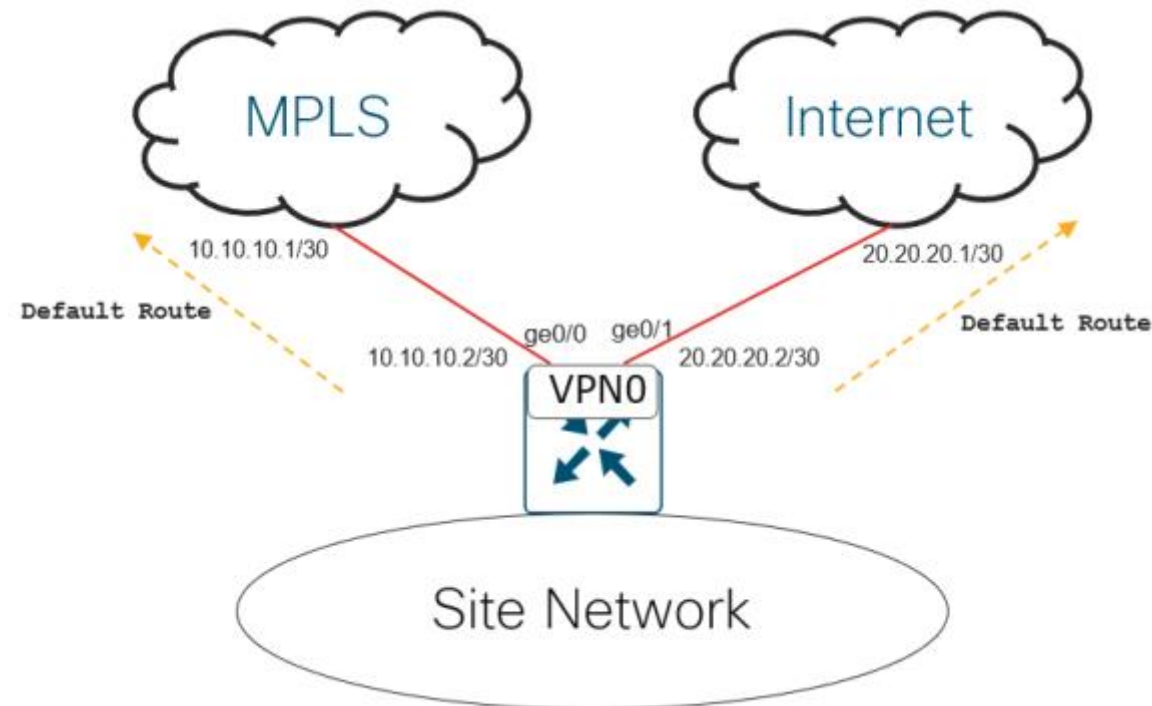


# Single vs dual WAN Edge router sites





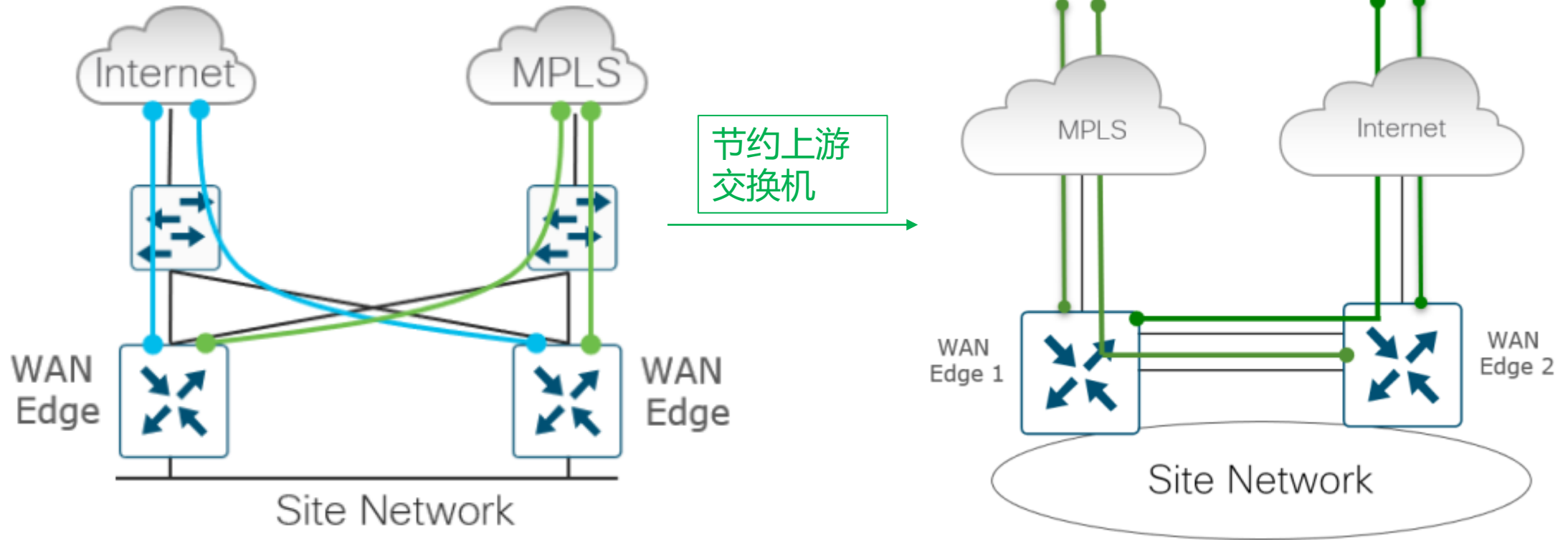
## 多条默认路由



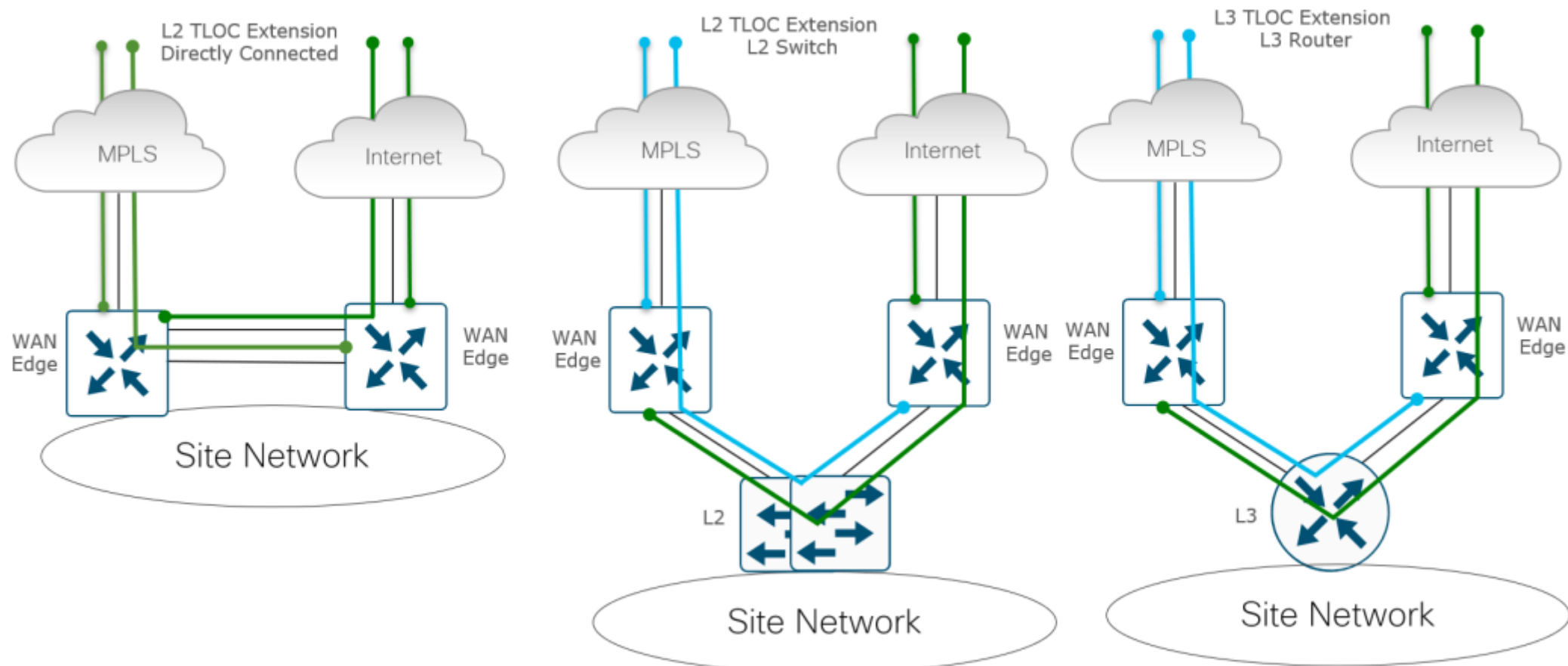
Typically, all that is needed for routing in VPN 0 is a default route specifying the next hop IP address for each transport[一般情况每一个介质一个默认路由即可]. Its purpose is to build IPsec-encapsulated data tunnels to other WAN Edge routers and build control plane DTLS/TLS tunnels to the SD-WAN controllers. Multiple default routes can exist within VPN 0 because the route that is chosen depends on the tunnel source IP address, which should be in the same subnet as the default-route next-hop IP address.



