

## 【专家问答】问题汇总\_思科 SD-WAN：设计、部署、操作和维护快速指南— 思科社区全球活动

2021 年 3 月 8 日至 19 日，在[思科社区全球专家问答活动](#)中，思科技术专家与大家一起了解 Cisco SD-WAN 的设计方式及其主要优点。探索从基本解决方案设计、选择哪个许可证或选择哪个路由器到总体设计和部署最佳实践的所有内容。vManage 允许您配置设备、模板、安全性/控制策略以及更多内容...。如果由于某些原因 vManage 失败怎么办？我们与您一起掌握策略框架和常见的故障排除工具，并从编程方法中学习如何在 SD-WAN 环境中创建备份。本次活动面向思科 SD-WAN 初学者和高级专业人员。

感谢大家的积极提问以及专家的细致解答，本期【专家问答】活动圆满结束。我们汇总了本期活动用户提出的问题及专家的解答，以方便小伙伴查阅。

---

### 问题一

Q：不好意思，由于对 SD-WAN 不太熟悉，所以提几个特别基础的问题。先谢谢各位专家：

- 1、请问 Viptela 和 Cisco 的 ISR、ASR 系列是否可以在一套 SD-WAN 网络中共存？
- 2、Viptela 的设备目前似乎正在被淘汰，请问 ISR、ASR 等设备升级到 SD-WAN 镜像，相比 Viptela 有什么优点？
- 3、vManage,vBond,vSmart,vEdge，它们在 SD-WAN 网络中的主要角色是什么，以及它们最少&最多可以在 SD-WAN 网络中存在多少个？
- 4、是否只有 vEdge 有云和硬件产品，vManage，vBond,vSmart 都只有云产品，需要安装在虚拟环境？
- 5、vEdge 上线应该不需要手动干预吧？可以做到 0 接触吧，vEdge 上线的详细过程是如何的呢？

6、SD-WAN 的策略框架是什么？

7、SD-WAN 网络中通常会用到的排障工具有什么？哪些比较常用。

8、SD-WAN 的备份是指哪方面的备份，针对主题中所涉及的备份，应该如何操作呢？

**A (社区用户):** 我们单位刚用了思科的 SDWAN 差不多半年左右时间, 你问的问题有几个我能简单回答下。

1、Viptela 和 Cisco 的 ISR、ASR 系列是可以在一套 SD-WAN 网络中共存的

3、vManage 是用来统一管理 SD-WAN 的各种设置的策略服务器，只是用来管理。

vSmart 类似于 MPLS VPN 的路由器反射器一样，上面有各个成功连接站点的路由

vBond 就是 SD-WAN 的边缘设备，可以理解为 CE 吧。

最少多少个，三件套每样至少一个，最多没有详细研究过，不确定。

但是 v M a n a g e 比较耗费资源，只要三台才能组成 HA

4、vManage, vBond, vSmart 都可以虚拟化部署，我们就是搭建在 VM 环境下使用的。

5、0 接触是可以的，具体没有操作过，我们上线的时候都是我远程到各个站点的 local IT 的电脑上远程简单设置一下然后上线的。

6， 7、我也不是很懂，我也在慢慢摸索中。

8、我的备份比较简单粗暴，直接虚拟机快照加备份的，因为 VM 有 HA 的所以不用担心。

如果想把 v m a n a g e 做 HA，只要三台，没有那么多的硬件资源，只能这么通过其他简单粗暴的方法来备份了。

**A (社区用户):** 1、对

2、你还会用 BB 机和同事通信么

3、管理平面，编排平面，控制平面，数据平面

vsmart 是 BGP 中 RR 路由反射器角色，而不是 MPLS-VPN 的反射器，因为 OMP 协议本来就是参

考 BGP 的精简化，建议重学 MPLS 和 BGP

4、yes

5、不需要，设备 DHCP 获取能上网的 IP 地址自动注册到思科 PNP 公网服务器获取初始化配置

6、自行看资料

7、自行看资料

8、vManage 配置备份，数据库备份，FTP 备份导出即可，怎么操作自己看手册

**A:** 您好，非常感谢您参加论坛活动，欢迎提出任何问题。

1. Viptela 和 Cisco 的 ISR 和 ASR 系列能否在 SD-WAN 网络中共存？

绝对地，XE 和 Viptela 操作系统可以在一个 SD-WAN Fabric 中完全互操作。

2. 如今，Viptela 设备似乎已过时。与 Viptela 相比，将 ISR，ASR 和其他设备升级到 SD-WAN 镜像有什么优势？

从 XE 的 17.x 版本开始，我们有了一个通用映像，可让您在自治模式(传统 XE)或控制器模式(SD-WAN)下运行，仅需单个命令即可。与 Viptela 操作系统相比，XE 提供了更丰富的功能集，同时具有 Viptela 操作系统带给 Cisco SD-WAN 的嵌入式 SD-WAN 功能。仅提及 XE 可以提供而 Viptela OS 无法提供的一些功能，即 URL-F 和 IPS，它们是 XE 体系结构内的容器上托管的功能。请记住，思科已经发布了新的路由器 Catalyst 8000 Edge，它也可以提供帮助。您可以在 [https://www.cisco.com/c/es\\_mx/solutions/enterprise-networks/sd-wan/index.html#~case-studies](https://www.cisco.com/c/es_mx/solutions/enterprise-networks/sd-wan/index.html#~case-studies) 上查看更多详细信息

3. vManage, vBond, vSmart, vEdge, 它们在 SD-WAN 网络中的主要作用是什么，至少（最多）可以在 SD-WAN 网络中存在多少？

vManage 是一个单一的窗格，您可以从中进行操作，配置，故障排除和监视 SD-WAN 网络。 vBond 充当协调器，并利用 Cisco 值得信赖的系统以及 STUN 服务器来处理结构元素的私有/公共寻址。 vSmart 是操作的大脑，处理加密密钥和所有智能功能-意味着将路由信息传播到数据平面-路由器-。最后但同样重要的是，WAN Edges 可以执行控制器指示的内容，同时保持其智能和强大的功能来开发诸如 QoS, ACL 等任务。

