用户手册

Cisco Small Business

CVR100W **Wireless-N 300M** 无线路由器

美国总部

Cisco Systems,Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Small Business 支持美国
联系电话 :1-866-606-1866

思科系统（中国）网络技术公司

中国北京市朝阳区建国门外大街 2 号
北京银泰中心银泰写字楼 C 座 7-12 层
邮政编码：100022
http://www.cisco.com.cn
总机：（8610） 8515 5000
传真：（8610） 8515 5963

Chapter 1: 简介 7

产品概述 7
LAN 端口 8
无线接入点 8
无线安全性 8
防火墙与 VPN 8
无线分布式系统 (WDS) 8
服务质量 (QoS) 8
虚拟网络 9
配置与管理 9
了解 CVR100W 9
前面板 9
后面板 11
出厂默认设置 12
安装 CVR100W 12
安放提示 12
壁挂式安装 13
连接外部设备 13
使用快速安装向导 14
连接状态 15
快速导航 16
基本配置 16
其它配置 17
设备状态 17
相关链接 17
页面跳转 18
保存设置 18
返回连接状态页面 18
查看帮助 18
高级配置 18
验证硬件安装 18

接入无线网络 19

Chapter 2: 网络配置 20

WAN 接口配置 20
DHCP - 自动获取 IP 地址 21
PPPoE - 拨号上网 21
Static - 手动配置 IP 地址 22
其它设置 23
MAC 地址克隆 23
LAN 接口配置 24
基本配置 24
IPv4 24
DHCP 服务器配置 25
VLAN 配置 27
静态 DHCP 28
DMZ 配置 28
路由配置 29
运行模式 29
动态路由 30
静态路由 30
VLAN 间路由 31
路由表 32
DDNS 配置 32
IP 模式配置 33
IPv6 配置 34
IPv6WAN 配置 34
设置 IP 模式 34
自动配置 -DHCPv6 35
静态 IPv6 35
IPv6LAN 配置 36
设置 IP 模式 36
IPv6 36
服务器配置 （DHCPv6） 37

IPv6 地址池配置 37
IPv6 静态路由 38
路由 （RIPng） 39
6to4 隧道 40
IPv6 隧道状态 40
路由器通告 40
通告前缀 42

Chapter 3: 无线配置 43

无线安全 43
无线安全提示 43
网络安全指南 44
路由器无线网络 45
基本配置 45
基本无线配置 45
配置无线网络 46
设置安全模式 47
配置 WEP 47
配置 WPA-Personal、 WPA2-Personal 与 WPA2-Personal Mixed 48
配置 WPA-Enterprise、 WPA2-Enterprise 与 WPA2-Enterprise Mixed 49
设置 MAC 过滤 50
访问时间控制 51
设置访客网络 51
高级配置 52
配置 WDS 54
配置 WPS 55
启用 WPS 56
WPS 配置方法 56
WPS 配置方法 1 56
WPS 配置方法 2 57
WPS 配置方法 3 57

Chapter 4: 安全配置 58

路由器安全特性 58
访问策略 58
端口转发 59
基本配置 60
计划管理 61
服务管理 62
访问控制 63
默认访问策略 63
访问控制列表 63
限制上网列表 65
单端口转发 67
多端口转发 67
多端口触发 68

Chapter 5: VPN 配置 69

VPN 客户端 69
创建与管理 QuickVPN 用户 69
导入 VPN 客户端设置信息 70
证书管理 71
生成新证书 71
导入证书 71
导出管理证书 71
导出客户证书 72
VPN 透传 72

Chapter 6: QoS 配置 73

带宽管理 73
配置带宽 73
配置带宽优先级 74
QoS 端口配置 75
CoS 配置 76

DSCP 配置 76

Chapter 7: 系统管理 77

用户管理 77
远程管理 78
睡眠模式 79
时间设置 79
Bonjour 80
故障诊断 81
网络工具 81
端口镜像 82
日志管理 83
日志配置 83
远程日志服务器 83
配置管理 84
备份 84
恢复 84
固件升级 85
设备重启 86
恢复出厂设置 86
快速安装向导 86

Chapter 8: 设备状态 88

控制面板 88
设备概览 91
连接设备 93
DHCP 信息 94
端口统计 95
无线统计 96
访客信息 97

VPN 信息 97
日志信息 98

Chapter 9: 配置 Cisco Smart Connect 100

关于思科锐联 100
启用思科锐联 100
配置 CSC 无线网络 101
通过设备管理器设置 CSC 无线网络 101
使用 CSC 网管版软件设置 CSC 无线网络 103
接入 CSC 无线网络 104
自定义思科锐联二维码 104

Chapter A: 使用思科 QuickVPN 106

准备工作 106
安装思科 QuickVPN 软件 107
使用思科 QuickVPN 软件 107

Chapter B: 相关资料 111

1

简介

本章介绍思科 CVR100W Wireless-N 300M 无线路由器 （以下简称 CVR100W）的主要功能与特性，以便您能尽快地了解和使用 CVR100W。

本章包括以下内容：

- 产品概述
- 了解 CVR100W
- 安装 CVR100W
- 连接外部设备
- 使用快速安装向导
- 连接状态
- 快速导航
- 验证硬件安装
- 接入无线网络

产品概述

感谢您选择思科 CVR100W Wireless-N 300M 无线路由器。CVR100W 为您提供高级 Internet 共享网络解决方案，能够很好地满足中小企业与家庭用户的需求。不论您的办公室或家中的网络接入是有线还是无线， CVR100W 都能够使您足不出户，畅享 Internet 网络。

CVR100W 在有线连接方面秉承了思科路由器的传统特性，通过 10/100 Mpbs 快速以太网 WAN 端口能够轻松地与您的调制解调器或家庭网关相连接。 CVR100W 支持 IEEE 802.11n/g/b 标准协议，理想的连接速率可达 300 Mbps。 CVR100W 支持 VPN 功能，帮助远端用户安全便捷地访问您的内部网络。

LAN 端口

CVR100W 提供 4 个全双工 10/100 Mbps 快速以太网 LAN 端口，供您连接 4 个外部设备。您也可以将其中一个端口连接至思科交换机，从而扩展您的内部网络以连接更多的外部设备。

无线接入点

CVR100W 的无线接入点支持 IEEE 802.11n 标准协议，使用 MIMO 技术。相比于 IEEE 802.11g 网络， CVR100W 能够提供更好的数据吞吐与网络覆盖。

无线安全性

CVR100W 在无线安全性方面支持以下标准：WPA-Personal、 WPA-Enterprise、WPA2-Personal、 WPA2-Enterprise 和 WEP-Security，涵盖了您不同情景下的使用需求。与此同时， CVR100W 提供诸多无线安全特性，例如禁用 SSID 广播、基于 MAC 地址过滤、 Internet 访问时间控制等。其合理有效的安全配置能够为您量身打造专属于您的无线网络安全方案。

防火墙与 VPN

CVR100W 支持 SPI 防火墙功能与 DoS 防范，为您的内部网络筑起铜墙铁壁；而在 VPN 方面， CVR100W 支持最多 3 条客户端到网关的隧道，帮助您建立安全便捷的访问通道，为您移动办公、远端用户访问提供通信连接与安全保障。

无线分布式系统 (WDS)

CVR100W 的无线接入点支持无线分布式系统，该特性能够扩展 CVR100W 的无线覆盖范围，帮助您摆脱传统有线网络的束缚。

服务质量 (QoS)

CVR100W 在服务质量方面支持以下标准：Wi-Fi Multimedia (WMM)、 Wi-Fi Multimedia Power Save (WMM-PS)、 IEEE 802.1p、 DSCP 以及 CoS，极大地提升您的网络访问质量，尤其在您使用对延迟敏感的 VoIP 应用与带宽密集型的视频数据流应用时， CVR100W 能够为您保证更好的服务。

虚拟网络

CVR100W 使用基于 IEEE 802.1Q 的 VLAN 技术，最多支持 4 个相互独立的虚拟网络，并为其分配不同的 SSID。

配置与管理

通过 CVR100W 内置的 web 服务器，您可以使用浏览器访问 CVR100W 的设备管理页面，配置相关信息。

CVR100W 支持以下浏览器：Microsoft Internet Explorer 6.0 及其以上版本、Mozilla Firefox 3.0 及其以上版本、 Apple Safari 3.0 及其以上版本和 Chrome 5.0 及其以上版本。

CVR100W 也为您提供了快速安装向导，方便您快速地设置 CVR100W 的基本网络参数。

了解 CVR100W

在使用 CVR100W 之前，请预先了解 CVR100W 前面板按键和指示灯以及后面板各种接口的详细说明。

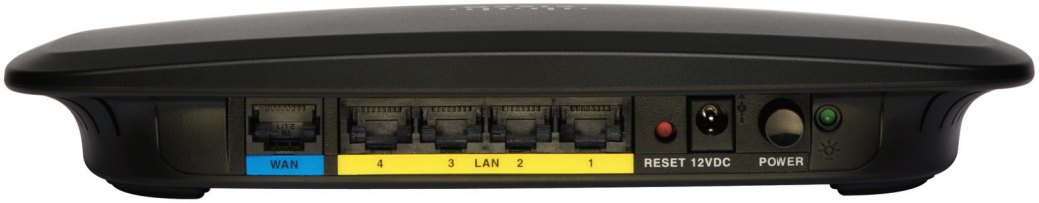
前面板

CVR100W 前面板上共有 8 个指示灯与 3 个按键。白色外壳的 CVR100W 前面板指示灯亮起时显示为绿色。黑色外壳的 CVR100W 前面板指示灯亮起时显示为蓝色。

LAN (1-4)	每个 LAN 指示灯的编号都对应于后面板上每个 LAN 端口的编号。 ▪ 指示灯亮起：表示 LAN 端口已正常连接； ▪ 指示灯闪烁：表示正在通过该 LAN 端口收发数据； ▪ 指示灯熄灭：表示 LAN 端口没有连接。
WPS	▪ 指示灯亮起：表示 WPS 成功配置； ▪ 指示灯每秒闪烁一次 (1 Hz)：表示 WPS 过程发生错误； ▪ 指示灯熄灭：表示 WPS 配置完成或未配置。
无线	▪ 指示灯亮起：表示无线功能已开启且 Wi-Fi 信号强度为 100% ； ▪ 指示灯橙色：表示无线功能已开启且 Wi-Fi 信号强度为 50% ； ▪ 指示灯闪烁：表示正通过无线网络收发数据； ▪ 指示灯熄灭：表示无线功能未启用。
WAN	▪ 指示灯亮起：表示 WAN 端口已正常连接； ▪ 指示灯闪烁：表示正在通过 WAN 端口收发数据； ▪ 指示灯熄灭：表示 WAN 端口没有连接。
电源	▪ 指示灯亮起：表示 CVR100W 已通电并处于正常运行状态； ▪ 指示灯闪烁：表示 CVR100W 正在启动或者处于升级固件的过程中； ▪ 指示灯熄灭：表示 CVR100W 未通电。
睡眠模式开关	用于开启或关闭前面板的工作指示灯，不影响 CVR100W 的正常工作状态。 ▪ 睡眠模式开启后，前面板所有指示灯全部熄灭，后面板睡眠模式指示灯亮起。 ▪ 睡眠模式未启用时，前面板指示灯正常亮起，后面板睡眠模式指示灯熄灭。
WPS 按键	用于启用您所在网络的 WPS 功能。
无线开关	用于开启或关闭 CVR100W 的无线功能。

后面板

CVR100W 后面板上有网络接口、重置按钮、电源接口与开关以及睡眠模式指示灯。



WAN	WAN 端口用于连接至 Internet。
LAN (1-4)	LAN 端口用于连接至局域网设备。
重置按钮 **(RESET)**	使用回形针或笔尖长按重置按钮可重启设备或恢复出厂设置： ▪ 重启 CVR100W：长按重置按钮至少 1 秒，但不能超过 5 秒。 ▪ 恢复出厂设置：长按重置按钮超过 5 秒。该操作会重启 CVR100W 并将其恢复为出厂设置。您之前对 CVR100W 所做的任何配置信息都将丢失。
电源接口 **(12VDC)**	连接到提供 12 V/0.5 A 交流电的电源适配器上。
电源开关 **(POWER)**	打开或关闭 CVR100W 的电源。
睡眠模式指示灯	显示睡眠模式工作状态： ▪ 指示灯亮起：表示睡眠模式已开启且 CVR100W 运行正常； ▪ 指示灯闪烁：表示睡眠模式已开启但网络连接异常； ▪ 指示灯熄灭：表示睡眠模式未开启。

出厂默认设置

请使用以下出厂默认设置登录基于 web 的设备管理器配置您的网络参数：

参数	描述
用户名	cisco
密码	cisco
路由器 IP	192.168.1.1
DHCP 地址池范围	192.168.1.100 - 192.168.1.149

注 如需恢复设备出厂设置，可使用回形针或笔尖长按后面板的重置按钮 (RESET) 超过 5 秒。设备将自动重启并恢复到出厂设置。您之前所做的任何配置信息都将丢失。

安装 CVR100W

CVR100W 支持以下两种安装方式：

- 将其放置在平面上。详细信息请参考安放提示。
- 将其固定在墙上。详细信息请参考壁挂式安装。

安放提示

请勿在如下环境中部署设备：

- 环境温度：环境温度不得超过 40 摄氏度。
- 通风情况：必须保持 CVR100W 两个侧面板周围通风顺畅，以防过热。
- 机械负载：必须保持 CVR100W 水平、稳固和安全，以防止其滑动或移位。

建议将 CVR100W 水平置于平整表面， CVR100W 底部的橡胶脚垫能够很好地发挥稳定作用。

壁挂式安装

CVR100W 可固定在墙壁上。您需要自行准备合适的安装组件将 CVR100W 固定在墙壁上。壁挂式安装 CVR100W 时，应使其端口朝上或朝下。请勿使 CVR100W 的端口朝向侧面，因为这会导致挤压端口部件。

连接外部设备

CVR100W 默认开启无线接入功能。首次配置时，为了避免不必要的麻烦 （例如无线连接设置不正确、无线信号未找到等问题），您最好将主机和其它 Internet 设备 （例如调制解调器）通过有线方式连接到 CVR100W。当然您也可以选择无线方式连接到 CVR100W。在您首次配置无线连接时，可参考 CVR100W 设备底部的标签获取默认的无线网络名称 （SSID）和安全密钥等信息。详见接入无线网络。

步骤 1 关闭包括调制解调器、 CVR100W、用来配置 CVR100W 的 PC 以及其他网络设备在内所有设备的电源。

步骤 2 将电源适配器的一端插入到 CVR100W 的电源插孔中 (12VDC)，另一端插入电源插座中。请确保 CVR100W 后面板的电源开关处于关闭状态。

注意 请使用随机标配的电源适配器。使用其它的电源适配器可能会损坏 CVR100W。

步骤 3 将以太网线的一端连接至调制解调器的以太网端口，另一端连接至 CVR100W 后面板的 WAN 端口。

步骤 4 将以太网线的一端连接至主机或其他网络设备的以太网端口，另一端连接至 CVR100W 后面板的 LAN 端口。

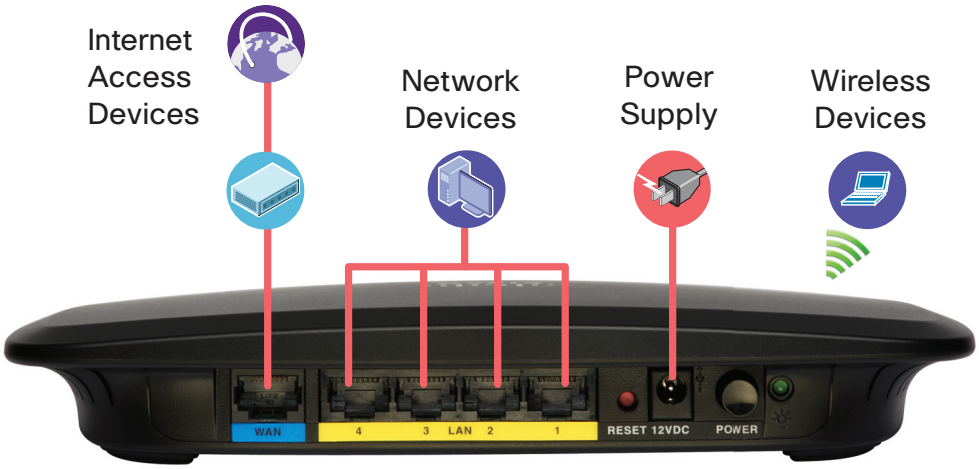
注 如希望将 PC 通过无线方式连接至 CVR100W，请跳过此步骤。

步骤 5 开启所有连接设备的电源。

步骤 6 按下 CVR100W 后面板的 POWER 按钮，开启 CVR100W。

步骤 7 如需通过无线方式连接至 CVR100W，请使用设备底部标签上的密钥信息将您的 PC 连接至 CVR100W 默认的无线网络。详细信息请参考接入无线网络。

至此，您已成功连接至 CVR100W 并可以开始访问互联网。



使用快速安装向导

快速安装向导与设备管理界面支持 Microsoft Internet Explorer 6.0、 Mozilla Firefox 3.0、 Apple Safari 3.0 或 Google Chrome 5.0 或以上浏览器的更高版本。

请按照以下步骤完成快速安装向导的配置：

步骤 1 将一台主机与 CVR100W 后面板的 LAN 端口相连。启动这台主机后，它将自动获取一个在 192.168.1.xxx 范围内的 IP 地址。

步骤 2 打开网页浏览器。在地址栏中输入 CVR100W 的 IP 地址 (默认为 **192.168.1.1**) 并按下 Enter 键即可访问至 CVR100W 的设备管理界面。

步骤 3 首次访问时弹出的登录页面，选择设备管理界面使用的语言并输入用户名与密码。默认的用户名与密码均为 **cisco**。

步骤 4 点击 “登录”。首次登录时，自动打开快速安装向导。

步骤 5 遵循屏幕上的说明进行快速安装向导的配置，共 4 步。

- 配置路由器密码 （第 1 步，共 4 步）。

  在这一步骤中，建议您更改 CVR100W 的默认管理密码，以便更好地保护您的设备安全，防止未经授权的访问。新密码建议使用字母及数字的组合，长度至少 6 位。不建议您勾选 “空密码” 选项。

输入新密码后，单击 “下一步”，继续。

- 配置网络连接 （第 2 步，共 4 步）。

  在这一步骤中，您需要选择您的 Internet 连接类型。如果您不确定选择哪种类型，请联系您的网络服务提供商。

  选择正确的连接类型并配置正确参数后，单击 “下一步”，继续。

- 配置无线安全 （第 3 步，共 4 步）。

  在这一步骤中，您需要配置您的无线网络。首先为您的无线网络输入一个名称（SSID），例如 MyNetwork。接下来您需要为无线网络选择安全模式，并根据您选择的安全模式设定相应的加密算法以及安全密钥等。我们强烈建议您启用安全程度更高的安全模式来充分保护您的无线网络。

