

思科最初NCS 1.1部署指南

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[安装](#)

[物理设备：ISO安装](#)

[虚拟设备：VMware卵安装](#)

[请使用vSphere客户端安装卵](#)

[物理/virtual设备升级](#)

[开始NCS](#)

[移植从WCS到NCS](#)

[从WCS的数据迁移](#)

[从WCS的出口数据](#)

[迁移WCS数据到NCS](#)

[从NCS 1.0.x的升级NCS到1.1](#)

[从WCS的导入地图](#)

[高可用性-操作基本理论](#)

[Catalyst 交换机配置](#)

[无线网络规划](#)

[计划的工具](#)

[地图编辑器](#)

[导入地图从WCS到NCS](#)

[请使用NCS部署无线局域网](#)

[配置模板](#)

[配置组\(设置组\)](#)

[监控的使用NCS/排除故障无线网络](#)

[RRM /CleanAir](#)

[建立与思科最初NCS 1.1的一RF配置文件](#)

[应用RF配置文件给有NCS的AP组](#)

[请使用NCS对修正问题](#)

[请使用NCS优化无线网络的操作](#)

[控制板](#)

[区域图的自定义](#)

[监控客户端和用户](#)

[有线的/无线客户端故障排除](#)

[无线客户端故障排除](#)

[有线的客户端故障排除](#)

[RF/Wireless功能](#)

[跟踪客户端](#)

[未知用户ID](#)

[实时热量地图](#)

[监控思科Catalyst交换机使用NCS](#)

[生成树](#)

[思科Stackwise](#)

[VLAN资讯台](#)

[客户端列表页](#)

[报告\(交叉启动和缩放\)](#)

[新的报告](#)

[报警/事件](#)

[快速过滤器](#)

[先进的过滤器](#)

[AAA用户认证通过TACACS+/RADIUS使用ACS 4.2](#)

[相关信息](#)

简介

思科填充网络控制系统(NCS)是Cisco网络管理平台下一代管理有线的/无线访问网络的。

WLAN生命周期管理：全面的WLAN生命周期管理包括各种各样的规划、部署、监听和故障排除、修正和优化。

- 计划—内置的规划和设计工具简化定义接入点放置和覆盖。另外，从第三方地点调查工具的信息在WLAN设计和部署可以导入到思科NCS帮助。
- 部署—清楚的套集成控制器和访问接入节点配置模板提供快速和有效部署。网络审计为有效的配置管理支持。NCS在监听也提供工具帮助，升级和移植Cisco Aironet独立(自治)接入点运行作为轻量级接入点和运行CAPWAP。基于任务的访问控制提供灵活性分段无线网络到单个思科NCS平台控制的一个或更多虚拟域。
- 监听和故障排除—整个WLAN帮助的集中化监听维护稳健WLAN性能和—最佳的无线体验。思科CleanAir提供关于RF干扰事件、空气质量和干扰安全威胁的详细信息效率更高帮助估计，优先安排和管理RF干扰问题。易用图形显示起一起点作用对于维护、安全、故障排除和将来容量规划。图表、图和表为快速配置和重新配置是交互。分层的映射树、颜色编码和图标支持快速可视化和对网络、设备和空气质量的状态鉴定。老在报警摘要提供稳健故障、事件和告警管理。不变搜索工具实现对立即和有历史的信息的网络访问关于任何地方在访问网络和资产查找的设备，包括终端和会话属性、关联历史记录、端点位置、RF性能、统计信息、高级无线电资源管理(RRM)和空气质量。嵌入客户端故障排除工具提供一个逐步方法分析所有有线的和无线客户端设备的问题。此稳健客户端故障排除工具帮助通过加速故障单的解决方法降低运营成本各种各样的wi-fi客户端设备设备类型的。

NCS作用在网络

此图表示与思科最初NCS的Cisco无线网络架构。多种网元之间的交互作用，是无线局域网控制器、AP、Cisco Catalyst交换机、移动服务引擎，网络控制系统、客户端网络管理站和第三方应用。

NCS使用的端口

设备支持和软件版本

设备类型	支持的软件Version*
Cisco Catalyst 2000系列交换机：2960， 2975	Cisco IOS软件版本独立报
Cisco Catalyst 3000系列交换机：3560， 3750-E， 3750-X	Cisco IOS软件版本独立报
Cisco Catalyst 4500系列交换机	Cisco IOS软件版本独立报
Cisco Catalyst 6000系列交换机	Cisco IOS软件版本独立报
思科2x00， 4x00， 5500无线控制器集成WLAN (WLCM， WiSM， WiSM2)	4.2.x， 6.x， 7.x
Cisco Aironet自治AP	Cisco IOS软件版本12.3(7)JA和以后

* -支持的控制器软件版本在NCS版本注释列出。

NCS有两个部署选项：

1. 硬件设备
2. 虚拟设备

虚拟设备是在VMware ESX/ESXi 4.x和5.0可以部署的卵文件。此表为NCS管理的设备提供缩放编号。

台秤				
	Unified AP	aIOS AP	交换机	无线 LAN 控制器
小虚拟设备	3,000	1,000	1,000	240
中等虚拟设备	7,500	2,500	2,500	600
大虚拟设备	15,000	5,000	5,000	1,200

注意：无线局域网控制器的(WLC台秤编号; s)最大。缩放。WLCs不计数NCS许可证计数。

此表列出根据有线的/无线等级的虚拟设备的硬件需求。

虚拟设备-硬件需求			
	处理器	DRAM	硬盘
小虚拟设备	2个核心@ 2.93GHz	8 GB	200 GB
中等虚拟设备	4个核心@ 2.93GHz	12 GB	300 GB
大虚拟设备	8个核心@ 2.93GHz	16 GB	400 GB

NCS主页

NCS 1.1提供能力监控IPv6客户端。一新的主页dashlet，由IP地址类型的客户端计数，提供根据IP地址类型的客户端一台目视指示器。是指不可能确定IP地址的客户端;典型地有线的客户端，在监听的IPv6不是可用/支持在设备处。

浏览器支持

NCS 1.1支持这些浏览器：

- Firefox 3.6及以上版本
- 谷歌镀铬物12.0.742.x
- 有[镀铬物plug-in](#)的微软Internet Explorer**注意**：不支持本地Internet Explorer。

本文为NCS部署提供结构上了解和设计指导。

[先决条件](#)

[要求](#)

本文档没有任何特定的要求。

[使用的组件](#)

本文档中的信息根据思科最初NCS 1.1。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[安装](#)

[物理设备：ISO安装](#)