叠加层上 Edges 的数量可能会有所不同，具体取决于客户，但是该数量将直接取决于我们在叠加层中拥有的 vManage, vBond 和 vSmart 实例的数量。常见部署有 1 个 vManage, 2 个 vBonds 和 2 个 vSmarts。但是您最多可以有 6 个 vBonds, 20 个 vSmarts 和 6 个 vManages。为了按照最佳做法进行设计，请确保您检查 <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/hardware-and-software-installation.html> , 思科团队始终乐于帮助您根据客户要求设计最佳实践。

4. vEdge 同时具有云和硬件产品，而 vManage / vBond / vSmart 仅具有云产品，对吗？是否需要在虚拟环境中安装它们？

正确，vEdge 具有物理设备和 VNF 或虚拟实例 (vEdge 云)。 cEdge (XE OS) 也会发生同样的情况，当需要 IaaS 时，公共云提供商市场中可以使用 CSR1000V 和 C8KV。如果需要内部部署，则可以根据以下链接将其实例化：

ESX:

[https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/b\\_CSR1000v\\_Configuration\\_Guide/b\\_CSR1000v\\_Configuration\\_Guide\\_chapter\\_011.html](https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/b_CSR1000v_Configuration_Guide/b_CSR1000v_Configuration_Guide_chapter_011.html)

KVM:

[https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/b\\_CSR1000v\\_Configuration\\_Guide/b\\_CSR1000v\\_Configuration\\_Guide\\_chapter\\_0101.html](https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/b_CSR1000v_Configuration_Guide/b_CSR1000v_Configuration_Guide_chapter_0101.html)

HyperV:

[https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/b\\_CSR1000v\\_Configuration\\_Guide/b\\_CSR1000v\\_Configuration\\_Guide\\_chapter\\_0110.html](https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/b_CSR1000v_Configuration_Guide/b_CSR1000v_Configuration_Guide_chapter_0110.html)

要查看更多具体信息，请查看此前的问题回复。

#### 5. vEdge 可以在没有手动干预的情况下上线吗？可以零接触吗？启动 vEdge 的详细过程是什么？

是的，思科 SD-WAN 提供真正的零接触配置（ZTP），您可以在此处获取详细信息：

<https://blogs.cisco.com/networking/cisco-sd-wan-delivers-true-zero-touch-provisioning-oid-psten019112>

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-wan-edge-onboarding-deploy-guide-2020nov.pdf>

基本上，Cisco 的 PnP 服务会映射您已为组织许可的设备，一旦连接设备并通过 DHCP 和 DNS 获得 IP，就会有回叫（从 PnP 检索验证）和从 vBond 进行身份验证的功能。在安装到 SD-WAN 结构上后，最近下载了配置模板，这是一个先决条件，必须为您的设备分配一个配置模板序列号。

#### 6. SD-WAN 的战略框架是什么？

思科 SD-WAN 通过不同的策略为您提供最精细，可定制的路由框架，这是解决方案中更具战略意义的部分，您可以在此处查看详细信息：

<https://www.cisco.com/c/en/我们/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/policy-framework.html>

#### 7. SD-WAN 网络中通常使用哪些故障排除工具？

在每个设备的“网络”>“故障排除”下，您可以检查“设备启动”阶段，“控制连接”，使用 Ping 或 TraceRoute 进行特定设置，这是所有网络工程师常用的。当您需要查看应用程序的运行方式时，可以使用 App Route 可视化或模拟流程。 Packet Capture 也是了解真相的好工具。

[https://www.cisco.com/c/en/us/td/docs/routers/sdwan/vManage\\_How-Tos/vmanage-howto-book/m-troubleshooting.html](https://www.cisco.com/c/en/us/td/docs/routers/sdwan/vManage_How-Tos/vmanage-howto-book/m-troubleshooting.html)

## 8. SD-WAN 备份指的是哪种备份，我们应该如何操作本主题中涉及的备份？

关于如何备份和/或还原设备模板、功能模板、策略或列表，您可以使用编程方式，因为这是 Cisco SD-WAN 的本机部分，建议查看 <https://github.com/CiscoDevNet/sastre> 并查看 <https://developer.cisco.com>

希望这些回答对您有所帮助。

**Q:** 感谢大佬的解答和小 M 的回复。多谢!

### 问题二

**Q:** 请问服务器需要满足什么样的要求，才可以安装 SD-WAN?

**A:** 您好。Cisco SD-WAN 在云中包括所有管理组件（vManage，vBond 和 vSmart），并支持以下平台 at

the edge:

- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco 1000 Series ISRs
- Cisco 4000 Series ISRs
- Catalyst 8000
- Cisco 5400 ENCS with the ISRv
- Cisco UCS with the ISRv
- CSR 1000v

话虽如此，如果您使用云部署模型，并且将 Catalyst 8000、ASR 或 ISR 用作边缘设备，则由于没有使用服务器，因此没有特定的服务器要求。

如果您希望所有管理组件都在内部部署。以下链接提供了针对 Cisco vBond Orchestrator 服务器, Cisco

vManage 服务器和 Cisco vSmart Controller 服务器的 ESX / KVM 服务器建议:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/hardware-and-software-installation.html>

在 VMware vSphere ESXi 或基于内核的虚拟机（KVM）服务器上运行每个组件 Cisco vBond Orchestrator, Cisco vSmart Controller 和 Cisco vManage 服务器所需的资源将因您在覆盖网络中部署的设备数量而异。还请注意，所有操作系统卷都必须在固态硬盘（SSD）上。

如果您的边缘设备不是 Catalyst 8000, ASR 或 ISR 路由器，而是运行在 Cisco UCS 服务器和/或 Cisco ENCS 平台上的 ISRV：

服务器必须至少支持以下各项：

1.5 GHz 或更高频率的 Intel®Atom®或 Xeon®CPU

AMD®嵌入式 R 系列

千兆以太网接口

ISRV 需要虚拟服务器硬件中的以下内容：

CPU：1 到 4 个虚拟 CPU（取决于吞吐量和功能集）

内存：4 GB 到 16 GB（取决于吞吐量和功能集）

磁盘空间：8 GB

网络接口：两个或多个 vNIC，虚拟机监控程序允许的最大数量（26）

关于 CSR 1000v，此处的要求适用于：

ESX：

[https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/b\\_CSR1000v\\_Configuration\\_Guide/b\\_CSR1000v\\_Configuration\\_Guide\\_chapter\\_011.html](https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/b_CSR1000v_Configuration_Guide/b_CSR1000v_Configuration_Guide_chapter_011.html)