  完成无线安全配置后，单击 “下一步”，继续。

- 确认配置信息 （第 4 步，共 4 步）。

  在这一步骤中，您将看到之前步骤中所填写的配置信息，包括新管理密码、网络连接类型和无线网络信息。

  在您确认后，单击 “保存并退出”，完成快速安装向导配置；您也可以直接单击 “退出”放弃之前的配置并退出。

  完成快速安装向导配置之后，会转到 “连接状态”页面。详见连接状态。

连接状态

当您首次登录并完成快速安装向导的配置之后，或当您非首次访问基于 web 的设备管理器时，打开 “连接状态”页面。

您无须提供用户名和密码，通过 “连接状态”页面可以查看 CVR100W 当前的 WAN、 LAN 和 WLAN 连接状态。包括以下信息：

参数	描述
WAN	
连接方式	显示是否连接到 Internet 以及连接到 Internet 的方式。

参数	描述
IP 地址	WAN 接口的 IP 地址。
子网掩码	WAN 接口的子网掩码。
默认网关	默认网关的 IP 地址。
DNS 地址	主 DNS 服务器和副 DNS 服务器的 IP 地址。
LAN	
主机名	连接到 CVR100W 的 LAN 侧主机名称。
IP 地址	LAN 侧主机的 IP 地址。
MAC 地址	LAN 侧主机的 MAC 地址。
WLAN	
信号强度	显示无线信号的强度。

如需实时刷新页面数据，点击 “刷新”。如需启动快速安装向导，点击 “快速安装向导”。如需访问 CVR100W 产品主页以便了解更多产品信息，点击 “产品主页”。

如需配置 CVR100W 的高级参数，点击 “高级配置”。此时您需要输入用户名和密码。成功登录后，将首先打开 “快速导航”页面。详见快速导航。

快速导航

“快速导航”页面显示 CVR100W 的常用配置链接。使用这些链接可以直接跳转到相关配置页面。

基本配置

更改用户密码	单击该链接会打开 “系统管理” - “用户管理”页面，您可以在该页面修改管理员密码。详见用户管理。
快速安装向导	单击该链接会启动 “快速安装向导”。
配置 **WAN**	单击该链接会打开 “网络配置” - “**WAN** 接口配置” - “**Internet** 配置”页面。详见 WAN 接口配置。

配置 **LAN**	单击该链接会打开 “网络配置” - “**LAN** 接口配置” - “基本配置” 页面。详见 LAN 接口配置。
配置无线	单击该链接会打开 “无线配置” - “基本配置” 页面。详见基本无线配置。

其它配置

升级固件	单击该链接会打开 “系统管理” - “固件升级” 页面。详见固件升级。
配置 **VPN**	单击该链接会打开 “**VPN** 配置” - “**VPN** 客户端” 页面。详见 VPN 客户端。
配置防火墙	单击该链接会打开 “安全配置” - “基本配置” 页面。详见基本配置。

设备状态

设备概览	单击该链接会打开 “设备状态” - “设备概览” 页面。详见设备概览。
无线状态	单击该链接会打开 “设备状态” - “无线统计” 页面。详见无线统计。
VPN 状态	单击该链接会打开 “设备状态” - “**VPN** 信息” 页面。详见 VPN 信息。

相关链接

产品主页	单击该链接会访问 CVR100W 产品主页。
技术论坛	单击该链接会访问思科在线支持中心。

页面跳转

您可以使用左侧面板中的导航树打开相关配置页面，具体操作是：单击相应选项展开目录，然后单击相应子目录进行操作或者显示子菜单。

保存设置

当您在配置页面中完成相关修改时，单击 “保存”，保存您的设置信息；单击 “取消”，放弃您之前所做的修改。

返回连接状态页面

如果您希望返回到 “连接状态”页面，请单击页面右上方的 “主页”链接。点击 “注销”退出登录，您也将返回到 “连接状态”页面。此时如您需要配置高级参数，请再次输入用户名和密码。

查看帮助

如果您希望获取当前配置页面的更多信息，请单击页面右上方的 “帮助”链接。

高级配置

在您使用安装向导配置 CVR100W 之后，我们强烈建议您手动修改一些默认设置，这样可以为您的网络带来更好的安全性与性能。建议的操作如下：

- 如果在您的网络中已经拥有DHCP服务器，并且您不希望CVR100W作为您网络中的 DHCP 服务器，您需要修改相关设置。详见 LAN 接口配置。
- 配置您的 VPN，您需要使用 QuickVPN 软件。详见使用思科 QuickVPN。

验证硬件安装

如果您希望验证硬件安装是否正确，请执行以下步骤：

- 检查指示灯状态。详见了解 CVR100W。
- 将一台主机连接到一个可用的LAN端口上，验证其能否访问Internet上的站点，例如：尝试访问 www.cisco.com。
- 将一个设备接入您的无线网络，验证无线网络是否正常。详见接入无线网络。

接入无线网络

将一个设备 （本例中使用一台主机）接入您的无线网络，您首先需要在该设备上配置无线连接的相关信息，这些信息是在您使用 CVR100W 快速安装向导时所配置的。

以下步骤信息只是作为一个示例供您参考，您可能需要不同的配置方法来配置您的设备，具体的配置方法请参考您的设备使用手册。

步骤 1 打开您主机上的无线连接设置窗口或程序。

您的主机可能拥有一些特定的软件管理无线连接，或者您可以使用控制面板下的无线连接或者网络相关的设置窗口。（具体位置取决于您使用的操作系统）。

步骤 2 在安装向导中输入无线网络的 SSID。

步骤 3 在安装向导中选择加密类型，输入安全密钥。

注 如您希望通过无线网络完成 CVR100W 的初始配置 （首次访问 CVR100W 的设备管理界面进行配置），在以上两步骤中请分别填入设备底部标签上提供的默认无线网络名称 （SSID）和密钥。

如果您不希望启用加密 （不建议），请将加密类型与安全密钥区域留空。

步骤 4 验证您的无线连接并保存您的设置信息。

2

网络配置

本章为您介绍如何配置 CVR100W 的网络设置。包括以下内容：

- WAN 接口配置
- LAN 接口配置
- 路由配置
- DDNS 配置
- IP 模式配置
- IPv6 配置

WAN 接口配置

“WAN 接口配置”中包含两项子菜单：“Internet 配置”与 “MAC 地址克隆”。

在 “**Internet** 配置”页面，您需要根据不同的 WAN 环境，配置正确的网络连接类型，主要包括以下内容：

- DHCP - 自动获取 IP 地址
- PPPoE - 拨号上网
- Static - 手动配置 IP 地址
- 其它设置

在 “**MAC** 地址克隆”页面，您可以将您主机的 MAC 地址或者其它设备的 MAC 地址克隆到 CVR100W。

- MAC 地址克隆

DHCP - 自动获取 IP 地址

如果您的网络服务提供商 （Internet Service Provider， ISP）使用动态主机配置协议（DHCP）分配用户的 IP 地址 （即：用户每一次登录都会得到一个新分配的 IP 地址），请按以下步骤配置网络连接类型：

步骤 1 单击 “网络配置” - “**WAN** 接口配置” - “**Internet** 配置”。

步骤 2 在 “网络连接类型”下拉菜单中选择 “**DHCP -** 自动获取 **IP** 地址”。

步骤 3 （可选）如果您需要修改其它可选设置项，详见其它设置。

步骤 4 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

PPPoE - 拨号上网

将网络连接类型配置为 “**PPPoE -** 拨号上网”的的步骤：

步骤 1 单击 “网络配置” - “**WAN** 接口配置” - “**Internet** 配置”。

步骤 2 在 “网络连接类型”下拉菜单中选择 “**PPPoE -** 拨号上网”。

步骤 3 您需要输入以下信息：（您可能需要联系网络服务提供商，获取 PPPoE 的登录信息）

用户名	网络服务提供商分配给您的用户名。
密码	网络服务提供商分配给您的密码。
按需连接	如果您所在的网络服务提供商按连接时长收费，建议您选择此选项。 即：当您需要访问外部网络时，打开网络连接；当你不需要访问外部网络时，关闭网络连接。 如果您选择 “按需连接”，请输入 “最大空闲时间”。（单位：分钟）
保持连接	如果您希望始终保持网络连接，请选择此项。 即：网络连接始终处于打开状态。 如果您选择 “保持连接”，请输入 CVR100W 的 “重拨周期”。（单位：秒）

认证类型	▪ 自动协商：服务器发送安全算法的相关参数配置请求， CVR100W 自动使用相应的安全认证方式连接。 ▪ **PAP**：CVR100W 使用 PAP 方式连接网络服务提供商。 ▪ **CHAP**：CVR100W 使用 CHAP 方式连接网络服务提供商。 ▪ **MS - CHAP**：CVR100W 使用 MS-CHAP 方式连接网络服务提供商。 ▪ **MS - CHAPv2**：CVR100W 使用 MS-CHAPv2 方式连接网络服务提供商。

步骤 4 （可选）如果您需要修改其它可选设置项，详见其它设置。

步骤 5 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

Static - 手动配置 IP 地址

如果您的网络服务提供商分配给用户的是静态 IP 地址，您需要通过以下步骤配置网络连接类型：

步骤 1 单击 “网络配置” - “**WAN** 接口配置” - “**Internet** 配置”。

步骤 2 在 “网络连接类型”下拉菜单中选择 “**Static -** 手动配置 **IP** 地址”。

步骤 3 您需要输入以下信息：

WAN IP 地址	WAN 端口的 IP 地址
子网掩码	WAN 端口的子网掩码
默认网关	默认网关的 IP 地址
静态 **DNS 1**	第一 DNS 服务器 IP 地址
静态 **DNS 2**	第二 DNS 服务器 IP 地址

步骤 4 （可选）如果您需要修改其它可选设置项，详见其它设置。

步骤 5 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

其它设置

您可以在 “其它设置”中进行与 WAN 接口相关的其它可选设置。

步骤 1 单击 “网络配置” - “**WAN** 接口配置” - “**Internet** 配置”。

步骤 2 在 “其它设置”中，您可以配置以下信息：

设备名称	CVR100W 的设备名称。
域名	您所在网络的域名。
MTU 配置	MTU （Maximum Transmit Unit）是指网络中可被传输的最大数据包的长度。以太网络中标准 MTU 值为 1500 字节；在 PPPoE 连接中， MTU 值为 1492 字节。 如果您所在的网络服务提供商没有特殊要求，建议您选择 “自动”，即默认的 MTU 值 （1500 字节）。 如果您所在的网络服务提供商自定义 MTU 设置，请选择 “手动”并输入相应 MTU 值。
MTU 大小	MTU 值。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

MAC 地址克隆

您可能需要将 CVR100W WAN 端口的 MAC 地址设置为与您主机或者其它设备的 MAC 地址相同，该操作称为 MAC 地址克隆。

例如：某些网络服务提供商会在您首次使用网络服务时绑定您主机的 MAC 地址。因此当您将 CVR100W 置于 Cable Modem 或者 DSL Modem 后端时，网络服务提供商不能识别 CVR100W WAN 端口的 MAC 地址，这将导致您不能访问外部网络。此时您需要克隆您主机的 MAC 地址，使得网络服务提供商能够识别 CVR100W。

MAC 地址克隆的步骤：

步骤 1 单击 “网络配置” - “**WAN** 接口配置” - “**MAC** 地址克隆”。

步骤 2 在 “**MAC** 地址克隆”部分，勾选 “启用”，启用 MAC 地址克隆。

步骤 3 根据克隆 MAC 地址的来源不同，请选择以下操作之一：

- 克隆主机 MAC 地址时，单击 “克隆本机 **MAC** 地址”。
- 克隆其它 MAC 地址时，在 “**MAC** 地址”部分手动输入。

步骤 4 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

LAN 接口配置

CVR100W 的 DHCP 与 TCP/IP 默认设置适用于绝大多数应用情景。如果您将 CVR100W 连接到一个已配置 LAN 的调制解调器或者其它类似设备 （该设备的子网为 192.168.1.x）时， CVR100W 会自动将子网的网段由 192.168.1.x 改至 10.x.x.x，从而避免可能出现的 IP 地址冲突。

基本配置

在 “基本配置”页面，您可以修改 CVR100W 的 IP 地址以及与 DHCP 相关的配置。

IPv4

修改 CVR100W 的 LAN IP 地址的步骤：

步骤 1 单击 “网络配置” - “**LAN** 接口配置” - “基本配置”。

步骤 2 在 “**IPv4**”部分，您需要配置以下信息：

VLAN	在下拉菜单中选择相应的 VLAN。
本地 **IP** 地址	输入 CVR100W 的 LAN IP 地址。 您必须确保该 IP 地址未被其它设备使用。

子网掩码	在下拉菜单中选择子网掩码。 默认设置为 255.255.255.0。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

需要注意的是，在您修改 CVR100W 的 LAN IP 地址后，您与 CVR100W 的连接将断开。

步骤 4 您需要根据您主机 IP 地址的分配方式，进行以下操作之一：

- 如果您主机的 IP 地址是动态分配（即 CVR100W DHCP 已配置），您需要释放您主机原有的 IP 地址并重新获取 IP 地址。
- 如果您是手动配置主机的 IP 地址，您必须将主机的 IP 地址与 CVR100W 的 LAN IP 地址配置在同一子网中。例如：如果您将 CVR100W 的 IP 地址修改为 10.0.0.1，那么您主机的 IP 地址必须在 10.0.0.2 到 10.0.0.255 的范围内。

步骤 5 重启浏览器，输入修改后的 CVR100W 的 LAN IP 地址，连接 CVR100W。

DHCP 服务器配置

默认设置下， CVR100W 的 “DHCP 服务器” 启用。 CVR100W 作为 DHCP 服务器，其 IP 地址即为您所在网络的网关地址， CVR100W 向网内主机分配 IP 地址、提供 DNS 服务。

CVR100W 的地址池 IP 地址范围是 192.168.1.100 到 192.168.1.149， CVR100W 从该范围分配内网主机的 IP 地址。如果您需要为内网中的主机设置静态 IP 地址，请使用 192.168.1.2 到 192.168.1.99 范围内的地址，以保证两者之间不冲突。

如果您希望将网络中的某台主机设置为 DHCP 服务器，或者希望手动配置网络中的所有主机，请禁用 “DHCP 服务器”。同时，如果您不希望使用 DNS 服务，您也可以使用 WINS （Windows Internet Name Server，视窗网络命名服务）达到相同的功能。

WINS 从功能上等价于 DNS，都是将网络域名 （例如：www.cisco.com）映射至相应的 IP 地址，区别在于 WINS 使用 NetBIOS 协议解析主机名。 CVR100W 在发送到 DHCP 客户端的数据包中已包含 WINS 的 IP 地址，从而确保您使用 WINS 服务的可行性。

配置 DHCP 的步骤：

步骤 1 单击 “网络配置” - “LAN 接口配置” - “基本配置”。

步骤 2 在 “VLAN” 下拉菜单中选择相应 VLAN。

步骤 3 在 “DHCP 服务器”部分，选择相应配置：

启用	选中启用 CVR100W DHCP 功能。 CVR100W 在网内作为 DHCP 服务器。
禁用	选中禁用 CVR100W DHCP 功能。 如果您希望使用其它设备作为网内 DHCP 服务器，或者您希望手动配置网内主机，请禁用 DHCP 功能。
DHCP Relay	选中启用 DHCP Relay。 CVR100W 在网内作为 DHCP 服务器中继代理。

步骤 4 如果您启用 DHCP 服务器，您需要输入以下信息：

DHCP 起始 **IP** 地址	输入 IP 地址池的起始地址。每一个新进入 LAN 的 DHCP 客户端都会从该地址池获取 IP 地址。（地址池的结束地址由 “DHCP 最大用户数”决定）
DHCP 最大用户数	输入 DHCP 客户端的最大数量。
DHCP 分配 **IP** 地址范围	（只读) 显示可供 DHCP 客户端使用的 IP 地址范围。
DHCP 地址租期	输入分配给 DHCP 客户端的 IP 地址的使用时长。（单位：分钟）
静态 **DNS 1**	输入第一 DNS 服务器的 IP 地址。
静态 **DNS 2**	输入第二 DNS 服务器的 IP 地址。
静态 **DNS 3**	输入第三 DNS 服务器的 IP 地址。
WINS 服务器	输入 WINS 服务器的 IP 地址。

步骤 5 如果您启用 “**DHCP Relay**”，您需要在 “**DHCP Relay** 服务器地址”部分输入中继网关地址。中继网关在多个子网间传输 DHCP 消息。

步骤 6 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

VLAN 配置

VLAN （Virtual Local Area Network，虚拟局域网）是功能上相关联或者拥有诸多共性的一组网络终端的集合，与基于物理位置的局域网不同， VLAN 可以不考虑设备以及用户的物理位置而组成新的工作组。

创建 VLAN 的步骤：

步骤 1 单击 “网络配置” - “**LAN** 接口配置” - “**VLAN** 配置”。

步骤 2 在 “**VLAN** 配置列表”中，单击 “添加条目”。

步骤 3 在新建的 VLAN 表项中，您需要输入以下信息：

VLAN ID	输入 VLAN ID。VLAN ID 必须在 4 到 4094 之间。VLAN ID 1 用作默认 VLAN，用于接收端口上的无标记帧；VLAN ID 2 预留； VLAN ID 3 用作访客网络。
描述	输入新建 VLAN 的描述。
LAN 1 **LAN 2** **LAN 3** **LAN 4**	您可以将 CVR100W 上的 VLAN 关联到相应的 LAN 端口。默认设置下，全部 4 个端口都属于 VLAN 1。您可以修改这些端口将其关联到其它 VLAN，修改时需要选择各端口的外出帧类型： 无标记：LAN 端口是该 VLAN 的一个无标记成员，该 VLAN 发送到该端口的信息帧是无标记的。 有标记：LAN 端口是该 VLAN 的一个标记成员，该 VLAN 发送到该端口的信息帧是有标记的，在新建 VLAN 时所有的端口都是这一状态。 不包括：LAN 端口不是该 VLAN 的成员。

步骤 4 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

如果您希望修改 VLAN 的相关设置，请选择相应的 VLAN 并单击 “编辑”；如果您希望删除相应的 VLAN，请选择相应的 VLAN 并单击 “删除”；单击 “保存”，保存您之前所作的配置。

静态 DHCP

您可以通过配置静态 DHCP，为指定 MAC 地址的设备分配固定的 IP 地址配置静态 DHCP 的步骤：

步骤 1 单击 “网络配置” - “**LAN** 接口配置” - “静态 **DHCP**”。

步骤 2 在 “**VLAN**”下拉菜单中选择相应 VLAN。

步骤 3 在 “静态 **DHCP** 列表”中，单击 “添加条目”。

步骤 4 在新建的静态 DHCP 客户端表项中，您需要输入以下信息：

描述	输入该设备的描述。
IP 地址	输入分配给该设备的 IP 地址。 DHCP 地址池被用作公共池，我们建议您输入的 IP 地址在 DHCP 地址池的范围之外。
MAC 地址	输入该设备的 MAC 地址。 MAC 地址的格式为：XX:XX:XX:XX:XX:XX。其中 X 为 0 到 9 的数字或 A 到 F 的字母。

