ZoneDirector1000/3000　AC 设备使用指南

服务指南

文档版本　01

发布日期　2009-08-14

RuckusWireless Inc.为客户提供全方位的技术支持，用户可与就近的优科办事处联系，也可直接与公司总部联系。

RuckusWireless Inc.

网址： http://www.ruckuswireless.com

客户服务邮箱： Support@ruckuswireless.com

商标声明

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

插图目录

表格目录

1 优科 ZD1000/3000 简介

1.1 ZD1000/3000 概述

优科 ZD1000/3000 作为优科接入点（简称 AP）集中控制系统，提供了简化配置和更新、WLAN 安全控制、射频管理，及通过以太网连接 AP 之间相互协调。

ZD1000/3000 将网络、射频(RF)和位置管理集成到一个系统中。用户身份验证可以通过集成的强制网络门户和内部数据库实现，或者转发到外部 AAA 服务器，如 RADIUS 或 Active Directory。一旦用户通过身份验证，用户数据就无需通过 ZD1000/3000，因而消除了再使用高速 Wi-Fi 技术（如 802.11n）时可能出现的带宽瓶颈。

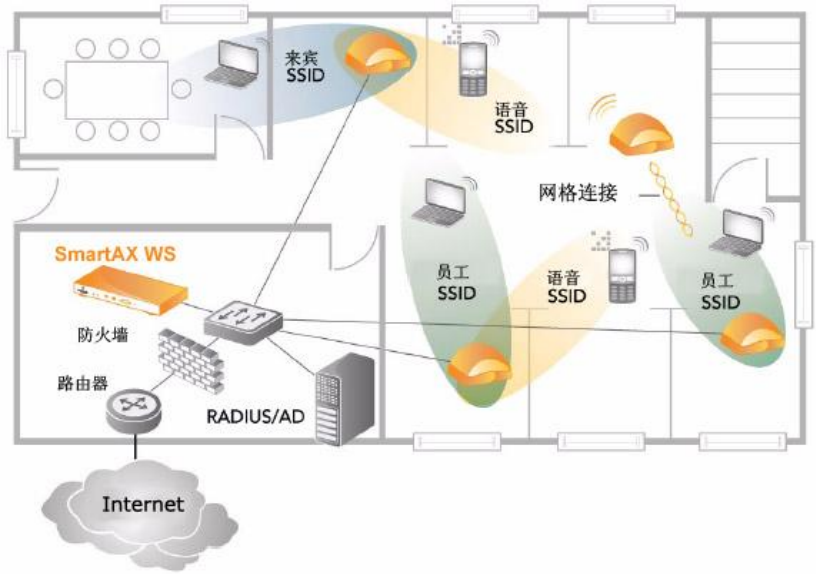
此外，ZD1000/3000 还支持可疑 AP 检测，能够将网络中的一些用户设备列入黑名单，所有这些功能都可在系统范围内轻松地配置和启用。当多个 AP 比较接近时，ZD1000/3000 会自动调整 AP 的发射功率和通道设置，从而整体上尽可能地提供最佳覆盖范围和适应性。

表 1-1列出了在网络中使用 ZD1000/3000 的优点。

表 1-1 ZD1000/3000 优点摘要

灵活的部署选项	ZD1000/3000与现有的网络和安全系统无缝集成，提供网络范围的动态射频管理以解决AP的部署问题。
IT精简部署在5分钟内即可完成，易于使用和管理	通过基于Web的配置向导，任何计算机用户都可在几分钟内配置好整个WLAN。优科AP可自动发现网络上的ZD1000/3000。
易于监控和处理故障	可自定义的仪表板提供了全面网络的信息概览，方便管理员详细查看以确定可能的无线问题。
用户自动安全性	每个用户无需使用相同的加密密钥配置和更新 PC 客户端设备。
完整的集成	将网络管理、动态射频管理、位置管理和接入点控制集成到一个低成本解决方案中。
高级 WLAN 特性和功能	基于角色的用户策略、WLAN 分组、内部身份验证数据库、可疑 AP 检测和每个AP可接入的用户数阈值。
智能网格简化了成本高昂且复杂的部署过程	集成的智能网格技术可自动完成部署过程，这样就不必将以太网电缆铺设到每个智能 WiFi 接入点。

图 1-1 ZD1000/3000 可以部署到 2 层或 3 层网络内的任何位置。所有支持的优科接入点都会自动发现 ZD1000/3000 并由其自动配置。



1.2 ZD1000/3000 的物理特性

本部分介绍了 ZD1000/3000 的物理特性。

图 1-2 ZD1000 前面板

图 1-3 ZD3000 前面板

1.2.1 按钮、端口和连接器

表 1-2介绍了 ZD1000 和 ZD3000 上的按钮、端口和连接器。

表 1-2 ZD1000 和 ZD3000 上的按钮、端口和连接器

标签	ZD1000	ZD3000
Power（电源）	（位于前面板上）按此按钮可打开 ZD1000 的电源。	（位于后面板上）按此按钮可打开 ZD3000 的电源。
Console（控制台）	用于访问 ZD1000 命令行界面的 DB-9 端口。	用于访问 ZD3000 命令行界面的 RJ-45 端口。
10/100/1000 Ethernet（10/100/1000 以太网）	两个自动协商 10/100/1000Mbps 以太网端口。欲了解两个以太网指示灯的含义，可参考表 1-3。	
Reset（重置）	使用此按钮可重新启动 ZD1000，或将其恢复到出厂默认设置。 要重新启动 ZD1000，可按一下 Reset（重置）按钮。 要将 ZD1000 恢复到出厂默认设置，需按住 Reset（重置）按钮至少 5 秒钟。欲了解详情，可参考2-16页中的“其他还原出厂默认设置方法 警告：将 ZD1000 恢复到出厂默认设置会删除所有已更改的配置。	要重新启动 ZD3000，可按一下 Reset（重置）按钮。
F/D（仅限 ZD3000）	不存在	要将 ZD3000 恢复到出厂默认设置，需按住 F/D 按钮至少 5 秒钟。欲了解详情，可参考2-16页中的“其他还原出厂默认设置方法”。 警告：将 ZD3000 恢复到出厂默认设置会删

标签	ZD1000	ZD3000
		除所有已更改的配置。
USB	不存在	仅供优科技术支持工程师使用

1.2.2 前面板指示灯

表 1-3介绍了 ZD1000/3000 前面板上的指示灯。

表 1-3 前面板指示灯

指示灯标签	状态	含义
Power（电源） 注意： ZD1000 的电源指示灯内嵌在前面板的 Power（电源）按钮中。	呈绿色	ZD1000/3000 已通电。
	熄灭	ZD1000/3000 未通电。如果电源线或电源适配器已连接到电源，需检查电源插头是否已正确插入 ZD1000/3000 后面板上的电源插孔中。
Status（状态）	呈绿色长亮	状态正常
	呈绿色闪烁	尚未配置 ZD1000/3000。可登录到 Web 界面，使用安装向导配置 ZD1000/3000。
	呈琥珀色	ZD1000/3000 已关闭（但仍与电源连接）。
	呈琥珀色闪烁	ZD1000/3000 正在启动或关闭。
Ethernet Link	呈绿色	端口已连接到设备。

指示灯标签	状态	含义
（以太网链路）	呈绿色闪烁	端口正在传输或接收用户数据。
	熄灭	端口未连接网络电缆，或者未收到链路信号。
Ethernet Rate（以太网速率）	呈琥珀色	端口已连接到 1000Mbps 设备。
	呈绿色	端口已连接到 100Mbps 设备。
	熄灭	端口已连接到 10Mbps 设备。

根据接入点指示灯判断网格的状态

如果启用了网格，还可以根据接入点的指示灯来判断网格的状态。优科接入点上有两个指示网格状态的指示灯，分别是：

- WLAN/无线设备关联指示灯 – 指示下行链路状态和客户端关联状态
- 信号/空气质量指示灯 – 指示上行链路状态和接入点的无线信号质量

WLAN/无线设备关联指示灯

WLAN 指示灯在根 AP 和网格 AP 上的工作方式相同。可参考下表，查看根 AP 和网格 AP 的指示灯可能出现的颜色和工作方式，以及这些颜色和工作方式所指示的网格状态。

指示灯颜色/工作方式	根 AP/网格 AP
呈绿色长亮	无网格下行链路，且 至少存在一个与此 AP 关联的客户端

指示灯颜色/工作方式	根 AP/网格 AP
呈琥珀色	无网格下行链路，且 不存在与此 AP 关联的客户端
呈绿色快速闪烁	至少存在一个网格下行链路，且 至少存在一个与此 AP 关联的客户端
呈绿色缓慢闪烁	至少存在一个网格下行链路，且 不存在与此 AP 关联的客户端

信号/空气质量指示灯

指示灯颜色/工作方式	根 AP	网格 AP
呈绿色长亮	无	• 已连接到根AP或其他网格AP • 信号质量良好
呈绿色快速闪烁	无	• 已连接到根AP或其他网格AP • 信号质量一般
呈绿色缓慢闪烁	无	AP 正在搜索上行链路
熄灭	此 AP 为根 AP	无

1.3 确保接入点可以与 ZD1000/3000 通信

接入点必须首先发现网络上的 ZD1000/3000，ZD1000/3000 才可能开始管理接入点。这要求接入点，即使位于不同的子网，也能访问到 ZD1000/3000 的 IP 地址。本部分介绍了为确保接入点可以发现 ZD1000/3000 并向其注册而应执行的步骤。

注意

本指南假定已将网络上的 AP 配置成可从 DHCP 服务器获取 IP 地址。如果为 AP 分配了静态 IP 地址，则这些 AP 必须使用本地 DNS 服务器，用户可以将该 DNS 服务器配置成使用 ZD1000/3000.{DNS domain name}或 ZoneDirector（如果该 DNS 服务器上未定义任何域名）来解析 ZD1000/3000 IP 地址。

注意

ZD1000/3000 和优科接入点可以通过 2 层或 3 层连接相互通信。如果希望使用 2 层连接，则 ZD1000/3000 和接入点必须位于同一广播域(VLAN)和同一 IP 子网上。

1.3.1 如何确保接入点能够发现网络上的 ZD1000/3000

如果 AP 和 ZD1000/3000 部署在不同的子网上，要确保这两个设备之间成功通信，有以下三种选择：

- 选择 1：在一个子网上执行自动发现，然后将 AP 转移到目标子网
- 选择 2：自定义 DHCP 服务器
- 选择 3：向 DNS 服务器注册 ZD1000/3000

如果 AP 和 ZD1000/3000 部署在同一个子网上

如果 AP 和 ZD1000/3000 部署在同一个子网上，则无需执行其他配置，仅需将 AP 连接到 ZD1000/3000 所在的网络即可。AP 启动时，会发现 ZD1000/3000 并向其注册。如果禁用了自动审批功能，则需手动审批注册请求。

选择 1：在一个子网上执行自动发现，然后将 AP 转移到目标子网

如果 AP 和 ZD1000/3000 部署在不同的子网上，可以先让 AP 在 ZD1000/3000 所在的子网上执行自动发现，然后再将 AP 转移到另一个子网。因此，首先要将 AP 连接到 ZD1000/3000 所在的网络。AP 启动时，会发现 ZD1000/3000 并向其注册。如果禁用了自动审批功能，则需手动审批注册请求。

AP 向 ZD1000/3000 成功注册后，将其转移到目标子网。AP 重新连接到其他子网后，能够发现 ZD1000/3000 并与其通信。

注意

如果使用此方法，需确保在 AP 发现 ZD1000/3000 并向其注册后，不会更改 ZD1000/3000 的 IP 地址。如果更改了 ZD1000/3000 的 IP 地址，AP 将无法与之通信，也无法再发现它。

选择 2：自定义 DHCP 服务器

要自定义 DHCP 服务器，需要使用网络上的 ZD1000/3000 设备的 IP 地址来配置 DHCP 选项 43 (043 Vendor Specific Info)（043 供应商特定信息）。当 AP 请求 IP 地址时，DHCP 服务器会将 ZD1000/3000 的 IP 地址列表发送给 AP。如果网络上有多个 ZD1000/3000 设备，AP 将从该 IP 地址列表中
自动选择一个 ZD1000/3000 并向其注册。

注意

以下过程介绍了如何自定义 Microsoft Windows 上运行的 DHCP 服务器。如果 DHCP 服务器在其他操作系统上运行，该过程可能有所不同。

如果网络上只有 ZD1000/3000（没有 ZD1000/3000 子码）

步骤 1　在Windows Administrative Tools（Windows管理工具）中，打开**DHCP**，然后选择要配置的DHCP服务器。

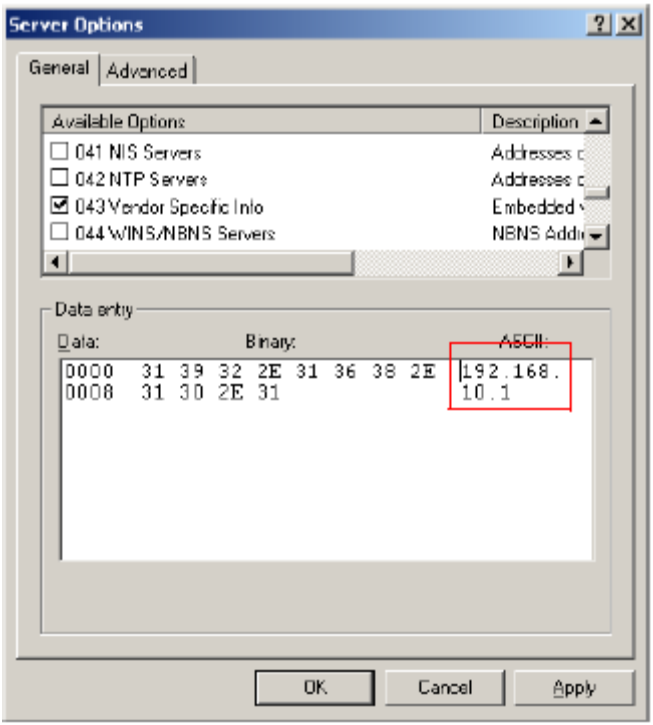
步骤 2　如果**Scope**（作用域）文件夹处于折叠状态，单击加号(+)将其展开。

步骤 3　右键单击**Scope Options**（作用域选项），然后单击**Configure Options**（配置选项）。此时将显示Scope Options（作用域选项）对话框的General（常规）选项卡。

步骤 4　在Available Options（可用选项）下，找到**43 Vendor Specific Info**（43 供应商特定信息）复选框，并将其选中。

步骤 5　将光标放在Data Entry（数据项）部分的ASCII文本区域，然后输入ZD1000/3000设备的IP地址。下图中，ZD1000/3000设备的IP地址为192.168.10.1。

图 1-4 在 ASCII 区域中，输入 ZD1000/3000 设备的 IP 地址



Binary（二进制）文本区域中显示了对应的十六进制 ZD1000/3000 IP 地址。

注意

如果网络上有多个 ZD1000/3000 设备，则在 ASCII 文本区域中输入所有 IP 地址，并使用逗号 (,) 分隔各个 IP 地址。

步骤 6　单击**Apply**（应用）保存更改。

步骤 7　单击**OK**（确定）以关闭Scope Options（作用域选项）对话框。

现在即完成了对自定义 DHCP 服务器的自定义，此后，系统将自动为支持的 AP 提供 ZD1000/3000 IP 地址。

如果网络上只有 ZD1000/3000（有 ZD1000/3000 子码）

步骤 1　在Windows Administrative Tools（Windows管理工具）中，打开**DHCP**，然后选择要配置的DHCP服务器。

步骤 2　如果**Scope**（作用域）文件夹处于折叠状态，单击加号(+)将其展开。

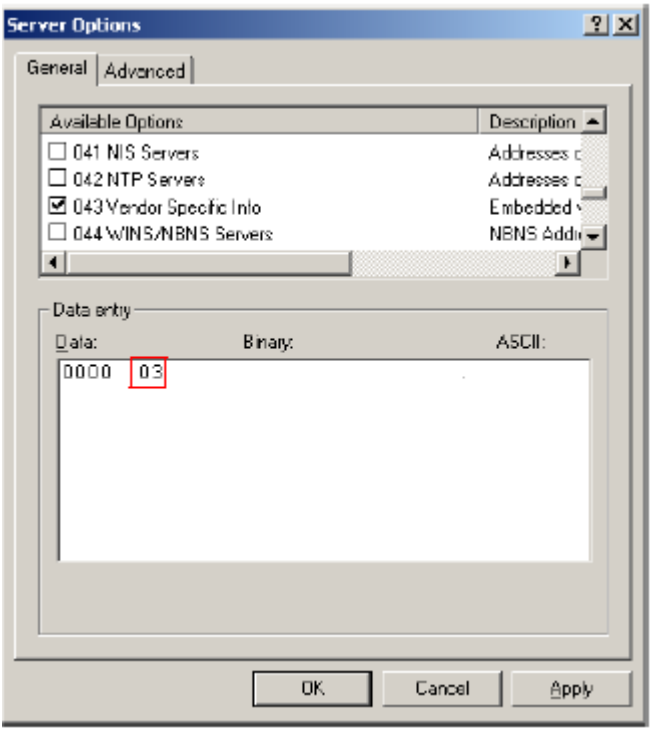
步骤 3　右键单击**Scope Options**（作用域选项），然后单击**Configure Options**（配置选项）。此时将显示Scope Options（作用域选项）对话框的General（常规）选项卡。

步骤 4　在**Available Options**（可用选项）下，找到**43 Vendor Specific Info**（43 供应商特定信息）复选框，并将其选中。

步骤 5　在**Data Entry**（数据项）下，突出显示其中的值，然后按键盘上的**<Delete>**键。

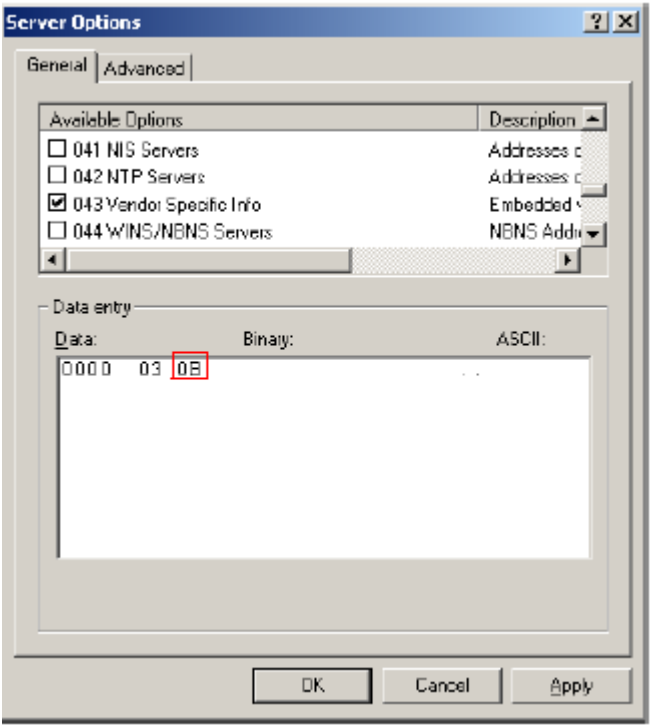
步骤 6　在**Binary**（二进制）文本区域中，再次将光标放在最后一个八进制数（此例中为72）上，然后输入03（ZD1000/3000的子码）。

图 1-5 在 Binary（二进制）文本区域中，输入 03（ZD1000/3000 的子码）



步骤 7　在ZD1000/3000子码(03)的后面输入ZD1000/3000 IP地址长度对应的十六进制长度。例如，如果ZD1000/3000 IP地址为192.168.10.1，则十进制长度为12，对应的十六进制长度为0B。

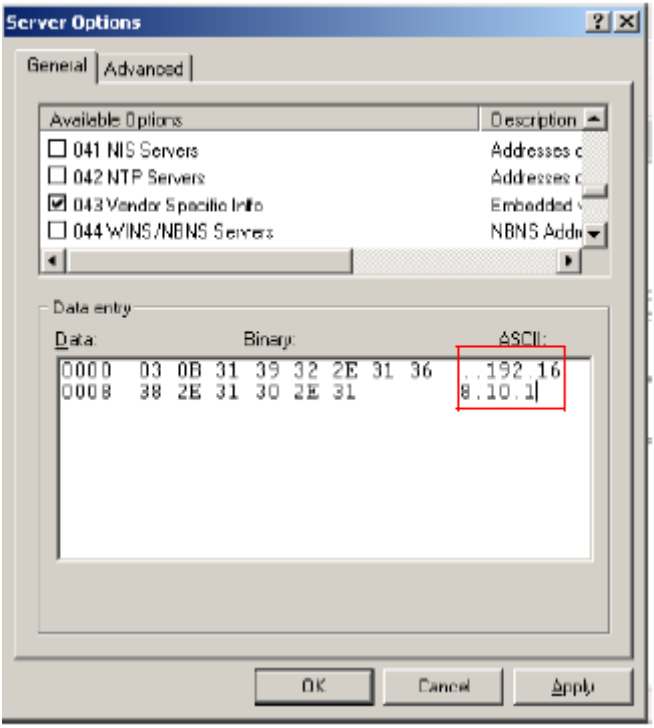
图 1-6 在 ZD1000/3000 子码的后面输入 ZD1000/3000 IP 地址长度对应的十六进制长度。



步骤 8 将光标放在ASCII文本区域中，然后输入ZD1000/3000 IP地址。输入十六进制ZD1000/3000 IP地址时，ASCII文本区域中应已填有两个字节（由两个句点表示）。

下例中，ZD1000/3000 IP 地址是 192.168.10.1。

图 1-7 在 ASCII 文本区域中，输入 ZD1000/3000 IP 地址



步骤 9 单击**Apply**（应用）保存更改。

步骤 10 单击**OK**（确定）以关闭Scope Options（作用域选项）对话框。

现在即完成了对 DHCP 选项 43 的配置，此后，系统将自动为支持的 AP 提供 ZD1000/3000 IP 地址。

选择 3：向 DNS 服务器注册 ZD1000/3000

向 DNS 服务器注册 ZD1000/3000 后，向 DHCP 服务器请求 IP 地址的 AP 也会获取 DNS 相关信息，AP 可通过这些信息发现网络上的 ZD1000/3000 设备。使用通过 DHCP 请求获取的 DNS 信息时，AP 将尝试使用 ZoneDirector{DNS domain name}来解析 ZD1000/3000 IP 地址（或 IP 地址）。

向 DNS 服务器注册 ZD1000/3000 设备

- 步骤 1：在 DHCP 服务器上设置 DNS 域名
- 步骤 2：在 DHCP 服务器上设置 DNS 服务器 IP 地址
- 步骤 3：向 DNS 服务器注册 ZD1000/3000 IP 地址

注意

以下过程介绍如何自定义 Microsoft Windows Server 上运行的 DHCP 服务器。如果 DHCP 服务器在其他操作系统上运行，该过程可能有所不同。

步骤 1：在 DHCP 服务器上设置 DNS 域名

步骤 1　在Windows Administrative Tools（Windows管理工具）中，打开**DHCP**，然后选择要配置的DHCP服务器。

步骤 2　单击加号(+)将**Scope**（作用域）展开。

步骤 3　右键单击**Scope Options**（作用域选项），然后单击**Configure Options**（配置选项）。此时将显示Scope Options（作用域选项）对话框的**General**（常规）选项卡。

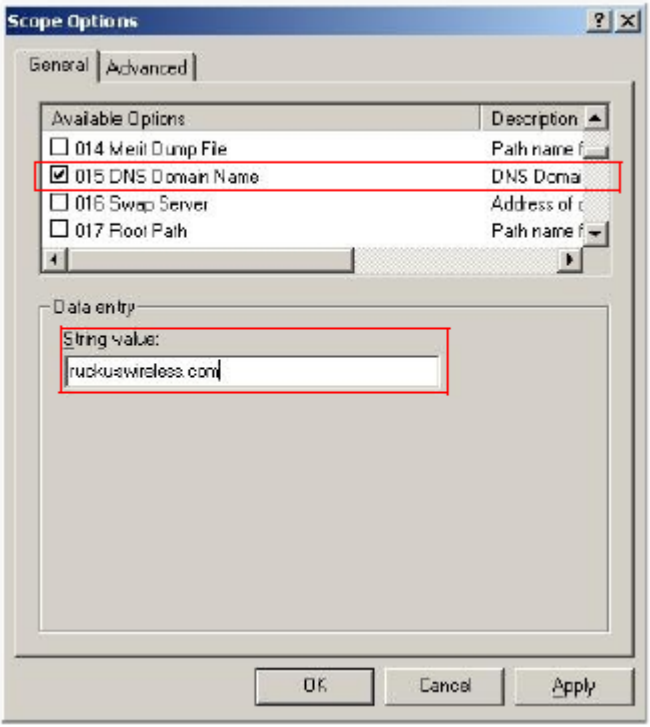
步骤 4　在**Available Options**（可用选项）下，找到**15 DNS Domain Name**（15 DNS域名）复选框，并将其选中。

步骤 5　在**Data Entry**（数据项）下的**String value**（字符串值）文本框中，输入公司域名。

步骤 6　单击**Apply**（应用）保存更改。

步骤 7　单击**OK**（确定）关闭Scope Options（作用域选项）对话框。

图 1-8 选中 015 DNS Domain Name（015 DNS 域名）复选框，然后在 String value（字符串值）中输入公司域名



步骤 2：在 DHCP 服务器上设置 DNS 服务器 IP 地址

步骤 1　在Windows Administrative Tools（Windows 管理工具）中，打开**DHCP**，然后选择要配置的DHCP服务器。

步骤 2　如果**Scope**（作用域）文件夹处于折叠状态，单击加号**(+)**将其展开。

步骤 3　右键单击**Scope Options**（作用域选项），然后单击**Configure Options**（配置选项）。此时将显示Scope Options（作用域选项）对话框的**General**（常规）选项卡。