KVM：

[https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/b\\_CSR1000v\\_Configuration\\_Guide/b\\_CSR1000v\\_Configuration\\_Guide\\_chapter\\_0101.html](https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/b_CSR1000v_Configuration_Guide/b_CSR1000v_Configuration_Guide_chapter_0101.html)

HyperV:

[https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/b\\_CSR1000v\\_Configuration\\_Guide/b\\_CSR1000v\\_Configuration\\_Guide\\_chapter\\_0110.html](https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/b_CSR1000v_Configuration_Guide/b_CSR1000v_Configuration_Guide_chapter_0110.html)

### 问题三

**Q:** 可以分享一个 **DIA** 部署的示例吗?

**A (社区用户):** <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-secure-direct-internet-access-usecase-guide.html>

**A:** DIA 通过允许分支机构用户直接从分支机构访问 Internet 资源和 SaaS 应用程序来改善用户体验。传统上, 分支机构通过集中式数据中心访问 SaaS 应用程序, 这导致应用程序延迟增加和用户体验无法预测。随着 SD-WAN 的发展, 访问 SaaS 应用程序的其他网络路径成为可能, 包括直接 Internet 访问 (DIA) 以及通过区域网关或托管站点的访问。但是, 网络管理员可能无法从远程站点了解 SaaS 应用程序的性能, 因此, 选择哪种网络路径来访问 SaaS 应用程序以优化最终用户体验可能会遇到问题。另外, 当发生网络更改或损害时, 可能没有简便的方法将受影响的应用程序移动到备用路径。

使用 Cisco SD-WAN, 此功能称为 Cloud onRamp。它使您可以直接从 Internet 或通过网关位置轻松配置对 SaaS 应用程序的访问。它不断地探查, 测量和监视通向每个 SaaS 应用程序的每条路径的性能, 并根据损耗和延迟选择性能最佳的路径。如发生损害, SaaS 流量将动态智能地移动到更新的最佳路径。

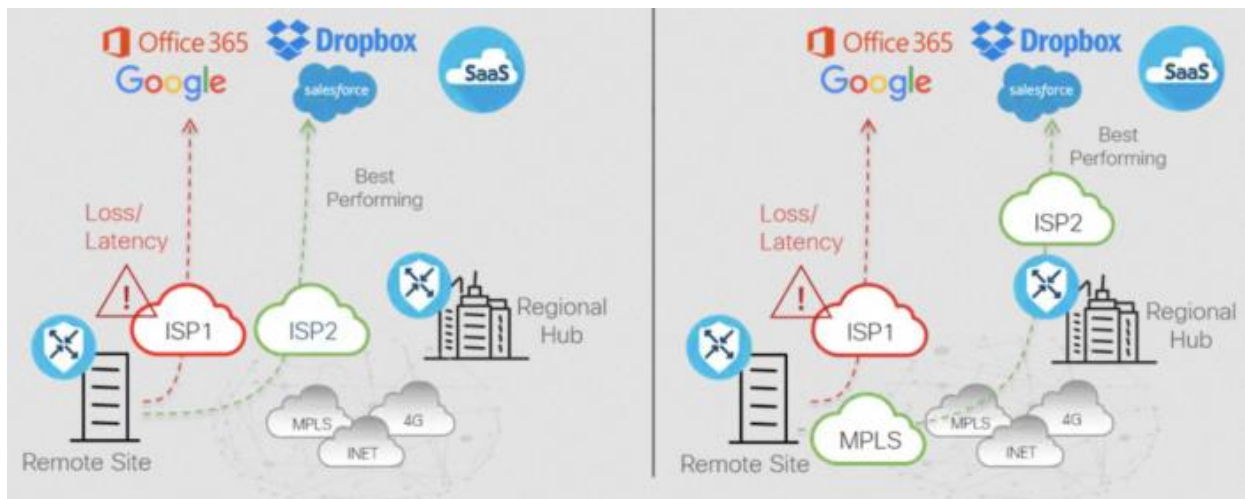
可以利用此功能的应用程序示例为:

- Office 365
- Salesforce
- Google App
- Box
- Dropbox
- Concur



Intuit  
AWS  
GoToMeeting  
Oracle  
SugarCRM  
Zendesk  
Zoho CRM

适用于 SaaS 的 Cloud onRamp –选择了最佳性能的路径



第二个示例是用于 IaaS 的 DIA。 IaaS 可以按需向最终用户提供网络，计算和存储资源，这些资源可以通过 Internet 在公共云（例如 AWS, Azure 或 Google Cloud）中使用。传统上，对于分支机构来说，要获得 IaaS 资源，就不能直接访问公共云数据中心，因为它们通常需要通过数据中心或托管站点进行访问。另外，在从分支机构到公共云之间没有一致的分段或 QoS 策略的情况下，对 MPLS 的依赖也无法在私有云数据中心到达 IaaS 资源。

适用于 IaaS 的 Cisco Cloud onRamp 是一项功能，可自动从数据中心或分支机构连接到公共云中的工作负载。它会自动在公共云中部署 WAN Edge 路由器实例，这些实例将成为 SD-WAN 覆盖的一部分，并建立与位于数据中心或分支机构中的路由器的数据平面连接。它将完整的 SD-WAN 功能扩展到云中，并在 SD-WAN 架构和云中扩展了通用策略框架。适用于 IaaS 的 Cisco Cloud onRamp 消除了需要遍历数据中心的 SD-WAN 站点的流量，从而提高了公共云中托管的应用程序的性能。它还为云中托管的应用程序提供了高可用性和路径冗余，这也非常具有成本效益。

Regards.

