配置管理：最佳实践白皮书

目录

[简介](#)
[配置管理高级流程](#)
[创建标准](#)
[软件版本控制和管理](#)
[IP 寻址标准和管理](#)
[命名规则和 DNS/DHCP 分配](#)
[标准配置和描述符](#)
[配置升级过程](#)
[解决方案模板](#)
[维护文档](#)
[当前设备、链路和终端用户登记](#)
[配置版本控制系统](#)
[TACACS 配置日志](#)
[网络拓扑结构文件](#)
[验证和审查标准](#)
[配置完整性检查](#)
[设备、协议和介质审核](#)
[标准和文档回顾](#)
[相关信息](#)

简介

配置管理是一种收集过程和工具，可以促进网络一致性，追踪网络更改，并提供最新网络说明文件和可视性。通过构建和维护配置管理的最佳实践，您能获得几大好处，例如改进网络可用性和降低成本等。这些新发展包括：

- 被动支持问题减少，因而支持成本降低。
- 由于识别未使用的网络组件的设备、电路、用户跟踪工具和进程而降低网络成本。
- 被动支持成本降低且解决问题所需的时间缩短，因而网络可用性得以改进。

我们注意到缺乏配置管理会导致以下问题：

- 无法确定网络更改对用户的影响
- 被动支持问题增多，可用性降低
- 解决问题所需的时间延长
- 因未使用的网络组件导致网络成本增加

此最佳实践文档提供了用于成功实施配置管理计划的过程流程图。我们将详细了解以下步骤：创建标准、维护文档以及验证和审核标准。

配置管理高级流程

下面的图表显示您如何能使用重要成功因素以及性能指示实施成功的配置管理计划。

创建标准

创建网络一致性标准能帮助减少网络复杂性、意外停机时间和暴露给网络冲击事件等。我们建议采用以下标准以实现最佳网络一致性：

- 软件版本控制和管理
- IP 寻址标准和管理
- 命名约定和域名系统/动态主机配置协议 (DNS/DHCP) 分配
- 标准配置和描述符
- 配置升级过程
- 解决方案模板

软件版本控制和管理

软件版本控制是指在类似的网络设备上部署统一的软件版本的行为。这将增加所选软件版本的验证和测试机会，极大限制网络中发现的软件缺陷数量和互操作性问题。采用用户界面、命令或管理输出、升级行为和功能行为，有限软件版本可以降低意外行为的风险。这样做会使环境更为简单且更易于获得支持。总之，软件版本控制可改进网络可用性，并且有助于降低被动支持成本。

注意：相似的网络设备定义为标准网络设备，使用提供通用服务的通用机箱。

实施以下步骤以实现软件版本控制：

- 根据机箱、稳定性和新功能要求确定设备的分类。
- 确定类似设备各自的软件版本。
- 对选定的软件版本进行测试、验证和试运行。
- 记录成功的版本，将其作为同类设备采用的标准版本。
- 始终为所有类似设备部署或将其升级到标准软件版本。

IP 寻址标准和管理

IP地址管理是在网络中分配、再循环和对IP地址及子网进行存档的过程。IP 寻址标准定义了子网大小、子网分配、网络设备分配以及子网范围内的动态地址分配。推荐的IP地址管理标准可以减少子

网交迭或复制、网络中的非汇总，相同IP地址设备分配、IP地址空间浪费和不必要的复杂性。

成功管理 IP 地址的第一步是了解网络中使用的 IP 地址块。在许多情况下，网络组织必须依靠RFC 1918地址空间，该地址空间不是互联网可寻址的，但可与网络地址转换(NAT)一起用于访问网络。一旦您定义了地址块，并把它们分配到网络区域，就可以促进汇总。在许多情况下，您还必须根据定义范围内的子网数量和大小，进一步细分这些模块。您应当为标准应用定义标准子网大小，例如构建子网大小、WAN链路子网大小、环回子网大小或WAN站点子网大小。然后您可以在一个更大的汇总块内的子网块外为新应用分配子网。

例如，构建一个大型企业网络，包括东海岸校园、西海岸校园、国内广域网、欧洲WAN和其他主要国际站点。组织向这些区域分配邻接的IP无类别域间路由(CIDR)块，以促进IP汇总。组织然后在那些模块内定义子网大小，并将每个模块的子部分分配给某个特定的IP子网大小。每个主要块或整个IP地址空间可以记录在电子表中，表示块内的每种可用子网大小的分配、使用和可用子网。

下一步是分别创建各子网范围内的 IP 地址分配标准。在子网之内的路由器和热备份路由协议(HSRP)虚拟地址可以在范围之内被分配第一个可用地址。交换机和网关可能被分配下一个可用地址，其次是其他固定的地址分配，最后是DHCP动态地址。例如，所有的用户子网可能都是 /24 子网，可用地址分配为 253 个。路由器可以分配地址1和地址2，HSRP地址可以分配地址3，通过地址9可以交换地址5，DHCP范围包含地址10到地址253。不论您开发什么标准，它们都应当进行存档，并参考所有网络工程计划文件，以帮助确保一致配置。

