

思科企业园区基础设施

最佳实践指南

2014 年 12 月

目录

执行摘要	4
简介	4
企业园区网络设计方案	5
园区多层网络设计建议	5
Cisco Catalyst 系统级设计最佳实践	6
接入层系统设计建议	6
接入层系统冗余最佳实践	7
分布层系统设计建议	9
分布层系统冗余最佳实践	10
分布层网络设计建议	10
分布层网络设计方案	10
虚拟交换系统恢复能力	11
虚拟交换域和最佳实践	11
虚拟交换管理引擎高可用性最佳实践	13
虚拟交换链路设计和最佳实践	13
系统和网络连接最佳实践	16
园区网络超订用最佳实践	16
接入层网络连接最佳实践	17
分布层网络连接最佳实践	20
思科多机箱第 2 层 EtherChannel 最佳实践	20
多机箱 EtherChannel 最佳实践	21
园区多层网络设计最佳实践	24
多层 VLAN 网络设计建议	24
多层网络协议最佳实践	24
VLAN 中继协议建议	25
动态中继协议 (DTP) 建议	25
VLAN 中继设计建议	25
生成树协议建议	26
单向链路检测建议	27
VSS MAC 地址表同步建议	28
园区核心层网络设计最佳实践	28
核心层上行链路设计建议	28
思科多机箱第 3 层 EtherChannel 最佳实践	28
增强型内部网关路由协议设计建议	29
自治系统和网络最佳实践	29
安全路由最佳实践	30
网络路由汇总最佳实践	30
高可用性最佳实践	31
开放最短路径优先路由协议设计建议	31
区域和网络设计最佳实践	32
安全路由最佳实践	32
网络路由汇总最佳实践	33
高可用性最佳实践	33
组播路由协议建议	35
PIM 稀疏模式最佳实践	35
安全组播最佳实践	36
高可用性最佳实践	36
一般路由建议	37

等价多路径路由最佳实践	37
单播 IP 路由项清除最佳实践	38
IP 事件阻尼	38
小结	39
参考资料	39

执行摘要

思科® 统一接入建立了一个能够随时随地使用任何设备，安全、可靠且无缝地将任何人连接到任何资源的框架。该框架可以为所有员工提供各种高级服务，从而利用智能的企业级网络提高收入、工作效率及客户满意度，同时减少企业内部运营效率低下的问题。思科统一接入包含了拥有丰富服务的网络边缘系统，并结合了一个核心网络基础设施，基础设施中嵌入了可提高工作效率的各种高级技术集成，包括 IP 通信、移动、安全、视频和协作服务。

此类任务关键型商业应用要求企业实施具有恢复能力和灵活性的网络，以快速适应不断变化的需求，并安全地支持新的服务和新兴服务。

简介

本文档不仅包含企业园区网络设计和部署指南，还包含了多个详细《思科验证设计指南》中的多项最佳实践。最佳实践结论源自于对多级系统类型、网络设计方案及企业应用的全面解决方案级端到端特征描述。

通过遵循本指南中的最佳实践，企业园区网络可以显著简化网络运营、优化应用性能并构建恢复能力，从而在各种计划内和计划外故障期间，以确定的顺序运营网络。本文档的侧重点是在园区接入层、分布层和核心层系统之间建立坚实的基础和基础设施。它提供了一系列适当的建议，可基于网络中的角色应用于各种平台。

图 1. 大型企业园区分布层网络设计

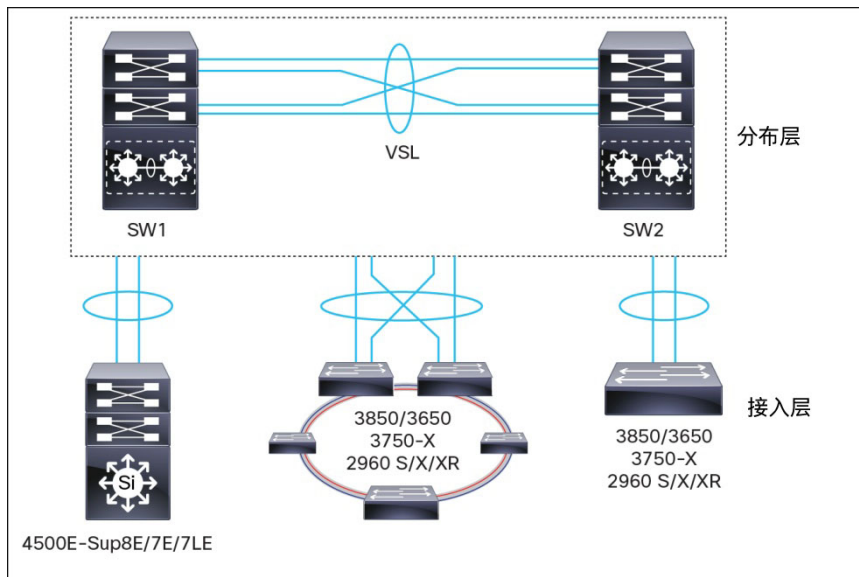


表 1 总结了本文档中包含的硬件和软件修订。

表 1. Cisco Catalyst 交换机硬件和软件版本

网络层	Cisco Catalyst 交换机	软件版本
分布层	Cisco Catalyst 6800 系列交换机	15.1(2)SY2
接入层	Cisco Catalyst 4500 管理引擎 8-E、7-E 和 7L-E	3.3.1.XO
	Cisco Catalyst 3850/3650 系列交换机	3.6.1.SE
	Cisco Catalyst 3750-X/3560-X 系列交换机	3.6.1.SE
	Cisco Catalyst 2960 S/X/XR 系列交换机	15.0.2-EX5

企业园区网络设计方案

这一部分针对园区设计模式中的各层提供较详细的网络基础设施指南。每个设计建议均已优化，可以简化网络并保持成本效益，同时不会影响网络可扩展性、安全性和恢复能力。

园区多层网络设计建议

企业园区网络部署规模和容量多种多样。思科提供广泛、丰富的 Cisco Catalyst® 交换产品组合，可满足各个客户要求的确切业务和技术需求。利用各种各样的系统提供不同的端口密度、交换性能、可扩展性和恢复能力，可以帮助用户设计并建设高性能的端到端多层网络基础设施。

图 2. 园区多层网络部署模式

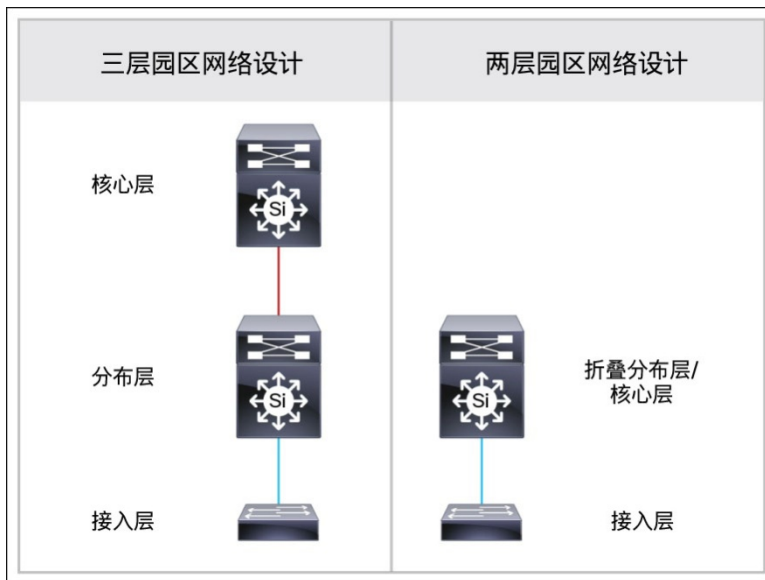


图 2 显示了多层部署模式。根据分布层网络块数量、可扩展性和性能要求不同，园区可以部署以上两种模式中的任意一种。

作为一种最佳实践，当分布层块超过两个时，思科建议部署三层 LAN 设计。部署三层 LAN 网络的主要优势如下：

- **层次：**
 - 帮助理解每个设备在每一层的角色
 - 简化部署、操作和管理
 - 减少每一层的故障域
- **模块化：**根据需要实现无缝网络的扩展和集成服务的启动
- **恢复能力：**满足用户对始终保持网络运行的期望
- **灵活性：**使用所有网络资源来支持智能流量负载共享

Cisco Catalyst 系统级设计最佳实践

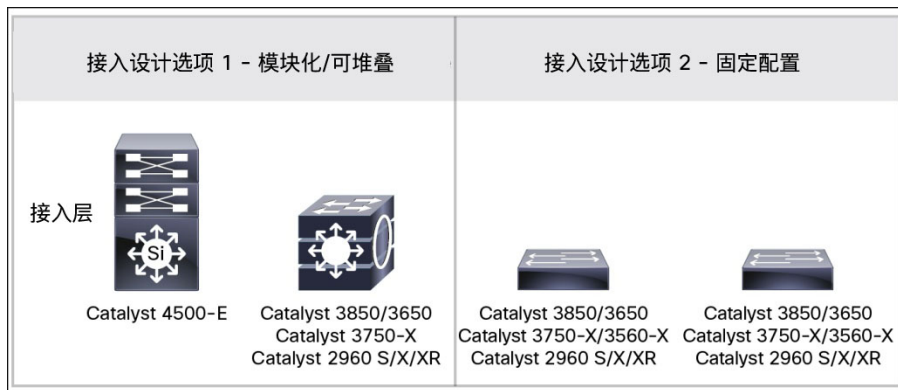
在支持通信基础设施的不同领域和行业中，企业园区网络规模多种多样。新一代综合性 Cisco Catalyst 交换产品组合旨在满足所有部署模式的可扩展性。要为不同网络层上的独特且关键的角色选择合适的产品，必须分析业务、技术和应用需求。这一部分提供了产品指南和多个系统级最佳实践，帮助您建设具有更高安全性、可扩展性和恢复能力的端到端网络。

接入层系统设计建议

接入层是园区的第一层或边缘；在接入层，PC、打印机、IP 视频监视摄像头、Cisco TelePresence® 设备等终端设备连接到园区网络的有线部分。在这一层还会部署 IT 托管设备，可将网络进一步延伸一个级别，例如连接有线或无线最终用户的 IP 电话和无线接入点。可连接的各种设备类型，以及必要的各种服务和动态配置机制，使得接入层成为企业园区网络中功能最丰富的一个部分。

根据各种各样的企业通信设备和端点、网络接入需求和功能，可以部署以下两种接入层设计选项，如图 3 所示。

图 3. 接入层系统设计方案



主要优势：模块化/可堆叠系统设计

- **模块化：**在不改变基础设施的情况下顺畅实现配线间网络扩展，从而提供投资保护。
- **灵活性：**轻松集成新的网络模块或堆栈成员交换机，同时不会中断操作。
- **恢复能力：**
 - Cisco Catalyst 4500E：双管理引擎可提供一流的系统级冗余。作为最佳实践，思科建议部署冗余的管理引擎，以使用状态切换 (SSO) 技术保护单宿主端点。在计划内故障（例如服务中软件升级 (ISSU) 或异常的管理引擎故障）期间，将会全面保护单宿主设备的网络可用性和容量。
 - Cisco Catalyst 3850/3650 StackWise®：新一代 StackWise 技术支持 SSO，可提供协议冗余和采用分布式转发架构的转发状态机。但是，在堆栈成员交换机的单次故障中，单宿主端点将会受到影响。
 - Cisco Catalyst 3850 Cisco StackPower®：网络管理员必须考虑在一个堆栈中的各组 Cisco Catalyst 3850 之间实施电源冗余。即使在外部停电或供电设备发生故障等灾难性故障中，Cisco Catalyst 3850 也能实现不间断转发。

接入层系统冗余最佳实践

模块化交换机与固定配置交换机上的系统级冗余支持并不相同。当按照思科建议的最佳实践设计并部署时，它将实现具有恢复能力的基础设施，以维持关键端点设备的网络通信。

管理引擎和 StackWise 最佳实践

表 2 提供了在配备双管理引擎模块的 Cisco Catalyst 4500E 以及以 StackWise 模式部署的新一代 Cisco Catalyst 3850/3650 系列固定配置交换机上，使用 SSO 技术部署系统级冗余的最佳实践指南。

表 2. 分布层系统恢复能力最佳实践

最佳实践	Cisco Catalyst 4500/3850/3650
在部署了双管理引擎模块的 Cisco Catalyst 4500E 系统上启用 SSO (默认)	4500E(config)#redundancy 4500E(config-red)#main-cpu 4500E(config-r-mc)#mode sso
在以 StackWise 模式部署的 3850/3650 系统上启用 SSO (默认)	3850-Stack(config)#redundancy 3850-Stack(config-red)#mode sso

FlexStack 和 FlexStack Plus 模式下的 Cisco Catalyst 3750-X StackWise-Plus 和 2960 系列平台不支持 SSO 技术。

StackWise 软件自动升级最佳实践

当这些交换机以 StackWise 模式堆叠在一起时，Cisco Catalyst 3850/3650 中的软件恢复能力取决于 Cisco IOS® 软件的高可用性框架。与 4500E 等模块化平台一样，这些新一代固定配置交换机支持 1+1 高可用性 SSO 功能。因此，每个堆栈成员交换机上必须安装一致的 Cisco IOS 软件和许可证，才能提供 1+1 及 N:1 的活动堆栈系统冗余。

如果运行不同软件版本的一台新 3850/3650 加入使用当前运行版本的堆栈环，则此交换机将迫使堆栈环进入路由处理器冗余 (RPR) 状态。在此状态下，系统将保持完全关闭。

作为一种最佳实践，新加入的交换机可以从活动交换机接收一致的软件版本，并在无需用户干预的情况下恢复系统。

表 3 显示了为新加入的交换机自动下载一致软件版本的简单命令行。

表 3. Cisco Catalyst 3850/3650 软件自动升级最佳实践

最佳实践	Cisco Catalyst 3850/3650: StackWise
在 Cisco Catalyst 3850/3650 StackWise 交换机上启用软件自动升级，以在堆栈环中新加入的交换机上自动安装一致的 Cisco IOS 软件	3850-Stack(config)#software auto-upgrade enable

Cisco StackPower 最佳实践

Cisco Catalyst 3850 和 3750-X 系列平台支持创新的 Cisco StackPower 技术，可为固定配置交换机提供电源冗余解决方案。Cisco StackPower 将交换机中安装的所有电源统一起来，创建一个电源池，哪里有需要就将电源引向哪里。使用专门的思科专有 Cisco StackPower 电缆，最多可将 4 台交换机配置到一个 Cisco StackPower 堆栈。Cisco StackPower 电缆与 StackWise 数据线不同，所有 Cisco Catalyst 3850/3750X 型号均提供该电缆。Cisco StackPower 技术可在两种模式下部署：

