Dominion® KX II

KX2-116 KX2-216 KX2-416
KX2-132 KX2-232 KX2-432
KX2-464



用户指南

2.0 版

版权所有 © 2007 Raritan, Inc.

DKX2-0B-E

2007 年 5 月

255-62-4023-00

本页特意留空。

版权和商标信息

本文档包含受版权保护的专有信息。保留所有权利。未经 Raritan, Inc. 事先书面许可，不得对本文档的任何部分进行影印和复印或翻译为其它语言。

© 版权所有 2007 Raritan, Inc.，CommandCenter®、RaritanConsole、Dominion® 和 Raritan 徽标是 Raritan, Inc. 的商标或注册商标。保留所有权利。Java® 是 Sun Microsystems, Inc. 的注册商标。Internet Explorer 和 Active Directory 是 Microsoft® Corporation 的注册商标。Netscape® 和 Netscape Navigator 是 Netscape Communication Corporation 的注册商标。所有其它标记是其各自所属厂商的注册商标或商标。

© 版权所有 2007 GoAhead Software, Inc. 保留所有权利。

FCC 信息

该设备已经过测试，符合 FCC 规则第 15 部分中 A 类数字设备的限制。这些限制的目的在于为商业安装提供合理的保护，避免有害的干扰。该设备会产生、使用和辐射射频能量，如果不按照说明进行安装和使用，可能会对无线电通信造成有害干扰。在居住环境中使用该设备可能会造成有害干扰。

VCCI 信息（日本）

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

对于因意外、灾难、误用、滥用、非 Raritan 产品修改或其它除 Raritan 合理控制以外的事件所导致的或非正常操作条件下所造成的该产品的损害，Raritan 概不负责。

CE cULus LISTED 1F61 I.T.E.

如需在北美洲或南美洲获得帮助，请通过以下方式与 Raritan 技术支持团队联系：
电话：(732) 764-8886；传真：(732) 764-8887；电子邮件：tech@raritan.com

技术支持人员的工作时间是东部时间周一至周五，早 8 点到晚 8 点。

如需在其它国家/地区获得帮助，请参阅本指南最后一页，
了解所在国家/地区的 Raritan 办事处联系信息。

安全指导方针

为避免潜在的致命电击危险和可能给 Raritan 设备带来的损害，请遵循以下指导方针：

- 在任何产品线路连接中都不要使用 2 线电源线。
- 检测计算机和显示器的交流电源插座的正负极和接地是否正确。
- 计算机和显示器只使用接地的插座。使用后备式 UPS 时，应当切断计算机、显示器和设备的电源。

机架安装安全指导方针

在需要进行机架安装的 Raritan 产品中，请采取以下预防措施：

- 封闭式机架环境中的工作温度可能会高于室温。不要超过设备的最大额定环境温度（有关详细信息，请参阅附录 A：规格）。
- 确保机架环境空气流通良好。
- 小心安装机架中的设备，避免机械负载不均衡。
- 仔细连接设备与电源电路，避免电路过载。
- 将所有设备正确接地到分支电路，尤其是电源接线，如电源板（直接连接除外）。

目录

第 1 章：简介 1
Dominion KX II 概述 1
虚拟媒体 2
产品图片 3
产品功能 4
硬件 4
软件 4
术语 5
套装内容 5
用户指南 6
概要 6
章节内容预览 6
相关文档 6
第 2 章：入门 7
登录信息 7
默认 IP 地址 7
支持的操作系统（客户机） 7
支持的浏览器 7
支持的操作系统和 CIM（目标服务器） 8
第 3 章：安装和配置 9
概要 9
第 1 步：配置目标服务器 9
视频分辨率 9
桌面背景 10
鼠标设置 10
操作系统鼠标和视频设置 10
第 2 步：配置网络防火墙设置 15
第 3 步：连接设备 16
第 4 步：Dominion KX II 初始配置 18
更改默认密码 18
设定 IP 地址 19
为目标服务器命名 20
指定电源自动检测 20
CC-SG 用户注意事项 21
远程认证 22
支持的协议 22
认证与授权 23
用户、组和访问权限 24
概要 24
用户 24
组 24
用户与组之间的关系 24
第 4 章：连接到 Dominion KX II 25
用户界面 25
KX II 本地控制台—KX II 设备 25
KX II 远程控制台—KX II 设备 25
多平台客户端 (MPC) – KX I 和 KX II 设备 26
Raritan Remote Client (RRC) - 仅针对 KX I 设备 26
语言支持 27
语言支持注意事项 27
Java Runtime Environment (JRE) 27
启动 KX II 28
KX II 控制台布局 29
KX II 控制台导航 30
注销 30
KX II 控制台菜单树 31

管理收藏夹 32
“管理收藏夹”菜单 33
收藏列表 34
发现设备—本地子网 36
发现设备 - KX 子网 37
添加新收藏 38

第 5 章：访问目标服务器 39
“端口访问”页 39
“端口操作”菜单 40
连接到目标服务器 41
在目标服务器之间切换 41
断开目标服务器的连接 41
对目标服务器进行电源控制 42
实现目标服务器的电源循环 42
接通目标服务器的电源 42
断开目标服务器的电源 42

第 6 章：虚拟 KVM 客户机 43
选项 44
菜单树 44
工具栏 44
鼠标指针同步 45
“连接”菜单 46
“属性”对话框 46
连接信息 48
退出 48
“键盘”菜单 49
发送 Ctrl+Alt+Delete 49
键盘宏 49
“视频”菜单 53
刷新屏幕 53
自动感应视频设置 53
校准颜色 53
视频设置 54
“鼠标”菜单 56
同步鼠标 56
单鼠标光标 56
标准 57
智能 57
绝对 57
虚拟媒体 57
“工具”菜单 58
选项 58
“视图”菜单 59
查看工具栏 59
缩放 59
目标屏幕分辨率 59
“帮助”菜单 59
关于 Raritan 虚拟 KVM 客户机 59

第 7 章：虚拟媒体 61
概要 61
使用虚拟媒体的先决条件 62
使用虚拟媒体 62
打开 KVM 会话 63
连接到虚拟媒体 63
本地驱动器 63
CD-ROM/DVD-ROM/ISO 映像 64
断开虚拟媒体 65
文件服务器设置（仅针对文件服务器 ISO 映像） 66

第 8 章：用户管理 67
用户列表 68
添加新用户 69
修改现有用户 70
用户组列表 71
添加新用户组 72
设置权限 73
设置端口权限 73
基于组的 IP ACL（访问控制列表） 74
修改现有用户组 76
更改密码 78
认证设置 79
实现 LDAP 远程认证 81
实现 RADIUS 远程认证 83

第 9 章：设备管理 85
网络设置 86
网络基本设置 87
其它网络设置 88
LAN 接口设置 89
日期/时间设置 91
事件管理 93
事件管理 – 设置 93
事件管理 – 目标 95
SNMP 代理配置 96
SNMP Trap 配置 97
“电源设置”页 98
“端口配置”页 99
电源控制 100
连接电源板 100
命名电源板（电源板的“端口”页） 101
将目标服务器关联到插座（“端口”页） 102

第 10 章：安全设置 105
安全设置 106
登录限制 107
复合密码 107
用户阻止 108
加密与共享 109
IP 访问控制 111

第 11 章：维护 113
审计日志 114
设备信息 115
备份和恢复 116
CIM 升级 118
固件升级 119
升级报告 121
重新引导 122

第 12 章：诊断 123
“诊断”菜单 123
“网络接口”页 124
“网络统计信息”页 125
“Ping 主机”页 127
“跟踪到主机的路由”页 128
KX 诊断 129

第 13 章：KX II Local Console 131
KX II Local Console 131
实际连接 131
“复位”按钮 132
启动 KX II Local Console 133
KX II Local Console 界面 133
访问目标服务器 134
本地端口管理 136
本地端口设置（仅限 KX II Local Console） 136
出厂复位（仅限 KX II Local Console） 138

第 14 章：取消对 CC 的管理 141
概要 141
从 CC-SG 管理中删除 Dominion KX II 141

附录 A：规格 143
远程连接 144
KVM 属性 144
使用的 TCP 和 UDP 端口 145
目标服务器连接距离和视频分辨率 146

附录 B：更新 LDAP 架构 147
返回用户组信息 147
从 LDAP 147
从 Microsoft Active Directory 147
设置注册表以允许将操作写入架构 147
创建新属性 148
向类添加属性 148
更新架构高速缓存 149
编辑用户成员的 RCI 用户组属性 149

附录 C：常见问题解答 151
一般性问题 151
远程访问 152
通用虚拟媒体 154
以太网和 IP 网络 155
服务器 157
安装 158
本地端口 160
电源控制 161
可伸缩性 162
计算机接口模块 (CIM) 163
安全性 164
易管理性 165
其它问题 166
疑难排解 167

插图

图 1：Dominion KX II 配置 1
图 2：Dominion KX2-116 3
图 3：Dominion KX2-432 3
图 4：Dominion KX II CIMs：D2CIM-VUSB（左），D2CIM-PWR（右） 3
图 5：术语和拓扑 5
图 6：Solaris 鼠标配置 13
图 7：Dominion KX II 连接 16
图 8：网络设置 19
图 9：端口配置 20
图 10：认证/授权流程图 23
图 11：Dominion KX II 远程控制台登录页 28
图 12：KX II 远程控制台主页 29
图 13：KX II 本地控制台主页 29
图 14：菜单层次结构示例（痕迹导航） 30
图 15：KX II 控制台菜单树（本地和远程） 31
图 16：收藏设备（边栏） 32
图 17：“管理收藏夹”菜单 33
图 18：收藏列表 34
图 19：编辑（收藏信息） 35
图 20：发现设备 - 本地子网 36
图 21：发现设备 - KX 子网 37
图 22：添加新收藏 38
图 23：端口访问 39
图 24：“端口操作”菜单 41
图 25：“端口操作”菜单（电源选项） 42
图 26：“虚拟 KVM 客户机”窗口 43
图 27：虚拟 KVM 客户机菜单树 44
图 28：双鼠标光标 45
图 29：“属性”对话框 46
图 30：连接信息 48
图 31：键盘宏 49
图 32：添加键盘宏 50
图 33：键盘宏示例 51
图 34：“键盘”菜单中的“新建宏” 51
图 35：视频设置 54
图 36：单鼠标光标消息 56
图 37：（工具）选项 58
图 38：虚拟媒体连接 61
图 39：打开 KVM 会话 63

图 40：映射虚拟媒体驱动器 63
图 41：映射虚拟媒体 CD/ISO 映像 64
图 42：文件服务器设置 66
图 43：用户管理菜单 67
图 44：用户列表 68
图 45：“用户”页 69
图 46：用户组列表 71
图 47：“组”页 72
图 48：基于组的 IP 访问控制列表 74
图 49：IP ACL 示例 75
图 50：修改组 76
图 51：更改密码 78
图 52：认证设置 79
图 53：认证设置 (LDAP) 81
图 54：认证设置 (RADIUS) 83
图 55：“设备设置”菜单 85
图 56：网络设置 86
图 57：网络设置（网络基本设置） 87
图 58：网络设置（网络杂项设置） 88
图 59：网络设置（LAN 接口设置） 89
图 60：日期/时间设置 91
图 61：事件管理 – 设置 93
图 62：Syslog 配置 94
图 63：事件管理 – 目标 95
图 64：电源设置 98
图 65：端口配置 99
图 66：电源板连接 100
图 67：“端口”页（电源板） 101
图 68：“端口”页（KVM 端口） 102
图 69：“端口”页（D2CIM-VUSB 的目标服务器设置） 104
图 70：“安全”菜单 105
图 71：安全设置 106
图 72：安全设置（复合密码） 107
图 73：安全设置（用户阻止） 108
图 74：安全设置（加密与共享） 109
图 75：安全设置（加密模式警告消息） 109
图 76：IP 访问控制 111
图 77：“维护”菜单 113
图 78：审计日志 114
图 79：设备信息 115
图 80：备份/恢复 116

图 81：从 KX 闪存升级 CIM 118
图 82：固件升级 119
图 83：固件升级查看 120
图 84：固件升级成功 120
图 85：升级报告 121
图 86：重新引导 122
图 87：重新引导确认 122
图 88：“诊断”菜单 123
图 89：网络接口 124
图 90：网络统计信息（统计信息） 125
图 91：网络统计信息（接口） 125
图 92：网络统计信息（路由） 126
图 93：Ping 主机 127
图 94：跟踪到主机的路由 128
图 95：KX 诊断 129
图 96：诊断脚本 130
图 97：文件下载 130
图 98：Dominion KX II Local Console 131
图 99：Dominion KX II 上的本地面板 131
图 100：“复位”按钮（设备背面） 132
图 101：Local Console 端口访问 134
图 102：本地端口设置 136
图 103：出厂复位（仅限 Local Console） 138
图 104：“设备由 CC-SG 管理”消息 141
图 105：从 CC-SG 管理中删除 141
图 106：确认取消 CC 的管理 142
图 107：设备已从 CC 管理中取消 142
图 108：创建新属性 148
图 109：向类添加属性 149
图 110：ADSI 编辑 149
图 111：用户属性 150
图 112：编辑属性（将用户添加到 KX II 组） 150