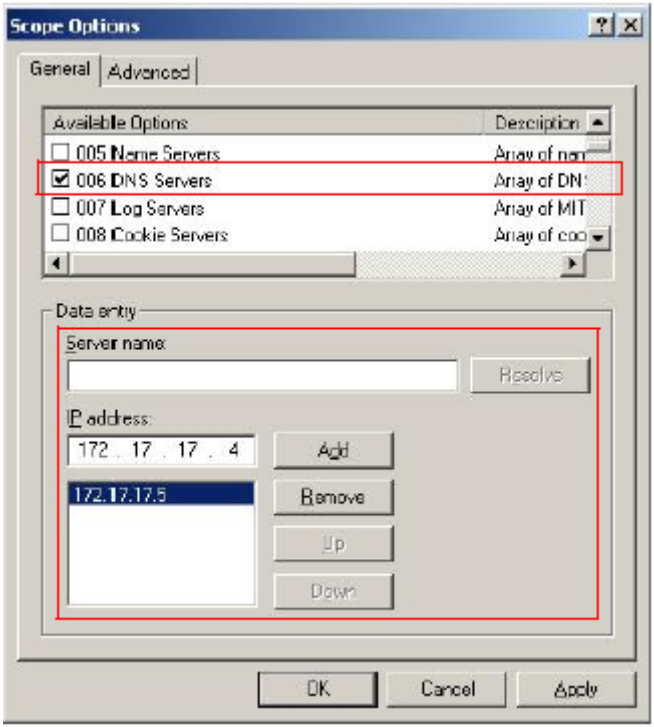
步骤 4　在**Available Options**（可用选项）下，找到**6 DNS Servers**（6 DNS服务器）复选框，并将其选中。

步骤 5　在**Data Entry**（数据项）下的IP地址框中，输入DNS服务器的IP地址，然后单击**Add**（添加）。如果网络上有多个DNS服务器，则可重复上述过程以添加其他DNS服务器。

步骤 6　单击**Apply**（应用）保存更改。

步骤 7　单击**OK**（确定）关闭Scope Options（作用域选项）对话框。

图 1-9 选中 6 DNS Servers（6 DNS 服务器）复选框，然后在 Data entry（数据项）下输入 DNS 服务器的 IP 地址



步骤 3：向 DNS 服务器注册 ZD1000/3000 IP 地址

使用 DNS 相关信息完成对 DHCP 服务器的配置之后，需要向 DNS 服务器注册网络上 ZD1000/3000 设备的 IP 地址。此任务的具体步骤视所用的 DNS 服务器软件而定。

欲了解在 Windows 上配置内置 DNS 服务器的信息，可访问以下网址：http://support.microsoft.com/kb/814591。

注意

当 DNS 服务器提示为每个 ZD1000/3000 IP 地址输入对应的主机名时，必须输入 ZoneDirector。这对确保 AP 能够解析 ZD1000/3000 IP 地址至关重要。

向 DNS 服务器注册 ZD1000/3000 IP 地址后，此过程便告完成。现在，网络上的 AP 应能够发现其他子网上的 ZD1000/3000。

1.4 使用 ZD1000/3000 Web 界面

ZD1000/3000 管理应用程序包括五个组件，通过这些组件，可以管理和监控优科 WLAN（包括 ZD1000/3000 和所有接入点）。

表 1-4 ZD1000/3000 Web 界面的组件

仪表板	首次通过 Web 界面登录到 ZD1000/3000 时，系统将显示一个配有多个小组件的仪表板，包括各种描述网络概况及当前网络状态的指示符和表。每个指示符、计量器或表都提供了相关链接，单击这些链接可显示相关网络元素的详细视图。 提示：可以将仪表板上的任何表或指示符最小化（隐藏），并通过左下角的“添加小组件”选项将其重新打开。
小组件	“小组件”是仪表板组件，每个小组件都包含一个单独的指示符或表，从而构成了当前的仪表板。可以添加或删除各个小组件，以调整 ZD1000/3000 仪表板上显示的摘要信息。
选项卡	有四个选项卡（仪表板、配置、监控和管理），可单击其中任意一个选项卡，并使用该选项卡的功能和选项。单击某个选项卡时，ZD1000/3000 将显示该选项卡特有的按钮*。利用各个选项卡中的按钮，可以对优科网络进行设置、管理和监控。注意：单击另外三个选项卡中的任意一个后，仪表板将成为第四个可用的选项卡。
按钮	左侧的按钮列将根据所选的选项卡而有所不同。网络管理员可以使用这些按钮来管理和监控网络。单击某个按钮可在右侧的工作区中查看相关选项。
工作区	按钮右侧的大块区域将显示特定的功能和选项集，具体视打开的选项卡和单击的按钮而定。

[* = 仪表板除外。]

1.4.1 浏览仪表板

仪表板提供了多个指示符和表，用于描述网络概况及当前网络状态。某些指示符中的值可链接到相关网络元素的详细视图。

图 1-10 仪表板

注意

初始视图中可能不显示某些指示符。可以通过屏幕左下方的“添加小组件”功能显示或隐藏指示符。可参考1-22页中的“使用指示符小组件”。

表 1-5列出了仪表板上提供的指示符。

表 1-5 仪表板指示符

指示符	说明
系统概述	显示 ZD1000/3000 系统信息，包括 IP 地址、MAC 地址、型号、许可接入的最大 AP 数、序列号、软件版本号和其他信息。
设备概述	显示 ZD1000/3000 正在管理的 AP 的数量，以及连接到这些 AP 的客户端的数量。此外，还显示 ZD1000/3000 检测到的可疑设备的数量。
使用情况摘要	显示过去 1 小时和 24 小时内的使用情况统计信息。

指示符	说明
Most Active Client Devices（最活跃的客户端设备）	通过 MAC 地址、IP 地址和用户名来标识最活跃的客户端。并基于每个客户端与 AP 相关联后所发送(Tx)和接收(Rx)的总字节数，计算带宽使用情况(MB)。
最近的用户活动	显示用户的活动。
最近的系统活动	显示与 ZD1000/3000 操作相关的系统活动。
最常用的接入点	列出目前处理客户端请求最多的接入点。
当前活动的 WLAN	显示当前处于活动状态的 ZD1000/3000 WLAN 的详细信息。
当前活动的 WLAN 组	显示可用 WLAN 组的详细信息。如果尚未创建任何 WLAN 组，将仅显示默认 WLAN 组。
当前管理的接入点	显示 ZD1000/3000 当前正在管理的接入点的详细信息。
支持	显示优科技术支持工程师的联系信息。

注意

可以通过单击列标题对仪表板中显示的信息进行排序（升序或降序）。

1.4.2 使用指示符小组件

仪表板小组件表示构成当前仪表板的指示符。可以添加或删除各个指示符小组件，以调整显示的 ZD1000/3000 摘要信息。

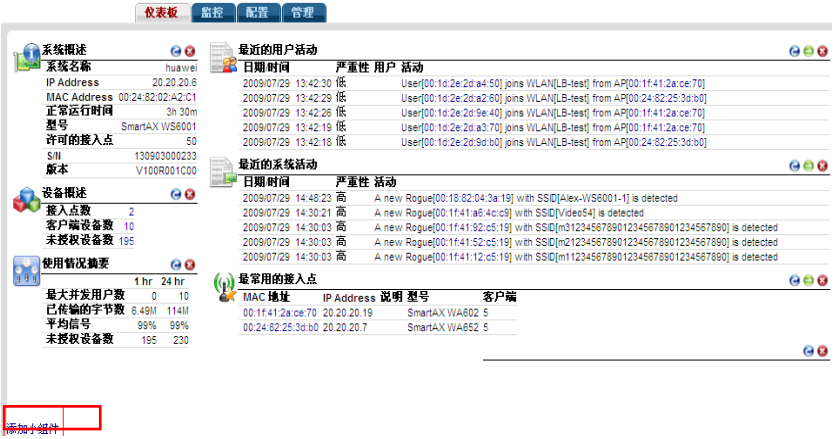
添加小组件

要添加小组件

步骤 1　打开仪表板。

步骤 2　单击仪表板页面左下角的“添加小组件”链接。

图 1-11 “添加小组件”链接位于仪表板的左下角



打开的小组件窗格位于仪表板的左上角。

步骤 3　选择任意小组件图标并将其拖放到仪表板上，添加该小组件。关闭某个小组件后，它将显示在此窗格中。

图 1-12 小组件图标显示在仪表板的左上角

步骤 4　单击小组件窗格中的“完成”关闭该窗格。

删除小组件

要删除仪表板中的小组件，可单击当前打开的小组件的图标。仪表板将即时刷新，删除的小组件将从页面中消失。

图 1-13 要删除某个小组件，可单击相应的红色 x 图标

1.5 关于优科 WLAN 的安全性

默认情况下，初次安装后，优科网络会将所有授权用户连接到内部 WLAN。基于 WPA 的 WLAN 已配置成向所有授权用户提供安全保护。（自带的“来宾”WLAN 为来宾用户提供明文但受控制的访问权限。）但优科无线设备还提供了可通过 ZD1000/3000 应用于内部 WLAN 的其他安全选项。

这些选项包括安全性较低的基于 WEP 密钥的配置、默认的基于 WPA 密码的配置以及安全性较高的基于证书的 802.1x EAP 配置。用户所做的选择通常取决于客户端设备所支持的客户端身份验证类型。

例如，由于客户端设备（计算机或无线网络适配器）的原因，一些 WLAN 用户可能只能使用基于 WEP 的安全系统。但通过 Web 界面，用户可以有以下多种选择：

- 将现有的内部配置从 WPA 更改为安全性较弱的 WEP，或者
- 通过 WEP 选项为需要 WEP 的用户添加自定义 WLAN，而其他用户仍使用原来的、安全性较强的内部 WPA 配置，或者
- 将默认 WPA 设置替换为安全身份验证/加密方法 802.1x EAP。802.1x 的缺点是设置起来比较麻烦，除了要执行其他任务外，还需要将根证书副本传送给用户，然后用户再将该证书导入到客户端设备中。如果有大量用户在使用网络，进行该设置可能会导致连接中断。

ZD1000/3000 支持一个或多个 WLAN；网络管理员可以像添加 WPA 内部 WLAN 一样，根据需要轻松地为用户添加 WEP WLAN。用户可以利用 Zero-IT Activation（零

IT 激活）功能来自动获取 WEP 密钥，也可以在客户端设备无线配置中手动输入 WEP 密钥。

如果偏好默认配置的安全性，可以使用不会中断当前用户连接的自定义选项。

3-11页中的“创建 WLAN”中详细介绍了三个基本选项（WEP、WPA 和 802.1x），网络管理员可以在该部分了解如何将其应用到 WLAN。

2 系统设置

2.1 更改网络地址

如果需要更新 ZD1000/3000 的 IP 地址和 DNS 服务器设置，可执行下列步骤。

注意

更改 IP 地址后，将断开与 ZD1000/3000 的 Web 界面连接。可以使用新 IP 地址在 Web 浏览器中再次登录 Web 界面。

步骤 1 转至“配置”>“系统”。

步骤 2 配置表 2-1中列出的设置。

表 2-1 “管理 IP”设置

设置	描述
手动或 DCHP	如果要手动为 ZD1000/3000 分配 IP 地址，可选择“手动”。选择此选项后，还需输入 IP Address（IP 地址）、Netmask（子网掩码）和 Gateway（网关）信息。 如果希望 ZD1000/3000 自动从网络上的 DHCP 服务器获取 IP 地址，可选择“DHCP”。选择此选项后，无需再输入其他信息。
IP Address（IP 地址）	输入要手动分配给 ZD1000/3000 的 IP 地址。
Netmask（子网掩码）	输入已分配给 ZD1000/3000 的 IP 地址的子网掩码。
首选 DNS 服务器	输入 ZD1000/3000 使用的首选 DNS 服务器。

设置	描述
备用 DNS 服务器	（可选）输入 ZD1000/3000 使用的备用 DNS 服务器。

步骤 3　单击“应用”保存设置。将断开与ZD1000/3000的连接。

要重新登录 Web 界面，使用新分配的 IP 地址打开 Web 浏览器或使用 UPnP 应用程序重新找到 ZD1000/3000。

图 2-1 “管理 IP”设置

2.2 更改系统名称

首次使用“安装向导”时，系统会提示为 ZD1000/3000 输入一个网络可识别的系统名称。如果需要，可以通过以下步骤更改该名称：

步骤 1　转至“配置”>“系统”。

步骤 2　删除“系统名称”（位于“标识”下）中的文本，然后输入一个新名称。

此名称长度应介于 6 到 32 个字符之间，名称中可使用字母、数字、下划线(_)和连字符(-)。不要使用空格或其他特殊字符。

步骤 3　单击“应用”保存设置。此更改立即生效。

图 2-2 “配置”>“系统”页面上的标识部分

2.3 配置内置 DHCP 服务器

ZD1000/3000 内置了 DHCP 服务器，可以为与其连接的设备分配 IP 地址。注意，必须首先为 ZD1000/3000 分配一个静态 IP 地址后，才能启用内置 DHCP 服务器。如果将 ZD1000/3000 配置为从 DHCP 服务器获取 IP 地址，则系统页面中不会显示内置 DHCP 服务器的配置界面。

2.3.1 启用内置 DHCP 服务器

注意

优科建议仅当网络中不存在其他 DHCP 服务器的情况下才启用内置 DHCP 服务器。注意，ZD1000/3000 中的 DHCP 服务器仅支持一个子网。

如果启用内置 DHCP 服务器，优科还建议启用多 DHCP 服务器检测程序。有关详细信息，参考4-12页中的“检测未授权 DHCP 服务器”。

步骤 1 转至“配置”>“系统”。

步骤 2 在“DHCP服务器”部分，配置表 2-2中列出的设置。

表 2-2 “DHCP 服务器”选项

设置	描述
启用 DHCP 服务器	要启用内置 DHCP 服务器，需选中此复选框。 要禁用内置 DHCP 服务器，则不要选中此复选框。
起始 IP	输入内置 DHCP 服务器将分配给 DHCP 客户端的第一个 IP 地址。注意，起始 IP 地址必须与分配给 ZD1000/3000 的 IP 地址位于同一子网中。如果输入的值无效，将显示一条错误消息并提示是否希望 ZD1000/3000 更正此值。单击“确定”可以自动更正。
IP 数	输入希望分配给客户端的 IP 地址的最大数量。内置 DHCP 服务器最多可分配 255 个 IP 地址，其中包括分配给 ZD1000/3000 的 IP 地址。 默认值为 200。
租用时间	设置分配给 DHCP 客户端 IP 地址的最大租用时间，范围从六个小时到两周（默认值为一周）。

步骤 3 单击应用。

注意

如果在任意文本框中输入的值都无效，将显示一条错误消息并提示是否希望 ZD1000/3000 自动更正此值。单击确定可以将其更改为正确的值。

图 2-3 “DHCP 服务器”选项

2.3.2 查看 DHCP 客户端

要查看当前的 DHCP 客户端列表，单击“若要查看 DHCP 服务器分配的所有 IP 地址”后的“请单击此处”。将显示一张表，其中列出了当前所有 DHCP 客户端的 IP 地址、MAC 地址和剩余租用时间。

图 2-4 要查看当前 DHCP 客户端，单击“单击此处”链接

2.4 更新系统时钟

初始安装期间，ZD1000/3000 中的时钟将自动与管理 PC 的时钟同步。可以使用 Web 界面检查当前系统时钟，系统时钟在“配置”界面静态显示。如果显示的系统时钟不正确，可以立即将系统时钟与 PC 时钟重新同步。

另一选项是设置 ZD1000/3000 的 NTP 服务器（下面将进行详细介绍），通过 NTP 服务器提供时钟同步和更新。

步骤 1 转至“配置”>“系统”。

步骤 2 在“系统时间”部分，配置表 2-3中列出的设置。

表 2-3 “系统时间”中列出的设置

设置	描述
刷新	单击此选项可更新系统时间的显示。
与计算机同步时间	如果需要，单击此选项可以立即将系统时钟与 PC 时钟重新同步。
使用 NTP 自动同步 ZoneDirector 时钟	默认情况下，此选项处于启用状态。要禁用此选项，则不要选中此复选框。

步骤 3 单击“应用”保存系统时钟和NTP配置结果。

图 2-5 “系统时间”选项

2.5 系统日志设置

ZD1000/3000 维护最新事件和警报的内部日志。日志的容量是固定的，日志内容到达一定程度后，ZD1000/3000 将开始删除旧内容以便为新内容腾出空间。日志的内容并非永久保存，如果关闭 ZD1000/3000，日志将被删除。若要永久保存日志，可以安装一个 syslog 服务器，使用 Web 界面配置 ZD1000/3000 将所有日志内容转发到该 syslog 服务器 – 后有详细介绍。

2.5.1 查看当前日志内容

步骤 1 转至“监控”>“所有事件/活动”。

步骤 2 查看此处列出的事件和警报。参阅图 2-6。

注意

日志条目按时间逆序列出（最新日志位于列表顶部）。

步骤 3 单击列标题可按类别对内容进行排序。

步骤 4 单击任意列两次可在按时间排序和按字母数字排序之间进行切换。

图 2-6 “所有事件/活动”页面

2.5.2 检查当前日志设置

可按照下列步骤来查看和自定义日志设置：

步骤 1 转至“配置”>“系统”。

步骤 2 向下滚动到“日志设置”。

步骤 3 在“日志设置”部分中，配置表 2-4中列出的设置。

表 2-4 日志设置

设置	描述
事件日志级别	选择三个日志级别中的一个：显示详细信息、警告和关键事件以及仅限关键事件。
远程 Syslog	要启用 syslog 远程日志记录功能，选中“对位于以下位置的远程 syslog 服务器启用报告”复选框，然后在所给框中输入 Syslog 服务器的 IP 地址。

步骤 4 单击Apply（应用）保存设置。更改立即生效。

图 2-7 Log Settings（日志设置）选项

2.6 设置电子邮件警报通知

如果检测到警报，ZD1000/3000 会在日志中记录。也可通过电子邮件将警报发送到所配置的电子邮件地址。

注意

有关生成电子邮件警报的事件类型，参考以下部分中的。

要启用此选项，请执行下列步骤：

步骤 1 转至“配置”>“警报设置”。将出现“电子邮件通知”配置界面。

步骤 2 配置表 2-5中列出的设置。

表 2-5 “电子邮件通知”设置

设置	描述
触发警报时发送电子邮件	要启用电子邮件通知，需选中此复选框。 要禁用电子邮件通知，则不要选中此复选框。
电子邮件地址	输入接收警报消息的电子邮件地址。
邮件服务器 IP 地址	输入邮件服务器的 IP 地址。

步骤 3 单击“应用”。将激活电子邮件通知功能。

图 2-8 “警报设置”页面

2.6.1 触发警报通知的事件

在 ZD1000/3000 中触发电子邮件警报通知的事件有多个。表 2-6中列出了所有这些事件。

表 2-6 触发警报通知的事件

事件	描述	警报通知
检测到可疑 AP	ZD1000/3000 检测到可疑 AP。	检测到一个 SSID 为{SSID}的新可疑 AP：{rogue AP name}。
检测到 ad-hoc 网络	ZD1000/3000 检测到 ad-hoc 网络。	检测到一个 SSID 为{SSID}的新 ad-hoc 网络：{adhoc network name}。
与AP 的通信中断	ZD1000/3000 与 AP 的通信中断，无法在 20 分钟后重建通信连接。	与{AP name}的通信中断。
检测到假冒 SSID 的 AP	ZD1000/3000 检测到一个非法 AP 正在假冒网络中某个 AP 的 SSID。	检测到一个假冒 SSID 的新非法 AP：{rogue AP name}，其 SSID 为{SSID}。
检测到假冒 MAC 地址的 AP	ZD1000/3000 检测到一个非法 AP 正在假冒某个 AP 的 SSID。	检测到一个具有{SSID}，假冒 MAC 的新{rogue AP name}。
检测到多个 DHCP 服务器	ZD1000/3000 在网络上检测到多个 DHCP 服务器。	在{ip}上检测到多个 DHCP 服务器。

如果发生上述任一事件，ZD1000/3000 将向在“配置”>“警报设置”页面上指定的电子邮件地址发送电子邮件通知。

注意

除与 AP 的通信中断事件外，ZD1000/3000 只为每个事件发送一次电子邮件警报通知。如果同一事件再次发生，则不再发送任何警报，直到在“监控”>“所有警报”页面上清除了警报。另一方面，每次发生与 AP 的通信中断事件时，ZD1000/3000 都会发送一个警报通知。

2.7 升级 ZD1000/ZD3000 和优科 AP

定期查看优科支持网站以获取适用于 ZD1000/3000 等优科网络设备以及所有优科 AP 的软件更新。将新的软件下载到管理 PC 上后，可以按照下列步骤完成网络升级（ZD1000/3000 和 AP）。

注意

升级 ZD1000/3000 和 AP 时会暂时中断网络的连接和服务。为尽量降低网络中断带来的影响，优科建议在非高峰时段进行升级。

步骤 1　转至“管理”>“升级”。

步骤 2　在“软件升级”部分，单击“浏览”。将出现“浏览”对话框。

步骤 3　浏览至保存升级软件的位置，然后单击“打开”。

步骤 4　文本字段框中显示升级文件名后，“浏览”按钮将变为“升级”按钮。

步骤 5　单击“升级”。

ZD1000/3000 将自动断开当前连接的用户，执行升级，然后重新启动。升级完成后，ZD1000/3000 上的状态指示灯将持续点亮。可用管理员身份重新登录到 Web 界面。

注意

完整的网络升级还包括后续的 AP 固件升级。ZD1000/3000 升级后，将与每个 AP 通信，将其升级，然后恢复到服务状态。

注意

AP 使用 FTP 从 ZD1000/3000 下载固件，进行更新。如果用户在 ZD1000/3000 和 AP 之间配置了访问控制列表或防火墙，请确保 FTP 流量可以通过以使 AP 成功下载固件，进行更新。

图 2-9 “升级”页面

2.8 使用备份文件

在成功配置好优科网络后，可能需要备份配置。生成的配置备份存档可用于恢复 ZD1000/3000 和网络。而且，还可以在每次修改设置后，创建新的备份文件。

2.8.1 备份系统配置

步骤 1 转至“管理员”>“备份”。

步骤 2 在“备份配置”部分，单击“备份”。将出现“文件下载”对话框。

步骤 3 单击“保存”。

步骤 4 显示“另存为”对话框时，输入欲保存文件的名称，选择目标文件夹，然后单击“保存”。

步骤 5 确保文件名以“.TGZ”扩展名结尾。

步骤 6 出现“下载完毕”对话框时，单击“关闭”。

图 2-10 “备份配置”选项

2.8.2 恢复 ZD1000/3000 的存档备份设置

注意

恢复存档备份设置将自动重启 ZD1000/3000 和当前其管理的所有 AP。与这些 AP 相关联的用户将临时断开连接；ZD1000/3000 和 AP 完成启动后，无线访问将自动恢复。

步骤 1 转至“管理员”>“备份”。

步骤 2 查看“还原配置”说明，然后单击Browse（浏览）。

步骤 3 使用Browse（浏览）对话框找到备份文件。

步骤 4 选择该文件，然后单击“打开”。

步骤 5 选择表 2-7中列出的还原选项之一。

表 2-7 “还原”选项

选项	描述
还原所有配置	如果希望设备使用在备份文件中的所有设置（包括 IP 地址、无线设置、访问控制列表以及所有其他设置），选择此选项。

还原除系统名称/IP 地址外的所有配置	如果要部署另一个 ZD1000/3000 以便实现冗余配置，选择此选项。
仅还原关于 WLAN、访问控制、用户角色和用户的配置	如果希望将备份文件用作配置模板，选择此选项。

步骤 6 单击“还原”按钮。

ZD1000/3000 还原备份文件。在此过程中，ZD1000/3000 将自动断开用户连接。还原过程完成后，ZD1000/3000 将自动重新启动，无线网络也将恢复使用

2.9 将 ZD1000/3000 还原为出厂设置

在某些极端条件下，可能要重新初始化 ZD1000/3000，并将其重置为“出厂默认设置”状态。在这种状态下，网络基本上可以使用，但需要手动重新配置所有用户/来宾/日志及其他记录、帐户和配置。

注意

此过程完成后，将需要重新执行一次完整配置。如果 ZD1000/3000 位于实际网络中，可能会配置新的 IP 地址。在这种情况下，系统可以由 UPnP 客户端应用程序发现，例如 Windows 网上邻居。如果连接的网络中不存在 DHCP 服务器，则系统的默认 IP 地址为 192.168.0.2，子网掩码为 255.255.255.0。

《入门指南》(QSG)中提供了一套完整说明。在将 ZD1000/3000 恢复为出厂默认设置之前，应打开并打印 QSG。在恢复为出厂默认设置状态后，应按照此说明设置 ZD1000/3000。