如果您希望修改静态 DHCP 相关设置，请选择相应设备并单击 “编辑”；如果您希望删除相应设备的静态 DHCP 绑定，请选择相应设备并单击 “删除”；单击 “保存”，保存您之前所作的配置。

DMZ 配置

CVR100W 支持 DMZ （Demilitarized Zones，隔离区）， DMZ 是在防火墙保护下并且对外部网络开放的内部子网区域。您可以配置内网中的一台主机，指定 IP 地址并进行配置，通过它将内网的 IP 地址映射到外部网络的 IP 地址。

我们强烈建议您只将诸如 Web、 E-mail 等允许外部访问的服务器置于 DMZ 网络。您可以通过设置防火墙规则控制指定服务与端口。当 DMZ 网络节点遭受攻击时， DMZ 的启用能够在一定程度上保护内网免遭攻击。

您必须为 DMZ 主机分配固定的 （静态） IP 地址，该 IP 地址必须与 CVR100W 所在局域网是同一网段，但不能是网关的 IP 地址。

配置 DMZ 的步骤：

步骤 1 单击“网络配置”-“**LAN** 接口配置”-“**DMZ** 配置”。

步骤 2 勾选“启用”，启用 DMZ。

步骤 3 在“**VLAN**”下拉菜单中，选择 VLAN ID。

步骤 4 在“主机 **IP** 地址”部分，输入 DMZ 主机的 IP 地址。

步骤 5 单击“保存”，保存您的设置。单击“取消”，不保存任何修改。

路由配置

在“路由配置”页面，您可以配置 CVR100W 上与路由相关的功能：

运行模式

配置 CVR100W 运行模式的步骤：

步骤 1 单击“网络配置”-“路由配置”。

步骤 2 在“运行模式”部分，请选择以下选项之一：

网关	将 CVR100W 用作网关模式。（建议选择此项） 如果您使用 CVR100W 控制进出 Internet 的网络连接，请保持此默认设置。
路由	将 CVR100W 用作路由模式。 需要注意的是：启用路由模式会禁用 NAT （Network Address Translation，网络地址转换）。

步骤 3 单击“保存”，保存您的设置。单击“取消”，不保存任何修改。

动态路由

RIP （Routing Information Protocol，路由选择信息协议）是 IGP （Interior Gateway Protocol，内部网关协议）的一种，在内部网络中使用。 RIP 允许路由器之间自动交换路由信息并动态调整路由表以适应网络变化。

动态 RIP 使得 CVR100W 可以自适应物理上的网络拓扑变化并与其它路由器交换路由表信息。 CVR100W 通过计算起始点与目标点之间最优化 （跳数最少）的路径选择数据包如何路由。默认情况下， RIP 处于禁用状态。

配置动态路由的步骤：

步骤 1 单击 “网络配置” - “路由配置”。

步骤 2 在 “动态路由”部分，您需要设置以下内容：

RIP	勾选 “启用”， CVR100W 使用 RIP 进行路由选择。
RIP 发送数据包版本	选择 RIP 发送数据包版本：RIPv1 或者 RIPv2。 发送路由更新的 RIP 数据包版本必须与网络上其它路由保持同步，因此版本号取决于其它路由器的配置。 建议您联系网络管理员确定 RIP 版本信息。 RIPv2 向下兼容 RIPv1。
RIP 接收数据包版本	选择 RIP 接收数据包版本。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

静态路由

您可以配置静态路由，指定数据包抵达目标节点的路径。静态路由预先设定了数据包的转发路径，包括必须经过的主机或网络。某些网络服务提供商会为用户建立静态路由而非使用动态路由协议。静态路由的优点在于不需要消耗 CPU 资源与对端路由器交换路由信息。

您也可以使用静态路由抵达不支持动态路由协议的对端路由器。静态路由可以与动态路由一同使用。

注意 设置静态路由时不要在网内引入路由环路。

配置静态路由的步骤：

步骤 1 单击 “网络配置” - “路由配置”。查看 “静态路由” 部分。

步骤 2 在 “路由表项” 下拉菜单中，选择一个路由表项。

如果您希望删除该路由表项，请单击 “删除该条目”。

步骤 3 配置所选择的路由表项需要输入以下信息：

路由名称	输入该静态路由的名称。
目标 **IP**	输入目标节点的 IP 地址。
子网掩码	输入目标网络的子网掩码。
网关	输入该路由所使用的网关 IP 地址。
设备接口	选择该路由发送数据包的接口： ▪ LAN：选中此项表示该路由发送数据包到 LAN。 ▪ WAN：选中此项表示该路由发送数据包到 Internet（WAN）。

步骤 4 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

VLAN 间路由

配置 VLAN 间路由的步骤：

步骤 1 单击 “网络配置” - “路由配置”。

步骤 2 在 “**VLAN** 间路由” 部分，勾选 “启用”，启用 VLAN 间路由。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

路由表

查看路由表信息的步骤：

步骤 1 单击 “网络配置” - “路由配置”。

步骤 2 在 “路由表” 部分，单击 “显示 **IPv4** 路由表”，显示 IPv4 路由表。

步骤 3 在 “路由表” 部分，单击 “显示 **IPv6** 路由表”，显示 IPv6 路由表。

只有在您的 LAN 端口和 WAN 端口使用 IPv6 模式时，才能够查看 IPv6 路由表。

步骤 4 路由表中显示以下信息：

目标 **IP**	（IPv4）该路由的目标节点的 IP 地址。
子网掩码	（IPv4）该路由的目标网络的子网掩码。
默认网关	（IPv4）该路由的目标网络的网关。
设备接口	（IPv4）该路由所通过的路由器接口。
目标	（IPv6）该路由的目标节点的 IP 地址。
下一跳	（IPv6）该路由的下一跳 IP 地址。
设备接口	（IPv6）该路由所通过的路由器接口。

DDNS 配置

DDNS （Dynamic DNS，动态域名服务）是一种能够将不同 IP 地址绑定到一个固定互联网域名的服务功能。在配置 DDNS 之前，您必须向动态域名提供商申请一个动态域名账号，例如：3322.org 或 peanuthull.com。

CVR100W 会向 DDNS 服务器提供 WAN 中 IP 地址的变化情况，以此确保您能够使用域名访问所在网络的服务。

配置 DDNS 的步骤：

步骤 1 单击 “网络配置” - “**DDNS** 配置”。

步骤 2 在 “**DDNS** 服务” 下拉菜单中，您可以执行以下操作之一：

- 选择 “禁用”，禁止 DDNS 服务。
- 选择相应动态域名提供商，启用 DDNS 服务。

步骤 3 如果您没有所选动态域名提供商的账号，请单击该提供商的链接，申请账号。

步骤 4 您需要输入以下信息：

用户名	输入 DDNS 账号的用户名。
密码	输入 DDNS 账号的密码。
设备名称	（3322.org）输入 DDNS 服务器的主机名称。
WAN IP 地址	（3322.org）显示 CVR100W 的 WAN IP 地址。
设备状态	（3322.org）显示 DDNS 账号信息是否成功发送到服务器。
域名	（peanuthull.com）显示 DDNS 账号所申请的域名。
用户级别	（peanuthull.com）显示 DDNS 账号的用户级别。
设备状态	（peanuthull.com）显示 DDNS 账号信息是否成功发送到服务器。

步骤 5 单击 “测试配置”，测试您之前所作的 DDNS 配置。

步骤 6 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

IP 模式配置

在 “IP 模式配置”页面，您可以配置 LAN 与 WAN 的 IP 模式。

配置 IP 模式的步骤：

步骤 1 单击 “网络配置” - “**IP** 模式配置”。

步骤 2 在 “**IP** 模式配置”下拉菜单中，请选择以下选项之一：

LAN:IPv4 WAN:IPv4	如果 LAN 端口与 WAN 端口都使用 IPv4，选择此项。

LAN:IPv6 WAN:IPv4	如果 LAN 端口使用 IPv6， WAN 端口使用 IPv4，选择此项。
LAN:IPv6 WAN:IPv6	如果 LAN 端口与 WAN 端口都使用 IPv6，选择此项。
LAN:IPv4+IPv6 WAN:IPv4	如果 LAN 端口使用 IPv4/IPv6， WAN 端口使用 IPv4，选择此项。
LAN:IPv4+IPv6 WAN:IPv4+IPv6	如果 LAN 端口与 WAN 端口都使用 IPv4/IPv6，选择此项。

步骤 3 （可选）如果您使用 IPv6 到 IPv4 的隧道。即：允许 IPv6 的数据包在 IPv4 网络上传输。请执行以下操作：

- 单击 “显示静态 **6to4 DNS**”。
- 在 “**Domain**” 与 “**IP**” 部分，输入 5 个 Domain 到 IP 地址的映射。

IPv6 到 IPv4 的隧道的典型运用是：当一个站点或者终端用户希望使用现有 IPv4 网络访问 IPv6 网络。

步骤 4 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

IPv6 配置

当 CVR100W 的 LAN 端口与 WAN 端口都使用 IPv6 模式时，“网络配置” 下新增 “IPv6 配置” 子菜单。您可以在 “IPv6 配置” 子菜单中进行以下内容的配置：

IPv6WAN 配置

您需要根据您所处的 WAN 环境配置 IPv6 的网络连接类型。

如果您的网络服务提供商动态分配 IPv6 地址，您需要将 CVR100W 配置用作 DHCPv6 客户端，自动获取动态 IP ；如果您的网络服务提供商提供静态 IPv6 地址，您需要在 CVR100W 上绑定该地址。

设置 IP 模式

您必须将 LAN 端口与 WAN 端口设为 IPv6 模式后才能进行 CVR100W 的 IPv6 WAN 配置。

您可以将 IP 模式设为 LAN:IPv6, WAN:IPv6 或者 LAN:IPv4+IPv6, WAN:IPv4+IPv6。详见 IP 模式配置。

自动配置 -DHCPv6

如果您的网络服务提供商动态分配 IP 地址，您需要将 CVR100W 设为 DHCPv6 客户端。

将 CVR100W 设为 DHCPv6 客户端的步骤：

步骤 1 单击 “网络配置” - “**IPv6**” - “**IPv6WAN** 配置”。

步骤 2 在 “**WAN** 连接类型”部分，选择 “自动配置 **- DHCPv6**”。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

静态 IPv6

如果您的网络服务提供商分配固定 （静态）的 IP 地址，您需要将 CVR100W 设为使用静态 IPv6 地址。

将 CVR100W 设为使用静态 IPv6 地址的步骤：

步骤 1 单击 “网络配置” - “**IPv6**” - “**IPv6WAN** 配置”。

步骤 2 在 “**WAN** 连接类型”部分，选择 “静态 **IPv6**”。

步骤 3 在 “静态 **IP** 地址”部分，您需要输入以下信息：

IPv6 地址	输入 WAN 端口的 IPv6 地址。
IPv6 前缀长度	输入由网络服务提供商定义的 IPv6 前缀长度。 IPv6 网络由 IP 地址中的初始比特位所识别，这些初始比特位被称作前缀，所有位于 IPv6 网络中的主机拥有相同的 IPv6 地址前缀。例如，在 IP 地址 2001:0DB8：AC10：FE01 中，前缀为 2001。 前缀长度的输入范围为 0-127。
默认 **IPv6** 网关	输入默认网关的 IPv6 地址。
静态 **DNS 1**	输入第一 DNS 服务器 IP 地址。
静态 **DNS 2**	输入第二 DNS 服务器 IP 地址。

步骤 4 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

IPv6LAN 配置

在 IPv6 模式下，局域网 DHCP 服务器默认启用 （类似于 IPv4 模式）。 DHCPv6 服务器使用已配置的地址池分配 IPv6 地址，该地址池使用局域网中设定的 IPv6 前缀长度。

设置 IP 模式

您必须将 IP 模式设置成以下模式之一时，才能够配置 CVR100W 的相关 IPv6 设置：

- 局域网：IPv6 ；广域网：IPv4。
- 局域网：IPv6 ；广域网：IPv6。
- 局域网：IPv4+IPv6 ；广域网：IPv4。

详见 IP 模式配置。

IPv6

配置 IPv6 LAN 地址的步骤：

步骤 1 单击 “网络配置” - “**IPv6**” - “**IPv6LAN** 配置”。

步骤 2 您需要输入以下信息，配置 IPv6 LAN 地址。

IPv6 地址	输入 CVR100W 的 IPv6 地址。 默认 IPv6 地址为 fec0::1。您可以修改该地址。
IPv6 前缀长度	输入 IPv6 前缀长度。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

服务器配置 （DHCPv6）

配置 DHCPv6 的步骤：

步骤 1 单击 “网络配置” - “**IPv6**” - “**IPv6LAN** 配置”。

步骤 2 您需要输入以下信息：

DHCP 状态	勾选 “启用”，启用 DHCPv6 服务。 启用状态下， CVR100W 会为网内请求 DHCP 服务的终端分配 IP 地址，这些 IP 地址在指定的地址池范围内。
域名	输入 DHCPv6 服务器的域名。
服务器首选项	输入 DHCP 服务器首选项 （优先级）。 拥有较高优先级的 DHCP 服务器在对网内主机发布通告消息时优于其它较低优先级的 DHCP 服务器。 输入范围为 0-255，默认设置为 255。
静态 **DNS 1**	输入第一 DNS 服务器 IP 地址。
静态 **DNS 2**	输入第二 DNS 服务器 IP 地址。
地址租期	输入地址租期时长 （单位：分钟），该时长表示网内终端的 IPv6 地址租约期限。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

IPv6 地址池配置

当 CVR100W 作为 DHCPv6 服务器时，内部网络客户端的 IP 地址由 CVR100W 分配，所分配的 IP 地址取自 IPv6 地址池。同时，您可以定义所分配的 IPv6 地址的前缀长度。

配置 IPv6 地址池的步骤：

步骤 1 单击 “网络配置” - “**IPv6**” - “**IPv6LAN** 配置”。

步骤 2 在 “**IPv6** 地址池列表” 中，单击 “添加条目”。

步骤 3 您需要输入以下信息：

起始地址	输入 IPv6 地址池的起始地址。
结束地址	输入 IPv6 地址池的结束地址。
IPv6 前缀长度	输入 IPv6 前缀长度。

步骤 4 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

如果您希望修改地址池相关设置，请选择相应地址池并单击 “编辑”；如果您希望删除相应地址池，请选择相应地址池并单击 “删除”；单击 “保存”，保存您之前所作的配置。

IPv6 静态路由

您可以配置静态路由，指定数据包抵达目标节点的路径。静态路由预先设定数据包的转发路径，包括必须经过的主机或网络。

某些网络服务提供商会为用户建立静态路由而非使用动态路由协议。静态路由的优点在于不需要消耗 CPU 资源与对端路由器交换路由信息。

您也可以使用静态路由抵达不支持动态路由协议的对端路由器。静态路由可以与动态路由一同使用。

创建静态路由的步骤：

步骤 1 单击 “网络配置” - “**IPv6**” - “**IPv6** 静态路由”。

步骤 2 在 “**IPv6** 静态路由列表”中，单击 “添加条目”。

步骤 3 您需要输入以下信息：

路由名称	输入路由名称。
目标	输入目标主机或网络的 IPv6 地址。
前缀长度	输入 IPv6 地址的前缀长度，该长度由目标子网定义。
网关	输入目标主机或网络所在网关的 IPv6 地址。
设备接口	在下拉菜单中选择接口类型：LAN、 WAN 或 IPv6 到 IPv4。

度量	输入路由优先级，由 2 到 15 的数字表示。当多个路由连接到同一个目标节点，拥有最低度量的路由会被使用。
启用	勾选 “**启用**”，启用该路由。 路由表中显示所有路由，包括处于激活与未激活状态的路由。未激活状态的路由不会被 CVR100W 所使用。您可以在任何时候激活该路由。 当您添加路由时，如果该路由所连接的网络不可用，您将不能激活该路由直到该路由所连接的网络恢复使用。

步骤 4 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

如果您希望修改静态路由相关设置，请选择相应静态路由并单击 “编辑”；如果您希望删除相应静态路由，请选择相应静态路由单击 “删除”；单击 “保存”，保存您之前所作的配置。

路由 （RIPng）

RIPng （RIP Next Generation，下一代路由信息选择协议）是一种基于距离矢量 （D-V）的路由协议。 RIPng 通过端口 521 使用 UDP 数据包交换路由信息。

RIPng 使用跳跃数测量起始节点与目标节点之间的距离，跳跃数是一种度量或者称之为一种代价。从一个路由器到一个直接连接的网络，其跳跃数为 0。两个直接相连的路由器之间跳跃数为 1。当跳跃数大于等于 16 时，我们认为目标网络或主机不可达。

默认设置下，路由信息每 30 秒更新一次；如果 CVR100W 在大于 180 秒的时间内未接收到相邻节点的路由更新信息，那么 CVR100W 认为该相邻节点不可达；如果 CVR100W 在之后大于 240 秒的时间内未接收到任何路由更新信息，那么 CVR100W 会将该路由从路由表中移除。

CVR100W 默认情况下禁用 RIPng。

配置 RIPng 的步骤：

步骤 1 单击 “网络配置” - “**IPv6**” - “路由 （**RIPng**）”。

步骤 2 勾选 “启用”，启用 RIPng。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

6to4 隧道

6to4 隧道 （IPv6-IPv4 隧道）允许 IPv6 数据包在 IPv4 网络上进行传输。

6to4 隧道的典型应用是：一个站点或者终端用户希望使用现有 IPv4 网络访问 IPv6。

配置 6to4 隧道的步骤：

步骤 1 单击 “网络配置” - “**IPv6**” - “**6to4** 隧道”。

步骤 2 在 “自动隧道” 部分，勾选 “启用”，启用 6to4 隧道。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

IPv6 隧道状态

“IPv6 隧道状态” 页面显示通过 WAN 端口建立的隧道。

查看 IPv6 隧道状态的步骤：

步骤 1 单击 “网络配置” - “**IPv6**” - “**IPv6** 隧道状态”。

步骤 2 单击 “刷新”，显示 IPv6 隧道的最新信息。

“**IPv6** 隧道状态列表” 显示隧道名称以及 IPv6 地址。

路由器通告

CVR100W 内置 RADVD （Router Advertisement Daemon，路由通告守护进程），监听 IPv6LAN 上对于 CVR100W 的请求并且以路由通告作为回应。

