思科业务新员工：设备和基本网络术语表

目标

本文档旨在让初学者熟悉思科企业（S系列）设备和一些您应该了解的一般术语。主题包括硬件可用、思科业务条款、一般网络条款、思科工具、数据交换基础知识、互联网连接基础知识和网络，以及它们如何结合。

简介

您是否刚刚开始使用思科设备建立网络？进入建立和维护网络的全新世界，将是一件不堪重负的事情。本文旨在帮助您熟悉一些基本知识。你知道的越多，就越不令人生畏！

思科业务提供的硬件

路由器

路由器将多个网络连接在一起，并将数据路由到需要的地方。它们还将这些网络上的计算机连接到Internet。路由器使所有联网计算机共享一个Internet连接，从而节省资金。

路由器充当调度程序。它分析通过网络发送的数据，选择数据传输的最佳路由，然后将其发送出去。

路由器将您的企业与世界连接起来，保护信息免受安全威胁，甚至可以决定哪些计算机优先于其他计算机。

除了这些基本的网络功能，路由器还附带了更多功能，可使网络更简单或更安全。例如，根据您的需求，您可以选择具有防火墙、虚拟专用网络(VPN)或互联网协议(IP)通信系统的路由器。

最近开发的Cisco Business路由器包括RV160、RV260、RV340和RV345系列。

交换机

交换机是大多数企业网络的基础。交换机充当控制器，将计算机、打印机和服务器连接到建筑物或园区的网络。

交换机允许网络上的设备相互通信，也允许其他网络通信，从而创建共享资源网络。通过信息共享和资源分配，交换机可节省资金并提高工作效率。

在网络基础知识中，有两种基本的交换机类型可供选择：托管和非托管。

> 非托管交换机开箱即用，但无法配置。家庭网络设备通常提供非管理型交换机。
> 可以配置托管交换机。您可以在本地或远程监控和调整受管交换机，从而更好地控制网络流量和访问。

有关交换机的更多详细信息，请查看交换机术语表。

最新开发的交换机包括思科业务交换机CBS110、CBS220、CBS250和CBS350系列。

如果您想了解CBS交换机之间的区别，请查看

无线接入点

无线接入点允许设备无需电缆即可连接到无线网络。无线网络使新设备易于联机，并为移动员工提供灵活的支持。

接入点充当网络的放大器。当路由器提供带宽时，接入点会扩展带宽，使网络能够支持许多设备，而且这些设备可以从更远的地方访问网络。

但接入点不仅仅是扩展Wi-Fi。它还可以提供有关网络中设备的有用数据，提供主动安全性，并服务于许多其他实际用途。

最近开发的无线接入点Cisco Business Wireless包括AC140、AC145和AC240，支持无线网状网络。如果您不熟悉网状无线网络，可以在欢迎使用思科企业无线网状网或Cisco企业无线网络常见问题(FAQ)中阅读更多内容。

如果您想了解无线接入点的一些常见术语，请查看WAP术语表。

多平台电话

MPP电话使用会话初始协议(SIP)提供IP语音(VoIP)通信。 这样就无需使用传统电话线，使电话在公司内更加便携。使用VoIP时，电话使用现有的网络基础设施和互联网连接，而不是昂贵的T1线路。这样，就能够用更少的“线路”管理更多呼叫。 其他有益选项包括保留呼叫、暂留呼叫、转接呼叫等。除VoIP外，某些型号还允许视频通信。

MPP电话的设计与普通电话类似，仅用于此目的，但本质上，它们是计算机，属于您的网络。MPP电话需要来自互联网电话服务提供商(ITSP)或IP专用分支交换(PBX)呼叫控制服务器的服务。WebEx呼叫、振铃中心和Verizon是ITSP的示例。与Cisco MPP电话

配合使用的IP PBX服务的一些示例包括星号、中心和Metaswitch平台。这些电话上的许多功能都是通过第三方提供商（如FreePBX）专门编程的，因此流程（停车、访问语音信箱等）可能有所不同。

最近开发的思科企业MPP电话包括6800、7800和8800系列。

思科业务中常用

管理指南和快速入门指南

这是两种不同的资源，可供搜索，以获取有关您的产品及其功能的非常详细的信息。使用型号执行站点或网络搜索时，可以添加一个或另一个以查看这些较长的指南。

默认设置

设备具有预选的默认设置。它们通常是管理员最常选择的设置。您可以根据需要更改设置。

默认用户名和密码

在较旧的思科企业设备中，用户名和密码*的默*认值为admin。现在，大多数用户的用户名和密*码都*默认为cisco。在IP语音(VoIP)电话上，您需要以管理员身份登录以*更改*许多配置。强烈建议您将密码更改为更复杂，以确保安全。