将 ZD1000/3000 重置为出厂默认设置

步骤 1 转至“管理员”>“备份”。

步骤 2 当出现“备份/还原”页面时，查找“还原为出厂设置”，并单击该按钮。

步骤 3 由于此操作影响较大，将出现一个或多个确认对话框。单击“确定”确认此操作。

此过程开始时，管理员将退出 Web 界面。

重置完成后，状态指示灯将呈红色闪烁，然后呈绿色闪烁，表明系统处于“出厂默认设置”状态。完成“安装向导”后，状态指示灯将呈长绿色状态。

图 2-11 “还原为出厂设置”部分

2.9.1 其他还原出厂默认设置方法

如果无法通过软件重置 ZD1000/3000，可以执行下面的“硬”重置：

注意

此过程完成前不能断开 ZD1000/3000 的电源。

步骤 1 找到ZD1000/3000前端面板右侧的小孔。

步骤 2 在小孔中插入拉直的曲别针并按住至少5秒钟。

重置完成后，状态指示灯将呈红色闪烁，然后呈绿色闪烁，表明系统处于“出厂默认”状态。

完成“安装向导”后，状态指示灯将呈长绿色状态。

2.10 使用 SSL 证书

如果使用 HTTPS 连接到 ZD1000/3000 Web 界面，每次连接到 Web 界面时，都会出现一条安全警告。这是因为 ZD1000/3000 用于 HTTPS 通信的默认 SSL 证书（或安全证书）由优科签署，而大多数 Web 浏览器不能识别该证书。

如果要防止这些安全警告出现，则需要导入由可识别的证书颁发机构（例如，VeriSign、Thawte 等）颁发的 SSL 证书。如果尚未拥有 SSL 证书，则需要创建证书签署请求并从证书颁发机构购买证书。

2.10.1 创建证书签署请求

如果没有现成的 SSL 证书，则需要创建证书签署请求(CSR)文件，并将其发送到证书颁发机构(CA)以购买 SSL 证书。ZD1000/3000 Web 界面提供了可用于创建 CSR 文的界面。

要创建证书请求文件：

步骤 1 转至“配置”>“SSL证书”。

步骤 2 在“生成请求”部分下，配置表 2-8中列出的设置。

表 2-8 CSR 设置

设置	描述
通用名称	输入 Web 服务器的 IP 地址。此地址必须完全匹配（例如 192.168.0.2）。
替代名称	输入 Web 服务器的完整域名。此域名必须完全匹配（例如 www.huawei.com）。

设置	描述
组织	输入组织的完整法律名称（例如 Huawei, Inc.）。 不要将组织名称缩写。
组织单元	输入组织中管理网络安全的部门名称（例如“网络管理”）。
地方/城市	输入组织所在的城市（例如北京）。
洲/省	输入组织法律意义上的位置所在的省/直辖市/自治区（例如北京）。不要将省/直辖市/自治区名称缩写。
国家	输入国家/地区的双字母 ISO 缩写（例如，如果是在中国，可输入 CN）。

步骤 3 单击“应用”。将显示一个对话框，提示保存已创建的CSR文件(myreq.csr)。

步骤 4 将该文件保存到计算机。

步骤 5 访问证书颁发机构的网站，按照说明购买SSL证书。

步骤 6 当系统提示输入证书签署请求时，复制并粘贴步骤 4中保存的文本文件的内容，然后完成证书购买过程。

在证书颁发机构批准 CSR 之后，将会收到通过电子邮件发送的 SSL 证书。下面是从证书颁发机构接收的一个已签署证书的示例：

−−−−−BEGIN CERTIFICATE−−−−−（证书开始）

MIIFVjCCBD6gAwIBAgIQLfaGuqKukMumWhbVf5v4vDANBgkqhkiG9w0
BAQUFADCBsDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTa
WduLCBJbmMuMR8wHQYDVQQLBgEFBQcBAQRtMGswJAYIKwYBBQUHMA
GGGGh0dHA6Ly9vY3NwLnZlcmlzaWduLmNvbTBDBggrBgEFBQcwAoY3Ahr
0cDovL1NWUlNlY3VyZS1haWEudmVyaXNpZ24uY29tL1NWUlNlY3VyZTIwMD
UtYWlhLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFowWDBWFglpbWFnZS9na
WYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEFGDAmFiRod
HRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZIhvcNAQEF
BQADggEBAI/S2dmm/kgPeVAlsIHmx751o4oq8+fwehRDBmQDaKiBvVXGZ5
ZMnoc3DMyDjx0SrI9lkPsn223CV3UVBZo385g1T4iKwXgcQ7WF6QcUYOE6HK+
4ZGcHermFf3fv3C1FoCjq+zEu8ZboUf3fWbGprGRA+MR/dDI1dTPtSUG7/zWjXO5
jC//0pykSldW/q8hgO8kq30S8JzCwkqrXJfQ050N4TJtgb/YC4gwH3BuB9wqpRjUahT
iK1V1ju9bHB+bFkMWIIMIXc1Js62JClWzwFgaGUS2DLE8xICQ3wU1ez8RUPGnw
SxAYtZ2N7zDxYDP2tEiO5j2cXY7O8mR3ni0C30=
-----END CERTIFICATE-----（证书结束）

步骤 7 复制已签署证书的内容，然后将其粘贴到一个文本文件中。保存文件。

现在可以将已签署的证书导入到 ZD1000/3000。参考下面的部分了解相关说明。

2.10.2 导入 SSL 证书

如果已有 SSL 证书，可以将证书导入到 ZD1000/3000 并将其用于 HTTPS 通信。要完成此过程，需要 SSL 证书文件和在创建证书签署请求(CSR)文件时设置的密钥对码。

要导入 SSL 证书：

步骤 1 将证书文件复制到可以从ZD1000/3000 Web界面访问的位置（本地驱动器上的位置或网络共享位置）。

步骤 2 登录到ZD1000/3000 Web界面，然后单击“配置”>“证书”。

步骤 3 在“导入证书”下，单击Browse（浏览），然后转至保存证书文件的位置。

步骤 4 单击“打开”。如果选择的证书文件有效，将出现“导入”按钮。

步骤 5 单击“导入”完成将证书文件导入到ZD1000/3000的过程。

图 2-12 “导入证书”部分

2.11 配置 SNMP

ZD1000/3000 支持简单网络管理协议(SNMP) v2，因此可以查询 ZD1000/3000 信息（例如系统状态、WLAN 列表、AP 列表和客户端列表）并配置系统。此外，还可以用 SNMP 陷阱来接收针对 AP 和客户端的实时告警。

2.11.1 启用 SNMP 代理

步骤 1　在“系统”页面的“网络管理”部分，向下滚动到页面底部。

步骤 2　在“SNMP代理”部分下，配置表 2-9中列出的设置。

表 2-9 “SNMP 代理”设置

设置	描述
启用 SNMP 代理	要启用 SNMP 代理，需选中此复选框。 要禁用 SNMP 代理，则不要选中此复选框。
SNMP RO community（SNMP 只读密码）	（必需）设置 read-only（只读）密码字符串。将 SNMP Get 请求发送到 ZD1000/3000（以检索信息）的应用程序需要在发送该请求的同时发送此字符串，然后才被允许进行访问。默认值 public。
SNMP RW community（SNMP 读写密码）	（必需）设置 read-write（读写）密码字符串。将 SNMP Set 请求发送到 ZD1000/3000（以设置某些 SNMP MIB 变量）的应用程序需要在发送该请求的同时发送此字符串，然后才被允许进行访问 默认值为 private。
系统联系信息	（可选）输入电子邮件地址。
系统位置	（可选）输入 ZD1000/3000 设备的位置。

步骤 3　单击“应用”保存更改。

图 2-13 启用 SNMP 代理

2.11.2 启用 SNMP 陷阱告警

如果网络上有 SNMP 陷阱告警服务器，可以配置 ZD1000/3000 向此服务器发送 SNMP 陷阱告警。如果要自动接收反映潜在网络问题的接入点和客户端等事件告警，可启用此功能（参阅2-24页中的“ZD1000/3000 发送的告警”）。

步骤 1　在“系统”页面的“网络管理”部分，向下滚动到页面底部。

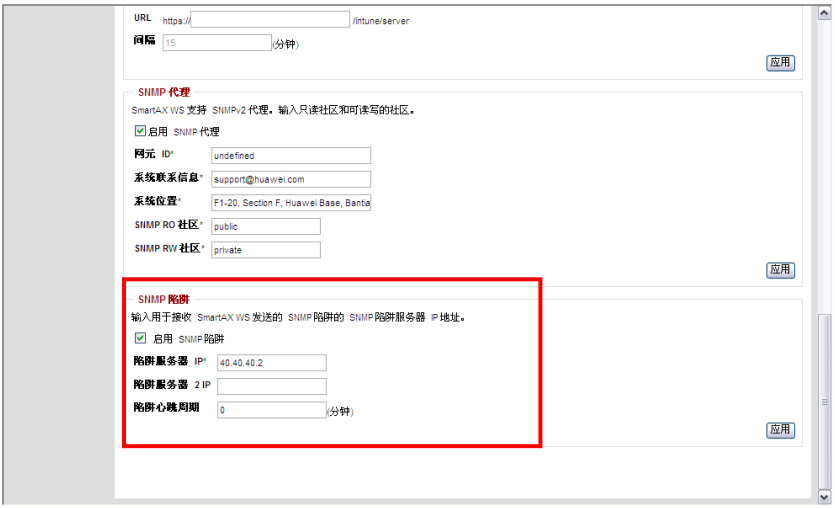
步骤 2　在“SNMP 陷阱”下，配置表 2-10中列出的设置。

表 2-10 SNMP 陷阱告警设置

设置	描述
启用 SNMP 陷阱	要启用 SNMP 陷阱告警，需选中此复选框。 要禁用 SNMP 陷阱告警，则不要选中此复选框。
陷阱服务器 IP	输入网络上 SNMP 陷阱告警服务器的 IP 地址。

步骤 3 单击“应用”保存更改。

图 2-14 启用 SNMP 告警



ZD1000/3000 发送的告警

ZD1000/3000 将向指定的 SNMP 告警服务器发送七个事件的告警。
表 2-11列出了 ZD1000/3000 发送的告警和发送时间。

表 2-11 陷阱通知

陷阱名称	描述
ruckusACEventAPJoinTrap	有一个 AP 加入到 ZD1000/3000。该 AP 的 MAC 地址包含在告警消息中。
ruckusACEventSSIDSpoofTrap	网络上检测到假冒 SSID 的 AP。该非法 AP 的 MAC 地址和 SSID 包含在告警消息中。
ruckusACEventMACSpoofTrap	网络上检测到假冒 MAC 地址的 AP。该非法 AP 的 MAC 地址和 SSID 包含在告警消息中。
ruckusACEventRogueAPTrap	网络上检测到可疑 AP。可疑 AP 的 MAC 地址和 SSID 包含在告警消息中。
ruckusACEventAPLostTrap	一个 AP 与 ZD1000/3000 的通信中断。该 AP 的 MAC 地址包含在告警消息中。
ruckusACEventAPLostHeartbeatTrap	一个 AP 的心跳中断。该 AP 的 MAC 地址包含在告警消息中。
ruckusACEventClientAuthFailBlockTrap	一个无线客户端向 AP 认证时多次失败。该客户端的 MAC 地址、AP 的 MAC 地址和 SSID 包含在告警消息中。

3 管理无线局域网

3.1 无线网络概述

ZD1000/3000 安装完成后，即可拥有功能完备的无线网络，该网络包括授权用户和来宾可访问的两个安全 WLAN（“内部”和“来宾”）。内部 WLAN 可为“标准”客户端设备（即运行 Windows XP/SP2 和使用现成 WPA NIC 的计算机）提供 Zero IT 连接。

除内部 WLAN 之外，以下两种情况需创建其他 WLAN：(1)将特定 WLAN 限制为仅供某些符合条件的用户组访问，以增强安全性，提高效率。例如，仅限少数用户访问的“工程”WLAN；(2)使用不同的安全设置配置特定 WLAN。例如，用户可能希望创建一个 WLAN，利用 WEP 加密技术对仅受其支持的无线手持设备进行加密。

第一种情况下，可以设置支持特定用户组的特定 WLAN（特别是与身份验证和加密算法有关）。这需要执行两步操作：(1)创建自定义 WLAN，然后按照“角色”将其链接到符合条件的用户帐户，(2)协助所有符合条件的用户准备客户端设备以进行自定义 WLAN 连接。

这样，用户将拥有默认的内部 WLAN，以及满足不同无线安全性要求所需的 WLAN。

3.2 自定义 WLAN 安全性

内部 WLAN 的默认安全环境是将基于 WPA 的身份验证密码和 TKIP 加密算法结合起来，并使用动态预共享密钥。要查看默认 WLAN 配置和可用选项，执行下列步骤。

3.2.1 查看初始安全配置

步骤 1　单击“监控”> **WLAN**。

步骤 2　当显示WLAN工作区时，WLAN表将列出在安装过程中创建的两个默认WLAN：corporate和guest。内部WLAN（corporate）是供授权用户使用的WLAN，可以单击该WLAN名称，查看其详细配置。参阅图 3-1。

步骤 3　对于内部WLAN，用户有三种选择：[1]继续使用当前配置；[2]优化基于WPA的现有模式；[3]用基于WEP的模式或802.1x模式完全替代此模式。在下列章节中，将分别说明两个WLAN的编辑过程。

图 3-1 监控> WLAN 页面

3.2.2 优化当前安全模式

步骤 1 在内部WLAN（corporate）行中，单击“编辑”（如果尚未执行此操作）。

步骤 2 选择表 3-1中的其中一个选项，在不中断用户连接的情况下增强默认的“Zero IT”保护。

表 3-1 安全选项

选项	说明
WPA2	如果用户倾向于使用 IEEE 802.11i 标准，可切换到此加密方法。
AES	要进行更严格的加密，可切换到此算法。
Passphrase（密码）	将当前密码替换为新密码。

步骤 3 单击“确定”应用所有更改。

3.2.3 切换到其他安全模式

用户也可以选择将内部 WLAN 的默认 WPA 模式替换为其他两个模式之一：

- 安全性保护较低的 WEP 密钥模式
- 安全性保护较高的 802.1x 模式

要将 WPA 配置替换为 802.1x，用户需更改优科连接配置，包括导入证书。

步骤 1 单击“配置”> **WLAN**。

步骤 2 当显示WLAN工作区时，需要查看并更改内部网络的安全性选项。要开始更改，在内部行中单击“编辑”。

步骤 3 当显示“编辑(corporate)”功能时，将显示两个主要类别 – Authentication Options（身份验证选项）和Encryption Options（加密选项）。

步骤 4 如果单击一个Authentication Option Method（身份验证选项方法）（如Open（开放）、Shared（共享）或802.1x），将显示不同的加密选项组（参阅表 3-2）。

表 3-2 身份验证选项

身份验证选项	说明
Open（开放）	可以配置基于 WPA 或基于 WEP 的加密，或者配置为 none（无）（如果确实希望如此）。选择 WPA 或 WEP 后，输入密码或密钥文本。
Shared（共享）	限制为只能使用 WEP 密钥加密。
802.1x EAP	可以从所有可用加密中进行选择，但是无需创建密钥或密码。
MAC Address（MAC 地址）	可以使用外部 RADIUS 服务器对无线客户端进行身份验证。要使用此选项，先将外部 RADIUS 服务器添加到 ZD1000/3000 的“配置”>“AAA 服务器”页面。用户还要规定允许在 RADIUS 服务器上使用的 MAC 地址。

步骤 5 根据所选择的Authentication Option Method（身份验证选项方法），检查并重新配置相关的Encryption Options（加密选项）。

步骤 6 查看Advanced Options（高级选项），根据需要更改设置。（例如，如果切换到 802.1x，用户需从菜单中选择一个身份验证服务器。）

步骤 7 完成后，单击“确定”应用所做的更改。

3.2.4 使用内置 EAP 服务器

（要求选择 Local Database（本地数据库）作为身份验证服务器。）要重新配置内部 WLAN 以使用 802.1x/EAP 身份验证，必须为无线用户生成并安装证书。借助内置 EAP 服务器和 Zero-IT 无线激活，可在最终用户的计算机上自动生成证书并安装它。用户只需依照 Zero-IT 无线激活时提供的指导进行操作即可。完成此任务后，用户就可以连接到使用 802.1x/EAP 身份验证的内部 WLAN。

3.2.5 使用外部 RADIUS 服务器进行身份验证

网络管理员可以使用外部 RADIUS 服务器对无线客户端进行 802.1x/EAP 身份验证。这种应用要求使用可识别 EAP 的 RADIUS 服务器。同时，可能需要管理员为无线客户端设备和所使用的 RADIUS 服务器部署自己的证书。这种情况下，在进行无线身份验证时，ZD1000/3000 将作为无线客户端和 RADIUS 服务器之间的桥梁。

仅当 RADIUS 服务器成功完成无线客户端的身份验证后，ZD1000/3000 才会允许无线客户端访问网络。

注意

如果无线网络使用 EAP/外部 RADIUS 服务器对客户端进行身份验证，并且用户使用的是 Windows Vista 客户端，确保已将其升级到 Vista Service Pack 1 (SP1)。SP1 中包含的修复程序可解决使用 EAP/外部 RADIUS 服务器时出现的客户端身份验证问题。

3.2.6 如果将内部 WLAN 更改为 WEP 或 802.1x

如果更改了内部 WLAN 的默认 WPA 配置，用户必须在其设备上重新配置无线 LAN 连接设置。此过程已有详细说明，在作为新用户登录到 WLAN 时可以执行此过程。

如果切换到基于 WEP 的安全性

步骤 1 每个用户都必须可以独立执行Zero-IT无线激活，并通过执行激活脚本安装WEP密钥。

步骤 2 此外，还必须可以将WEP密钥文本手动输入到无线设备连接设置。

如果切换到基于 802.1x 的安全性

步骤 1 （仅适用于使用内置EAP服务器的情况。）每个用户都必须可以独立执行Zero-IT无线激活，并下载ZD1000/3000生成的证书和激活脚本。

步骤 2 每个用户都必须先在自己的计算机上安装证书。

步骤 3 然后执行激活脚本，在计算机上配置正确的无线设置。

步骤 4 要手动配置802.1x/EAP设置以便供非Windows XP/SP2客户端使用，可使用ZD1000/3000生成的无线设置。

3.3 设置动态预共享密钥过期

网络管理员在启用 Dynamic PSK 的情况下首次激活对 WLAN 的访问权限时，将自动生成唯一的预共享密钥(PSK)以便进行身份验证。（默认情况下，将在 WLAN 安装向导中激活该访问权限。）

默认情况下，所有动态预共享密钥将在两个月后过期。管理员可以设置 PSK 何时过期、何时提示用户重新激活其无线访问权限。

设置 Dynamic PSK 过期

步骤 1　单击“配置”> **WLAN**。

步骤 2　在Dynamic PSK下的“PSK过期时间”中，选择希望Dynamic PSK过期的时间。表 3-3列出了可用的PSK过期时间选项。

表 3-3 PSK 过期时间选项

PSK 过期时间
无时间限制（PSK 永不过期）
一天
一周
两周
一个月
两个月
三个月
半年
一年
两年

步骤 3　单击“应用”保存设置。新设置将立即生效。

图 3-2 Dynamic PSK 选项

注意

如果更改 Dynamic PSK 过期时间，新的过期时间仅对新 PSK 有效。现有 PSK 的过期时间仍为自生成 PSK 起生效的过期时间。

3.4 配置访问控制列表

可以创建 L2/MAC 和 L3/L4 访问控制列表，确定允许哪些设备与接入点相关联。可以在“配置”>“访问控制”页面配置这些选项。

注意

除了每个 WLAN 的 ACL 外，还有适用于所有 WLAN 的系统级阻止列表。当管理员从“监控”/“当前活动的客户端”面板中选择阻止客户端时，将添加系统级阻止列表条目。管理员可以单击“配置”>“访问控制”>“阻止客户端”从系统级阻止列表中删除条目。如果某个 MAC 地址出现在系统级阻止列表中，那么即使其他 ACL 列表允许该地址，该地址仍会被阻止。

3.4.1 L2/MAC 访问控制

使用“访问控制”配置选项，可以定义第 2 层/MAC 地址 ACL，稍后可以将其应用到一个或多个 WLAN 中（创建或编辑 WLAN 时）。ACL 可以是 allow-only（仅允许）或 deny-only（仅拒绝），也就是说，可以将 ACL 设置为仅允许指定的客户端或仅拒绝指定的客户端。拒绝列表中的 MAC 地址在 AP 处而不是在 ZD1000/3000 处被阻止。

配置 L2/MAC ACL

步骤 1　单击“配置”>“访问控制”。

步骤 2　在L2/MAC访问控制中，单击“新建”。

步骤 3　配置表 3-4中列出的设置。

表 3-4 L2/MAC ACL 设置

设置	说明
名称	输入 ACL 的名称。
说明	输入 ACL 的说明。
限制	选择要使用的限制模式： • 仅允许以下列出的所有工作站 • 仅拒绝以下列出的所有工作站
MAC Address	在 MAC Address 文本框中输入 MAC 地址，然后单击“新建”保存该地址。添加的新 MAC 地址将显示在“工作站”字段旁边。最多可以输入 128 个 MAC 地址。

步骤 4　单击“确定”保存基于L2/MAC的ACL。

最多可以创建 32 条 L2/MAC ACL 规则，每条规则最多包含 128 个 MAC 地址。

图 3-3 配置 L2/MAC 访问控制列表

3.4.2 L3/L4 访问控制

除了基于 L2/MAC 的 ACL 外，ZD1000/3000 还在第 3 层和第 4 层提供访问控制选项。这意味着可以基于一组标准配置访问控制选项，包括：

- 目标地址
- 应用
- 协议
- 目标端口

创建基于 L3/L4/IP 地址的 ACL

步骤 1 单击“配置”>“访问控制”。

步骤 2 在“L3/4/IP地址访问控制”中，单击“新建”。

步骤 3 配置表 3-4中列出的设置。

表 3-5 基于 L3/L4/IP 地址的 ACL 设置

设置	说明
名称	输入 ACL 的名称。
说明	输入 ACL 的说明。
默认模式	设置默认情况下要向所有用户授予的默认访问特权（允许所有用户或拒绝所有用户）。
规则	单击“新建”或编辑现有规则。通过配置下列选项的组合，定义访问策略： • 类型：此策略授予的访问特权（允许或拒绝）。 • 目标地址：要允许或拒绝访问某个特定的 IP 地址、主机名或 URL，在此处输入。否则，选择 Any（所有）。 • 应用：要允许或拒绝访问某个特定的应用程序，从菜单中选择该应用程序。否则，选择 Any（所有）。如果在此处选择了除 Any（所有）以外的某个选项，将禁用“协议”和“目标端口”选项。 • 协议：要允许或拒绝某个网络协议，从菜单中选择该协议。否则，单击 **Any**（所有）。 • 目标端口：要允许或拒绝访问某个特定的目标端口，从菜单中选择该端口。否则，选择 Any（所有）。

步骤 4 单击“确定”保存ACL。

要创建基于 L3/L4/IP 地址的其他访问规则，重复上述步骤。最多可以创建 32 条基于 L3/L4/IP 地址的访问规则。

图 3-4 配置 L3/L4 访问控制列表

3.5 使用 WLAN

有时可能需要创建其他 WLAN。例如，可能希望为仅限 WEP 的客户端设备创建 WLAN。也可能希望创建使用 802.1x/EAP 和证书的 WLAN。以下章节将介绍如何创建使用不同安全设置的 WLAN。

3.5.1 创建 WLAN

步骤 1 单击“配置”> **WLAN**。

步骤 2 单击“新建”。

图 3-5 用于添加 WLAN 的“新建”表

“新建”工作区显示的选项如下所述。

常规选项

表 3-6 常规选项

选项	说明
名称/ESSID	输入此 WLAN 的简短名称（2 至 31 个字符/数字）。
说明	输入对此 WLAN 限定条件/用途的简短说明，如“工程”或“语音”。

身份验证方法选项

表 3-7 身份验证方法选项

选项	说明
Open（开放）	（默认）没有用于连接的身份验证机制。如果使用 WPA 或 WPA2 加密，这表示 WPA-PSK 身份验证。
Shared（共享）	如果单击 **Shared**（共享），则只有 WEP 加密可用，并出现 WEP Key（WEP 密钥）选项。使用共享 WEP 密钥进行身份验证。要求创建 WEP 密钥，具体方法如下所述。
802.1x EAP	使用 802.1x 身份验证机制。要求使用证书。

加密选项

方法

表 3-8 加密选项 – 方法

选项	说明
None（无）	（默认）未应用任何加密；通信以明文形式进行。
WPA/WPA2	（不适用于共享身份验证）提供更高级别的加密且更安全。WPA 和 WPA2 要求选择一种加密算法（具体如下所述）。
WEP-64	使用 64 位 WEP 加密，提供较低级别的加密，安全性较低。
WEP-128	使用 WEP 加密的 128 位密钥，提供较高级别的加密。

注意

如果将加密方法设置为 WEP-64（40 位）或 WEP-128（104 位），并且 WLAN 使用 802.11n AP，则 AP 将在 802.11g 模式下运行。

算法（仅适用于 WPA 或 WPA2 加密方法）

表 3-9 加密选项 – 算法

选项	说明
TKIP	（默认）此算法有效。由于某些客户端设备不支持 AES，已将它设置为默认项。
AES	此算法提供高度安全性。
WEP Key（WEP 密钥）	仅适用于 WEP 方法。在十六进制字段中单击并输入所需的密钥文本。如果此密钥用于 WEP 64 加密，则密钥文本的长度必须为 10 个字符。如果用于 WEP 128 加密，则输入长度为 26 个字符的密钥。
Passphrase（密码）	仅适用于 WPA/WPA2 PSK 方法。在此字段中单击并输入用于身份验证的密码。

注意

如果将加密算法设置为 TKIP，并且 WLAN 使用 802.11n AP，则 AP 将在 802.11g 模式下运行。

注意

如果将加密算法设置为 TKIP，则 AP 最多可以支持 25 个客户端。达到此限制后，其他客户端将无法与 AP 关联。另一方面，如果禁用加密或选择 AES，则 AP 最多可以支持 100 个客户端。如果还启用了无线网格技术，则 AP 支持的客户端将不足 100 个。