- **共享模式：**所有输入功率均可用于电源负载。电源堆栈中的所有交换机的总汇聚可用电源（最多四台）视为单个大型电源。堆栈中的所有交换机都可以为连接到以太网供电 (PoE) 端口的所有用电设备提供共享电源。在此模式下，全部可用电源都将用于电源预算决策，不会为了应对电源故障而预留电源。如果电源发生故障，用电设备和交换机可能会关闭。此模式为默认操作模式。
- **冗余模式：**从电源预算中减去系统中最大电源的电源，并预留该电源。这将减少 PoE 设备可用的总电源，但是会在发生电源故障时提供备用电源。虽然在整个池中交换机和用电设备可用的电源减少了，但是在出现电源故障或极端电源负载时必须关闭交换机或用电设备的可能性降低了。为了满足需求，建议预先计算所需电源，并利用双电源部署堆栈中的每个 Cisco Catalyst 3850/3750-X 交换机。如果其中一个供电设备出现故障，启用冗余模式可提供电源冗余作为备用电源。

作为一种最佳实践，为了在堆栈环内提供更有效的电源冗余，思科建议以冗余模式部署 Cisco StackPower。

由于 Cisco StackWise-480 最多可在堆栈环中包含九台 3850 系列交换机，因此必须用两个电源堆栈组部署 Cisco StackPower，以便最多容纳四台交换机。表 4 中的示例配置展示了如何以冗余模式部署 Cisco StackPower 并将堆栈成员分为电源堆栈组。为使新的电源配置生效，网络管理员必须针对网络中断制定计划，因为必须重新加载堆栈环中的所有交换机。

表 4. Cisco Catalyst 3850/3750-X Cisco StackPower 最佳实践

最佳实践	Cisco Catalyst 3850/3650: StackWise
在 3850 系列交换机上部署 Cisco StackPower 技术，以实现顺畅的电源状态切换。建议采用冗余模式	3850-Stack(config)#stack-power stack PowerStack-1 3850-Stack(config-stackpower)#mode redundant 3850-Stack(config)#stack-power switch 1 3850-Stack(config-switch-stackpower)#stack PowerStack-1

Cisco StackWise 和 FlexStack 堆栈 MAC 最佳实践

为了在网络中提供单个统一的逻辑网络视图，将从堆栈中主交换机的以太网 MAC 地址池中提取 StackWise 上第 3 层接口的 MAC 地址（物理、逻辑、交换机虚拟接口 (SVI)、端口通道）。从 StackWise 交换机到端点（例如 IP 电话、PC、服务器和核心网络系统）的所有第 3 层通信将取决于主交换机的 MAC 地址池。

在活动堆栈状态切换期间，以 StackWise 模式部署的 Cisco Catalyst 3850/3650 系列交换机上的堆栈 MAC 地址将保持堆栈 MAC。默认情况下，堆栈 MAC 持久计时器设置为无限制，这意味着无需修改第 3 层接口的 MAC 地址。作为最佳实践，建议保留默认设置，不要修改任何堆栈 MAC 配置。

表 5. Cisco Catalyst 3850/3650 和 3750X 堆栈 MAC 最佳实践

最佳实践	Cisco Catalyst 3850/3650: StackWise
保留 Cisco Catalyst 3850/3650 StackWise 交换机上的默认堆栈 MAC 持久设置	3850-Stack(config)#default stack-mac persistent timer

默认情况下，Cisco Catalyst 3750X StackWise-Plus 和 2960 S/X/XR 系列交换机不会像 Cisco Catalyst 3850/3650 那样保护堆栈 MAC 地址。因此，作为一种最佳实践，建议将堆栈 MAC 持久计时器设置为零（无限制），以防止网络中出现地址解析协议 (ARP) 和路由故障。

表 6. Cisco Catalyst 3750X 和 2960-XR/S 堆栈 MAC 最佳实践

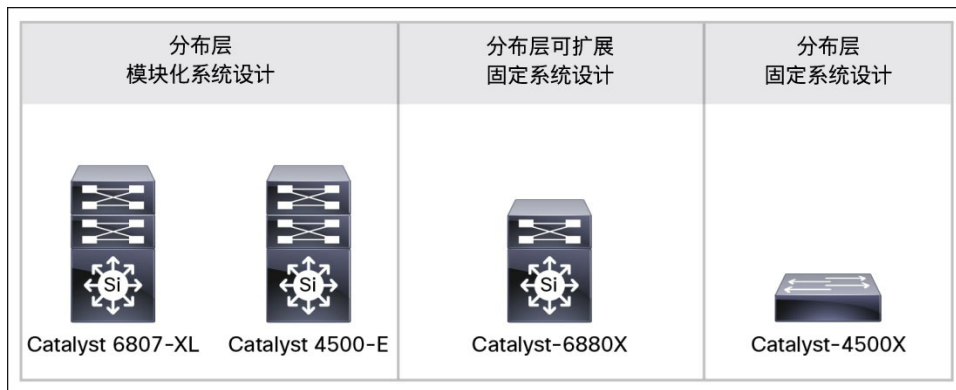
最佳实践	Cisco Catalyst 3750-X: StackWise
将 Cisco Catalyst 3750X 和 2960 S/X/XR 系列交换机上的默认堆栈 MAC 持久计时器修改为无限制	3750-Stack(config)#stack-mac persistent timer delay 0

分布层系统设计建议

分布层或汇聚层是第 2 层配线间网络与第 3 层路由园区核心网络之间的网络边界。使用生成树等传统第 2 层技术时，网络操作、可管理性和应用性能可能会变得异常复杂。分布层系统框架必须按照思科建议的最佳实践来进行设计，这样可以显著降低网络复杂性、提高可靠性并加快网络性能。为了使用三层模式建立强大的园区网络基础，分布层在整合网络和实施网络边缘策略方面发挥着至关重要的作用。

新一代固定和模块化 Cisco Catalyst 交换产品组合支持强大的纵向扩展和横向扩展网络架构，从而构建高性能的基础设施。必须分析和部署适当的 Cisco Catalyst 交换产品，以构建任务关键型分布层系统。图 4 显示了使用企业级网络的分布层部署的两种系统级设计。

图 4. 大型园区分布层系统设计方案



主要优势：模块化和可扩展的固定系统设计：

- **模块化：**通过无缝网络端口提供投资保护，并通过多 TB 交换背板实现吞吐量扩展，无需全面改变基础设施。
- **灵活性：**在一台交换机中轻松集成新的混合介质网络模块，同时不会中断当前网络和业务运营。
- **恢复能力：**
 - **管理引擎模块：**在分布层实现不间断的网络通信和完好无损的性能。在实时软件升级等计划内故障期间，或在灾难性软件故障等计划外故障期间，Cisco SSO 技术都能保护业务连续性。Cisco Catalyst 6880X 支持采用思科虚拟交换系统 (VSS) 技术的机箱间 SSO。
 - **网络模块：**为了在完成新的安装或迁移时不会引起系统停机，支持在线插入和删除网络模块。
 - **电源：**冗余电源可在系统中提供环境保护，以防出现停电或供电设备故障。采用模块化电源冗余设计，即可灵活更换故障设备，同时不会引起网络中断。
 - **风扇托架：**利用热插拔和冗余风扇托架，可以实现更好的冷却效果并可灵活更换故障托架，同时不会引起网络中断。

另外，Cisco Catalyst 4500E/4500X 或 3850 StackWise 还可以部署在分布层，以满足小到中型网络部署的需求。本最佳实践文档重点介绍 Cisco Catalyst 6800 系列系统在分布层的角色，并提供最佳实践指南。

分布层系统冗余最佳实践

Cisco Catalyst 6800 系列交换机是领先的企业级系统，具有极高的性能和可扩展性，可在园区分布层和核心层广泛部署。Cisco Catalyst 6880X 交换机建立在强大的 Cisco Catalyst 6500 系列管理引擎 2T 架构之上，但是外形小巧，在空间有限的环境中进行网络部署时，可实现一致的性能和可扩展性。

表 7 提供了以推荐的 Cisco VSS 模式或传统的单机模式部署 Cisco Catalyst 6807-XL 系列交换机的最佳实践指南，并且配备双管理引擎模块来增加系统级冗余。

表 7. 分布层系统恢复能力最佳实践

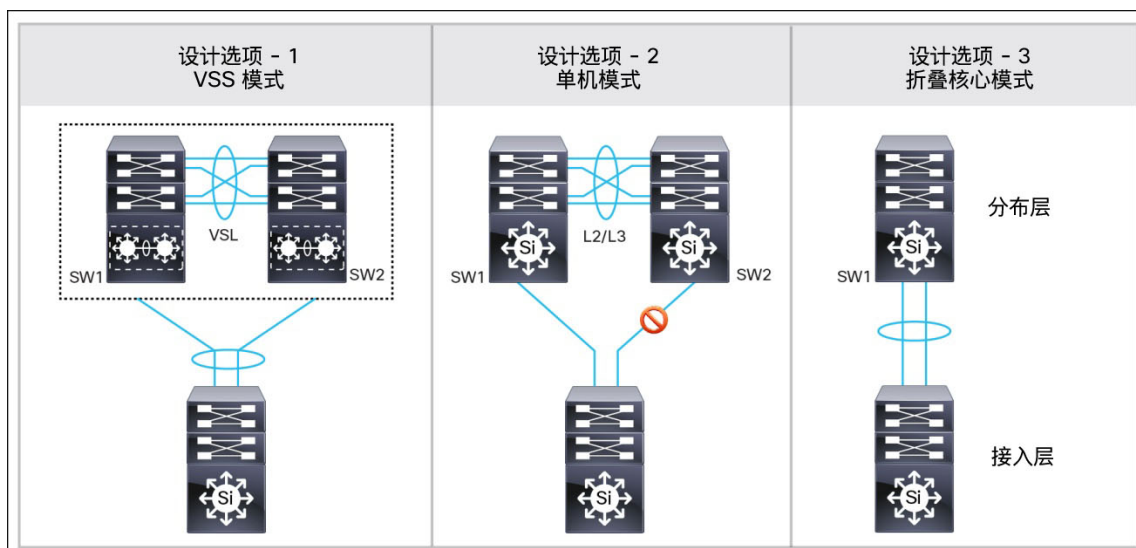
最佳实践	Cisco Catalyst 6800
管理引擎模块 在部署了双管理引擎模块的系统上启用 SSO（默认）。	Dist(config)#redundancy Dist(config-red)#main-cpu Dist(config-r-mc)#mode sso
网络模块 首先关闭网络模块，然后从服务中删除模块，从而降低较高的数据丢失。	VSS 配置模式 Dist(config)#no power enable switch [1 2] module [slot id] 单机配置模式 Dist(config)#no power enable module [slot id]
电源冗余 在灾难性停电或供电设备故障期间启用 1:1 电源冗余保护（默认）。	VSS 配置模式 Dist(config)#power redundancy-mode switch [1 2] redundant 单机配置模式 Dist(config)#power redundancy-mode redundant

分布层网络设计建议

分布层网络设计方案

企业园区分布层网络可以采用各种设计进行部署，从而满足业务、技术和服务需求。通常可以采用图 5 所示的任意设计选项进行部署。根据网络设计和主要技术要求不同，网络架构师必须做出适当的汇聚层设计选择，以实现统一的端到端访问网络服务。

图 5. 园区分布层网络设计方案



上文所述的所有分布层设计模式都能在系统层面提供一致的网络基础服务、高可用性、扩展灵活性和网络可扩展性。必须仔细评估每个设计选项，以比较可扩展性、性能、操作和恢复能力要求：

- 分布层设计选项 1：VSS 模式

该部署模式适用于采用 Cisco VSS 技术的大到中型企业园区网络部署。Cisco Catalyst 6800 支持多 TB 高性能汇聚块，可建立不间断的通信网络，且不影响用户级复杂性。

这是分布层系统的主要推荐部署模式。

- 分布层设计选项 2：单机模式

单机模式是默认模式，已在企业网络中经过多年验证。在分布层和接入层交换机上，可以通过高级微调以单机模式部署 Cisco Catalyst 6800E 系统，以基于生成树协议 (STP) 手动构建可靠的网络。当网络大幅扩展时，网络操作可能会变复杂，因而难以进行部署和故障排除。

这是分布层系统的次要推荐部署模式。本文档不重点介绍这种部署模式。

- 分布层设计选项 3：折叠核心层/分布层模式

这种部署模式对小型园区或远程分支机构网络来说已经足够了。任何 Cisco Catalyst 系列交换机都能够以折叠核心层和分布层角色部署，以在第 2 层和第 3 层网络边界之间提供分界。

本文档不重点介绍用于分布层系统的这种部署模式。

虚拟交换系统恢复能力

虚拟交换域和最佳实践

域 ID 最佳实践

定义 VSS 域标识符 (ID) 是实施带两个单机物理机箱的 VSS 的预迁移第一步。VSS 域 ID 的值范围是 1 到 255。虚拟交换机域 (VSD) 包括两个物理交换机，必须用通用的域 ID 配置它们。

作为一种最佳实践，当在多层园区网络设计中实施 VSS 时，不同 VSS 对之间使用唯一域 ID 可以防止出现网络协议冲突，同时也能简化网络操作、故障排除和管理。

图 6. VSS 域 ID 最佳实践

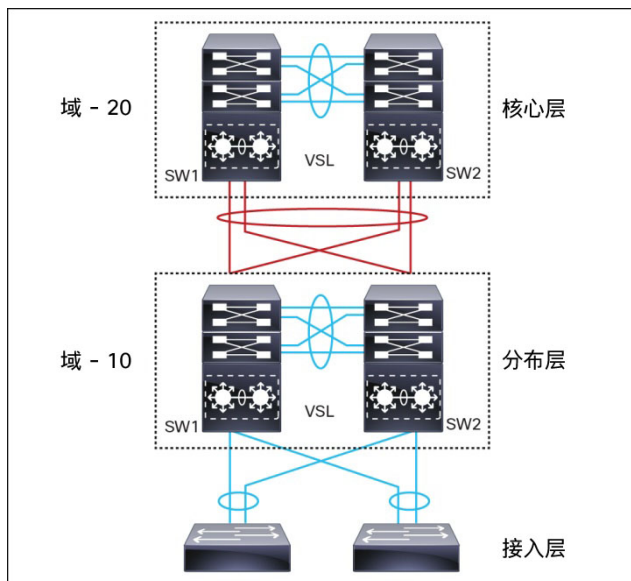


表 8. VSS 交换域和 ID 最佳实践

Cisco Catalyst 6800: SW1	Cisco Catalyst 6800: SW2
分布层: SW1 Dist-1(config)#switch virtual domain 10 Dist-1(config-vs-domain)#switch 1	分布层: SW2 Dist-2(config)#switch virtual domain 10 Dist-2(config-vs-domain)#switch 2
核心层: SW1 Dist-1(config)#switch virtual domain 20 Dist-1(config-vs-domain)#switch 1	核心层: SW2 Dist-2(config)#switch virtual domain 20 Dist-2(config-vs-domain)#switch 2

VSS 交换机优先级最佳实践

当两台交换机启动时，会协商交换机优先级，以确定虚拟交换机的控制平面所有权。优先级较高的虚拟交换机拥有控制平面的所有权，而优先级较低的交换机以冗余模式启动。默认交换机优先级是 100；当两个虚拟交换机节点均采用默认设置部署时，将以交换机 ID 较低者为准。

作为一种最佳实践，为了充分利用采用集中式控制和管理平面的分布式转发架构，建议使用相同的硬件和软件部署两个虚拟交换机节点。每个虚拟交换机节点上的控制平面操作都相同。