#### 问题四

**Q:** 思科 SD-WAN 能够提升我的 Office 365 连接性吗？

**A:** 您好，

- 企业可以利用 Cisco Cloud OnRamp for SaaS 功能智能地路由 Microsoft 365 流量，从而提供快速，安全和可靠的最终用户体验。
- Cloud OnRamp for SaaS 通过体验质量指标为网络管理员提供了对应用程序性能的卓越实时和历史可视性。
- 将连续监视分支机构，区域中心和数据中心从每个电路到 Microsoft 365 的所有路径的性能，并且将应用程序流量动态路由到性能最佳的路径，而无需人工干预。
- Cloud OnRamp for SaaS 通过体验质量指标为网络管理员提供了对应用程序性能的卓越实时和历史可视性。
- 思科 SD-WAN 技术使企业能够构建可扩展且与运营商无关的 WAN 基础架构，从而降低 WAN 传输成本和网络运营支出。
- Cisco SD-WAN 使客户能够应用以业务为中心，应用程序感知和差异化的路由策略-在分支机构为最终用户提供直接连接到性能密集型可信应用程序（例如 Microsoft 365）的同时，通过 SWG 路由通用 Internet 流量，CASB，或客户的数据中心。

以下链接供您参考：[https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white\\_paper-c11-741353.html](https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white_paper-c11-741353.html)

## 问题五

**Q:** 你好，

我想知道 **SDWAN** 虚拟映像之间的优缺点：**vEdgeCloud**，**CSR1000V** 和 **Cat8000v**。

在云服务提供商 (**AWS**，**AZR**，**GCP**) 中，这些类型的部署、性能和可用性的最佳实践是什么？

非常感谢。

**A:** vEdge Cloud 基于 Viptela 操作系统，而 CSR1000v 和 Catalyst 8000v 使用 IOS-XE。

实际上，Catalyst 8000v 是 CSR1000v 的演进，从版本 17.4 开始，只有 Catalyst 8000v 可用。

如何在它们之间进行选择？如果您当前的体系结构是基于 vEdge 设备构建的，则 vEdge Cloud 可能是最佳选择。

如果您使用绿色现场部署，则 Catalyst 8000v 可以提供更多服务。

Catalyst 8000v 可在 AWS，Azure 和 Google Cloud Platform 上使用。

可以在 Azure 和 AWS 市场中找到 vEdge Cloud。

在以下“Catalyst 8000v 配置指南”链接里，您可以看到一些部署示例：

<https://www.cisco.com/c/en/us/support/routers/catalyst-8000v-edge-software/products-installation-and-configuration-guides-list.html>

## 问题六

**Q:** 您好，我了解 **Controller UI** 可以立即使用。如何进行下一步更详细的配置？

**A:** Hi, Jackson, 你好。

首先，请记住此解决方案的业务目标是什么，部署它的原因是什么，您要实现的目标。

其次，花一些时间进行计划，然后再进行配置。提前计划您的系统 IP，创建结构化的站点 ID 方案，定义要使用的 TLOC Colors，设计有关 VPN 分段和拓扑的安全策略，等等。这样，您将调出配置中涉及的大多数细节，并且在创建配置模板后可以节省很多时间。

完成规划后，就该设置控制平面了。此时，您将配置基本连接并在 vManage、vBond 和 vSmart 控制器上部署证书。一旦控制平面启动并运行，并且建立了控制连接，您就可以开始创建配置模板并配置 WAN Edge 了。

希望对您有所帮助，如果还有其他疑问，请联系我们。

## 问题七

**Q:** 感谢这个活动。我有一个问题，如何确定安全计划？

**A:** 你好 Adolfo，

首先，控制平面使用带有 2048 位 RSA 密钥的数字证书来认证网络中的边缘路由器。

控制平面通过 DTLS 或 TLS 加密。这意味着所有边缘设备都将与业务流程组件建立安全连接。

我们通过结合使用以下两个安全元素来保持控制平面的完整性：AES-GCM 消息摘要以及公共和私有密钥。

由于我们的控制平面现在是安全和受信任的，因此我们正在构建 IPsec 隧道以进行数据通信（数据平面）。

这是一个简化的答案，您可以在以下文档找到有关 SD-WAN Fabric 内部安全性的所有详细信息：

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge-20-x/security-book/security-overview.html>

## 问题八

**Q:** 关于 SD-WAN 的认证，已经发布了哪些新材料，或者有可以支持我们考试的教程？

**A:** 谢谢你的问题。 我将尝试为您提供一些 Cisco 文档，书籍和实验室，以便您不仅可以获取理论知识，还可以使用 SD-WAN 进行一些实际操作。

思科 SD-WAN 设计指南：

<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html>

用户文档/配置指南：

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/config/ios-xe-sdwan17.html>

书籍：

思科软件定义的广域网：使用思科 SD-WAN 设计，部署和保护下一代 WAN

<https://www.ciscopress.com/store/cisco-software-defined-wide-area-networks-designing-9780136533177>

Cisco DevNet SD-WAN Sandboxes

<https://developer.cisco.com/sdwan/sandbox>

Cisco dCloud

<https://dcloud.cisco.com/>

\*某些实验室可能需要合作伙伴级别的访问权限。

SD-WAN Mastery Collection

<https://digital-learning.cisco.com/#/course/60680>

Implementing Cisco SD-WAN Solutions (SDWAN300) v1.0

实施思科 SD-WAN 解决方案 (SDWAN300) v1.0

<https://www.cisco.com/c/en/us/training-events/training-certifications/training/training-services/courses/implementing-cisco-sd-wan-solutions-sdwan300.html>

**A:** 您好，您还可以关注一门课程。有关该课程的所有详细信息，请访问以下链接：

[https://www.cisco.com/c/dam/en\\_us/training-events/training-services/course-overviews/sdwan300.pdf](https://www.cisco.com/c/dam/en_us/training-events/training-services/course-overviews/sdwan300.pdf)

## 问题九

**Q:** 您好，是否可以将 **Anyconnect** 与 **Cisco SD-WAN** 一起使用？

**A:** 你好 Thomas，抱歉现在这个还不支持

**Q:** 谢谢。目前，我相信没有采用 **Cisco SD-WAN** 的客户端 **VPN** 解决方案。是路线图上的东西还是根本没有？

用例是当客户无法为所有员工使用小型 **SD-WAN** 路由器而价格太昂贵时，使用客户端 **VPN** 软件连接到 **SD-WAN** 结构。

**A:** 目前尚无针对客户端 **VPN** 支持的公开路线图。

但是，如果需要，您可以将网络中的现有 **Cisco** 防火墙用作客户端 **VPN** 集中器，并使用数据中心中的 **SD-WAN WAN Edge** 创建一个传输网络。