配置 RADVD 步骤：

步骤 1 单击 “网络配置” - “**IPv6**” - “路由器通告”。

步骤 2 您需要输入以下信息：

RADVD 状态	选中 “启用”，启用 RADVD。

通告模式	请选择以下模式之一： ▪ 未经请求的组播：如果您选择该模式， CVR100W 会向组内所有接口发送路由通告。 ▪ 仅单播：如果您选择该模式，CVR100W 会严格限制路由通告的发送，只有已知地址的接口才会收到路由通告。
通告间隔	如果您选择 “未经请求的组播”作为通告模式，请输入通告间隔的数值 （4-1800），默认值为 30。 通告间隔是一个位于最小路由通告间隔与最大路由通告间隔之间的随机数。 最小路由通告间隔 =0.33 ×最大路由通告间隔
RA 标志位	如果您选择 “已管理”， CVR100W 将使用管理状态协议为地址进行自动配置。 如果您选择 “其它”， CVR100W 将使用管理状态协议为其它非地址信息进行自动配置。
路由器首选项	您可以从下拉菜单中选择 “高、中等、低”，默认值为 “中等”。 路由器首选项为默认路由器提供了一种优先级度量。这一度量使用路由通告报文中未被使用的空闲比特位，用于表示高、中等、低的优先级别。 这一扩展对于路由器与主机都是向下兼容的，在未实现路由器优先级的主机上这一比特位都会被忽略。
MTU	输入 MTU 的值 （0 或 1280 - 1500）。默认值为 1500。
路由器生命期	输入路由器的生命时长，表示路由通告存在的时间 （单位：秒）。默认值为 3600。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

通告前缀

配置通告前缀的步骤：

步骤 1 单击 “网络配置” - “**IPv6**” - “通告前缀”。

步骤 2 单击 “添加条目”。

步骤 3 在 “通告表前缀” 中输入以下信息：

IPv6 前缀类型	您需要从下拉菜单中选择以下类型之一： **IPv6** 到 **IPv4**：如果您选择该类型，将允许 IPv6 数据包在 IPv4 网络上进行传输。 6to4 隧道的典型应用是：一个站点或者终端用户希望使用现有的 IPv4 网络访问 IPv6。 全局 / 本地：如果您选择该类型，您可以使用一个全局唯一的 IPv6 地址或者本地唯一的 IPv6 地址。
SLA ID	如果您选择 “IPv6 到 IPv4” 作为 IPv6 前缀类型，请输入 SLA ID （Site - Level Aggregation ID，站点级聚合标识符）。
IPv6 前缀	如果您选择 “全局 / 本地” 作为 IPv6 前缀类型， IPv6 前缀指定 IPv6 网络地址。
IPv6 前缀长度	如果您选择 “全局 / 本地” 作为 IPv6 前缀类型，请输入前缀长度值。
前缀生命时长	路由器允许使用前缀的时长。

步骤 4 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

3

无线配置

本章为您介绍如何配置 CVR100W 的无线网络。包括以下内容：

- 无线安全
- 路由器无线网络
- 基本配置
- 高级配置
- 配置 WDS
- 配置 WPS

无线安全

无线网络技术拥有使用便捷、容易安装等优点，众多拥有高速网络接入的中小企业与家庭用户都愿意使用无线网络。然而，由于无线网络是通过无线信号收发数据，因此相比于传统有线网络更易遭受攻击。

无线安全提示

首先需要注意的是，您不可能从物理上阻止他人连接您的无线网络，但是您可以通过以下步骤提升您的无线网络安全性。

- 修改默认无线网络名称 （SSID）。

  每一个无线设备都拥有一个默认的无线网络名称 （SSID），用于标识该网络，名称长度可达 32 位。为了保护您的网络，请修改默认名称，修改的名称必须与您身边存在的其它无线网络名称不同，以此保证您无线网络名称的唯一性。

  当您修改无线网络名称时，请勿使用个人信息 （例如：您的身份证号），因为这些信息在他人搜索无线网络时是可见的。

- 修改默认密码。

每一个无线设备如无线接入点、路由器以及网关，都需要用户输入密码才能够修改其设置，这些设备一般都有一个默认密码。黑客了解这些默认值并且会尝试使用这些默认值连接您的无线设备，修改您的网络设置。所以您必须及时修改您的密码，阻止未经授权的访问。

- 启用 MAC 地址过滤。

  CVR100W 为您提供 MAC 地址过滤功能。 MAC 地址是每一个网络设备都拥有的唯一标识。通过 MAC 地址过滤功能，拥有指定 MAC 地址的网络设备才能够访问无线网络。例如：您可以只允许您信任的主机 MAC 地址，保证只有这些主机能够访问您的无线网络。

- 启用加密技术。

  加密技术可以保护无线网络上的数据传输。 WEP/WPA/WPA2 对于无线通讯提供不同级别的安全保护。现在 WIFI 认证的无线设备必须支持 WPA2，可选支持 WEP。

  WEP 是一种较老的加密标准，在一些较老的设备上可能只支持 WEP 不支持 WPA， WPA/WPA2 使用动态密钥进行加密，所以能够提供相比于 WEP 更为安全的网络保护。为了保护您的无线网络传输安全，您应该启用网络设备商所支持的最高等级的安全保护模式。

- 将无线路由器、无线接入点或者网关放置于远离外墙或窗户的位置。
- 在无线路由器、无线接入点或者网关未使用时请关闭电源或关闭无线信号。（例如：夜晚、假期）
- 请您使用至少 8 位以上的高安全级别密码，混合使用字母与数字，避免使用标准单词。

网络安全指南

如果您的内部网络设备本身并不安全，那么对于无线网络的安全措施只能是徒劳的。我们建议您采取以下防范措施：

- 用密码保护内部网络上的所有主机，并且对于敏感文件单独设置密码保护。
- 定期修改密码。
- 安装杀毒软件与防火墙。
- 禁用文件共享 （点对点），阻止未经授权的共享文件请求。

路由器无线网络

CVR100W 提供 4 个虚拟无线网络 （即 4 个 SSID）。您可以修改这 4 个虚拟无线网络的名称。下表描述了这些网络的默认设置：

SSID	cisco-xxxx	cisco-ssid2	cisco-ssid3	cisco-guest
启用	是	否	否	否
SSID 广播	启用	禁用	禁用	禁用
安全模式	WPA2 混合模式	禁用	禁用	禁用
MAC 地址过滤	禁用	禁用	禁用	禁用
VLAN	1	1	1	3
SSID 无线隔离	禁用	禁用	禁用	启用
WMM	启用	启用	启用	启用
WPS 按钮	启用	禁用	禁用	禁用

基本配置

基本无线配置

配置无线基本设置的步骤：

步骤 1 单击 “无线配置” - “基本配置”。

步骤 2 在 “无线” 部分，勾选 “启用”，启用 CVR100W 的无线功能。

默认设置下只有 1 个无线网络启用，即 cisco-xxxx。

步骤 3 在 “信号强度” 部分，从下拉菜单中选择 CVR100W 的 Wi-Fi 信号强度：100% 或 50%。

步骤 4 在 “工作模式” 部分，从下拉菜单中选择以下选项之一：

B/G/N-Mixed	如果您的网络中拥有 Wireless-N、 Wireless-B 与 Wireless-G 设备，请选择此项。此项是默认的无线网络模式 （建议启用此项）。
B-Only	如果您的网络中只有 Wireless-B 设备，请选择此项。
G-Only	如果您的网络中只有 Wireless-G 设备，请选择此项。
N-Only	如果您的网络中只有 Wireless-N 设备，请选择此项。
B/G-Mixed	如果您的网络中拥有 Wireless-B 与 Wireless-G 设备，请选择此项。
G/N-Mixed	如果您的网络中拥有 Wireless-G 与 Wireless-N 设备，请选择此项。

步骤 5 在 “工作频段”部分，选择无线网络的工作频段：20MHz、 20/40MHz 或 40MHz。

步骤 6 在 “信道选择”部分，从下拉菜单中选择相应的无线信道。

步骤 7 在 “**AP** 管理 **VLAN**”部分，如果您使用的是默认设置，请选择 VLAN 1。

只有处于管理 VLAN 中的无线客户端才能够访问 CVR100W。

该操作是出于安全目的，您可以通过修改 VLAN 管理以限制对 CVR100W 的访问。

步骤 8 （可选）在 “**U-APSD** （**WMM** 省电模式）”部分，勾选 “启用”，启用 U-APSD。

U-APSD 是一种用于优化实时应用 （如 VoIP 与 WLAN 上全双工传输）的协议，它将输出 IP 流量分类，赋予语音数据较高优先级，从而提高电能使用效率并使传输延迟最小。

步骤 9 （可选）在 “无线列表”部分，您可以配置 4 个无线网络的相关参数，详见配置无线网络。

步骤 10 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

配置无线网络

无线列表显示 CVR100W 支持的 4 个无线网络的相关信息。

配置无线网络的步骤：

步骤 1 在复选框中选择您希望配置的网络，单击 “编辑” 按钮。

步骤 2 进入以下设置项：

启用 **SSID**	勾选启用该无线网络。
SSID 名称	修改无线网络的名称。
SSID 广播	勾选启用 SSID 广播。
安全模式	（只读）详见设置安全模式。
MAC 过滤	（只读）详见设置 MAC 过滤。
VLAN	选择相应的 VLAN，将其关联到该无线网络。
二层隔离	勾选启用该 SSID 的无线隔离。
WMM	勾选启用 WMM (Wi-Fi Multimedia)。
WPS 硬件按钮	点选此项，与 CVR100W 前面板的 WPS 按键配合，启用无线网络的 WPS 功能。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

设置安全模式

您可以为无线网络配置以下安全模式之一：

配置 WEP

WEP 安全模式提供一种使用基本加密的安全防范模式，相比 WPA 安全性较弱。如果您的网络设备不支持 WPA，那么您只能配置使用 WEP。

如果您并不是有特殊需求必须使用 WEP，我们强烈建议您使用 WPA2。

配置 WEP 安全模式的步骤：

步骤 1 在 “无线列表” 部分 （“无线配置” - “基本配置”），选择您希望配置的网络。

步骤 2 单击 “设置安全模式”，转到 “安全配置” 页面。

步骤 3 在 “选择 **SSID**” 部分，请选择您希望配置安全模式的 SSID。

步骤 4 在 “安全模式” 菜单中，请选择 “**WEP**”。

步骤 5 在 “认证类型” 部分，请选择以下选项之一：

- 开放系统：此项为默认设置。
- 共享密钥：仅在您的网络管理员建议您选择此项是启用，如果您不确定，请保持默认选择。

在以上两种情况下，所有的无线客户端访问无线网络时必须提供共享密钥。

步骤 6 在 “加密算法” 部分，请选择加密技术类型：

- **10/64bit** （**5** 位 **ASCII** 码或 **10** 位十六进制数）：提供长度为 40bit 的密钥。
- **26/128bit**（**13** 位 **ASCII** 码或 **26** 位十六进制数）：提供长度为 104bit 的密钥，拥有更强的加密性，使密钥更难被破解。我们建议使用 128bit 的加密技术类型。

步骤 7 （可选）在 “口令” 部分，输入字母及数字的组合 （建议您输入的长度大于 8 位），然后单击 “生成密钥”，页面下方的 WEP 密钥区域会生成密钥。

如果您希望使用自己的密钥，请直接在 “密钥 **1**” 区域输入密钥。对于 64bit 的 WEP，密钥长度为 5 位 ASCII 码 （或 10 位十六进制字符）；对于 128bit 的 WEP，密钥长度为 13 位 ASCII 码 （或 26 位十六进制字符）。合法的十六进制字符为 0 到 9 与 A 到 F。

步骤 8 勾选 “显示密钥”，“密钥” 区域的密钥将以明文显示。

步骤 9 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

步骤 10 单击 “返回”，返回 “基本配置” 页面。

配置 WPA-Personal、 WPA2-Personal 与 WPA2-Personal Mixed

WPA-Personal、 WPA2-Personal 与 WPA2-Personal Mixed security 安全模式提供了优于 WEP 的安全性。

- **WPA-Personal**：WPA 是无线安全标准 （IEEE 802.11i）中的一部分，在 IEEE 802.11i 标准准备过程中， WPA 由 Wi-Fi 联盟标准化，并定义为取代 WEP 的过渡措施。 WPA-Personal 支持 TKIP 与 AES 加密。
- **WPA2-Personal**：（建议选择此项） WPA2 是 IEEE 802.11i 中安全标准的最终实现。 WPA2 支持 AES 加密，使用 PSK 进行认证。
- **WPA2-Personal Mixed**：允许 WPA 与 WPA2 客户端连接，使用 PSK 认证。

PSK 通过字母与数字组成的字符串实现个人用户认证，每个无线对等端共享该字符串。

配置 WPA Personal 安全模式的步骤：

步骤 1 在“无线列表”部分 （“无线配置” - “基本配置”），选择您希望配置的网络。

步骤 2 单击“设置安全模式”，转到 “安全配置”页面。

步骤 3 在 “选择 **SSID**”部分，请选择您希望配置安全模式设置的 SSID。

步骤 4 在 “安全模式”菜单中，选择 3 种 WPA-Personal 模式之一。

步骤 5 （以 WPA-Personal 为例）在 “加密算法”部分，请选择以下选项之一：

- **TKIP/AES**：选择此项，能够与较老的不支持 AES 的无线网络设备兼容。
- **AES**：选择此项，能够获得更高的安全性。

步骤 6 在 “安全密钥”部分，输入字母与数字的组合 （8 到 63 位 ASCII 码或者 64 位十六进制数）。

步骤 7 勾选 “显示密钥”，“安全密钥”区域的密钥内容将以明文显示。

步骤 8 在 “密钥更新周期”部分，输入密钥更新的时间间隔 （600-7200）。默认值为 3600 秒。

步骤 9 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

步骤 10 单击 “返回”，返回 “基本配置”页面。

配置 WPA-Enterprise、 WPA2-Enterprise 与 WPA2-Enterprise Mixed

WPA-Enterprise、 WPA2-Enterprise 与 WPA2-Enterprise Mixed 安全模式使用 RADIUS 服务器认证。

- **WPA-Enterprise**：通过 RADIUS 服务器认证使用 WPA。
- **WPA2-Enterprise**：通过 RADIUS 服务器认证使用 WPA2。
- **WPA2-Enterprise Mixed**：通过 RADIUS 服务器认证使用 WPA 与 WPA2。

配置 WPA-Enterprise 安全模式的步骤：

步骤 1 在 “无线列表”部分 （“无线配置” - “基本配置”），选择您希望配置的网络。

步骤 2 单击 “设置安全模式”，转到 “安全配置”页面。

步骤 3 在 “选择 **SSID**”部分，请选择您希望配置安全模式设置的 SSID。

步骤 4 在 “安全模式”菜单中，选择 3 种 WPA-Enterprise 模式之一。

步骤 5 （以 WPA-Enterprise 为例）在 “加密算法”部分，选择以下选项之一：

- **TKIP/AES**：选择此项，能够与较老的不支持 AES 的无线网络设备兼容。
- **AES**：选择此项，能够获得更高的安全性。

步骤 6 在 “**RADIUS** 服务器”部分，输入 RADIUS 服务器的 IP 地址。

步骤 7 在 “**RADIUS** 端口”部分，输入用于访问 RADIUS 服务器的端口。

步骤 8 在 “共享密钥”部分，输入字母与数字的组合 （8 到 63 位 ASCII 码或者 64 位十六进制数）。

步骤 9 在 “密钥更新周期”部分，输入密钥更新的时间间隔 （600-7200）。默认值为 3600 秒。

步骤 10 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

步骤 11 单击 “返回”，返回 “基本配置”页面。

设置 MAC 过滤

当某一设备请求访问无线网络时，您可以使用 MAC 地址过滤功能：根据该设备的 MAC 地址允许或者拒绝其访问。例如：您可以输入一组您所信任的主机的 MAC 地址，只允许这些主机访问您的无线网络。

您可以为每一个无线网络 （SSID）配置不同的 MAC 地址过滤。

配置 MAC 地址过滤的步骤：

步骤 1 在 “无线列表”部分 （“无线配置” - “基本配置”），选择您希望配置的网络。

步骤 2 单击 “设置 **MAC** 过滤”，转到 “无线 **MAC** 过滤”页面。

步骤 3 在 “**SSID**”部分，显示您正在配置 MAC 地址过滤的 SSID。

步骤 4 在 “无线 **MAC** 过滤”部分，勾选 “启用”，启用该无线网络的 MAC 地址过滤功能。

步骤 5 在 “接入控制”部分，选择连接控制类型：

- 黑名单：只阻止在 MAC 地址列表中的设备访问。默认选择此项。
- 白名单：只允许在 MAC 地址列表中的设备访问。

步骤 6 单击 “显示关联客户端列表”，显示该 SSID 无线网络内的主机或其它设备。

步骤 7 如果您希望将某个设备加入到 “无线 MAC 过滤列表”，请点击 “添加到无线 **MAC** 过滤列表”，将 “无线关联客户端列表”中所选的设备加入到 “无线 MAC 过滤列表”。

步骤 8 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

步骤 9 单击 “返回”，返回 “基本配置”页面。

访问时间控制

为了更进一步保护您的网络，您可以限制用户访问无线网络的具体时间范围。

配置访问时间控制的步骤：

步骤 1 在 “无线列表”部分 （“无线配置” - “基本配置”），选择您希望配置的网络。

步骤 2 单击 “访问时间控制”，转到 “访问时间控制”页面。

步骤 3 勾选 “启用”，启用该无线网络下的访问时间控制功能。

步骤 4 在 “开始时间”与 “结束时间”部分，输入一天 24 小时中允许访问网络的时间。

步骤 5 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

步骤 6 单击 “返回”，返回 “基本配置”页面。

设置访客网络

SSID4 （默认名为 cisco-guest）是 CVR100W 的访客网络，外部访客可以通过该 SSID 访问 Internet，同时保证中小企业或家庭用户的内部网络安全不受外部访客影响。

配置访客网络的步骤：

步骤 1 在 “无线列表”部分 （“无线配置” - “基本配置”），选择 SSID4 （默认名为 cisco-guest）。

步骤 2 单击 “设置访客网络”，转到 “访客网络配置”页面。

在 “访客网络用户名”部分，显示访客网络的名称。

步骤 3 在 “访客网络密码”部分，您可以设置访客网络的密码。

步骤 4 勾选 “隐藏密码”，密码以密文形式显示。

步骤 5 在 “访客网络租期”部分，您可以设置访客网络的租期时间 （1-9999 分钟），默认值为 120。

步骤 6 在 “允许访客总数”部分，您可以设置访客网络的用户上限 （1-10），默认值为 5。

步骤 7 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

步骤 8 单击 “返回”，返回 “基本配置”页面。

高级配置

如果您对无线网络并不十分熟悉，请不要随意修改无线网络高级配置，错误的设置将会导致无线网络性能降低。

配置无线高级设置的步骤：

步骤 1 单击 “无线配置” - “高级配置”，转到 “高级配置”页面。

步骤 2 您可以配置以下信息：

Frame Burst	启用此项可以提高您的无线网络性能，这具体取决于您的无线产品制造商。如果您不是十分了解此项，请保持默认设置 （启用）。
WMM No Acknowledgement	启用此项可以实现更高的网络吞吐量，但是如果您的无线网络频段有较大的噪声干扰，数据包传输会因此出现很高的错误率。默认设置为禁用。