NCS是可用的作为物理和虚拟设备。此部分提供步骤配置在一个物理设备的ISO镜像。

1. 对DVD的下载和烧录ISO。ISO在[下载软件\(仅限注册用户\)](#)被张贴。请使用您的Cisco.com用户名和密码。
2. 安装ISO。重新启动与插入的ISO的计算机。此窗口出现。选择选项1或2，依赖于怎样您连接到设备
3. 安装花费大约30分钟完成。在ISO镜像安装后，服务器重新启动。在您的设备重新启动后，请去物理/virtual设备设置部分。

[虚拟设备：VMware卵安装](#)

在VMware ESX/ESXi 4.x完成在此部分的这些步骤为了部署卵。在卵安装后，请继续物理/virtual设

备设置部分。它用部署变化基于网络连接速度对ESX主机的时间。

部署卵文件。卵在[下载软件\(仅限注册用户\)](#)被张贴。下载根据由此NCS服务器管理设备的数量的适当的卵。

[请使用vSphere客户端安装卵](#)

完成这些步骤：

1. 启动VMware vSphere客户端。选择**File>部署OVF模板**。文件，NCS VMware镜像包，当卵(开放虚拟化存档)。在上一个屏幕画面的菜单项是为OVF模板。卵是项目的一集在单个存档。这些项目典型地包括虚拟机说明文件(*.ova)，清单文件(*.mf)和虚拟硬盘驱动器文件(*.vmdk)。
2. 选择**浏览**并且寻找NCS卵文件。单击 **Next**。
3. 在卵文件选择后，VMware ESX/ESXi读卵文件属性。通过步骤继续为了选择您在ESX/ESXi要安装的卵文件。在磁盘格式化页，请选择**厚实的已配置格式**选项。
4. 汇总页列出选择的选项。单击 **Next**。NCS重新启动。在虚拟机被构件后，出现在窗口的左手边。为了启动虚拟机，请从列出已安装虚拟机的左边菜单选择它并且点击**开放控制台**图标。这时，NCS安装作为虚拟机。设置步骤的其余为物理和虚拟机是相同的。

[物理/virtual设备升级](#)

完成这些步骤：

1. 获取NCS升级镜像在服务器存储文件位置的URL。运行这些命令为了升级NCS安装：

```
ncsl/admin# ncs stop
Stopping Network Control System...
This may take a few minutes...
Network Control System successfully shutdown.
```

2. 一旦NCS被终止了，请输入配置模式并且放置文件位置URL到信息库：

```
ncsl/admin# conf t
Enter configuration commands, one per line. End with CNTL/Z.
ncsl/admin(config)# repository NCS58
ncsl/admin(config-Repository)# url http://xxxx/sanity/1.X.X.10/wcs-cars-appbundle/
ncsl/admin(config-Repository)# exit
ncsl/admin(config)# exit
```

3. 验证信息库访问文件及早指定与URL：

```
ncsl/admin# show repository NCS58
ncs-upgrade-bundle-1.1.0.58.tar.gz
```

4. 运行这些命令为了开始从信息库的升级进程。

```
ncsl/admin# application upgrade ncs-upgrade-bundle-1.1.0.58.tar.gz NCS58
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Initiating Application Upgrade...
```

5. 表明的消息应该出现升级进程当前完成。

[开始NCS](#)

在服务器重新启动后，请登录系统作为admin使用作为设置步骤一部分，您提供的密码。在您登录服务器后，请启动有admin@ncs-serverNCS服务器] # startncs。

当NCS运行，控制台信息指示。通过Web浏览器登录您的NCS服务器，有您在安装时选择的密码的用户根。在您通过浏览器登录后，登录NCS根密码可以更改。

移植从WCS到NCS

在您尝试进行迁移进程到NCS 1.1.x.x前，您必须升级他们的思科WCS服务器到这些版本之一。

- 7.0.164.3
- 7.0.172.0
- 7.0.220.0

此部分为如何移植在Windows或Linux服务器的WCS提供说明到NCS。NCS版本是主要版本提供的有线的和无线设备的聚合的管理和增加的可扩展性。NCS平台根据Linux 64位OS，并且后端数据库是Oracle DBMS。现有WCS平台是或者Windows或Linux 32位和后端数据库是固态DB。

从WCS的数据迁移

从WCS的出口数据

通过CLI导出从WCS 7.x的数据。CLI命令出口的**userdata**可用在WCS版本7.x和以后，创建.zip文件包含WCS Data文件。CLI不提供任何选项定制什么可以导出;所有非全局用户定义的项目导出。完成这些步骤为了导出WCS数据：

1. 中断WCS服务器。
2. 通过脚本文件运行出口命令并且提供路径并且导出文件名，当提示。
3. 对于Linux，请运行export.sh所有/data/wcs.zip命令。对于Windows，请运行export.bat全部数据\ wcs.zip命令。

迁移WCS数据到NCS

完成这些步骤为了迁移WCS数据：

1. 安置WCS出口.zip文件(例如， wcs.zip)在信息库或文件夹(例如， 信息库)。
2. 登陆作为管理员用户并且通过输入**stop命令的ncs**中断NCS服务器。配置在NCS设备的FTP信息库用**repository命令**：

```
ncs-appliance/admin#configure
ncs-appliance/admin(config)# repository ncs-ftp-repo
ncs-appliance/admin(config-Repository)# url ftp://209.165.200.227//
ncs-appliance/admin(config-Repository)# user ftp-user password plain ftp-user
```

注意： 确保归档文件用**显示信息库repositoryname**命令是可用的。

3. 输入**ncs移植**命令为了恢复WCS数据库。

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

4. 默认情况下，WCS事件没有被移植。在升级完成后，请输入**start命令的ncs**为了启动NCS服务器。登陆对NCS用户界面用根登录和根密码。此数据没有从WCS被迁移到NCS：报告的子集— AP镜像Predownload， AP配置文件状态、AP摘要、客户端计数、客户端摘要、客户端的流量、PCI报告、PCI法规遵从性被选派的和汇总报告、首选的呼叫网络汇总报告、恶意AP、临时歹徒、新建的临时歹徒和安全汇总报告。控制板自定义客户端工作站统计信息没有带有在Details页客户端图、的客户端，显示板和报告的旧有WCS数据。客户端历史会话信息得到升级。在WCS数据库存储的事件历史记录没有被移植到NCS。在迁移完成后，RADIUS/TACACS服务器IP和凭证没有被移植并且需要再被添加。您在TACACS+/RADIUS需要复制从NCS的最新的自定义属性和包括他们在用户认证/授权的AAA服务器。**注意：** 确保