第 1 章：简介

Dominion KX II 概述

Dominion KX II 是一个安全的企业级数字 KVM（键盘、视频、鼠标）切换器，提供了 BIOS（及更高）级访问，以及在全球任何地方通过 Web 浏览器控制多达 64 台服务器的功能。在机架本地，Dominion KX II 可以通过一套键盘、显示器及鼠标，为多达 64 台服务器及其它 IT 设备提供 BIOS 等级的控制和操作。利用 Dominion KX II 集成的远程访问功能，可以通过 Web 浏览器对服务器进行相同级别的控制。

Dominion KX II 可使用标准 UTP (Cat 5/5e/6) 线缆轻松安装。其高级功能包括虚拟媒体、128 位加密、双电源、远程电源控制、双以太网、LDAP、RADIUS、Active Directory、Syslog 集成和 Web 管理。通过这些功能，您可以随时随地获得更长的工作时间、更高的效率以及滴水不漏的安全性。

Dominion KX II 产品可作为独立的设备使用，无需依赖中央管理设备。对于大型数据中心和企业而言，可以使用 Raritan 的 CommandCenter Secure Gateway (CC-SG) 管理设备，将众多的 Dominion KX II 设备（以及用于远程串口控制台访问的 Dominion SX 设备和用于远程办公室/分支机构管理的 Dominion KSX）集成到*单个*逻辑解决方案中。

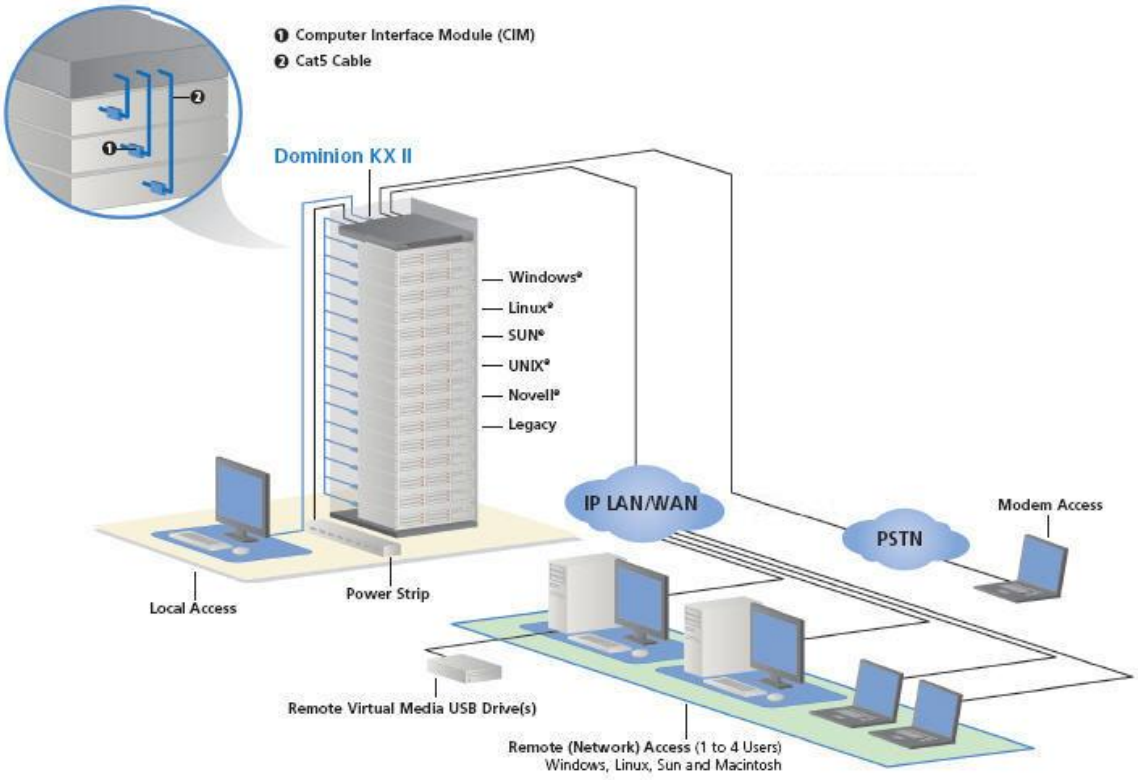


图 1：Dominion KX II 配置

虚拟媒体

所有型号的 Dominion KX II 都支持虚拟媒体。虚拟媒体的优势在于可以在目标服务器上安装远程驱动器/媒体，以支持软件安装、远程开机和诊断，现在所有型号的 Dominion KX II 都提供了该功能。

每个 Dominion KX II 都配备有虚拟媒体，可使用各种各样的 CD、DVD、USB、内部与远程驱动器和映像执行远程管理任务。与其它解决方案不同，Dominion KX II 还支持硬盘驱动器和远程安装映像的虚拟媒体访问，具有更高的灵活性和效率。

虚拟媒体会话使用 128 位 AES 或 RC4 加密方法保护。

对于支持 USB 2.0 接口的目标服务器，新的 D2CIM-VUSB CIM（计算机接口模块）支持其虚拟媒体会话。该新的 CIM 还支持 Absolute Mouse Synchronization™（绝对鼠标同步）以及远程固件更新。

产品图片



图 2：Dominion KX2-116



图 3：Dominion KX2-432



图 4：Dominion KX II CIMs：D2CIM-VUSB（左），D2CIM-PWR（右）

产品功能

硬件

- 采用 IP 信号 的 KVM 远程访问
- 1U 或 2U (KX2-464) 可机架安装，含托架
- 带故障切换的双电源；带电源故障警告的自动切换电源
- 16、32 或 64 个（KX2-464 上）服务器端口
- 支持多用户（1/2/4 个远程用户；1 个本地用户）
- UTP (Cat5/5e/6) 服务器线缆
- 带故障切换的双以太网端口 (10/100/1000 LAN)
- 可现场升级
- 用于机架内访问的本地用户端口
  - PS/2 键盘/鼠标端口
  - 用于支持的 USB 设备的 USB 2.0 端口，前面板上一个，后面板上三个
  - 与远程用户访问完全同步
  - 用于管理的本地图形用户界面 (GUI)
- 集中式访问安全性
- 集成的电源控制
- 用于指示双电源状态、网络活动和远程用户状态的 LED 指示灯
- 硬件复位按钮

软件

- 带 D2CIM-VUSB CIM 的虚拟媒体
- 带 D2CIM-VUSB CIM 的绝对鼠标同步
- 即插即用
- 基于 Web 的访问和管理
- 直观的图形用户界面 (GUI)
- 对完整的 KVM 信号（包括视频和虚拟媒体）进行 128 位加密
- LDAP、Active Directory、RADIUS 或内部认证和授权
- DHCP 或固定 IP 地址
- SNMP 和 Syslog 管理
- 电源控制与服务器直接关联，以防出错
- 与 Raritan 的 CommandCenter Secure Gateway (CC-SG) 管理设备集成
- 用于从 CC-SG 控制中删除设备的 CC 暂停管理功能

术语

对于 Dominion KX II 典型配置中的组件，本手册使用以下术语：

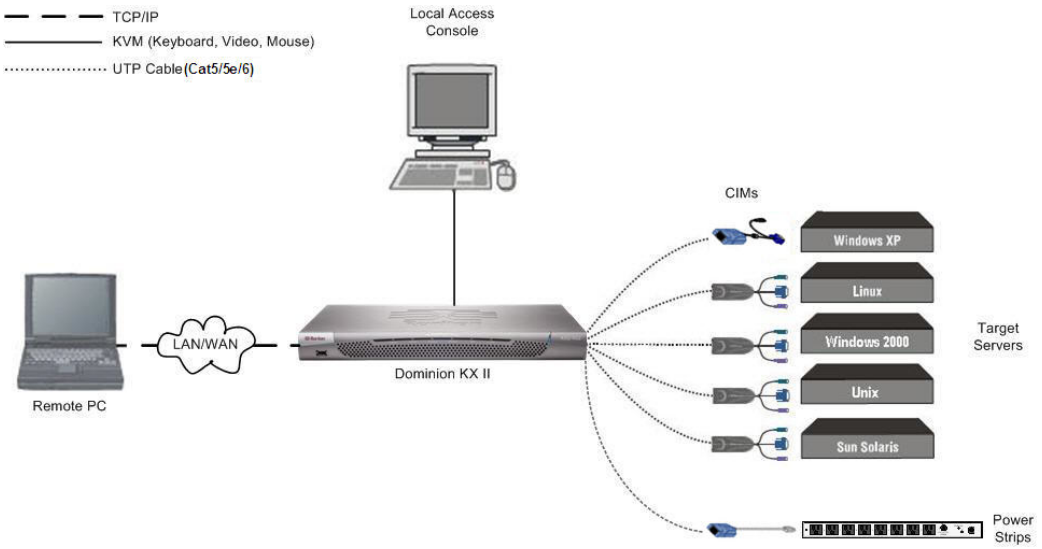


图 5：术语和拓扑

远程 PC（客户机）	用于访问和控制连接到 Dominion KX II 的目标服务器的联网计算机。有关 Dominion KX II 远程支持的操作系统列表，请参阅支持的操作系统（客户机）。
本地访问控制台（客户机）	与 Dominion KX II 直接相连以在本地（直接在机架本地，而不是通过网络）控制目标服务器的可选用户控制台（包括键盘、鼠标和多同步 VGA 显示器）。
CIM（计算机接口模块）	连接每台目标服务器和 Raritan 电源板的硬件保护装置。可用于所有支持的操作系统。有关 Dominion KX II 支持的 CIM 的信息，请参阅支持的 CIM。
目标服务器	通过 Dominion KX II 远程访问的带显卡和用户界面（如 Windows®、Linux®、Solaris™ 等）的服务器。有关支持的操作系统和 CIM 的列表，请参阅支持的操作系统和 CIM（目标服务器）。
电源板	通过 Dominion KX II 远程访问的 Raritan 电源板。

套装内容

每个 Dominion KX II 在交付时均为采用标准 1U（KX2-464 为 2U）19 英寸机架的完全配置的独立产品。每个 Dominion KX II 设备均附带以下内容：

(1) Dominion KX II 设备
(1) Dominion KX II 快速安装和设置指南
(1) Raritan 用户手册 CD-ROM
(1) 机架安装工具包
(2) 交流电源线
(1) Cat5 网线
(1) Cat5 交叉网线
(1) 4 个橡胶垫脚（用于桌面使用）
(1) 应用程序说明
(1) 质保卡

用户指南

概要

Dominion KX II 用户指南提供了有关安装、设置及配置、访问目标服务器和电源板，使用虚拟媒体，管理用户和安全性，以及维护和诊断 Dominion KX II 的信息。

本用户指南专门针对 Dominion KX II（2.0 版），有关 1.4 版的信息，请参阅“Dominion KX 1.4 用户指南”(Dominion KX 1.4 User Guide)。

章节内容预览

本用户指南的组织结构如下：

- 第 1 章，*简介*。概要、功能、术语和套装内容。
- 第 2 章，*入门*。登录信息；默认 IP 地址；支持的操作系统、浏览器和 CIM。
- 第 3 章，*安装和配置*。目标服务器配置；防火墙设置；物理设备连接；KX II 设备初始配置；远程认证；以及用户、组和访问权限。
- 第 4 章，*连接到 Dominion KX II*。用户界面；启动 KX II 远程控制台；Dominion KX II 收藏夹。
- 第 5 章，*访问目标服务器*。访问、控制目标服务器以及在目标服务器之间切换。
- 第 6 章，*虚拟 KVM 客户机*。目标服务器控制、鼠标指针同步、键盘宏和视频设置。
- 第 7 章，*虚拟媒体*。虚拟媒体配置和访问。
- 第 8 章，*用户管理*。用户和组管理、密码、基于组的 IP 访问控制和认证设置。
- 第 9 章，*设备管理*。网络设置、日期/时间、事件管理、电源设置、端口配置和电源控制。
- 第 10 章，*安全性设置*。安全性设置和 IP 访问控制。
- 第 11 章，*维护*。审计日志；设备信息；备份和恢复；固件和 CIM 升级；重新引导。
- 第 12 章，*诊断*。网络接口、网络统计信息、ping 主机、跟踪主机路由和 KX 诊断。
- 第 13 章，*KX II 本地控制台*。启动 KX II 本地控制台、访问目标服务器和本地端口管理。
- 第 14 章，*CC 非托管*。从 CC-SG 控制中删除 KX II。
- 附录 A，*规格*。物理规格、所用端口、目标服务器连接距离和视频分辨率
- 附录 B，*更新 LDAP 架构*。更新 LDAP 架构（针对有经验的用户）。
- 附录 C，*常见问题解答*。一般性问题、远程访问、通用虚拟媒体、以太网及 IP 网络、服务器、安装、本地端口、电源控制、可伸缩性、计算机接口模块 (CIM)、安全性、易管理性、其它杂项和疑难排解。

相关文档

有关 Raritan Multi-Platform Client (MPC) 的详细信息，请参阅“Raritan Multi-Platform Client (MPC) 和 Raritan Remote Client (RRC) 用户指南”(Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide)。

有关整个 Raritan 产品线的详细信息，请参阅“Raritan 用户手册和快速设置指南 CD ROM”或 Raritan 的网站：http://www.raritan.com/support/productdocumentation。