基本速率	此项设置的基本速率并非实际的传输速率，而是 SRP（Services Ready Platform）可以达到的一组最大速率。 CVR100W 会将基本速率通告网内的所有无线设备，告知它们 CVR100W 会使用的速率。 SRP 也会通告：它会自动选择最佳传输速率。 默认设置为 “默认值”。 CVR100W 可以工作在所有标准无线速率（1-2Mbps， 5.5Mbps， 11Mbps， 18Mbps，24Mbps 等）下，支持 Wireless-B、 Wireless-G 和 Wireless-N 的速率。 “1-2Mbps”选项用于较老的无线技术环境； “全部”选项使得 CVR100W 可以工作在任何速率。 基本速率并不是数据传输的真实速率。如果您希望指定 CVR100W 的数据传输速率，请通过 “传输速率”进行配置。
传输速率	数据传输速率取决于您的无线网络连接速率。 您可以在传输速率范围内选择合适的数值，或者选择 “自动”， CVR100W 会自动使用可达的最快数据传输速率并启用自适应功能。 自适应功能够在 CVR100W 与无线客户端之间商议得出最佳的速率。默认设置为 “自动”。
N Transmission Rate	Wireless-N 数据传输速率取决于您的 Wireless-N 网络连接速率。 您可以在传输速率范围内选择合适的数值，或者选择 “自动”， CVR100W 会自动使用可达的最快数据传输速率并启用自适应功能。 自适应功能会在 CVR100W 与无线客户端之间商议得出最佳的速率。默认设置为 “自动”。
CTS Protection Mode	当您的 Wireless-N 与 Wireless-G 设备在拥堵的 IEEE 802.11b 网络环境下发生严重问题不能传输数据到 CVR100W 时， CVR100W 自动运行该模式。 该模式增强 CVR100W 捕获所有 Wireless-N 与 Wireless-G 传输的能力，但会严重降低性能。默认设置为 “自动”。

Beacon 间隔	该数值表示 Beacon 的发送频率。 Beacon 是 CVR100W 用于同步无线网络的群发数据包。 输入的数值必须在 40 到 3500 毫秒之间。默认值为 100 毫秒。
DTIM 间隔	DTIM 的间隔时间用于 DTIM 倒数计时通知客户端准备用于监听广播与组播消息的窗口。 当 CVR100W 正在缓冲相关的客户端广播或者组播消息时， CVR100W 在 DTIM 时间间隔后发送下一个 DTIM。客户端监听到并唤醒自身接收广播与多播消息。 输入的数值必须在 1 到 255 之间。默认值为 1。
Fragmentation 临界值	数据进行传输时会划分为多个数据包，该数值决定了每一个数据包的最大长度。如果您的网络存在较高的数据报错误率，您可以略微提高该数值。 需要注意的是该数值设置过小会导致较差的网络性能，所以我们建议您如果修改，请只是略微减小默认值以保证性能。默认值为 2346。
RTS 临界值	如果您遇到不一致的数据流，请略微减小该数值。默认值为 2347，我们建议保持此默认值。 如果网络中的数据包长度小于预设的数值， RTS/CTS 机制不会启用。 SRP 会给特定站点发送 RTS 帧，并协商数据帧的发送。 无线站点在收到 RTS 帧之后，会以 CTS 帧确认开始传输。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

配置 WDS

WDS （Wireless Distribution System，无线分布式系统）是一种能够使无线接入点之间相互桥接的系统，从而扩大无线覆盖范围。与此同时 WDS 并不会影响无线接入点本身的无线传输功能。

为了建立 WDS， CVR100W 与其它 WDS 对等端必须保证下列属性配置一致：无线网络模式、无线信道、无线频率以及加密类型。

注意 只有 SSID 1 （默认名称 cisco-xxxx）支持 WDS。

配置 WDS 的步骤：

步骤 1 单击 “无线配置” - “**WDS**”。

步骤 2 勾选 “允许无线信号被中继”，启用 WDS 功能。

步骤 3 您需要选择以下选项之一：

- 选择 “自动”，自动搜索周围开启 WDS 功能的无线接入点并进行中继；
- 选择 “手动”，手动输入中继 MAC 地址。

步骤 4 （手动）单击 “显示 **SSID** 搜索结果”。

在 “可用网络表” 中，显示可供连接的无线网络。

- （可选）单击 “刷新” 按钮，刷新表中的记录。
- 在 “可用网络表” 中，您最多可以选择 3 个接入点进行中继。
- 单击 “连接”，将所选接入点的 MAC 地址加入到下方的 MAC 地址区域。

步骤 5 如果您之前选择 “手动”，请输入 1-3 个无线接入点进行中继。

步骤 6 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

配置 WPS

您可以配置 WPS，使得支持 WPS 的设备可以方便快捷地连接无线网络。

通过 CVR100W 前面板上的 WPS 指示灯，您可以获取 WPS 功能的运行信息：

成功启动 **WPS**	WPS 指示灯显示为绿色并长亮， 120 秒后指示灯熄灭。
WPS 启动中	WPS 指示灯每 2 秒闪烁 1 次 （0.5Hz），持续 30 秒。
WPS 发生错误	WPS 指示灯每 1 秒闪烁 1 次 （1Hz），持续 30 秒。

会话重叠	WPS 指示灯快闪 （每 0.1 秒闪烁 1 次，即 0.1Hz） 1 秒熄灭 1 秒，持续 120 秒。
WPS 已成功配置或未配置	WPS 指示灯熄灭。

启用 WPS

步骤 1 单击 “无线配置” - “**WPS**”。打开 “**WPS**” 页面。

步骤 2 在 “**SSID**” 下拉菜单中，请选择您希望启用 WPS 的无线网络。

步骤 3 在 “**WPS**” 部分，勾选 “启用”，启用 WPS 功能。

步骤 4 在客户端设备上配置 WPS 的方法有 3 种。详细内容请参考 WPS 配置方法。

在您成功配置 WPS 后，“**WPS**” 页面下方会显示以下信息：

WPS 状态、网络名称 （SSID）以及安全模式。

WPS 配置方法

在客户端设备上配置 WPS 的方法有 3 种，包括：

WPS 配置方法 1

如果您的客户端设备拥有 WPS 按钮，请选择此方法。

步骤 1 按下客户端设备上的 WPS 按钮。

步骤 2 在 “**WPS**” 页面上，单击 “**WPS**” 图标按钮。当 WPS 配置完成时，会弹出提示框。

步骤 3 单击 “确定”。

其它的指导信息请参考您客户端设备的说明文档。

WPS 配置方法 2

如果您的客户端设备拥有 WPS PIN 号码，请选择此方法。

步骤 1 在 “**WPS**” 页面，输入客户端设备上的 PIN 号码。

步骤 2 单击 “注册”。

步骤 3 在配置完成之后，单击 “确定”。

其它的信息指导请参考您客户端设备的说明文档。

WPS 配置方法 3

如果您的客户端设备需要从 CVR100W 获取 PIN 号码，请使用 WPS 页面上列出的号码。

4

安全配置

本章为您介绍如何配置 CVR100W 的安全特性。包括以下内容：

- 路由器安全特性
- 基本配置
- 计划管理
- 服务管理
- 访问控制
- 单端口转发
- 多端口转发
- 多端口触发

路由器安全特性

访问策略

访问策略是用户通过 CVR100W 控制网络访问的方式，您可以创建符合您需求的访问策略，以此保护您的网络。访问策略将有选择地阻止或允许您指定的网络流量，在您创建访问策略前，您需要了解访问策略包含的具体内容：

- 阻止或允许的服务类型以及流量类型 （例如：网页浏览、 VoIP）。
- 网络流量的 “开始区域”（LAN/WAN）与 “目标区域”（LAN/WAN）。
- 计划管理，设置使用访问策略的时间。
- 阻止或允许的关键词 （域名或网页 URL）。
- 通过 MAC 地址过滤，阻止那些试图访问您所在网络的设备。
- 通过端口触发机制，阻止或允许指定端口的服务。

- 记录的日志类型。

在您明确以上内容之后，您可以基于访问时间、网址或关键词建立相应的访问策略：阻止本地用户对某些应用与服务 （聊天室或游戏）的访问、保护本地主机不被外网访问。下面为您简要介绍入站规则与出站规则。

入站规则 （WAN 到 LAN）的作用是限制从外网到本地的流量，有选择地允许外网用户访问您的本地资源。默认设置下，除了响应来自于 LAN 的请求，其它所有来自于不安全 WAN 站点的访问请求都会被阻止。如果您希望外网设备能够安全地访问本地资源或服务，您必须为相应的服务创建安全规则。

出站规则 （LAN 到 WAN）的作用是限制从本地到外网的流量，有选择地允许本地用户访问外网资源。默认设置下，只允许来自安全区域 （LAN）到外网的访问。如果您希望希望禁止本地主机访问外网 （不安全 WAN）的服务，您必须为相应的服务创建安全规则。

最后，如果您希望开放您的内部网络，您必须将 CVR100W 的 WAN 端口 IP 地址对外公开。如何使您的 WAN 端口 IP 地址被外网所知取决于您的 WAN 端口配置：如果您的 WAN 端口 IP 地址是静态分配，您应该公布您的 IP 地址；如果您的 WAN 端口 IP 地址是动态的，您需要使用 DDNS。

端口转发

端口转发用于重定向来自于 Internet 的流量，将访问 WAN 侧某个端口的流量转发到 LAN 侧的某个端口。您可以配置公共服务或者自定义服务的端口转发。

注意 端口转发并不适用于局域网上的服务器。

端口转发功能在您使用一些特定的应用时是十分必要的。例如：当一个外部设备连接到某一应用时，该设备需要在一个指定的端口 （或端口范围）接收数据，才能够正常运行。此时您必须配置 CVR100W，使其能够在指定的端口 （或端口范围内）将输入数据传送到相应的应用。

另一个需要您使用端口转发的情况是：网关拥有一个需要开放的端口列表，包含公共应用和游戏的端口。您需要定义流量类型与输入输出端口范围，创建端口转发规则开放这些端口。

基本配置

进行基本安全配置的步骤：

步骤 1 单击 “安全配置” - “基本配置”。

步骤 2 您需要配置以下安全配置信息：

DoS 防护	勾选 “启用”，启用 DoS 防护功能。
禁止 **WAN** 侧请求	勾选 “启用”，阻止从 WAN 到 CVR100W 的访问请求。
IPv4 组播 **(IGMP Proxy)**	勾选 “启用”，启用组播功能。
UPnP	勾选 “启用”，启用 UPnP 功能。 UPnP 自动发现能够与 CVR100W 通信的设备。
允许用户配置	（UPnP）勾选 “启用”，应用 UPnP 端口匹配规则。
允许用户禁用 **Internet** 访问	（UPnP）勾选 “启用”，允许用户禁用 Internet 访问。
禁止 **Java**	勾选禁止加载 Java applets。 Java applets 是嵌入 web 网页的小程序，用于实现页面的动态功能。一个恶意 Java applet 会危害您的主机。 单击 “自动”，禁止加载 Java applets ； 单击 “手动”，禁止指定端口加载 Java applets。
禁止 **Cookies**	勾选禁止使用 cookies。 cookies 一般用于储存网站的登录信息，也有网站使用 cookies 储存用户轨迹信息与浏览习惯。勾选此项将过滤由网站创建的 cookies。 注意：许多网站要求必须使用 cookies 才能正确访问。禁止 cookies 可能会导致这些网站访问异常。 单击 “自动”，禁止使用 cookies ； 单击 “手动”，禁止指定端口使用 cookies。

禁止 **ActiveX**	勾选禁止加载 ActiveX。 与 Java applets 相似， ActiveX 在用户使用浏览器时会加载到网页。一个恶意 ActiveX 会危害您的主机。 单击 “自动”，禁止加载 ActiveX ； 单击 “手动”，禁止指定端口加载 ActiveX。
禁止 **HTTP Proxy**	勾选禁止 HTTP Proxy。 HTTP Proxy 允许您的主机通过代理访问其它主机或网络，在这个过程中可能会绕开某些安全规则。例如：安全规则已设置阻止访问某一特定 IP 地址，但是通过代理仍然可以将这一访问请求发出，导致安全规则失效。 单击 “自动”，禁止代理服务器； 单击 “手动”，禁止指定端口使用代理服务器。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

计划管理

您可以创建安全计划，设置应用访问规则的时间日期。

创建安全计划的步骤：

步骤 1 单击 “安全配置” - “计划管理”。

步骤 2 单击 “添加条目”，转到 “添加 / 编辑计划” 页面。

步骤 3 在 “计划名称” 部分，输入安全计划的名称。

在 “访问控制” 页面的 “访问控制列表” 中，当您添加 / 编辑访问控制时，您可以选择该安全计划。详见访问控制。

步骤 4 在 “计划日期” 部分，请在下拉菜单选择以下选项之一：

- “所有日期” 表示该计划将在所有日期内应用；
- “指定日期” 表示该计划将在某些日期内应用。如果您选择 “指定日期”，请勾选您希望的日期 （周一到周日）。

步骤 5 在 “每日的计划时间” 部分，请在下拉菜单选择以下选项之一：

- “所有时间”表示该计划将在一天 24 小时内都应用；
- “指定时间”表示该计划将在您指定的某个时段内应用。如果您选择 “指定时间”，请在 “开始时间”和 “结束时间”部分，选择您希望应用规则的时段。

步骤 6 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

步骤 7 单击 “返回”，返回 “基本配置”页面。

如果您希望修改安全计划的相关设置，请选择相应的安全计划并单击 “编辑”；如果您希望删除相应的安全计划，请选择相应的安全计划并单击 “删除”；单击 “保存”，保存您之前所作的配置。

服务管理

在访问规则中，您需要设置访问规则应用的服务，该服务可以是普通类型的服务，也可以是您自定义的服务。在 “服务管理”页面，您可以查看所有服务，当然您可以创建自定义服务，在您添加 / 编辑访问规则时，您可以选择该服务。

创建自定义服务的步骤：

步骤 1 单击 “安全配置” - “服务管理”。

步骤 2 单击 “添加条目”。

步骤 3 在 “服务名称”部分，输入服务的名称。

步骤 4 在 “协议”部分，您需要从下拉菜单中选择服务所使用的协议：

- TCP
- UDP
- TCP & UDP
- ICMP

步骤 5 在 “起始端口”部分，输入服务所使用的 TCP 或者 UDP 起始端口。

步骤 6 在 “结束端口”部分，输入服务所使用的 TCP 或者 UDP 结束端口。

步骤 7 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

如果您希望修改自定义服务的相关设置，请选择相应的服务并单击 “编辑”；如果您希望删除相应的服务，请选择相应的服务并单击 “删除”；单击 “保存”，保存您之前所作的配置。

访问控制

默认访问策略

您可以配置默认访问策略，控制从 LAN 到 WAN 的访问策略。

配置默认访问策略的步骤：

步骤 1 单击 “安全配置” - “访问控制” - “默认访问策略”。

步骤 2 在 “访问策略”部分，选择 “允许”或 “阻止”。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

访问控制列表

在 “访问控制规则列表”中，显示所有已配置的访问规则，您可以通过 “根据规则动作查看”下拉菜单根据不同的类型显示访问规则。

创建访问规则的步骤：

步骤 1 单击 “安全配置” - “访问控制” - “访问控制列表”。

步骤 2 单击 “添加条目”，转到 “添加 / 编辑访问规则”页面。

步骤 3 在 “访问类型”下拉菜单中，您需要选择以下选项之一：

- 出站 （**LAN - WAN**）：选择此项，创建一个 LAN 到 WAN 的出站规则。
- 入站 （**WAN - LAN**）：选择此项，创建一个 WAN 到 LAN 的进站规则。

步骤 4 在 “动作”下拉菜单中，您需要选择以下选项之一：

- 总是阻止：总是阻止符合该规则的流量。
- 总是允许：总是允许符合该规则的流量。
- 按计划禁止：根据计划方案阻止符合该规则的流量。

- 按计划允许：根据计划方案允许符合该规则的流量。

步骤 5 在“计划”下拉菜单中，您需要选择您在“计划管理”（“安全配置”-“计划管理”）中所配置的计划。

单击“配置计划”按钮，转到“计划管理”页面。该操作会使您丢失之前对于访问规则所作的修改。

步骤 6 在“服务”下拉菜单中，您需要选择您在“服务管理”（“安全配置”-“服务管理”）中所配置的服务。

单击“配置服务”按钮，转到“服务管理”页面。该操作会使您丢失之前对于访问规则所作的修改。

选择“**All Traffic**”，表示选中所有的服务。您也可以选择如下的单个服务：

- Domain Name System (DNS)
- File Transfer Protocol (FTP)
- Hyptertext Transfer Protocol (HTTP)
- HTTP Secondary
- Secure Hypertext Transfer Protocol (HTTPS)
- HTTPS Secondary
- Trivial File Transfer Protocol (TFTP)
- Internet Message Access Protocol (IMAP)
- Network News Transport Protocol (NNTP)
- Post Office Protocol (POP3)
- Simple Network Management Protocol (SNMP)
- Simple Mail Transfer Protocol (SMTP)
- Telnet
- Telnet Secondary
- Telnet SSL
- Voice (SIP)

步骤 7 在“源 **IP**”下拉菜单中，您需要选择以下选项之一：

- 任何：该规则应用于所有 IP 地址。

- 单个地址：该规则应用于指定 IP 地址。请在 “开始地址” 部分输入该地址。
- 地址范围：该规则应用于指定 IP 地址范围。请在 “开始地址” 部分输入开始地址，在 “结束地址” 部分输入结束地址。

步骤 8 在 “目的 **IP**” 下拉菜单中，您需要选择以下选项之一：

- 任何：该规则应用于所有 IP 地址。
- 单个地址：该规则应用于指定 IP 地址。请在 “开始地址” 部分输入该地址。
- 地址范围：该规则应用于指定 IP 地址范围。请在 “开始地址” 部分输入开始地址，在 “结束地址” 部分输入结束地址。

步骤 9 在 “记录日志” 下拉菜单中，您可以选择以下选项之一：

- 从不：该规则的任何信息不会记录到日志。
- 总是：该规则的任何信息总是记录到日志。

步骤 10 在 “QoS 优先级” 部分，为该规则涉及的服务分配 QoS 优先级。

优先级的定义为：1 （最低）、 2、 3、 4 （最高）。

步骤 11 在 “规则状态” 部分，勾选 “启用”，启用该规则。

步骤 12 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

步骤 13 单击 “返回”，返回 “访问控制” 页面。

限制上网列表

CVR100W 支持多种方式的内容过滤。例如：您可以禁止访问含有指定关键词的站点。如果这些关键词出现在站点名称 （例如：站点 URL 或者新闻组名称）中，对于这些站点的访问就会被禁止。