因此，修改默认交换机优先级是可选的设置，可以保留默认值，因为每个虚拟交换机节点都可以为网络 and 用户提供透明操作。

路由 MAC 最佳实践

当热备份交换机成为活动交换机时，在状态切换事件中，接口的 MAC 地址分配不会发生变化。但是，如果两个机箱同时重新启动，活动交换机的顺序就会发生变化（旧的热备份交换机会首先成为活动交换机），则整个 VSS 域会使用该交换机的 MAC 地址池。在网络通信过程中，不支持免费 ARP 的任何互联设备都会受到影响，直到默认网关/接口的 MAC 地址刷新或超时。

为了避免此类影响，思科建议使用 VSS 提供的配置选项，在这种情况下，第 2 层和第 3 层接口的 MAC 地址来自预留的地址池。这样就可以利用虚拟交换机域标识符来生成 MAC 地址。无论启动顺序如何，VSS 域的 MAC 地址与虚拟 MAC 地址的使用方式一致。

作为一种最佳实践，建议在 VSS 迁移过程中实施路由 MAC，以免系统重复启动。如果已经在没有路由 MAC 地址的情况下实施了 VSS，则应计划停机时间，以在下次重新启动时采用新的虚拟 MAC 地址。

表 9. VSS 路由 MAC 最佳实践

Cisco Catalyst 6800: SW1	Cisco Catalyst 6800: SW2
分布层: SW1 Dist-1(config)#switch virtual domain 10 Dist-1(config-vs-domain)#mac-address use-virtual	分布层: SW2 Dist-2(config)#switch virtual domain 10 Dist-2(config-vs-domain)#mac-address use-virtual

备用机箱恢复最佳实践

虚拟交换机中的活动管理引擎会定期将动态转发信息更新到对等的热备份管理引擎模块以及本地和远程分布式转发卡 (DFC) 线卡，以提供完整的分布式转发功能。

通过这种活动同步，可快速状态切换到替代互联路径，这有助于保护用户和应用体验，同时系统可以执行恢复程序。故障设备可以恢复使用，在重新初始化状态中，模块和端口变为运行状态，然后再从当前活动交换机中重新同步实际转发信息。

重新加入的虚拟交换机处于部分运行状态，这会吸引对等设备的数据平面，同时转发信息仍然处于待定状态。因此，在网络级别上，它会在系统恢复过程中造成比实际系统损失更大的数据丢失。

作为一种最佳实践，思科建议在备用机箱端口上实施一个延迟计时器，使其在启动时变为运行状态。采用这个建议之后，备用机箱将有足够的时间，首先从活动交换机同步转发表，然后提供来自对等设备的用户数据。

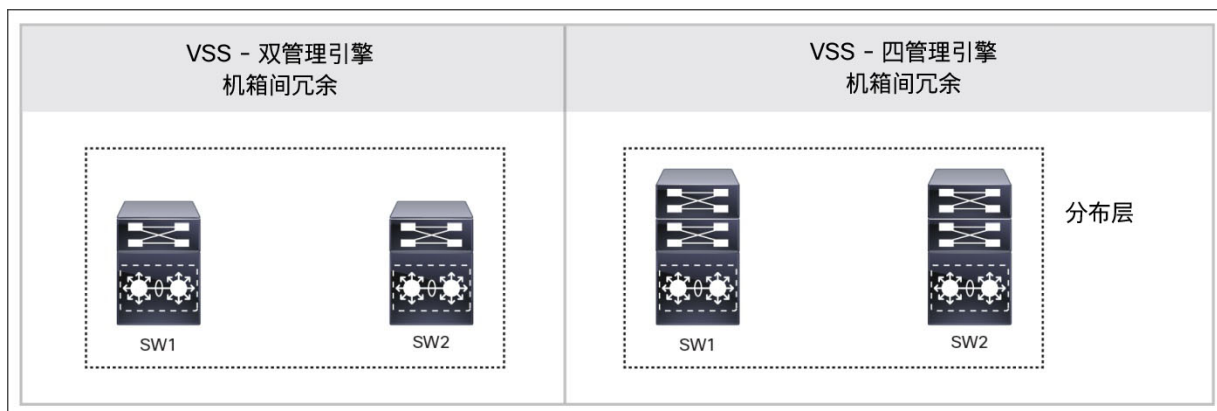
表 10. VSS 路由 MAC 最佳实践

最佳实践	Cisco Catalyst 6800: VSS
将备用延迟计时器配置为 300 秒	<pre>Dist(config)#switch virtual domain 10 Dist(config-vs-domain)#standby port delay 300 Dist(config-vs-domain)#standby port bringup 1 2</pre>

虚拟交换管理引擎高可用性最佳实践

Cisco VSS 技术采用经过充分验证的 SSO 技术提供管理引擎模块冗余，从而延伸到单个系统之外。Cisco Catalyst 6800 系列 VSS 系统中的新一代管理引擎 2T 支持多维冗余，可防止管理引擎模块和机箱发生重置或故障。图 7 显示了用于建立简单且具有恢复能力的分布层网络的两种管理引擎冗余方案。

图 7. 双管理引擎和四管理引擎冗余



- 双管理引擎冗余模式：**这种部署模式是在每个 Cisco Catalyst 6807-XL 模块化系统上部署单个管理引擎 2T 模块。该系统仅限于机箱间 SSO 冗余，可为所有双宿主互联设备提供不间断的通信。在任意虚拟交换机系统上重置的管理引擎需要完成机箱重置，包括引起性能下降一半和恢复时间增加的网络模块，具体取决于重置起因、故障类型等因素。

出于系统架构原因，处于 VSS 模式的固定配置 Cisco Catalyst 6880X 只能支持这种冗余模式。

- 四管理引擎冗余模式：**这种部署模式适用于两个 6807-XL 系统，每个系统以 VSS 模式部署两个管理引擎 2T 模块。一共四个管理引擎 2T 模块，系统级冗余翻了两番，可在计划内和计划外网络故障期间保护网络可用性和容量。这种冗余模式还为直接连接到 Cisco Catalyst 6807-XL VSS 系统的所有单宿主网络设备提供冗余。

作为一种最佳实践，当业务和技术要求需要具有恢复能力的一流基础设施，以在计划内或计划外网络故障期间支持网络可用性和容量时，建议采用四管理引擎冗余模式。

虚拟交换链路设计和最佳实践

要将两个物理机箱整合为一个逻辑实体，借助 Cisco VSS 技术可将不同类型的单机箱内部系统组件扩展到多机箱级别。必须使用直接物理链路部署每个虚拟交换机，直接物理链路可以延伸背板通信边界（称为虚拟交换机链路 [VSL]）。VSL 可以视为两个虚拟交换机节点之间的第 1 层物理链路，无需使用网络控制协议即可运行。因此，VSL 无法建立网络协议邻接，在建立网络拓扑表时将被排除。

VSL 物理链路连接最佳实践

Cisco Catalyst 6807-XL 或 6880X 在任何受支持的 10G 或 40G 网络模块上支持 VSL 功能。在两个系统之间部署 VSL 物理连接时，必须注意确保其达到最佳的冗余级别，以应对各种各样的外部或内部故障条件。作为一种最佳实践，思科建议在管理引擎 2T 和网络模块之间平均分散 VSL 光纤连接。图 8 显示了当 Cisco Catalyst 6800 系列系统以 VSS 模式部署时的 VSL 连接最佳实践。

图 8. Cisco VSS VSL 最佳实践



VSL 容量规划最佳实践

当虚拟交换机找不到用来交换流量的本地转发路径时，Cisco VSS 最后选择通过 VSL 转发用户数据平面。为了尽量减少 VSL 接口上的拥塞，作为一种最佳实践，网络管理员还必须考虑 VSL 容量规划。容量规划应确保 VSL 接口具有充足的汇聚带宽，以在主要本地路径发生故障时重新路由用户数据平面。在计算所需的 VSL 带宽容量时，必须考虑以下四个主要因素：

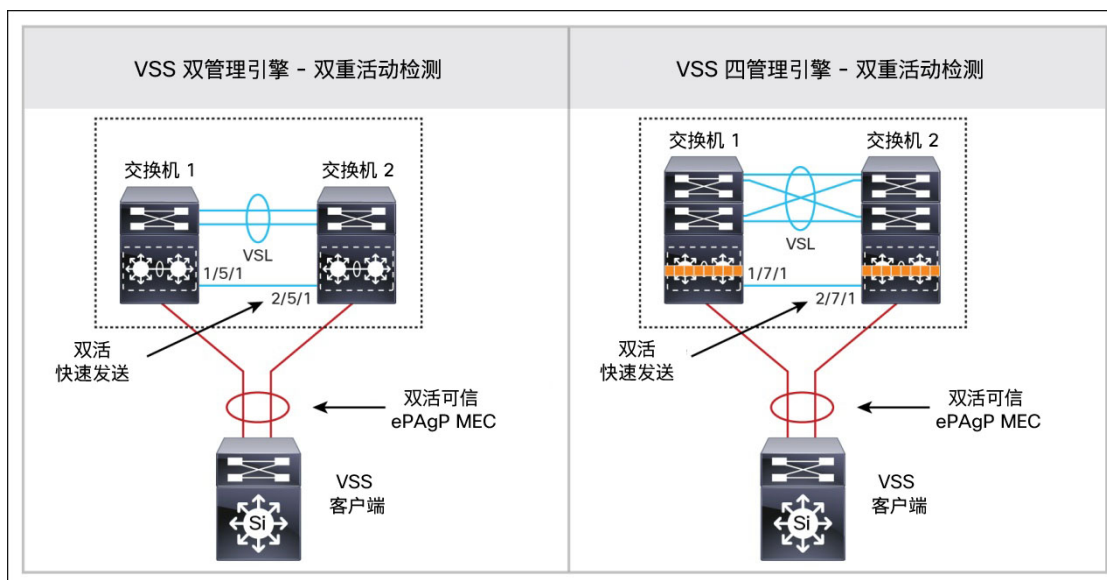
- 每个虚拟交换机节点上的汇聚网络上行链路带宽容量（例如 2 x 10GE）分散到同一个远程核心系统。
- 设计采用单宿主设备连接的网络（无多机箱 EtherChannel [MEC]）。不建议采用单宿主网络设备连接。
- 远程交换端口分析器 (SPAN) 从一个交换机成员到另一个虚拟交换机系统。
- 如果 6807-XL 系统使用集成服务模块（即 ASA-SM、WiSM2 等等）部署，则根据服务模块转发设计和容量，可以通过 VSL 捆绑包传输用户数据。

最大 VSL EtherChannel 接口最多可以传输 8 个 10G/40G 端口。为了实现 VSL 成员链路之间的最优流量负载共享，建议以 2 的幂（即 2、4、8）捆绑 VSL 成员链路。

VSL 冗余最佳实践

VSL EtherChannel 可以作为一个可扩展的背板链路，通过传输机箱间控制流量、网络控制平面和用户数据流量，可实现系统虚拟化。统一控制平面协议和分布式转发条目的状态机可在两个虚拟交换机节点之间动态同步。VSL 组件上触发的任何故障都会中断系统虚拟化，并使网络出现双活状态。图 9 显示了在网络和终端用户应用受到影响之前检测此类故障状态并快速恢复系统的两种技术。

图 9. 双活检测最佳实践



- 双活快速发送最佳实践：
 - 在进行双活快速发送检测时，最多可以使用四个任意链路类型和速度的端口进行配对。建议至少使用一个端口。
 - 管理引擎和网络模块端口上均支持双活快速发送。对于双管理引擎网络设计，可以使用板载管理引擎 1G 端口实现快速发送。对于四管理引擎网络设计，应选择网络模块中的其中一个可用端口，以在任意一个管理引擎模块出现故障时获得更有效的冗余。
 - 双活快速发送可以与增强型端口汇聚协议 (ePAGP) 共存。建议同时实施两种机制，以获得更有效的冗余。

表 11. 实施双活快速发送

Cisco Catalyst 6800: VSS
Dist(config)#interface range Gig 1/3/1, Gi2/3/1
Dist(config-if-range)#dual-active fast-hello

- 增强型 PAgP+ 最佳实践：
 - 双重活动检测方法中可使用许多第 2 层或第 3 层支持 PAgP 的 EtherChannel。为了实现更有效的冗余，建议至少使用两个双活可信 MEC。
 - 可信第 2 层 MEC 可以是接入层交换机。第 3 层 MEC 可以是核心层交换机。两者可以共存，建议同时使用两者。
 - 在第 2 层或第 3 层上启用或禁用双活信任设置要求接口处于管理性关闭状态。因此，作为一种最佳实践，建议规划一个短期停机来实施解决方案。

表 12. PAgP MEC 上的 VSS 双活信任最佳实践

Cisco Catalyst 6800: VSS	双活 PAgP VSS 客户端
Dist(config)#interface range Port-Channel 101-102 Dist(config-if-range)#shutdown	无需配置
Dist(config)#switch virtual domain 1 Dist(config-if-range)#dual-active detection pagp trust channel-group 101 Dist(config-if-range)#dual-active detection pagp trust channel-group 102	
Dist(config)#interface range Port-Channel 101-102 Dist(config-if-range)#no shutdown	

• 双活排除最佳实践:

- 在双活状态下，恢复机箱会自动禁用所有端口，以防网络出现故障。作为一种最佳实践，建议从每个虚拟交换机机箱中排除第 3 层带外管理端口，以在故障排除和调试期间保持运行。
- 从管理引擎和网络模块可以使用任意管理端口。对于双管理引擎网络设计，可以使用板载管理引擎 1G 端口。对于四管理引擎网络设计，应选择网络模块中的其中一个可用端口，以在任意一个管理引擎模块出现故障时获得更有效的冗余。
- 必须能通过单独的第 2 层/第 3 层网络基础设施访问排除的这些管理端口，而不是从核心路由空间。
- 要连接本地子网之外的网络，需要使用来自每个第 3 层排除接口的静态路由。

表 13. VSS 双活信任排除接口最佳实践

Cisco Catalyst 6800: VSS
Dist(config)#interface Gig1/3/2 Dist(config-if)#ipaddress <address><mask> Dist(config-if)#no shutdown
Dist(config)#interface Gig2/3/2 Dist(config-if)#ip address <address><mask> Dist(config-if)#no shutdown
Dist(config)#switch virtual domain 1 Dist(config-if-range)#dual-active exclude interface Gi1/3/2 Dist(config-if-range)#dual-active exclude interface Gi2/3/2
Dist(config)#ip route <network><mask><gateway-1> Dist(config)#ip route <network><mask><gateway-2>