默认IP地址

大多数思科设备都提供路由器、交换机和无线接入点的默认IP地址。如果您不记得IP地址，并且没有特殊配置，可以使用打开的回形针在设备上按重置按钮至少10秒。这将重置为默认设置。如果您的交换机或WAP未连接到启用了DHCP的路由器，并且您直接连接到交换机或计算机的WAP，则这些是默认IP地址。

思科企业路由器的默认IP地址是192.168.1.1。
思科企业交换机的默认IP地址为192.168.1.254。
小型企业无线接入点(AP)的默认IP地址是192.168.1.245。新网状无线接入点没有默认IP地址。

重置为出厂默认设置

有时，您可能希望将思科企业路由器、交换机或无线接入点重置为出厂默认设置并从头开始。当您将设备从一个网络移动到另一个网络时，这种方法非常方便，或者，当您无法解决配置问题时，这是最后的选择。重置为出厂默认设置时，将丢失所有配置。

您可以备份配置，以便在出厂重置后恢复配置。有关详细信息，请点击以下链接：

- 通过基于Web的实用程序重新启动或恢复RV34x系列路由器的出厂默认设置
- 交换机上的备份和恢复或交换固件

- 在无线接入点上下载、备份、复制和删除配置文件
- 管理WAP125或WAP581接入点上的配置文件

如果不备份配置，则需要从头开始重新设置设备，以确保您拥有连接详细信息。大多数型号都有文章详细介绍重置要遵循的步骤，但最简单的方法是使用打开的回形针，并在设备上按重置按钮至少10秒。这不适用于MPP电话，因此请选中重置Cisco IP电话以了解详细信息。

Web用户界面(UI)

除100系列非管理型交换机外，思科企业设备的每件设备都配有Web UI。

此类型的接口（您在屏幕上看到的）显示了选择选项。您无需知道任何命令即可浏览这些屏幕。Web UI有时也称为图形用户界面(GUI)、基于Web的界面、基于Web的指导、基于Web的实用程序或Web配置实用程序。

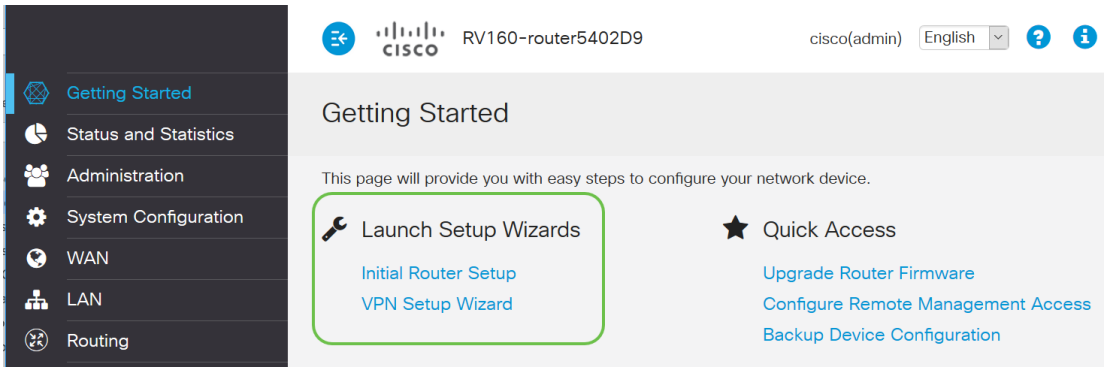
更改设备配置的最简单方法之一是通过Web UI。Web UI为管理员提供了一个工具，其中包含可更改以修改设备性能的所有可能功能。

登录思科设备后，您将看到Web UI屏幕，其中左侧包含导航窗格。它包含设备的顶级功能列表。导航窗格有时也称为导航树、导航栏或导航地图。

根据设备和固件版本的不同，此页面的颜色和顶级功能可能有所不同。

设置向导

这是一个交互式屏幕，在您首次登录思科S系列设备时，您将导航该屏幕，可能在此之后。它是让您在网络上正常运行的绝佳方式。预先选择了多个可更改的默认设置。某些设备带有多个安装向导。此示例显示两个设置向导、*初始路由器*设置和*VPN设置向导*。



Cisco 专有

由思科专门开发和拥有。例如，思科发现协议(CDP)是思科专有协议。通常，思科专有协议只能用于思科设备。

系列中的型号

思科为小型企业所有者提供多种不同的型号，以满足其公司的需求。通常，提供的型号具有不同的功能、端口数、以太网供电甚至无线。如果系列中有多个型号，思科将设置

一个x来代替不同型号的数字或字母，但该信息适用于该系列中的所有型号。例如，RV34x系列中提到路由器RV340和RV345。如果设备的末端有P，则提供以太网供电。如果设备名称以W结尾，则它提供无线功能。通常，型号数量越多，设备的功能就越高。要查看有关此项的详细信息，请查阅以下文章：