RADIUS/TACACS服务器启用作为在管理>AAA >AAA模式设置页的AAA模式。有根虚拟域的仅报警从版本7.0被移植到NCS。根密码没有从版本7.0.164.3或7.0.172.0被移植到NCS版本1.1.x.x。在安装应用程序期间，用户必须更改根密码。无根的用户和他们的凭证在迁移时被移植。报警类别和子范畴没有恢复，在对NCS报警摘要以后的迁移。

[从NCS 1.0.x的升级NCS到1.1](#)

您能从NCS版本1.0.0.96、1.0.1.4、1.0.2.28和1.0.2.29升级到NCS 1.1.x.x。

这些项目应该是要注意的在升级进程之前：

- 保证您执行一个备份，在您尝试升级前。
- 禁用高可用性，在您执行升级前。
- 在您执行升级前，请关闭NCS。运行**stop命令的ncs**为了终止NCS。

请使用此命令为了从NCS 1.0升级到NCS 1.1.x.x：

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

在前面的命令，**NCS-upgrade-bundle-1.1.x.x.tar.gz**是升级套件文件，是可用的在[下载软件\(仅限注册用户\)](#)。用于示例的信息库，WCS ftp**回购**，可以是所有有效信息库。这些是信息库配置示例：

FTP信息库：

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

SFTP信息库：

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

TFTP信息库：

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

[从WCS的导入地图](#)

地图出口/导入功能是可用的在WCS 7.0。此功能在[WCS 7.0配置指南](#)详细描述。

在您从您的WCS服务器的export map，您能导入此套在您的NCS服务器后的地图。导入您的地图的步骤在[WCS 7.0配置指南](#)报道。

注意：重要的是在您的WCS服务器的AP首先被添加到您的NCS服务器在导入地图之前，因为在您的WCS地图的AP在出口进程中也包括。未被添加到您的NCS，然而的AP是存在地图导致错误显示的导出的楼层，当您导入那些地图到NCS时。

[高可用性-操作基本理论](#)

在NCS的NCS HA实施允许两个主要的NCS系统故障切换到一第二(备份) NCS。有充足的资源的第二个服务器要求(CPU, 硬盘驱动器, 网络连接)为了接收NCS操作, 在主要的NCS发生故障情况下。在附属NCS的每数据库实例对应的主要的NCS的是一热备件。

使用描述主要的和附属系统的符号是 $N M$, 运转中的主系统 $N =$ 编号和备份主系统附属系统的 $M =$ 编号。

在NCS, 支持这些HA配置:

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

大小辅助服务器一定大于或等于对主服务器, 例如, 如果主要的NCS服务器是中等卵, 然后附属NCS服务器必须是中等或大卵。

主要的和辅助服务器可以是一个物理和虚拟设备的混合。例如, 如果主要的NCS服务器是一个物理设备, 辅助服务器可以是或者物理设备或大卵虚拟设备, 例如, 大卵服务器配置和大小是相同的象物理设备。

健康监控(嗯)是在NCS实现的续签过程, 那是管理系统的HA操作的主要组件。嗯分开成这些多个子模, 其中每一个运用特定的功能:

- 核心嗯—负责对这些任务: 整体HA系统的配置保存HA系统的状态机开始/停嗯和NCS JVM其他子模开始/停和监视器在嗯内的处理首选/备用的对的注册验证嗯特定会话做出关于故障切换和故障回退的所有决策
- 心·跳—心·跳子模块对维护主要的和第二HMs之间的通信负责。通信在HTTPS发生(默认端口是8082)。超时值是2秒。重试机制是设立P-HM和S-HM之间的实现的重试连接。如果嗯不在发送在超时周期的一检测信号请求以后收到答复, 通过发送另一检测信号请求再试建立通信。重试次数总数是3。在通信有不建立后, 在3重试次数, HMs根据定义后的方案采取适当行为: 主服务器断开: 这是经典故障切换事例。在此方案中, 当S-HM不收到检测信号要求6秒(3重试次数x 2秒)时, 它启动在附属NCS的故障切换机制。辅助服务器断开: 在此方案中, P-HM不收到从S-HM的检测信号答复6秒(3重试次数x 2秒)。当这发生时, P-HM更改其状态对 PRIMARY_ALONE, 发出报警并且更改到侦听模式—等待收到从第二的所有消息重新建立的P-HM和S-嗯之间的链路。
- 应用程序箴言报—应用程序箴言报子模块对与NCS框架(NCS JVM)的通信负责在当地服务器获取状态信息。通信是通过在HTTPS的SOAP。
- DB箴言报—DB箴言报子模配置复制的DB。因为这通过数据库所有权复制协议, 是实现的对DB复制不负责。
- 文件同步—文件同步子模有4个子部件: 文件Archiver: 周期地扫描寻找修改了的文件的目录。它收集任何如此文件并且添加他们到TAR存档文件传输代理程序(FTA): 负责对转接压缩TAR存档对目的地(即其他服务器, 主要的对第二或第二对主要的)。文件加载Servlet (FUS): 在辅助服务器的运行和是副本对FTA。当它接收文件时, FUS放出它直接地到TAR提取器而不是创建在本地磁盘的文件(避免多余的磁盘活动)。FTA和FUS在HTTPS通信。统计信息收集器: 保持文件传输操作统计信息从服务器启动的时间的。

没有数据丢失, NCS数据库是系统的核心数据存储存储元件, 并且必须复制在实时-时间的主要的和备份系统之间。这是基本的对NCS HA的操作。数据在1 2种方式中存储:

1. NCS数据库
2. 应用程序数据

应用程序数据是包含此数据的一套展开文件:

- 数据库密码文件：复制在实时(11秒)
- NCS许可证文件：复制通过批处理(每500秒)
- 在tftp根目录下的所有文件：复制通过批处理(每500秒)
- 被安排的生成的报告：复制在实时(11秒)

健康监控：健康监控(嗯)是管理/的主要组件监控系统的HA可用性。有运用与嗯的多种功能的多子模块。

核心嗯：负责对这些谈话：

- 配置HA系统
- 保存HW系统的状态机
- 开始/停嗯
- 开始/停和请监控在嗯内的其他子模
- 处理主要的第二对的注册
- 做出关于故障切换和故障回退的所有决策

[故障切换操作](#)

在NCS以后初始部署，主要的NCS整个配置复制到附属NCS的主机。在正常操作时(即主要的NCS是可操作的)，从主要的数据库复制对附属NCS。

除数据库复制之外，应用程序数据数据文件也复制对附属NCS。复制频率是11秒(实时-时间文件)和500秒(批处理文件)。

[NCS需求为使用NCS HA功能](#)