选项

表 3-10 选项

选项	说明
Guest Usage（来宾访问）	如果创建的WLAN用于来宾访问，则选中“此WLAN用于来宾访问”复选框。选中该复选框后，“无线客户端隔离”选项将自动被选中且无法取消选中。 来宾 WLAN 受来宾访问策略限制，如重定向和子网访问限制。
Web Authentication（Web 身份验证）	（仅可以用于 Open（开放）或 Shared（共享）身份验证。）单击该复选框可要求所有 WLAN 用户在每次尝试连接时都基于 Web 登录到此网络。
Authentication Server（身份验证服务器）	进行 Web Authentication（Web 身份验证）时，使用此选项可指定用于验证基于 Web 的用户登录的服务器。进行 802.1x 身份验证时，使用此选项可将“本地数据库”或配置好的 RADTUS 服务器指定为身份验证源。
Wireless Client Isolation（无线客户端隔离）	无线客户端隔离对来宾进行子网限制。如果 WLAN 的无线客户端隔离已启用，与此 WLAN 关联的所有工作站都将无法访问本地 LAN，只能访问 Internet。同样，与此 WLAN 关联的工作站无论与哪个 AP 关联，它们彼此之间都无法进行通信。工作站的行为将和与来宾 WLAN 关联的工作站完全相同。启用无线客户端隔离的 WLAN 和来宾 WLAN 之间的唯一区别在于，来宾 WLAN 要求用户必须输入来宾通行证才能访问网络。来宾 WLAN 和启用无线客户端隔离的 WLAN 采用的来宾策略相同。
Zero IT Activation（Zero IT 激活）	将此选项保持活动状态（默认设置），因为它将在自动“新建用户”过程中激活优科 ZD1000/3000 共享，迅速有效地配置新用户的 PC 供 WLAN 使用。

注意

如果启用了 Guest Usage（来宾访问）或 Wireless Client Isolation（无线客户端隔离）（如下所述），SpeedFlex 无线性能工具可能无法正常工作。例如，用户可能无法通过 http://{ZD1000/3000-ip-address}/perf 网址访问 SpeedFlex，或 SpeedFlex 提示需在目标客户端上安装 SpeedFlex 应用程序，即使该客户端已经安装了该程序。

使用 SpeedFlex 之前，验证 Guest Usage（来宾访问）和 Wireless Client Isolation（无线客户端隔离）选项是否已禁用。

有关详细信息，参考8-3页中的“使用 SpeedFlex 测量无线网络吞吐量”使用 SpeedFlex 测量无线网络吞吐量使用 SpeedFlex 测量无线网络吞吐量。

注意

要使“Zero IT 配置”适用于 HP iPAQ，必须安装 Internet Explorer Mobile 7.6（或更高版本）。如果 HP iPAQ 用户使用 Internet Explorer Mobile 的早期版本，优科强烈建议升级到最新版本再连接到无线网络。

高级选项

参阅步骤 3。

表 3-11 高级选项

选项	说明
Access Controls（访问控制）	打开此下拉列表，选择用于此 WLAN 的 ACL。必须先创建 ACL，然后才可在此处使用。参阅3-7页中的“配置访问控制列表”。
Rate Limiting（速率限制）	速率限制保证对网络的公平访问。如果启用了该选项，各个网络设备（即客户端）的网络流量吞吐量将受流量策略中规定的速率限制，并且可以将该策略应用到上行链路或下行链路。 打开“上行链路”和/或“下行链路”下拉列表，限制 WLAN 客户端上传/下载数据的速率。 Disabled（禁用）表示禁用速率限制，即没有流量限制。
VLAN	选中“附加 VLAN 标记”复选框，激活 VLAN 功能，然后输入已分配给无线网络的用户/客户端的相关 VLAN ID。（ID 应为 1 至 4094。）

选项	说明
Hide SSID（隐藏 SSID）	如果不希望广播此WLAN的SSID，可激活此选项。这不会影响性能，也不会强制 WLAN 用户执行任何不必要的任务。
Tunnel Mode（隧道模式）	如果希望将WLAN流量通过ZD1000/3000集中转发，选中此复选框。通过隧道模式，无线客户端可以在不同子网中的不同AP之间漫游而不中断。如果WLAN中的客户端（如VoIP设备和PDA）要求跨子网的无线连接不能中断，优科建议启用隧道模式。

步骤 3 完成后，单击“确定”保存这些条目。此WLAN现可供使用。

步骤 4 现在，为用户分配角色时可从这些WLAN中选择，详情参阅5-3页中的“新建用户角色”。

3.5.2 配置客户端身份验证

如果用户使用的是运行 Windows XP SP2/Vista 的计算机，操作系统将自动配置无线网卡以适应 ZD1000/3000 上的 WLAN 安全设置。如果用户连接的是运行 Windows、Mac OS X、Linux 或其他操作系统早期版本的计算机，则不会为用户提供激活脚本；而是为用户提供一个详细的页面，其中包含所有必需的无线设置。用户必须根据这些设置手动配置计算机。下表记录了详细信息。

表 3-12 客户端身份验证选项

身份验证选项	加密选项	客户端配置
Open（开放）	WPA WPA-2 WEP-64 WEP-128	用户必须执行以下操作之一：(1)在无线网络配置中手动输入相同的 WEP 密钥；(2)手动输入 WPA 密码。
Shared（共享）	WEP-64 WEP-128	用户必须手动输入存储在无线网络配置中 ZD1000/3000 中的 WEP 密钥文本。
802.1x	WEP-64 WEP-128 WPA/WPA2	用户必须获取生成的证书，并安装在计算机上。无需输入任何密钥或密码。

3.5.3 新建 WLAN 供工作组使用

如果希望基于现有的内部 WLAN 再创建一个 WLAN，并将其限制为仅供选定的用户组（例如，营销人员或工程设计人员）使用，可以执行下列步骤：

步骤 1 创建用户组列表（使用运行Windows XP/SP2的客户端设备的理想用户）。

步骤 2 单击“监控”> **WLAN**。

出现 WLAN 页面时，将在表中列出默认的 corporate 和 guest 网络（创建 WLAN 后，它也将在此表中显示）。

步骤 3 如果不需要对此新WLAN自定义身份验证或加密方法，查找corporate WLAN记录，然后单击“克隆”。

将出现一个工作区，显示新 WLAN 的默认设置，它使用的 zero-IT 配置设置与“Corporate”相同。

步骤 4 为此WLAN输入一个描述性名称，然后单击“确定”。新WLAN现可供选定的用户使用。

现在可以将此新 WLAN 的访问权限分配给一组有限的 corporate 用户，具体操作方法如5-3页中的“新建用户角色”中所述。

3.5.4 将新接入点添加到 WLAN

如果员工需求或无线覆盖范围需求增加，可以快速轻松地将 AP 添加到网络中。根据网络安全首选项，可以自动检测和激活新 AP，或者在激活之前，新 AP 可能要求手动审批每台设备。

默认情况下，Auto-JOIN（自动加入）自动 AP 激活过程处于活动状态。如有必要，可以禁用 Auto-JOIN（自动加入）。如果选择禁用该选项，ZD1000/3000 将检测新 AP，报告它们的状态，然后等待手动“审批”激活它们，如本指南中所述。

注意

要使 Auto-JOIN（自动加入）起作用，添加的 AP 必须与 ZD1000/3000 处于相同的 IP 子网或 VLAN 中。

将 AP 连接到 WLAN

步骤 1 将新的AP放在适当位置。

步骤 2 写下MAC地址（在每台设备的底部）并在分配AP时注明每个AP的特定位置。

步骤 3 使用以太网电缆将AP连接到LAN。

步骤 4 将每个AP连接到电源。

注意

如果使用的优科AP可以通过以太网供电，当电源不方便获得时，可以将AP连接到支持太网供电的集线器或交换机，它们将通过以太网电缆获得电源。

验证/审批新 AP

步骤 1 单击“监控”>“接入点”。“接入点”页面将出现，显示已经审批或等待审批的前15个接入点。如果ZD1000/3000管理的接入点超过15个，则页面底部将出现“显示详细信息”按钮。要显示列表中的其他接入点，单击“显示详细信息”。当所有接入点都显示在该页面上后，“显示详细信息”按钮将消失。

步骤 2　查看“当前管理的接入点”表。参阅图 3-6。

- 单击“配置”>“接入点”>“接入点策略”>“审批”复选框，所有新 AP 都将列在该表中，且“状态”为“已连接”。
- 如果禁用 Auto-JOIN（自动加入），将列出所有新 AP，但是它们的状态将为 Approval Pending（待审批）。

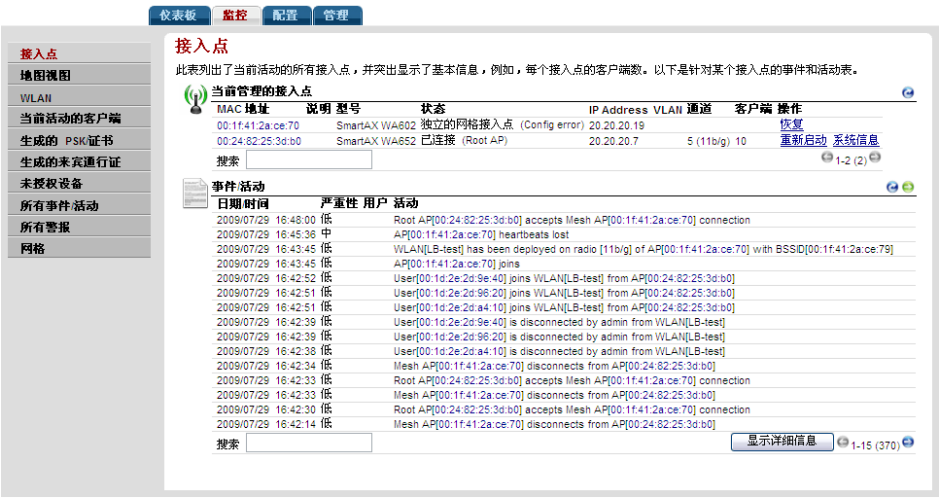
步骤 3　在“操作”列下，单击“允许”。当状态从“断开连接”更改为“已连接”后，将激活新AP供用户使用。

步骤 4　单击“应用”保存设置。

注意

使用“地图视图”（在“监控”选项卡上）放置最近审批的所有 AP 的标记图标。有关详细信息，参阅4-13页中的“估计并扩大网络覆盖范围”。

图 3-6 监控 > 接入点页面



3.6 查看当前接入点策略

“接入点策略”选项包括如何检测和审批用于 WLAN 覆盖范围的新 AP。要查看并修订常规接入点策略，执行下列步骤：

步骤 1 单击“配置”>“接入点”。

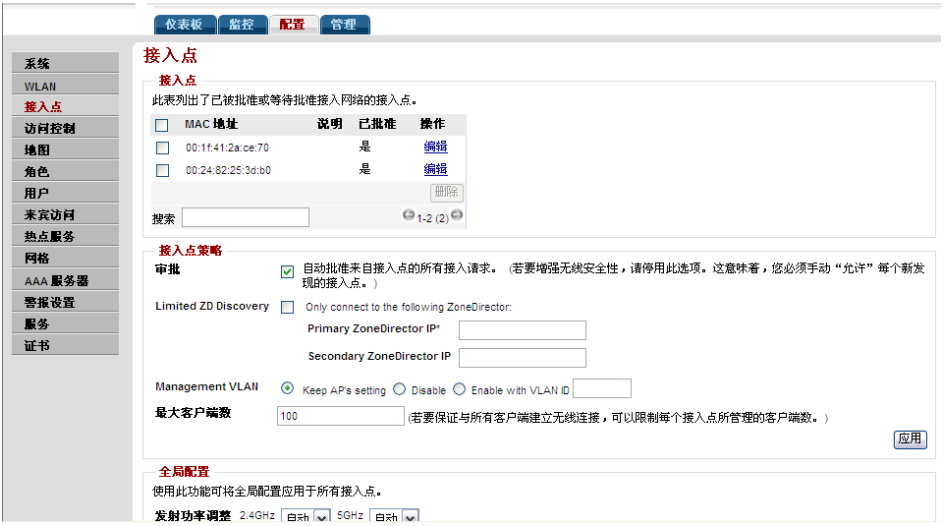
步骤 2 查看“接入点策略”中的当前设置。可以更改表 3-13中列出的设置。

表 3-13 接入点策略

策略	说明
审批	根据用户喜好，如果希望手动查看并审批将新 AP 添加到 WLAN 的过程，可以禁用此选项。

步骤 3 单击“应用”保存设置。这仅会影响到新的/未经审批的AP。

图 3-7 配置 > 接入点页面



3.7 编辑接入点参数

通过编辑 AP 参数，用户可以添加说明，更改通道化、通道，或者传输托管接入点的电源设置。

编辑接入点参数

步骤 1　单击“配置”>“接入点”。

步骤 2　查找要在“接入点”表中进行编辑的AP，然后在“操作”列下单击“编辑”。

步骤 3　编辑表 3-14中列出的任何设置。

表 3-14 接入点设置

设置	说明
说明	输入 AP 的说明，如位置。
通道化	（仅适用于 802.11n）“通道宽度”确定传输期间频谱的使用方式。
通道	这是 AP 网络使用的通道。
发射功率	指定与标定功率相对的最大发射功率电平。

步骤 4　如果AP当前已连接到ZD1000/3000，将出现“管理IP”选项（如表 3-15中所述）。使用这些选项配置AP的IP设置。

表 3-15 “管理 IP”选项

设置	说明
保留接入点设置	如果希望 AP 保留当前 IP 地址，单击“保留接入点设置”。如果尚未设置 AP 的 IP 地址，它将自动尝试通过 DHCP 获取 IP 地址。
DHCP	如果希望 AP 自动从网络上的 DHCP 服务器获取 IP 地址设置，可单击 By-DHCP（通过 DHCP）中的 DHCP 选项。不需要配置其他设置（子网掩码、网关和 DNS 服务器）。
手动	如果希望为 AP 分配静态 IP 地址，单击 **By-DHCP**（通过 DHCP）中的“手动”选项，然后设置下列选项的值： • IP Adrress（IP 地址）：输入要手动分配给 AP 的 IP 地址。 • Netmask（子网掩码）：输入已分配给 AP 的 IP 地址的子网掩码。 • Gateway（网关）：输入 AP 进行连接所用的网关设备的 IP 地址。 • Primary DNS Server（首选 DNS 服务器）：输入希望 AP 使用的网络上的首选 DNS 服务器。 • Secondary DNS Server（备用 DNS 服务器）：（可选）输入希望 AP 使用的网络上的备用 DNS 服务器。

步骤 5 在“高级选项”>“上行链路选择”中，选择“手动”单选按钮。网格中的其他AP将出现在该选项中。

步骤 6 选中可以作为上行链路的当前AP对应的复选框。

注意

如果将 AP 的“上行链路选择”设置为“手动”，但是选定的上行链路 AP 已关闭或不可用，则“监控”>“接入点”页面上的 AP 状态将显示为 Isolated Mesh AP（孤立网格 AP）。

步骤 7　单击“确定”保存设置。

图 3-8 “上行链路选择”选项

3.8 在 VLAN 环境中部署 ZD1000/3000 WLAN

可以将 ZD1000/3000 无线 LAN 部署到支持 VLAN 网络中，ZD1000/3000 和 AP 之间的管理流量选择带或不带 VLAN 标记。如果选择不带 VLAN 标记，那么 VLAN 交换机的配置需要符合特定的条件：

- 检验VLAN交换机是否支持端口私有 VLAN(PVLAN)。私有 VLAN(PVLAN) 将该端口输出/输入的普通以太网帧指定到该私有 VLAN(PVLAN)。

例如，如果 802.1Q 端口分配有 VLAN 2、3 和 4，且 VLAN 2 是该端口的私有 VLAN(PVLAN)，则输出该端口 VLAN 2 的帧的 802.1Q 标记被删除（即是普通以太网帧）。将输入此端口的普通以太网帧插入 VLAN 2 的 802.1Q 标记。而与 VLAN 3 和 4 相关的流量直接转发。

- 将ZD1000/3000和任何接入点(AP)连接到VLAN交换机的中继端口。
- 检验这些交换机端口是否具有相同的私有 VLAN(PVLAN)。

注意

通过管理 VLAN，未经身份验证的无线客户端中的 HTTP 流量都将从 AP 传递到 ZD1000/3000 上。如果该客户端属于特定 VLAN，则在将流量传递到相应有线网络之前，ZD1000/3000 将添加相应的 VLAN 标记。执行客户端身份验证后，客户端流量将可以直接从 AP 转到有线网络，这将添加相应的 VLAN 标记。

配置示例（图 3-9）：VLAN ID 55 用于管理，wlan1 带有 VLAN ID 10 标记。

图 3-9 VLAN 配置示例

ZD1000/3000 和 AP 之间的管理流量要求带 VLAN 标记,即管理 VLAN。那么假如 ZD1000/3000 和 AP 都处于同一交换机或二层网络上，ZD1000/3000 和 AP 都需要连接到交换机的支持该管理 VLAN 的中继端口上。如下图，VLAN ID 55 用于管理，AP 和 ZD1000/3000 之间管理流量传输。wlan1 使用 VLAN ID 10 标记，传输应用业务流量。

ZD1000/3000 需要经过适当配置后才能支持管理 VLAN，具体配置步骤如下（配置 ZD1000/3000 支持 VLAN ID 55 的管理 VLAN）：

步骤 1 转至“配置”>“系统”。

步骤 2 向下滚动到“管理VLAN（Management VLAN）”。

步骤 3 在“ZoneDirector的管理VLAN”部分，输入管理VLAN ID（如55）。

步骤 4 单击**Apply**（应用）保存设置。更改立即生效。

注意

如果你当前是通过PC或服务器直接与ZoneDirector的以太网端口连接进行配置，那么配置了管理 VLAN 并且生效后，由于一般 PC 或服务器均不支持带 VLAN 标记的以太网帧，所以对ZoneDirector的管理连接将中断。必须将PC或服务器连接到交换机上的一个已经配置了与管理 VLAN 相同 VLAN ID 的接入端口，才能继续访问和管理 ZoneDirector1000/3000。

图 3-10 配置 ZD1000/3000 支持 VLAN ID 55 的管理 VLAN

同样 AP 也需要进行相应的配置以支持管理 VLAN。根据 AP 所处位置的不同，AP 的管理 VLAN 可以和 ZD1000/3000 的相同（AP 和 ZD1000/3000 之间是二层网络），也可以不同（AP 和 ZD1000/3000 之间是三层网络）。配置步骤如下：

步骤 1 转至“配置”>“接入点”。

步骤 2 向下滚动到“管理VLAN(Management VLAN)”。

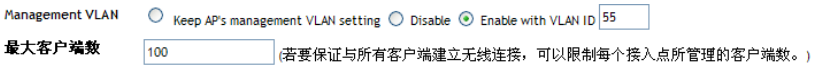
步骤 3 根据实际应用场景，配置下表相关设置。

表 3-16 AP 管理 VLAN 设置

设置	描述
保留 AP 管理 VLAN 设置（Keep AP's Management VLAN Setting）	保留 AP 关于管理 VLAN 的现有设置。如果 AP 在被 ZD1000/3000 管理之前已经设置了管理 VLAN，那么保留其设置不变。如 AP 和 ZD1000/3000 之间是三层网络时，AP 的管理 VLAN 可能是任意一个 VLAN
关闭管理 VLAN（Disable）	AP 的管理流量将以普通以太网帧进行传输。如 AP 接在交换机的接入(ACCESS)端口时。
设置管理 VLAN ID（Enable with VLAN ID）	将 AP 的管理 VLAN 设置为指定值。如下面的配置将 AP 的管理 VLAN 配置为 55

步骤 4 单击Apply（应用）保存设置。更改立即生效。

图 3-11 “管理 VLAN（Management VLAN）”部分



3.9 使用 WLAN 组

如果无线网络覆盖大型物理环境（例如，多层或综合办公楼），并且需要为不同的环境区域提供不同的 WLAN 服务，可以通过 WLAN 组来实现。例如，如果无线网络覆盖三个楼层（第 1 层到第 3 层）并且需要为第 1 层的访客提供无线访问，可以执行下列操作：

步骤 1 创建仅提供来宾级访问权限的WLAN服务（例如，Guest Only Service（仅来宾服务））。

步骤 2 创建WLAN组（例如，Guest Only Group（仅来宾组）），然后将Guest Only Service（仅来宾服务）（WLAN服务）分配给Guest Only Group（仅来宾组）（WLAN组）。

步骤 3 将第1层（该层的访客需要无线访问权限）的AP分配给Guest Only Group（仅来宾组）。

任何与分配给 Guest Only Group（仅来宾组）的 AP 关联的无线客户端都将获得在 Guest Only Service（仅来宾服务）中定义的来宾访问特权。第 2 层和第 3 层上的 AP 可以继续分配给默认 WLAN 组并提供正常访问权限。

注意

创建 WLAN 组是可选的。如果不需要为环境中的不同区域提供不同的 WLAN 服务，就不需要创建 WLAN 组。

注意

有一个名为 **Default** 的默认 WLAN 组。所创建的前八个 WLAN 会自动分配给该默认 WLAN 组。

注意

单个 WLAN 组只可分配给 AP 上的一个无线接收器，并且最多拥有八个成员 WLAN。如果其中启用了网格技术，WLAN 组最多只能拥有六个成员 WLAN。

3.9.1 创建 WLAN 组

步骤 1　单击“配置”> **WLAN**。

步骤 2　在“WLAN组”部分，单击“新建”。将显示“新建”表。

步骤 3　配置表 3-17中列出的设置。

表 3-17 新建 WLAN 组设置

设置	说明
名称	输入该 WLAN 组的描述性名称。例如，如果此 WLAN 将包含给来宾用户指定的 WLAN，可以将其命名为来宾 WLAN 组。
说明	（可选）输入关于此组的备注或注释。
成员 WLAN	选中希望作为该 WLAN 组成员的 WLAN 对应的复选框。

步骤 4　如果网络上有现成的VLAN并且需要标记来自成员WLAN的流量，选中**Enable VLAN override**（启用VLAN覆盖）复选框，然后为每个成员WLAN配置VLAN覆盖设置。表 3-18列出了可用的VLAN覆盖设置。

表 3-18 VLAN 覆盖设置

设置	说明
No Change（无更改）	如果希望 WLAN 保留相同 VLAN 标记（如果创建 WLAN 服务时配置了 Attach VLAN Tag（附加 VLAN 标记）选项），单击此选项。
Untag（取消标记）	如果特定 WLAN 连接到不包含任何 VLAN 的本地网络，单击此选项。
Tag（标记）	如果需要标记来自特定 WLAN 的流量以使其与 VLAN 成功绑定，单击此选项。

注意

在隧道模式下无法标记 WLAN。

步骤 5 单击“确定”。“新建”表消失，并且将在“WLAN组”下方的表中显示用户创建的WLAN组。

可以立即将此 WLAN 组分配给 AP。

3.9.2 将 WLAN 组分配给 AP

步骤 1 单击“配置”>“接入点”。

步骤 2 在接入点列表中，找到要分配给WLAN组的AP的MAC地址，然后单击“编辑”。

步骤 3 在“WLAN组”中，选择要向其分配AP的WLAN组。一个AP只能分配给一个WLAN组。

步骤 4 单击“确定”保存所做的更改。

3.9.3 查看属于 WLAN 组的 AP 列表

步骤 1 单击“监控”> **WLAN**。

步骤 2 在Currently Active WLAN Groups（当前活动的WLAN组）下，单击要查看其成员AP列表的WLAN组名称。

步骤 3 在加载的页面上，查找“成员AP”部分。将列出属于此WLAN组的所有AP。

3.10 编辑 WLAN 组

可以随时更改现有 WLAN 组的设置。

步骤 1　单击“配置”> **WLAN**。

步骤 2　在“WLAN组”部分，单击要编辑的WLAN组所在行中的“编辑”链接。将出现“编辑(WLAN_group_name)”表。

步骤 3　根据需要编辑设置。可以编辑“名称”、“说明”描述、“成员WLAN”和VLAN覆盖设置。

步骤 4　单击“确定”保存所做的更改。

3.11 阻止客户端设备

用户登录 ZD1000/3000 网络时，将记录并跟踪其客户端设备（例如，便携式计算机和 PC）。如果出于某种原因，需要阻止客户端使用网络，可以在 Web 界面执行。下文介绍了用户监控、阻止和跟踪客户端设备时需执行的所有任务。

3.11.1 监控客户端设备

步骤 1　转至“仪表板”（如果尚未显示）。

步骤 2　在“设备概述”下，查看“客户端设备数”。

图 3-12　“设备概述”小组件

步骤 3　单击当前数字，该数字同时也是一个链接。此时将显示“当前活动的客户端”页面（位于“监控”选项卡上），显示当前连接到ZD1000/3000的前15个客户端。如果当前活动的客户端多于15个，该页面底部将出现“显示详细信息”按钮。要在列表中显示更多客户端，单击“显示详细信息”。所有活动的客户端都显示在该页面上后，“显示详细信息”按钮将消失。