## 问题十

**Q:** 您拥有哪种类型的 **DNA** 许可证？我应该如何选择一个来实现我的 **SD-WAN** 网络目标？

**A:** Hi, Alain,

共有三个主要许可级别，可根据客户需求进行调整：DNA Essentials 具有简化的管理和从一个单一窗口中获得的安全性； DNA Advantage 具有无限制的分段功能；云部署模型和丰富的分析附件； DNA Premier 具有所有包含的功能 在 Essentials 和 Advantage 中使用，但具有高级云交付的安全性。

有关更多详细信息，请查看：<https://www.cisco.com/c/en/us/products/software/dna-subscription-wan/index.html>

希望这会有所帮助。

## 问题十一

**Q:** 对 SD-WAN 不太熟悉，提的问题可能比较基础。感谢各位专家：

- 1、SD-WAN 对流量调整基于类似 SR-TE，还是路由，又或者应用？
- 2、vEdge 或 cPE 是否可以穿越较恶劣的网络环境，如多重 NAT、4G
- 3、未来 SD-WAN 是否会有 Lite 版本，用于体验或者测试

**A:** 感谢您的问题

1. 首先要了解的是，在 Cisco SD-WAN 中，路由器将通过 IPsec 数据传输隧道建立 BFD 会话。BFD 不仅可以用于链路故障检测，还可以用于探测和监视网络特性，例如隧道上的丢失，等待时间和抖动。

Cisco SD-WAN 已经有关于 WAN Edge 上可用的每种传输的性能 SLA 信息。

因此，对于基于应用程序的路由，有一个关键功能称为应用程序感知路由（AAR）策略。AAR 允许我们为关键业务应用程序定义 SLA，它将负责探测网络和路径特征，以动态地在满足指定应用程序 SLA 要求的 WAN 传输链路上实时动态地重新路由应用程序流量。

请查看此文档以获取更多信息：

<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-application-aware-routing-deploy-guide.html>

2. 是的，只要存在 IP 连接，就应该建立 IPsec 隧道而不会出现问题。

3. 对于实验室和测试，请查看以下链接：

思科 DevNet SD-WAN Sandboxes: <https://developer.cisco.com/sdwan/sandbox>

思科 dCloud: <https://dcloud.cisco.com>

\*可能需要合作伙伴级别的访问权限

希望以上信息对您有所帮助。

## 问题十二

**Q:** 与其它厂商对比思科 **SD-WAN** 的优势是什么？中小企业如何在各 **SD-WAN** 厂商中选出适合自己的 **SD-WAN** 解决方案？

**A:** 您好，与其他供应商相比，思科具有很多优势。我建议您查看以下链接以获得主要好处：  
<https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/benefits.html>

关于第二个问题，我建议您直接与您的思科销售代表联系，他们会更愿意帮助您确定合适的解决方案和平台。（您可以致电 4008 100 110,北京时间 | 上午 9 点至下午 6 点）谢谢！

## 问题十三

**Q:** 可以在本地实例化 **Cisco SD-WAN** 控制和管理吗？



**A:** 是的，可以在本地运行控制器（vBond, vSmart, vManage）。但是，在这种情况下，您将负责整个配

置过程，备份和灾难恢复。我建议看一下《设计指南》上的“本地控制器部署”主题：

<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html#OnPremiseControllerDeployment>

**A:** 当然。与云托管选项相比，Cisco SD-WAN 为您提供了在主要公共云提供商上部署控制器或在您自己的

DC 中进行虚拟化的灵活性。有关本地的详细服务器要求，请查看：

[https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/hardware-and-software-installation.html#c\\_Server\\_Hardware\\_Recommendations\\_7477.xml](https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/hardware-and-software-installation.html#c_Server_Hardware_Recommendations_7477.xml)

请注意：考虑到与云托管选项相比，本地虚拟化为您提供了创建、维护、操作的全部所有权。

#### 问题十四

**Q:** SD-WAN 许可证 (L-LIC-DNA-ADD) 是否包含从下载软件站点下载 vManage、vSmart 和 vBond 软

件的许可？我想下载 SD-WAN 软件进行我的复制工作。

**A:** 您提到的部件号 (L-LIC-DNA-ADD) 是购买 Cisco 称为 DNA for Routing 时使用的顶级 SKU。

用于路由的 DNA 是一种订阅许可证，使您的组织有权运行特定的 SD-WAN Router 实例。该许可证与您的思科智能帐户 (Cisco Smart Account) 关联。

路由 DNA 许可证还授予您在 Cisco 的云中实例化 SD-WAN 控制器的权利，换句话说，如果您想让它们在云上运行，则 Cisco 将托管您的控制器 (vBond, vSmart 和 vManage)。

借助 Cisco DNA 软件许可，您的组织还将获得嵌入式 SWSS，其中涵盖了 24x7x365 的 Cisco 技术支持中心 (TAC) 支持，软件版本更新，高级支持分析和指定的服务管理。

考虑到这一点，在配置 vManage（云实例或本地实例）时，有时需要将其与您的智能帐户同步或手动将文件与 WAN Edge 列表一起上传。

因此，总而言之，您需要的是一个 DNA for Routing 许可证，用于每个将成为 SD-WAN 结构一部分的路由器（物理或虚拟）的。

希望这对您有帮助。

## 问题十五

**Q:** 您能告诉我们从思科到思科 **SD-WAN** 的不同许可层中包括什么吗？

**A:** 你好，希望以下内容对您有帮助。

The subscription licensing offers for Cisco SD-WAN are as follows:

- Cisco DNA Essentials: Standard SD-WAN upto 50 devices.
- Cisco DNA Advantage: Cloud-Scale SD-WAN
- Cisco DNA Premier: Advanced Cloud security SD-WAN

These subscriptions are available on a 3-year or 5-year subscription.