命名规则和 DNS/DHCP 分配

一致地、有结构地使用设备的命名规则和DNS能够帮助您用下列方式管理网络：

- 创建一个连接至各路由器的一致访问点，以访问与设备相关的所有网络管理信息。
- 降低 IP 地址重复的概率。
- 创建简单的设备标识，其中显示位置、设备类型和用途。
- 提供了一种更简单的方法来识别网络设备，从而改进库存管理。

大多数网络设备均设有一到两个用于管理设备的接口。这些接口可能是一个带内或带外以太网接口和一个控制台接口。您应该为与设备类型、位置和接口类型有关的接口建立命名规则。由于可以从不同接口访问回环接口，所以我们强烈建议在路由器上将回环接口作为主要管理接口。您还应配置环回接口，作为陷阱、SNMP 和 Syslog 消息的源 IP 地址。单个接口然后拥有识别设备、位置、目的和接口的命名规则。

我们也推荐识别DHCP范围，并将它们添加到DNS中（包括用户位置）。这可能是 IP 地址或物理位置的一部分。示例可能是"dhcp-bldg-c21-10" 到"dhcp-bldg-c21-253"，即C栋第二楼第1配线间的IP地址。您还可以使用精确的子网进行识别。一旦为设备和DHCP创建了命名规则，您将需要工具来追踪和管理条目，如Cisco Network Registrar。

标准配置和描述符

标准配置适用于协议和媒体配置以及全局配置命令。描述符是用于描述接口的界面命令。

我们推荐为每个设备分类创建标准配置，例如路由器、LAN交换机、广域网交换机或ATM交换机。

每种标准配置都应包含维护网络一致性所需的全局、媒体和协议配置命令。媒体配置包括 ATM、帧中继或快速以太网配置。协议配置包括标准 IP 路由协议配置参数、常用服务质量 (QoS) 配置、常用访问列表及其他所需的协议配置。全局配置命令适用于所有类似设备，并且包括以下参数：服务命令、IP命令、TACACS命令、vty配置、横幅、SNMP配置和网络时间协议(NTP)配置。

描述符是通过创建一种适用于每个接口的标准格式建立的。描述符包括接口的目的和位置、与该接口连接的其它设备或位置、电路标识符。描述符能帮助您的支持组织更好地了解接口有关的问题范围，然后更快地提供解决方法。

我们建议在标准配置文件中保留标准配置参数，并在配置协议和接口之前把文件下载到每个新的设备。另外，您应该提供证明标准的配置文件，包括每个全局配置参数的解释和它为什么重要。Cisco Resource Manager Essentials (RME) 可用于管理标准配置文件、协议配置和描述符。

配置升级过程

升级过程可帮助确保软件和硬件升级顺利进行，将停机时间缩至最短。更新程序包括供应商验证、供应商安装参考，如版本说明、更新方法学或步骤、配置指南和测试需求等。

升级过程可能因网络类型、设备类型或新的软件要求不同而存在很大差异。单个路由器或交换机的升级需求可以在体系结构组内制定和测试，并在所有更改文档中引用。对涉及整个网络的其他升级进行测试不可能如此简单。这些升级可能要求更加详细的计划、供应商的介入和其它步骤以保证成功。

您应配合任何新的软件部署或已确定的标准版本来创建或更新升级过程。程序应该定义所有升级步骤，参考与更新设备相关的厂商文档，以及升级后的设备验证的测试程序。一旦升级程序经过定义和验证，该升级程序 应在所有适合该升级的文档中被引用。

解决方案模板

您可以使用解决方案模板定义标准的模块化网络解决方案。网络模块可能是配线柜、WAN 现场办公室或访问集中器。在每个案例中，您需要定义、测试和记录解决方案，确保以完全相同的方式执行类似的部署。由于解决方案的行为做好了定义，因此能够保证企业的未来变化的风险级别降低很多。

为更高风险的配置和解决方案创建的解决方案模板将部署多次。解决方案模板包含适用于网络解决方案的所有标准硬件、软件、配置、布线和安装要求。解决方案模板的具体详细信息显示如下：

- 硬件和硬件模块，包括内存、闪存、电源和卡布局。
- 逻辑拓扑，包括端口分配、连接、速度和媒体类型。
- 软件版本，包括模块或固件版本。
- 所有非标准、非设备特定配置包括路由协议、媒介配置、VLAN配置、访问列表、安全、交换路径，生成树参数和其他。
- 带外管理要求。
- 电缆要求。

- 安装要求，包括环境、电源和机架位置。

请注意，解决方案模板未包含许多要求。整体配置管理惯例包括特定需求，如特定解决方案的IP编址、命名、DNS分配、DHCP分配、PVC分配、接口描述符和其他。更多的一般要求，如标准配置、变更管理计划、文档更新流程或网络管理更新流程等应包括在一般配置管理方法中。

维护文档

我们推荐对网络和网络中近似实时的变化进行记录。您能使用这些准确的网络信息进行排除故障、网络管理工具设备清单、库存、验证和审计等。我们建议使用以下网络文档关键成功因素：