客户一定运行在主要的和附属NCS服务器的同样NCS版本。NCS HA功能是透明对无线控制器，即没有WLC、AP和MSE的软件版本要求。

[HA功能的配置](#)

在主要的NCS必须配置这些参数：

- 附属NCS的名称/IP地址
- 网络管理员电子邮件地址系统通知的
- 手工或自动故障切换选项

附属NCS必须总是新的安装，并且必须在NCS安装进程中选择此选项。例如，独立或主要的NCS不可能转换到附属NCS。独立NCS可以转换到主要的HA。

注意：在P-NCS和S-NCS之间的数据库复制使用端口1522，因此请保证此端口是开放的在所有网络设备，例如防火墙，交换机，路由器等等，沿主要的和附属NCS服务器之间的网络路径。

[示例-安装和配置过程](#)

在本例中，这是1:1 NCS HA系统

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

第一步将安装和配置附属NCS。当配置HA的时主要的NCS，附属NCS需要是安装和可及的由主要的NCS。

注意：记住的关键点是，当P-NCS运行/可操作时，S-NCS不运行。当辅助服务器在备用模式时，这些服务在辅助服务器运作：嗯、Apache和数据库。当P-NCS去故障状态时，辅助服务器的嗯开始NCS JVM进程。那时执行变得的S-NCS可访问。

健康监控端口在目标NCS安装计算机需要设置。默认端口值是端口8082。此端口号只有本地设备意义(本地设备端口)。

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

必须在安装过程中也创建健康监控的认证密钥。P -嗯和S -嗯内部只使用此密钥验证。它必须是在主要的和辅助服务器的同一密钥。

如陈述前，仅一个NCS服务器许可证需要采购。例如，一个分开的NCS许可证不需要为附属NCS采购。同一NCS许可证文件在主要的和附属NCS驻留。因为NCS JVM在主要的只运行或附属(不是两个)，许可证文件只是活跃的在一个系统在给的此刻。

网络管理员也需要为HA进程的电子邮件通知提供电子邮件服务器设置。这为手工的HA操作(系统管理器干预)要求。导航对此页如下：**管理>Settings >邮件服务器**

[在主要的NCS第二的配置](#)

NCS设置

选择**Administration >高可用性**。如突出显示，HA在此系统当前没有配置。

从在屏幕的左手边的菜单，请选择**HA配置**。这把你带对此窗口。当您输入在一般标题部分的请求的信息并且点击“**Save**” & **启用按钮**时，配置保存，并且HA启用。

您需要输入此信息：S-NCS的IP地址，认证密钥，能将发送的通知的电子邮件地址，故障切换类型。您能选择保存此信息，无需启用HA，或者请保存并且启用HA。

[监控NCS HA操作](#)

在您完成上一步后，在NCS的消息状态信息在HA配置提供信息，并且是否启用。

[健康监控-附属NCS](#)

在附属NCS的健康监控显示器屏幕，您能看到配置附属NCS和故障切换类型的状态信息。并且这允许网络管理员设置日志消息级别类型和能力捕获/下载日志文件。您能也查看与相关的时间戳的S-HM看到的事件。

[主要的失败示例-手工的故障切换](#)

在本例中，附属NCS配置与手工的故障切换。例如，网络管理员通过电子邮件通知主要的NCS体验情况。在附属NCS的健康监控检测主要的NCS故障情况。因为手工的故障切换配置，网络管理员需要手工触发S-NCS接收NCS功能从主要的NCS。如果登录S-HM，这执行。即使S-NCS不运行，S-HM可以连接到通过此语法：

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

S-HM关于被看到的事件显示消息。因为手工的故障切换配置，S-HM等待系统管理员调用故障切换进程。一旦手工的故障切换选定的，此消息显示作为S-NCS开始。一旦故障切换进程完成，因此意味着NCS数据库复制进程完成，并且S-NCS JVM进程开始，然后S-NCS是活动NCS。

在NCS第二的健康监控提供主要的NCS和辅助服务器状态信息。一旦P-NCS从故障情况，恢复Failback可以通过S-HM启动。Failback进程手工总是开始至于避免能有时发生的飘荡情况，当有网络连接问题时。

[Failback](#)

当在主机P-NCS解决了的服务器的的问题，Failback可以手工启动。一旦这执行，屏幕在S-NCS显示。当您启动Failback，在S-NCS的NCS数据库和任何时更改的其他文件，自从S-NCS接收了NCS操作同步在S-NCS和P-NCS之间。一旦数据库同步完成，P-NCS JVM由P-HM开始。当P-NCS JVM运行时，此屏幕在S-HM显示。

[自动故障切换](#)

自动故障切换是一个简单过程。所有配置步骤是相同的，除了自动故障切换选择。一旦配置，网络管理员不需要与S-嗯呼为了故障切换操作能发生。仅在Failback期间是要求的人为干预。

[添加控制器到NCS](#)

- 选择**配置>控制器>Add控制器**为了添加交换机。Cisco无线控制器(WLCs)可以被添加在手工或通过CSV文件。
- 在您添加控制器后，他们在**监视器>未知设备**页临时地安置，当NCS尝试与控制器时联络您补充说。一旦通信用控制器是成功的，控制器从**监视器>未知设备**页移动向**监视器>控制器**页。如果NCS不能用控制器成功通信，在**监视器>未知设备**保持，并且错误情况显示。

[添加交换机到NCS](#)

选择**配置>交换机>Add交换机**为了添加交换机。交换机可以单个被添加或多个交换机可以通过CSV文件导入。

在交换机被添加后，在**监视器>交换机**页临时地安置，当NCS尝试与此交换机时联络。一旦通信用交换机是成功的，NCS移动从**监视器>未知设备**页的交换机向**监视器>交换机**页。如果NCS不能用交换机成功通信，在**监视器>未知设备**依然是，并且错误情况显示。

[Catalyst 交换机配置](#)

有客户端安全配置的三个步骤在思科Catalyst交换机：AAA、RADIUS和802.1x/MAC验证。

AAA配置

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip  
repository ncs-ftp-repo
```

参考的[AAA概述](#)欲知更多信息。

此配置是RADIUS验证的Cisco交换机配置思科ISE/ACS和非Cisco的RADIUS服务器的。

IOS配置

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip  
repository ncs-ftp-repo
```

有关详细信息，请参阅以下文档：

- [RADIUS服务器在失败重拨](#)
- [在访问请求的RADIUS属性8 \(framed-ip-address\)](#)
- [Cisco IOS安全命令参考](#)

802.1X和MAC验证配置—此交换机配置提供三个功能：802.1x客户端的验证，在网络允许出故障802.1x验证的客户端继续(事件生成/发送对失败的802.1x验证的NCS)，MAC验证旁路(MAB)没有802.1x请求方的IP设备的。