Feature	Cisco DNA Essentials	Cisco DNA Advantage	Cisco DNA Premier
Device limit	Up to 50 devices	Unlimited devices	Unlimited devices
vManage for Centralized management (cloud or on-premises)	✓	✓	✓
Flexible topology (hub and spoke, partial mesh, full mesh)	✓	✓	✓
Application-based policies (including application-aware routing policies)	✓	✓	✓
L3/L4/App-Aware Firewall	✓	✓	✓
Snort IPS/IDS with Talos signature updates	✓	✓	✓
DNS monitoring and connector for Cisco Umbrella	✓	✓	✓
Basic path optimization capabilities including Forward Error Correction (FEC)	✓	✓	✓
Dynamic routing protocols (OSPF/BGP)	✓	✓	✓
Unlimited segmentation		✓	✓
vAnalytics		✓	✓
Cloud OnRamp for Infrastructure-as-a-Service (IaaS)		✓	✓
Cloud OnRamp for Infrastructure-as-a-Service (IaaS)		✓	✓
Cisco Advanced Malware Protection (AMP)		✓	✓
Cisco Umbrella cloud-app discovery		✓	✓
Cisco Umbrella Insights			✓
Cisco Threat Grid 200 samples per day			✓

## 问题十六

**Q:** 晚上好，请问什么是用于 Cisco SD-WAN 的 Cisco vAnalytics?

**A:** vAnalytics 平台使用为各个应用程序定制的 vQoE 值来计算应用程序性能。该值的范围是从零到十，其中零是最差的性能，十是最好的性能。vAnalytics 平台会根据延迟、丢失和抖动来计算 vQoE，从而为每个应用程序自定义计算。

vAnalytics 平台可洞悉 WAN 的规划及其运营方面，从历史性能到预测，再提供优化 WAN 的建议。

vAnalytics 平台可存储数月的数据，应用机器学习算法，并提供独特的见解和建议。vAnalytics 平台提

供：

- 可见性-vAnalytics 平台基于从叠加层收集的信息以及其他网络的相关信息，提供对应用程序和网络性能的可见性。这使您可以深入了解一段时间内性能最佳的应用程序和异常的应用程序。
- 预测-vAnalytics 平台可以帮助您计划在未来三到六个月内可能需要更多带宽的站点。
- 假设方案—假设方案可帮助您确定平衡成本，性能以及网络 and 应用程序可用性的机会。
- 建议-vAnalytics 平台运行机器学习算法，以识别微调 WAN 的机会。例如，vAnalytics 平台可以根据您环境中的历史信息推荐可识别应用程序的路由策略。此外，vAnalytics 平台可以跨各种网络服务提供商挖掘数据，并为特定位置推荐网络服务提供商。

## 问题十七

**Q：** 如何正确设置思科 **sdwan** 的大小？ 有什么要考虑的。

**A：** 首先需要考虑客户的网络规模。

基于此，需要确定控制器的大小。 这是第一步。

思科建议根据客户可能拥有的设备数量来确定控制器的大小。

以下内容提供了服务器建议：

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/compatibility-and-server-recommendations/server-requirements.html>

**Q：** 感谢你的快速回复。

那 **WAN Edge** 呢？ 假设我要去托管 **Cisco** 的 **SDWAN** 云， 如何确定正确的 **Wan Edges** 大小？

**A：** 调整路由器大小时，您始终要考虑每个路由器上的总带宽，但这并不是唯一的问题。您必须考虑将要运

行其他哪些服务，拓扑将是怎样的等等。这样，您将可以为您的用例选择最有效的平台和许可证。

## 问题十八

**Q:** 根据您的经验，哪种路由器型号是您最常使用或最推荐的？

**A:** 这取决于客户的（网络）要求。

某些网络可能较小而另一些网络较大，以及云计算与非云计算也不一样，在确定给定站点的设备类型（分支、DC、Colo、远程等）时，这些都需要考虑进来。

## 问题十九

**Q:** 大家好，有没有一种方法可以检查来宾流量是否通过 **GUEST VRF**，其余流量是否遵循全局路由方案？

**A:** 谢谢你的问题。

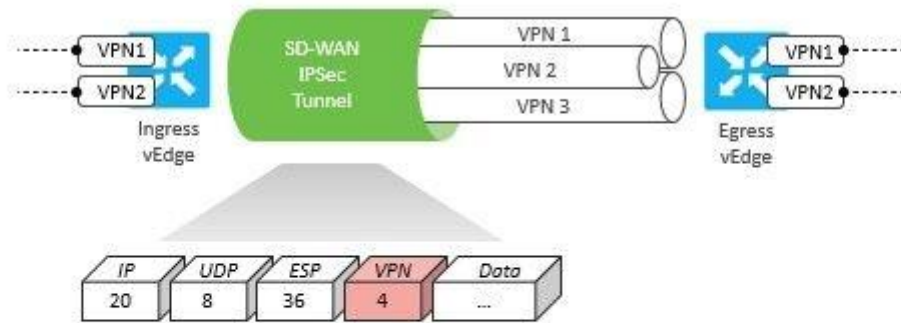
绝对没错。思科 SD-WAN 具有一个名为 Simulate Flows 的故障排除工具，可在 vManage 中访问该工具。您可以使用此工具来确保流量遵循期望的路径。