- 产品解码器环 — 路由器
- 产品ID解码器 — 交换机
- 产品解码器环 — WAP
- 思科业务无线型号解码器（网状无线）

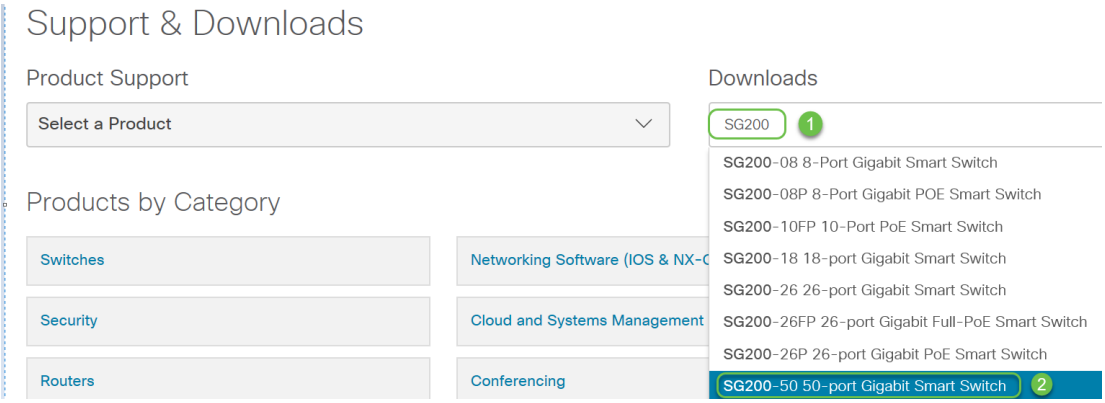
固件

也称为图像。控制设备操作和功能的程序。

升级固件

升级固件对于每台设备的最佳性能至关重要。发布升级时安装升级非常重要。思科发布固件升级时，通常包含一些改进，例如新功能或修复可能导致安全漏洞或性能问题的漏洞。

转到Cisco Support，并在“Downloads”下输入需要升级的设备的*名称*。应显示下拉菜单。向下滚动并选择您拥有的特定型号。



提示：查看各种版本的思科固件时，每个固件都采用x.x.x.x格式。这些二进制八位数被视为四个二进制八位数。当有次要更新时，第四个二进制八位数会改变。第三个二进制八位数在更大变化时会改变。第二个二进制八位数表示重大更改。如果第一个二进制八位数是彻底修改，则它会改变。

如果需要指导，请点击此链接以在任何设备上下载和升级固件。

本文提供一些故障排除思想，以防您遇到交换机升级问题：在200/300系列交换机上升级固件。

一般网络术语

一旦您拥有了设备，您就应该熟悉网络中的一些常见术语。

接口

接口通常是指系统之间的空间。可与计算机通信的任何设备，包括端口。通常为网络接口分配本地IP地址。用户界面允许用户与操作系统交互。

节点

一个通用术语，用于描述在网络内建立连接或进行交互的任何设备，或者可以发送、接收和存储信息、与Internet通信并具有IP地址的任何设备。

主机

主机是网络上通信的终端设备，主机可以向其他节点提供数据或服务（如DNS）。根据拓扑，交换机或路由器可以是主机。所有主机也是节点。示例包括计算机、服务器或打印机。

计算机程序

计算机程序携带可在计算机上运行的指令。

应用

应用程序软件是帮助您执行任务的程序。由于它们相似，因此它们通常被互换使用，但并非所有程序都是应用程序。

最佳实践

用于设置和运行网络的推荐方法。

拓扑

设备的物理连接方式。网络图。

配置

这是指事物的设置方式。您可以保留默认设置，即在购买设备时预配置的设置，或者可以根据特定需求进行配置。默认设置是基本配置，通常推荐。登录设备时，可能会有一个安装向导来指导您完成操作。

Mac 地址

每台设备的唯一标识符。位于物理设备上，可通过Bonjour、LLDP或CDP检测。交换机在与设备交互时跟踪设备上的MAC地址并创建MAC地址表。这有助于交换机知道将信息包路由到何处。