Cisco IOS配置

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip  
repository ncs-ftp-repo
```

参考[配置IEEE 802.1X基于端口的验证](#)欲知更多信息。

陷阱的(非标识客户端) MAC通知—此Cisco IOS交换功能转发从交换机的SNMP陷阱到NMS，例如，NCS服务器，MAC通知的，non-802.1x客户端。

Cisco IOS配置

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip  
repository ncs-ftp-repo
```

调试Debug snmp packets命令

显示Show mac命令地址表通知更改

参考[配置MAC修改提示陷阱](#)欲知更多信息。

Syslog配置(只有标识客户端) —此配置转发系统消息从Catalyst交换机到NCS服务器。

IOS配置

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip  
repository ncs-ftp-repo
```

[无线网络规划](#)

[计划的工具](#)

嵌入规划工具为确定的什么网络管理员提供一个方式在无线网络的部署要求。作为计划进程一部分，多种标准输入到规划工具。完成这些步骤：

1. 指定AP前缀和AP放置方法(自动与指南)。
2. 选择AP类型并且指定2.4GHz和5GHz的天线波段。
3. 选择协议(波段)和最低希望的吞吐量每个为此规划要求的波段
4. 启动预先的选项的规划模式数据的，语音，位置。数据和语音为设计帮助提供安全限度。安全限度帮助为特定的RSSI阈值设计，在线帮助被选派。位置同监控模式在可能部署增添位置准确性的AP析因。位置比数据和位置复选框帮助对通告的位置准确性典型地要求一更加密集的部署计划。
5. 需求和覆盖选项允许计划对有高密度客户端在线状态这样会议室或教室的所有特殊情况。生成的建议包含这些：平面图详细信息免责声明/范围/假定报价的AP放置覆盖和数据速率
Heatmap覆盖分析

[地图编辑器](#)

在NCS帐户对象的和阻碍的集成地图编辑器在楼层。楼层地图特性的修改导致在预测热量地图显示的一个更加准确的RF传播型号。对象和阻碍帮助预测引擎的衰减特性显示一张更加可实现的预测热量地图。编辑做难倒地图帮助指定区域和地区例如：

- 用于位置通知和标记—的覆盖区域
- 周边—定义了外边界
- 位置用于位置事件和通知—的包括和排除区域

可能指定的对象和阻碍：

- 墙壁(灯和大量) -2db和13dB
- 房间(墙壁) -1db
- 门(灯和大量) — 4dB和15dB
- 玻璃(门、windows，墙壁) — 1.5dB

[导入地图从WCS到NCS](#)

地图出口/导入功能是可用的在WCS 7.0。此功能在[WCS 7.0配置指南](#)详细描述。

在地图的出口从来源WCS服务器的，此套地图可以导入到目的地NCS服务器后。导入您的地图的步骤在NCS配置指南报道。

注意：重要的是在WCS服务器的AP首先被添加到NCS服务器在导入地图之前，因为在WCS地图的AP在出口进程中也包括。未被添加到您的NCS，然而的AP是存在地图导致显示的错误的导出的楼层，当您导入那些地图到NCS时。

[请使用NCS部署无线局域网](#)

[配置模板](#)

配置模板是可能应用到在系统或全局级别的设备的套配置。他们可以被重新使用为了修改现有配置。模板可能也用于复制配置到随后被添加的其它设备。配置模板可以用于安排设置更改在预定义的日期和时间。在NCS的审计功能能也有效利用设置模板确定在NCS和现有控制器配置之间的设置区别。

[配置组\(设置组\)](#)

设置组是逻辑上分组控制器的简单的方法。此功能提供一个方式管理有相似的配置的控制器。模板可以从现有控制器解压缩设置新建的控制器或现有控制器有更多的配置参数的。设置组可能也使用从设置安排配置集。控制器重新启动可能根据操作要求也被安排/层叠。使用设置组，移动组，DCA和控制器配置审计可能也管理。

设置组使用，当一起分组站点更加容易的管理(移动组、DCA和管理域设置)时和安排的远程配置配置更改。分组站点保证遵照配置策略。

- 添加控制器—提交在WCS的控制器并且可以最近移过去向配置组
- 应用模板—已发现或已经现在模板可能然后应用到控制器
- 审计—保证基于模板的审计选择在审计设置然后审计控制器在组中保证他们符合策略

[监控的使用NCS/排除故障无线网络](#)

[RRM /CleanAir](#)

两个RF配置文件创建模板的NCS版本1.1和AP组模板支持RF配置文件和组。如果使用NCS 1.1通过模板的创建创建RF配置文件，这给管理员简单方法一致创建和运用模板对控制器的组。进程流同样先前讨论在与一些较小，但是重要差异的控制器特性组。

进程如前所论及是相同的您首先创建RF配置文件，然后通过AP组应用配置文件。差异在这如何执行从NCS和在使用模板部署在间网络。

[建立与思科最初NCS 1.1的RF配置文件](#)

在思科最初NCS有两种方式您能接近建立或管理RF配置文件。选择**配置>控制器> (控制器的IP地址) > 802.11 > RF配置文件**为了访问一个单个控制器的配置文件。

这当前显示所有RF配置文件在选定的控制器并且允许您做对配置文件或AP组分配的变动。关于当前应用给AP组的配置文件的同样限制实际上是和控制器GUI。您必须禁用网络或非分配从AP组的RF配置文件。

当您创建新配置文件时，NCS提示您选择现有的模板。如果这第一次是访问，您处理对802.11控制器模板的模板创建对话。

选择**配置>控制器模板跳板> 802.11 > RF配置文件**为了直接地去控制器模板跳板。

在两种情况下，一新的RF配置文件在NCS创建通过使用模板。因为允许管理员有效利用NCS workflow和运用模板和配置到所有或选择控制器的组和减少配置错误和不匹配，这是首选方法。

完成这些步骤：

1. 为了创建RF配置文件模板，请选择新：
2. 模板/设置的配置是几乎相同的增加模板名称。在将来使此说明性为容易识别。更改设置当必要时或要求并且选择**保存**。**注意**：如果选择TPCv2的一阈值，并且它不是RF组的选定的TPC算法，则此值忽略。**注意**：更改的一简单设置为验证是最低的TPC电源。最低的电源可以被上升，如果选择比RRM分配的当前功率电平是更多的dbm值。这帮助验证RF配置文件操作。