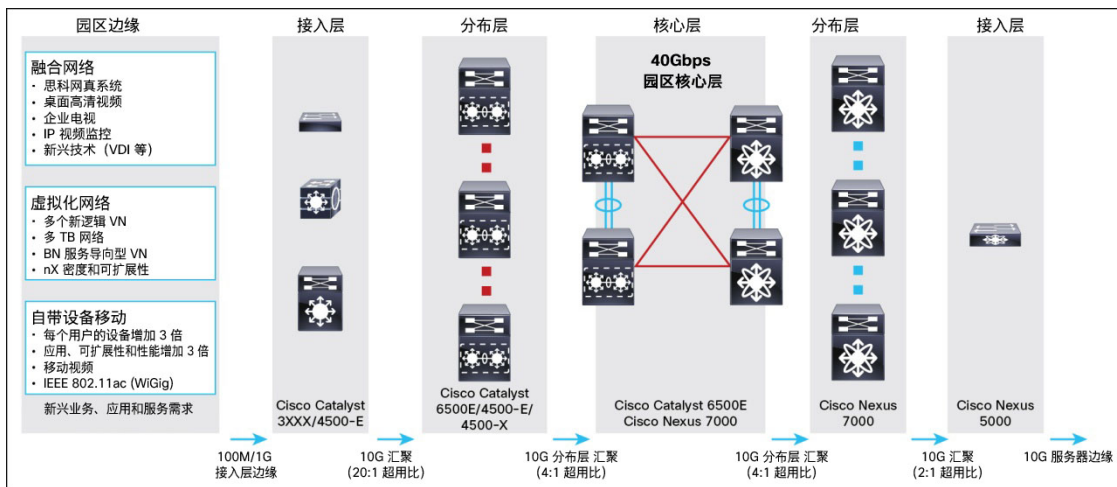
系统和网络连接最佳实践

园区网络超订用最佳实践

交换性能需求可与每个网络层的扩展因素结合考虑。大多数多层架构的大型企业园区网络处于超订用状态。边缘网络扩展通常需要刷新园区核心交换容量，但是要在新一代配线间网络中使用 10G 维持超用比，难度逐渐加大。由于以下几个原因，高速交换容量需求逐渐加大：1G 桌面等新设备、无线 802.11AC、视频、移动设备激增等等。为了随着可扩展性和性能需求增加维持一致的体验质量 (QoE)，IT 部门需要重新评估园区网络中的两个主要瓶颈点。这些瓶颈在于园区分布层，可汇聚 10G 物理连接和核心交换容量来维持 4:1 的超用比。

作为一种最佳实践，为了降低园区和数据中心核心可扩展性和性能挑战，并保护 4:1 的超用比，可利用 Cisco Catalyst 6800-E 和 Cisco Nexus® 7000 系统中的 40G 以太网创新，轻松顺畅地从现有的 10G 核心基础设施升级。分布层应在分布-接入网络中维持 20:1 的超用比。如果中间分配框 (IDF) 中的接入层交换机的容量增加十倍，则网络架构师必须确保汇聚交换机、模块和端口能够达到所需性能。在模块化分布层设计中，领先的 Cisco Catalyst 6800 系列系统可与带有 Cisco Catalyst 6904 或 6816 线卡模块的新一代管理引擎 2T 一起部署，从而实现 10G 端口汇聚。

图 10. 网络超订用最佳实践



接入层网络连接最佳实践

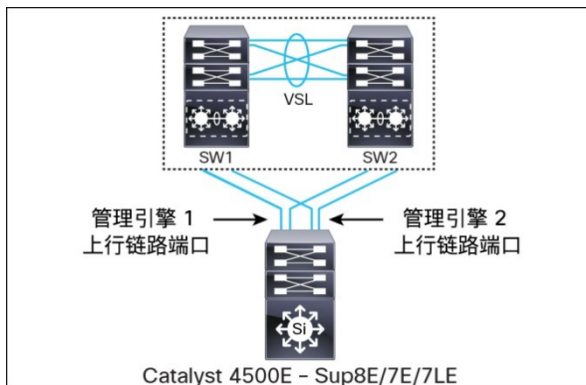
为了优化应用性能和网络恢复能力，采用从各种接入层模式交换机到分布层系统的上行链路网络连接设计至关重要。这种最佳实践可确保用户数据平面充分实现负载均衡，以优化所有系统资源的利用率，同时可确保网络协议构建冗余转发路径，以在各种计划内和计划外网络故障期间快速实现状态切换。

Cisco Catalyst 4500-E 冗余管理引擎上行链路建议

在冗余模式中，Cisco Catalyst 4507R+E 或 4510R+E 机箱在冗余 SSO 配置中部署双管理引擎 8-E 或 7-E 模块。每个管理引擎模块上有四个 1G/10G 上行链路端口，分为两个端口组：端口组 1（端口 1 和 2）和端口组 2（端口 3 和 4）。当 Cisco Catalyst 4500E 系统检测到机箱中安装了冗余模块时，两个管理引擎模块上的端口组 2 都会自动变为非活动状态。

如图 11 所示，作为一种最佳实践，可将两个管理引擎上的四个上行链路端口全部用于冗余的 Cisco Catalyst 6800 系列分布层 VSS 系统。两个管理引擎模块可与冗余上游系统平均分散端口组 1，以实现与非冗余模式相同的一致带宽容量、负载均衡和链路冗余。

图 11. 4500-E 冗余管理引擎上行链路建议



Cisco StackWise 和 FlexStack 上行链路建议

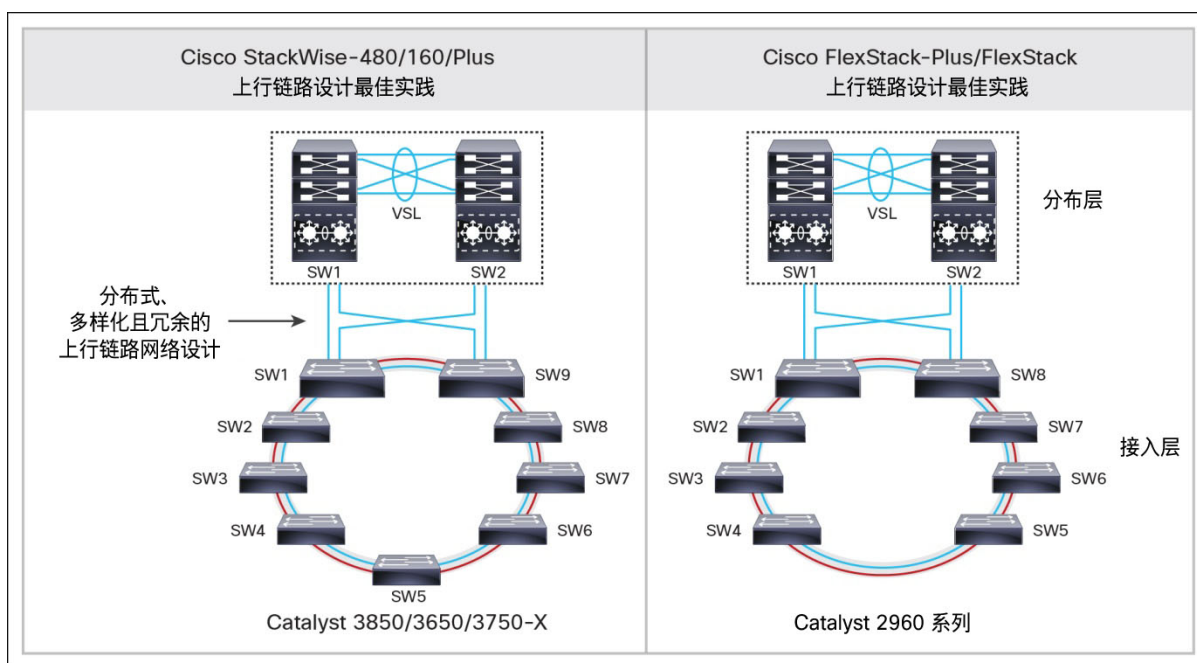
Cisco Catalyst 3850/3650、3750-X 和 2960 系列交换机最多支持用 4 个物理上行链路端口连接分布层交换机。为了在配线间实现最佳负载均衡和冗余，通常最多从接入层交换机部署 2 个物理上行链路接口。

当以堆栈配置模式部署这些交换机时，建议遵循与双堆栈成员系统相同的上行链路连接设计原则。例如，一个堆栈环中部署的 9 个 Cisco Catalyst 3850 交换机中，会有来自交换机 1 的 2 个不同上行链路端口和来自交换机 9 的 2 个不同上行链路端口。其余 7 个交换机会使用高速堆栈背板向核心层转发数据。

从应用性能到最优用户体验，建议的这种上行链路端口设计具有诸多优势：

- 利用堆栈成员 Cisco Catalyst 交换机之间的多个分布式高速 10Gbps 上行链路增加汇聚堆栈交换容量，从而提高应用性能
- 利用堆栈环内部及所有分布式上行链路物理端口之间的智能网络数据负载共享，加强双向流量工程
- 利用硬件资源的分布式转发架构优势提高系统和应用性能：缓冲区、队列、三重内容可寻址存储器 (TCAM) 等等
- 保护堆栈和网络级冗余，并尽量减少接入层或分布层重大故障引起的分布式汇聚系统拥塞。

图 12. Cisco StackWise 和 FlexStack 上行链路建议



Cisco StackWise 和 FlexStack 交换机优先级建议

思科在每一代交换产品组合上推出了一代又一代 StackWise 和 FlexStack 技术。每一代新技术都提供了各种高级功能，不仅优化了可扩展性、性能和恢复能力，也保持了用户和网络的简便性。

通过将所有堆栈成员交换机的控制和管理平面集中到堆栈环中动态选举的单个交换机，提高了堆栈技术的简便性。通过构建完整的分布式转发架构优化堆栈背板和所有不同系统资源（例如上行链路光纤端口、TCAM 等等）的利用率，优化了交换性能。

作为一种最佳实践，必须分离 StackWise 和 FlexStack 交换机中的控制和管理平面操作与上行链路端口操作。为每个堆栈成员交换机静态分配交换机 ID，即可达到这一目的。优先级较高的交换机会选举为堆栈环中的活动/主交换机角色。为了快速完成重新选举，可以使用下一级优先级预先设置辅助交换机。这项最佳实践可以在堆栈中的活动/主交换机发生故障时减少网络重新收敛的时间。

图 13. Cisco StackWise 和 FlexStack 交换机优先级建议

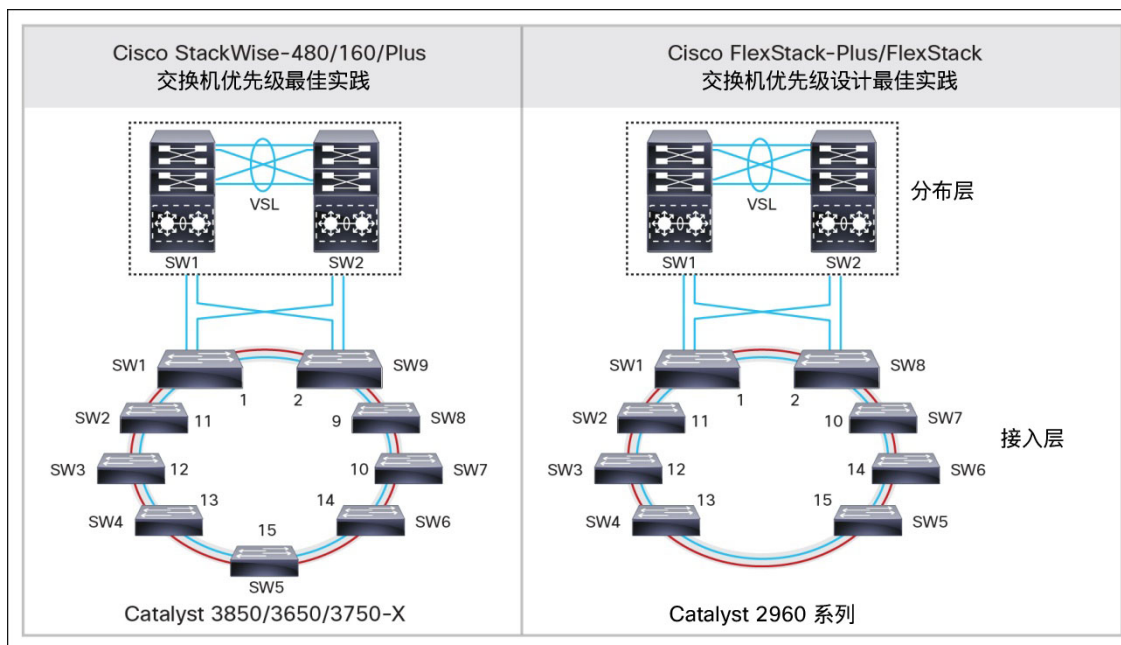


表 14 提供了在 Cisco Catalyst 3850/3650、3750-X 和 2960 系列交换机上静态配置交换机优先级的最佳实践配置。

表 14. Cisco StackWise 交换机优先级最佳实践

Cisco Catalyst StackWise 和 FlexStack 交换机	Cisco StackWise 和 FlexStack 交换机优先级
<pre>3850-Stack#switch 1 priority 1 !Switch 1 with Uplink ports 3850-Stack#switch 2 priority 11 3850-Stack#switch 3 priority 12 3850-Stack#switch 4 priority 13 3850-Stack#switch 5 priority 15 3850-Stack#switch 6 priority 14 3850-Stack#switch 7 priority 10 3850-Stack#switch 8 priority 9 3850-Stack#switch 9 priority 2 ! Switch 9 with Uplink ports</pre>	<pre>3750X-Stack#config terminal 3750X-Stack(config)#switch 1 priority 1 ! Switch 1 with Uplink ports 3750X-Stack(config)#switch 2 priority 11 3750X-Stack(config)#switch 3 priority 12 3750X-Stack(config)#switch 4 priority 13 3750X-Stack(config)#switch 5 priority 15 3750X-Stack(config)#switch 6 priority 14 3750X-Stack(config)#switch 7 priority 10 3750X-Stack(config)#switch 8 priority 9 3750X-Stack(config)#switch 9 priority 2 ! Switch 9 with Uplink ports</pre>

表 15. Cisco FlexStack 交换机优先级最佳实践

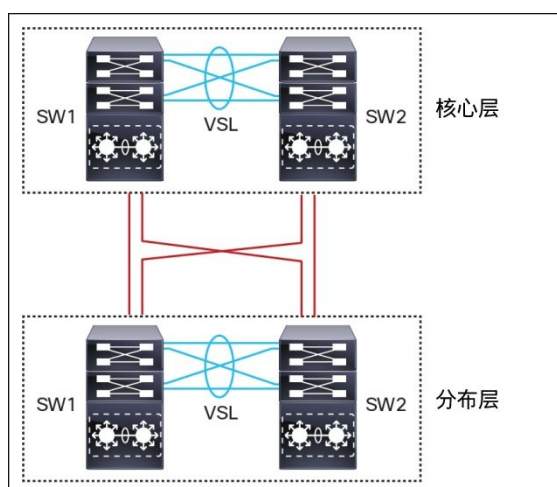
Cisco Catalyst StackWise 和 FlexStack 交换机	Cisco StackWise 和 FlexStack 交换机优先级
<pre>2960XR-Flex#config terminal 2960XR-Flex(config)#switch 1 priority 1 ! Switch 1 with Uplink ports 2960XR-Flex(config)#switch 2 priority 11 2960XR-Flex(config)#switch 3 priority 12 2960XR-Flex(config)#switch 4 priority 13 2960XR-Flex(config)#switch 5 priority 15 2960XR-Flex(config)#switch 6 priority 14 2960XR-Flex(config)#switch 7 priority 10 2960XR-Flex(config)#switch 8 priority 2 ! Switch 8 with Uplink ports</pre>	<pre>2960S-Flex#config terminal 2960S-Flex(config)#switch 1 priority 1 ! Switch 1 with Uplink ports 2960S-Flex(config)#switch 2 priority 14 2960S-Flex(config)#switch 3 priority 15 2960S-Flex(config)#switch 4 priority 2 ! Switch 4 with Uplink ports</pre>