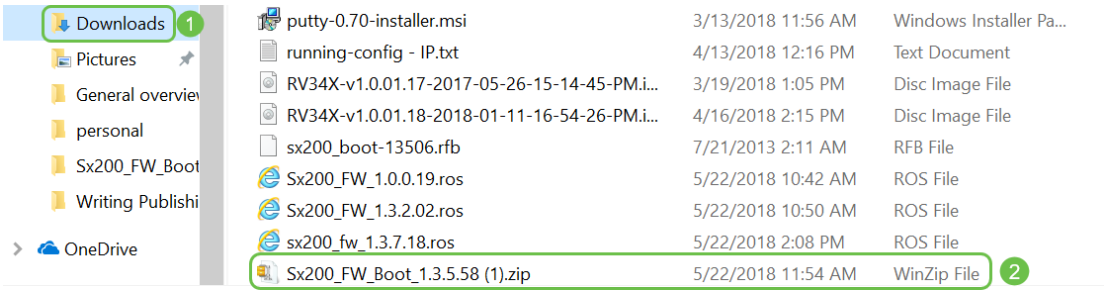
开源

一个向公众免费提供的计划。

Zip文件

一组文件压缩到一个zip文件中。当您想在一个步骤中传输多个文件时，会使用它。接收方可以打开zip文件并分别访问每个文件。zip文件以.zip结*尾*。

如果看到以.zip结尾的格式的文件，*则*必须解压该文件。如果您没有解压程序，则需要下载一个。在线提供多种免费选项。下载解压程序后，单击“下**载**”并找到解压*所需*的.zip文件。



右键单击zip文件的名称，屏幕将显示类似此的屏幕。将鼠标悬停在解压软件上，然后选择“**Extract Here**”。在本例中，使用7-Zip。

命令行界面 (CLI)

命令行界面(CLI):有时称为终端。这用作在路由器和交换机等设备上选择配置的另一个选项。如果您有经验，设置事物的方法会简单得多，因为您无需浏览各种Web UI屏幕。这种情况的失败在于，你需要了解命令并完美输入它们。由于您正在为初学者阅读文章，因此CLI可能不是您的首选。

虚拟机

大多数机器的功能都超出了他们的需求。计算机可进行调配，以容纳运行多台计算机所需的一切。问题在于，如果一个部分发生故障或需要重新启动，它们都会跟进。

如果安装VMware或Hyper-V，您可以在一台计算机上加载软件、Web服务器、电子邮件服务器、FindIT等。虚拟机甚至可以使用不同的操作系统。它们在逻辑上相互独立。每个设备都执行独立设备的功能，而实际上不是一台设备。虽然硬件是共享的，但每台虚拟机都会为每个操作系统分配一部分物理资源。这可以节省资金、能源和空间。

您可能使用的思科工具

思科业务控制面板(CBD)