第 2 章：入门

登录信息

- 默认的 Dominion KX II 登录用户名是 **admin**，默认密码是 **raritan**。该用户具有管理权限。
- 密码区分大小写，输入时大小写必须与创建时的组合形式完全一致。例如，默认密码 **raritan** 必须全部以小写字母输入。
- 第一次启动 Dominion KX II 时，需要更改默认密码。

提示：出于备份和业务连续性的目的，强烈建议您创建一个备份管理员用户名及密码，并将该信息置于安全之处。

默认 IP 地址

Dominion KX II 附带有默认的 IP 地址：192.168.0.192。

支持的操作系统（客户机）

Dominion KX II 远程控制台、Virtual KVM Client™（虚拟 KVM 客户机）和多平台客户机 (MPC) 上支持以下操作系统：

客户机操作系统	客户机上是否支持虚拟媒体 (VM)
Windows XP	是
Windows 2000 SP4	是
Windows Vista	是
Red Hat Linux 9.0	是，ISO 映像位于本地，从 KX 直接安装远程文件服务器
Red Hat Enterprise Workstation 3.0 和 4.0	是，ISO 映像位于本地，从 KX 直接安装远程文件服务器
SUSE Linux Professional 9.2 和 10	是，ISO 映像位于本地，从 KX 直接安装远程文件服务器
Fedora™ Core 5 及更高版本	是，ISO 映像位于本地，从 KX 直接安装远程文件服务器
Mac®	否
Solaris	否

支持的浏览器

Dominion KX II 支持以下浏览器：

- Internet Explorer 6 和 7
- Firefox® 1.5 和 2.0
- Mozilla® 1.7
- Safari 2.0

支持的操作系统和 CIM（目标服务器）

除了支持新的 Dominion KX II D2CIM，还支持大多数 Paragon® 和 Dominion KX I CIM。下表显示了支持的目标服务器操作系统、CIM、虚拟媒体和鼠标模式：

目标服务器	支持的 CIM			VM	鼠标模式		
	PARAGON CIM	DOMINION KX I DCIM	DOMINION KX II D2CIM		AM	IM	SM
Windows XP Windows 2000 Windows 2000 Server Windows 2003 Server Windows Vista	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓	✓	✓
Red Hat Linux 9.0 Red Hat Enterprise Workstation 3.0 和 4.0	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB（不包括 Red Hat Enterprise Workstation 3.0）	✓			✓
SUSE Linux Professional 9.2 和 10	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD P2CIM-USBG2 UKVMC USKVMC P2CIM-PS2DUAL	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Fedora Core 3 及更高版本	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD P2CIM-USBG2 UKVMC USKVMC P2CIM-PS2DUAL	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Mac OS	P2CIM-AUSB UUSBPD P2CIM-USBG2	DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓		
Dominion KX I 中支持的所有 Solaris 操作系统	USKVMC P2CIM-SUN P2CIM-SUSB	DCIM-SUN DCIM-SUSB					✓
IBM AIX	P2CIM-PS2 P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
HP UX	P2CIM-PS2 P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
远程电源板			D2CIM-PWR				
串口设备	P2CIM-SER P2CIM-SER-EU AUATC						

图例：

- VM：虚拟媒体（仅针对 D2CIM-VUSB）
- AM：绝对鼠标同步（仅针对 D2CIM-VUSB）
- IM：智能鼠标模式
- SM：标准鼠标模式
- ✓: 支持

***注意：** Sun (Solaris) 目标服务器不支持 D2CIM-VUSB。*

第 3 章：安装和配置

概要

本节简要概述安装过程。本章后面的部分将详细介绍每个步骤。

安装和配置 Dominion KX II：

1. 配置目标服务器。
2. 配置网络防火墙设置。
3. 连接设备。
4. 配置 Dominion KX II 设备。

第 1 步：配置目标服务器

目标服务器是通过 Dominion KX II 访问和控制的计算机。在安装 Dominion KX II 之前，应当先配置*所有*目标服务器以确保获得最佳性能。此配置仅适用于*目标服务器*，不适用于用于远程访问 Dominion KX II 的客户机工作站（远程 PC）。有关详细信息，请参阅第 1 章：简介，术语。

配置目标服务器：

- 检查视频分辨率。
- 检查桌面背景。
- 调整鼠标设置。
- 执行特定于操作系统的鼠标和视频配置。

视频分辨率

请确保 Dominion KX II 支持每台目标服务器的视频分辨率和刷新率，并且信号为*逐行扫描*。

支持的视频分辨率

Dominion KX II 支持以下分辨率：

640x350 @70 Hz	720x400 @85 Hz	1024x768 @90 Hz
640x350 @85 Hz	800x600 @56 Hz	1024x768 @100 Hz
640x400 @56 Hz	800x600 @60 Hz	1152x864 @60 Hz
640x400 @84 Hz	800x600 @70 Hz	1152x864 @70 Hz
640x400 @85 Hz	800x600 @72 Hz	1152x864 @75 Hz
640x480 @60 Hz	800x600 @75 Hz	1152x864 @85 Hz
640x480 @66.6 Hz	800x600 @85 Hz	1152x870 @75.1 Hz
640x480 @72 Hz	800x600 @90 Hz	1152x900 @66 Hz
640x480 @75 Hz	800x600 @100 Hz	1152x900 @76 Hz
640x480 @85 Hz	832x624 @75.1 Hz	1280x960 @60 Hz
640x480 @90 Hz	1024x768 @60 Hz	1280x960 @85 Hz
640x480 @100 Hz	1024x768 @70 Hz	1280x1024 @60 Hz
640x480 @120 Hz	1024x768 @72 Hz	1280x1024 @75 Hz
720x400 @70 Hz	1024x768 @75 Hz	1280x1024 @85 Hz
720x400 @84 Hz	1024x768 @85 Hz	1600x1200 @60 Hz

注意：*Composite Sync 和 Sync-on-Green 视频需要额外的适配器。*

桌面背景

为使带宽效率和视频性能达到最佳，运行图形用户界面（如 Windows、Linux、X-Windows、Solaris 和 KDE）的目标服务器需要进行配置。桌面背景并不需要完全是纯色的，但将照片或复杂的渐变作为桌面背景可能会使性能降低。

鼠标设置

Dominion KX II 可运行在以下多种鼠标模式下：

- 绝对鼠标同步（仅针对 D2CIM-VUSB）
- 智能鼠标模式（不使用动画鼠标）
- 标准鼠标模式

对于标准鼠标模式和智能鼠标模式，鼠标参数必须设置为特定值，本手册后面将就此进行介绍。对于绝对鼠标同步，无需更改鼠标参数。该模式需要使用 D2CIM-VUSB。在不同的目标操作系统上，鼠标配置也不同。有关详细信息，请参阅操作系统文档。

智能鼠标模式在大多数 Windows 平台上通常都运行良好。如果目标服务器设置为活动桌面，那么智能鼠标模式可能会产生无法预知的结果。有关智能鼠标模式的其它信息，请参阅“*Raritan Multi-Platform Client (MPC) 和 Raritan Remote Client (RRC) 用户指南*”*(Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide)*（*附录 B：智能鼠标同步条件*），可在 Raritan 网站 http://www.raritan.com/support/productdocumentation 或 Dominion KX II 附带的“Raritan 用户手册和快速设置指南 CD ROM”上找到它们。

操作系统鼠标和视频设置

本节提供了目标服务器上所用操作系统特定的视频模式和鼠标信息。

Windows XP/Windows 2003 设置

配置运行 Microsoft Windows XP/2003 的目标服务器：

1. 配置鼠标设置：
   a. 选择“开始”**(Start)** >“控制面板”**(Control Panel)** >“鼠标”**(Mouse)**。
   b. 打开“指针选项”**(Pointer Options)** 选项卡。在“动作”**(Motion)** 组中：
      - 将鼠标动作速度精确设置为中等速度。
      - 禁用“增强的指针精度”**(Enhanced pointer precision)** 选项。
      - 单击“确定”**(OK)**。
2. 禁用过渡效果：
   a. 从“控制面板”**(Control Panel)** 中选择“显示”**(Display)**。
   b. 打开“外观”**(Appearance)** 选项卡。
   c. 单击“效果”**(Effects)** 按钮。
   d. 清除“为菜单和工具提示使用下列过渡效果”**(Use the following transition effect for menus and tooltips)** 选项。
   e. 单击“确定”**(OK)**。
   f. 关闭控制面板。

注意：对于运行 Windows 2000 或 XP 的目标服务器，您可以创建一个只用于通过 Dominion KX II 进行远程连接的用户名。这样一来，您便可以使目标服务器较慢的鼠标指针运动/加速设置专门用于 Dominion KX II 连接。

Windows XP 和 2000 登录屏幕恢复到预设的鼠标参数，这些参数与为获得 Dominion KX II 最佳性能所建议的参数值是不同的。因此，对于这些屏幕而言，鼠标同步可能不是最优的。如果您方便调整 Windows 目标服务器上的注册表，可以使用 Windows 注册表编辑器更改以下设置 (HKEY_CURRENT_USER\Control Panel\Mouse)，以使登录屏幕获得更好的 Dominion KX II 鼠标同步：MouseSpeed = 0，MouseThreshold 1= 0，MouseThreshold 2 = 0。

Windows 2000 设置

配置运行 Microsoft Windows 2000 的目标服务器：

1. 配置鼠标设置：
   a. 选择“开始”**(Start)** >“控制面板”**(Control Panel)** >“鼠标”**(Mouse)**。
   b. 打开“动作”**(Motion)** 选项卡。
      - 将加速设置为“无”**(None)**。
      - 将鼠标动作速度精确设置为中等速度。
      - 单击“确定”**(OK)**。
2. 禁用过渡效果：
   a. 从“控制面板”**(Control Panel)** 中选择“显示”**(Display)**。
   b. 打开“效果”**(Effects)** 选项卡。
   c. 清除“为菜单和工具提示使用下列过渡效果”**(Use the following transition effect for menus and tooltips)** 选项。
   d. 单击“确定”**(OK)**。
   e. 关闭控制面板。

Windows Vista

配置运行 Microsoft Windows Vista 的目标服务器：

1. 配置鼠标设置：
   a. 选择“开始”**(Start)** >“设置”**(Settings)** >“控制面板”**(Control Panel)** >“鼠标”**(Mouse)**。
   b. 打开“指针选项”**(Pointer Options)** 选项卡。在“动作”**(Motion)** 组中：
      - 将鼠标动作速度精确设置为中等速度。
      - 禁用“增强的指针精度”**(Enhanced pointer precision)** 选项。
      - 单击“确定”**(OK)**。
2. 禁用动画和淡化效果：
   a. 从“控制面板”**(Control Panel)** 中选择“系统”**(System)** 选项。
   b. 选择“高级系统设置”**(Advanced system settings)**。将打开“系统属性”**(System Properties)** 对话框。

c. 打开“高级”**(Advanced)** 选项卡。

d. 在“性能”**(Performance)** 组中单击“设置”**(Settings)** 按钮。将打开“性能选项”**(Performance Options)** 对话框。

e. 在“自定义”**(Custom)** 选项下，清除以下复选框：

动画选项：	
	动画窗口中的控件和元素 (Animate controls and elements inside windows)
	在最大化和最小化时动画窗口 (Animate windows when minimizing and maximizing)
淡化选项：	
	在视图中淡入淡出或滑动菜单 (Fade or slide menus into view)
	在视图中淡入淡出或滑动工具条提示 (Fade or slide ToolTips into view)
	在单击后淡出菜单项 (Fade out menu items after clicking)

f. 单击“确定”**(OK)**。

g. 关闭控制面板。

Linux 设置

***注意：**以下设置仅针对标准鼠标模式。*

配置运行 Linux（图形用户界面）的目标服务器：

1. 配置鼠标设置：
   a. 选择“系统”**(System)** > “首选项”**(Preferences)** > “鼠标”**(Mouse)**。将打开“鼠标首选项”**(Mouse Preferences)** 对话框。
   b. 打开“动作”**(Motion)** 选项卡。
   c. 将“速度加速”**(Speed Acceleration)** 设置为 1。
   d. 将“拖放阈值”**(Drag & Drop Threshold)** 设置为 1。
2. 配置屏幕分辨率：
   a. 选择“系统”**(System)** > “首选项”**(Preferences)** > “屏幕分辨率”**(Screen Resolution)**。将打开“屏幕分辨率首选项”(Screen Resolution Preferences) 对话框。
   b. 选择 Dominion KX II 支持的“分辨率”**(Resolution)** 和“刷新率”**(Refresh Rate)**。

***注意：**在许多 Linux 图形环境中，可以使用命令 <**Ctrl**> <**Alt**> <+> 滚动浏览 XF86Config 文件中保持启用的所有可用分辨率，从而更改视频分辨率。*

配置运行 Linux（命令行）的目标服务器：

1. 将鼠标加速精确设置为 1，将阈值精确设置为 1。输入以下命令：**xset mouse 1 1**。要在登录时执行，必须这样设置。
2. 请确保运行 Linux 的每台目标服务器使用的是 Dominion KX II 支持的标准 VESA 分辨率和刷新率。
3. 还应当设置每台 Linux 目标服务器，以使消隐时间在 VESA 标准值的 +/- 40% 范围内。
   - 转到 Xfree86 配置文件 XF86Config。
   - 使用文本编辑器，禁用 Dominion KX II 不支持的所有分辨率。
   - 禁用虚拟桌面功能（Dominion KX II 不支持）。
   - 检查消隐时间（VESA 标准值的 +/- 40%）。
   - 重新启动计算机。