创建限制 Internet 访问规则的步骤：

步骤 1 单击 “安全配置” - “访问控制” - “限制上网列表”。

步骤 2 单击 “添加条目”。转到 “添加 / 编辑限制 **Internet** 访问规则” 页面。

步骤 3 在 “规则状态” 部分，勾选 “启用”，启用该规则。

步骤 4 在 “规则名称” 部分，输入限制 Internet 访问规则的名称。

步骤 5 在 “动作” 下拉菜单中，选择以下选项之一：

- 限制所有：限制所有的 Internet 访问。
- 限制 **URL**：限制访问指定的 URL （链接地址或关键词）。
- 按计划限制所有：根据计划方案限制所有的 Internet 访问。
- 按计划限制 **URL**：根据计划方案限制访问指定的 URL。

步骤 6 如果您选择了 “按计划限制所有” 或者 “按计划阻止 **URL**”，您需要在 “计划” 下拉菜单中选择一个计划方案。

单击 “配置计划” 按钮，转到 “计划管理” 页面。该操作会使您丢失之前对于访问规则所作的修改。

步骤 7 在 “限制主机列表” 部分，单击 “添加条目”。

在 “类型” 下拉菜单中选择如何识别主机 （MAC 地址、 IP 地址、 IP 范围）。

在 “值” 部分，根据您上一步所选择的类型，输入以下类型之一的数值：

- **MAC** 地址：主机 MAC 地址 （XX:XX:XX:XX:XX:XX）。
- **IP** 地址：主机 IP 地址。
- **IP** 范围：IP 地址范围的开始地址与结束地址。

步骤 8 在 “限制站点列表” 部分，单击 “添加条目”。

在 “类型” 下拉菜单中选择如何识别主机 （链接地址、关键词）。

在 “值” 部分，根据您上一步所选择的类型，输入以下类型之一的数值：

- 链接地址：禁止站点的 URL。
- 关键词：禁止站点的关键词。

步骤 9 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

步骤 10 单击 “返回”，返回 “限制上网列表” 页面。

单端口转发

添加单端口转发规则的步骤：

步骤 1 单击 “安全配置” - “单端口转发”，打开 “单端口转发” 页面。

步骤 2 在 “服务名称” 部分，输入需要配置端口转发的服务名称。

步骤 3 在 “外部端口” 部分，输入端口号。当输出流量发出连接请求时该端口触发本端口转发规则。

步骤 4 在 “内部端口” 部分，输入端口号。该端口号用于远程系统响应它所收到的请求。

步骤 5 在 “协议” 下拉菜单中，选择相应的协议：TCP、 UDP 或 TCP&UDP。

步骤 6 在 “**IP** 地址” 部分，输入 IP 地址。

步骤 7 勾选 “启用”，启用该单端口转发规则。

步骤 8 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

多端口转发

添加多端口转发规则的步骤：

步骤 1 单击 “安全配置” - “多端口转发”，打开 “多端口转发” 页面。

步骤 2 在 “服务名称” 部分，输入需要配置端口转发的服务名称。

步骤 3 在 “起始端口” 部分，输入启用端口转发的起始端口号。

步骤 4 在 “结束端口” 部分，输入启用端口转发的结束端口号。

步骤 5 在 “协议” 下拉菜单中，选择相应的协议：TCP、 UDP 或 TCP&UDP。

步骤 6 在 “**IP** 地址” 部分，输入 IP 地址。

步骤 7 勾选 “启用”，启用该单端口转发规则。

步骤 8 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

多端口触发

端口触发是一种动态端口转发。端口触发为指定类型的流量在输出端口上打开输入端口。端口触发相较于静态端口转发更为灵活 （端口触发能够在配置安全规则时应用），因为安全规则不需要参照指定的本地 IP 地址或者 IP 地址范围。端口在不使用时也不会处于开放状态，由此也提供了端口转发不能提供的安全性。

添加多端口触发规则的步骤：

步骤 1 单击 “安全配置” - “多端口触发”，打开 “多端口触发” 页面。

步骤 2 在 “服务名称” 部分，输入需要配置多端口触发的服务名称。

步骤 3 在 “触发端口范围” 部分，输入端口或端口范围，当输出流量请求外部连接时，会使用该规则。如果输出连接仅使用一个端口，那么请在两个部分内输入同一个端口。

步骤 4 在 “转发端口范围” 部分，输入端口或端口范围，这些端口号用于远程系统响应其接收到的请求。如果输入连接仅使用一个端口，那么请在两个部分内输入同一个端口。

步骤 5 勾选 “启用”，启用该多端口触发规则。

步骤 6 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

5

VPN 配置

本章为您介绍如何配置 CVR100W 上与 VPN 相关的信息。包括以下内容：

- VPN 客户端
- 证书管理
- VPN 透传

VPN 客户端

创建与管理 QuickVPN 用户

创建 QuickVPN 用户的步骤：

步骤 1 单击 “**VPN** 配置” - “**VPN** 客户端”。

步骤 2 在 “**VPN** 客户端列表” 中，单击 “添加条目”。

步骤 3 请输入以下信息：

启用	勾选 “启用”，启用该用户。
用户名	输入该用户的用户名。（4 到 32 个字符）。
密码	输入该用户的密码 （4 到 32 个字符）。
允许用户修改密码	勾选 “启用”，允许该用户修改密码。

步骤 4 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

如果您希望修改 QuickVPN 用户相关设置，请选择相应 QuickVPN 用户并单击 “编辑”；如果您希望删除相应 QuickVPN 用户，选择相应 QuickVPN 用户并单击 “删除”；单击 “保存”，保存您之前所作的配置。

如果您希望了解更多关于 QuickVPN 的信息，详见使用思科 QuickVPN。

导入 VPN 客户端设置信息

您可以使用 Microsoft Excel 创建包含 VPN 客户端信息 （客户端的用户名和密码）的 CSV 文件，该文件必须包含一行用作标题以及至少一行用作 VPN 客户端信息。

例如，以下 CSV 文件包含两个 VPN 客户端用户的设置信息：

PROTOCOL	USERNAME	PASSWORD
QuickVPN	user1	password1
QuickVPN	user2	password2

注意 导入 VPN 客户端设置信息会删除当前设置信息。

导入 VPN 客户端设置信息的步骤：

步骤 1 单击 “**VPN** 配置” - “**VPN** 客户端”。

步骤 2 在 “导入 **VPN** 客户端设置” 部分，单击 “浏览”，找到需要导入的文件。

步骤 3 单击 “导入”，导入该文件。

步骤 4 当弹出提示 “该操作会覆盖已存在的 VPN 客户端设置信息。您是否确认继续？” 时，单击 “确定”。

步骤 5 您的设置已生效并保存到 CVR100W。

证书管理

CVR100W 使用数字证书实现 IPsec VPN 的认证与 SSL 验证 （HTTPS 情况下）。

生成新证书

您可以为 CVR100W 生成新证书取代已存在的证书。

生成新证书的步骤：

步骤 1 单击 “**VPN** 配置” - “证书管理”。

步骤 2 选择 “生成新证书”。

步骤 3 单击 “生成证书”。

导入证书

导入证书的步骤：

步骤 1 单击 “**VPN** 配置” - “证书管理”。

步骤 2 选择 “从文件导入证书”，单击 “浏览”找到证书文件。

步骤 3 单击 “安装证书”。

导出管理证书

管理证书包含私钥，所以管理证书必须存放在一个安全的位置作为备份。如果 CVR100W 配置被重置为出厂设置，您可以导入备份的管理证书进行恢复。

导出管理证书的步骤：

步骤 1 单击 “**VPN** 配置” - “证书管理”。

步骤 2 单击 “导出管理证书”。

步骤 3 浏览器中弹出下载提示框，将管理证书保存到本地。

导出客户证书

拥有客户证书的用户才能够使用 QuickVPN 远程连接 CVR100W。 QuickVPN 用户必须将客户证书放置于 QuickVPN 客户端的安装目录。

导出客户证书的步骤：

步骤 1 单击 “**VPN** 配置” - “证书管理”。

步骤 2 单击 “导出客户证书”。

步骤 3 浏览器中弹出下载提示框，将客户证书保存到本地。

VPN 透传

配置 VPN 透传的步骤：

步骤 1 单击 “**VPN** 配置” - “**VPN** 透传”。

步骤 2 选择允许 CVR100W 透传的 VPN 流量类型：

IPsec 透传	勾选 “启用”，允许 IPsec 隧道流量通过 CVR100W。
PPTP 透传	勾选 “启用”，允许 PPTP 隧道流量通过 CVR100W。
L2TP 透传	勾选 “启用”，允许 L2TP 隧道流量通过 CVR100W。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

6

QoS 配置

本章为您介绍如何配置 CVR100W 的 QoS （Quality of Service，服务质量）设置。包括以下内容：

- 带宽管理
- QoS 端口配置
- CoS 配置
- DSCP 配置

带宽管理

您可以使用 CVR100W 的带宽管理功能，管理从 LAN 到 WAN 的带宽。

配置带宽

配置带宽大小的步骤：

步骤 1 单击 “**QoS** 配置” - “带宽管理”。

步骤 2 在 “带宽管理” 部分，勾选 “启用”，启用带宽管理。

步骤 3 在 “带宽设置” 列表中，分别各个接口的上行和下行带宽：

上行	从 LAN 到 WAN 的带宽速率 （kb/s）。
下行	从 WAN 到 LAN 的带宽速率 （kb/s）。

步骤 4 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

配置带宽优先级

在 “带宽优先级设置” 区域，您可以为不同服务分配不同的优先级，从而更好地管理带宽。

配置带宽优先级的步骤：

步骤 1 单击 “**QoS** 配置” - “带宽管理”。

步骤 2 在 “带宽管理” 部分，勾选 “启用”，启用带宽管理。

步骤 3 在 “带宽优先级设置” 列表中，单击 “添加条目”。

步骤 4 输入以下信息：

启用	勾选 “启用”，启用指定服务的带宽优先级管理。
服务名称	从下拉菜单中选择希望进行带宽优先级管理的服务。
方向	从下拉菜单中选择希望进行带宽优先级管理的数据传输方向 （上行或下行）。
优先级	选择相应的优先级 （低、正常、中等、高）。

步骤 5 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

如果您希望修改服务带宽优先级的相关设置，请选择相应的服务并单击 “编辑”；如果您希望删除服务带宽优先级设置，请选择相应的服务并单击 “删除”；单击 “保存”，保存您之前所作的配置。

如果您希望添加一个新服务，单击 “配置服务” 按钮，转到 “安全配置” - “服务管理” 页面，您可以在该页面上新的服务。详见服务管理。

QoS 端口配置

您可以为 CVR100W 上的 LAN 端口进行 QoS 配置，每个 LAN 端口支持 4 个优先级队列，这 4 个优先级队列会根据流量的不同优先级采取不同的措施。

为 CVR100W 上 LAN 端口配置 QoS 的步骤：

步骤 1 单击 “**QoS** 配置” - “**QoS** 端口配置”。

步骤 2 在 “**QoS** 端口配置列表”中，输入以下信息：

LAN 端口	显示 LAN 端口号。
信任模式	从下拉菜单中选择以下选项之一： ▪ 端口：选择此选项启用基于端口的信用模式。您可以为指定的端口设置优先级。流量队列优先级从优先级最低的 1 开始，到优先级最高的 4 结束。 ▪ **DSCP**：（Differentiated Services Code Point，差分服务代码点）选择此选项启用基于 DSCP 的信用模式。通过局域网的网络流量优先级会参照 DSCP 队列，该队列与 “DSCP 设置”页面（“QoS 配置” - “DSCP 配置”）的设置相匹配。 ▪ **CoS**：（Class of Service，服务等级）选择此选项启用基于 CoS 的信任模式。通过局域网的网络流量优先级会参照 CoS 队列。该队列与 “CoS 设置”页面 （“QoS 配置” - “CoS 配置”）的设置相匹配。
缺省流量转发队列 **(** 端口信任模式 **)**	如果您启用基于端口的信任模式，需要为每个端口的出站流量选择一个优先级 （1 至 4）。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

如果您希望恢复 QoS 端口默认配置，请单击 “恢复默认配置”，并单击 “保存”。

CoS 配置

您可以将 CoS 优先级设置映射到 CVR100W 上的流量转发队列。点击页面上的链接转到 “**QoS** 端口配置” 页面，启用基于 CoS 的信任模式。

将 CoS 优先级设置映射到流量转发队列的步骤：

步骤 1 单击 “**QoS** 配置” - “**CoS** 配置”。

步骤 2 您需要为 “**CoS** 配置列表” 中的每一个 CoS 优先级选择一个流量转发队列，该值通过 “流量转发队列” 下拉菜单选取，它标志着各流量类型的流量优先级。即：流量优先级是取决于流量类型的。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

如果您希望恢复 CoS 默认配置，请单击 “恢复默认配置”，并单击 “保存”。

DSCP 配置

您可以将 DSCP 映射到 QoS 队列。点击页面上的链接转到 “**QoS** 端口配置” 页面，启用基于 DSCP 的信任模式。

配置 DSCP 到 QoS 队列的映射的步骤：

步骤 1 单击 “**QoS** 配置” - “**DSCP** 配置”。

步骤 2 您可以点选 “仅查看 **RFC** 值” 或 “查看所有 **DSCP** 值”，以不同的方式显示 “**DSCP** 配置列表”。

步骤 3 您需要为 “**DSCP** 配置列表” 中的每一个 DSCP 值选择一个流量转发队列，该值通过 “队列” 下拉菜单选取。 DSCP 将映射到选定的队列。

步骤 4 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

如果您希望恢复 DSCP 默认配置，请单击 “恢复默认配置”，并单击 “保存”。

7

系统管理

本章为您介绍 CVR100W 的系统管理功能。包括以下内容：

- 用户管理
- 远程管理
- 睡眠模式
- 时间设置
- Bonjour
- 故障诊断
- 日志管理
- 配置管理
- 固件升级
- 设备重启
- 恢复出厂设置
- 快速安装向导

用户管理

“用户管理”页面允许您修改系统管理员的用户名和密码。

配置用户管理的步骤：

步骤 1 单击 “系统管理” - “用户管理”。

步骤 2 如需修改系统管理员账号的设置，输入以下信息：

新用户名	输入新用户名。
旧密码	输入当前密码。
新密码	输入新密码。 我们建议您在设置新密码时，混合使用字母 （包括大小写）、数字与符号，并且不包含标准单词。密码长度最大支持 30 个字符。

步骤 3 勾选 “隐藏密码”，密码将以密文形式显示。

步骤 4 勾选 “空密码”，将使用空密码作为新密码 （不建议您选择此项）。

步骤 5 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

远程管理

“远程管理”页面允许您设置远程管理的相关参数。您可以从本地或 WAN 侧访问设备管理界面对 CVR100W 进行配置，包括查看系统参数，修改设备配置，升级固件版本等。

配置远程管理的步骤：

步骤 1 单击 “系统管理” - “远程管理”。

步骤 2 在 “页面访问”部分，选择从本地 LAN 侧访问 CVR100W 设备管理界面的方式：

- **HTTP**：以 HTTP（超文本传输协议）方式从本地 LAN 侧访问 CVR100W 设备管理界面。
- **HTTPS**：以 HTTPS （安全超文本传输协议）方式从本地 LAN 侧访问 CVR100W 设备管理界面。

步骤 3 在 “远程管理”部分，勾选 “启用”，启用远程管理功能，允许从 WAN 侧远程管理 CVR100W。

步骤 4 在 “远程访问”部分，选择从 WAN 侧远程访问 CVR100W 设备管理界面的方式：HTTP 或 HTTPS。

步骤 5 在 “远程升级”部分，勾选 “启用”，启用远程升级功能。

步骤 6 在 “远程管理 **IP** 地址”部分，设定允许远程访问 CVR100W 的 IP 地址：

- 任何 **IP** 地址：允许任何 IP 地址远程访问 CVR100W。
- **IP** 地址范围：输入被允许远程管理 CVR100W 的 IP 地址范围。

步骤 7 在 “远程管理端口”部分，输入远程访问 CVR100W 的端口号。

步骤 8 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

睡眠模式

睡眠模式是 CVR100W 的一项人性化设计。睡眠模式启用时， CVR100W 前面板上的指示灯全部熄灭，有助于您夜晚的入睡 （不受 CVR100W 前面板指示灯影响）。与此同时 CVR100W 后面板睡眠模式指示灯亮起，作为睡眠模式已开启的标志。当睡眠模式关闭时， CVR100W 前面板上的指示灯恢复正常，后面板睡眠模式指示灯熄灭。

启用或关闭睡眠模式的步骤：

步骤 1 单击 “系统管理” - “睡眠模式”。

步骤 2 勾选 “启用”，启用睡眠模式。取消勾选 “启用”，关闭睡眠模式。

步骤 3 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

时间设置

您可以在 “时间设置”页面配置您所在的时区、是否设置夏令时、 NTP 服务器等与日期时间相关的功能。

在您配置完成之后 CVR100W 将从 NTP 服务器取得日期时间信息，或者使用您手动设置的时间信息。

配置 NTP 与时间设置的步骤：

步骤 1 单击 “系统管理” - “时间设置”。

步骤 2 配置以下信息：

当前时间	（只读）显示当前时间信息。
当前时区	请从下拉菜单中选择您的时区，根据格林威治标准时间（GMT）。
夏令时设置	如果您所在地区使用夏令时，请勾选启用此选项。
设置系统时间	选择如何设置日期时间：“自动”或“手动”。
NTP 服务器	如果您希望使用默认的 NTP 服务器，请选择“使用默认配置”。 如果您希望使用指定的 NTP 服务器，请选择“自定义 **NTP** 服务器”并且在输入区域内输入 NTP 服务器域名或者 IP 地址。
手动设置时间	手动设置当前日期时间信息。

步骤 3 单击“保存”，保存您的设置。单击“取消”，不保存任何修改。

Bonjour

Bonjour 是一种服务通告与发现协议。

启用 Bonjour 的步骤：

步骤 1 单击“系统管理”-“**Bonjour**”。

步骤 2 勾选“启用”，启用 Bonjour。

步骤 3 在“**Bonjour** 接口控制列表”中，您可以勾选相应 VLAN 的“启用 **Bonjour**”选项，启用指定 VLAN 的 Bonjour 功能，从而使得该 VLAN 上的设备能够发现 CVR100W 所提供的 Bonjour 服务（诸如 HTTP/HTTPS）。