这是用于监控和维护网络的思科工具。CBD可帮助您识别网络中的思科设备以及其他有用的管理功能。

如果您在家中运行或监管多个网络，则此工具非常有用。CBD可在虚拟机上运行。有关CBD的详细信息，请参阅思科业务控制面板支持站点或思科业务控制面板概述。

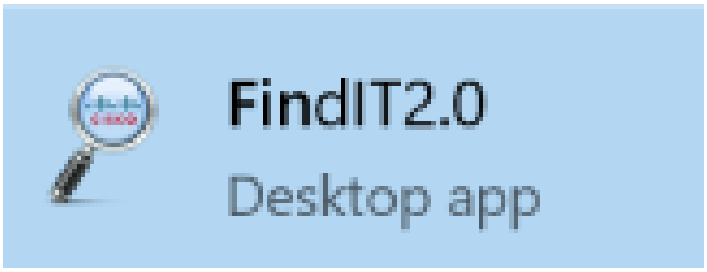
FindIT网络发现实用程序

这个简单的工具非常基本，但可以帮助您快速发现网络中的思科设备。Cisco FindIT会自动发现与PC位于同一本地网段的所有受支持的思科S系列设备。

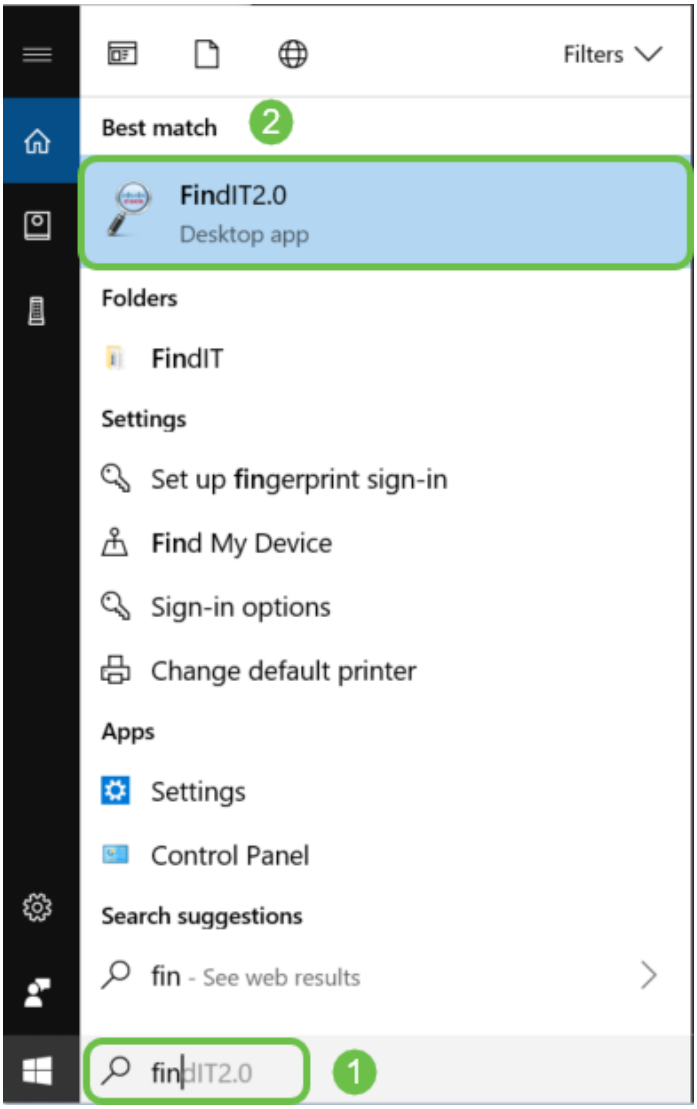
单击以了解详情并下载思科S系列FindIT网络发现实用程序。

单击此链接可阅读有关如何安装和设置Cisco FindIT网络发现实用程序的文章。

Windows 10的应用程序如下所示。



下载后，您可以在Windows 10中找到它。



AnyConnect（RV34x系列路由器/VPN）

此VPN专门用于RV34x系列路由器（以及企业/大型企业设备）。 Cisco AnyConnect安全移动客户端为远程用户提供安全VPN连接。它为远程最终用户提供思科安全套接字层(SSL)VPN客户端的优势，还支持基于浏览器的SSL VPN连接中不可用的应用和功能。AnyConnect通常由远程员工使用，它使员工可以像在办公室一样连接到公司计算机基础设施，即使他们不在办公室。这增加了员工的灵活性、移动性和工作效率。使用AnyConnect需要客户端许可证。Cisco AnyConnect与以下操作系统兼容：Windows 7、8、8.1和10、Mac OS X 10.8及更高版本以及Linux Intel(x64)。

有关详细信息，请参阅以下文章：

- 在 Windows 计算机上安装 Cisco AnyConnect Secure Mobility Client
- 在 Mac 计算机上安装 Cisco AnyConnect Secure Mobility Client

数据交换的基础

数据包

在网络中，信息以数据块（称为数据包）形式发送。如果存在连接问题，数据包可能会丢失。

延迟

传输数据包时的延迟。

冗余

在网络中，配置冗余，以便在部分网络出现故障时，整个网络不会发生故障。如果主配置发生问题，请将其视为备份计划。

协议

两台设备需要具有相同的设置才能通信。把它当作一种语言。如果一个人只说德语，而另一个人只说西班牙语，他们就无法沟通。不同的协议可以协同工作，并且可能有多个协议相互传输。协议有不同的用途；下面列出并简要介绍了一些示例。

编址协议

- **会话初始协议(SIP):**这是IP语音(VoIP)的主要协议，即通过互联网通信的电话。网络两端必须使用相同的协议进行设置才能进行通信，因此它们都需要SIP来通过VoIP发起通信。
- **动态主机配置协议(DHCP)**管理可用IP地址池，在主机加入网络时将其分配给主机。
- **地址解析协**议(ARP):将动态IP地址映射到LAN中的永久物理MAC地址。
- **IPv4：这**是目前使用的最常见的IP版本。IP地址写为4组数字（也称为八位组），每组数字之间用句点分隔。每个集都可以是一个介于0和255之间的数字。IPv4地址的示例是8.8.8.8，即Google的公共DNS服务器。对于IPv4，设备比唯一IP地址多，因此购买永久公有IP地址可能成本高昂。
- **IPv6：此**最新版本使用8组数字，每组数字之间带冒号。它使用十六进制数字系统，因此IP地址中可能有字母。公司可以同时运行IPv4和IPv6地址。

由于我们讨论的是IPv6，下面是有关此编址协议的一些重要详细信息：

IPv6缩写：如果几个集中的所有数字都为零，则一行中的两个冒号可以代表这些集，此缩写只能使用一次。例如，Google的IPv6 IP地址之一是2001:4860:4860::8888。某些设备对IPv6地址的所有八个部分使用单独的字段，因此无法接受IPv6缩写。如果是，请输入2001:4860:4860:0:0:0:0:8888。