分布层网络连接最佳实践

园区分布层和核心层系统通常具有模块化硬件，在管理引擎模块上完成集中式处理，在高速网络模块上完成分布式转发。使用多样化、分布式且冗余的物理路径构建具有恢复能力的园区网络设计的基础不会随着角色、系统或部署的配置模式而变化。每个分布层到核心层的物理上行链路连接可以使用单个或两个上行链路第 3 层接口。单个链路可构建方形物理拓扑，而这种拓扑不具有最佳的负载均衡和冗余。由于在计划内系统或网络级故障期间，网络恢复速度较慢，它还会影响应用性能。

遵循通用的物理层网络设计原则，作为一种最佳实践，思科建议在所有网络层部署全网状冗余物理连接，如图 14 所示。

图 14. 全网状分布层与核心层连接最佳实践



思科多机箱第 2 层 EtherChannel 最佳实践

传统的园区网络采用单机网络系统和等价多路径 (ECMP)，无法灵活地使用冗余设备或路径充当单个逻辑实体，从而简化网络设计。利用 Cisco Catalyst 交换平台上的思科系统虚拟化创新，例如 VSS、StackWise 和 FlexStack，园区网络设计不断演变，三个层上均可重新设计。以上每种虚拟化技术都能将多个物理系统整合到单个大型且统一的逻辑系统，多个分布式的并行物理路径现在可以捆绑到两个系统之间的逻辑点对点 EtherChannel 接口。当园区设备或链路需要以逻辑模式运行时，构建全网状物理园区网络的原则应保持不变。

采用 EtherChannel 在两个系统之间设计多层或园区主干网络具有多种优势：

- **简化：**将多个 ECMP 路径捆绑为逻辑 EtherChannel 可减少冗余协议邻接、路由数据库和转发路径。
- **优化：**减少控制平面操作数量并优化系统资源，例如 CPU/内存利用率。提供灵活的第 2 层到第 4 层变量，以跨每个捆绑接口智能共享负载，并利用所有资源传输网络数据流量。
- **降低复杂性：**简化网络操作实践并减少分析和调试问题所需的网络配置和故障排除。
- **增加容量：**在所有捆绑的第 2 层上行链路上利用所有资源（带宽、队列、缓冲区等等），减少多层设计中的协议驱动限制并使交换容量加倍。
- **提供恢复能力：**提供确定性的硬件驱动网络恢复，以实现无缝的业务运营。在最小的网络故障期间将路由数据库重新计算和拓扑更改降至最低，例如链路故障。

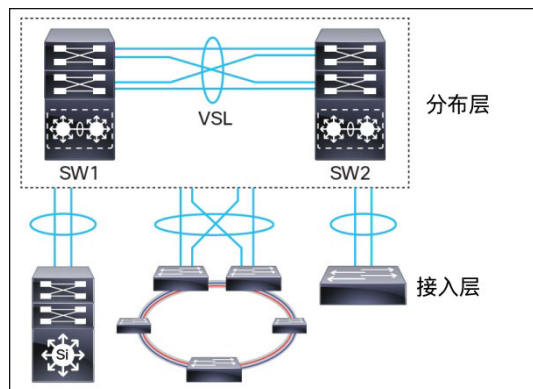
多机箱 EtherChannel 最佳实践

Cisco MEC 技术是一项突破性的创新，可跨多个物理交换机创建逻辑点对点 EtherChannel，从而在 VSS 域中提供具有高度恢复能力的虚拟交换机。利用 VSS 部署第 2 层或第 3 层 MEC 具有以下优势：

- 除了所有 EtherChannel 优势，MEC 中的分布式转发架构还可帮助增加网络带宽容量。
- 与传统 EtherChannel 技术相比，可消除单点故障，从而提高网络可靠性。
- 在单个逻辑捆绑接口中简化网络控制平面、拓扑和系统资源，而不使用多个单独的并行物理路径。
- 除了网络可扩展性以外，MEC 还提供基于硬件的亚秒级网络恢复。
- 在 VSS 模式的 Cisco Catalyst 6800 系列系统上，MEC 技术对远程对等设备保持透明。

思科建议在设计园区网络时，尽可能地在所有层上将并行路径捆绑为逻辑 EtherChannel 或 MEC。如果任何设备无法以逻辑方式捆绑接口，例如单机园区核心层系统，则可采用混合 EtherChannel 和 ECMP 网络设计部署园区网络。图 15 显示了建议的端到端 EtherChannel/MEC 网络设计，这种设计可简化端到端网络操作。

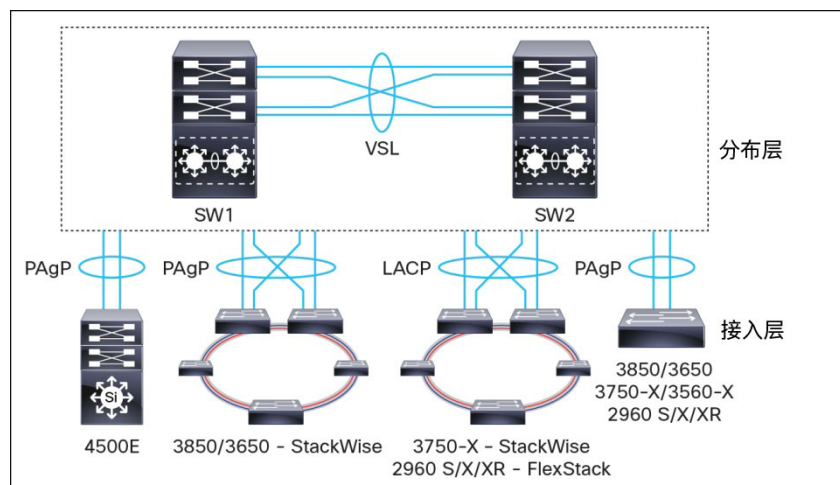
图 15. 多机箱 EtherChannel 建议



思科增强型 PAgP 和 LACP 最佳实践

EtherChannel 采用链路捆绑协议，利用每端口信令机制在本地物理端口和远程系统上进行各种参数检查。EtherChannel 的成员链路必须使用思科增强型 PAgP 或行业标准 IEEE 链路汇聚控制协议 (LACP) 端口汇聚协议，加入端口通道接口。如图 16 所示，建议将分布块或核心层中实施的 EtherChannel 与增强型 PAgP 或 LACP 一起实施。

图 16. 思科增强型 PAgP 和 LACP 建议



两种协议都可提供一致的链路功能；但是思科增强型 PAgP 协议还具有一个解决方案优势，即双重活动检测。实施这些协议可获得以下附加优势：

- 确保两个系统之间的链路汇聚参数一致性和兼容性。
- 确保符合汇聚要求。
- 动态响应本地和远程 EtherChannel 系统上的运行时更改和故障。
- 检测并删除 EtherChannel 捆绑包中的单向链路和多点以太网连接。

所有 Cisco Catalyst 交换平台支持思科增强型 PAgP 和行业标准 LACP 协议。表 16 显示了基于软件功能在两个系统之间配置思科增强型 PAgP 和 LACP 协议的配置指南。

表 16. Cisco Catalyst 增强型 PAgP 和 LACP 最佳实践

建议协议	分布层交换机	接入层交换机
增强型 PAgP	Cisco Catalyst 6800 VSS interface range <id> - <id> channel-protocol pagp channel-group <id> desirable !	Cisco Catalyst 4K/3K/2K interface range <id> - <id> channel-protocol pagp channel-group <id> desirable !
IEEE LACP	Cisco Catalyst 6800 VSS interface range <id> - <id> channel-protocol lacp channel-group <id> active !	Cisco Catalyst 3750-X Stack interface range <id> - <id> channel-protocol lacp channel-group <id> active !
	Cisco Catalyst 6800 VSS interface range <id> - <id> channel-protocol lacp channel-group <id> active !	Cisco Catalyst 2960 Series FlexStack interface range <id> - <id> channel-protocol lacp channel-group <id> active !

静态 EtherChannel 最佳实践

目前，大多数新一代思科或其他供应商的网络设备都支持使用增强型 PAgP 或 IEEE LACP 来实现动态 EtherChannel 链路捆绑。但是，某些系统类型（例如 Cisco ISR、Cisco 5508 WLC 等等）支持静态或非协商配置模式的 EtherChannel 功能，而不是支持动态模式。静态模式的 EtherChannel 不提供成员链路配置、参数和功能一致性方面的错误检测，但是它们可以像动态 EtherChannel 一样提供负载均衡和冗余。

作为一种最佳实践，思科建议检查此类设备的更新软件版本和最新 EtherChannel 功能，以确定是否支持 PAgP 或 LACP。如果支持，则建议使用动态模式，不要使用静态模式。如果不支持，则必须仔细评估接口每一端的静态模式 EtherChannel 配置，确保链路类型、配置及其功能保持一致，以在 EtherChannel 中的成员链路之间实现最高水平的负载共享。

表 17. 静态 EtherChannel 最佳实践

建议协议	分布层交换机	远程 EtherChannel 设备
静态	Cisco Catalyst 6800 VSS interface range <sw1-id> - <sw2-id> channel-group <id> on !	远程设备 interface range <id> - <id> channel-group <id> on ! 远程设备上的静态 EtherChannel 配置取决于操作系统/CLI 支持

EtherChannel 负载均衡

企业园区网络设计中的应用数量及其功能千差万别，尤其是当网络作为业务运营、园区安全和开放可访问性的通用平台时。必须提高网络的智能感知能力，使用数据链路进行传输层数据包检测，并使用负载共享流量优化所有可用网络资源的利用率。

微调 EtherChannel 和 MEC 接口可为网络增添额外的计算智能，在多个本地成员链路路径之间做出协议感知出口转发决策。对于每个流量，微调之后可以利用来自源主机的多级变量信息（即从第 2 层到第 4 层）优化出口路径选择过程。EtherChannel 负载均衡方法取决于 Cisco Catalyst 交换和路由平台。图 17 显示了建议的端到端 EtherChannel 负载均衡方法。

图 17. EtherChannel 负载均衡最佳实践

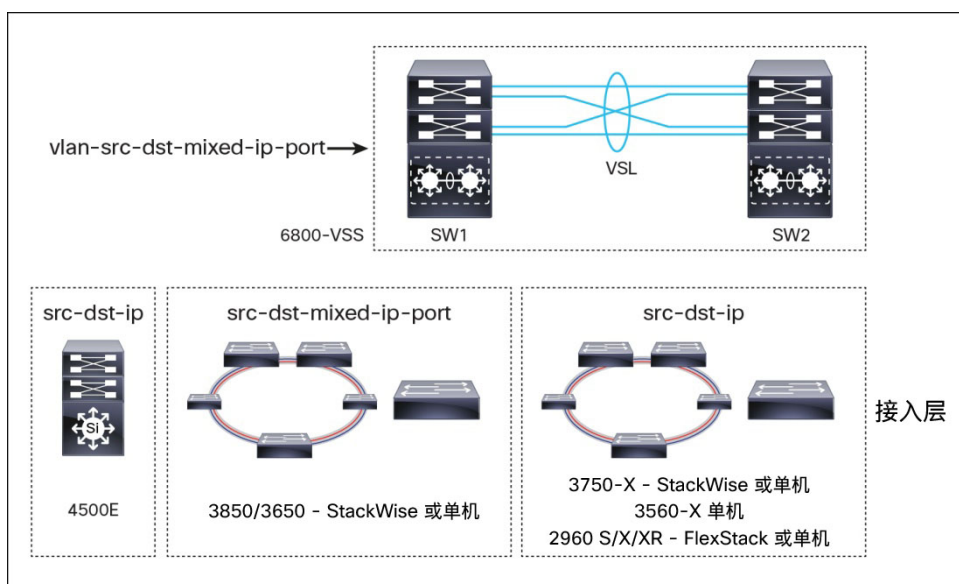


表 18. EtherChannel 负载均衡最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#port-channel load-balance vlan-src-dst-mixed-ip-port
接入层	Cisco Catalyst 4500E 4500E(config)#port-channel load-balance src-dst-ip
	Cisco Catalyst 3850/3650 3850(config)#port-channel load-balance src-dst-mixed-ip-port
	Cisco Catalyst 3750-X/3560-X 3750(config)#port-channel load-balance src-dst-ip
	Cisco Catalyst 2960 S/X/XR 2960(config)#port-channel load-balance src-dst-ip

园区多层网络设计最佳实践

多层 VLAN 网络设计建议

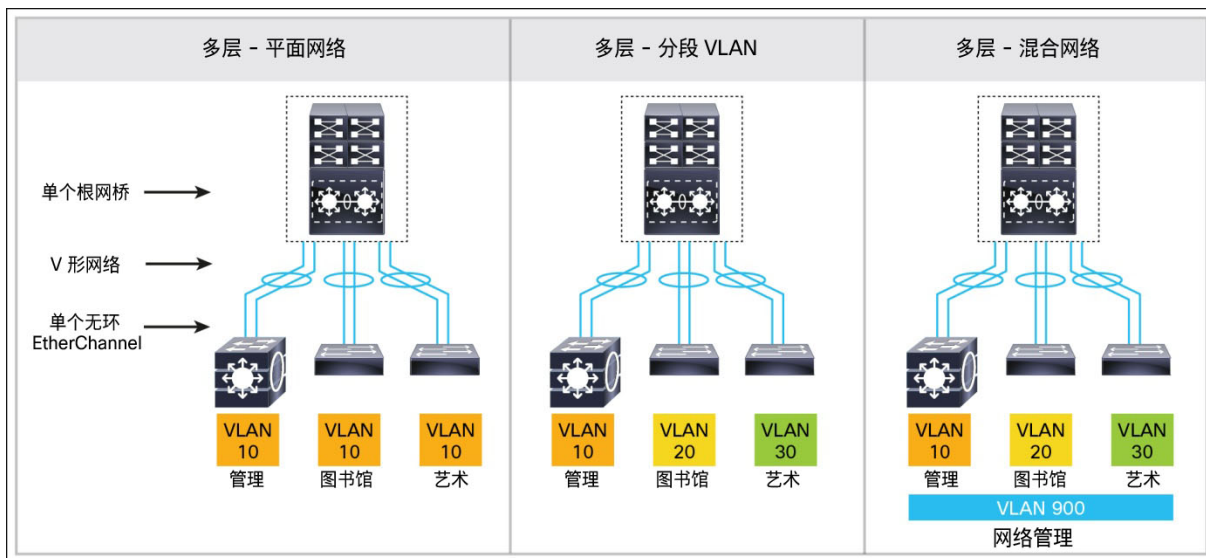
多层网络是传统、简单且广泛部署的场景，与网络规模无关。园区网络边缘的接入层交换机与各种端点连接，可提供智能的第 1 层/第 2 层服务。接入层交换机使用第 2 层中继互联分布层交换机，并依靠分布层汇聚交换机执行智能第 3 层转发，以及设置策略和访问控制。