例如，如果您未启用 VLAN 2 上的 Bonjour 功能， VLAN 2 内的设备与主机不能发现 CVR100W 上运行的 Bonjour 服务。

步骤 4 单击“保存”，保存您的设置。单击“取消”，不保存任何修改。

故障诊断

CVR100W 为您提供多个诊断工具，帮助您解决网络问题。本节包括以下内容：

网络工具

Ping

您可以使用 Ping 测试 CVR100W 与网络上其它设备的连通性；您也可以使用 Ping 测试 CVR100W 与 Internet 的连通性，此时您需要 Ping 一个完整有效的域名或 IP 地址（例如， www.cisco.com）。

使用 Ping 的步骤：

步骤 1 单击 “系统管理” - “故障诊断” - “网络工具”。

步骤 2 在 “**IP** 地址 / 域名” 区域，输入 IP 地址或者域名 （例如：www.cisco.com）进行 Ping 操作。

步骤 3 单击 “**Ping**” 按钮。 Ping 的结果会显示在页面上，告知您该地址或域名是否可达。

步骤 4 当您完成操作后，单击 “关闭”。

Traceroute

Traceroute 工具能够显示从 CVR100W 到目标 IP 地址之间的所有路由信息。

使用 Traceroute 的步骤：

步骤 1 单击 “系统管理” - “故障诊断” - “网络工具”。

步骤 2 在 “**IP** 地址 / 域名” 区域，输入 IP 地址或者域名 （例如：www.cisco.com）进行 Traceroute 操作。

步骤 3 单击 “**Traceroute**” 按钮。 Traceroute 的结果会显示在页面上。

步骤 4 当您完成操作后，单击 “关闭”。

DNS Lookup

您可以使用 DNS Lookup 查询 Internet 上的终端 （例如：Web 服务器、 FTP 服务器或者邮件服务器）的 IP 地址。

使用 DNS Lookup 的步骤：

步骤 1 单击 “系统管理” - “故障诊断” - “网络工具”。

步骤 2 在 “域名” 区域，输入域名 （例如：www.cisco.com）进行 DNS Lookup 操作。

步骤 3 单击 “查找”， DNS Lookup 的结果会显示在页面上。如果域名存在，您将会得到一个 IP 地址。如果您未得到有效的 IP 地址，则说明您输入的域名不存在。

步骤 4 当您完成操作后，单击 “关闭”。

端口镜像

端口镜像将指定端口上进出的所有数据包复制到镜像端口，以此侦测该端口的相关数据包或者端口行为。您也可以将端口镜像用作诊断工具或者调试工具，用于防范攻击或者观察用户从 LAN 到 WAN 的流量信息。

配置端口镜像的步骤：

步骤 1 单击 “系统管理” - “故障诊断” - “端口镜像”。

步骤 2 在 “源端口” 部分，选择被镜像的端口 （可多选）。

步骤 3 在 “镜像端口” 部分，选择镜像端口 （只可单选）。

步骤 4 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

日志管理

CVR100W 允许您配置以下与日志相关的功能：

日志配置

进行日志配置的步骤：

步骤 1 单击 “系统管理” - “日志管理”。

步骤 2 在 “系统日志” 部分，勾选 “启用”，启用系统日志功能。

步骤 3 在 “本地日志级别” 部分，勾选启用相应级别的日志：

Emergency	致使系统不可用的事件。
Alert	致使需要用户采取行动的事件。
Critical	致使系统处于危机状况的事件。
Error	致使系统处于错误状况的事件。
Warning	致使系统发出警告的事件。
Notification	系统功能正常，但致使系统发出通知的事件。
Information	设备信息。
Debugging	提供事件的相关信息。

步骤 4 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

远程日志服务器

配置远程日志服务器的步骤：

步骤 1 单击 “系统管理” - “日志管理”。

步骤 2 在 “系统日志” 部分，勾选 “启用”，启用系统日志功能。

步骤 3 在 “远程日志服务器列表” 中，单击 “添加条目”。

步骤 4 在 “远程日志服务器” 部分，输入远程日志服务器的 IP 地址。

步骤 5 在 “日志记录级别” 部分，勾选相应的日志级别。

步骤 6 在 “启用” 部分，勾选 “启用”，启用该远程日志服务器。

步骤 7 单击 “保存”，保存您的设置。单击 “取消”，不保存任何修改。

如果您希望修改远程日志服务器的相关设置，请选择相应的远程日志服务器并单击 “编辑”；如果您希望删除远程日志服务器，请选择相应的远程日志服务器并单击 “删除”；单击 “保存”，保存您之前所作的配置。

配置管理

您可以备份 CVR100W 的当前配置信息，为今后需要恢复时使用；您也可以将 CVR100W 恢复到已备份的上一版本的配置状态。

注意 在恢复过程中，请您不要执行以下操作：访问 Internet、关闭 CVR100W、关闭主机。恢复过程需要一些时间。当 CVR100W 电源指示灯长亮时，说明 CVR100W 已重启完毕，正常运作。

备份

备份配置信息的步骤：

步骤 1 单击 “系统管理” - “配置管理”。

步骤 2 单击 “备份”。

步骤 3 浏览器中弹出下载提示框，将配置文件保存至本地。

恢复

您可以通过之前备份的配置文件将 CVR100W 恢复到较早版本，步骤如下：

步骤 1 单击 “系统管理” - “配置管理”。

步骤 2 单击 “浏览”，找到相应配置文件。

步骤 3 选择该文件，单击 “打开”。

步骤 4 单击 “恢复”。

CVR100W 导入配置文件并使用其设置更新当前的系统配置。更新完毕后，CVR100W 重新启动并使用新的配置信息。

固件升级

您可以在 “固件升级”页面升级 CVR100W 的固件版本。

注意 在固件版本升级的过程中，请您不要执行以下操作：访问 Internet、关闭 CVR100W、关闭主机或者以任何其它方式打断升级过程。升级过程需要一些时间，包括重启。

固件升级的步骤：

步骤 1 单击 “系统管理” - “固件升级”。

步骤 2 在 “设备型号”部分，显示 CVR100W 的设备型号。

步骤 3 在 “**PID VID**”部分，显示 CVR100W 的产品型号与版本号。

步骤 4 在 “当前固件版本”部分，显示 CVR100W 当前固件版本。

步骤 5 在 “下载最新固件”部分，单击 “下载”可从指定的网站上下载最新版本的固件。

步骤 6 在 “请选择升级文件”部分，单击 “浏览”，选择已下载的升级文件。

步骤 7 （可选）如果您希望在固件版本升级之后将 CVR100W 恢复到出厂设置，勾选 “恢复到出厂设置”。

步骤 8 单击 “开始升级”，开始 CVR100W 的固件版本升级，升级完成之后 CVR100W 自动重启。

注意 将 CVR100W 重置为出厂设置会清除您所有的自定义设置。

步骤 9 您可以在 CVR100W 重启之后，查看固件版本信息以确认固件升级是否成功。

设备重启

重启 CVR100W 的步骤：

步骤 1 单击 “系统管理” - “设备重启”。

步骤 2 单击 “设备重启”，重启 CVR100W。

恢复出厂设置

注意 在恢复出厂设置过程中，请不要执行以下操作：访问 Internet、关闭 CVR100W、关闭主机。恢复出厂设置需要一些时间。当 CVR100W 电源指示灯长亮时，说明 CVR100W 已重启完毕，恢复到出厂设置。

恢复出厂设置的步骤：

步骤 1 单击 “系统管理” - “恢复出厂设置”。

步骤 2 单击 “恢复出厂设置”。

快速安装向导

“快速安装向导”允许您快速设置基本的网络参数，快速配置您的 CVR100W。用户首次登录时，快速安装向导将会自动启动。您也可以从设备管理页面手动启动快速安装向导并进行配置。

运行快速安装向导的步骤：

步骤 1 单击 “系统管理” - “快速安装向导”。

步骤 2 遵循屏幕上的说明完成快速安装向导配置，共 4 步。

- 配置路由器密码 （第 1 步，共 4 步）。

在这一步骤中，建议您更改 CVR100W 的默认管理密码，以便更好地保护您的设备安全，防止未经授权的访问。新密码建议使用字母及数字的组合，长度至少 6 位。不建议您勾选 “空密码” 选项。

输入新密码后，单击 “下一步”，继续。

- 配置网络连接 （第 2 步，共 4 步）。

  在这一步骤中，您需要选择您的 Internet 连接类型，如果您不确定选择哪种类型，请联系您的网络服务提供商。

  选择正确的连接类型后，单击 “下一步”，继续。

- 配置无线安全 （第 3 步，共 4 步）。

  在这一步骤中，您需要配置您的无线网络。首先为您的无线网络输入一个名称（SSID），例如 MyNetwork。接下来您需要为无线网络选择安全模式，并根据您选择的安全模式选择相应的加密算法以及安全密钥。我们强烈建议您启用安全程度更高的安全模式和密钥来充分保护您的无线网络。

  配置完成无线安全配置后，单击 “下一步”，继续。

- 确认配置信息 （第 4 步，共 4 步）。

  在这一步骤中，您将看到之前步骤中所填写的配置信息，包括管理密码、网络连接类型和无线网络信息。

  在您确认后，单击 “保存并退出”，完成快速安装向导配置；也可以直接单击 “退出” 放弃之前的配置并退出。

8

设备状态

本章为您介绍如何查看 CVR100W 的实时统计以及状态信息。包括以下内容：

- 控制面板
- 设备概览
- 连接设备
- DHCP 信息
- 端口统计
- 无线统计
- 访客信息
- VPN 信息
- 日志信息

控制面板

“控制面板”页面显示 CVR100W 上重要信息的概览。

查看 “控制面板”页面的步骤：

步骤 1 单击 “设备状态” - “控制面板”。

步骤 2 在 “刷新频率”下拉菜单中，选择刷新频率。该操作会使 “控制面板”页面定时更新信息。

步骤 3 如果您希望查看 CVR100W 的面板交互图，请单击 “显示面板视图”。

在该视图中，以绿色标明正在使用的端口。

- 如果您希望查看端口的连接信息，请将鼠标移至该端口。
- 如果您希望刷新端口的连接信息，请单击 “刷新”。

- 如果您希望关闭端口的信息显示，请单击 “关闭”。

端口的连接信息包括：

摘要	
类型	端口类型。
设备接口	端口所对应的设备物理端口。
连接状态	端口是否连接。
速率状态	端口的速率状态，如 100 Mbps 全双工。
自动跳转	端口是否启用自动跳转功能。
统计	
TX 帧	端口已发送的数据帧。
RX 帧	端口已接收的数据帧。

步骤 4 “控制面板”页面显示以下信息：

设备信息	
系统名称	CVR100W 的名称。
固件版本	CVR100W 当前运行的固件版本。
序列号	CVR100W 的序列号。
系统状态	
CPU	CPU 使用情况。
内存	内存使用情况
当前时间	当前时间信息。
运行时间	系统运行总时长。
睡眠模式	CVR100W 睡眠模式的状态 （启用或禁用）。
系统日志	

显示 CVR100W 是否记录以下类别的系统事件：

- Emergency
- Alert
- Critical
- Error
- Warning

如果您希望查看系统日志，请点击 “详细信息”。详见日志信息。

如果您希望管理系统日志，请点击 “日志管理”。详见日志管理。

LAN

如果您希望查看 LAN 设置的相关信息，请单击 “详细信息”。详见 LAN 接口配置。

MAC 地址	CVR100W 本地 MAC 地址。
IPv4 地址	CVR100W 本地 IPv4 地址。
IPv6 地址	CVR100W 本地 IPv6 地址 （当 CVR100W 启用 IPv6 时显示）。
DHCP 服务器	显示 DHCP 服务器是否启用。

DHCPv6 服务器	显示 DHCPv6 服务器的状态 （当 CVR100W 启用 IPv6 时显示）。
WAN 如果您希望查看 WAN 设置的相关信息，请单击 “详细信息”。详见 WAN 接口配置。	
MAC 地址	WAN 接口的 MAC 地址。
IPv4 地址	WAN 接口的 IPv4 地址。
IPv6 地址	WAN 接口的 IPv6 地址 （当 CVR100W 启用 IPv6 时显示）
状态	Internet 连接状态 （在线或离线）。
无线 显示 4 个无线网络的状态以及无线信号强度。如果您希望查看无线相关信息，请单击 “详细信息”。详见无线统计。	
信号强度	显示 Wi-Fi 信号强度。
cisco-xxxx	显示 4 个无线网络的名称以及是否启用等信息。
VPN	
QuickVPN 用户	QuickVPN 已连接用户与可用连接数量。

设备概览

“设备概览”页面显示 CVR100W 的重要信息概览。

查看 “设备概览”页面的步骤：

步骤 1 单击 “设备状态” - “设备概览”。

步骤 2 在 “刷新频率”下拉菜单中，选择刷新频率。该操作会使 “设备概览”页面定时更新信息。

步骤 3 “设备概览”页面显示以下信息：

基本信息	
固件版本	CVR100W 当前运行的固件版本。
固件 MD5 校验码	用于验证文件完整性。
运行时间	系统运行总时长。
当前时间	当前时间信息。
PID VID	CVR100W 的产品型号与版本号。
IPv4 信息	
LAN IP 地址	CVR100W 的 LAN IP 地址。
WAN IP 地址	CVR100W 的 WAN IP 地址。 如需释放 WAN 接口的 IP 地址，点击 “释放地址”。 如需重新获取一个 WAN 接口的 IP 地址，点击 “更新地址”。
默认网关	CVR100W 所在网段的网关地址。
运行模式	如果启用 NAT， CVR100W 用作网关模式；反之 CVR100W 用作路由模式。
DNS 1	第一 DNS 服务器的 IP 地址。
DNS 2	第二 DNS 服务器的 IP 地址。
DNS 3	第三 DNS 服务器的 IP 地址。
DDNS	显示 DDNS 是否启用。
IPv6 信息 （当 **CVR100W** 启用 **IPv6** 时显示）	
LAN IP 地址	CVR100W 的 LAN IP 地址。
WAN IP 地址	CVR100W 的 WAN IP 地址。
默认网关	CVR100W 所在网段的网关地址。
DNS 1	第一 DNS 服务器的 IP 地址。
无线摘要	
SSID 1	SSID 1 的无线网络名称。
安全模式	SSID 1 的无线安全模式。
SSID 2	SSID 2 的无线网络名称。

安全模式	SSID 2 的无线安全模式。
SSID 3	SSID 3 的无线网络名称。
安全模式	SSID 3 的无线安全模式。
SSID 4	SSID 4 的无线网络名称。
安全模式	SSID 4 的无线安全模式。
防火墙状态	
DoS	是否已启用 DoS 攻击防护功能。
禁止 WAN 侧请求	是否禁止 WAN 侧请求 （例如：Ping 命令）。
允许远程管理	是否允许远程管理 CVR100W。
VPN 状态	
QuickVPN 可用连接数	允许的最大 QuickVPN 连接数量。
QuickVPN 已连接用户数	当前已连接的 QuickVPN 用户数量。

连接设备

“连接设备”页面显示连接到 CVR100W 的设备信息。

查看 “连接设备”页面的步骤：

步骤 1 单击 “设备状态” - “连接设备”。

步骤 2 如果您希望显示指定接口类型的设备信息，请在 “根据接口类型查看”下拉菜单中选择相应选项。

您可以选择以下选项之一：

全部	显示所有连接到 CVR100W 的设备信息。
无线	显示通过无线连接到 CVR100W 的设备信息。
有线	显示通过以太网接口连接到 CVR100W 的设备信息。
WDS	显示通过 WDS 连接到 CVR100W 的设备。

步骤 3 ARP 列表显示以下信息：

设备名称	连接设备的名称。
IP 地址	连接设备的 IP 地址。
MAC 地址	连接设备的 MAC 地址。
类型	连接设备的连接类型。
静态 **DHCP**	显示连接设备上是否启用静态 DHCP 功能。
接口类型	连接设备通过何种方式接入 CVR100W。

DHCP 信息

CVR100W 内置的 DHCP 服务器能够自动配置内网中各主机的 TCP/IP 协议。“DHCP 信息”页面显示 DHCP 客户端信息。

查看 “DHCP 信息”页面的步骤：

步骤 1 单击 “设备状态” - “**DHCP** 信息”。

步骤 2 在 “**DHCP** 信息”页面中，以不同的 VLAN 进行区分，给出每一个 VLAN 的 DHCP 客户端列表。

DHCP 列表中显示以下信息：

设备名称	显示 DHCP 客户端的设备名称。
IP 地址	显示 DHCP 客户端的 IP 地址。
MAC 地址	显示 DHCP 客户端的 MAC 地址。
绑定静态 **DHCP**	勾选启用静态 DHCP （将当前 IP 地址静态绑定到该设备）。

步骤 3 单击页面下方的 “保存”按钮后生效。单击 “取消”，不保存任何修改。

端口统计

“端口统计”页面显示端口统计信息， CVR100W 重启后端口统计信息会被重置。

查看 “端口统计”页面的步骤：

步骤 1 单击 “设备状态” - “端口统计”。

步骤 2 在 “刷新频率”下拉菜单中，选择刷新频率。该操作会使 “端口统计”页面定时更新信息。

步骤 3 （可选）勾选 “显示精简模式”并单击 “保存”后，页面以精简模式显示端口统计信息。

步骤 4 在端口统计列表中，显示 WAN、 LAN 以及 WLAN 端口上的数据传输统计信息：

设备接口	网络接口的名称
数据包	已收发数据包的数量。
字节	已收发数据包的字节数量。
错误	已收发错误数据包的数量。
丢弃	已丢弃数据包的数量。
组播	已发送的组播数据包的数量。
冲突	该端口上信号冲突发生的数量。 当一个端口尝试发送数据的同时存在另一路由器或者主机正连接该端口，会产生冲突。

步骤 5 如果您希望重置端口统计信息，请单击 “清除记录”。

无线统计

“无线统计”页面显示无线统计信息。 CVR100W 重启后无线统计信息会被重置。

查看 “无线统计”页面的步骤：

步骤 1 单击 “设备状态” - “无线统计”。

步骤 2 在 “刷新频率”下拉菜单中，选择刷新频率。该操作会使 “无线统计”页面定时更新信息。

步骤 3 勾选 “显示精简模式”并单击 “保存”后，页面以精简模式显示无线统计信息。

步骤 4 无线统计列表中显示以下信息：

SSID 名称	无线网络的名称
数据包	每个 SSID 已收发无线数据包的数量，以及 4 个 SSID 已收发无线数据包的总数。
字节	每个 SSID 已收发无线数据包的字节数量，以及 4 个 SSID 已收发无线数据包的字节总数。
错误	每个 SSID 已收发无线错误数据包的数量，以及 4 个 SSID 已收发无线错误数据包的总数。
丢弃	每个 SSID 收发信息时已丢弃数据包的数量，以及 4 个 SSID 收发信息时已丢弃数据包的总数。
组播	通过每个 SSID 传输的组播数据包的数量，以及通过 4 个 SSID 传输的组播数据包的总数。
冲突	每个 SSID 收发信息时数据包冲突的数量，以及 4 个 SSID 收发信息时数据包冲突的总数。