步骤 4　“监控”选项卡中出现“当前活动的客户端”页面时，查看“客户端”表。

要阻止列出的任意客户端设备，执行下列步骤。

3.11.2 临时断开特定客户端设备的连接

按照以下步骤操作可以临时断开客户端设备与 WLAN 的连接。（如果需要，可以手动重新连接。）这有助于解决网络连接问题。

步骤 1 查看“状态”列以确定所有“未授权”的用户。

步骤 2 在特定用户行的“操作”列中单击“删除”按钮。

将从 Active/Current Client（活动/当前客户端）列表中删除相应条目，列出的设备会断开与优科 WLAN 的连接。

注意

如果事实证明这样做会产生问题，用户可以随时重新连接，系统可能会提示用户考虑以下客户端选项。

3.11.3 永久阻止特定客户端设备

按照以下步骤操作可以永久阻止客户端设备与 WLAN 的连接。

步骤 1　查看“状态”列以确定所有未授权的用户。

步骤 2　在特定用户行的“操作”列中单击“阻止”按钮。

状态将更改为“已阻止”。这将阻止列出的设备（及其用户）使用优科 WLAN。

3.11.4 查看先前被阻止的客户端列表

步骤 1　单击“配置”>“访问控制”。

步骤 2　查看“被阻止的客户端”表。

步骤 3　单击与列出的任意MAC地址对应的“取消阻止”按钮，可以取消阻止该MAC地址。

3.12 优化接入点性能

通过 ZD1000/3000 的 Web 界面，可以远程监控和调整每个网络 AP 上的关键硬件设置。评估网络性能中的 AP 性能后，可以根据需要重置通道并调整发射功率。

3.12.1 使用地图视图评估当前性能

要求：4-2页中的“导入地图视图的平面布置图”和4-3页中的“放置 AP 到相应位置”中详细介绍了平面布置图导入和 AP 布局。

步骤 1　单击“监控”>“地图视图”。

如果“地图视图”显示带有活动设备符号的平面布置图，可以从覆盖范围角度评估各 AP 的性能。（有关“地图视图”的详细信息，参阅4-4页中的使用“地图视图”工具。）

步骤 2　在“覆盖范围”选项中，单击“是”。

步骤 3　出现“热图”时，在地图右上角查看Signal%（信号百分比）比例。

步骤 4　注意整体颜色范围，尤其是表示小覆盖范围的颜色。

步骤 5　查看平面布置图并评估当前覆盖范围。可以根据下列详细说明进行调整。

3.12.2 扩大 AP RF 覆盖范围

步骤 1 单击各AP标记并将其拖到“地图视图”平面布置图中的新位置，直到达到最佳RF覆盖范围。可能需要其他AP来填补较大覆盖范围的空白。

步骤 2 完成调整后，记下重定位AP标记的新位置。

步骤 3 根据地图视图布局从物理位置上重定位实际AP后，断开AP的电源连接，然后重新连接。

步骤 4 要刷新“地图视图”，运行完整系统RF扫描，有关详细信息，参阅8-9页中的“启动射频扫描”。

步骤 5 完成RF扫描且ZD1000/3000重新校准地图视图后，用户可以评估更改，并根据需要进一步调整。

3.12.3 使用“接入点”表评估当前性能

步骤 1 单击“监控”>“接入点”。

步骤 2 出现“接入点”页面时，查看“当前活动的AP”的特定设置，尤其是“通道”和“客户端”列。

步骤 3 如果用户想要更改各个AP设置，继续执行下一任务。

3.12.4 调整 AP 设置

步骤 1 单击“配置”>“接入点”。

步骤 2 查看“接入点”表并确定要调整的AP。

步骤 3 单击该AP行中的“编辑”按钮。

步骤 4 查看并调整表 3-19中列出的任意“编辑(AP)”设置。

注意

根据审批状态，某些设置为只读。

表 3-19 编辑(AP)设置

设置	说明
MAC 地址	MAC 地址从 AP 获得。无法在 ZD1000/3000 中修改。

说明	输入此设备及其当前位置的简短说明。
无线电 B/G 通道	从此下拉列表中选择 802.11b/g 设备使用的特定通道。
发射功率	选择分配给该通道的发射功率。默认设置是“自动”，选项范围从“完整”到“最小”。

步骤 5　单击“确定”。将自动重新启动已调整的AP，此AP处于活动状态时可用于网络连接。

3.13 使用热点服务

热点是向具有无线网络功能的设备（例如，便携式计算机、PDA 和其他便携式设备）提供无线 Internet 访问的地点或区域。热点通常用于公共场所，例如，旅馆、机场、饭店和大型购物中心。

ZD1000/3000 具有内置热点功能，用户可以启用并配置这一功能并通过 WLAN 实现热点服务。除 ZD1000/3000 和它管理的 AP 外，部署热点时还需要：

- 强制网络门户：一个特殊的 Web 页面（通常是登录页），与热点相关联的用户通常被重定向到该网页进行身份验证。用户必须先输入有效的用户名和密码，才能通过热点访问 Internet。开源强制网络门户包（例如 Chillispot）可在 Internet 上获得。要获取开源和商用强制网络门户软件的列表，访问 http://en.wikipedia.org/wiki/Captive_portal#Software_Captive_Portals。
- RADIUS 服务器：用户可以通过远程身份验证拨号用户服务(RADIUS)进行身份验证。

有关强制网络门户和 RADIUS 服务器软件的安装和配置说明，参阅随附的文档。

3.13.1 创建热点服务

创建热点服务配置，用户可以将配置部署到希望其提供热点服务的 WLAN 上。完成下面的步骤后，用户需要设置希望其提供热点服务的 WLAN。

创建热点服务

步骤 1　单击“配置”>“热点服务”。

步骤 2 单击“新建”。将显示“新建”表。

步骤 3 在“登录页”（位于“重定向”下）中，输入强制网络门户（热点用户可以登录以访问服务的页面）的URL。

步骤 4 根据需要配置表 3-20中列出的可选设置。

表 3-20 可选热点设置

设置	说明
Start Page（起始页）	配置用户成功登录后将被重定向的位置。用户可以重定向到要访问的页面，或者设置其他页面（用户将被重定向到该页面），例如公司的网站。
Session Timeout（会话超时）	选中该复选框，然后设置一个最长的会话时间（以分钟为单位），超过该时间后会话将自动重新启动。
Idle Timeout（空闲超时）	选中该复选框，然后设置一个最长的空闲时间（以分钟为单位），超过该时间后空闲用户将被自动注销。
Authentication Server（身份验证服务器）	选择要用来对用户进行身份验证的 AAA 服务器。
Accounting Server（计费服务器）	如果已安装计费服务器，配置要检索计费数据的频率（以分钟为单位）。
Walled Garden（围墙花园）	输入用户无需经过身份验证即可访问的网络目标位置（URL 或 IP 地址）。
Restricted Subnet（受限制的子网）	输入阻止热点用户访问的子网。

步骤 5 单击“确定”。

将刷新页面并在列表中显示创建的热点服务。现在，可以分配要提供热点服务的WLAN。

3.13.2 分配 WLAN 以提供热点服务

配置热点服务后，用户需要指定要部署热点配置的 WLAN。要将现有 WLAN 配置为提供热点服务，执行以下操作：

步骤 1　单击“配置”> **WLAN**。

步骤 2　在WLAN部分，查找要分配作为热点WLAN的WLAN，然后在同一行单击“编辑”链接。将显示“编辑（WLAN名称）”表。

步骤 3　配置表 3-21中列出的设置。

表 3-21 热点服务设置

设置	说明
类型	单击 **Hotspot Service (WISPr)**（热点服务(WISPr)）。
可用热点服务	选择先前创建的热点服务的名称。

步骤 4　单击“确定”保存所做的更改。

4 监控无线网络

4.1 查看 ZD1000/ZD3000 监控选项

表 4-1列出了包含监控选项的主要选项卡及其用途。

表 4-1 ZD1000/3000 界面上的主要监控选项卡

选项卡	说明
仪表板	每次通过Web界面登录到ZD1000/3000后，将显示所有状态。该仪表板可用作网络监控的起点。数据用蓝色的链接表示，通过链接可以进一步了解具体的活动或设备。
监控	通过“地图视图”可快速扫描主要网络因素：AP（合法、相邻以及未授权）、客户端设备和射频(RF)覆盖范围。用户可以通过平面布置图查看设备的位置，大致估计一下网络覆盖范围。 通过左列按钮中的其他监控选项卡选项，可以查看WLAN性能和单独设备活动的相关数据。与“仪表板”一样，链接到某些数据条目可以获得更多信息。所有事件日志将按时间顺序显示用户、设备和网络的最新操作。
配置	使用此选项卡中的选项可以评估WLAN用户当前的状态、任何受限制的WLAN以及来宾访问设置和用户角色等。 管理员还可以结合使用此选项卡中的选项与“管理”选项卡中的选项，执行系统诊断和其他预防性任务。

4.2 导入地图视图的平面布置图

打开“监控”选项卡的“地图视图”后，如果 ZD1000/3000 未显示工作场所的平面布置图，可以按照本节中的步骤，导入平面布置图并在相应位置标记 AP。

导入到 ZD1000/3000 中的平面地图数量不受限制。但是在 ZD1000 上导入的所有平面地图的总文件大小不能超过 2MB，在 ZD3000 上不能超过 10MB。如果超过文件大小限制，会显示错误消息。

4.2.1 要求

- 平面布置图应采用.GIF、.JPG或.PNG格式
- 图像应为单色或灰度图
- 文件大小不得超过200KB
- 平面布置图的每条边不得超过10英寸（720像素）。

4.2.2 导入平面布置图

步骤 1　单击“配置”>“地图”。将显示“地图”页面。

步骤 2　单击“新建”，将显示“新建”界面。

步骤 3　配置表 4-2中列出的设置。

表 4-2 导入新平面布置图的选项

选项	说明
名称	为将要导入的平面布置图命名。
说明	输入对平面布置图的说明。
Browse（浏览）	单击此按钮选择要导入的平面布置图。出现Choose File（选择文件）对话框，浏览到存储平面布置图文件的位置，选中该文件，然后单击“打开”将其导入。成功导入后，平面布置图的缩略图将显示在“当前图像”区域。

步骤 4　单击“监控”>“地图视图”查看此图像。

现在可以用“地图视图”标记接入点。

图 4-1 导入平面布置图的“新建”界面

4.2.3 放置 AP 到相应位置

使用“配置”>“地图”选项导入平面布置图后，可以使用“监控”选项卡中的“地图视图”，在相应的位置将 AP 标记出来。这样才能进行有效监控。

注意

如果导入了多个平面布置图（表示建筑中的多个楼层），必须确保在正确的平面布置图上放置 AP 到相应位置。

步骤 1 准备好AP列表，包括MAC地址和位置。

步骤 2 单击“监控”>“地图视图”（如果尚未显示）。

步骤 3 找到左上角的AP标记图标。每个AP都应有一个对应的标记图标，图标顶部有一个小红色问号。

步骤 4 查看标记图标下的MAC地址标注以识别标记。

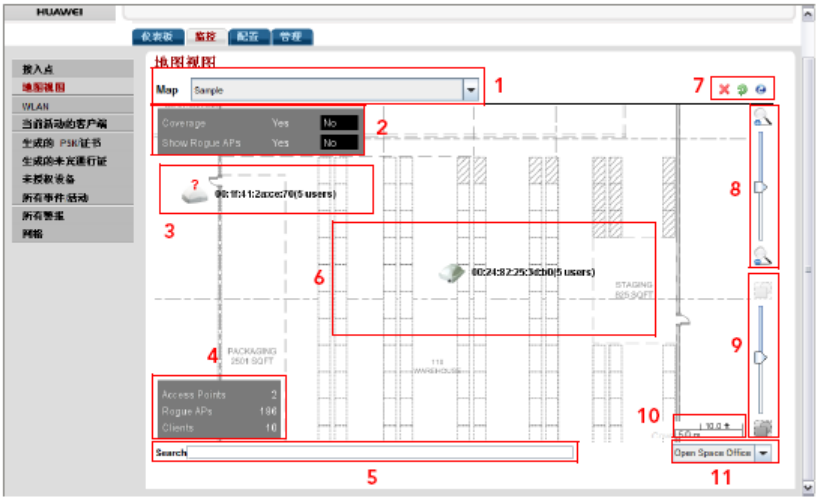
步骤 5 将每个标记图标从左上角拖到平面布置图上的相应位置。

完成后，可以立即使用地图视图优化无线覆盖，如3-32页中的“优化接入点性能”中所述。

4.3 使用“地图视图”工具

如果已扫描完工作场所平面布置图并完成 AP 绘制，“地图视图”将显示优科物理网络的 AP 分布图。

图 4-2 “地图视图”中的元素



有关地图视图中内置元素（如图 4-2所示）的说明，可参考表 4-3。

表 4-3 地图视图元素

编号	元素	说明
1	Map（地图）下拉列表	从Map（地图）下拉列表选择要查看的平面布置图。
2	Coverage（覆盖范围）和 Show Rogue APs（显示未授权AP）框	在 Coverage（覆盖范围）框中，如果选择 Yes（是），将启用已布置 AP 的信号强度视图。这将在地图视图右侧打开 Signal (%)（信号百分比）图例。有关 Signal (%)（信号百分比）的说明，参阅第 8 条。在 Show Rogue APs（显示未授权 AP）框中，如果选择 Yes（是），将在平面布置图中显示检测到的未授权 AP。

编号	元素	说明
3	未定位的AP区域	如“导入地图视图的平面布置图”中所述，第一次打开“地图视图”时，新添加的 AP 将显示在此区域。如果这些 AP 已获得批准可以使用（参阅3-19页中的“将新接入点添加到 WLAN”，可以将其拖到平面布置图中的相应位置。未定位的 AP 可以在上传的所有平面布置图中使用。管理员可以切换地图（参阅第 1 条），然后将每个 AP 放在相应的地图中。有关各种 AP 图标的说明，参阅4-6页中的“估计并扩大网络覆盖范围”。
4	Access Points（接入点）、Rogue APs（未授权AP）和 Clients（用户）框	此框位于左下角，显示活动AP、未授权（未批准或非法）AP以及所有相关用户的数目。
5	Search（搜索）文本框	输入字符串，例如AP名称或MAC地址的一部分，将对地图进行筛选，仅显示匹配的结果。清除搜索值将返回到筛选前的地图视图。
6	平面布置图区域	平面布置图显示在主要区域。使用屏幕上的工具，可以调整平面布置图的大小和角度。
7	图标	注意以下图标： • ：单击此图标，然后单击平面布置图中的 AP 可将其删除。 • ：单击此图标可旋转平面布置图。单击后，旋转交叉线将显示在地图的中心；单击并按住这些交叉线，然后移动光标可旋转视图。 • ：刷新平面布置图。
8	Signal (%)（信号百分比）	在Coverage（覆盖范围）（参阅第2条）中，如果选择Yes（是），此彩色图例将显示信号强度覆盖范围。有关详细信息，可参阅4-13页中的“估计并扩大网络覆盖范围”。

编号	元素	说明
9	上滑块	上滑块是缩放滑块，用于放大或缩小平面布置图。这有助于准确标记AP并估计是否存在影响RF覆盖范围的物理障碍。
10	下滑块	下滑块是图像对比度滑块，可以使显示的平面布置图变暗或变亮。如果看不清平面布置图，可以移动该滑块，直到标记与平面布置图细节都可以清晰显示。
11	比例尺图例	为正确估计平面布置图中的距离，可以使用标尺将AP放在最精确的位置。在未放大/缩小的平面布置图视图中使用比例尺效果最佳。比例尺的计量单位有英尺和米。为判断平面布置图上的距离，可使用物理对象作为参考刻度。例如，剪一张与比例尺长度相同的纸，然后用这张纸在平面布置图上测量距离增量。
12	Open Space Office（开放空间管理处）下拉列表	Open Space Office（开放空间管理处）是指根据当前环境计算 RF 覆盖范围/信号百分比（即热图）的方法。

4.3.1 AP 图标

每个 AP 标记的特征都是变化的，这些特征用于指示身份和状态：

表 4-4 地图视图上出现的 AP 图标

	通常，在 AP 标记下会显示该设备的以太网 MAC 地址。图标上面是“用户”数，即当前通过此 AP 连接且处于活动状态的用户数。
	如果 AP 标记尚未定位，图标上方将显示“?”（问号）。

	未授权AP的显示为“bug”标志的红色小图标。
	对于独立的 AP，图标上方将显示红色“X”。
	启用无线网格时，AP 图标旁边将显示带圆圈的数字，表示这是一个网格 AP。数字表示从该网格 AP 到根 AP 的跳数。
	启用无线网格时，如果出现内含箭头的蓝色方框，表示这是具有活动下行链路的根 AP。连接此 AP 与其他 AP 的虚线表示活动的下行链路。
	启用无线网格时，如果出现内含箭头的灰色方框，表示此根 AP 没有活动的下行链路。

4.4 查看当前警报

如果检测到警报条件，ZD1000/3000 会将其记录在事件日志中；如果已进行配置，将发送电子邮件警告。要查看当前警报，并清除所有已解决的警报记录，执行下列步骤：

步骤 1 单击“监控”>“所有警报”。

步骤 2 显示“所有警报”页面，“警报”表列出了未解决的警报，最近出现的警报位于顶部。

步骤 3 查看表中的内容。“活动”列中将提供详细信息。

步骤 4 如果某个列出的警报条件已消除，可单击右侧的**Clear**（清除）链接。也可以单击“全部清除”，一次性解决所有警报。

图 4-3 “所有警报”页面

4.5 查看最近的网络事件

可采用两种方式查看网络中的事件：[1]打开所有事件的完整列表；[2]查看每个“监控”选项卡工作区中的特定事件列表，例如 WLAN 工作区的“事件/活动”表。

步骤 1　打开ZD1000/3000仪表板，然后查看Most Recent User Activities（最近的用户活动）表和Most Recent System Activities（最近的系统活动）表中的网络活动摘要。

步骤 2　单击“监控”选项卡。

步骤 3　单击任一选项，例如WLAN、“接入点”或“当前活动的客户端”。

步骤 4　查找所选WLAN类别的“所有事件”表。

步骤 5　在“监控”选项卡下，单击“所有警报”按钮或“所有事件/活动”按钮查看完整列表，所有类别按时间顺序显示。

4.6 清除最近的事件/活动

要查看当前事件，并根据需要清除所有已解决的事件，执行下列步骤：

步骤 1 单击“监控”>“所有事件/活动”。

步骤 2 显示“所有事件/活动”页面，“事件/活动”表列出了未解决的事件，最近的事件位于顶部。

步骤 3 查看表中的内容。“活动”列中将提供详细信息。

步骤 4 可以单击底部的“全部清除”，解决并清除该视图中的所有事件。

4.7 查看当前用户活动

管理员可以通过执行下列步骤逐个监控当前的客户端：

步骤 1 单击“监控”>“当前活动的客户端”。

步骤 2 显示“当前活动的客户端”页面时，查看表以了解大致状况。

步骤 3 单击任一客户端设备MAC地址链接，以监控该客户端的详细状况。

要查看被阻止的客户端，可单击“配置”>“已阻止的客户端”。

4.8 监控接入点状态

ZD1000/3000 提供了多项功能，以监控优科 AP 的性能和状态：

步骤 1 打开“仪表板”，查看最活跃的AP的快照视图。单击任一AP记录的MAC地址链接以查看详细信息。

步骤 2 单击“监控”>“地图视图”，然后单击射频以查看反映当前RF覆盖范围的热图。

步骤 3 单击“监控”>“接入点”，查看AP的使用情况和覆盖范围。单击任一AP的MAC地址链接以查看详细信息。

步骤 4 单击**System Info**（系统信息）链接，检索AP的support.txt文件。

4.9 检测未授权的接入点

与相邻 WLAN 中的“相邻”接入点(AP)不同，“未授权”AP 会使无线网络出现问题。未授权 AP 通常以如下形式出现：某员工获取其他生产商的 AP 并将其连接到 LAN，以对其他 LAN 资源进行无线访问。这样做可能会使更多未授权用户能够访问公司的 LAN，从而造成安全风险。未授权 AP 还会干扰附近的优科 AP，导致整个无线网络的覆盖范围缩小。

ZD1000/3000 未授权检测选项包括确定是否存在未授权 AP，并在该 AP 离开之前在工作场所平面布置图中确定其位置。如果未授权 AP 位于相邻网络（即在工作场所之外，不会造成威胁），可以将其标记为“已知”。

检测未授权 AP

步骤 1　单击“仪表板”（或单击“监控”>“未授权设备”）。

步骤 2　在“设备概述”下，查看“未授权设备数”。

图 4-4 “未授权设备”指示

步骤 3　如果至少检测到一台未授权设备，单击数字以查看详细信息。

步骤 4　单击“监控”>“未授权设备”，将列出以下两个表：

- “当前活动的未授权设备”表
- “已知/已识别的未授权设备”表。

步骤 5　查看“当前活动的未授权设备”表。表 4-5列出了ZD1000/3000识别的未授权AP的类型。只要ZD1000/3000检测到其中一种未授权AP，就会生成一个警报。

表 4-5 ZD1000/3000 识别的未授权 AP 的类型

未授权 AP 的类型	说明
AP	ZD1000/3000 未知的接入点。
AP（假冒 SSID）	使用与 ZD1000/3000 AP 相同的 SSID 的未授权 AP，也称为双面恶魔 AP。
AP（假冒 MAC）	BSSID (MAC)与 ZD1000/3000 管理的虚拟 AP 相同的未授权 AP。

Encryption（加密）列指示未授权设备已加密还是属于开放式设备。

步骤 6 如果所列AP位于附近其他相邻网络中，单击“标记为已知”。此AP将被标识为不会产生威胁，同时此记录将被复制到“已知/已识别的未授权设备”表。

步骤 7 要查找确实会对内部WLAN带来威胁的未授权AP，单击设备的MAC地址以打开“地图视图”。

步骤 8 如果工作场所平面布置图已导入到“地图视图”窗口，且AP已布置到该地图中，可按照相对精度确定未授权AP。

步骤 9 打开“地图视图”，查看是否存在未授权AP的图标。这是查找未授权AP的线索。

现在可以找到未授权 AP 并将其断开。如果未授权 AP 实际上是相邻网络中的组件，可以将其标记为“已知”。

注意

如果办公室或工作场所位于多层建筑中的某个楼层，则上层和下层相邻的无线接入点可能会显示在“地图视图”上，看起来像是在用户自己的办公场地中。由于优科在垂直空间中无法对这些无线接入点进行定位，可能需要进一步调查以确定 AP 所在的位置，以及是否应该将其标记为“已知”。

4.10 检测未授权 DHCP 服务器

未授权 DHCP 服务器是指不受网络管理员控制的 DHCP 服务器。如果将未授权 DHCP 服务器接入网络，该服务器可能会分配无效 IP 地址、破坏网络连接或阻止客户端设备访问网络服务。还可能被黑客利用，危及网络安全。未授权的 DHCP 服务器通常是用户启用（通常是无意地）的、具有内置 DHCP 服务器功能的网络设备（例如路由器）。

ZD1000/3000 可以检测出未授权 DHCP 服务器，此功能可以避免未授权的 DHCP 服务器可能带来的连接和安全问题。启用此功能后，ZD1000/3000 每 5 秒扫描一次网络以检测是否有未授权 DHCP 服务器，并且每次检测到未授权 DHCP 服务器时都会生成一个事件。

检测未授权 DHCP 服务器的情况取决于是否已启用 ZD1000/3000 的内置 DHCP 服务器：

- 如果已启用内置 DHCP 服务器，则当 ZD1000/3000 检测到网络上有任何其他 DHCP 服务器时，将生成一个事件。
- 如果已禁用内置 DHCP 服务器，则当 ZD1000/3000 检测到网络上有两个或多个 DHCP 服务器时，将生成事件。管理员需找到这些 DHCP 服务器，确定哪些是未授权的服务器，然后将其断开或关闭其 DHCP 服务。

图 4-5 “未授权 DHCP 服务器检测”选项

在 ZD1000/3000 上启用“未授权 DHCP 服务器检测”

步骤 1 单击“配置”>“服务”。

步骤 2 在“未授权DHCP服务器检测”下，选中“启用未授权DHCP服务器检测”复选框。

步骤 3 单击“应用”。

未授权 DHCP 服务器检测已启用。优科建议定期检查“监控”>“所有事件/活动”页面，确定 ZD1000/3000 是否检测到任何未授权的 DHCP 服务器。如果 ZD1000/3000 检测到任何未授权 DHCP 服务器，“所有事件/活动”页面上将显示下列事件：

Rogue DHCP server on [IP_address] has been detected（在[IP_address]处检测到未授权 DHCP 服务器）。

4.11 估计并扩大网络覆盖范围

如果工作场所 WLAN 覆盖范围内存在间隙或盲点，可以使用 ZD1000/3000 估计网络 RF 覆盖范围，然后重新布置 AP 以扩大覆盖范围。记住，优科 AP 可使用任何频率在平均广播功率设置下覆盖半径为 30 英尺到 50 英尺的范围。工作场所内的建筑障碍物可能会限制覆盖范围。

步骤 1 单击“监控”>“地图视图”。

步骤 2 如果“地图视图”显示带有活动设备符号的平面布置图，则可以从覆盖范围的角度评估各个AP的性能。（有关设置地图视图的信息，参阅4-2页中的“导入地图视图的平面布置图”。）