Red Hat 9 目标服务器注意事项

如果您使用 D2CIM-VUSB 在目标服务器上运行 Red Hat 9，并且遇到了与键盘和/或鼠标有关的问题，则您可以尝试另一种配置设置。

提示：即使操作系统是刚刚安装的，您可能也需要执行这些步骤。

配置使用 D2CIM-VUSB 的 Red Hat 9 服务器：

1. 找到系统中的配置文件（通常是 **/etc/modules.conf**）。
2. 使用您选择的编辑器，确保 **modules.conf** 文件中的 **alias usb-controller** 行如下所示：

```
alias usb-controller usb-uhci
```

***注意：**如果 /etc/modules.conf 文件中有另一行使用 usb-uhci，则必须将该行删除或注释掉。*

3. 保存该文件。
4. 为使更改生效，请重新引导系统。

Sun Solaris 设置

配置运行 Sun Solaris 的目标服务器：

将鼠标加速值精确设置为 1，将阈值精确设置为 1。该设置可通过以下方式进行：

- 从图形用户界面：

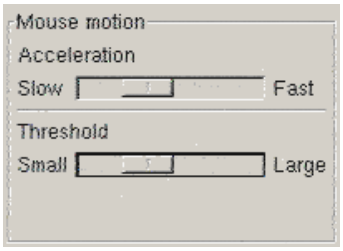


图 6：Solaris 鼠标配置

- 通过命令行：

```
xset mouse a t
```

（其中，“a”是加速，“t”是阈值。）

所有目标服务器必须配置为 Dominion KX II 所支持的某个显示分辨率。Sun 计算机支持的最常用的分辨率如下：

1024	x	768	@	60	Hz
1024	x	768	@	70	Hz
1024	x	768	@	75	Hz
1024	x	768	@	85	Hz
1152	x	900	@	66	Hz
1152	x	900	@	76	Hz
1280	x	1024	@	60	Hz

运行 Solaris 操作系统的目标服务器必须输出 VGA 视频（HV 同步，而非复合同步）。

将 Sun 显卡输出由复合同步更改为非默认的 VGA 输出：

1. 使用 **Stop+A** 命令下降到 bootprom 模式。
2. 使用以下命令更改输出分辨率：

```
setenv output-device screen:r1024x768x70
```

3. 使用 **boot** 命令重新引导服务器。

您还可以与 Raritan 销售代表联系，购买视频输出适配器：

如果计算机为：	请使用该视频输出适配器：
带复合同步输出的 Sun 13W3	APSSUN II Guardian 转换器
带复合同步输出的 Sun HD15	用于从 HD15 转换为 13W3 的 1396C 转换器，以及支持复合同步的 APSSUN II Guardian 转换器
带独立同步输出的 Sun HD15	APKMSUN Guardian 转换器

***注意：**某些标准的 Sun 背景屏幕在某些 Sun 服务器上可能不会准确地居中，而是带一个黑色边框。可以使用其它背景或在左上角放置一个浅颜色的图标。*

Apple Macintosh 设置

对于运行 Apple Macintosh 操作系统的目标服务器，首选的方法是使用 D2CIM-VUSB 和绝对鼠标同步。

***注意：**如果遇到问题，请启用“端口”(Port) 页上的“MAC 服务器的绝对鼠标缩放”(Absolute mouse scaling for MAC server) 选项。*

IBM AIX 设置

配置运行 IBM AIX 的目标服务器：

转到“样式管理器”**(Style Manager)**，单击“鼠标设置”**(Mouse Settings)**，并将“鼠标加速”**(Mouse acceleration)** 设置为 1.0，将“阈值”**(Threshold)** 设置为 3.0。

第 2 步：配置网络防火墙设置

要通过网络防火墙访问 Dominion KX II，防火墙必须允许通过 TCP 端口 5000 或您指定的其它端口进行通信。有关指定其它发现端口的详细信息，请参阅网络设置。

防火墙设置

要使用 DOMINION KX II 的功能：	防火墙必须允许通过该端口进行入站通信：
Web 访问功能	端口 443 - 用于 HTTPS 通信的标准 TCP 端口
将 HTTP 请求自动重定向至 HTTPS（即，使用户能键入更常用的“http://xxx.xxx.xxx.xxx”代替“https://xxx.xxx.xxx.xxx”）	端口 80 - 用于 HTTP 通信的标准 TCP 端口

第 3 步：连接设备

将 Dominion KX II 连接到电源、网络、本地 PC 和目标服务器。下图中的数字对应于介绍其连接的小节。

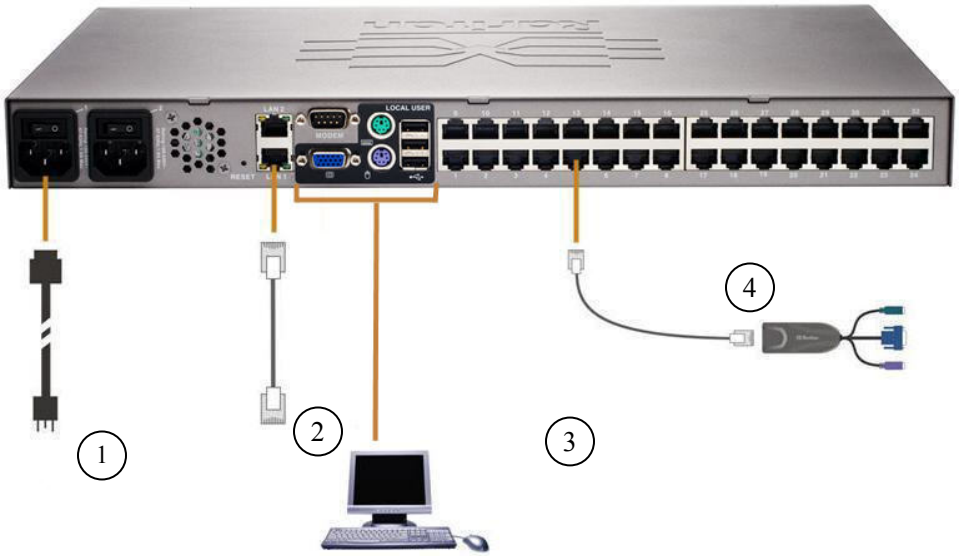


图 7：Dominion KX II 连接

1. 交流电源

连接电源：

1. 将附带的交流电源线接到 Dominion KX II 上，并插到交流电源插座上。
2. 为了实现双电源故障切换保护，请将附带的第二条交流电源线的一端连接到 Dominion KX II，将另一端插入与第一条电源线不同的电源插座中。

***注意：**如果只接一根电源线，则 Dominion KX II 前面板上的电源 LED 将显示红色，因为系统设置为自动检测双电源。有关关闭未使用电源的自动检测的信息，请参阅“电源设置”(Power Supply Setup) 页。*

---

2. 网络端口

Dominion KX II 提供了两个以太网端口用于故障切换（而非负载平衡）。默认情况下，只有 LAN1 处于活动状态，自动故障切换为禁用状态。当启用该功能时，如果 Dominion KX II 内部网络接口或与 Dominion KX II 相连的网络交换器变得不可用，将使用*相同的* IP 地址启用 LAN2。

连接网络：

1. 用附带的标准以太网线从标记为 LAN1 的网络端口连接到以太网交换器、集线器或路由器。
2. 使用可选的 Dominion KX II 以太网故障切换功能：
   - 用一根标准的以太网线从标记为 LAN2 的网络端口连接到以太网交换器、集线器或路由器。
   - 在“网络配置”**(Network Configuration)** 屏幕上启用自动故障切换（有关详细信息，请参阅网络设置、LAN 接口设置）。

仅当要将两个网络端口中的一个作为故障切换端口时，才使用两个端口。

---

3. 本地访问端口（本地 PC）

要在机架本地方便地访问目标服务器，可使用 Dominion KX II 本地访问端口。虽然本地端口是进行安装和设置所*必需的*，但在后续使用中是*可选的*。本地端口为管理和目标服务器访问提供了 KX II 本地控制台图形用户界面。

连接本地端口：

将多同步 VGA 显示器、鼠标和键盘分别连接到各自的本地用户端口（使用 PS/2 或 USB 键盘和鼠标）。

4. 目标服务器端口

Dominion KX II 使用标准的 UTP 线缆 (Cat5/5e/6) 连接每台目标服务器。有关详细信息，请参阅附录 A：规格。

将目标服务器连接到 Dominion KX II：

1. 使用适当的计算机接口模块 (CIM)。有关适用于各个操作系统的 CIM 的详细信息，请参阅支持的 CIM。
2. 将 CIM 的 HD15 视频连接器接到目标服务器的视频端口上。请确保目标服务器的视频已配置为支持的分辨率和刷新率。对于 Sun 服务器，还应确保目标服务器的显卡已设置为输出标准的 VGA（HV 同步），而不是复合同步。
3. 将 CIM 的键盘/鼠标连接器接到目标服务器的相应端口上。使用标准的直通 UTP (Cat5/5e/6) 线缆，将 CIM 连接到 Dominion KX II 设备背面的可用服务器端口上。

更改键盘布局代码（Sun 目标服务器）

如果您使用的是 DCIM-SUSB，而且希望将键盘布局更改为其它语言，那么可使用以下方法。

更改键盘布局代码（仅针对 DCIM-SUSB）：

1. 在 Sun 工作站上打开一个文本编辑器窗口。
2. 检查 **Num Lock** 键是否激活，并按键盘左侧的 **Ctrl** 键和 **Del** 键。**Caps Lock LED** 开始闪烁，表示 **CIM** 处于布局代码更改模式。
   文本窗口中显示：Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX)。
3. 键入所需的布局代码（例如，**31** 为日语键盘）。
4. 按 **Enter**。
5. 关闭设备并再次接通电源。DCIM-SUSB 将执行复位（电源循环）。
6. 使用 MPC，键入某些内容以检验字符是否正确。

第 4 步：Dominion KX II 初始配置

第一次接通 Dominion KX II 设备的电源时，您需要通过 KX II 本地控制台执行以下初始配置：

- 更改默认密码。
- 分配 IP 地址。
- 为目标服务器命名。
- 指定电源自动检测。

更改默认密码

Dominion KX II 附带有默认密码。*第一次启动 Dominion KX II 时，需要更改该密码。*

更改默认密码：

1. 使用设备背面的电源开关接通 Dominion KX II 的电源。请等候 Dominion KX II 设备启动。（启动完成后会发出“嘟嘟”的信号。）
2. 设备启动之后，连接到 Dominion KX II 本地端口的显示器上将显示 KX II 本地控制台。键入默认用户名 **(admin)** 和密码 **(raritan)**，然后单击“登录”**(Login)**。将显示“更改密码”**(Change Password)** 屏幕。
3. 在“旧密码”**(Old Password)** 字段中键入原来的密码 **(raritan)**。
4. 在“新密码”**(New Password)** 字段中键入新密码，然后在“确认新密码”**(Confirm New Password)** 字段中重新键入新密码。密码的长度最多为 64 个字符，可以包括英文字母数字字符以及这些步骤之后的表格中所列出的特殊字符。
5. 单击“应用”**(Apply)**。
6. 此时将收到密码更改成功的确认。单击“确定”**(OK)**。将显示“端口访问”**(Port Access)** 页。

注意：*还可以从 Raritan Multi-Platform Client (MPC) 更改默认密码。有关详细信息，请参阅“Raritan Multi-Platform Client (MPC) 和 Raritan Remote Client (RRC) 用户指南”(Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide)。*

有效的特殊字符

字符	说明	字符	说明
!	感叹号	:	冒号
"	双引号	;	分号
#	数字记号	=	等号
$	美元符号	>	大于号
%	百分号	?	问号
&	与号	@	at 符号
'	单引号	[	左中括号
(	左括号	\	反斜杠
)	右括号	]	右中括号
*	星号	^	脱字号
+	加号	_	下划线
,	逗号	`	重音符号
-	破折号	{	左大括号
.	句点	|	管道符号
/	斜杠	}	右大括号
<	小于号	~	波形符

设定 IP 地址

以下过程介绍如何使用“网络设置”(Network Settings) 页分配 IP 地址。有关该页的所有字段和操作的完整信息，请参阅网络设置。

1. 从 **KX II** 本地控制台中选择“设备设置”**(Device Settings) >** “网络设置”**(Network Settings)**。将打开“网络设置”(Network Settings) 页。