设计多层网络可以采用三种设计变体；必须在 V 形物理网络设计中部署所有变体，并且必须提供无环路拓扑：

- **平面：**某些应用和用户访问类型要求广播域设计涵盖多个配线间交换机。采用多层网络设计，可灵活地构建采用扩展星形拓扑的单个大型广播域。
灵活性带来了可扩展性、性能和安全挑战，可能需要特别注意防止网络出现错误配置和错误接线，否则可能导致生成树环路和降低网络稳定性。
- **分段：**为不同的组织部门和企业业务智能分段提供唯一的 VLAN，建立每个部门的逻辑网络。不同企业和管理组之间的所有网络通信通过分布层定义的路由和转发策略进行传递。
- **混合：**混合逻辑网络设计可将未跨越不同接入层交换机的 VLAN 工作组分段，同时允许某些 VLAN（例如网络管理 VLAN）跨越接入层-分布层块。混合网络设计支持第 2 层平面通信而不会影响网络，还可帮助减少使用的子网数量。

图 18 显示了多层网络的三种独特 VLAN 设计变体。

图 18. 园区多层 VLAN 网络设计方案



作为一种最佳实践，建议混合多层接入层-分布层块设计提供广播域和故障域较小的无环路网络拓扑，同时有限的 VLAN 跨越简化操作所需的所有接入交换机，例如设备管理 VLAN。

多层网络协议最佳实践

传统多层网络由多个协议构成，在企业园区或分支机构网络中构建可扩展的高性能汇聚块。每个网络协议都专门用于建立动态寻址、最佳转发表或高可用性，为任务关键型网络提供恢复能力。

这个子部分介绍在分布层和接入层部署可靠的第 2 层网络基础设施的最佳实践和部署指南。

VLAN 中继协议建议

VLAN 中继协议 (VTP) 是思科专有第 2 层消息协议，负责在网络范围内添加、删除和重命名 VLAN。Cisco VTP 简化了交换网络中的管理。VTP 可以配置为三种模式：服务器、客户端和透明。

作为一种最佳实践，建议在透明模式下部署 VTP，以提升 VLAN 可控性、安全性和可管理性。

表 19. Cisco VTP 最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#vtp domain <name> 6800-VSS(config)#vtp mode transparent 6800-VSS(config)#vtp version 2 6800-VSS(config)#vtp password <password>
接入层	Cisco Catalyst 4K/3K/2K 4500E(config)#vtp domain <name> 4500E(config)#vtp mode transparent 4500E(config)#vtp version 2 4500E(config)#vtp password <password>

动态中继协议 (DTP) 建议

默认情况下，在所有第 2 层以太网端口上启用思科动态中继协议 (DTP)。Cisco DTP 协议确保交换机在中继任意一端对发送 IEEE 802.1Q 帧的过程中涉及的不同参数（例如配置封装类型、本地 VLAN 和硬件功能）进行了约定。Cisco DTP 还可确保非中继端口及其相邻端口的状态一致，从而帮助防范非中继端口标记帧泛洪（这是一种潜在的严重安全性风险）。

作为一种最佳实践，思科建议在第 2 层中继端口将 DTP 设置保留为默认值。无论对等设备为何种类型，即无论是交换机、路由器、无线 LAN 控制器、防火墙还是其他设备，都应遵行这些建议。

表 20. 思科动态中继协议最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#interface range <sw1-id> - <sw2-id> 6800-VSS(config-if)#switchport 6800-VSS(config-if)#switchport mode trunk 6800-VSS(config-if)#default switchport nonegotiate
接入层	Cisco Catalyst 4K/3K/2K 4500E(config)#interface range <id> - <id> 4500E(config-if)#switchport 4500E(config-if)#switchport mode trunk 4500E(config-if)#default switchport nonegotiate

VLAN 中继设计建议

在典型的园区网络设计中，为单个接入交换机部署多个 VLAN，如数据 VLAN 和语音 VLAN。分布层和接入层设备之间的第 2 层网络连接是中继接口。添加 VLAN 标记，以便在整个中继的 VLAN 之间保持逻辑分离。

建议在静态模式而非协商模式下实施 802.1Q 中继封装，以提供快速的链路建立性能。

中继 VLAN 最佳实践

在端口通道上启用第 2 层中继可自动对接入层和分布层之间的所有活动 VLAN 启用通信。这样可能会对大规模网络造成不良影响，因为接入层交换机可能会接收到本应发给另一接入交换机的泛洪流量。因此，应通过静态允许活动 VLAN 来限制第 2 层中继端口上的流量，确保网络性能高效安全，这一点非常重要。只允许在中继端口上分配的 VLAN 自动筛选其余流量。

表 21. 第 2 层中继最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#interface range <sw1-id> - <sw2-id> 6800-VSS(config-if)#switchport trunk allowed vlan <range>
接入层	Cisco Catalyst 4K/3K/2K 4500E(config)#interface range <id> - <id> 4500E(config-if)#switchport trunk allowed vlan <range>

本地 VLAN 最佳实践

默认情况下，在 Cisco Catalyst 交换机上，每个第 2 层中继端口上的本地 VLAN 都是 VLAN 1，不能禁用或从 VLAN 数据库中删除。本地 VLAN 在所有接入交换机第 2 层端口上都保持活动状态。必须正确配置默认本地 VLAN，以避免多种安全性风险：蠕虫、病毒或数据失窃。源自 VLAN 1 中的任何恶意流量都将横跨接入层网络。借助 VLAN 跳跃攻击，能够对 VLAN 1 之外的系统进行攻击。

作为一种最佳实践，降低这种安全性风险的最好方法就是将未使用的唯一 VLAN ID 实施为接入交换机和分布交换机之间第 2 层中继上的本地 VLAN。例如，在接入交换机 1 和分布交换机上配置 VLAN 801。然后更改两个交换机上的默认本地 VLAN 设置。之后，不得在任何地方出于任何目的在同一接入层-分布层块中使用 VLAN 801。

表 22. 本地 VLAN 最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#interface range <sw1-id> - <sw2-id> 6800-VSS(config)#desc Connected to Access SW-1 6800-VSS(config-if)#switchport trunk native vlan <id-1> 6800-VSS(config)#interfacerange <sw1-id> - <sw2-id> 6800-VSS(config)#desc Connected to Access SW-2 6800-VSS(config-if)#switchport trunk native vlan <id-2>
接入层 (SW1)	Cisco Catalyst 4K/3K/2K 及任何其他设备 4500E(config)#interface range <id> - <id> 4500E(config-if)#switchport trunk native vlan <id-1>
接入层 (SW2)	Cisco Catalyst 4K/3K/2K 及任何其他设备 3850(config)#interface range <id> - <id> 3850(config-if)#switchport trunk native vlan <id-2>

生成树协议建议

生成树协议 (STP) 是第 2 层协议，可防止存在冗余链路的交换网络中产生逻辑环路。无线园区设计在接入层和分布交换机之间使用 EtherChannel 或 MEC (点对点逻辑第 2 层捆绑) 连接，从而简化了 STP 拓扑和操作。在点对点网络设计中，STP 操作在 EtherChannel 逻辑端口而非每个物理端口上进行，因此，将会针对所有分配的 VLAN 在转发状态下自动分配 STP 操作。多年来，STP 协议已发展出以下版本：

- **增强型每 VLAN 生成树 (PVST+)**：为网络中的每个活动 VLAN 提供独立的 802.1D STP。

- **IEEE 802.1w-rapid PVST+**: 提供每 VLAN 快速生成树协议 (RSTP) (802.1w) 的实例。它易于实施, 在支持 Cisco Catalyst 6800 系列系统中最多 3000 个逻辑端口的大规模网络中之行之有效, 极大地缩短了网络恢复时间。
- **IEEE 802.1s 多生成树 (MST)**: 提供最多 16 个 RSTP (802.1w) 实例, 并将许多具有相同物理和逻辑拓扑的 VLAN 合并到一个常用 RSTP 实例中。

作为一种最佳实践, 建议在分布层和每个接入层系统中的多层网络设计中实施快速 PSVT+ STP 协议。对于大规模分布层块, 网络管理员可考虑将 IEEE MST 作为备选解决方案, 以简化生成树实例。分布层系统为物理网络和由完整构建块组成的第 2 层网络提供汇聚点, 应针对所有扩展 VLAN 范围将分布层系统静态指定为 STP 根交换机。接入层的 STP VLAN 优先级应保留默认值。如果修改默认设置, 事后应该复原成默认优先级, 如表 23 所示。

表 23. 思科生成树协议模式和根最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#spanning-tree mode rapid-pvst 6800-VSS(config)#spanning-tree vlan 1-4094 root primary
接入层	Cisco Catalyst 4K/3K/2K 4500E(config)#spanning-tree mode rapid-pvst 4500E(config)#default spanning-tree vlan 1-4094 root

单向链路检测建议

单向链路检测 (UDLD) 是第 2 层协议, 可结合第 1 层功能来确定链路物理状态。在第 1 层, 自动协商功能负责物理信令和故障检测。UDLD 执行自动协商无法执行的任务, 如检测邻居身份和关闭误连接端口。同时启用自动协商和 UDLD 后, 第 1 层和第 2 层检测方法相互配合可防止物理和逻辑单向连接和协议故障。UDLD 协议在第 2 层或第 3 层物理端口上透明工作。

作为协议级最佳实践, 应按照以下建议部署两个系统之间的单向通信:

- **第 2 层网络**: 在多层单机或基于 EtherChannel 的网络设计中, 可在接入交换机和分布交换机之间的每个中继端口上启用 UDLD 协议。
- **第 3 层 ECMP**: 在第 3 层基于 ECMP 的园区核心网络或路由接入网络设计中, 第 3 层路由协议 (而非 UDLD) 可检测两个系统之间的单向通信, 因为它在每个物理接口上运行。
- **第 3 层 EtherChannel**: 在建议的基于 EtherChannel 的网络设计中, 应在两个第 3 层系统之间实施 UDLD。在每个第 3 层成员链路中启用 UDLD 可检测单向转发路径并禁用 MEC 中的此类端口。

UDLD 在整个系统级别在以下一种模式下运行:

- **正常模式 (建议)**: 如果双向 UDLD 表明信息超时, 假定网络中没有故障, 并且不采取进一步措施。将 UDLD 的端口状态标记为未确定, 该端口按照 STP 状态进行操作。建议将 UDLD 消息时间保留为默认值, 以便在 CPU 使用率高、接口拥塞或管理引擎状态切换时将错误的正误差率降至最低。
- **积极模式**: 如果双向 UDLD 表明信息超时, UDLD 如检测到端口上的链路可以工作, 则会尝试重新建立端口状态。如果无法与 UDLD 邻居重新建立通信, 则会强制端口进入错误禁用状态。如配置为在指定时间间隔内自动恢复, 必须由用户或交换机进行手动恢复。

表 24. Cisco UDLD 最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#udld enable 6800-VSS(config)#default udld message
接入层	Cisco Catalyst 4K/3K/2K 4500E(config)#udld enable 4500E(config)#default udld message

VSS MAC 地址表同步建议

Cisco VSS 活动系统与对等网络设备和端点进行通信，并持续维持一种完全分布式转发架构。MAC 地址信息无需更多配置，也避免了操作员级复杂性，可在两个机箱上实现全局同步。此 MAC 地址同步过程称为 MAC 带外 (OOB) 同步。在线卡和管理引擎策略功能卡 (PFC) 的 DFC 上针对本地交换决策流程对此转发信息进行动态编程。默认情况下，MAC 地址信息每 160 秒与对等管理引擎和启用 DFC 的线卡模块同步一次。

作为一种最佳实践，建议保留 160 秒的 MAC OOB 计时器默认设置，将老化计时器设置为 480 秒（即 3 倍）。

表 25. Cisco VSS MAC OOB 最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#mac address-table synchronize activity-time 160

园区核心层网络设计最佳实践

核心层上行链路设计建议

如[分布层网络连接最佳实践](#)部分中所述，在分布层和核心层系统之间构建全网状物理网络设计可以在园区主干中实现最佳的负载均衡和恢复能力。必须设计高度可靠且稳定的核心网络基础设施，目标是通过在计划内或计划外网络故障期间不中断地完成工作，尽量消除应用影响。即使高可用性要求非常严格，也不应过高配置虚拟系统和网络，从而影响操作复杂性，这样可实现与 Cisco IOS 软件中内置各级智能相同的效果。

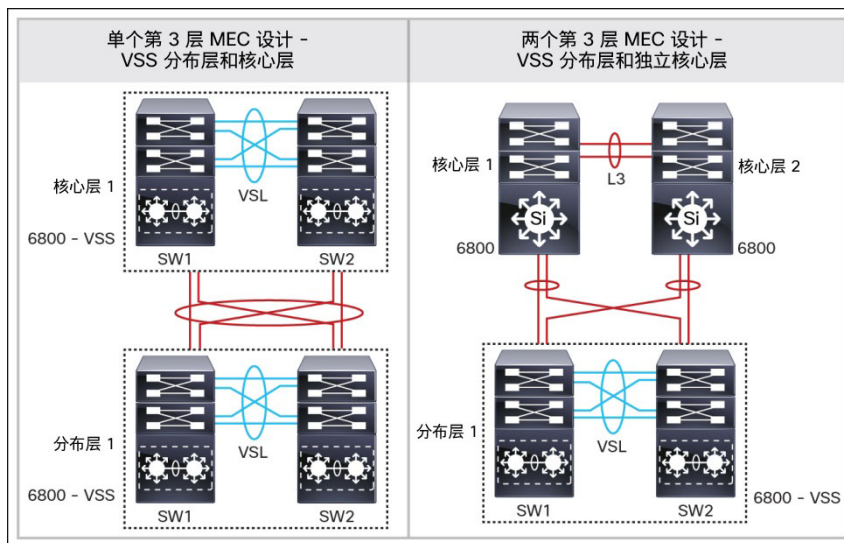
作为一种最佳实践，可在核心层和分布层系统之间安装附加的等效全网状物理接口集，以提高容量和恢复能力。

思科多机箱第 3 层 EtherChannel 最佳实践

Cisco VSS 系统对于对等设备和网络协议而言，是一种单一大型逻辑系统。为了获得最佳负载均衡和冗余，动态单播和组播路由协议需要在分布层和核心层系统之间安装的每个平行路径上独立工作。思科快速转发负载均衡散列算法通过结合第 3 层和第 4 层单播 IPv4 或 IPv6 数据包元组进一步计算出一个唯一值，以确定到每个第 3 层接口的数据转发结果。使用第 3 层 MEC 可极大地简化和优化这种分布层和核心层网络设计，正如在多层环境中，使用第 2 层 MEC 可简化 STP。

作为一种最佳实践，在分布层和核心层系统之间实施第 3 层 MEC 对于构建可扩展、高性能、非常简单且具有恢复能力的基础设施而言至关重要。无论是在 Cisco Catalyst 6800 系列 VSS 模式下还是在传统单机模式下，第 3 层 MEC 设计都取决于核心层系统设计。图 19 说明了针对核心层两种系统模式的第 3 层 MEC 设计建议，而 Cisco Catalyst 6800 系列系统部署在园区分布层网络的 VSS 模式下。