步骤 3 对于Coverage（覆盖范围）选项，单击**Yes**（是）。

步骤 4 当显示“热图”时，在地图的右上角查找Signal%（信号百分比）比例尺。

步骤 5 注意颜色范围，尤其是表示低覆盖范围的颜色。

步骤 6 查看平面布置图并估计当前覆盖范围。

4.11.1 将 AP 移动到更适当的位置

现在可以将 AP 移动到更适当的位置。

步骤 1　在地图视图的平面布置图上单击并拖动各个AP标记，直到达到最佳RF覆盖范围。（如果覆盖范围的间隙较大，可能需要其他AP来填充。）

步骤 2　要关闭热图，然后恢复平面布置图以方便查看，单击Coverage（覆盖范围）选项中的**No**（否）。

步骤 3　记下重定位的AP标记的新物理位置。

步骤 4　根据地图视图重定位重新布置AP的实际位置后，断开每个AP的电源，然后重新连接。

ZD1000/3000 在每个 AP 重新接通后会重新校准地图视图，管理员可以评估更改效果，并根据需要进一步调整。

4.12 自定义后台射频扫描

作为网络监控的重要元素，ZD1000/3000 会定期抽测所有接入点的活动，以评估射频(RF)使用情况。扫描时在每个 AP 中抽测一个通道，因此不会影响网络使用。扫描信息稍后将应用于地图视图和其他 ZD1000/3000 监控功能。

步骤 1　单击“配置”>“服务”。

步骤 2　选中“每隔以下时间运行一次后台扫描”复选框，输入每次扫描之间的间隔（以秒为单位，默认值为20）。

可取消选中此复选框以禁用此功能，这会稍微提高 AP 性能，但在 ZD1000/3000 监控过程中不会进行未授权 AP 检测。

也可以降低扫描频率，因为降低扫描频率可以改进 AP 的整体性能。

步骤 3　单击“应用”保存设置。

图 4-6 “后台扫描”选项

5 管理用户和来宾访问

5.1 向 ZD1000/3000 添加新用户帐户

设置无线网络后，ZD1000/3000 可以使用外部 Active Directory 服务器，LDAP 服务器或 RADIUS 服务器对无线用户进行身份验证，或使用 ZD1000/3000 内部用户数据库中对用户进行身份验证。在内部用户数据库中创建新用户帐户，对用户进行身份验证，可执行下列步骤：

步骤 1 单击“配置”>“用户”。

步骤 2 在“内部用户数据库”表中单击“新建”。将出现“新建”界面。

步骤 3 配置表 5-1中列出的设置。

表 5-1 新用户设置

选项	说明
用户名	输入字母、数字和句点(.)等字符作为用户的名称，最大长度为 32 个字符且区分大小写。
全名	输入指定用户的名字和姓氏。
密码	输入用户的唯一密码，可以使用字母和数字的组合，长度在 4 到 32 个字符之间。密码不允许使用空格且区分大小写。
确认密码	重新输入用户密码进行确认。

步骤 4 如果已为用户或组创建了角色，则打开“角色”菜单，然后为用户选择相应的角色。有关角色及其作用的详细信息，可参阅5-3页中的“新建用户角色”。

步骤 5 单击“确定”保存设置。确保将用户名和密码通知给相应的最终用户。

图 5-1 将用户添加到内部数据库的“新建”界面

5.2 管理当前用户帐户

ZD1000/3000 允许管理员查看和更改内部用户数据库中的用户及其属性。

5.2.1 更改现有用户帐户

步骤 1　单击“配置”>“用户”。

步骤 2　出现“用户”功能时，在“内部用户数据库”面板中找到要更改的用户帐户，然后单击“编辑”。

步骤 3　在“编辑[用户名]”界面上进行更改。

步骤 4　如果必须更换角色，可打开菜单并为此用户选择新角色。[有关详细信息，可参阅5-3页中的“新建用户角色”。]

步骤 5　单击“确定”保存设置。确保将更改情况通知给相应的最终用户。

5.2.2 删除用户记录

步骤 1　单击“配置”>“用户”。

步骤 2 出现“用户身份验证”功能时，查看“内部用户数据库”。

步骤 3 要删除一条或多条记录，可选中这些记录旁边的复选框。

步骤 4 单击当前处于活动状态的“删除”按钮。

步骤 5 出现“删除确认”对话框时，单击“确定”保存设置。这些记录将从内部用户数据库中删除。

5.3 新建用户角色

步骤 1 ZD1000/3000缺省创建了一个应用于所有新用户帐户的Default（默认）角色，将用户链接到对应的WLAN并允许用户为访客/来宾产生来宾通行证。管理员还可以创建其他角色并分配给选定的无线网络用户，以指定可访问的WLAN、进行登录或授予他们生成来宾通行证的权限。（管理员也可以编辑Default（默认）角色，禁用来宾通行证生成选项。）单击“配置”>“角色”。将出现“角色和策略”页面，并在“角色”表中显示Default（默认）角色。

步骤 2 单击“角色”表下的“新建”。将出现“新建”界面。

步骤 3 配置表 5-2中列出的设置。

表 5-2 新用户角色设置

设置	说明
名称	输入用户角色的名称。
说明	输入有关用户角色的说明。
组属性	仅在创建具有管理员权限的用户角色并使用 Active Directory 作为身份验证服务器时才填写此字段。在此处输入 Active Directory 用户组名称。具有相同组属性的 Active Directory 用户将自动映射到此用户角色。
允许所有 WLAN	有两个选项：(1)允许访问所有 WLAN，或(2)指定 WLAN 访问。如果选择第二个选项，则必须单击每个 WLAN 旁边的复选框来指定 WLAN。此选项要求在设置此策略之前创建 WLAN。可参阅3-18页中的“新建 WLAN 供工作组使用”。
来宾通行证	如果希望此角色的用户具有生成来宾通行证的权限，可选中此选项。

注意

欲了解如何使用外部身份验证服务器来验证管理员身份，可参阅5-21页中的“使用外部服务器进行用户身份验证”。

步骤 4 配置完成后，单击“确定”保存设置。此角色就可以分配给授权用户了。

如果要使用不同策略创建更多角色，可重复此过程。

图 5-2 添加角色的“新建”界面

5.4 管理来宾访问

默认情况下，允许所有用户为访客或来宾颁发临时的“日用”来宾通行证。此类来宾通行证允许访客或来宾连接到 WLAN。应事先确定是否允许所有用户还是部分用户可以生成来宾通行证。

此外，管理员还应检查来宾通行证的网络默认设置和策略，并根据网络实际环境或要求及进行优化。

本部分介绍如何配置来宾访问和来宾通行证生成选项。主题包括：

- 配置系统级来宾访问策略
- 激活“生成来宾通行证”功能
- 控制来宾通行证生成权限
- 创建可生成来宾通行证的用户角色
- 将通行证生成者角色分配给用户帐户
- 监控生成的来宾通行证
- 配置来宾用户可访问的网络
- 自定义来宾登录页面

5.4.1 配置系统级来宾访问策略

通过“启用来宾访问”选项，管理员可定义系统级的来宾访问策略。用户可以要求来宾接受通行证验证、接受使用条款并重定向到指定的 URL。

步骤 1 单击“配置”>“来宾访问”。将出现“来宾访问”页面。

步骤 2 配置表 5-3中列出的设置。

表 5-3 来宾访问策略设置

设置	说明
启用来宾访问	选择要使用的身份验证类型： • 使用来宾通行证身份验证：允许访客或来宾使用来宾WLAN之前，先将其重定向到来宾通行证验证的页面。 • 允许多个用户共享一个来宾通行证：如果希望多个来宾能够使用同一个来宾通行证，则选中此复选框。 • 无身份验证：不要求重定向和来宾通行证验证。
使用条款	如果选中“显示使用条款”复选框，来宾用户就需要在使用前阅读并接受使用条款。可将使用条款输入（或剪贴）到较大的文本框内。
重定向	选择下列某个单选按钮，设置是否使用重定向功能： • 重定向到用户要访问的URL：使来宾用户不必重新输入就可以继续访问目标URL。 • 重定向到以下URL：在将用户转到目标位置之前，先将其重定向到指定的页面（在后面的文本框中输入网址）。来宾用户转到此页面后，页面上会显示其来宾通行证的到期时间。

步骤 3 单击“应用”保存设置。

图 5-3 “来宾访问”页面

5.4.2 激活“生成来宾通行证”功能

可以向通过身份验证的用户授予生成来宾通行证的权限。具体步骤如下：

步骤 1 单击“配置”>“来宾访问”。将出现“来宾访问”页面。

步骤 2 向下滚动到“生成来宾通行证”部分。

步骤 3　配置表 5-4中列出的设置。

表 5-4 “生成来宾通行证”设置

设置	说明
身份验证服务器	选择用来对要生成来宾通行证的用户进行身份验证的服务器。 • 如果在“配置”>“AAA服务器”页面上配置了AAA服务器（RADIUS或Active Directory），并希望使用该服务器对用户进行身份验证，可从下拉菜单中选择该服务器的名称。（可参阅5-21页中的“使用外部服务器进行用户身份验证”）。 • 如果要使用ZD1000/3000的本地数据库，可选择**Local Database**（本地数据库）。
有效期限	通过选择下列某个选项设置来宾通行证有效期： • 自创建起生效：此类来宾通行证从创建时起到指定的到期时间内均有效，即使未被任何最终用户使用也是如此。 • 自首次使用起生效：此类来宾通行证自用户使用它通过ZD1000/3000身份验证起到指定的到期时间内均有效。可以配置其他参数（在X天内未使用的来宾通行证将过期），指定未使用的来宾通行证的到期时间。默认值是7天。

步骤 4　完成后，单击“应用”保存设置并激活此新策略。

注意

记住要告诉用户他们可以访问“生成来宾通行证”页面，网址为：https://{ZD1000/3000y-hostname-or-ipaddress}/guestpass。

在图 5-4的示例中，生成来宾通行证的 URL 是 https:192.17.17.150/guestpass。

图 5-4 “来宾通行证”页面上的“生成来宾通行证”部分

5.4.3 控制来宾通行证生成权限

如果要禁止 Default（默认）角色用户的来宾通行证生成权限，可执行下列步骤：

步骤 1 单击“配置”>“角色”。出现“角色和策略”页面时，表中会列出现有的全部角色，包括Default（默认）角色。

步骤 2 单击Default（默认）角色行中的“编辑”。

步骤 3 在“策略”选项中，不要选中“允许生成来宾通行证”复选框。

步骤 4 单击“确定”保存设置。角色为Default（默认）的用户将不再拥有生成来宾通行证的权限。

5.4.4 创建可生成来宾通行证的用户角色

要创建来宾通行证生成者的用户角色，可执行下列步骤：

步骤 1 单击“配置”>“角色”。

步骤 2 在“角色”表中单击“建”将出现“新建”界面。

步骤 3 配置表 5-5中列出的设置。

表 5-5 来宾通行证生成者角色设置

设置	说明
名称	输入角色的名称。
说明	输入关于角色作用的简短描述。
组属性	此字段仅在选择 Active Directory 作为身份验证服务器的情况下才启用。在此处输入 Active Directory 用户组名称。具有相同组属性的 Active Directory 用户将自动映射到此用户角色。
允许所有 WLAN	有两个选项：(1)允许此角色的所有用户连接到所有 WLAN，或者(2)仅允许此角色的用户连接到特定 WLAN，然后选出他们可以连接到的 WLAN。
来宾通行证	如果希望此角色的用户具有生成来宾通行证的权限，可选中此选项。

步骤 4　单击“确定“保存设置。此角色已可应用于授权用户。

5.4.5 将通行证生成者角色分配给用户帐户

下面详细介绍了将来宾通行证生成者角色分配给用户帐户的过程。

步骤 1　单击“配置”>“用户”。

步骤 2　在“内部用户数据库”的底部单击“新建”。

步骤 3　出现“新建”界面时，在文本字段中输入相应内容。

步骤 4　打开“角色”菜单，选择为此用户分配的角色。

注意

如果需要，可以编辑现有用户帐户并重新分配通行证生成者角色。

步骤 5　单击“确定”保存设置。确保将角色、用户名和密码通知给相应的最终用户。

5.4.6 自定义来宾通行证使用说明

来宾通行证使用说明是一张可打印的 HTML 页面，其中包含对来宾用户如何成功连接到无线网络的指导说明。通过身份验证的用户，如果要生成来宾通行证，则需要打印此 HTML 页面并将其提供给来宾用户。默认情况下提供英文版的来宾通行证。

管理员可以自定义来宾通行证使用说明。例如，如果接待了讲其他语言的访客，就可以创建和输出相应语言版本的来宾通行证。

要自定义来宾通行证使用说明

步骤 1 单击“配置”>“来宾访问”。

步骤 2 向下滚动至页面底部的“来宾通行证输出自定义”部分。

步骤 3 单击此部分下的“请单击此处”链接，下载默认的来宾通行证使用说明（HTML格式）。将该HTML文件保存到计算机。

步骤 4 使用文本或HTML编辑器自定义来宾通行证使用说明。可执行下列任何（或所有）操作：

- Reword the instructions（重述说明）
- Translate the instructions to another language（将说明翻译成另一种语言）
- Customize the HTML formatting（自定义 HTML 格式）

来宾通行证使用说明包含多个标记或变量，生成来宾通行证时会用实际数据代替这些标记或变量。自定义来宾通行证使用说明时，注意不要删除这些标记。有关这些标记的详细信息，可参阅5-12页中的“来宾通行证使用说明标记”。

步骤 5 返回到“来宾通行证使用说明自定义”页面，然后单击“新建”。将出现“新建”界面。

步骤 6 配置表 5-6中列出的设置。

表 5-6 来宾通行证使用说明自定义设置

设置	说明
名称	输入要创建的来宾通行证使用说明的名称。例如，如果此来宾通行证使用说明要使用西班牙语，可以输入 Spanish。
说明	（可选）关于来宾通行证使用说明的简短说明。
浏览	单击此按钮可选择先前自定义的 HTML 文件，然后单击“打开”。ZD1000/3000 将把该 HTML 文件复制到自己的数据库中。

步骤 7 单击“导入”，将HTML文件保存到ZD1000/3000数据库中。

自定义来宾通行证输出操作完成。生成来宾通行证后，所创建的自定义使用说明将作为可打印选项显示出来（可参阅图 5-6）。

来宾通行证使用说明标记

表 5-7列出了来宾通行证使用说明中使用的标记。自定义来宾通行证使用说明时，注意不要删除这些标记。

表 5-7 可以在来宾通行证使用说明中使用的标记

标记	说明
{GP_GUEST_NAME}	来宾通行证用户名
{GP_GUEST_KEY}	来宾通行证密钥
{GP_IF_EFFECTIVE_FROM_CREATION_TIME}	如果在“生成来宾通行证”部分将来宾通行证的有效期设置为“自创建起生效”，此标记将显示来宾通行证的创建时间和到期时间。

标记	说明
{GP_ELSEIF_EFFECTIVE_FROM_FIRST_USE}	如果在“生成来宾通行证”部分将来宾通行证的有效期设置为“自首次使用起生效”，此标记将显示来宾通行证激活后的生效天数。即使未激活来宾通行证，仍显示其到期日期和时间。
{GP_ENDIF_EFFECTIVE}	此标记与{GP_ELSEIF_EFFECTIVE_FROM_FIRST_USE}或{GP_ENDIF_FFECTIVE}标记结合使用。
{GP_VALID_DAYS}	来宾通行证的生效天数。
{GP_VALID_TIME}	来宾通行证的到期日期和时间。
{GP_GUEST_WLAN}	来宾用户可以访问的 WLAN 的名称。

5.4.7 生成并打印来宾通行证

可以向有权生成来宾通行证的用户提供以下说明。

注意

用户可通过以下步骤生成和打印来宾通行证。开始前，确保计算机连接到本地或网络打印机。

步骤 1 在计算机上启动Web浏览器。

步骤 2 在地址栏或位置栏中输入“生成来宾通行证”页面的URL：

https://{ZD1000/3000y-hostname-or-ipaddress}/guestpass

步骤 3 在“用户名”字段中输入用户名。

步骤 4 在“密码”字段中输入密码。

步骤 5 单击“登录”。此时会显示Guest Information（来宾信息）页面。在此页面上需要提供来宾用户的相关信息，以便ZD1000/3000生成来宾通行证。

步骤 6　在Guest Information（来宾信息）页面上，填写表 5-8中列出的以下选项。

表 5-8 Guest Information（来宾信息）页面选项

选项	说明
Full Name（全名）	输入来宾用户（要为其生成来宾通行证）的姓名。
Valid for（有效期限）	指定来宾通行证的有效期。在空白框中输入数字，然后选择时间单位（**Days**（天）、**Hours**（小时）或 **Weeks**（周））即可。
Remarks（备注）	（可选）输入任意注释或评论。例如，如果来宾用户是合作单位的员工，则可以输入该单位的名称。
Key（密钥）	如果要使用 ZD1000/3000 生成的随机密钥，则不必自己输入。如果希望使用容易记住的密钥，可删除随机密钥，然后输入自己的密钥。例如，如果 ZD1000/S3000 成了随机密钥 OVEGS-RZKKF，可以将其更改为 oe-guest-ey。自定义的密钥必须由 1 到 16 个 ASCII 字符组成。

步骤 7　单击**Next**（下一步）。将出现Guest Pass Generated（来宾通行证已生成）页面。

步骤 8　在下拉菜单中，选择要输出的来宾通行证说明。如果未自定义来宾通行证使用说明，则选择**Default**（默认）。

步骤 9　单击**Print Instructions**（打印说明）。将出现新的浏览器页面并显示来宾通行证说明。同时将出现Print（打印）对话框。

步骤 10　选择要使用的打印机，然后单击**OK**（确定）打印来宾通行证说明。

为来宾用户生成和打印来宾通行证这一过程现在已完成。

图 5-5 Guest Information（来宾信息）页面

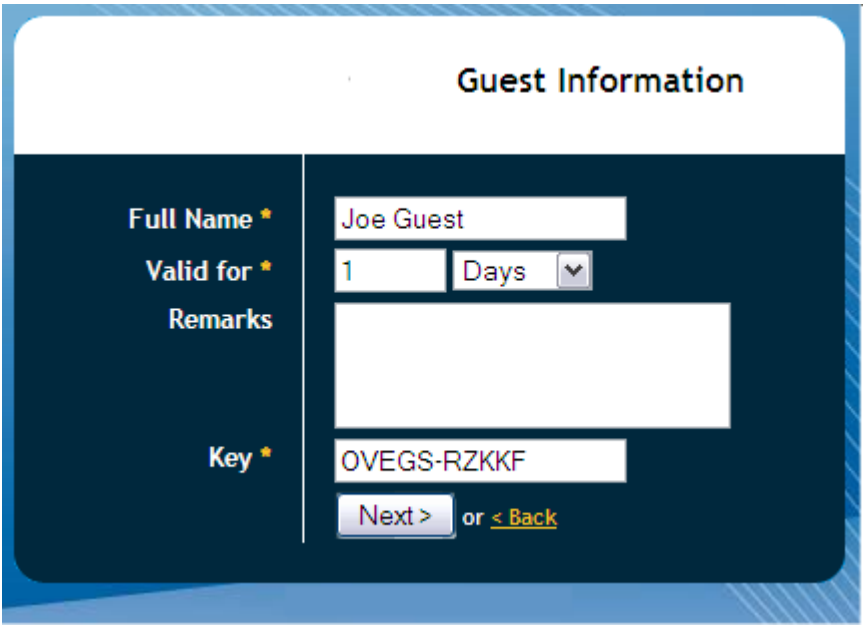


图 5-6 Guest Pass Generated（来宾通行证已生成）页面（使用自定义密钥）

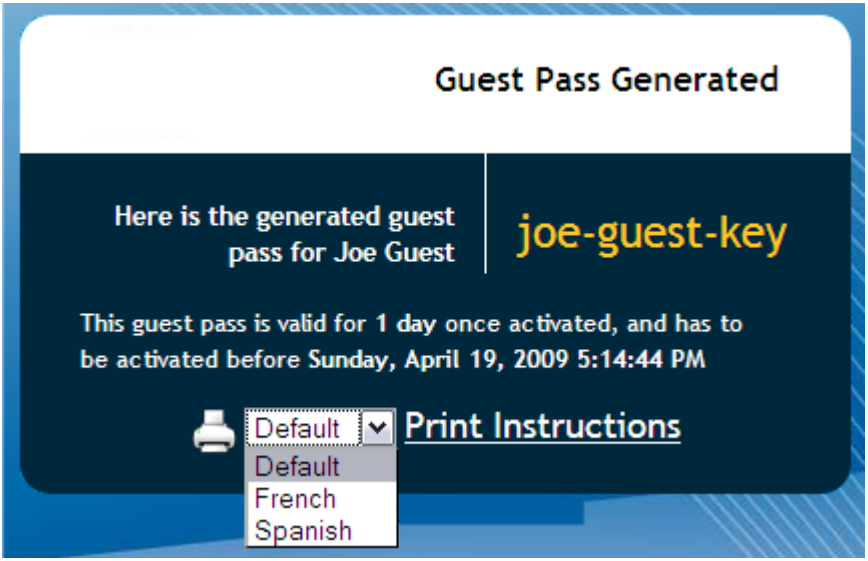
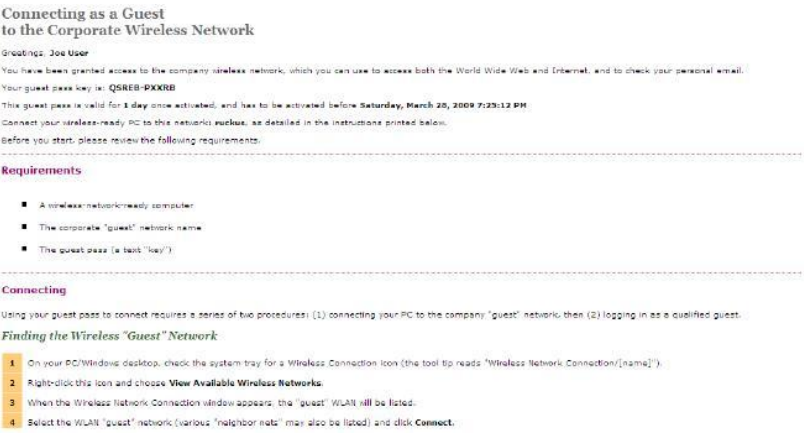


图 5-7 来宾通行证使用说明示例



Connecting as a Guest
to the Corporate Wireless Network

Greetings, **Joe User**

You have been granted access to the company wireless network, which you can use to access both the World Wide Web and Internet, and to check your personal email.

Your guest pass key is: **QSREB-PXXRB**

This guest pass is valid for **1 day** once activated, and has to be activated before **Saturday, March 28, 2009 7:25:12 PM**

Connect your wireless-ready PC to this network **ruckus**, as detailed in the instructions printed below.

Before you start, please review the following requirements.

Requirements

- A wireless-network-ready computer
- The corporate "guest" network name
- The guest pass (a text "key")

Connecting

Using your guest pass to connect requires a series of two procedures: (1) connecting your PC to the company "guest" network, then (2) logging in as a qualified guest.

Finding the Wireless "Guest" Network

1. On your PC/Windows desktop, check the system tray for a Wireless Connection icon (the tool tip reads "Wireless Network Connection/[name]").
2. Right-click this icon and choose **View Available Wireless Networks**.
3. When the Wireless Network Connection window appears, the "guest" WLAN will be listed.
4. Select the WLAN "guest" network (various "neighbor nets" may also be listed) and click **Connect**.