3. 一旦压下保存在底部的选项的屏幕更改选择**适用于控制器**，并且控制器对话框看上去显示此NCS服务器管理的控制器列表。
4. 选择保存设置闪烁，选择控制器您希望有配置文件联机，并且选择**保存**。
5. 现在，当您查看RF配置文件屏幕时，您能看到创建的新的模板。上一个步骤可以被重复为了创建和申请另外的模板如所需求，例如，802.11b。

应用RF配置文件给有NCS的AP组

如同RF配置文件的WLC配置，他们分配的新建立的配置文件可以应用到一个控制器通过使用AP组。为了执行此，以前可以使用已保存AP组VLAN模板或新建立的模板。

选择**配置>控制器模板跳板**并且选择**AP组VLAN**。

为了创建一个新的模板，请选择**新**并且填写必填信息。

选择**RF Profiles**选项为了添加RF配置文件。

如果保存模板，警告消息出现。

如上一条留言所述，已分配WLAN使用接口的更改打乱在此组中AP VLAN映射应用的FlexConnect的。保证接口是相同的，在您继续前。

一旦选择**好**，对话用选项**适用于替换控制器**。选择此选项。

选择模板需要应用的控制器。

NCS回应运行状态模板是否顺利地应用到选定控制器。

如果模板未顺利地推送，NCS提供陈述失败的原因的一个消息。在本例中，应用给组的RF配置文件不是存在模板应用的其中一个控制器。

再，特别地适用于RF配置文件该控制器然后重新应用AP组为了生成一个成功的消息。

一旦AP组配置有应用的RF配置文件(请选择**应用到接入点按钮**)，只有附加的接入点对AP组成功部署的控制器是可用选择从。

注意：到此为止，包含新的RF配置文件的实时变动未做对RF基础设施，但是这更改，当AP搬入组时。当AP移动到或在AP组外面，AP重启为了占去新的配置。

选择AP为了添加到AP组和选择**好**。警告消息出现。

NCS显示更改的状况。

请使用NCS对修正问题

- CleanAir
- 客户端故障排除
- 审计工具
- 安全控制板
- SPT

请使用NCS优化无线网络的操作

- 报告
- 无线网络性能(RRM)
- 性能(WAN带宽)

控制板

控制板组件在NCS 1.0被提高了那里是一定数量的增强到主页组件：

- 有线的/无线集成：组件也当前显示有线的客户端和交换机信息
- 组分自定义 workflow：什么可以定制，如何定制
- 独立组件可以刷新。刷新率可以单个配置。
- 组件和主页自定义方便：所有编辑直接地在主页(没有需要完成导航到Edit页)。组件的添加的/移动鼠标拖放
- 直观 workflow：组分超链接提供定位方便，即客户端验证分配给已过滤客户端列表页

这些是控制板的主要用户自定义：

- dashlet拖放：组件在页可以被重新整理
- 添加/删除显示板：添加/删除新建的选项卡
- 控制板重拔
- 控制板重命名
- 编辑布局：能指定dashlets的列数，dashlets的添加/删除
- 重命名dashlets
- dashlet多个实例：用户能添加同样dashlet和定制在每一个的内容
- 用户可配置的控制板布局：在页的列数组件的

Dashlet自定义：

- 手工的刷新：允许用户刷新各自的dashlet内容
- 编辑dashlet名称
- 调整大小：最小化(请减少题为和状态栏)，恢复(对原始尺寸的恢复)，最大化(活动dashlet占用控制板区域)
- 分开：分开/重新显示在新窗口的dashlet内容
- close：从控制板删除dashlet。能通过“添加Dashlet”屏幕再被添加
- 多个显示选项：图表或表
- 显示的目视指示器dashlet是否定制。

单个观点的dashlet的有线的/无线客户端

有在有线的/无线客户端提供信息的十一个dashlet组件：

- 由关联/验证的客户端计数
- 由无线的客户端计数/配线
- 客户端流量
- 客户端报警和事件汇总
- 客户端流量
- 客户端故障排除
- 客户端状态状态

- 库存详细信息状态
- 设备正常运行
- 由CPU利用率的名列前茅5设备
- 由存储器利用率的名列前茅5设备

有线的dashlets

- 有线的客户端速度分配
- 由客户端计数的名列前茅5交换机

[区域图的自定义](#)

在dashlets的图类似客户端由无线计数/配线，并且由关联验证的客户端计数有取决于图临时过滤器柱状图选择在过滤器柱状图有所有/无线/电线”并且关联/验证的多个区域区域图，分别因为选项。被看到的区域图可以重叠(多个区域互相交叉)或被堆积(多个区域垂直被堆积-一个在其他)。征兆是否被堆积或重叠沿着Y轴标题显示。不同种类的原因的视图(被堆积或重叠)是给予用户显示的数据集的更加好的征兆。

[监控客户端和用户](#)

NCS提供能力监控配线和无线客户端(监视器>客户端和用户)。这在网络提供统一的观点的所有客户端。这些过滤器是可用的。

默认情况下在对客户端和用户列表的定位时页，所有相关的客户端显示。有允许用户查看客户端的一子集的14个现在过滤器。细节在表里提供。另外，有选项创建自定义过滤器：

- 快速过滤器
- 先进的过滤器

客户端列表过滤器	
过滤器	结果
所有	所有客户端包括非激活
2.4GHz客户端	使用2.4 GHz无线频段的所有活动无线客户端
5GHz客户端	使用5.0 GHz无线频段的所有活动无线客户端
所有轻量级客户端	所有客户端连接对轻量AP
所有自治客户端	所有客户端连接对自治AP
所有有线的客户端	NCS直接地连接的交换管理所有客户端
相关的客户端	所有客户端连接不管是否它验证
MSE检测的客户端	MSE检测的所有客户端包括有线的和无线
在为时检测的客户端 24个小时	在为时检测的所有客户端24个小时
有问题的客户端	关联的客户端，但是未完成策略。
排除的客户端	控制器被排除的所有轻量级无线客户端

本地验证的H-REAP	客户端连接对H-REAP AP并且验证本地
在为时检测的新的客户端24个小时	所有在为时检测的新建的客户端24个小时
运行客户端	完成所有集合策略并且在运行状态的客户端。
WGB客户端	所有WGB客户端

在客户端列表表的列直接地在此页可以定制。

在客户端列表表的列直接地在**客户端**和用户列表可以定制页。选择或取消选择列为了立即显示或隐藏列。

默认套显示的列，并且他们的顺序可以是Reset to Default值通过**reset**按钮。

按顺序o请重拨列，扯拽列直接地在页并且搬到它希望的命令/位置。

客户端和用户页：列详细信息	