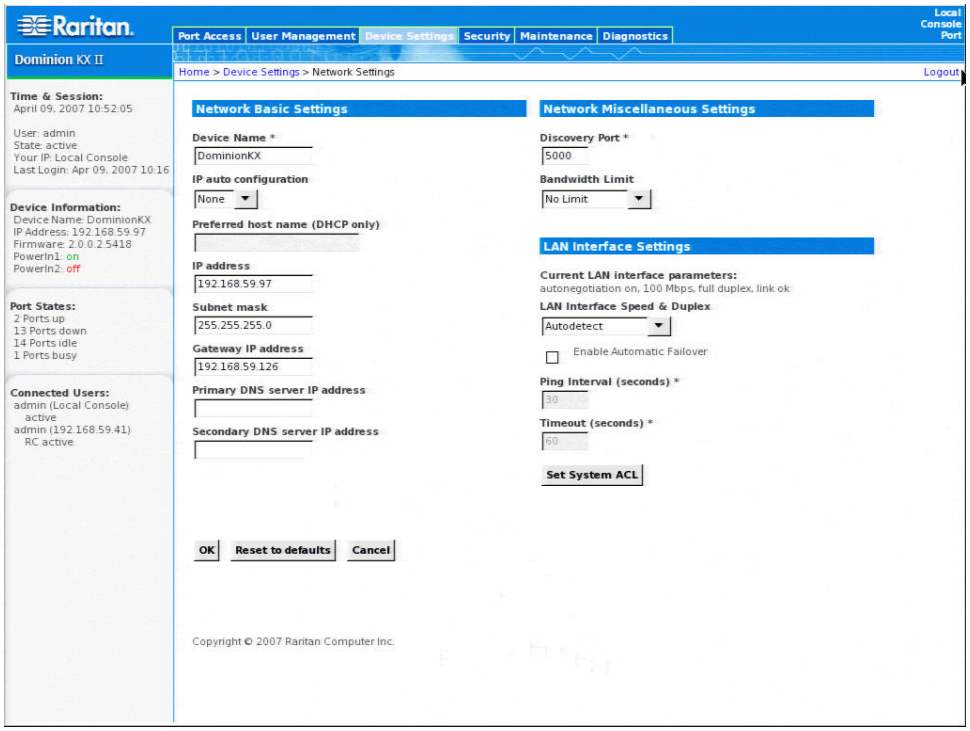


图 8：网络设置

2. 为 Dominion KX II 设备指定有意义的“设备名称”**(Device Name)**，该名称最多为 16 个字母数字字符或特殊字符，不能有空格。
3. 从下拉列表中选择“**IP** 自动配置”**(IP auto configuration)**：
   - **无 (None)（静态 IP）**。该选项要求您手动指定网络参数。推荐采用该选项，因为 Dominion KX II 为基础架构设备，其 IP 地址不应当更改。
   - **DHCP**。如果采用该选项，则网络参数由 DHCP 服务器分配。
4. 如果将 **IP** 配置指定为“无”**(None)**，请为 **Dominion KX II** 设备键入以下 **TCP/IP** 参数：**IP 地址 (IP address)**、**子网掩码 (Subnet mask)**、**网关 IP 地址 (Gateway IP address)**、**主 DNS 服务器 IP 地址 (Primary DNS server IP address)** 和（可选）**辅助 DNS 服务器 IP 地址 (Secondary DNS server IP address)**。
5. 完成后，单击“确定”**(OK)**。

现在 Dominion KX II 设备可通过网络访问了。

注意：*在某些环境中，“自动检测”(Autodetect) 的“LAN 接口速度及双工”(LAN Interface Speed & Duplex) 默认设置未正确设置网络参数，从而导致网络问题。此时，将 Dominion KX II 的“LAN 接口速度及双工”(LAN Interface Speed & Duplex) 字段设置为“100 Mbps/全双工”（或适用于您所用网络的任何选项）可解决该问题。有关详细信息，请参阅网络设置。*

为目标服务器命名

为目标服务器命名：

1. 如果尚未连接所有目标服务器，则连接它们（如第 3 步：连接设备，目标服务器端口中所述）。
2. 使用 KX II 本地控制台，选择“设备设置”**(Device Settings)** >“端口配置”**(Port Configuration)**。将打开“端口配置”(Port Configuration) 页：

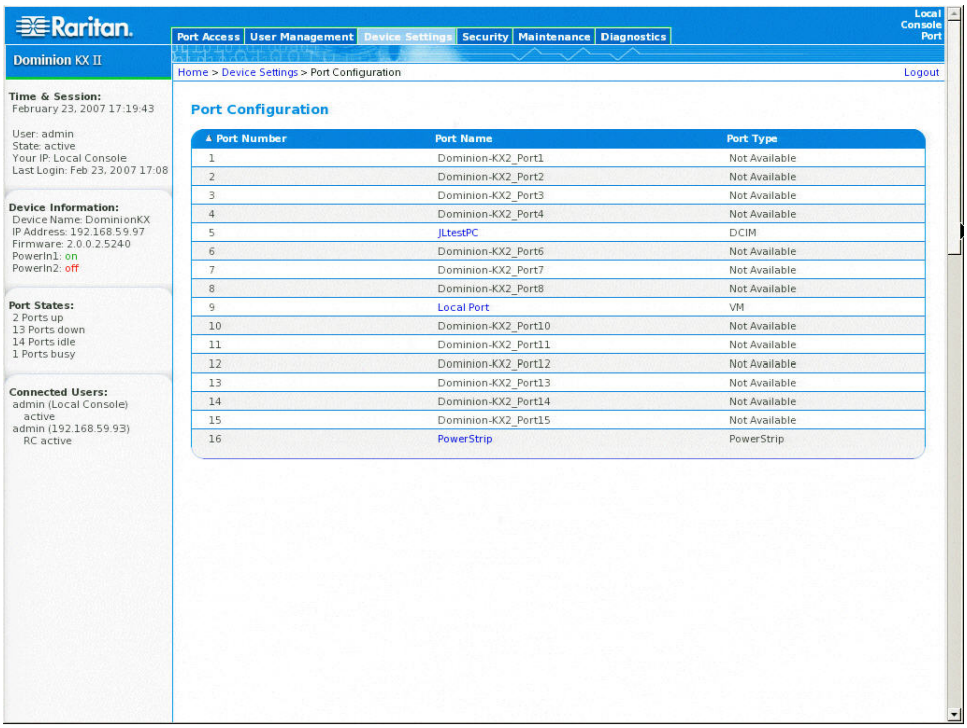


图 9：端口配置

3. 单击要重命名的目标服务器的“端口名称”(Port Name)。将打开“端口”页。
4. 指定一个名称，以标识与该端口相连的服务器。名称最多可以有 32 个字符，可以包括字母数字字符和特殊字符。
5. 单击“确定”**(OK)**。

指定电源自动检测

Dominion KX II 提供了双电源，可以自动进行检测并提供有关这些电源的状态的通知。正确的配置可确保在电源出现故障时 Dominion KX II 能发送相应的通知。“电源设置”(Power Supply Setup) 页配置为自动检测这两个电源；可使用该页禁用不在使用的电源的自动检测。

禁用不在使用的电源的自动检测：

1. 使用 KX II 本地控制台，选择“设备设置”**(Device Settings)** >“电源设置”**(Power Supply Setup)**。将打开“电源设置”(Power Supply Setup) 页。
2. 清除**不** 在使用的电源的自动检测。

有关详细信息，请参阅“电源设置”页。

CC-SG 用户注意事项

如果在 CC-SG 配置中使用 Dominion KX II，请执行上述安装步骤，并在完成后参阅“CommandCenter Secure Gateway 用户指南”(CommandCenter Secure Gateway User Guide)、“CommandCenter Secure Gateway 管理指南”(CommandCenter Secure Gateway Administrator Guide) 或“CommandCenter Secure Gateway 部署指南”(CommandCenter Secure Gateway Deployment Guide) 以继续操作（所有文档都可以在 Raritan 网站的 Support 下找到：http://www.raritan.com/support/productdocumentation）。

注意：*本用户指南的其余部分主要适用于在未集成 CC-SG 功能的情况下部署 Dominion KX II 设备。*

远程认证

CC-SG 用户注意事项

当 Dominion KX II 由 CommandCenter Secure Gateway 控制时，*除了*本地用户（需要本地端口访问）外，CC-SG 会对用户和组进行认证。本地用户认证取决于对 Dominion KX II 的配置。

有关 CC-SG 认证的详细信息，请参阅以下网址上的“CommandCenter Secure Gateway 用户指南”(CommandCenter Secure Gateway User Guide)、“CommandCenter Secure Gateway 管理指南”(CommandCenter Secure Gateway Administrator Guide) 或“CommandCenter Secure Gateway 部署指南”(CommandCenter Secure Gateway Deployment Guide)：http://www.raritan.com/support/productdocumentation。

支持的协议

为了简化用户名和密码的管理，Dominion KX II 提供了将认证请求转发到外部认证服务器这一功能。它支持以下两个外部认证协议：LDAP 和 RADIUS。

有关 Microsoft Active Directory 的说明

Microsoft Active Directory 本机使用 LDAP 协议，可充当 Dominion KX II 的 LDAP 服务器和认证源。如果包含 IAS（Internet 授权服务器）组件，那么 Microsoft Active Directory 服务器还可以作为 RADIUS 认证源。

认证与授权

认证是检验用户是否为他所声称身份的过程。一旦用户经过认证，则使用用户的组确定该用户的系统和端口权限。为用户分配的权限决定了所允许的访问类型。这称为授权。

如果 Dominion KX II 配置了远程认证，则外部认证服务器主要用于认证，而不是授权。

此流程图阐释了该过程：

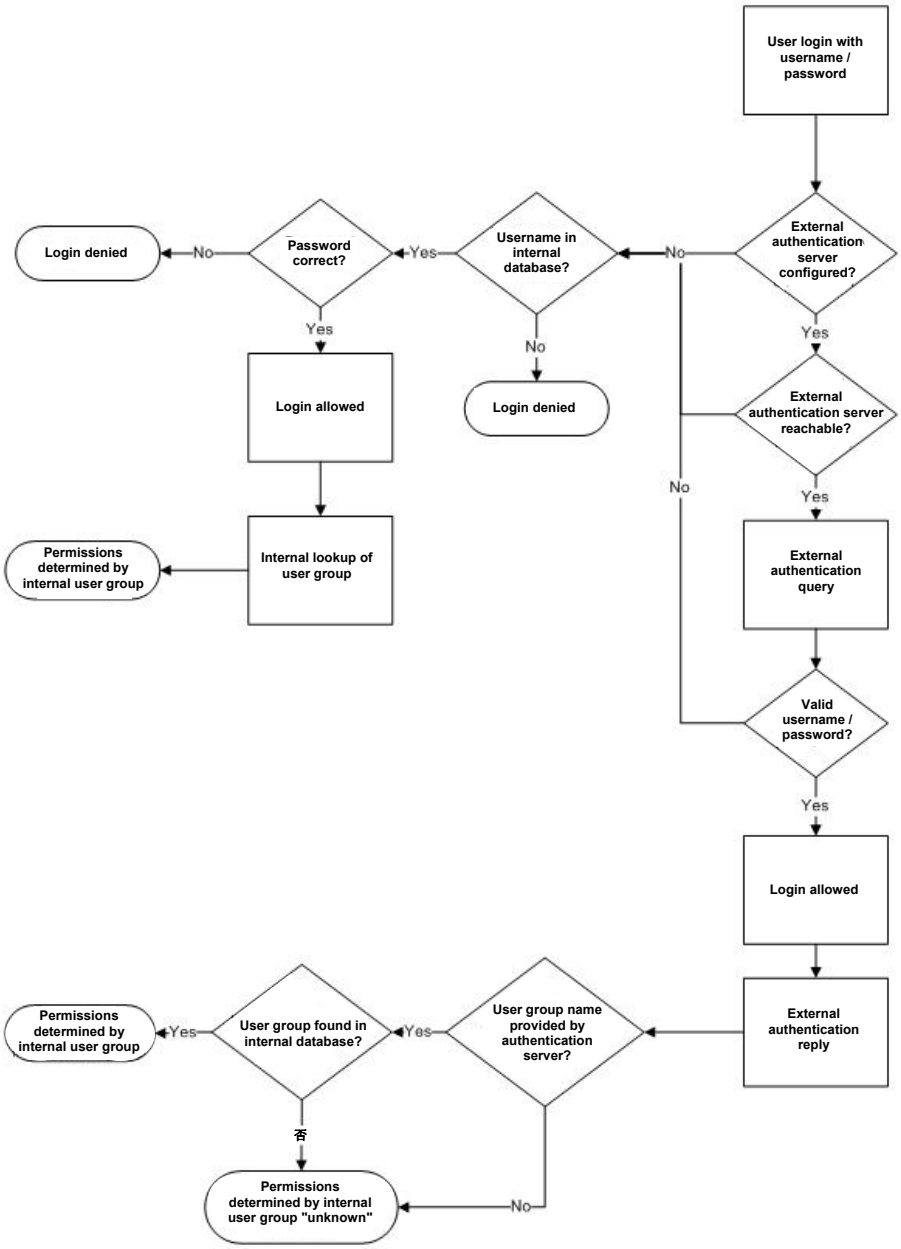


图 10：认证/授权流程图

请注意特定用户所属组的重要性，以及配置名为“未知”(Unknown) 组的必要性。如果外部认证服务器返回 Dominion KX II 无法识别的组名，则该用户的权限由名为“未知”(Unknown) 的永久组确定。

请参阅实现 LDAP 远程认证和实现 RADIUS 远程认证，以确定如何配置认证服务器，从而将用户组信息作为认证查询答复的一部分返回给 Dominion KX II。

用户、组和访问权限

概要

Dominion KX II 存储了所有用户和组名的内部列表，以确定访问授权和权限。该信息以加密的形式存储在内部。认证的形式有多种，其中一种是“本地认证”。所有用户都必须进行认证；如果 Dominion KX II 配置了 LDAP 或 RADIUS 认证，则首先执行该认证，然后执行本地认证。