十六进制：使用基数16而不是基数10的数字系统，这是我们在日常数学中使用的。数字0-9表示相同。10-15用字母A-F表示。

数据传输协议

- **传输控制协议(TCP)和用户数据报协议(UDP):**这两种方式传输数据。TCP在发送数据之前需要连接（称为三次握手），因此有时会有延迟。如果数据（数据包）丢失，它将再次发送。UDP不太可靠，但速度更快。语音和视频通常使用UDP。
- **文件传输协议(FTP):**此协议用于将文件从客户端传输到服务器。
- **超文本传输协议(HTTP)与安全超文本传输协议(HTTPS)：通**过互联网进行数据通信的一般基础。您将在网站的开头找到这些内容，这些内容写*为http://*和*https://*。以https://开头的*站点*使用更加安全。

- **路由信息协议(RIP):**此协议已经存在很久了。有三个版本，每个版本都增加了更多的安全性和功能。路由器之间共享路由。其目标是通过设置从一台路由器到下一台路由器的最大“跳数”来防止环路。其他更高效的路由协**议包括增强型内**部网**关路由协议(EIGRP)、开放最短路径优先(OSPF)**和**中间系统到中间系统(IS-IS)**。 最后三个扩展比RIP更好，但设置可能更复杂。
- **安全外壳(SSH):**为命令行流量提供安全路由的安全通道。它是用于与远程服务器通信的加密协议。SSH还带有许多其他技术。

发现协议

- **Cisco发现协议**(CDP)：发现与直连的其他Cisco设备相关的信息并保存该信息。**Bonjour**和**链路层发现协议(LLDP**)执行相同的功能，也可以获取有关非Cisco设备的信息。大多数小型企业设备使用LLDP。
- **层链路发现协议(LLDP):**使设备能够向相邻设备通告其标识、配置和功能，这些设备随后将数据存储在管理信息库(MIB)中。 邻居之间共享的信息有助于缩短将新设备添加到局域网(LAN)所需的时间，并提供排除许多配置问题所需的详细信息。LLDP可用于需要在非思科专有设备和思科专有设备之间工作的场景。交换机提供有关端口当前LLDP状态的所有信息，您可以使用此信息修复网络中的连接问题。这是网络发现应用（如FindIT网络管理）用于发现网络中设备的协议之一。

识别协议

- **域名系统(DNS):**一旦为IP地址分配了完全限定域名(FQDN)，就会将其放入数据库。例如，在搜索*www.google.com*时，可以输入网站名称，数据库会搜索该名称，并通过其IP地址将您转到该网站。您的**Internet服务提供商(ISP**)使用其DNS服务器作为默认服务器，并且已经配置。但是，如果您在使用互联网时发现速度较慢，可以手动更改此设置。
- **动态DNS:**也称为DDNS，使用主机名、地址或任何其他相关信息的活动配置自动更新DNS中的服务器。换句话说，DDNS为动态WAN IP地址分配固定域名。这样可节省购买永久IP地址的成本。
- **Internet协议(IP):**IP地址是唯一标识符，用于在Internet上的主机之间发送和接收数据。这通过公有Internet地址实现，需要从ISP处购买。
- **介质访问控制（MAC地址）：每**台设备都连接有唯一标识符。这不会改变。在设置网络和进行故障排除时，最好知道您的MAC地址。它通常位于设备上，包含字母和数字。交换机跟踪设备的MAC地址并创建MAC地址表。

排除协议故障

- **Ping:** Ping是常见的故障排除方法。ping会向IP地址发送ICMP回应消息。收到一条消息作为回复。成功的响应显示了双向物理连接。它是一种检查网络数据包是否可以无问题地分配给地址的方法。
- **Internet控制消息协议(ICMP)：有关**错误和操作信息的消息。执行PING测试时，会向目标发送ICMP回应消息。成功连接会从该设备获得响应。

服务器

向其他计算机提供服务的计算机或计算机上的程序。服务器可以是虚拟的，甚至可以是应用。一台设备上可能有多台服务器。服务器可以相互共享。它们可以与Windows、Mac或Linux配合使用。

Web服务器- Web浏览器的格式和显示网页
文件服务器 — 向网络上的用户共享文件和文件夹
电子邮件服务器 — 发送、接收和存储电子邮件
DNS服务器 — 将用户友好的名称(例如www.cisco.com)转换为IP地址173.37.145.84，例如
即时消息服务器 — 控制和管理即时消息(Jabber、Skype)的流量

服务质量 (QoS)

配置这些设置是为了确保为网络（通常是语音或视频）上的流量提供优先级，因为当数据包（数据）延迟时，这通常是最明显的。

Internet连接的基础

Internet 服务提供商 (ISP)

您需要ISP来访问网络上的Internet。连接速度和各种价格可供您选择，以满足您的业务需求。除了访问Internet，ISP还提供电子邮件、网页托管等服务。

Web 浏览器

设备上的应用。您还可以下载其他内容。下载后，您可以打开并输入要通过互联网访问的IP地址或网站。Web浏览器的一些示例包括：

Microsoft Edge

 ,

铬

 ,

Firefox

 ,

和萨法里。

 。

如果无法打开某些内容或遇到其他导航问题，则很容易尝试打开其他Web浏览器，然后重试。

统一资源定位符 (URL)