此外，解决方案中内置了端到端细分。这意味着，不仅在不同的路由表中隔离了来自 VPN（VRF）的流量，而且还使用标签进行了传输。

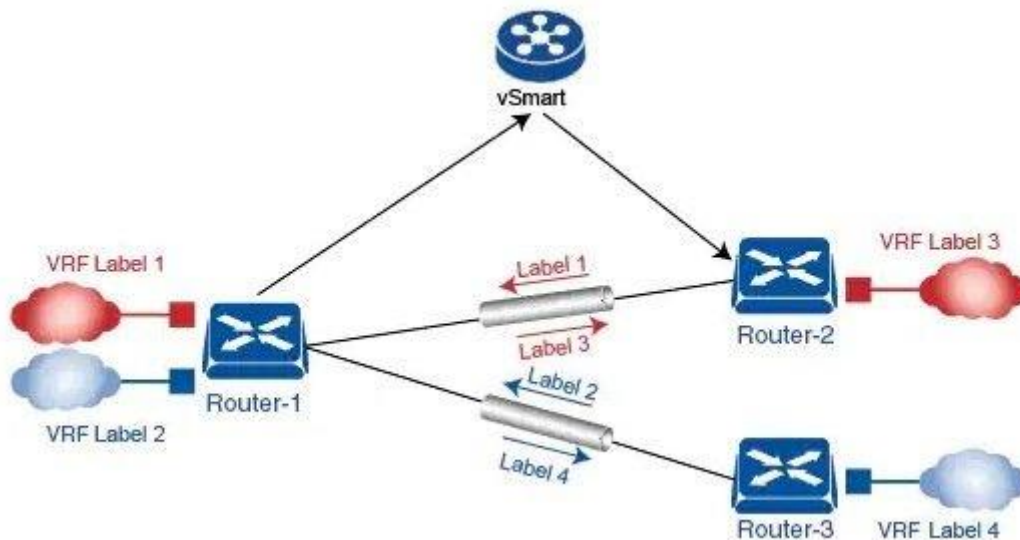
思科文档中的以下文本介绍了工作流程：

在路由器上配置 VRF 时，该 VRF 具有与其关联的标签。路由器将标签以及 VRF ID 发送到 vSmart 控制器。vSmart 控制器将此路由器到 VRF ID 的映射信息传播到域中的其他路由器。然后，远程路由器

使用此标签将流量发送到适当的 VRF。本地路由器在收到带有 VRF ID 标签的数据时，会使用该标签对数据流量进行多路分解。这类似于使用 MPLS 标签的方式。该设计基于标准 RFC，并符合诸如 PCI 和 HIPAA 的监管程序。



- Segment connectivity across fabric w/o reliance on underlay transport
- vEdge routers maintain per-VPN routing table
- Labels are used to identify VPN for destination route lookup
- Interfaces and sub-interfaces (802.1Q tags) are mapped into VPNs



希望以上对您有帮助。

## 问题二十

**Q:** 为什么思科 SD-WAN 在控制平面中使用 OMP 而不在传统路由协议中使用 OMP?

**A:** 因为 OMP 不仅用于传播路由，而且还用于传播有关 TLOC 的策略和信息。与传统协议相比，这提供了更大的灵活性。

希望以上对您有帮助。

## 问题二十一

**Q:** 如何定义警报以及如何使用 REST API 扩展？以及如何通过 Cisco SD-WAN 优化 SaaS 连接？

**A:** 借助用于 SaaS 的 Cloud OnRamp, SD-WAN 架构可通过分支机构中所有允许的路径连续测量指定 SaaS 应用程序的性能。对于每个路径，结构计算的体验质量得分范围为 0 到 10，其中 10 是最佳性能。该分数使网络管理员可以查看从未有过的应用程序性能。最重要的是，结构会自动做出实时决策，以选择远程分支机构的最终用户与云 SaaS 应用程序之间性能最佳的路径。企业可以根据其业务需求和安全要求灵活地以多种方式部署此功能。

## 问题二十二

**Q:** 思科 SD-WAN 可以集成到安全云提供商吗？

**A:** 是的，Cisco SD-WAN 可以集成到安全云提供商，请查看以下详细信息：

<https://umbrella.cisco.com/solutions/sd-wan-security>

## 问题二十三

**Q:** 思科 SD-WAN 包含哪些安全功能？

**A:** 思科 SD-WAN 建立在称为安全访问服务边缘 (SASE) 的架构上。当今的 WAN 安全性和功能必须是分布式的，基于云的，灵活且敏捷的。思科 SD-WAN 是业界首个完全集成的 SASE 产品，将同类最佳的 SD-WAN 与基于云的 Cisco Umbrella 或本地安全产品组合相结合。两种安全体系结构都为连接到云和 Internet 应用程序的企业提供了全面的保护。这些安全功能是：

- **企业防火墙：**精细的策略和对数以千计的应用程序的控制
- **安全的 Web 网关：**全面防御各种基于 Web 的攻击，包括 SSL 检查
- **DNS 层安全性和 URL 过滤：**尽早阻止威胁，显着减少事件
- **IPS：**基于 Snort®并由 Talos®提供支持的本地企业防火墙中的内置入侵防御系统
- **云访问安全代理 (CASB)：**防止帐户泄露，破坏和云应用生态系统中的其他主要风险
- **恶意软件防护：**使用 Cisco AMP 和 Threat Grid 的本地和云安全性的扩展安全功能，可通过沙箱防止和检测恶意文件

## 问题二十四

**Q:** 如果您正在运行的站点仅具有通过 DC 与 Internet 服务的 MPLS 连接，而其他站点仅具有 Internet 连接，那么拥有多个 vSMART 是否合理？一个 vSMART 托管在 MPLS 网络上，另一个托管在云中？

**IE.** 如果 DC 上的 vSMART 或 Internet 连接中断，解决方案的智能功能将不会受到影响？

**A:** 假设您要使用云托管的控制器，这种情况的共同点是在 MPLS 上突破 Internet，打开特定 IP 的特定端口（用于控制器的端口），而您只有一个链接类型的站点，而您的网络则使用 DC（同时存在两种类型的链接）作为相互连接网站的枢纽。作为最佳实践，您将通过环境中的两个链接访问控制器，因此您将弹性作为设计原则。



## 问题二十五

**Q:** 思科 SD-WAN 和 ACI 之间可能有哪些集成? 感谢你的回复!

**A:** Cisco ACI 版本 4.1 (1) 添加了对 WAN SLA 策略的支持。此功能使租户管理员可以应用预配置的策略，以指定 WAN 上租户流量的数据包丢失，抖动和延迟级别。将 WAN SLA 策略应用于租户流量时，Cisco APIC 会将已配置的策略发送到 Cisco vSmart Controller。在 Cisco ACI 中将 Cisco vSmart Controller 配置为提供 Cisco IOS XE SD-WAN 功能的外部设备管理器，它会选择满足 SLA 策略中指定的丢失，抖动和延迟参数的最佳 WAN 链路。WAN SLA 策略通过合同应用于租户流量。