用户

要访问 Dominion KX II 设备，必须使用用户名和密码。该信息用于认证尝试访问 KX II 设备的用户。有关添加和编辑用户的详细信息，请参阅用户管理。

组

每个 Dominion KX II 设备都提供了三个默认的用户组，这些组不能删除：

管理	作为该组成员的用户具备完全的管理权限。原始的出厂默认用户是该组的成员，具有完全的系统权限。
未知 (Unknown)	这是使用 LDAP 或 RADIUS 进行外部认证的用户的默认组。如果外部 LDAP 或 RADIUS 服务器无法识别某个有效的用户组，则使用“未知”(Unknown) 组。
个人 (Individual) 组	“个人”(Individual) 组实际上是一个用户的“组”。也就是说，某个用户在他自己的组中，与其它*真正的*组没有关联。“个人”(Individual) 组可由组名称中的“@”标识。

除了系统提供的以上默认组之外，您可以根据自己的需要创建组并执行适当的权限。有关创建和编辑用户组的详细信息，请参阅用户管理。

用户与组之间的关系

用户属于组，组具备权限。通过将 Dominion KX II 的各种用户划分为组，您可以同时管理组中所有用户的权限，而不用逐个用户地管理权限，从而节约了时间。

您还可以选择*不*将特定用户与组关联。此时，可以将该用户分类为“个人”(Individual)。

成功认证之后，设备使用**组**信息确定用户的权限—可以访问哪些服务器端口，是否允许重新引导设备以及其它功能。

第 4 章：连接到 Dominion KX II

用户界面

Dominion KX II 中有多个用户界面，使您可随时随地轻松访问。包括 KX II 本地控制台、KX II 远程控制台和多平台客户机 (MPC)。下表列出了这些界面以及是否可用于目标服务器的本地和远程访问及管理：

用户界面	本地		远程	
	访问 (ACCESS)	管理 (ADMIN)	访问 (ACCESS)	管理 (ADMIN)
KX II Local Console	✓	✓		
KX II 远程控制台			✓	✓
虚拟 KVM 客户机			✓	
多平台客户机 (MPC)			✓	✓

KX II 本地控制台 — KX II 设备

当您位于服务器机架处时，Dominion KX II 可通过 KX II 本地控制台提供标准的 KVM 切换和管理功能。KX II 本地控制台提供了与相连服务器的直接 KVM（模拟）连接，其性能与直接连接到服务器的键盘、鼠标和视频端口时完全一样。

KX II 本地控制台与 KX II 远程控制台图形用户界面之间有许多相似之处，同时也有不同之处，用户手册中对此进行了说明。KX II 本地控制台和 KX II 远程控制台用户界面几乎是一样的。以下是 KX II 本地控制台中有，但 KX II 远程控制台中*没有* 的选项：

- 本地端口设置 (Local Port Settings)
- 出厂复位 (Factory Reset)

KX II 远程控制台 — KX II 设备

Dominion KX II 远程控制台是基于浏览器的图形用户界面，您可以通过该界面访问与 Dominion KX II 相连的目标服务器并远程管理 KX II。

KX II 远程控制台提供了与相连目标服务器的数字连接。当您使用 KX II 远程控制台访问目标服务器时，将打开一个“虚拟 KVM 客户机”(Virtual KVM Client) 窗口。对于每台目标服务器，都将打开一个虚拟 KVM 客户机，只要特定 KX II 设备支持，便允许同时访问（例如，KX2-116 只支持一个远程会话）。

KX II 本地控制台与 KX II 远程控制台图形用户界面之间有许多相似之处，同时也有不同之处，用户手册中对此进行了说明。以下是 KX II 远程控制台中有，但 KX II 本地控制台中*没有*的选项：

- 虚拟媒体
- 收藏夹
- 备份/恢复
- 固件升级
- 升级报告
- KX 诊断

多平台客户端 (MPC) — KX I 和 KX II 设备

Raritan Multi-Platform Client (MPC) 是一个图形界面，您可以通过该界面远程访问与 Dominion 设备相连的目标设备。MPC 可安装以供独立使用，或通过 Web 浏览器访问。

安装 Dominion KX II 之后，可以下载独立版本的 Raritan MPC 并建立初始网络连接，也可以直接启动应用程序。

***注意：** MPC 同时支持 KX I 和 KX II 设备。如果您希望通过一个用户界面访问与 KX I 和 KX II 设备相连的服务器，可以使用 MPC。*

直接启动 MPC：

1. 要从运行任何浏览器的客户机启动 **MPC**，请在地址栏中键入 **http://IP-ADDRESS/mpc**，其中 **IP-ADDRESS** 是 **Raritan** 设备的 **IP** 地址。**MPC** 将在一个不包含菜单栏、工具栏、滚动条或地址栏的新窗口中启动。在该窗口中工作并使用 ALT+TAB 命令切换到其它已打开的窗口。
2. 当 MPC 启动时，屏幕左侧将显示在子网上找到的所有自动检测的 Raritan 设备的设备树。如果您在按名称列出的 Dominion KX II 设备中找不到自己的设备，那么可通过选择“连接”**(Connection) >**“新建配置文件”**(New Profile)** 手动创建一个图标。将打开“添加连接”(Add Connection) 窗口。
3. 键入设备说明，指定连接类型，添加 Dominion 设备的 IP 地址，然后单击“确定”**(OK)**。这些指定以后可以进行编辑。
4. 在屏幕左侧的导航窗格中，双击与您的 Dominion KX II 设备对应的图标。

有关安装和操作 MPC 的完整信息，请参阅 Raritan 网站 http://www.raritan.com/support/productdocumentation 或 Dominion 附带的“Raritan 用户手册和快速设置指南 CD ROM”上的“Raritan Multi-Platform Client (MPC) 和 Raritan Remote Client (RRC) 用户指南”(Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide)。

Raritan Remote Client (RRC) - 仅针对 KX I 设备

Raritan Remote Client (RRC) 是一个图形用户界面，提供了对目标服务器的远程访问。

***注意：** RRC **不能**用于 Dominion KX II，请改用 MPC。*

语言支持

Dominion KX II 支持以下语言的键盘：美国英语、英国英语、繁体中文、简体中文、日文、韩文、法文和德文。

语言支持注意事项

- 中文、日语和朝鲜语键盘只能用于显示。对于 KX II 本地控制台功能，目前不支持本地语言输入。
- 由于 Java® Runtime Environment (JRE) 中的一个限制，在英国英语键盘上，Fedora、Linux 和 Solaris 客户机会接收到来自 Alt Gr 的无效响应。对于 Java 1.4.2 或 1.5，Fedora、Linux 和 Solaris 不会接受 Alt Gr 组合键事件。Java 1.6 似乎在这一点上做出了改进，但 Alt Gr 的 *keyPressed* 和 *keyReleased* 事件仍将其识别为“未知的键代码”。

  而且，如将某一键与 Alt Gr 键同时按下（例如在英语键盘上按 Alt Gr-4，这是显示欧元符号的组合键），只会生成 *keyTyped* 事件，继而生成该值的 *keyReleased* 事件，而不会生成 *keyPressed* 事件。Java 1.6 也通过填入 *keyPressed* 事件改进了这一点。

Java Runtime Environment (JRE)

重要事项：建议您禁用 Java 高速缓存并清除 Java 高速缓存。有关详细信息，请参阅 Java 文档或“Raritan Multi-Platform Client (MPC) 和 Raritan Remote Client (RRC) 用户指南”(Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide)。

Dominion KX II 远程控制台和 MPC 需要 JRE 才能运行。Dominion KX II 远程控制台会检查 Java 版本。如果版本不正确或已过期，会提示您下载兼容的版本。

Raritan 建议您使用 Java Runtime Environment (JRE) 1.5 版以实现最佳性能，但是 Dominion KX II 远程控制台和 MPC 适用于 JRE **1.4.2_05** 版或更高版本（JRE 1.5.0_02 除外）。JRE 1.6 也受支持，但是尚未经过完全测试。

***注意：**为了在 KX II 远程控制台（虚拟 KVM 客户机）中使用多语言键盘，请安装 Java Runtime Environment (JRE) 的多语言版本。*

启动 KX II

重要事项：无论使用的是什么浏览器，都必须允许从 Dominion 设备的 IP 地址弹出的窗口，以启动 KX II 远程控制台。

注意：*根据您的浏览器和安全设置的不同，您可能看到不同的安全和证书警告。必须接受这些警告，才能启动 KX II 远程控制台。*

您可以在这些安全和证书警告消息中选中以下选项，从而减少以后的登录中的警告消息数量：

- ☐ *今后不显示此警告 (In the future, do not show this warning)*
- ☐ *总是信任来自此发行商的内容 (Always trust content from this publisher)*

启动 KX II 远程控制台：

1. 登录到与 Dominion KX II 设备通过网络连接并安装了 Java Runtime Environment v1.4.2_2 或更高版本（JRE 可从 http://java.sun.com/ 获得）的任何工作站。
2. 启动支持的 Web 浏览器，如 Internet Explorer (IE) 或 Firefox。
3. 键入以下 URL：**http://IP-ADDRESS**，其中 **IP-ADDRESS** 是分配给 Dominion KX II 设备的 IP 地址。也可以使用 https、管理员分配的 Dominion KX II 的 DNS 名称（假定配置了 **DNS** 服务器），或只是在浏览器中键入 IP 地址（KX II 始终会将 IP 地址由 HTTP 重定向至 HTTPS）。将打开“登录”(Login) 页：

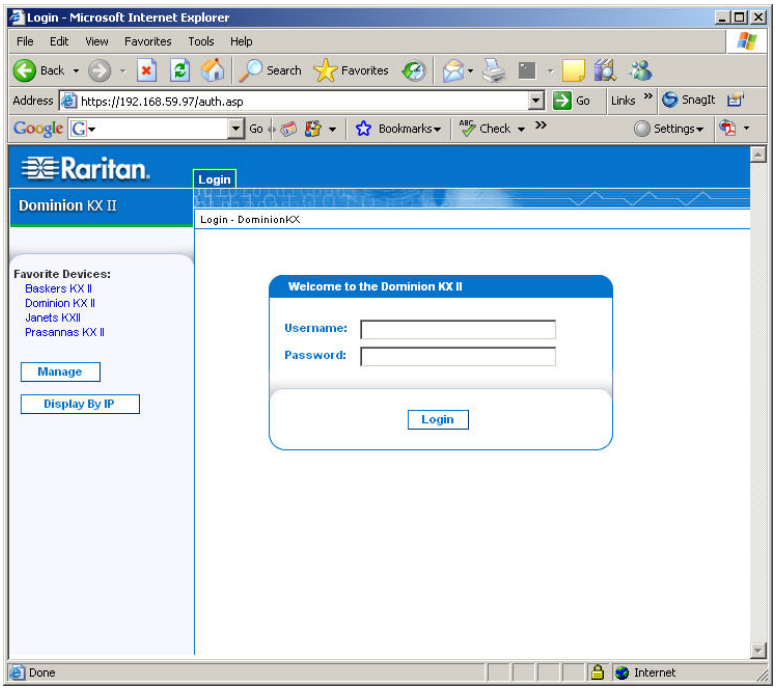


图 11：Dominion KX II 远程控制台登录页

4. 键入“用户名”**(Username)** 和“密码”**(Password)**。如果是第一次登录，请使用出厂默认用户名和密码（**admin** 和 **raritan**（全部为小写字母））进行登录。系统将提示您更改默认密码。有关详细信息，请参阅更改默认密码。
5. 单击“登录”**(Login)**。