在Web浏览器中，通常键入要访问的网站的名称，即URL和其Web地址。每个URL必须唯一。URL的示例为https://www.cisco.com。

默认网关

这是局域网流量用作Internet服务提供商(ISP)和Internet出口的路由器。换句话说，此路由器将您与建筑物外的其他设备以及互联网连接。

防火墙

防火墙是一种网络安全设备，它监控传入和传出的网络流量，并根据定义的一组安全规则(称为访问控制列表(ACL))决定是允许还是阻止特定流量。

几十年来，防火墙一直是网络安全的第一道防线。它们在可信和不可信的外部网络（例如Internet）的安全和受控内部网络之间建立了障碍。

防火墙可以是硬件、软件或两者。

有关详细信息，请参阅在RV34x系列路由器上配置基本防火墙设置。

访问控制列表 (ACL)

列出阻止或允许流量从特定用户发送和接收的流量。访问规则可以配置为始终有效或基于已定义的计划。访问规则根据各种条件进行配置，以允许或拒绝对网络的访问。访问规则根据需要将访问规则应用到路由器的时间进行安排。这些设置在安全或防火墙设置下。例如，企业可能希望阻止员工在工作时间内通过流媒体直播体育节目或连接Facebook。

带宽

在特定时间段内可以从一个点发送到另一个点的数据量。如果您的互联网连接带宽较大，则网络传输数据的速度会比带宽较低的互联网连接快得多。流视频比发送文件占用的带宽要多得多。如果您发现访问网页时存在延迟或流视频延迟，则可能需要提高网络带宽。

以太网电缆

网络中的大多数设备都有以太网端口。以太网电缆是连接有线连接时插入电缆的源。RJ45电缆两端相同，看起来与旧电话插孔相似。它们可用于连接设备和连接到互联网。电缆连接设备，用于访问互联网和文件共享。某些计算机需要以太网适配器，因为它们可能不提供以太网端口。

网络及其结合方式

局域网 (LAN)

一个网络，其大小可能与几栋建筑一样大，也可能与家一样小。连接到LAN的所有人都位于同一物理位置，并且连接到同一路由器。

在本地网络中，每台设备都分配有自己唯一的内部IP地址。它们遵循10.x.x.x、172.16.x.x - 172.31.x.x或192.168.x.x模式。这些地址仅在网络内部、设备之间可见，并被视为专用地址。有数百万个位置可能与您的企业具有相同的内部IP地址池。不重要，它们仅在自己的专用网络中使用，因此不会发生冲突。为了使网络中的设备相互通信，它们应与其它设备采用相同的模式，位于同一子网中，并且是唯一的。您不应将此模式中的任何这些地址视为公有IP地址，因为它们仅保留用于私有LAN地址。

所有这些设备都通过默认网关（路由器）发送数据以访问互联网。当默认网关收到信息时，它需要执行网络地址转换(NAT)，并更改IP地址，因为任何通过Internet传出的设备都需要唯一的IP地址。

广域网 (WAN)

广域网(WAN)是一种分布于全球的网络。许多LAN可以连接到单个WAN。

只有WAN地址才能通过Internet相互通信。每个WAN地址必须是唯一的。为了使网络内部设备能够通过互联网发送和接收信息，您必须在网络边缘（默认网关）有一台路由器，该路由器可以执行NAT。

单击以阅读在RV34x系列路由器上配置访问规则。

网络地址转换 (NAT)

路由器通过Internet服务提供商(ISP)接收WAN地址。 该路由器具有NAT功能，可接收离开网络的流量，将私有地址转换为公有WAN地址，然后通过互联网将其发送出去。在接收流量时，它会执行相反的操作。这是因为没有足够的永久IPv4地址可用于世界上的所有设备。

NAT的好处是，它通过有效隐藏整个内部网络，使其隐藏在唯一的公有IP地址之后，从而提供额外的安全性。内部IP地址通常保持不变，但是，如果断开一段时间，以某种方式进行配置，或重置为出厂默认设置，则可能不会。

静态 NAT

通过在路由器上配置静态动态主机配置协议(DHCP)，可以将内部IP地址配置为保持不变。公有IP地址不保证保持不变，除非您通过ISP购买静态公有IP地址。许多公司都为此服务付费，因此员工和客户可以更可靠地连接到其服务器（Web、邮件、VPN等），但成本可能很高。