- 当前设备、链路和最终用户清单
- 配置版本控制系统
- TACACS 配置日志
- 网络拓扑文档

当前设备、链路和终端用户登记

当前设备、链路和用终用户明细信息使您能跟踪网络设备明细和资源、问题影响及网络更改影响等。能够追踪用户需求相关的网络设备明细和资源，有助于确保可管理网络设备的积极使用，为审核提供必要信息，并且有助于管理设备资源。终端用户关系数据提供的信息定义更改风险和影响，以及更快地排除故障、解决问题的功能。设备、链路和最终用户清单数据库通常由许多领先的服务提供组织开发。网络库存软件的领先开发者是Visionael Corporation 。数据库可能包含类似于设备、链路、客户用户/服务器数据的列表，以便发生设备故障或网络更改时，您可以很容易了解终端用户的影响。

配置版本控制系统

配置版本控制系统维护所有设备当前运行的配置和早先运行版本的一套数量。此信息可用于排除故障和配置或更改审计。排除故障时，您可以比较当前运行配置与早先工作版本，了解配置是否以任何方式与问题相关。我们建议保留三到五个以前的配置工作版本。

TACACS 配置日志

要确定对配置做出更改的人员和时间，您可以使用 TACACS 日志记录和 NTP。当这些服务在Cisco网络设备上启用时，配置更改的同时用户ID和时间戳将添加到配置文件。之后，此标记会随配置文件一起复制到配置版本控制系统。TACACS可以作为不可管理变化的一种威慑，并且可以提供已发生变化的适当审核机制。使用思科安全产品启用 TACACS。当用户登录设备时，他或她必须通过户名和密码验证TACACS服务器。如果将设备指向NTP主时钟，很容易在网络设备上启用NTP。

网络拓扑结构文件

拓扑文档可帮助了解和支持网络。您能使用它来验证设计指南，并更好地了解网络，以便进行未来设计、更改或故障排除等。拓扑文档应该包括逻辑和物理文件，包括连接性、寻址、介质类型、设

备、机架布局、卡分配、有线路由、电缆证明、终止点、功率信息和电路标识信息。

维护拓扑文档是成功配置管理的关键所在。要创建可能产生拓朴文件维护的环境，必须强调说明文件的重要性，且信息必须可以用于更新。我们强烈建议，只要出现网络更改就要更新拓扑文档。

网络拓扑文档通常使用图形应用程序(如Microsoft Visio)进行维护。其他产品(如Visionael)提供了管理拓扑信息的卓越功能。

验证和审查标准

配置管理绩效指标提供了一种用于验证和审计网络配置标准和关键成功因素的机制。通过实施配置管理的流程改进程序，您能使用性能指标识别一致性问题，并改进整个配置管理。

我们建议组建一个跨职能部门的团队，以衡量配置管理成功与否，并改进配置管理过程。小组的第一个目标是实施配置管理性能指示器，以识别配置管理问题。我们将详细探讨以下配置管理绩效指标：

- 配置完整性检查
- 设备、协议和媒体审计
- 标准和文档审查

在对这些审计结果进行评估后，起动项目修正不一致的地方，然后确定问题的最初原因。潜在原因包括缺乏标准文档或缺乏一个一致进程。您可以改进标准文档，实施培训或者改进进程，以防止进一步配置的不一致。

我们建议每月进行一次审计，如果仅需要验证，也可以每个季度进行一次。对以往的审计进行审查，确认以往的问题均已得到解决。寻求整体改进和目标，以展示取得的进步和价值。创建度量标准，以显示高风险、中风险和低风险网络配置不一致的数量。

配置完整性检查

配置的完整性检查应评估网络的整体配置、复杂性和一致性及潜在问题等。对于思科网络，我们建议使用 NetSys 配置验证工具。此工具输入所有设备配置，并创建识别当前问题的配置报告，如相同IP地址、协议不匹配和不一致等问题。工具报告所有连接或协议问题，但不在每个设备上输入评估的标准配置。您可以手动审查配置标准或创建报告标准配置差异的脚本。

设备、协议和介质审核

设备、协议和介质审核是软件版本、硬件设备与模块、协议与介质、命名规则的一致性的性能指标。审计应该首先识别所有非标准问题，这将导致配置更新，以便对这些问题进行调整或改进。评估整体进程确定它们如何能够防止不最理想或非标准配置的发生。

Cisco RME是配置管理工具，能提供硬件版本、模块和软件版本的审核和报告。Cisco也在开发更全面的的介质和协议审核，报告与IP、DLSW、帧中继和ATM的不一致。如果没有进行协议或媒质审核，您可以使用手动审核，例如查看设备、网络中所有类似设备的版本和配置，或者抽查设备、版本和配置。

标准和文档回顾

此性能指示器参阅网络和标准文档，确保信息准确和最新。审计应该包括查看当前说明文档、推荐更改或者添加和审批新的标准。

您应每季度查看以下文档：标准配置定义、解决方案模板（包括建议的硬件配置）、当前标准软件版本、所有设备和软件版本的升级程序、拓扑文档、当前模板和IP地址管理。

相关信息

- 技术支持 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。