KX II 控制台布局

KX II 远程控制台和 KX II 本地控制台界面都提供了 HTML（类似 Web）界面，用于配置和管理，并列出和选择目标服务器。所有选项划分到各个选项卡中。

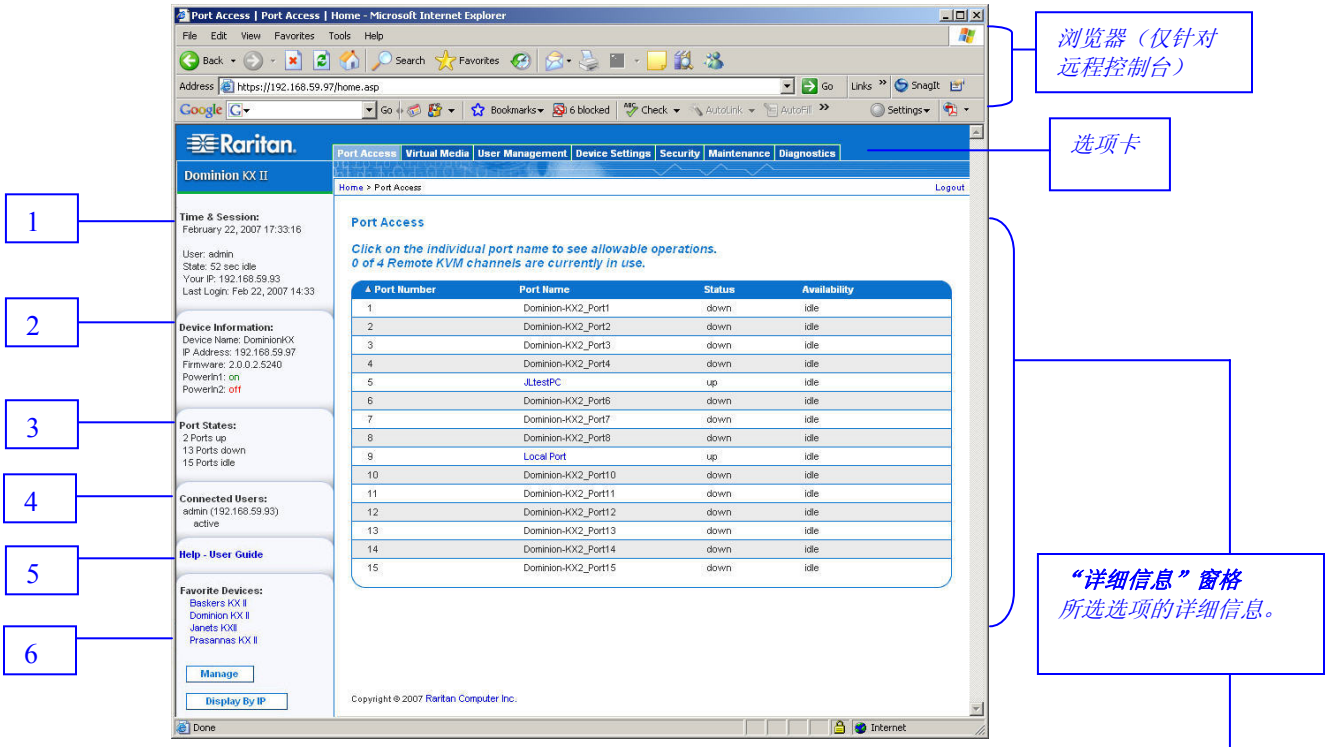


图 12：KX II 远程控制台主页

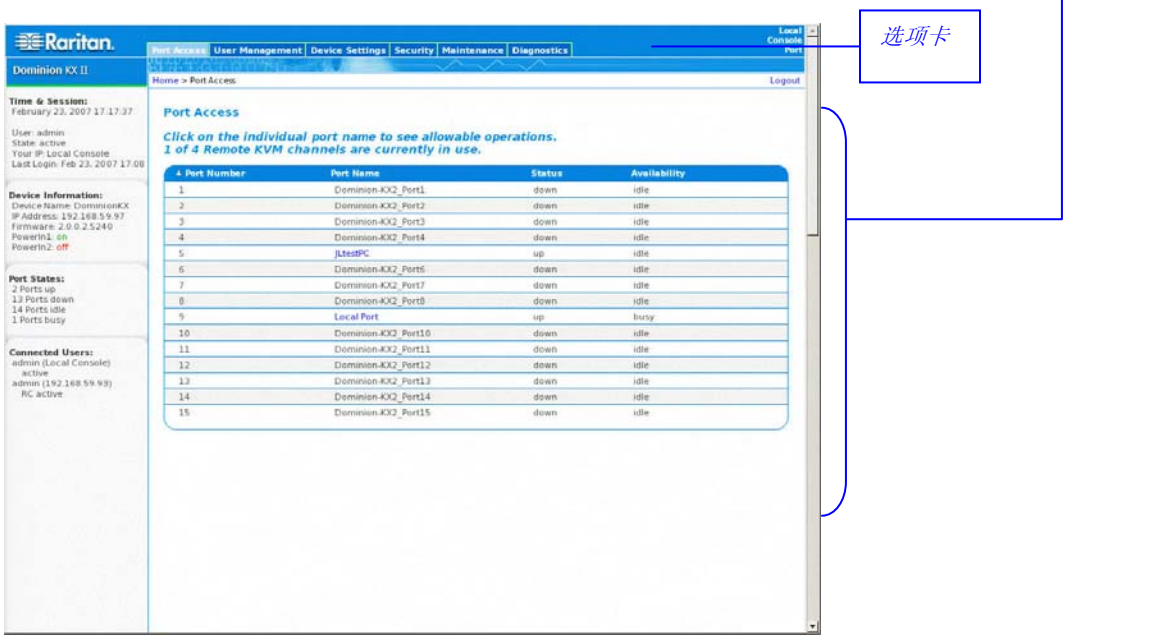


图 13：KX II 本地控制台主页

成功登录之后，将打开“端口访问”(Port Access) 页，其中列出了所有端口及其状态和可用性。您可以通过单击列标题按端口号、端口名称、状态（打开和关闭）以及可用性（空闲、已连接、忙碌、不可用和正在连接）排序。

下表中的编号对应于图 12 中的编号。

#	标题	说明
1	时间和会话 (Time & Session)	日期、时间、用户名、当前状态、客户机的 IP 地址以及上次登录时间
2	设备信息	设备名称、IP 地址、固件版本以及两个电源的状态
3	端口状态 (Port States)	所有 Dominion KX II 端口的当前状态
4	已连接用户 (Connected Users)	列出当前与 Dominion KX II 相连的所有用户
5	帮助 – 用户指南 (Help - User Guide)	访问此用户手册（仅针对 KX II 远程控制台）
6	收藏设备 (Favorite Devices)	访问和管理收藏列表（仅针对 KX II 远程控制台）

KX II 控制台导航

Dominion KX II 控制台界面（包括本地和远程）提供了多种导航和选择方法。

选择选项（使用以下任意方法）：

- 单击选项卡；将打开可用选项的页。
- 悬停在选项卡上方，并从菜单中选择合适的选项。
- 从分层显示的菜单中直接单击选项（“痕迹导航”）。

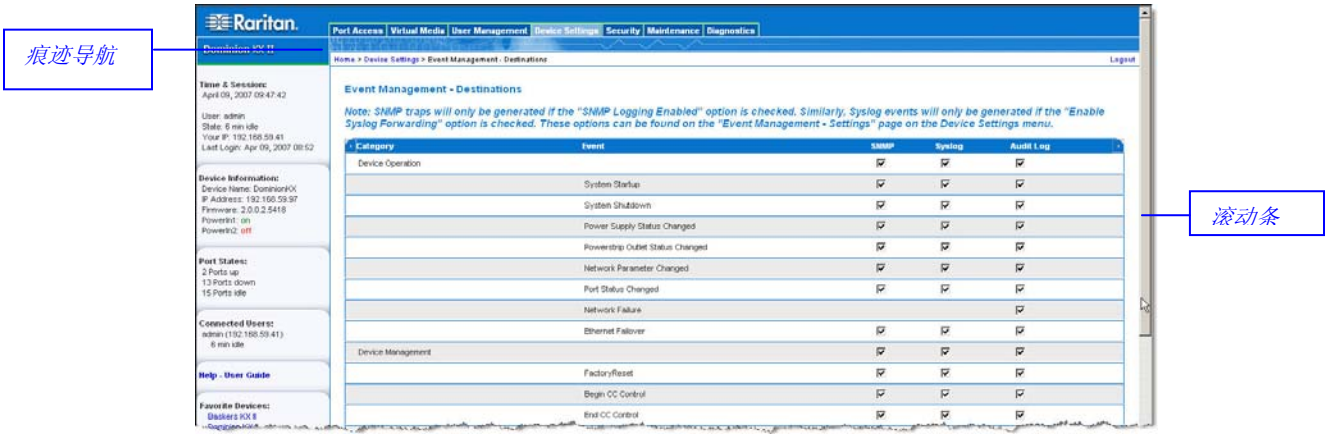


图 14：菜单层次结构示例（痕迹导航）

滚动长度超过屏幕的页面：

- 使用键盘上的 Page Up 和 Page Down 键，或
- 使用右侧的滚动条。

有关在 Raritan Multi-Platform Client (MPC) 中进行导航和选择的详细信息，请参阅“Raritan Multi-Platform Client (MPC) 和 Raritan Remote Client (RRC) 用户指南”(Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guid)。

注销

退出 Dominion KX II 控制台：

单击页面右上角的“注销”(Logout)。

注意：*注销还会关闭打开的所有虚拟 KVM 客户机会话。*

KX II 控制台菜单树

下图显示了 KX II 远程控制台和 KX II 本地控制台界面中可用的*所有*菜单选项。其中标出了 KX II 本地控制台与 KX II 远程控制台之间的差异。

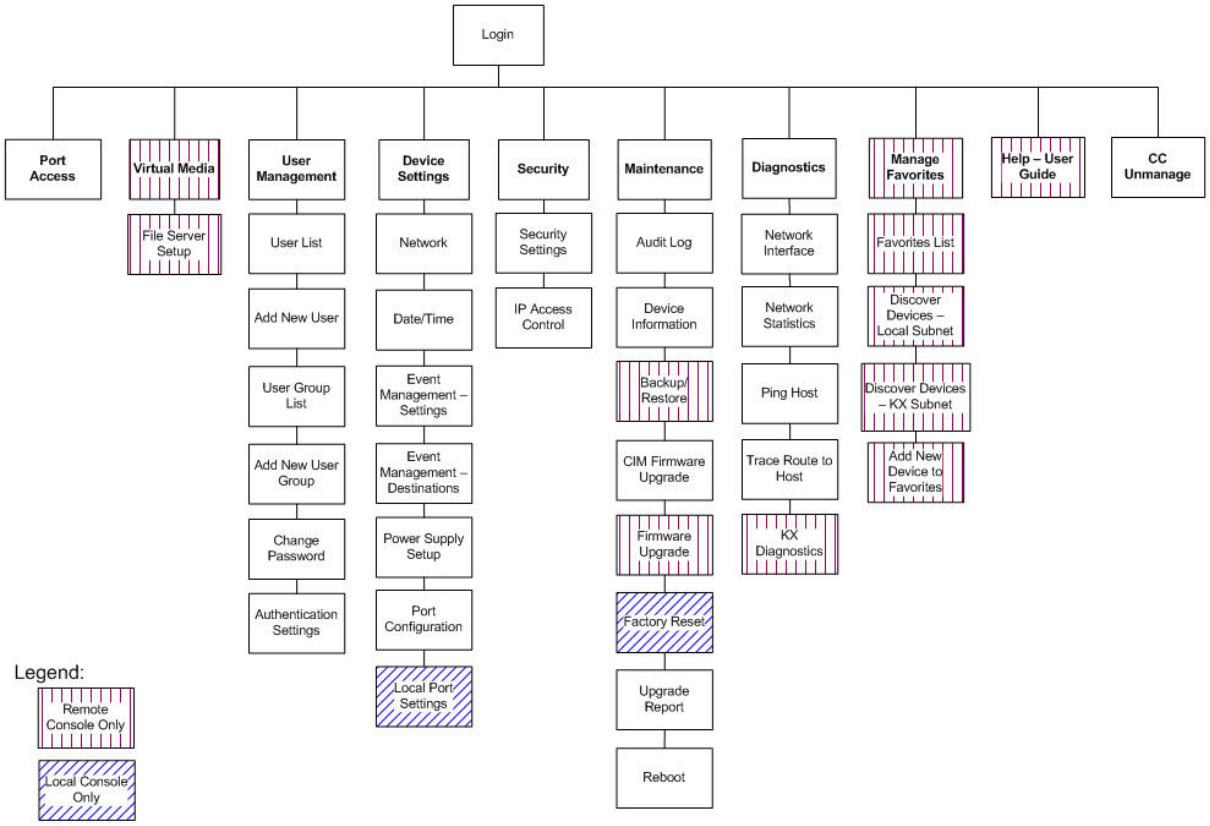


图 15：KX II 控制台菜单树（本地和远程）

除了在上面的菜单树中标出以外，下表中也列出了 KX II 本地控制台与 KX II 远程控制台之间菜单选项的差异：

选项	本地控制台	远程控制台
虚拟媒体		✓
文件服务器设置		✓
备份/恢复		✓
固件升级		✓
KX 诊断		✓
管理收藏夹 (Manage Favorites)		✓
收藏列表		✓
发现设备 - 本地子网		✓
发现设备 - KX 子网		✓
将新设备添加到收藏夹 (Add New Device to Favorites)		✓
帮助 – 用户指南		✓
本地端口设置	✓	
出厂复位 (Factory Reset)	✓	

管理收藏夹

提供收藏夹功能的目的是为了让您能组织和快速访问常用的设备。“收藏设备”(Favorite Devices) 部分位于“端口访问”(Port Access) 页的左下部（边栏），提供了以下功能：

- 创建和管理收藏设备列表
- 快速访问常用设备
- 按名称或 IP 地址列出收藏设备
- 在子网上发现 Dominion KX II 设备（登录前和登录后）
- 从连接的 KX 设备中检索发现的 Dominion KX II 设备（登录后）