静态NAT将私有IP地址的一对一转换映射到公有IP地址。它创建私有地址到公有地址的

固定转换。这意味着您需要将公有地址数量与私有地址数量相等。当需要从网络外部访问设备时，此功能非常有用。

单击以阅读在RV160和RV260上配置NAT和静态NAT。

CGNAT

运营商级NAT是允许多个客户端使用相同IP地址的类似协议。

VLAN

虚拟局域网(VLAN)允许您将局域网(LAN)逻辑分段到不同的广播域。在敏感数据可以在网络上广播的情况下，可以创建VLAN来通过将广播指定给特定VLAN来增强安全性。只有属于VLAN的用户才能访问和操作该VLAN上的数据。VLAN还可以通过减少向不必要目的地发送广播和组播的需求来增强性能。

VLAN主要用于在主机之间形成组，而不管主机的物理位置如何。因此，VLAN通过在主机之间组成来提高安全性。创建VLAN时，在手动或动态将VLAN连接到至少一个端口之前，VLAN不会生效。设置VLAN的最常见原因之一是为语音设置单独的VLAN，为数据设置单独的VLAN。这会将数据包定向到两种类型的数据，尽管使用的是同一网络。

有关详细信息，请阅读《Cisco Business Routers的VLAN最佳实践和安全提示》。

子网

子网通常称为子网，它是IP网络内部的独立网络。

SSID

服务集标识符(SSID)是无线客户端可以连接到无线网络中的所有设备或在其中共享的唯一标识符。它区分大小写，并且不能超过32个字母数字字符。这也称为无线网络名称。

虚拟专用网络 (VPN)

技术已经发展，业务通常在办公室外进行。设备更具移动性，员工通常在家或出差时工作。这可能导致一些安全漏洞。虚拟专用网络(VPN)是以安全方式连接网络上远程工作人员的绝佳方法。VPN允许远程主机像位于同一本地网络一样工作。

VPN设置为提供安全的数据传输。设置VPN和加密数据的方式有不同的选项。VPN使用安全套接字层(SSL)、点对点隧道协议(PPTP)和第二层隧道协议。

VPN连接允许用户通过公共或共享网络（例如Internet）访问、发送和接收数据到私有网络或从私有网络发送和接收数据，但仍然确保与底层网络基础设施的安全连接以保护私有网络及其资源。

VPN隧道建立一个专用网络，该专用网络可以使用加密和身份验证安全地发送数据。公司办公室大多使用VPN连接，因为即使员工不在办公室，也允许其访问私有网络既有用

也是必要的。

在路由器配置了Internet连接后，可以在路由器和终端之间设置VPN连接。VPN客户端完全依赖于VPN路由器的设置才能建立连接。

VPN支持网关到网关隧道的站点到站点VPN。例如，用户可以在分支站点配置VPN隧道以连接到公司站点的路由器，以便分支站点可以安全地访问公司网络。在站点到站点VPN连接中，任何人都可以发起通信。此配置具有持续的加密连接。

IPsec VPN还支持主机到网关隧道的客户端到服务器VPN。当从笔记本电脑/PC通过VPN服务器从家连接到企业网络时，客户端到服务器VPN非常有用。在这种情况下，只有客户端可以启动连接。

单击以阅读Cisco Business VPN概述和最佳实践。

证书

设置VPN的安全步骤是从证书颁发机构(CA)获取证书。 这用于身份验证。从任意数量的第三方站点购买证书。这是证明您的站点是安全的官方方式。本质上，CA是可信赖的来源，用于验证您是合法企业且可信。对于VPN，您只需以最低成本获得较低级别的证书。CA会签出您，一旦他们验证您的信息，他们会向您颁发证书。此证书可以作为文件下载到您的计算机上。然后，您可以进入路由器（或VPN服务器）并上传它。

客户端通常不需要证书即可使用VPN;它仅用于通过路由器进行验证。OpenVPN是例外，它需要客户端证书。

为简单起见，许多小型企业选择使用密码或预共享密钥代替证书。这不太安全，但可以免费设置。

关于此主题的一些文章，您可能会喜欢：

- RV160和RV260系列路由器上的证书（导入/导出/生成CSR）
- 在RV34x系列路由器上将默认自签名证书替换为第三方SSL证书
- 在RV34x系列路由器上管理证书

预共享密钥(PSK)

这是在配置VPN之前决定和共享的共享密码，可用作使用证书的备用密码。PSK可以是您想要的，它只需在站点上匹配，并在客户端设置为其计算机上的客户端时匹配。请记住，根据设备，可能有禁止使用的符号。

密钥生命期

系统更改密钥的频率。此设置也需要与远程路由器相同。

结论

现在，你拥有了很多基本功能，可以让你踏上自己的道路。

如果您想继续学习，请查看这些链接！

设置静态IP地址的最佳实践 思科业务VPN概述和最佳实践 思科业务路由器的VLAN最佳实践和安全提示 Internet备份 — Windows 互联网备份 — Mac 如何登录交换机