属性	备注
IP Address	客户端 IP 地址
Mac 地址	客户端 MAC 地址
用户名	根据802.1x验证的用户名。未知为客户端显示连接，不用用户名
类型	图标代表轻量，一个自治或一个有线的客户端。
供应商	从OUI派生的设备供应商
AP 名称	仅无线
设备名	网络验证设备名，即WLC，交换机。
地图位置	连接的设备的地图位置。
状态	最新的客户端状态状态
SSID	仅无线
配置文件名称	仅无线
VLAN	VLAN设备打开
状态	当前客户端状态
接口	控制器接口(无线)或交换机接口(有线)该客户端是连接。
协议	有线的802.11 -无线802.3 -。
速度	-只有线的以太网端口速度。显示“N/A”无线的
关联时间	最后AP关联开始时间，仅无线
会话长度	会话长度
认证类型	WPA、WPA2、802.1x等等。
授权类型	从ISE的有线的授权类型
流量(MB)	流量(传送/接收)在MB的此会话上
平均的会话吞吐量(Kbps)	平均的会话吞吐量在Kbps

自动化的测验运行	指示客户端是否是在自动测试模式
AP MAC地址	仅无线
AP IP地址	仅无线
锚控制器	仅轻量级无线
运行	客户端完成所有集合策略。
CCX	仅轻量级无线
客户端主机名	有线的和无线。DNS反向查找结果。
设备的 IP 地址	连接的设备(WLC的IP地址、交换机或者aIOS AP)。
波尔特	在WLC的Switchport
E2E	仅轻量级无线。
加密密码器	仅无线
MSE	管理此客户端的MSE服务器
RSSI	仅无线
SNR	仅无线
会话 ID	用于ISE和交换机的审计会话ID
会话时间	激活的会话会话启动时间会话结束时间的 会话开始时间非激活会话的
出售商名称	从OUI获得的出售商名称

工具栏客户端/用户列表提供在选定的一套工具(一个或更多)客户端可以被调用。

监视器>客户端和用户：支持的命令	
命令	客户端的类型
排除故障	所有
Test菜单	
林克测验	仅轻量级无线
无线电评定	仅轻量级无线
V5统计信息	仅轻量级CCX v5无线
操作参数	仅轻量级CCX v5无线
禁用	仅轻量级无线
删除	仅轻量级无线
更多菜单	
配置文件	轻量(CCXv5)
漫游原因	仅轻量级无线
最近的地图	仅轻量级无线
现在地图	仅轻量级无线
塞申斯	所有
检测AP	仅轻量级无线
位置历史记录	仅轻量级无线
Enable (event)镜像模式	仅轻量级无线
语音量度	仅轻量级无线
跟踪客户端	仅轻量级无线

识别未知客户端	所有
---------	----

示例操作：操作参数

对左手边的单选按钮选择特定的客户端显示在此客户端列表的客户端详细信息。

轻量级无线客户端

有线的客户端

在此屏幕画面，列表的底部的客户端是轻量无线客户端(类型：轻量级无线)。

示例是为有线的客户端。

[有线的/无线客户端故障排除](#)

在NCS 1.0，有线和无线监听和故障排除集成与身份服务。在有线的/无线网络管理之间的集成通过三网元达到：

- Cisco无线LAN控制器(WLC)
- Cisco Catalyst交换机安全功能：AAA、RADIUS、802.1x和MAC验证，MAC通知陷阱(非标识客户端)，Syslog (只有标识客户端)
- 思科身份服务引擎(ISE)

所有客户端-有线的和无线-在客户端和用户页显示([监视器>客户端和用户](#))。

有线的客户端显示AP名称作为N/A.交换机端口信息在[接口](#)提供。

[无线客户端故障排除](#)

为了启动客户端故障排除工具，请在客户端列表项目左边点击单选按钮。一旦客户端选择，请点击在工具栏的[故障排除](#)图标。

窗口为客户端显示。

日志消息可以从有使用的控制器被检索日志分析工具。

参考的[策略执行模块\(PEM\)](#)关于PEM状态的更多信息。

事件历史记录工具提供用户从客户端和AP的事件消息。

测试分析工具(CCXv5客户端)

[有线的客户端故障排除](#)

NCS 1.0提供有线的和无线设备/客户端集成管理。其中一个在NCS 1.0的主要功能是监控和排除故障为有线的和无线客户端。SNMP用于发现客户端和收集客户端数据。ISE周期地轮询收集客户端统计信息和其他属性填充相关控制板组件和报告。

如果ISE被添加到系统，并且设备验证对它，客户端选派的页显示作为安全被标记的其他详细信息。

为了导航到客户端故障排除页，请点击在工具菜单的[故障排除](#)图标在页顶部。

这把用户带对在屏幕画面显示的页。在本例中，客户端设备有链路连接，但是失败的MAC验证。

在屏幕的右边是与这些项目的一个工具栏所有相关对排除故障：

- 客户端故障排除工具
- 日志分析
- 事件记录
- 上下文意识历史记录

事件历史记录为此客户端提供与连接事件涉及的消息。在本例中，客户端失败成功验证。日期/时间是提供的协助排除故障的此客户端网络管理员。

ISE提供验证记录给NCS通过其余API。网络管理员能选择获取的验证记录时间从ISE。在本例中，验证记录表明用户在ISE数据库未找到。

[RF/Wireless功能](#)

[跟踪客户端](#)

当这些客户端连接对网络时，此功能允许网络管理员跟踪特定客户端和通知。此功能从监视器>用户和客户端页启用。

要跟踪单个客户端，请点击**Add按钮**，并且子窗口出现用户能与跟踪有效期一起的地方输入客户端的MAC地址(从未或指定的结束日期)。

如果用户要跟踪广泛客户端，客户端列表可以导入。发生的窗口允许用户对客户端MAC地址海关进口货物分类表通过CSV文件。

示例CSV文件可以下载提供数据格式。

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

[通知设置](#)

有通知的三个选项：

1. 清除的已到期条目—用户在NCS数据库能设置持续时间保留被跟踪的客户端。客户端可以清除：
：在1周之后在2周之后在1个月之后在2数月之后在6数月之后无限地保持
2. 通知频率—用户能指定，当NCS发送被跟踪的客户端的通知时：在第一检测在每检测
3. 通知方法—用户能指定为了被跟踪的客户端事件能生成报警或发送电子邮件。

[显示被跟踪的客户端](#)

在被跟踪的用户信息输入后，被跟踪的客户端窗口允许用户查看存在被跟踪的客户端状况。

[未知用户ID](#)

不是所有的用户/设备通过802.1x (即打印机)验证。在此事件，网络管理有选项分配名称到设备。

如果客户端设备验证通过网络通过Web验证，WCS可能没有该客户端的用户名信息。在此方案中，客户可能要有用户名被映射对客户端，即使他们使用Web验证。