图 19. 多机箱第 3 层 EtherChannel 最佳实践



增强型内部网关路由协议设计建议

增强型内部网关路由协议 (EIGRP) 是均衡的混合路由协议，可在每个自治系统上构建邻居邻接和平面路由拓扑。在企业园区网络中设计和部署时，必须构建一个通用自治系统并运用各种最佳实践，以优化 EIGRP 性能并构建安全的路由邻接和具有恢复能力的设计，从而在出现故障时快速实现故障恢复。

自治系统和网络最佳实践

作为一种最佳实践，思科建议在园区分布层和核心层网络中实施 EIGRP 之前考虑以下重要设计任务：

- **EIGRP 自治系统：**必须将企业园区基础设施部署在单个 EIGRP 自治系统中，这样可简化操作任务并防止路由重分布、环路和因误配置可能引发的其他问题。必须避免多个 EIGRP 自治系统和路由重分布，才能构建可靠且可扩展的路由基础设施。
- **EIGRP 路由器 ID：**网络中的每个 EIGRP 系统都应配置网络范围内的静态唯一路由器 ID。作为一种最佳实践，建议使用一个本地环回接口来提高启用 EIGRP 的网络中的可靠性和稳定性。
- **EIGRP 自动汇总：**默认情况下，EIGRP 系统会将所有无类别网络通告给邻居，而不执行任何自动路由汇总。作为一种最佳实践，建议防止自动路由汇总，因为这样可在网络中创建重叠汇总项，影响用户和应用。默认情况下，禁用自动汇总，建议保留默认值。

表 26. EIGRP 自治系统最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#router eigrp <AS ID> 6800-VSS(config-router)#eigrp router-id <loopback_ip_address> 6800-VSS(config-router)#no auto-summary 6800-VSS(config-router)#eigrp log-neighbor-changes 6800-VSS(config-router)#network <address><wildcard_mask>

安全路由最佳实践

作为一种最佳实践，思科建议端到端保护 EIGRP 路由邻接，以实现网络级保护。通过保护 EIGRP 域，可靠托管对等设备的路由邻接受到保护，并按照可控的确定顺序工作。可靠的对等邻接应使用消息摘要算法 5 (MD5) 密钥建立邻居关系，确保对邻居间的通信进行加密，并保证其在网络上的安全。这样可以保护内部系统的 EIGRP 邻接，从而提高网络基础设施效率并提升保护能力。

- **EIGRP 邻居控制：**通过对与网络中非 EIGRP 设备（如 PC、无线 LAN 控制器等）连接的物理或逻辑接口进行被动模式配置，以阻止 EIGRP 邻居处理。这种最佳实践可帮助降低 CPU 使用率，如果与不可靠的设备存在未受保护的 EIGRP 邻接，可对网络提供安全保护。表 27 提供在可靠接口和所有系统接口块上启用 EIGRP 协议通信的最佳实践指南。必须在网络中的所有 EIGRP 第 3 层系统上运用这种建议的最佳实践。

表 27. EIGRP 邻居控制最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#router eigrp <AS ID> 6800-VSS(config-router)#passive-interface default 6800-VSS(config-router)#nopassive-interface <L3 Interface ID>

- **网络安全：**必须在网络中每个启用 EIGRP 的系统中使用 MD5 身份验证方法，以验证局域网/广域网络中每个 EIGRP 邻居的可靠性。作为一种最佳实践，对每个非被动 EIGRP 接口进行建议的 EIGRP MD5 邻接身份验证配置可与远程邻居建立安全的通信。必须在网络中的所有 EIGRP 系统上运用这种建议的最佳实践。

表 28. EIGRP 邻居身份验证最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#key chain <name> 6800-VSS(config-router)#key <ID> 6800-VSS(config-router)#key-string <password> 6800-VSS(config)#interface <ID> 6800-VSS(config-if)#ip authentication mode eigrp <AS> md5 6800-VSS(config-if)#ip authentication key-chain eigrp <AS><key-chain-name>

网络路由汇总最佳实践

Cisco EIGRP 路由协议可允许网络管理员在将多个独立和连续网络通告给邻居之前汇总为单一的汇总网络。独立网络需要网络中的每个路由器来同步路由拓扑，路由汇总通过隐藏独立网络中的故障帮助提升网络性能、稳定性和融合。

作为一种最佳实践，思科建议设计和部署结构化 IP 子网，以实现轻松扩展，并改善运营、管理和故障排除。为了将多个无类别网络汇聚成园区主干网络中一个唯一的有类网络，建议在园区网络中使用园区分布层。表 29 针对运行分布层系统第 3 层接口的每个 EIGRP 提供 EIGRP 路由汇总部署指南。

表 29. EIGRP 路由汇总最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#interface <ID> 6800-VSS(config-if)#ip summary-address eigrp <AS><network><address>

高可用性最佳实践

以往，园区网络恢复能力在很大程度上取决于路由协议恢复能力，路由协议恢复能力可快速检测网络故障、传播拓扑更改并重新聚合网络。任何路由协议的默认设置都很灵活，可防止网络在出现此类故障时出现错误的正误差率；但是，默认设置的副作用是导致恢复过程变慢。网络管理员需要深入了解网络设计和协议层，以微调高级参数，缩短恢复时间。

作为一种最佳实践，在基于 VSS 部署园区网络时，思科建议将路由协议设置保留为默认值。Cisco VSS 融入了基于硬件的内置智能，可快速检测故障并自启动恢复流程，但不会过高设置任何协议配置。

EIGRP 协议计时器

EIGRP 支持 hello 计时器和 hold 计时器，以保持与每个对等设备的路由邻接。在建议的园区网络设计中，在两个 EIGRP 邻居之间直接连接第 3 层接口，部署孤立的主干网络无需安装中间设备。对于这种拓扑，每个系统上的故障检测和恢复都采用硬件驱动来检测本地路径故障，并为路由表中的下一个预安装路径启动转发恢复流程。此类恢复流程在发生故障时提供确定的亚秒级网络融合时间。

作为一种最佳实践，思科建议将 EIGRP hello 计时器和 hold 计时器保留为默认设置，不作修改。将 EIGRP 计时器调整为较高频率会对在 VSS 机箱上 SSO 过程中的系统恢复流程产生不利影响。

表 30. EIGRP Hello 计时器和 Hold 计时器最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#interface <ID> 6800-VSS(config-if)#default ip hello-interface eigrp <AS> 6800-VSS(config-if)#default ip hold-time eigrp <AS>

EIGRP 正常重启实现不间断转发

在使用 SSO 冗余模式的系统中实施不间断转发 (NSF) 技术时，网络中断对于园区用户和应用是透明的，即使在重置控制平面处理模块（管理引擎/路由处理器）期间仍可提供高可用性。在出现故障时，底层第 3 层启用 NSF 的协议执行正常的网络拓扑再同步。冗余处理器或分布线卡硬件上的预设转发信息保持不变，并继续传送给交换网络数据包。这种服务可用性显著降低了平均修复时间 (MTTR)，并延长了平均故障间隔时间 (MTBF)，在最大程度上提高了网络可用性。

作为一种最佳实践，对于启用 VSS 的系统而言，针对单播路由协议启用 NSF 功能是一种基本要求。

表 31. EIGRP 正常重启 NSF 最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#router eigrp <AS> 6800-VSS(config-router)#nsf

开放最短路径优先路由协议设计建议

开放最短路径优先 (OSPF) 是一种广泛部署的针对异构供应商企业网络环境的 IETF 标准链路状态和自适应路由协议。与 EIGRP 不同，OSPF 网络将结构化网络边界构建成多个区域，帮助传播汇总网络拓扑信息并快速执行 OSPF 数据库计算，以做出智能转发决策。

区域和网络设计最佳实践

OSPF 将路由边界分成多个连接到单个核心主干区域的非主干区域，这种设计有助于简化管理并优化网络流量和资源利用率。OSPF 协议支持各种类型的区域；该最佳实践指南建议在企业园区网络中实施以下两种区域类型：

- **主干区域：**园区核心层是网络主干的核心，作为一种最佳实践，必须在 OSPF 主干区域内配置园区核心层。必须以区域边界路由器 (ABR) 角色实施园区汇聚层系统，该系统互连到核心主干区域，然后互连接到接入层非主干区域 OSPF 系统。思科建议实施连续的 OSPF 路由和主干区域设计。
- **末节/完全末节区域：**园区接入层网络需要来自分布层系统的精确网络拓扑信息和默认路由，以便与外部网络通信。在多层网络中，到终端站的默认网关由分布层交换机提供服务，而之间的第 2 层交换机是透明的转接设备。因此，必须将分布层和接入层之间的非 OSPF 主干区域配置为末节区域或完全末节区域模式。只有非主干区域可部署为末节区域或完全末节区域模式。

OSPF 支持多种网络类型，每种都可在各种网络连接和设计中以最佳状态运行。对于在基于以太网的网络上运行的 OSPF 协议而言，默认网络类型为广播类型。以太网是多路访问网络，可灵活地互连部署在单个第 2 层广播域中的多个 OSPF 邻居。

作为一种最佳实践园区网络设计，每个 OSPF 系统必须依据一个本地环回接口静态分配路由器 ID，实现路由域的稳定性。而且，两个第 3 层 OSPF 系统直接互连，因此形成了直接的点对点通信。思科建议在运行 Cisco IOS 软件和任何支持对等设备的系统上，将默认 OSPF 网络类型从广播修改为点对点类型。OSPF 点对点网络可消除灾难恢复/备份和灾难恢复处理并降低所有启用 OSPF 的系统之间的路由复杂性，从而优化邻接关系。

表 32. OSPF 区域和网络设计最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#router ospf <ID> 6800-VSS(config-router)#router-id <Loopback_IP_Address> 6800-VSS(config-router)#network <core_network><wildcard_mask> area 0 6800-VSS(config-router)#network <loopback_network><wildcard_mask> area 0
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#router ospf <ID> 6800-VSS(config-router)#network <access_network><wildcard_mask> area <non-backbone-area-id> 6800-VSS(config-router)#area <non-backbone-area-id> stub no-summary
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#interface <ID> 6800-VSS(config-if)#ip ospf network point-to-point

安全路由最佳实践

如前面在 [EIGRP 路由设计建议](#) 部分中 [安全路由最佳实践](#) 子部分中所述，思科建议端到端保护 OSPF 路由邻接，以实现网络级保护。如果 EIGRP 域安全，可靠托管对等设备的路由邻接受到保护，并按照可控的确定顺序工作。可靠的对等邻接应使用 MD5 密钥建立邻居关系，以确保对邻居间的通信进行加密，并确保其在网络上的安全。这样可以保护内部系统的 OSPF 邻接，从而提高网络基础设施效率并提升保护能力。

- **OSPF 邻居控制：**通过对与网络中非 EIGRP 设备（如 PC、无线 LAN 控制器等）连接的物理或逻辑接口进行被动模式配置，以阻止 EIGRP 邻居处理。这种最佳实践可帮助降低 CPU 使用率，如果与不可靠的设备存在未受保护的 OSPF 邻接，可对网络提供安全保护。表 32 提供在可靠接口和所有系统接口块上启用 OSPF 协议通信的最佳实践指南。必须在网络中的所有 OSPF 第 3 层系统上运用这种建议的最佳实践。

表 33. OSPF 邻居控制最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#router ospf <ID> 6800-VSS(config-router)#passive-interface default 6800-VSS(config-router)#nopassive-interface <L3 Interface ID>

- **网络安全：**必须在网络中每个启用 OSPF 的系统中使用 MD5 身份验证方法，以验证局域网/广域网络中每个 OSPF 邻居的可靠性。作为一种最佳实践，对所有实施的 OSPF 区域进行建议的 OSPF MD5 邻接身份验证配置可与远程邻居建立安全的通信。必须在网络中的所有 OSPF 第 3 层系统上运用这种建议的最佳实践。

表 34. OSPF 邻居身份验证最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#router ospf <ID> 6800-VSS(config-router)#area 0 authentication message-digest 6800-VSS(config-router)#area <non-backbone-area-id> authentication message-digest 6800-VSS(config)#interface <ID> 6800-VSS(config-if)#ip ospf message-digest-key <key><password>

网络路由汇总最佳实践

作为一种最佳实践，OSPF 路由汇总必须在连接 OSPF 主干和多个汇聚非主干的 ARB 上进行；通常，ABR 路由器是园区分布层。路由汇总的主要优势是在将多个独立网络和连续网络传送到 OSPF 主干区域之前汇总为一个单一汇总网络。独立网络需要网络中的每个路由器来同步路由拓扑，路由汇总通过隐藏独立网络中的故障帮助提升网络性能、稳定性和融合。

表 35. OSPF 路由汇总最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#router ospf <ID> 6800-VSS(config-router)#area <non-backbone-area> range <network><mask>

高可用性最佳实践

OSPF 正常重启实现 NSF

基于 Cisco IOS 软件的系统中的 OSPF NSF 功能和帮助功能可确保 NSF 系统在进行 SSO 状态切换时，对 OSPF 邻接和动态学习路由进行保护。默认情况下，每个运行 Cisco IOS 软件的 OSPF 系统都可具有 NSF 帮助功能。对于 OSPF 正常重启恢复流程，每个 VSS 或双管理引擎 OSPF 系统必须按照 OSPF 路由流程实施 NSF 功能。

NSF 信令可在两种模式下交换：思科专有模式和基于 IETF 标准模式。作为一种最佳实践，思科建议当 Cisco VSS 系统将 OSPF 与运行 Cisco IOS 软件的对等系统配对时，应启用“nsf cisco”或“nsf”。如果对等系统不支持 Cisco NSF 但支持 IETF NSF，则网络管理员必须配置“nsf ietf”，以使用支持 IETF 的对等系统成功完成正常的恢复流程。

表 36. OSPF 正常重启实现 NSF 最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS ! 如果远程 OSPF 系统为思科设备, 应配置 “nsf cisco” 6800-VSS(config)#router ospf <ID> 6800-VSS(config-router)#nsf cisco
分布层	Cisco Catalyst 6800 VSS ! 如果远程 OSPF 系统为非思科设备并支持 IETF NSF 功能, 应配置 “nsf ietf” 6800-VSS(config)#router ospf <ID> 6800-VSS(config-router)#nsf ietf

OSPF 自动成本计算和静态接口成本计算

OSPF 接口指标根据到达目标的较低指标或成本确定最佳转发路径。默认情况下, 在运行 Cisco IOS 软件的 Cisco Catalyst 交换机上, 根据一个固定公式 (108/以 bps 为单位的带宽) 自动计算 OSPF 接口的指标或成本。例如, 10Gbps 链路的 OSPF 成本计算为 1。在第 3 层基于 EtherChannel/MEC 的网络设计中, 将多个 10Gbps 或 40Gbps 链路捆绑为一个逻辑端口通道接口的方法可动态提高汇聚带宽; 但是, 由于在整个系统中使用固定的静态自动成本计算参考带宽公式, 因此 OSPF 成本仍然为 1。同样, 可调整接口层的默认 OSPF 成本, 以生成一个与 Cisco IOS 软件中自动计算的不同的值。

作为一种最佳实践, 建议在全局路由流程级和每个端口级将自动成本计算参考带宽保留为默认值。最大的默认 1G 成本不会进行调整, 或强制 OSPF 拓扑重新计算数据库, 这将导致进一步传播, 在某些情况下, 会在网络中形成次优转发路径。