5.4.8 监控生成的来宾通行证

为来宾生成通行证后，可以监控通行证，必要时可以删除。

步骤 1 单击“监控”> **Generated Guest Passes**（生成的来宾通行证）。

步骤 2 查看生成的来宾通行证。

步骤 3 若要删除来宾通行证，可选中该通行证的对应复选框。

步骤 4 单击**Delete**（删除）按钮。

5.4.9 配置来宾用户可访问的网络

默认情况下，使用来宾通行证的来宾或访客不能访问 ZD1000/3000 所在的和来宾用户关联的 AP 所在的网络（格式：A.B.C.D/M）。如果要增加其他允许或限制来宾用户访问特定网络的规则，可使用“来宾通行证”>“受限制的子网访问”页面。

用户最多可以创建 22 条子网访问规则，这些规则将在 ZD1000/3000 端（针对隧道/重定向通信）和 AP 端（针对本地桥接通信）强制执行。

注意

所有来宾遵循同一个子网访问策略。

要创建子网的来宾访问规则

步骤 1 单击“配置”>“来宾访问”。

步骤 2 在“受限制的子网访问”部分，单击“新建”。将在下方显示文本框，管理员可以输入用来定义访问规则的参数。

步骤 3　配置表 5-9中列出的设置。

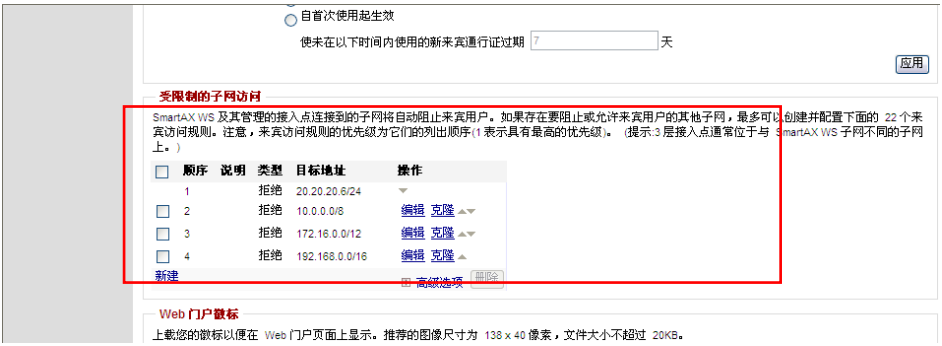
表 5-9 来宾访问规则设置

设置	说明
说明	输入要创建的访问规则的名称或说明。
类型	如果此规则阻止来宾用户访问特定子网，则选择“拒绝”；如果此规则允许来宾用户访问特定子网，则选择“允许”。
目标地址	输入要允许或拒绝来宾用户访问的 IP 地址和子网掩码（格式：A.B.C.D/M）。
高级选项	如果要根据使用的应用程序、协议或目标端口允许或限制访问子网，可单击“高级选项”链接，然后进行相应的配置。

步骤 4　单击“确定”保存子网访问规则。

重复步骤 2 到步骤 7，可最多创建 22 条子网访问规则。

图 5-8 “受限制的子网访问”选项



5.4.10 自定义来宾登录页面

可以自定义来宾用户登录页面，使其显示公司徽标并提供帮助说明以及“欢迎”标题。

如果要在页面中包含徽标，需要准备支持 Web 的图形文件，有三种可识别的格式（.JPG、.GIF 或.PNG）。徽标文件不得超出以下限制：

- 长度：任何边均不超过 2 英寸
- 文件大小：不超过 20KB

要自定义来宾登录页面

步骤 1 单击“配置”>“来宾访问”。

步骤 2 向下滚动到“Web门户徽标”部分。

步骤 3 如果已准备好要使用的徽标，可单击**Browse**（浏览）打开用于导入徽标文件的对话框。（如果文件过高或过宽，ZD1000/3000将会提示）。

步骤 4 向下滚动到“来宾访问自定义”部分。

步骤 5 （可选）删除“标题”字段中的文本，并输入简短的描述性标题或“欢迎”消息。

步骤 6 单击“应用”保存设置。将显示Setting applied!（设置已应用！）确认消息。

图 5-9 “来宾访问自定义”选项

5.5 使用基于 Web 的身份验证

如果 WLAN 配置了基于 Web 的身份验证，所有关联到该 WLAN 的用户在每次连接时将被强制定向到指定的登录界面。

在热区/热点 WLAN 配置了基于 Web 的身份验证时，必须配置用户登录页面的 URL。这些用户应该已存在于内部数据库或外部身份验证服务器的数据库中。用户关联到相应的 WLAN 后，打开浏览器，然后被强制定向到配置好的登录页面并输入所需的登录信息（用户名和密码）。

步骤 1 单击“配置”> WLAN。将显示“WLAN”页面。

步骤 2 查找要编辑的WLAN，然后单击同一行上的“编辑”链接。

步骤 3 出现“编辑(WLAN_Name)”界面时，找到“Web身份验证”选项。可参阅图 5-10。

步骤 4　单击复选框以启用门户/Web身份验证。

步骤 5　从“身份验证服务器”下拉菜单中选择要使用的身份验证服务器（对于Web身份验证）。

步骤 6　单击“确定”保存设置。

对要启用 Web 身份验证的每个 WLAN 重复上述步骤。

图 5-10 “编辑 WLAN”页面

5.6 管理自动生成的用户证书和密钥

使用优科 Zero-IT 无线激活功能，可以自动为用户生成唯一的密钥或证书。更确切地说就是，对于已配置 WPA-PSK/WPA2-PSK 且已启用动态 PSK 的 WLAN，会为每个无线用户生成唯一的随机密钥。同样，对于已配置 802.1X/EAP 身份验证的 WLAN，会为每个无线用户创建唯一的证书。

使用内部用户数据库时，只要用户数据库中的用户帐户被删除，对应的自动生成的用户证书和密钥即被删除。如果使用 Windows Active Directory 服务器或 RADIUS 服务器作为身份验证服务器，可以执行以下步骤来删除生成的用户密钥和证书：

步骤 1　单击“监控”> **Generated PSK/Certs**（生成的PSK/证书）。将显示Generated PSK/Certs（生成的PSK/证书）页面。

步骤 2　选中要删除的PSK和证书的复选框。

步骤 3 单击**Delete**（删除）将所选项目删除。

所选的 PSK 和证书将从系统中删除。

如果用户的 PSK 或证书已被删除，在未获得新密钥或新证书的情况下将无法连接到无线网络。

5.7 使用外部服务器进行用户身份验证

配置无线网络时，可以指示 ZD1000/3000 使用外部的 Active Directory 服务器或 RADIUS 服务器对无线用户进行身份验证，或在内部用户数据库上新建用户帐户。

要使用 RADIUS 或 Active Directory 服务器作为身份验证服务器

步骤 1 单击“配置”>“AAA服务器”。将显示“身份验证服务器”页面。

步骤 2 单击“身份验证服务器”表中的“新建”链接。将出现“新建”界面。

步骤 3 配置表 5-10中列出的设置。

表 5-10 外部服务器身份验证设置

设置	说明
名称	输入身份验证服务器的描述性名称（例如，Active Directory）。
类型	确认已选定 Active Directory 或 RADIUS。
IP Address（IP 地址）	输入 Active Directory 服务器的 IP 地址。
端口	如果默认端口号不是 389（对于 Active Directory）或 1812（对于 RADIUS），则输入端口号。
域名（仅适用于 Active Directory）	输入 Active Directory 服务器的域名，例如 domain.huawei.com。
共享密钥（仅适用于 RADIUS）	输入共享密钥，然后在 **Confirm Secret**（确认密钥）字段中重新输入密钥。

步骤 4　单击“确定”保存此服务器的设置。

注意

如果要测试与身份验证服务器的连接，可在“测试身份验证设置”面板中输入现有用户名和密码，然后单击“测试”。在使用 RADIUS 服务器进行测试之前，确保已在 RADIUS 服务器上启用了“密码验证协议”(Password Authentication Protocol，PAP)，否则测试会失败。

图 5-11 添加身份验证服务器的“新建”界面

6 部署智能网格

6.1 智能网格概述

智能网格是一种对等的多跳无线网络，其中参与的节点相互协作转发数据。在优科网格中，转发节点（即构成网络的优科 AP）或“网格节点”构成网络的骨干。客户端（如便携式计算机及其他移动设备）将连接到这些网格节点，并通过此骨干相互通信，在允许情况下还可以与 Internet 上的节点进行通信。借助网格，用户可以通过在“跳”节点间创建一个路径来访问其他系统。

智能网格有以下优点：

- 具有自愈功能：如果某个节点发生故障，则其他所有节点都会发现该故障并重新路由数据。
- 具有自组织功能：新节点出现时将自动加入网格。

在优科智能网格中，会对所有通过网格链路进行的数据通信加密。所有网格节点都使用同一个密码以保证数据通信安全。

部署网格时，优科 AP 通过有线 LAN 链路或与其他优科 AP 构建的无线链路与 ZoneDirector 通信。

6.2 智能网格术语

优科建议网络管理员在开始部署智能网格之前，先了解下列术语。本文档使用这些术语来说明无线网格。

表 6-1 网格术语

术语	定义
网格节点	启用了网格功能的优科 AP。具有网格功能的优科 AP 型号包括 ZONEFLEX 系列、WA632 和。
根接入点（根 AP）	通过以太网接口（即有线接口）与 ZD1000/3000 通信的网格节点。
网格接入点（网格 AP）	通过无线接口与 ZD1000/3000 通信的网格节点。
网格树	每个网格 AP 只通过一条上行链路连接到其他网格 AP 或根 AP。而每个网格 AP 或根 AP 都可连接多个网格 AP。由此形成树形拓扑。网格树的深度不受配置限制。 一个 ZD1000/3000 设备可以管理多个网格树。ZD1000/3000 可管理的网格树数目仅取决于其可管理的 AP 数目。
跳	数据包从网格 AP 到达根 AP 所经过的无线网格链路数。例如，如果根 AP 是网格 AP 1 的上行链路，则网格 AP 1 与根 AP 之间相距一跳。如果网格 AP 1 又是网格 AP 2 的上行链路，则网格 AP 2 与根 AP 之间相距两跳。

6.3 支持的网格拓扑

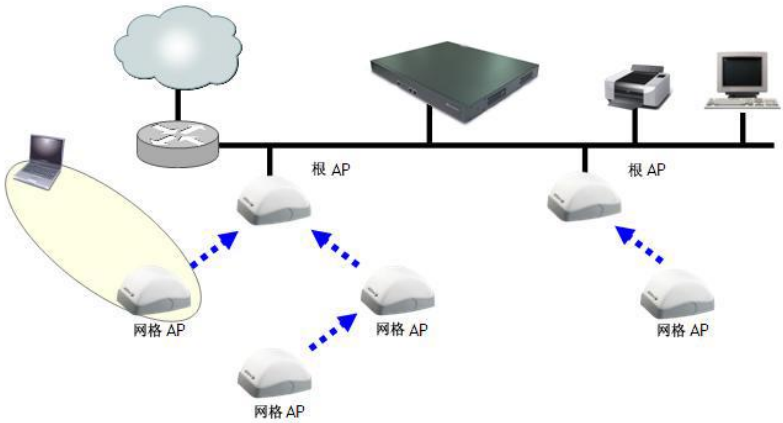
智能网格支持以下两种拓扑：

- 标准拓扑
- 无线桥接拓扑

6.3.1 标准拓扑

如果需要扩展无线网络的覆盖范围，则可以使用标准拓扑设置网格。在此拓扑中，ZD1000/3000 和上游路由器连接在同一个有线 LAN 网段上。通过形成多个网格树（参考图 6-1）并将其连接到有线 LAN 网段，可以扩展无线网络的范围。每个网格树中的所有客户端都可充当无线客户端。

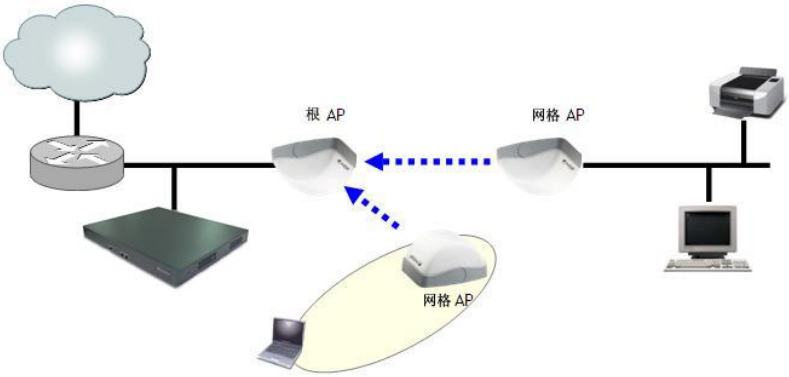
图 6-1 网格 – 标准拓扑



6.3.2 无线桥接拓扑

如果要桥接独立的有线 LAN 网段，可以使用无线桥接拓扑设置网格。在此拓扑中，ZD1000/3000 和上游路由器位于主有线 LAN 网段，而另一个独立有线网段需要桥接到该主 LAN 网段。可以通过在这两个有线 LAN 网段间构建网格链路将它们桥接起来，如图 6-2所示。

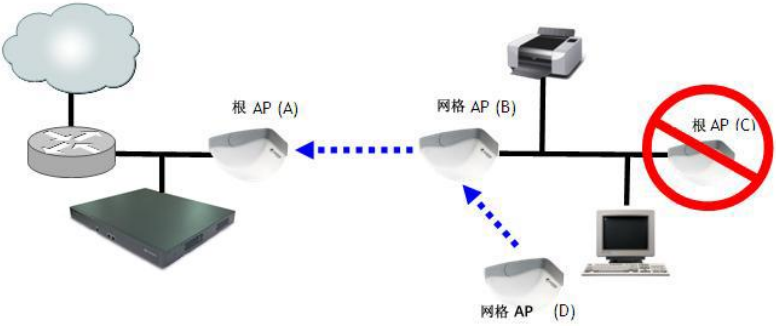
图 6-2 网格 – 无线桥接拓扑



但不可以将其他有线 AP 连接到桥接网段，如图 6-3所示。此配置的问题在于，由于 C 可以通过网格链路 B-A 连接 ZD1000/3000，并且 C 的以太网端口处于活动状态，因此尽管它不是根 AP，但还是满足了成为根 AP 的两个条件（可连接到 ZD1000/3000 且可以使用以太网）。因此这是一个非法拓扑。

但是，可以在此物理位置添加其他无线 MAP，以扩大覆盖范围并增加网格容量。如图 6-3所示，RAP-C 为非法拓扑，因为它是通过以太网连接到此桥接有线网段的。但是，使用无线 MAP-D 扩展网格是合法的。

图 6-3 网格 – 非法桥接拓扑



6.4 通过 ZD1000/3000 部署无线网格

通过 ZD1000/3000 部署无线网格的步骤如下：

- 步骤 1：准备进行无线网格部署
- 步骤 2：在 ZD1000/3000 上启用网格功能
- 步骤 3：配置和部署网格节点
- 步骤 4：确认无线网格是否已成功建立

步骤 1：准备进行无线网格部署

优科建议网络管理员在开始部署无线网格之前，先执行下列任务，以确保部署可以顺利进行。

- 规划无线网格 – 考察部署现场，确定要部署的 AP 数（包括根 AP 和网格 AP 的数目），然后画出每个根 AP 和网格 AP 部署位置的简单草图。记住根 AP 需通过以太网端口连接到 ZD1000/3000。如果尚未布线，确保可以轻松连线到根 AP 位置。
- 确保接入点支持网格 – 具有网格功能的优科 AP 型号包括 ZONEFLEX 系列，确认要接入无线网格的所有接入点是否都具有网格功能。注意，只有版本 6.0.0.0.* 及更高版本的固件（适用于优科 AP 和 ZD1000/3000）支持网格。

启用自动审批功能 – 如果网络管理员希望在每个网格 AP 加入无线网格时，不必手动审批它们的加入请求，可以启用自动审批功能。欲了解如何启用自动审批功能，参考3-19页中的“将新接入点添加到 WLAN”。

步骤 2：在 ZD1000/3000 上启用网格功能

如果完成“安装向导”后未在 ZD1000/3000 上启用网格功能，可以在“配置”>“网格”页面上启用该功能。

图 6-4 在“配置”>“网格”中启用网格

要启用网格功能

步骤 1 登录到**ZD1000/3000** Web界面。

步骤 2 单击“配置”选项卡。

步骤 3 在菜单中，单击“网格”。

步骤 4 配置表 6-2中列出的设置。

表 6-2 “启用网格”设置

设置	说明
启用网格	● 要启用网格，可选中“启用网格”复选框。 ● 要禁用网格，可取消选中“启用网格”复选框。
网格名称(ESSID)	输入网格的名称。也可以使用 ZD1000/3000 生成的默认网格名称。

设置	说明
网格密码	输入至少包含 12 个字符的密码。ZD1000/3000 将使用此密码来确保网格 AP 间数据通信的安全。也可以单击“生成”，生成一个包含 32 个或 32 个以上字符的随机密码。

步骤 5 单击“应用”保存设置。

现在即已在 ZD1000/3000 上启用网格功能。此后，可以配置和部署要接入无线网格的 AP。

步骤 3：配置和部署网格节点

在此步骤中，需要将每个 AP 连接到 ZD1000/3000 所在的有线网络，以配置与网格相关的设置。完成对 AP 的配置之后，必须重新启动该 AP，使与网格相关的设置生效。

要配置和部署网格节点

步骤 1 通过AP的任意一个以太网端口，将该AP连接到ZD1000/3000所在的有线网络，然后接通该AP。该AP将检测ZD1000/3000，并向其发送加入请求。

步骤 2 如果启用了自动审批功能，可直接跳到步骤3。如果禁用了自动审批功能，则需登录到ZD1000/3000，并查看网络管理员要配置的AP中当前处于活动状态的接入点列表，然后单击相应的“允许”链接，批准其加入请求。欲了解审批加入请求的详细步骤，参考3-19页中的“验证/审批新AP”。

步骤 3 完成对AP的配置之后，断开其与有线网的连接，拔下电源线，然后将此设备移到相应部署位置。

- 如果要将该 AP 设置为根 AP，可通过任意一个以太网端口将其重新连接到有线网络，然后接通。当 AP 通过以太网端口再次检测到 ZD1000/3000 时，它会将自己设置为根 AP，然后接受来自网格 AP 的关联请求。
- 如果要将 AP 设置为网格 AP，可以仅将其接通但不重新连接到有线网。如果 AP 未能通过以太网端口在 90 秒内检测到 ZD1000/3000，则会搜索其他网格 AP，且在建立了网格邻居关系后，便会构成网格树。

注意

配置完处于出厂设置状态的 AP 后，需要重新启动该 AP 以启用网格功能。

对要接入无线网格的各个网格 AP 和根 AP 重复执行步骤 1 至步骤 3。配置和部署完所有网格节点后，确认该无线网格是否已成功建立。

步骤 4：确认无线网格是否已成功建立

当网络管理员将所有网格节点都部署到网络上的相应位置后，可以查看 ZD1000/3000 Web 界面上的“地图”视图，确认是否已建立网格关联并形成网格树。

步骤 1　在“区域控制器”Web界面上，单击“监控”选项卡，然后单击菜单上的“地图”视图。将显示“地图”视图，并显示当前处于活动状态的网格节点。

步骤 2　检查“地图”视图上是否显示了所有已配置和部署的网格节点。

步骤 3　检查网格节点之间是否出现了虚线，以确认是否已建立网格。这些虚线表示在当前网格中建立的邻居关系。

图 6-5 虚线表示这些 AP 已接入无线网格

AP 图标旁边的符号表示该 AP 是根 AP 还是网格 AP。参见下表：

表 6-3 启用了网格的 AP 的图标图例

	带有向上箭头的 AP 是根 AP。
	带有带圈数字的 AP 是网格 AP。数字表示网格 AP 与根 AP 之间的跳数。

6.5 了解与网格相关的 AP 状态

除了使用“地图”视图监控网格状态之外，还可以通过查看“监控”选项卡上的“接入点”页面来了解与网格相关的 AP 状态。下表列举了与网格相关的所有可能的 AP 状态，以及解决网格相关问题所需执行的所有操作。

表 6-4 与网格相关的 AP 状态

状态	说明	建议操作
已连接	AP 已连接到 ZD1000/3000，但网格处于禁用状态	如果在 AP 上启用了网格，可能需要重新启动该 AP 以激活网格功能。
已连接（根 AP）	AP 已通过以太网端口连接到 ZD1000/3000	
已连接（网格 AP，n 跳）	AP 已通过无线接口连接到 ZD1000/3000，并且与根 AP 相距 n 跳。	

状态	说明	建议操作
独立的网格接入点	AP 已断开与 ZD1000/3000 网格的连接	• AP 的配置可能不正确。需确认此 AP 上配置的网格 SSID 和密码是否正确。 • 如果“上行链路选择”设置为“手动”，则为此 AP 指定的上行链路 AP 可能已关闭或不可用。

6.6 手动设置网格上行链路

在无线网格中，默认情况下，网格 AP 会自动连接到数据吞吐量最大的网格节点（网格 AP 或根 AP）上。此过程称为智能上行链路选择。

如果要构建网格或强制实现某种拓扑，则必须禁用“智能上行链路选择”，并手动设置 AP 可以连接的网格节点。

图 6-6 将“上行链路选择”设置为“手动”

要手动设置 AP 的网格上行链路

步骤 1 在ZD1000/3000 Web界面上，单击“配置”选项卡。

步骤 2 在菜单中，单击“接入点”。

步骤 3 在“接入点”表中，找到要限制的AP，然后单击“操作”列下的“编辑”。此时将在选定内容下方显示编辑表。

步骤 4 单击“高级选项”>“上行链路选择”，选中“手动”复选框。将在该复选框下方显示网格中的其他AP。

步骤 5 只要某个AP可用作当前AP的上行链路，就选中其对应的复选框。

注意

如果将 AP 的“上行链路选择”设置为“手动”，并且选定的上行链路 AP 处于关闭状态或不可用，“监控”>“接入点”页面上的 AP 状态将显示为“独立的网格接入点”。

步骤 6 单击“确定”保存设置。

6.7 对独立的网格接入点进行故障排除

独立的网格接入点是指曾由 ZD1000/3000 管理但现在无法连接的 AP。这些 AP 已接入并运行，并且持续搜索网格上行链路，却无法连接到任何根 AP。可以单击“监控”选项卡>“接入点”页面，检查网络中是否存在独立的网格接入点。

注意

网格实质上是动态的。要解决任何与网格有关的问题之前，需等待 15 分钟以使网格稳定下来。某些问题会在网格稳定后自动解决。

6.7.1 了解独立的网格接入点的状态

网格 AP 变成独立 AP 可能有 5 种原因。下表列出了可能显示在“监控”>“接入点”页面上所有可能的独立的网格接入点状态，并列出了可能原因以及解决问题的建议步骤。

表 6-5 独立的网格接入点的状态

状态	可能原因
手动上行链路选择中无 AP	已将上行链路选择设置为“手动”，但指定的上行链路 AP 都不可用或无法连接。 要解决此问题，可单击 ZD1000/3000 Web 界面上的“配置”>“接入点”页面，然后单击“智能选择”。
在限定跳数内无 AP	此 AP 无法在内部规定的跳数内找到其他 AP。跳数限制机制有助于网格 AP 保持理想的网络性能。 要解决此问题，可在此独立的网格接入点和最近的根 AP 之间添加其他有线 AP。
正在搜索上行链路	AP 仍在搜索上行链路。这只是一种临时状态，一般在 15 分钟内网格稳定后会自动消除。如果网络上存在大量 AP，那么 AP 可能需要等待更多的时间才能解决此问题。

状态	可能原因
配置错误	AP 试图建立网格上行链路但未成功。如果网络管理员最近更新了网格 SSID 和密码，可能是因为所做更改尚未正确传送到此 AP（例如，网络管理员更新网格 SSID 和密码时，此 AP 处于脱机状态）。 要解决此问题，按照6-13页中的“恢复独立的网格接入点”中的说明进行操作。
AP 的无线电类型不匹配	AP 无法找到具有同一无线电类型的其他网格 AP。在优科智能网格技术的当前版本中，具有同一无线电类型的 AP 才能通过网格相互连接。例如，802.11n 网格 AP 只能连接到其他 802.11n AP，而 802.11b/g 网格 AP 只能连接到其他 802.11b/g AP。 要解决此问题，在此 AP 附近布置具有同一无线电类型的其他有线 AP 或网格 AP。

6.7.2 恢复独立的网格接入点

要执行此过程，需要：

- 一台具有无线上网功能的笔记本计算机。如果在此计算机上运行 Windows XP，确保已安装 WPA2 补丁或 Service Pack 3。
- 最新的 AP 网格配置（下文介绍了获取此信息的步骤）。
- SSH 客户端，如 PuTTY 和 OpenSSH。

步骤 1：获取最新的 AP 网格配置

步骤 1 在ZD1000/3000 Web界面上，单击“监控”>“接入点”。

步骤 2 在“当前管理的接入点”下，查找状态消息“独立的网格接入点(Config error)”，然后单击同一行的“恢复”链接。

图 6-7 单击“恢复”以获取最新的 AP 网格配置

将显示一个介绍最新 AP 网格配置的页面。此页面上的网格信息包括：

- AP 的 MAC 地址
- 最新的网格 SSID（网格名称）
- 最新的网格 PSK（网格密码）

步骤 3　在纸上记下这些详细信息。下一步中将用到这些信息。

步骤 2：设置计算机以与 AP 进行无线连接

步骤 1　将以下IP地址设置分配给计算机：

- IP 地址：192.168.54.34
- 掩码：255.255.255.252

步骤 2　从计算机创建无线网络。如果运行的是Windows XP，可以使用“无线网络安装向导”创建无线网络。使用表 6-6中列出的设置配置无线网络。

表 6-6 使用以下设置配置无线网络

设置	说明
关联模式	WPA2
加密方法	AES
SSID	输入最新的 AP SSID（已在上一步获取）
PSK	输入最新的 AP PSK（已在上一步获取）

步骤 3：连接到 AP 并更新其 ESSID 和密码

步骤 1 创建无线网络后，将计算机放在离AP足够近的地方以便可以进行关联。

步骤 2 当计算机与AP建立关联后，启动SSH客户端，然后连接到192.168.54.33（AP的IP地址）。

步骤 3 使用登录ZD1000/3000 Web界面的用户名和密码通过SSH登录AP。

步骤 4 输入命令set meshcfg ssid "current_ssid"，其中current_ssid是网格当前使用的SSID。

步骤 5 输入命令set meshcfg passphrase "current_passphrase"，其中current_passphrase是网格当前使用的密码或PSK。

步骤 6 关闭SSH客户端。

现已恢复独立的网格接入点。稍后应该可以再次管理此接入点。至少等待 15 分钟使网格稳定下来，然后尝试通过 ZD1000/3000 管理此接入点。

7 管理员首选项配置

7.1 使用外部服务器验证管理员身份

ZD1000/3000 支持使用外部身份验证服务器（例如 RADIUS 或 Active Directory）验证管理员身份。每个管理员帐户一般有下列两种权限之一：

- 完全权限 – 可执行所有配置和管理任务
- 有限权限 – 只能执行监控任务

本部分简要说明如何将 ZD1000/3000 设置为使用外部身份验证服务器验证管理员身份。

第 1 步：在身份验证服务器上设置组属性

根据用户使用的是 RADIUS 还是 Active Directory，在身份验证服务器上设置组属性的步骤略有不同。

注意

欲了解详细步骤，可参考身份验证服务器附带的文档。

7.1.1 使用 RADIUS 进行身份验证

步骤 1 设置供应商属性。记住所设置的属性；在ZD1000/3000中创建管理员角色（参见步骤3）时需要输入这些信息。

- 优科专有属性
  - 供应商ID：25053
  - 供应商类别/属性编号：1 (Huawei-User-Groups)
  - 值格式：group_attr1,group_attr2group_attr3, ...

- Cisco 专有属性（如果用户网络使用的是 Cisco 访问控制服务器）
  - 供应商ID：9
  - 供应商类别/属性编号：1 (Cisco-AVPair)
  - 值格式：shell: roles="group_attr1 group_attr2 group_attr3 ..."