步骤 5 如果您希望重置无线统计计数，请单击 “清除记录”。

访客信息

“访客网络”页面显示通过 SSID4 （默认名称为 “cisco-guest”）连接至 CVR100W 的设备信息。

CVR100W 同一时间至多支持 10 个访客设备。当访客设备的连接数量达到设置的最大数量时， CVR100W 会拒绝新增的访客请求并弹出警告。对于每一个访客连接，CVR100W 有连接时长限制，当剩余时间为零时， CVR100W 会断开该连接。您也可以在任何时间强制断开访客设备与 CVR100W 的连接。

默认设置下，访客设备的最大连接数量为 5，连接时长为 2 小时。

查看 “访客信息”页面的步骤：

步骤 1 单击 “设备状态” - “访客信息”。

步骤 2 如果您希望手动断开访客设备与 CVR100W 的连接，请选择相应的设备并单击列表中的 “强制退出”。

步骤 3 “访客网络统计”列表中显示以下信息：

设备名称	显示通过 SSID4 连接到 CVR100W 上的设备名称。
IP 地址	显示该设备的 IP 地址。
MAC 地址	显示该设备的 MAC 地址。
剩余时间	显示该设备能够连接 CVR100W 的剩余时间。
设备状态	显示该设备是否正在通过 CVR100W 连接到 Internet。
强制退出	用于强制断开该访客设备。

VPN 信息

“VPN 信息”页面显示 VPN 用户连接的状态。

查看 “VPN 信息”页面的步骤：

步骤 1 单击 “设备状态” - “**VPN** 信息”。

步骤 2 在 “**VPN** 用户连接状态”列表，可查看连接到 CVR100W 的 VPN 用户信息。

用户名	VPN 用户的用户名。
客户端 **IP** 地址	显示远程 QuickVPN 客户端的 IP 地址，如果该客户端位于 NAT 路由器之后，该 IP 地址可以是 NAT 或者公共 IP。
设备状态	显示 QuickVPN 用户当前的状态。“离线”表示 QuickVPN 隧道没有被 VPN 用户发起或者建立；“在线”表示 QuickVPN 隧道已被 VPN 用户发起或者建立，处于激活状态。
开始时间	VPN 用户建立连接的开始时间。
结束时间	VPN 用户终止连接的结束时间。
持续时间 （秒）	VPN 用户建立与终止连接之间的时间跨度 （时长）。
协议	用户所使用的协议：QuickVPN。
断开连接	如果您希望终止一个处于激活状态的 VPN 连接，请单击 “断开连接”。

日志信息

“日志信息”页面显示了 CVR100W 的系统日志信息。

查看系统日志的步骤：

步骤 1 单击 “设备状态” - “日志信息”。

步骤 2 单击 “刷新日志”，显示最新的日志信息。

步骤 3 如果您希望显示指定级别的日志信息，请在 “根据日志级别查看”中选择相应选项，单击 “应用”按钮之后生效。

您可以选择以下选项之一：

Emergency	致使系统不可用的事件。
Alert	致使需要用户采取行动的事件。
Critical	致使系统处于危机状况的事件。

Error	致使系统处于错误状况的事件。
Warning	致使系统发出警告的事件。
Notification	系统功能正常，但致使系统发出通知的事件。
Informational	设备信息。
Debugging	提供事件的相关信息。

步骤 4 系统日志列表简要显示 CVR100W 所记录的系统日志。

系统日志列表中显示以下信息：

日志索引	该系统日志的记录序号。
日志时间	该系统日志的记录时间。
日志级别	该系统日志的严重级别。
描述	该系统日志的简要描述。

步骤 5 如果您希望删除日志列表中的所有条目，请单击 “清除日志”；

步骤 6 如果您希望将所有的日志信息保存到本地，请单击 “保存日志”；

步骤 7 如果您希望指定每页所显示的日志数量，请在下拉菜单中选择相应数值。

步骤 8 使用页面导航按钮，可以在日志页面中操作、移动。

9

配置 Cisco Smart Connect

本章为您介绍如何配置 Cisco Smart Connect (CSC，思科锐联)。包括以下内容：

- 关于思科锐联
- 启用思科锐联
- 配置 CSC 无线网络
- 接入 CSC 无线网络
- 自定义思科锐联二维码

关于思科锐联

Cisco Smart Connect (CSC，思科锐联) 可使您为拥有手持设备的企业访客、商铺顾客等目标人群提供安全、便捷的无线访问，并能基于此项功能拓展出更多的商业应用模式。

如需了解更多关于思科锐联的相关信息，请访问 CVR100W 产品主页：www.cisco.com/go/cn/cvr100w。

启用思科锐联

在开始使用思科锐联功能之前，您首先需要登录 CVR100W 的设备管理界面启用此功能，然后设置 CVR100W 的 CSC 无线网络，用于建立 CSC 无线连接。

启用思科锐联功能， CVR100W 首先将预设的四个无线接入点均恢复到出厂默认设置，然后启用 SSID2 作为 CSC 无线网络，专门用来接受 CSC 无线连接请求。禁用思科锐联功能， CVR100W 预设的四个无线接入点均恢复到出厂默认设置。

首次启用思科锐联功能时，CSC 无线网络的名称将默认设为 Cisco-Smart-Connect，并采用与 SSID1 相同的无线安全模式和安全密钥。当您再次启用此功能时 （无恢复出厂设置操作）， CVR100W 将自动导入您上次所配置的 CSC 无线网络参数。

请按照以下步骤启用思科锐联功能：

步骤 1 登录 CVR100W 的设备管理界面。默认情况下打开网页浏览器，在地址栏中输入 192.168.1.1 并按下 Enter 键。详见使用快速安装向导。

步骤 2 打开 “高级配置” - “**Smart Connect**”页面。

步骤 3 在 **Smart Connect** 区域，勾选 “启用”，启用思科锐联功能。默认为关闭。

步骤 4 单击 “保存”。

配置 CSC 无线网络

启用思科锐联功能后，您需要配置 CVR100W 的 CSC 无线网络参数，然后无线用户才能使用手持设备上安装的 CSC 用户版应用程序与您的思科锐联卡或对应的二维码图片进行交互，并接入到 CVR100W 的 CSC 无线网络。

您可以通过 2 种方式配置 CSC 无线网络：

- 登录 CVR100W 的设备管理界面设置 CSC 无线网络。详细信息可参考通过设备管理器设置 CSC 无线网络。
- 使用手持设备上安装的CSC网管版应用程序设置CSC无线网络。详细信息可参考使用 CSC 网管版软件设置 CSC 无线网络。

注意 当启用思科锐联功能时， CVR100W 预设的第二个无线接入点 （SSID2）将会作为 CSC 无线网络，专门用来接受 CSC 无线连接请求。此时，您将无法配置 SSID2、SSID3 和 SSID4 三个无线接入点的相关参数。但是您在 “Smart Connect”页面对 CSC 无线网络所作的设置将会应用到 SSID2 上。

通过设备管理器设置 CSC 无线网络

请按照以下步骤登录 CVR100W 的设备管理界面设置 CSC 无线网络：

步骤 1 登录 CVR100W 的设备管理界面，启用思科锐联功能。详细信息可参考启用思科锐联。

步骤 2 设置 CSC 无线网络的以下参数：

SSID 名称	启用思科锐联功能后，CSC 无线网络的名称默认设为 Cisco-Smart-Connect。 如果您拥有一张思科锐联卡，您可以在此处输入思科锐联卡上提供的 SSID 名称。如果您希望自定义 CSC 无线网络名称，请输入一个新的 SSID 名称。 **注意：**设置新的 CSC 无线网络名称，将要求您重新生成与之相对应的思科锐联二维码并打印出来。详细信息请参考自定义思科锐联二维码。
安全模式	显示 CSC 无线网络采用的无线安全模式 （默认为 **WPA2-Personal Mixed**）。 启用思科锐联功能后， CSC 无线网络将采用 SSID1 默认的无线安全模式。您不能修改 CSC 无线网络的安全模式。
安全密钥	启用思科锐联功能时， CSC 无线网络采用 SSID1 默认的安全密钥。 如果您拥有一张思科锐联卡，您可以在此处输入思科锐联卡上提供的默认安全密钥。如果您希望自定义安全密钥，请输入一个新的安全密钥。 **注意：**修改 CSC 无线网络的安全密钥，将要求您重新生成与之相对应的思科锐联二维码并打印出来。详细信息请参考自定义思科锐联二维码。
显示密钥	勾选以明文形式显示安全密钥。
SSID 广播	勾选启用 SSID 广播功能。默认为开启。
访问网络时段	无线用户通过 CSC 用户版应用程序接入 CSC 无线网络后，可访问互联网，但不能访问 CVR100W 的设备管理页面对 CVR100W 进行管理。 您可以限制 CSC 无线用户访问互联网的时间。设置范围为 0 到 1440 分钟。默认值为 0，表示无限制。 **注意：**此设定只适用于 CSC 无线用户。通过其它方式接入到 SSID2 （即 CSC 无线网络）的无线用户不受此功能限制。
允许普通无线用户访问网络	勾选允许通过其它方式接入到 CSC 无线网络的普通无线用户访问互联网。取消勾选禁止其访问互联网。默认为开启。

步骤 3 单击 “保存”。

使用 CSC 网管版软件设置 CSC 无线网络

您可以安装 CSC 网管版应用程序到一台手持设备 （如安卓智能手机 / 平板电脑），并通过无线方式配置 CSC 无线网络。

注 通过 CSC 网管版应用程序仅允许您设定 CSC 无线网络的 SSID 名称和安全密钥。

步骤 1 访问 CVR100W 产品主页，打开 “思科锐联”标签页。

步骤 2 下载 CSC 网管版应用程序并安装到您的手持设备。

注 目前 CSC 网管版应用程序仅支持安卓系统的智能手机。您可以查看产品主页上的产品发布声明了解最新的智能手机操作系统的支持情况。

步骤 3 启用您手持设备上的无线功能，找到 CVR100W 默认的无线接入点 (SSID1)，连接到 CVR100W。您需要输入 SSID1 对应的安全密钥。

步骤 4 运行 CSC 网管版应用程序，输入以下信息：

- 无线路由器用户名：输入 CVR100W 的管理员用户名。
- 无线路由器密码：输入 CVR100W 的管理员密码。
- 无线网络 **SSID**：输入 CSC 无线网络的名称。通常，输入您的思科锐联卡上提供的 SSID 名称。
- 无线网络密钥：输入 CSC 无线网络的安全密钥。通常，输入您的思科锐联卡上提供的安全密钥。

步骤 5 点击 “设置”。您输入的 SSID 名称和安全密钥将被应用到 CVR100W 的 CSC 无线网络。

此时，您的每位企业访客、商铺顾客可使用手持设备 (如手机、平板电脑) 中的 CSC 用户版应用程序与您的思科锐联卡进行信息交互后，快速连接至 CVR100W 相应的 CSC 无线网络。

接入 CSC 无线网络

启用思科锐联功能并设置好 CSC 无线网络后，无线用户通过安装有 CSC 用户版应用程序的手持设备与您的思科锐联卡进行信息交互后，可快速连接到 CSC 无线网络。

步骤 1 访问 CVR100W 产品主页，打开 “思科锐联”标签页。

步骤 2 下载 CSC 用户版应用程序并安装到一台手持设备上。

步骤 3 将手持设备与思科互联卡进行信息交互 （此步骤可通过 NFC 扫描或二维码拍摄），CSC 用户版应用程序在成功获取 CSC 无线网络的相关信息后，通过无线接入到 CVR100W 的 CSC 无线网络。

如果 CSC 无线网络限制 CSC 无线用户访问互联网的时间，当无线用户在线时间超过上限时，其无线连接将被断开。

自定义思科锐联二维码

思科锐联卡预置了唯一的 SSID 名称和安全密钥，并打印了这些信息所对应的二维码，用来配置 CSC 无线网络和方便无线用户进行信息交互。

如果您需要定制 CSC 无线网络名称和安全密钥，或根据 CSC 无线网络名称和安全密钥生成相应的二维码并打印成图片，可访问 CVR100W 产品主页进行定制。

注意 CSC 无线网络名称或安全密钥被更改后，您需要生成新的二维码图片并打印出来，并且原先的思科锐联卡将失效。无线用户需重新扫描新生成的二维码才能接入 CVR100W 的 CSC 无线网络。

步骤 1 访问 CVR100W 产品主页，打开 “思科锐联”标签页。

步骤 2 在 “定制二维码”区域，分别输入以下信息：

- 连接类型：显示 CSC 无线网络的无线安全模式。
- **SSID**：如需自定义 CSC 无线网络名称，在此处输入新的 SSID 名称。
- 密码：如需自定义 CSC 无线网络的安全密钥，在此处输入新的安全密钥。

步骤 3 点击 “生成”，生成与新的 CSC 无线网络名称和安全密钥相对应的二维码。

步骤 4 点击 “打印”，将生成的二维码图片打印出来。

步骤 5 此时，您需要按照 “配置 CSC 无线网络”一节中介绍的方法，使用您自定义的 CSC 无线网络名称和安全密码重新配置 CVR100W 的 CSC 无线网络。

步骤 6 无线用户与打印好的二维码图片进行信息交互后，接入到 CVR100W 的 CSC 无线网络。

A

使用思科 QuickVPN

本附录介绍如何安装和使用思科 QuickVPN 软件。您可以从思科网站上下载 QuickVPN 软件。 QuickVPN 软件支持的操作系统有：Windows 7、 Windows XP、Windows Vista 以及 Windows 2000 （其它操作系统需使用第三方 VPN 软件）。

本附录包括以下内容：

- 准备工作
- 安装思科 **QuickVPN** 软件
- 使用思科 **QuickVPN** 软件

准备工作

QuickVPN 软件只能与经过正确配置后可接受 QuickVPN 连接的 CVR100W 建立有效的 VPN 连接。

如需使用 QuickVPN 建立 VPN 连接，首先在 CVR100W 上完成以下配置：

步骤 **1** 启用远程管理。详见远程管理。

步骤 **2** 创建 QuickVPN 用户账号。在用户账号创建以后，认证证书才能够被 QuickVPN 客户端使用。详见 **VPN** 客户端。

安装思科 QuickVPN 软件

请按照以下步骤从 Internet 下载和安装 QuickVPN 软件：

步骤 1 在附录 B “相关资料”中，找到 “客户支持中心”的链接。

www.cisco.com/support

步骤 2 打开 “**Download**”标签页，在搜索框中输入 “**QuickVPN**”，找到 QuickVPN 软件。

步骤 3 下载 QuickVPN 安装文件并解压缩。

步骤 4 双击安装文件 （.exe 文件），依据屏幕上的提示进行操作，直至完成 QuickVPN 软件的安装。

使用思科 QuickVPN 软件

步骤 1 双击桌面或者系统托盘上的思科 QuickVPN 图标。

QuickVPN 桌面图标：

QuickVPN 系统托盘图标：

弹出 QuickVPN 登录窗口。

步骤 **2** 在“**Profile Name**（配置文件名称）”部分，输入配置文件名称。

步骤 **3** 在“**User Name**（用户名）”与“**Password**（密码）”部分，输入用户名与密码。

用户名与密码信息详见 **VPN** 客户端。

步骤 **4** 在“**Server Address**（服务器地址）”部分，输入 CVR100W 的 IP 地址。

步骤 **5** 在“**Port for QuickVPN**（QuickVPN 端口）”部分，输入 QuickVPN 用户连接远程 VPN 路由器的端口号，或者保持默认设置：“**Auto**（自动）”。

步骤 **6** 如果你希望保存该配置文件，请单击“**Save**（保存）”；

如果您希望删除该配置文件，请单击“**Delete**（删除）”；

获取更多信息请单击“**Help**（帮助）”。

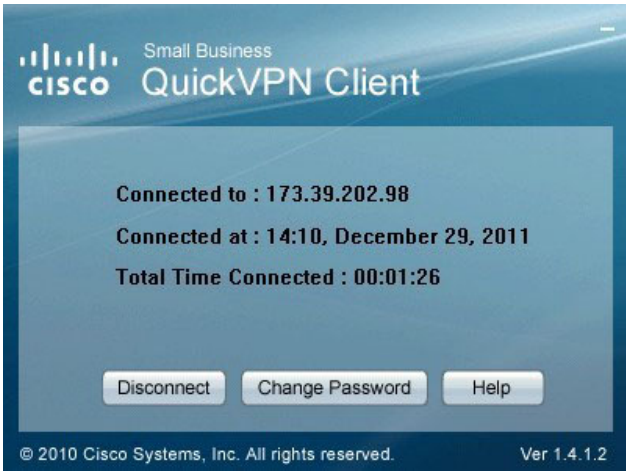
注 如果您需要与多个站点间建立隧道，您必须为每一条隧道创建相应的配置文件。但同一时间内只能有一条隧道处于激活状态。

步骤 **7** 单击“**Connect**（连接）”，启动您的 QuickVPN 连接。

连接的过程依次为：Connecting（连接中）、Provisioning（准备设置）、Activating Policy（激活策略）、Verifying Network（验证网络）。

步骤 **8** 在您的 QuickVPN 连接建立完成之后， QuickVPN 的托盘图标变为绿色，并且出现 QuickVPN 的状态窗口。

该窗口显示 VPN 隧道远程终端的 IP 地址、 VPN 隧道的启动时间、运行时长。



单击 “**Disconnect** （断开连接）” 终止 VPN 隧道连接；

单击 “**Help** （帮助）”，获取更多信息。

步骤 **9** 如果您希望修改密码，点击 “**Change Password** （修改密码）”。

注 只有 “允许用户修改密码” 功能被启用的 VPN 用户才被允许修改密码。详情参见 **VPN** 客户端。

步骤 **10** 在 “**Old Password** （旧密码）” 部分，输入您当前的密码。

步骤 **11** 在 “**New Password** （新密码）” 部分，输入您的新密码；

在“**Confirm New Password** （确认新密码）”部分，再次输入新密码。

步骤 **12** 单击“**OK** （确定）”保存您的新密码。

B

相关资料

思科为您提供丰富完整的资料文档，以帮助您获取更多关于思科 CVR100W Wireless-N 300M 无线路由器的信息。

资源	地址
CVR100W 产品主页	www.cisco.com/go/cn/cvr100w
客户支持中心	www.cisco.com/support
产品渠道合作伙伴中心 (需合作伙伴登录)	www.cisco.com/web/CN/partners
开放源许可通知	www.cisco.com/go/cn/cvr100w
产品兼容性和安全信息	www.cisco.com/go/cn/cvr100w
软件下载	www.cisco.com/web/CN/solutions/industry/segment_sol/small/index.html#small_down
产品保修信息	www.cisco.com/web/CN/solutions/industry/segment_sol/small/index.html#~service
产品服务热线	8008888168 （固定电话） 4006282616 （移动电话）