作为使用此功能的示例，请考虑一种部署，其中分支机构使用 MPLS、Internet 和 4G 等多种传输技术通过 WAN 连接到数据中心。在这样的部署中，分支机构和数据中心之间可以有多个路径。在这些情况下，此功能可根据应用程序组和 SLA 提供优化的路径选择。

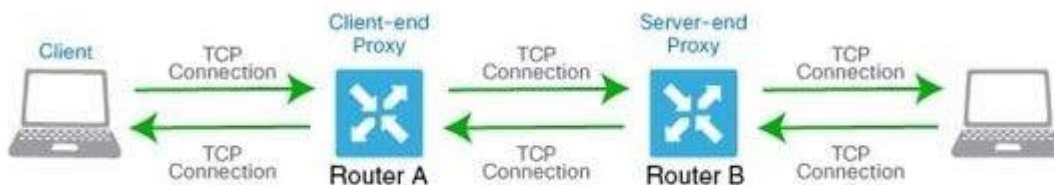
Cisco APIC 版本 4.2 (1) 增加了对从远程站点返回流量的支持，该远程站点发往 ACI 数据中心，以通过 WAN 接收差异化服务。租户管理员将 Cisco APIC 注册到 vManage 之后，Cisco APIC 从 vManage 中提取 WAN-SLA 策略和 WAN-VPN。然后，Cisco APIC 将 DSCP 分配给每个 WAN-SLA 策略并推送前缀列表。如果此 EPG 和 L3Out 之间的合同配置了 WAN-SLA，则从 EPG 提取前缀列表，从而启用返回流量上的服务质量。WAN-SLA 策略和 WAN-VPN 均可在租户公用区中使用。租户管理员将 WAN-VPN 映射到远程站点上的 VRF。

## 问题二十六

**Q:** 可以请您解释一下 TCP 优化的工作原理吗？

**A:** 首先，请记住，TCP 是双向协议，并且仅在 ACK 消息及时确认连接初始化消息（SYN）时才运行。思科 SD-WAN 具有内置的 TCP 优化功能，使我们可以微调 TCP 数据流量的处理，从而减少往返延迟并提高吞吐量。

通过 TCP 优化，路由器可以充当正在启动 TCP 流的客户端和正在侦听 TCP 流的服务器之间的 TCP 代理，如下图所示：



当我们在上述两个路由器上启用 TCP 优化时，路由器 A 终止来自客户端的 TCP 连接，并与路由器 B 建立 TCP 连接。然后，路由器 B 与服务器建立 TCP 连接。这两个路由器将 TCP 通信量缓存在其缓冲区中，以确保来自客户端的通信量到达服务器而不会允许 TCP 连接超时。

**A:** vEdge 和 cEdge 平台均支持 TCP 优化。

请参考以下链接，以了解此功能的工作方式以及如何在相关平台上启用该功能。

# 对于 vE1000, vE2000 和 vE2K

<https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-2.pdf#page=530>

# 对于运行 IOS-XE 的 cEdge

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/optimization-ha/ios-xe-16/network-optimization-high-availability-book-xe/m-tcp-optimization.html>

希望以上对您有帮助。

## 问题二十七

**Q:** 使用来自 **GRE**、**IPSEC** 和 **OMP** 的其他标头，如何在路由器之间定义 **MTU**？

**A:** OMP 是专用于控制平面的协议，也就是说，它传播路由、策略、TLOC。它不会用于传输或封装数据流量。在数据平面中，我们将使用 IPsec 或 GRE 进行封装（默认使用 IPsec），在这种情况下，是的，需要考虑间接费用。请记住，我们在 SD-WAN 路由器之间通过传输隧道建立了 BFD 会话。BFD 将用于链路故障检测，等待时间，丢失和应用感知路由所使用的其他统计信息的测量。BFD 还将协助每种可用传输中的 PMTU 发现过程。

**A:** 在 SDWAN 环境中，我们有两种计算 PMTU 的方法。

\*通过 VPN 0 中的物理接口在传输端完成

\*通过 BFD 运行在数据路径上的两个终端节点之间

详情请参考以下链接：

<https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/configuration/config-18-3.pdf#page=494>

## 问题二十八

**Q:** 考虑到使用基于云的控制器的 **Cisco SD-WAN** 部署，如果 **WAN Edge** 与控制器之间的通信丢失，会发生什么情况？**WAN Edge** 是否能够继续转发数据流量？

**A:** 是的。从边缘设备到 vSmart 的 DTLS 之上运行的 OMP 具有 GR（优美的计时器）值。

当 Edge 失去与 vSmart 的连接时-GR 将启动。默认计时器为 12 小时，并且是可配置的。

详细请参考：

[https://sdwan-docs.cisco.com/Product\\_Documentation/Software\\_Features/SD-WAN\\_Release\\_16.2/03Routing/02Configuring\\_OMP](https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.2/03Routing/02Configuring_OMP)

**A:** 除了以上专家的答复外，环境会根据最新的 OMP 信息继续正常运行。这在 vSmart 端和 WAN Edge 端均有效。默认情况下，OMP 信息会在缓存中保留 12 个小时，可以通过调整称为“OMP Graceful Restart”的选项来更改此信息。

## 问题二十九

**Q:** 哪些路由器型号可以在 Cisco SD-WAN 覆盖内工作？

**A:** 每个需求都有路由器，您可以在此处查看常规清单列表：

<https://www.cisco.com/c/en/us/products/collateral/software/one-wan-subscription/guide-c07-740642.html>

## 问题三十

**Q:** 如何定义警报以及如何使用 REST API 扩展？

**A:** 通过以下链接中的表格，您可以找到如何根据严重性（次要，中等，主要，严重）定义警报。

[https://sdwan-docs.cisco.com/Product\\_Documentation/vManage\\_Help/Release\\_18.4/Monitor/Alarms](https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.4/Monitor/Alarms)

关于 REST API 扩展，对于“警报和监视”，我的建议是使用 Webhooks。它是一种推送模型机制，用于实时发送通知。Webhooks 的例子

<https://developer.cisco.com/codeexchange/github/repo/suchandanreddy/sdwan-webhooks/>

使用传统 REST API 的另一种选择是频繁轮询 vManage 的数据。