# TLOC extension



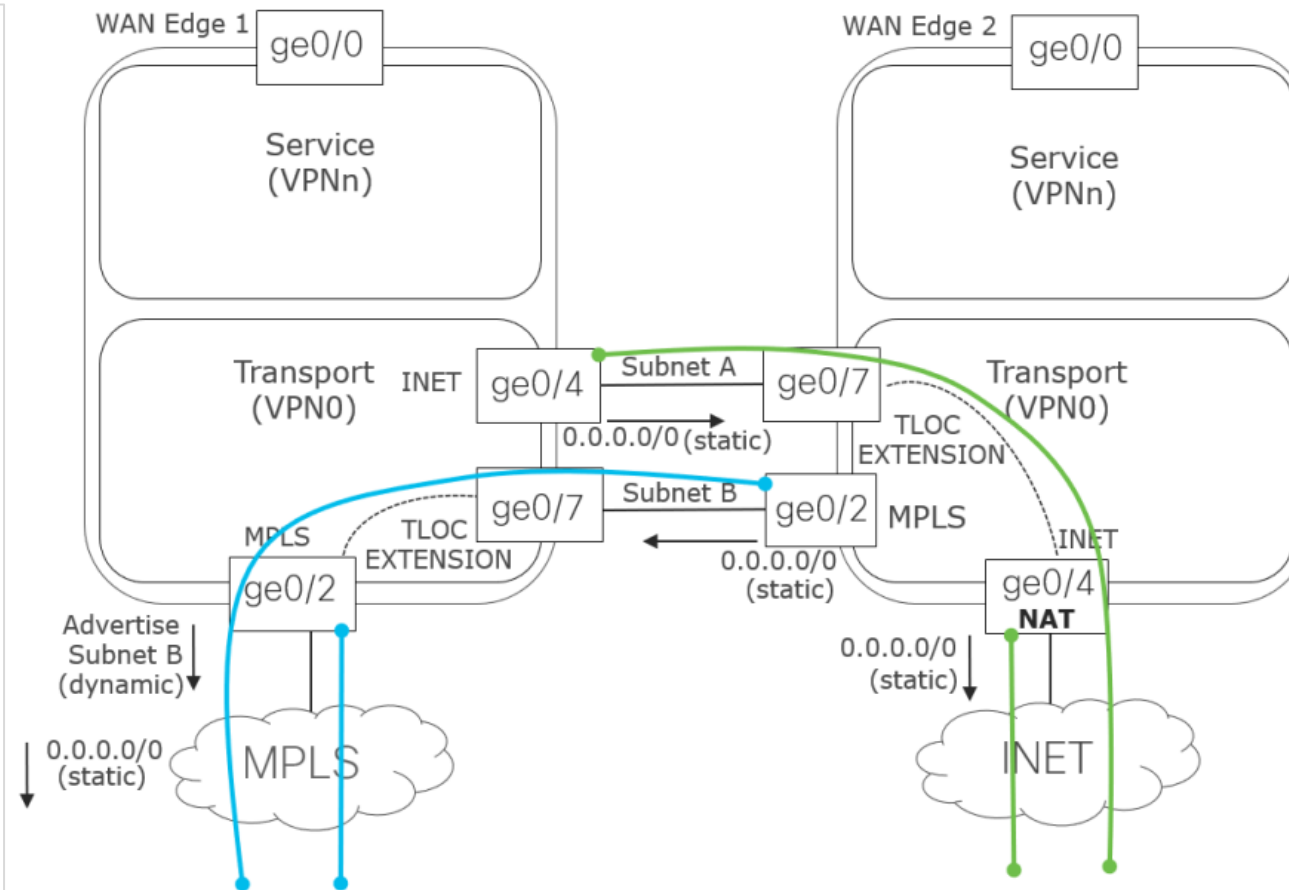
## L2 vs L3 TLOC extension部署



- L3 TLOC extensions are implemented **using GRE tunnels**. Note that TLOC extensions can be separate physical interfaces or subinterfaces (if bandwidth allows).
- L3 TLOC extension **is only supported on IOS XE SD-WAN routers** – they are not supported on vEdge routers



## TLOC extension案例



To reach the **MPLS** transport, WAN Edge 2's MPLS interface should be configured with a default route pointing to WAN Edge 1's ge0/7 IP address. To ensure traffic can be **routed back to the TLOC extension** interface, a routing protocol (typically BGP, or OSPF) can be run in the transport VPN (VPN 0) of WAN Edge 1 to advertise subnet B so that the MPLS provider has a route to subnet B through WAN Edge 1

To reach the **INET** transport, WAN Edge 1's INET interface (ge0/4) should be configured with a default route pointing to WAN Edge 2's ge0/7 IP address. If subnet A is in a private address space, then **NAT** should be configured on WAN Edge 2's ge0/4 transport interface to ensure traffic can be routed back from the Internet to WAN Edge 1 over the TLOC Extension.