1. 选择**监视器>客户端**。无线和有线的客户端显示。如前所述，工具栏在允许用户调用一定数量的操作客户端的上一个列表查找：排除故障测试(链路测验、无线电测量、CCXv5统计信息，操作参数)禁用删除(请取消关联无线客户端)
2. 点击在工具栏的**识别未知用户**图标。这用弹出窗口结果。
3. 单击**添加**为了输入客户端详细信息。单个MAC地址和对应的用户名可以被添加。一旦客户端和MAC地址被添加了，WCS使用此表根据匹配MAC地址的客户端查找。

[实时热量地图](#)

其中一在NCS 1.0的新特性，是选项显示实时热量地图。默认情况下启用该接口。选择**监视器>地图>Properties**为了导航到设置。

[监控思科Catalyst交换机使用NCS](#)

这些方法取决于有线的库存信息：

- 有线的客户端发现通过SNMP陷阱、SNMP轮询和系统消息从交换机
- 其他信息的ISE向北的API，例如状态，仿形铣床，核算，等等

NCS与WCS 7.x客户端监听的和报告的提供功能奇偶校验在所有客户端(有线和无线)。另外，NCS排除故障为有线的客户端的交叉启动ISE。进一步级别ISE集成是通过ISE报告交叉启动与在WCS没包含的数据的。

此交换机信息在NCS被提供：

- 实物资产，例如，机箱、模块、端口和电源从实体MIB
- 闪存设备/分区/文件
- 软件安装的镜像
- 以太网接口
- IP接口
- VLAN接口
- VLAN和VTP
- EtherChannel
- STP
- Stackwise (仅支持Cisco Catalyst 3750交换机)

监视器>交换机显示此交换机信息：

- IP 地址
- 设备名称：主机名如给在交换机IOS配置方面
- 设备类型：交换机型号
- 可接通性：SNMP连接
- 客户端计数：客户端编号直接地连接对交换机

显示的IP地址是超链接，并且单击对此采取用户**配置>以太网交换机>(IP地址)>汇总屏幕**。

有线的客户端通过SNMP陷阱、SNMP轮询和系统消息发现从交换机。

使用NCS，思科Catalyst交换机可以监控对于此信息：

- 机箱：UDI，模型名称，正常运行
- Memory/CPU利用率
- 端口/接口状态
- Layer2 (VLAN，VTP，生成树)
- 环境：电源状态和风扇
- 内存和文件在系统
- 客户端(有线)

[生成树](#)

提供每个生成树实例的生成树细节：

- STP波尔特
- 端口角色
- 端口优先级
- 路径成本
- 端口状态
- 端口类型

[思科Stackwise](#)

对于支持Stackwise技术的思科Catalyst交换机，其中每一交换在堆叠的角色提供包括其在堆叠的角色，交换优先级、状态和软件版本。

接口详细信息

关于所有以太网接口的状态信息显示。

也提供第3层信息(对映射的IP子网的VLAN)。

[VLAN资讯台](#)

VLAN详细信息从NCS也是可得到。系统默认和用户配置的VLAN显示。VLAN ID、名称和类型在单银幕显示。

[客户端列表页](#)

[报告\(交叉启动和缩放\)](#)

NCS 1.0提供有线的和无线设备/客户端集成管理。SNMP用于收集客户端数据。ISE周期地轮询收集客户端统计信息和其他属性填充相关报告。

选择**报告>报告跳板**。选择创建/自定义的报告。

[新的报告](#)

前N个连接

这报告显示根据这些量度的一个给的时期的前N个用户：

- 连接尝试
- 合格尝试
- 失败的尝试

此报告包含这些列：

- 用户名
- 总连接尝试编号
- 合格连接尝试编号
- 失败的连接尝试编号

AP关联

此报告目录无线客户端的所有AP关联详细信息和类似于客户端会话报告。

状态状态计数

此报告提供一趋势图表随着时间的推移显示客户端状态状态。图表是区域图;底下区域是客户端数量通过状态检查，并且顶端是失败状态检查客户端的数量。

[报警/事件](#)

报警和事件为有线的和无线提供报警和事件一张单页的视图。不变报警摘要和浏览器在屏幕的右下显示不管什么屏幕用户是在。NCS 1.0提供通用的报警视图包括这些页：

- 报警列表页
- 报警详细信息页
- 事件列表页
- 事件详细信息页
- 报警搜索按类别&子类别
- 报警摘要窗口
- 报警控制板
- 报警操作(请确认，清除，分配，unassign、删除等等)
- 告警通知(电子邮件，陷阱)
- 报警页定位(从和对不同的视图)
- 报警概述面板-对已过滤列表的drilldown
- 从报警页的启动现有WCS故障排除页

列可以定制例如显示，隐藏和重拨。行动在一个或更多报警可以同时采取。

[快速过滤器](#)

此功能在根据文本字符串的一个或更多列允许用户过滤输入在过滤器被归档在每列顶部。它为有线的和无线报警提供报警一张可选已过滤视图。

报警页-快速过滤器

[先进的过滤器](#)

先进的过滤器提供更加了不起的搜索功能。它在特定字段提供能力搜索以多种条件，例如包含，不包含，开始从，并且结束与。此图表显示多种过滤器选项。另外，提前的过滤器允许将指定的情况和布尔(并且/或者)情况嵌套。

报警页-先进的过滤器

同样地，事件可以显示和过滤器容易地。它也预先设定，快速和先进的过滤器。这些过滤器以与这些相似的方式工作在报警的同样过滤器。

[事件页](#) [事件页-快速过滤器](#) [事件页-先进的过滤器](#)

[AAA用户认证通过TACACS+/RADIUS使用ACS 4.2](#)

为了使TACACS+用户成功验证在NCS，一些个变化要求在ACS 4.2上。新的服务NCS HTTP在Interface Configuration页需要被添加TACACS+(Cisco IOS)。

如AAA用户的，屏幕画面所显示整个套NCS用户组任务列表TACACS+自定义属性在NCS HTTP自定义属性正文需要复制。同样对负有益于用户组。

对于RADIUS用户验证，您需要复制在思科IOS/PIX 6.x RADIUS属性部分的新的NCS用户组任务列表Radius自定义属性用户/用户组的。

从NCS，请添加在**管理>AAA > TACACS+服务器/Radius**的新的TACACS+/Radius服务器项。相应地设置在**管理>AAA > AAA模式设置**的AAA模式为TACACS+/Radius。重新登录作为AAA用户。

[相关信息](#)

- [技术支持和文档 - Cisco Systems](#)