步骤 2 在RADIUS服务器上设置共享密钥。用户需要在ZD1000/3000 Web界面上输入这个共享密钥，以使ZD1000/3000能够与RADIUS服务器通信并通过身份验证。

使用 Active Directory 进行身份验证

建立两个组 – 一组是拥有完全权限的管理员，另一组是拥有有限权限的管理员。向这两个组中添加需要管理员访问权限的用户。一种添加方法是编辑每个用户的成员资料，然后添加用户所属的组。

记住设置的组名称；在 ZD1000/3000 中创建管理员角色（参见步骤 3）时需要输入这些信息。

第 2 步：将 ZD1000/3000 设置为使用身份验证服务器

步骤 1 登录到ZD1000/3000 Web界面。

步骤 2 单击“配置”选项卡，然后单击菜单上的“身份验证服务器”。

步骤 3 在“身份验证服务器”下，单击“新建”链接。将出现“新建”界面。

步骤 4 配置表 7-1中列出的设置。

表 7-1 身份验证服务器设置

设置	说明
名称	输入身份验证服务器的名称。这一步结束后所显示的身份验证服务器实际名称中会包含此名称和身份验证服务器类型。例如，如果在“名称”字段中输入 HEDY，并在“类型”选项中选择 RADIUS，将看到身份验证服务器的实际名称为 HEDY RADIUS。
类型	选择要使用的身份验证服务器类型。选项有 **Active Directory** 和 **RADIUS**。
IP 地址	输入身份验证服务器的 IP 地址。

设置	说明
端口	输入身份验证服务器的端口号： 如果使用 Active Directory，默认端口号为 389。 如果使用 RADIUS，默认端口号为 1812。
Windows 域名	如果选择 **Active Directory**，需要在“Windows 域名”字段中输入 Active Directory 域名。
共享密钥	如果选择 **RADIUS**，需要输入第 1 步中在 RADIUS 上设置的共享密钥，然后再输入一次进行确认。

步骤 5 单击“确定”。

身份验证服务器页面将刷新，表中显示所创建的服务器。
现在 ZD1000/3000 已设置为使用外部身份验证服务器进行管理员身份验证。

图 7-1 身份验证服务器页面

第 3 步：创建管理员角色

步骤 1　单击“配置”>“角色”。将显示“角色和策略”页面。

步骤 2　在“角色”下单击“新建”链接。将出现“新建”界面。

步骤 3　配置图 7-2中列出的设置。

图 7-2 管理员角色设置

设置	说明
名称	输入管理员角色的名称。例如，如果要创建拥有有限权限的管理员角色，可以输入 admin-limited。
说明	输入有关此管理员角色的说明。
组属性	输入第 1 步中在身份验证服务器上配置的组名或属性。要通过身份验证，在此框中输入的组名或属性必须与身份验证服务器上的组名或属性完全相同。
允许所有 WLAN	有两个选项：(1)允许访问所有 WLAN 和(2)指定 WLAN 访问。如果选择第二个选项，必须通过单击每个 WLAN 旁边的复选框指定 WLAN。此选项要求在设置该策略之前创建 WLAN。参见3-18页中的“新建 WLAN 供工作组使用”。
来宾通行证	如果希望此管理员角色拥有生成来宾通行证的权限，可启用此选项。
管理	选中“允许 **ZoneDirector** 管理”复选框，然后单击下列某个选项： • 完全权限（可执行所有配置和管理任务） • 有限权限（只能监控和查看运行状态）

注意

如果未选中“允许 ZoneDirector 管理”复选框，即使所有其他设置都正确，分配了此角色的管理员仍无法登录到 ZD1000/3000。

步骤 4 单击“确定”保存更改。

管理员角色创建成功。

图 7-3 “角色和策略”页面

第 4 步：测试身份验证设置

执行这一步可确保 ZD1000/3000 能连接到身份验证服务器并检索每个用户帐户的组/属性。

步骤 1 单击“配置”选项卡，然后单击菜单上的“身份验证服务器”。

步骤 2 在“测试身份验证设置”部分，从“测试对象”下拉菜单中选择要使用的身份验证服务器。

步骤 3 在“用户名”和“密码”字段中，输入RADIUS或Active Directory用户名和密码。

步骤 4 单击“应用”。

如果 ZD1000/3000 可以连接到该身份验证服务器并检索配置的组/属性，则会在页面底部显示相关信息。下面是 ZD1000/3000 成功使用此服务器进行身份验证时显示的示例消息：

Success! Groups associated with this user are "{group_name}". This user will be assigned a role of {role}

第 5 步：指定要使用的身份验证服务器

步骤 1 单击“管理”选项卡，然后单击菜单上的“首选项”。

步骤 2 在“管理员名称/密码”下选择“用身份验证服务器进行身份验证”。

步骤 3 从下拉菜单中选择用来验证管理员身份的身份验证服务器的名称。下拉菜单中显示的身份验证服务器名称与“配置”>“身份验证服务器”页面上显示的服务器名称相同。

步骤 4 确保选中“如果失败，请重新输入管理员名称/密码”复选框。选中此复选框可确保在身份验证服务器不可用时，管理员仍然能够登录到ZD1000/3000 Web界面。

步骤 5 如果需要，可以更改管理员名称和密码。

步骤 6 单击“应用”。

恭喜！您已将 ZD1000/3000 设置为使用外部服务器验证管理员身份。拥有管理员权限的用户每次登录到 ZD1000/3000 Web 界面时，系统都会记录一个事件。下面是用户将看到的事件详细信息示例：

Admin [user_name] login (authenticated by {Authentication Server} with {Role})。

7.2 更改 ZD1000/3000 管理员用户名和密码

ZD1000/3000 管理员登录密码一般需要每月更改一次，但管理员用户名仅在必要时更改。

注意

如果已选择使用外部服务器进行身份验证，并且禁用了“如果失败，请重新输入管理员名称/密码”复选框，将无法编辑用户名和密码。要编辑用户名和密码，需要执行以下步骤:

步骤 1 选中“如果失败，请重新输入管理员名称/密码”复选框以激活用户名和密码框。

步骤 2 更改用户名和密码。

步骤 3 取消选中“如果失败，请重新输入管理员名称/密码”复选框。

步骤 4 单击“应用”保存更改。

要编辑或替换当前名称或密码：

步骤 1　单击“管理”>“首选项”。将显示“首选项”页面。

步骤 2　配置表 7-2中列出的设置。

表 7-2 管理员名称和密码设置

设置	说明
管理员名称	删除此字段中的文本并输入新管理员帐户名称（仅在通过 Web 界面登录 ZD1000/3000 时使用此名称。）
密码	删除此字段中的文本，然后输入要使用的密码。
确认密码	再次输入刚才输入的密码进行确认。

步骤 3 单击“应用”保存更改。这些更改将立即生效。

图 7-4 “首选项”页面

7.3 更改 Web 界面显示语言

用户可以根据自己的喜好随意更改 Web 浏览器使用的 Web 界面语言。默认语言是“英语”。

此更改仅影响 Web 界面的显示语言，不会修改操作系统或浏览器的设置（后者通过其他操作实现）。

步骤 1 单击“管理”>“首选项”。

步骤 2 当出现“首选项”页面时，打开“语言”菜单并选择要使用的语言。参见图 7-4。

注意

此操作仅影响 ZD1000/3000 Web 界面的显示，不会修改操作系统或 Web 浏览器的设置。

步骤 3　单击“应用”保存更改。这些更改将立即生效。

7.4 升级许可证

根据使用 ZD1000/3000 管理的优科接入点数量，用户可能需要升级许可证。通过 Web 界面加载许可证后，许可证会立即生效。

Web 界面上会显示当前许可证信息（说明、订单号和状态等）。

注意

导入许可证后，系统不会重启。

要导入新许可证文件：

步骤 1　单击“管理”>“许可证”。

步骤 2　单击Browse（浏览）找到许可证。

步骤 3　找到许可证并关闭Browse（浏览）窗口后，ZD1000/3000将立即验证并安装此许可证。

图 7-5 “许可证”页面

8 故障处理

8.1 用户登录失败

摘要：本节主要说明如何解决用户在配置其客户端以及登录 WLAN 时可能会遇到的问题。

在配置向导完成后，优科 ZoneDirector 将自动激活一个默认的 WLAN，该 WLAN 的主要特点是“零 IT”配置，它大大简化了配置工作和登录步骤，对于新用户来说非常实用。只有运行 Windows XP SP2/Vista，并且具有支持 WPA 的无线网络适配器的客户端才支持“零 IT”配置。

如果用户在登录配置“零 IT”设置的 WLAN 时失败，只有下面两个原因：

- 用户的客户端运行的是其它操作系统，或者运行的是 Windows XP/SP2 之前的版本。（其中包括 XP/SP1。）
- 用户客户端的无线网络适配器不支持WPA。

按照下面的顺序检查用户登录失败的原因：

步骤 1 如果客户端计算机上使用的是Windows XP SP2/Vista，检查无线网络适配器以验证是否支持WPA。

步骤 2 将客户端计算机的系统升级到Windows XP SP2/Vista，如果需要，请安装支持WPA的无线网络适配器。完成这些更改后，用户可以重新尝试“零IT”登录。

步骤 3 如果用户使用的是旧版Windows，或者使用的是其他操作系统，那么必须在网络配置中手动输入WPA密钥。

步骤 4 如果无法升级客户端操作系统，并且无线网络适配器只能使用WEP加密。需要经过两个步骤：

- ZoneDirector- [1]以网络管理员身份为非标准客户端连接创建一个补充 WLAN，[2]为此 WLAN 创建一个用户角色，[3]将该角色分配给受影响的用户帐户。
- 用户配置 – 在用户端网络配置中输入所需的 WEP 密钥。

在多数解决方案中，需要打开 Windows 控制面板并输入所提供的 WPA 密钥或 WEP 密钥（如果将默认 WLAN 修改为采用 WEP 加密，就必须向用户提供密钥）。一旦口令或密钥存储到客户端的 Windows 系统后，用户就可以登录 WLAN。

8.2 修复用户连接

如果有用户报告无法连接到 WLAN，可以使用下面介绍的方法来解决。基本方法是将该用户从 ZoneDirector 的“活动的客户端”表中删除，当用户连接自动更新后，前面的所有问题就可能消失。

诊断活动的用户连接

步骤 1　单击“监控”>“当前活动的客户端”。

步骤 2　出现“当前活动的客户端”页面后，在“客户端”表中找到有问题的客户端。

步骤 3　单击**Delete**（删除）。

该客户端将自动从 ZoneDirector 中注销。

一、两分钟后，该客户端会自动重新登录到 WLAN，此时“客户端”表将重新显示该客户端，用户以后遇到的问题就会比较少，甚至不会遇到任何问题。

图 8-1 “当前活动的客户端”页面

8.2.1 如果 WLAN 连接仍有问题

如果上面介绍的方法无法解决用户客户端的连接问题，可能需要指导用户重新设置 WLAN。这样就需要先删除用户后再新建用户记录（此期间，用户需要重复“新建用户连接”的两个登录过程，下载和安装新的 WLAN 配置）。

步骤 1 让用户断开WLAN连接，直到收到进一步的通知。

步骤 2 单击“配置”>“用户”。

步骤 3 出现“用户身份验证”功能后，在“内部用户数据库”表中找到并删除该用户。

步骤 4 为该用户创建新的用户帐户，然后通知该用户，并说明如何重新配置客户端并登录到WLAN。

完成上述步骤后，用户应该可以重新连接。如果问题仍然存在，可能是 Windows 或无线网络适配器有问题。

8.3 使用 SpeedFlex 测量无线网络吞吐量

SpeedFlex 是 ZoneDirector 中的一种无线性能工具，可用来测量无线客户端与关联接入点（AP）之间的下行吞吐量。进行现场勘验时，可以使用 SpeedFlex 来帮助确定 AP 在网络中相对于用户位置的最佳位置。

注意

运行SpeedFlex之前，先要在“配置”>WLAN>“编辑{WLAN 名称}”页面上禁用“来宾访问”和“无线客户端隔离”选项。同时启用这两个选项或仅启用其中一个之后，SpeedFlex 无线性能工具可能无法正常运行。例如，用户可能无法通过 http://{ZoneDirector-ip-address}/perf 网址访问 SpeedFlex，或者 SpeedFlex 可能提示用户在目标客户端上安装 SpeedFlex 应用程序，即使已经安装了该程序。

注意

下面介绍如何从 ZoneDirector Web 界面上运行 SpeedFlex 来测量无线客户端的吞吐量。有关用户如何从无线客户端运行 SpeedFlex 的说明，可参考8-7页中的“用户如何测量自己的无线吞吐量”。

从 Web 界面测量接入点或客户端的吞吐量

步骤 1 找到需要测试的接入点或无线客户端的MAC地址。

步骤 2 如果测试客户端吞吐量，需确保此无线客户端与要测试的接入点相关联。

步骤 3 登录到ZoneDirector Web界面。可以使用需要测试的无线客户端或另一台计算机登录到Web界面。

步骤 4 如果要测试接入点吞吐量，可单击“监控”>“接入点”。如果要测试客户端吞吐量，可单击“监控”>“当前活动的客户端”。

步骤 5 在接入点或客户端列表中，找到要测试的接入点或无线客户端的MAC地址，然后单击同一行上的SpeedFlex链接。此时将加载SpeedFlex Wireless Performance Test（SpeedFlex无线性能测试）界面，显示速度计以及要测试的接入点或客户端的IP地址。

注意

如果 ZoneDirector 无法确定要测试的无线客户端的 IP 地址（例如，如果此无线客户端使用的是静态 IP 地址），该客户端的 SpeedFlex 链接将不会显示在“当前活动的客户端”页面上。

步骤 6 如果要测试接入点吞吐量，可以选择同时测试Downlink（下行）和Uplink（上行）吞吐量。这两个选项都是默认选中。如果只想测试其中一项，可以不选中另一个选项的复选框。

步骤 7 单击**Start**（开始）按钮。

- 如果目标客户端没有安装 SpeedFlex，将显示一条消息，说明必须在此客户端上安装并运行 SpeedFlex，无线性能测试才可以继续进行。单击此消息的“确定”按钮，从 SpeedFlex 界面下载适当的 SpeedFlex 版本（Windows 版或 Mac 版），然后将其发送给客户端用户进行安装。在客户端上安装并运行 SpeedFlex 后，再次单击 Start（开始）继续进行无线性能测试。

当 SpeedFlex 生成流量来测量下行或上行吞吐量时，速度计下面将显示一个进度条。一项吞吐量测试通常运行 10-30 秒。如果测试的是 AP 吞吐量，并且同时选中了 Downlink（下行）和 Uplink（上行）两个选项，完成测试可能需要一分钟。

测试完成后，Start（开始）按钮下面将显示测试结果。显示的信息包括下行/上行吞吐量以及测试期间丢失数据包的百分比。

图 8-2 SpeedFlex 界面

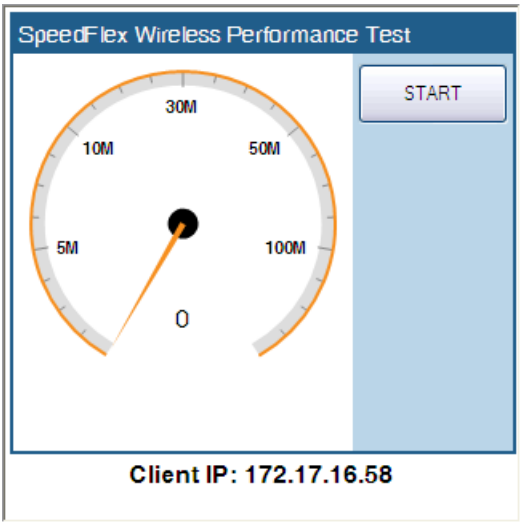


图 8-3 单击目标客户端操作系统的下载链接

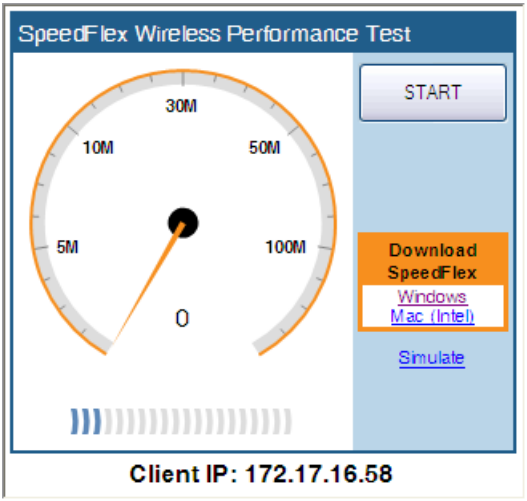


图 8-4 当 SpeedFlex 测量无线吞吐量时会显示进度条

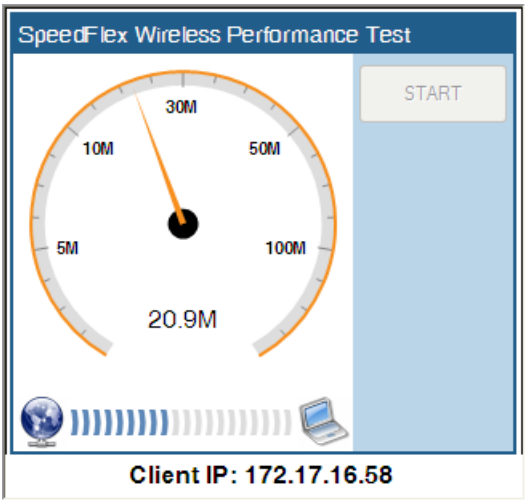
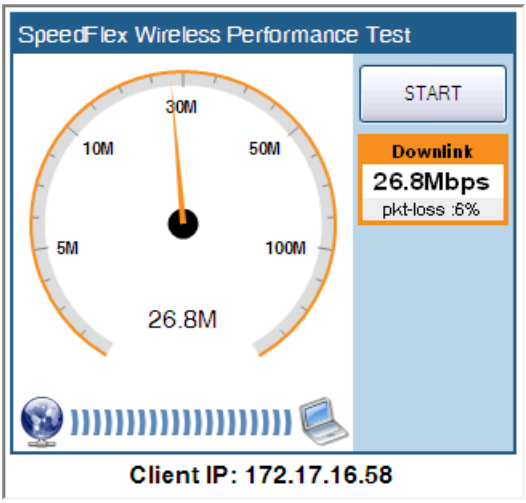


图 8-5 测试完成后，此工具将显示下行吞吐量和数据包丢失百分比



8.3.1 用户如何测量自己的无线吞吐量

ZoneDirector 还提供了一个不要求身份验证的 SpeedFlex 无线性能测试应用程序版本。此版本可通过以下站点下载：http://{ZoneDirector-ip-address}/perf

如果希望无线用户能够测量自己的无线吞吐量，可向他们提供此链接以及下面的说明。发送这些说明前，切记要用实际 ZoneDirector IP 地址替换{ZoneDirector-ip-address}变量。

如何测量无线连接速度

下面描述了 SpeedFlex 的使用方法，这是优科生产的一种无线性能测试工具，可用于测量无线连接到接入点的速度。

步骤 1 确保无线设备仅连接到无线网络。如果无线设备还连接到有线网络，则拔掉网络电缆。

步骤 2 启动Web浏览器，然后在地址栏或位置栏中输入以下网址：

http://{ZoneDirector-ip-address}/perf

浏览器中将加载 SpeedFlex 无线性能工具界面。

步骤 3 单击Start（开始）按钮。出现如下消息：

Your computer does not have SpeedFlex running. Click the OK button, download the SpeedFlex application for your operating system, and then double-click SpeedFlex.exe to start the application.（计算机没有运行 SpeedFlex。单击“确定”按钮下载与操作系统匹配的 SpeedFlex 应用程序，然后双击 SpeedFlex.exe 启动该应用程序。）

When SpeedFlex is running on your computer, click Start again to continue with the wireless performance test.（当 SpeedFlex 在计算机中运时，再次单击 Start（开始）继续进行无线性能测试。）

步骤 4 单击“确定”。SpeedFlex无线性能测试界面上将出现Windows和Mac（Intel）版SpeedFlex的下载链接。

步骤 5 单击与操作系统匹配的SpeedFlex版本，下载SpeedFlex文件，然后将其保存到计算机的硬盘上。

步骤 6 下载SpeedFlex文件后，找到该文件，然后双击启动SpeedFlex。将出现命令提示符窗口并显示如下消息：

Entering infinite loop. Enjoy the ride.（正在进入无限循环，可开始执行操作。）

这说明 SpeedFlex 已成功启动。保持命令提示符窗口处于打开状态。

步骤 7 在SpeedFlex Wireless Performance Test（SpeedFlex无线性能测试）界面上，再次单击Start（开始）按钮。当工具生成流量来测量从AP到客户端的下行吞吐量时，速度计下面将出现一个进度条。这项测试通常运行10到30秒。

测试完成后，Start（开始）按钮下面将出现测试结果。显示的信息包括无线设备和接入点之间的下行吞吐量（以 Mbps 表示）以及测试期间的数据包丢失分比。

如果数据包丢失百分比较高（说明无线连接质量较差），可尝试将无线设备移到其他位置，然后再次运行该工具。也可以与网络管理员联系寻求帮助。

8.4 调试性能不佳的网络

可以尝试使用下面的故障诊断处理方法来解决网络性能不佳的问题。

步骤 1 单击“监控”>“地图视图”。

步骤 2 查看可疑接入点的地图。如果可疑接入点很多，并且属于相邻的网络，则进行下一步。

步骤 3 单击“配置”>“接入点”。

步骤 4 编辑每个接入点，为每个设备分配不会干扰其他接入点的通道。

例如，如果有三个优科接入点，则打开每个接入点中的“无线电 B/G 通道”下拉列表并为每个接入点选择“1”、“6”和“11”。不管有多少 AP，都要确保每个接入点有固定通道且不与附近接入点的通道接近

8.5 启动射频扫描

此任务是对 ZoneDirector 中内置的自动射频扫描功能的补充。自动扫描每次评估一个频道，大约每 20 秒一次。要手工启动完整的射频扫描，一次性评估全部设备中所有频道，可执行以下步骤：

步骤 1 单击“管理”>“诊断”。

步骤 2 在出现的“诊断”页面上查找“手动扫描”选项，然后单击“扫描”。

注意

此操作将中断所有当前用户的活动网络连接。

步骤 3 打开“仪表板”或单击“监控”>“地图视图”查看扫描结果。其中包括可疑设备检测和最新覆盖范围计算结果。

图 8-6 “诊断”页面

8.6 调整射频管理和入侵防御选项

优科设备的这项功能为现有监控增加了自动调整的特点，使 ZoneDirector 可以有效调整接入点的特定设置和资源来提高覆盖性能。

步骤 1 单击“配置”>“服务”。

步骤 2 查看并更改下列射频管理选项（默认均为启用）：

- **自动发射功率调整**：如果启用此功能（默认设置）且接入点的发射功率设置为自动（默认设置），接入点将自动减小或增大发射功率以提供最佳的无线服务。
- **自动信道调整**：如果接入点在当前信道检测到干扰，就自动更换信道以避免干扰。

步骤 3 查看并更改下列入侵防御选项（均默认启动）：

- **防止过多的无线请求：**如果启用了此功能（默认设置），则会丢弃恶意攻击发出的过多802.11探测请求帧和管理帧。
- **暂时阻止身份验证重复失败的无线客户端：**如果启用此功能，任何身份验证重复失败的客户端都将被暂时加入到黑名单中。默认值是30秒。

步骤 4 单击“应用”保存设置。新设置将立即生效。

8.7 生成诊断文件

注意

除非技术支持人员要求，否则不要执行此操作。

如果需要生成并保存诊断文件，可执行以下步骤：

步骤 1 单击“管理”>“诊断”。

步骤 2 查看“调试日志”选项的设置，并根据要求从三个级别下拉列表中选择相应的诊断级别。（如果无需指定任何设置，可忽略这一步。）

- **APD**：有关无线接入点和 ZoneDirector 的信息
- **ACD**：有关无线客户端活动的信息
- **EMF**：有关 Web 界面操作的信息

步骤 3 如果更改了级别设置，则单击“应用”保存更改。

步骤 4 在“保存诊断信息”选项中，单击“保存诊断信息”。

步骤 5 出现“文件下载”对话框时，单击“保存”。

步骤 6 出现“另存为”对话框时，选择合适的目标文件夹，输入文件名，然后单击“保存”。

步骤 7 出现“下载完毕”对话框时，单击“关闭”。

保存文件后，可以用电子邮件将其发送给技术支持工程师。

注意

诊断文件已加密，只有优科的技术支持工程师才能解密此文件。

8.8 重新启动接入点

解决网络覆盖问题的一个实用方法是重新启动各个接入点。执行此操作的步骤如下：

步骤 1 单击“监控”>“接入点”。

步骤 2 在“接入点”页面上的接入点摘要表中查找具体接入点。

“状态”列应显示“已连接”。

步骤 3 单击“重新启动”。“状态”列会显示“已断开连接”以及ZoneDirector上次与接入点通信的日期和时间。

在重新启动完成且优科 ZoneDirector 重新检测到该活动的接入点后，接入点状态将恢复到“已连接”状态。

8.9 重新启动 ZoneDirector

有三个重新启动选项:[1]断开和重新连接 ZoneDirector 的电源[2]本节将要描述的，同时重新启动 ZoneDirector 和所有接入点，和[3]重新启动接入点（“重新启动接入点”中有详细介绍。）

重新启动 ZoneDirector（和当前的所有活动接入点）

步骤 1 单击“管理”>“重新启动”。

步骤 2 出现“重新启动/关闭”功能时，单击“重新启动”。

此时将自动从 ZoneDirector 中注销。稍等片刻，当状态指示灯稳定发光时，便可重新登录 ZoneDirector。

图 8-7 “重新启动/关闭”页面