表 37. OSPF 自动成本计算和静态接口成本计算最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#router ospf <ID> 6800-VSS(config-router)#default auto-cost
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#interface <id> 6800-VSS(config-if)#default ip ospf cost

OSPF 协议计时器和数据库配置

OSPF 支持各种协议和数据库计时器, 可在网络中实现快速故障检测、传播和恢复流程。当任何一部分 OSPF 网络出现系统或接口级稳定性问题时, 默认值可稳定 OSPF 路由域并将错误的正误差率降至最低。

默认情况下, OSPF 路由器每 10 秒钟传输 hello 数据包, 如果邻居在四个时间间隔或停滞 40 秒内无法接收到 hello 数据包, 便终止 OSPF 邻接。在这种优化的最佳实践网络设计中, 思科建议在运行 Cisco VSS 的所有启用 OSPF 的平台和对等设备上保留默认 OSPF hello 计时器和 hold 计时器。如果 hello 处理计时器和停滞时间设置较高, 可能会对所有冗余园区层系统 (如 VSS 或双管理引擎单机系统) 上的正常恢复流程造成不利影响。

表 38. OSPF 协议计时器最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#interface <id> 6800-VSS(config-if)#default ip ospf hello-interval 6800-VSS(config-if)#default ip ospf dead-interval

OSPF 数据库设置应保留为默认值，因为使用 Cisco VSS 时，本地故障检测和恢复流程是基于硬件的，而不是机械地基于协议。配置高级 OSPF 数据库功能或参数可能会造成冗余，因为 Cisco VSS 可使用默认 OSPF 值提供确定的亚秒级融合。

表 39. OSPF 数据库计时器最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#router ospf <ID> 6800-VSS(config-router)#default timers lsa arrival 6800-VSS(config-router)#default timers throttle lsa 6800-VSS(config-router)#default timers throttle spf

组播路由协议建议

由于单播通信基于一对一转发模式，在路由和交换决策中可以更轻松地执行目的地址查找、通过扫描转发表确定出口路径并交换流量。在前一部分讨论的单播路由和交换技术中，可能需要通过允许某些应用（其中的相同内容或应用必须复制给多个用户）来提高网络效率。

IP 组播尽可能使用最少的网络资源将源流量发送给多个接收者，同时不会给源或接收者造成更多负担。网络中的组播数据复制由启用协议无关组播 (PIM) 的系统完成，该系统可动态构建转发表。

PIM 稀疏模式最佳实践

要在网络中启用端到端组播操作，组播接收者和源之间的每个中间系统必须支持组播功能。组播会生成与单播路由和交换模式不同的转发表。为了启用通信，组播需要特定组播路由协议和动态组成员身份。

企业园区设计必须能够建立数据包分配树，分配树会在源子网和每个包含组播组成员的每个子网之间指定一个唯一的转发路径。构建分配树的主要目标是确保在树的每个分支上最多只转发每个数据包的一个副本。

PIM 协议分为以下两种模式，可支持两种类型的组播分布树：

- **密集模式**：假定网络中几乎所有的路由器都需要为每个组播组分配组播流量（例如，网络上的几乎所有主机都属于每个组播组）。密集模式下的 PIM 可构建分配树，方法是先使整个网络泛洪，然后剪掉少数没有接收者的路径。
- **稀疏模式 (SM)**：假定在网络中，每个组播需要的路由器相对较少。组内的主机分布稀疏，广域网上的大多数组播都属于这种情况。因此，PIM-SM 开始时分配树为空，并且只有当互联网组管理协议 (IGMP) 发出明确的加入分配请求时才会添加分支。

选择 PIM 模式取决于使用各种机制构建组播分配树的组播应用。根据组播比例因子和统一接入园区网络基础设施中适用于一对多组播通信的集中式源部署设计，思科建议部署静态 PIM-SM，因为它可以高效智能地构建组播分配树。

表 40. IP 组播 PIM 静态汇集点最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#ip multicast-routing 6800-VSS(config)#ip pim rp-address <RP_IP_Address> 6800-VSS(config)#interface loopback <ID> 6800-VSS(config-if)#ip pim sparse-mode 6800-VSS(config)#interface <ID> 6800-VSS(config-if)#ip pim sparse-mode 6800-VSS(config)#interface VLAN <ID> 6800-VSS(config-if)#ip pim sparse-mode

安全组播最佳实践

作为一种最佳实践，在企业园区网络中设计和部署 IP 组播时，为了构建安全的组播网络基础设施，网络管理员必须防范以下两种主要安全问题：

- **恶意组播源：**在 PIM-SM 网络中，可使用 `pim accept-register` 配置来控制不需要的流量源。当源流量到达第一跳路由器时，第一跳路由器 (DR) 建立 (S, G) 状态，并向汇集点发送 PIM 源寄存器消息。如果接受寄存器筛选器列表（配置在汇集点）中未列出源，则汇集点拒绝寄存器发出的消息，并向 DR 发回立即停止寄存器消息。使用这种源筛选方法的缺点是，在汇集点使用 `pim accept-register` 命令时，源的第一跳路由器上仍然建立 PIM-SM (S, G) 状态。这样可导致流量到达位于源和汇集点之间的源的本地接收者。而且，由于 `pim accept-register` 命令作用于汇集点的控制平面上，因此可用于借助虚假寄存器消息使汇集点超载，进而有可能导致拒绝服务状态。

作为一种最佳实践，应在汇集点使用简单的接入控制列表 (ACL) 来筛选只设置了接受寄存器配置的源地址。还可以在汇集点使用扩展 ACL 来筛选源和组。

表 41. IP PIM 恶意组播源安全最佳实践

网络层	Cisco Catalyst 交换机
核心层或任何网络层的 PIM 汇集点	Cisco Catalyst 6800 VSS 6800-VSS(config)#ip access-list extended <ACL_NAME> 6800-VSS(config-ext-nacl)#permit ip <MCAST_SRC_IP_Subnet><wildcard_mask><MCAST_GRP_Address><wildcard_mask> 6800-VSS(config-ext-nacl)#deny ip any any 6800-VSS(config)#ip pim accept-register list <ACL_NAME>

- **恶意 PIM 汇集点：**与组播源一样，任何路由器都可能被误配置或作为网络中具备有效组播组地址的组播汇集点恶意通告。使用静态汇集点配置，可将网络中每个启用 PIM 的路由器配置为针对组播源使用静态汇集点，并覆盖网络中的任何其他自动汇集点或自举路由器 (BSR) 组播路由器通告。

作为一种最佳实践，园区网络中每个启用 PIM 的系统应该仅接受静态汇集点发出的 PIM 通告，并忽略网络中任何其他不受管理的汇集点发出的动态组播组通告。

表 42. IP PIM 恶意汇集点安全最佳实践

网络层	Cisco Catalyst 交换机
所有第 3 层系统	Cisco Catalyst 6800 VSS 6800-VSS(config)#ip access-list standard <ACL_NAME> 6800-VSS(config-std-nacl)#permit 224.0.1.39 6800-VSS(config-std-nacl)#permit 224.0.1.40 6800-VSS(config-std-nacl)#deny any 6800-VSS(config)#ip pim rp-address <RP_IP_Address><ACL_NAME> override

高可用性最佳实践

部署在 VSS 或双管理引擎模式下的 Cisco Catalyst 6800 系列系统在本地支持全状态 IP 组播协议冗余，并使用与单播路由由协议相同的 SSO 技术。IP 组播协议状态机和分布转发项信息与辅助管理引擎模块进行热同步，从而可以在计划内或计划外网络故障期间在组播流之间正常切换。对于某些网络设计和拓扑，可以调整 PIM 邻居邻接和路由计时器，以实现快速故障检测，并触发一个恢复流程来重建组播转发表。但是在启用 VSS 的网络基础设施中，故障检测和恢复流程均独立于任何网络协议。

作为一种最佳实践，思科建议在 SSO 过程中将 IP 组播路由计时器保留为默认值，并将邻居查询计时器保留为默认值，这样 VSS 系统就能在管理引擎进行状态切换时正常恢复。当新管理引擎处于恢复过程中时，组播数据继续与网络中最近已知良好的转发项交换。将默认值修改为较高数值可能导致组播网络出现错误的正误差率，并可能对应用造成影响。

表 43. IP PIM 计时器最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#default ip multicast redundancy routeflush maxtime
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#interface <ID> 6800-VSS(config-if)#default ip pim query-interval

在大规模 IP 组播环境中，当端口向不同 VLAN 接口传送一些组播组流量时，由于只有一份出接口列表 (OIL)，因而会创建一份很大的组播路由表。当添加此类物理端口或从配置的 EtherChannel 中删除端口时，不会破坏 IP PIM 组播转发拓扑；数据重路由由决策基于硬件，VSS 系统必须在内部重新计算一种新的转发规则，为端口通道找到下一个可用的备用转发路径。这种重新计算可能会造成应用融合延误几秒，而这种延误在任务关键型 IP 组播园区网络环境中是无法接受的。

作为一种最佳实践，思科建议微调端口通道接口上的组播恢复流程，以实现与规模无关的启用组播的确定应用网络恢复流程。

表 44. IP 组播转发快速重定位最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#interface Port-Channel <ID> 6800-VSS(config-if)#platform multicast forwarding fast-redirect

一般路由建议

等价多路径路由最佳实践

以各种 IP 路由设计部署企业园区网络。在园区核心层部署 Cisco VSS 技术后，应将分布层的 VSS 与主干中的单个第 3 层 MEC 结合起来，因为这种架构本身可以为网络管理员带来多种优势，比如可以简化网络操作，显著提升系统、网络和应用性能。

但在某些情况下，在园区核心层部署 Cisco VSS 技术并不是一种好的选择。由于在物理上网络中存在两个独立核心系统，并具有传统的独立控制和管理平面，因而它会改变路由基础设施设计。网络管理员仍然可以部署两个独立的第 3 层 MEC EtherChannel，从 VSS 到每个上游独立核心系统都具有不同的光纤连接。这种网络设计创建了 ECMP 路由设计，而来自每个第 3 层 MEC 的出口数据转发决策分为两步：思科快速转发负载均衡和 MEC 负载均衡。

作为一种基于 ECMP 第 3 层网络的最佳实践，思科建议微调思科快速转发负载均衡，使其包含第 3 层和第 4 层元组，以便计算并完成两个上游第 3 层 MEC 接口之间的第一步最佳转发决策流程。[多机箱 EtherChannel 负载均衡](#)部分介绍第二步第 3 层 MEC 负载均衡的最佳实践。

表 45. ECMP 思科快速转发负载均衡最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#platform ip cef load-sharing full

单播 IP 路由项清除最佳实践

在基于 ECMP 的路由设计中，路由表中的路由项安装和清除功能以往都由 Cisco IOS 软件操作系统完成。为了满足某些网络拓扑对提高融合速度的要求，以前，默认行为在从路由数据库向路由信息库 (RIB)、随后向转发信息库 (FIB) 安装下一个最佳路径时很慢。为了在这种网络拓扑中优化融合，已在最新的 Cisco IOS 软件版本中修改了默认行为。

动态路由项删除流程已经是一项路由协议功能，当第 3 层物理接口或整个 MEC 接口出现故障时可以使用此流程。网络管理员需要微调 OSPF 链路状态通告/最短路径优先 (SPF) 计时器，而链路状态数据库 (LSDB) 可以快速计算拓扑更改，并将其传播给 OSPF 网络的其余部分。单播数据平面网络总体恢复时间在很大程度上取决于在网络中每个系统的路由流程上实施的高级 OSPF 调整。

如之前的建议，如果企业园区网络设计在物理上为全网状，并在逻辑上使用 Cisco VSS 和 MEC 技术实现了控制和管理平面虚拟化，那么转发和重路由决策流程为硬件驱动。因此，作为一种最佳实践，可使用简单配置部署园区网络，并使用内置 Cisco VSS 弹性技术提供确定的亚秒级融合，而无需对网络进行任何高级微调。网络管理员必须在所有第 3 层 ECMP 网络上应用以下最佳实践，以便在园区网络中复原基于 Cisco IOS 软件的传统路由安装和清除行为。

表 46. 单播 IP 路由项清除最佳实践

网络层	Cisco Catalyst 交换机
所有 ECMP 路由系统	Cisco Catalyst 6800 VSS 6800-VSS(config)#no ip routing protocol purge-interface

IP 事件阻尼

物理网络连接不稳定与信令质量差或连接断开可能会造成持续的端口摆动。如果不使用最佳实践指南将企业园区网络部署为在汇聚层汇总网络边界，一次接口摆动就会对整个园区网络的稳定性和可用性造成严重影响。路由汇总是一种用于隔离故障域并将本地网络故障控制在域内的技术。

为了确保端口摆动时本地网络域的稳定性，可对所有第 3 层接口实施 IP 事件阻尼，其基本原理与边界网关协议 (BGP) 阻尼相同。第 3 层接口每次出现摆动时，IP 阻尼会跟踪并记录摆动事件。出现多次摆动时，向端口分配逻辑处罚，并在端口稳定之前禁止向 IP 路由发送链路状态通知。

作为一种最佳实践，建议在运行路由协议的第 3 层端口上启用 IP 事件阻尼，如表 47 所示。

表 47. IP 事件阻尼最佳实践

网络层	Cisco Catalyst 交换机
分布层	Cisco Catalyst 6800 VSS 6800-VSS(config)#interface Port-Channel <id> 6800-VSS(config-if)no switchport 6800-VSS(config-if)dampening
核心层	Cisco Catalyst 6800 VSS 6800-VSS(config)#interface Port-Channel <id> 6800-VSS(config-if)no switchport 6800-VSS(config-if)dampening

小结

思科统一接入实现的企业园区网络以思科新一代架构为基础构建，这种架构可安全、可靠、顺畅地提供全新工作空间体验，使用任何设备即可随处将任何人与任何资源连接。具有恢复能力的强健智能网络用于满足全局工作空间的需求，只有这种网络才能实现这种统一体验。思科推出的网络平台是这种架构的主要组成部分，可提供无界服务，如移动、安全、媒体意识、定位和 Cisco EnergyWise®，从而提供最佳用户体验。通过在边缘构建智能型网络设计，可提供移动与安全协作以及整体基础设施主干，以便在网络范围内提供差异化服务，实现一致可靠的高可用性用户体验。思科统一接入实现了创新业务模式，提供全新的用户体验，可提高客户满意度和忠诚度。

参考资料

无线园区设计指南

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/Borderless_Campus_Network_1-0/Borderless_Campus_1-0_Design_Guide.pdf

Cisco VSS 设计指南

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/VSS30dg/campusVSS_DG.pdf

企业园区服务质量

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.pdf

安全性

<http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html>

园区局域网思科验证设计

<http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-CampusWiredLANSDesignGuide-AUG14.pdf>



美洲总部
Cisco Systems, Inc.
加州圣荷西

亚太总部
Cisco Systems (USA) Pte, Ltd.
新加坡

欧洲总部
Cisco Systems International BV Amsterdam.
荷兰

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 中列出了各办事处的地址、电话和传真。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的注册商标。要查看思科商标的列表，请访问此 URL：www.cisco.com/go/trademarks。
本文提及的第三方商标均归属其各自所有者。使用“合作伙伴”一词并不暗示思科和任何其他公司存在合伙关系。(1110R)