注意：*只有 Dominion KX II 远程控制台提供了该功能（Dominion KX II 本地控制台不具备该功能）。*

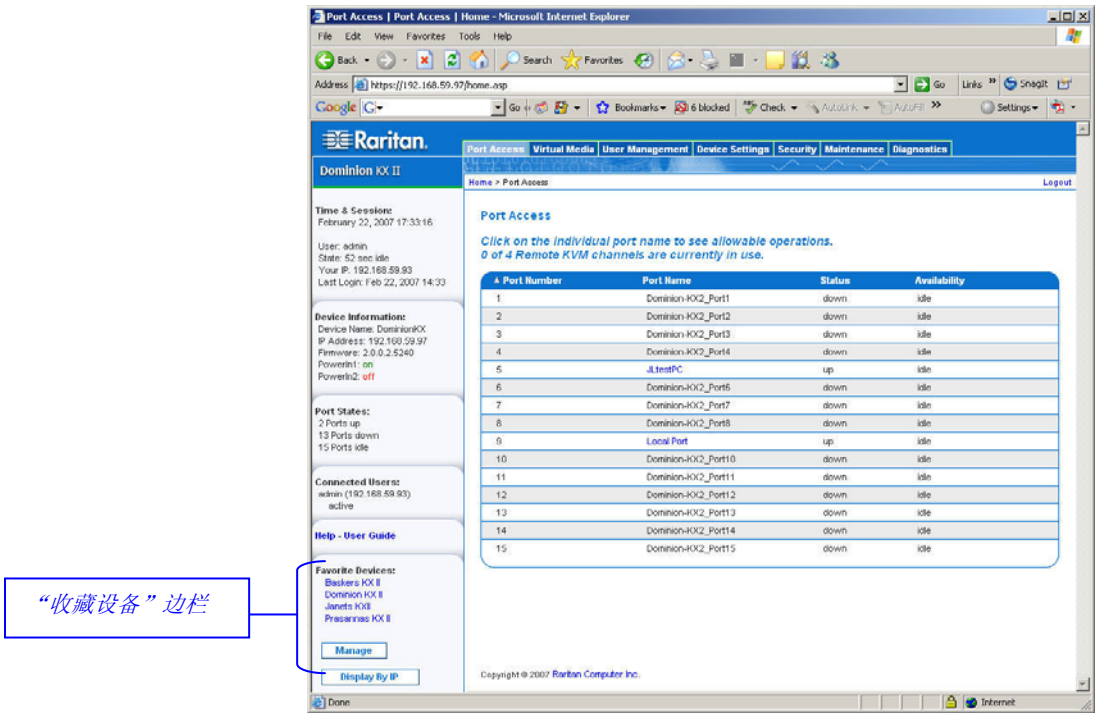


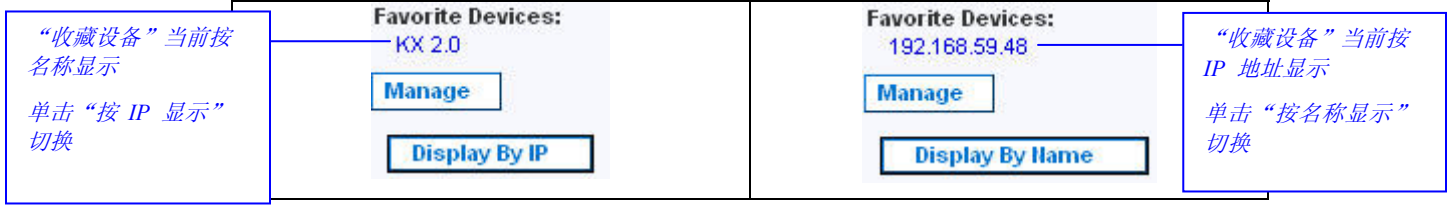
图 16：收藏设备（边栏）

访问收藏的 KX II 设备：

单击该设备的名称（列在“收藏设备”**(Favorite Devices)** 下）。将为该设备打开一个新的浏览器。

在名称和 IP 地址之间切换“收藏设备”**(Favorite Devices)** 列表显示：

按 IP 地址显示收藏夹：	按名称显示收藏夹：
单击“按 IP 显示”**(Display by IP)** 按钮。	单击“按名称显示”**(Display by Name)** 按钮。



“管理收藏夹”菜单

“管理收藏夹”(Manage Favorites) 菜单提供了以下选项：“收藏列表”(Favorites List)、“发现设备 - 本地子网”(Discover Devices - Local Subnet)、“发现设备 - KX 子网”(Discover Devices - KX Subnet) 和“将新设备添加到收藏夹”(Add New Device to Favorites)。

打开“管理收藏夹”(Manage Favorites) 菜单：

单击“管理”**(Manage)** 按钮。将打开“管理收藏夹”(Manage Favorites) 页：

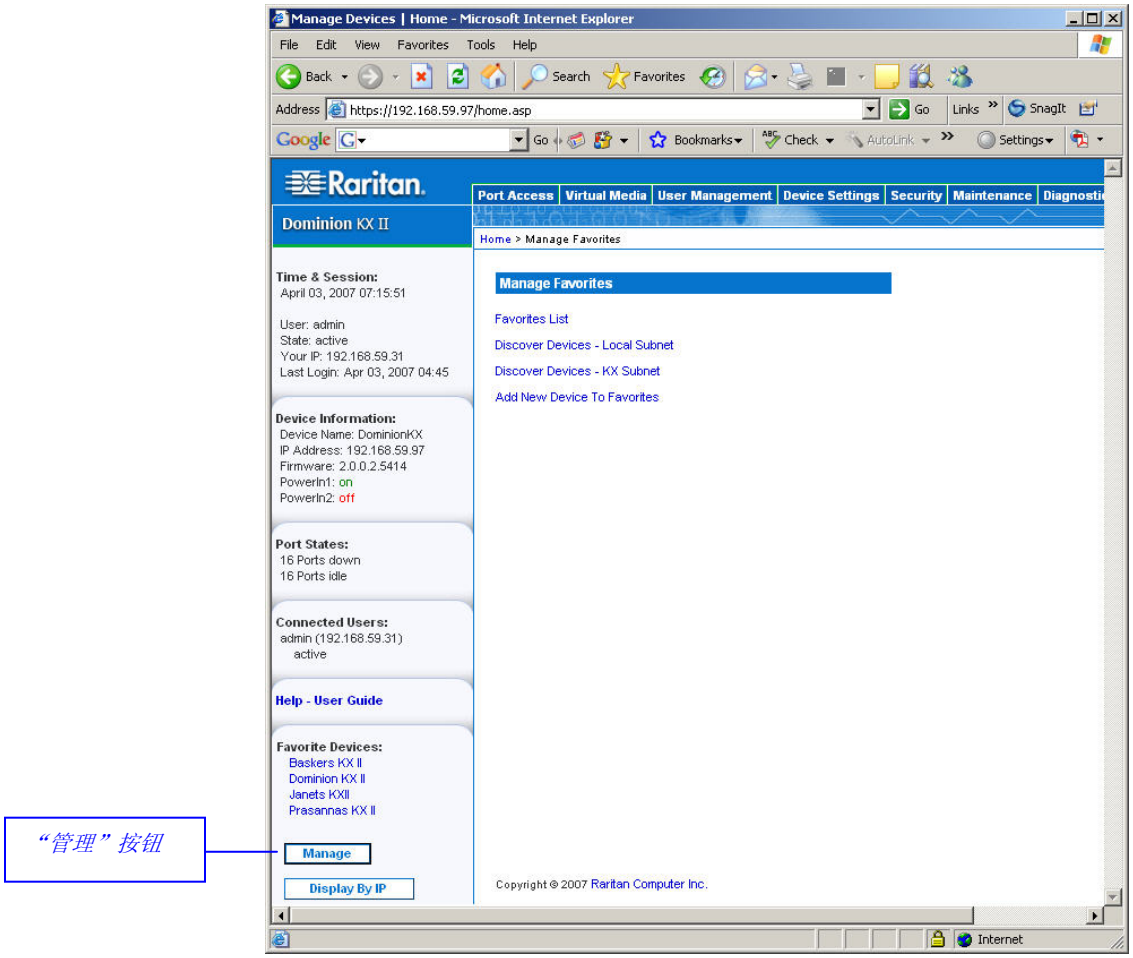


图 17：“管理收藏夹”菜单

使用：	目的：
收藏列表	管理收藏设备列表。
发现设备 - 本地子网	发现本地子网上的设备。
发现设备 - KX 子网	发现 KX 设备子网上的设备。
将新设备添加到收藏夹 (Add New Device to Favorites)	在收藏夹的列表中添加、编辑和删除设备。

收藏列表

在“收藏列表”(Favorites List) 页中，可以在收藏夹的列表中添加、编辑和删除设备。

打开“收藏列表”(Favorites List) 页：

选择“管理”**(Manage) >**“收藏列表”**(Favorites List)**。将打开“收藏列表”(Favorites List) 页：

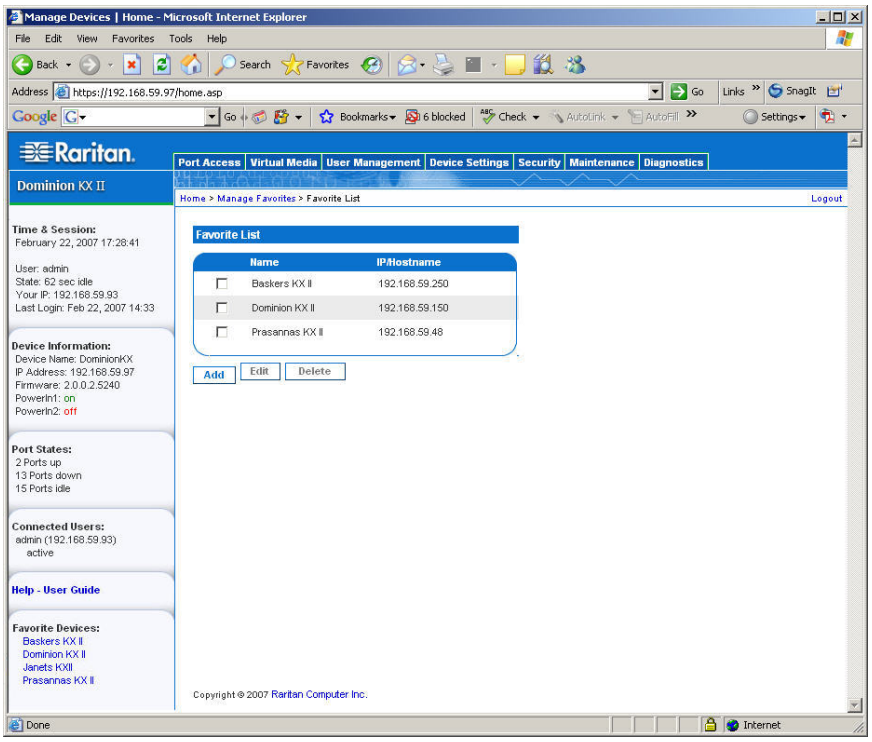


图 18：收藏列表

添加收藏：

单击“添加”**(Add)** 按钮。将打开“添加新收藏”(Add New Favorite) 页。

删除收藏：

重要事项：在删除收藏时请小心谨慎，系统不会提示您确认删除。

1. 选中相应 Dominion KX II 设备旁的复选框。
2. 单击“删除”**(Delete)** 按钮。收藏将从收藏列表中删除。

编辑收藏：

1. 在“收藏列表”(Favorites List) 页中，选中相应 Dominion KX II 设备旁的复选框。
2. 单击“编辑”**(Edit)** 按钮。将打开“编辑”(Edit) 页。

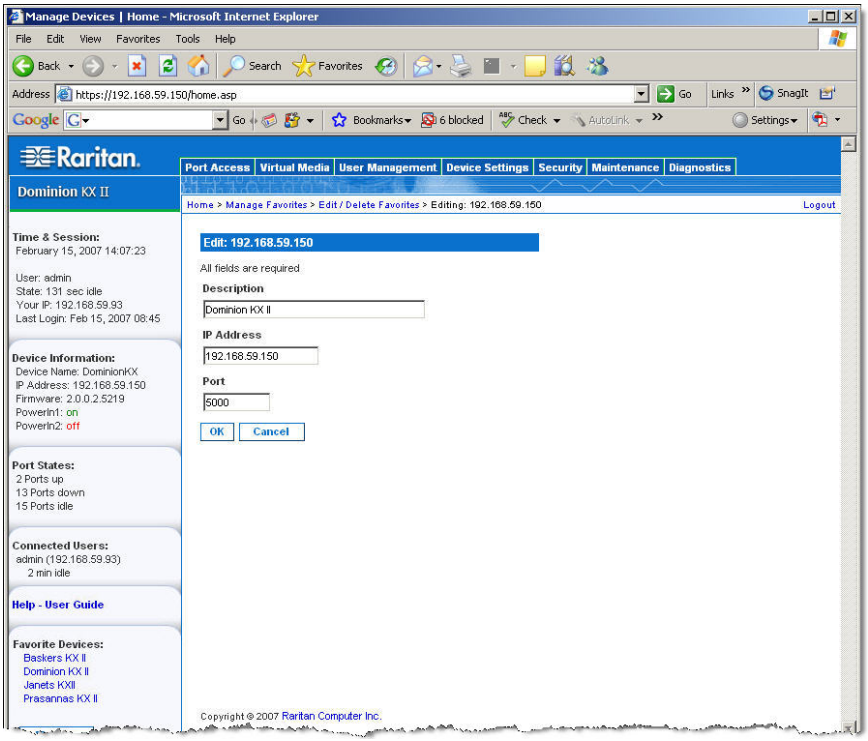


图 19：编辑（收藏信息）

3. 根据需要更新以下字段：
   - 说明 **(Description)**。键入某些有意义的内容。
   - IP 地址 **(IP Address)**。键入 Dominion KX II 设备的 IP 地址。
   - 端口 **(Port)**。更改发现“端口”**(Port)**（如有必要）。
4. 单击“确定”**(OK)**。

发现设备 — 本地子网

该选项用于发现本地子网（即运行 Dominion KX II 远程控制台的子网）上的设备。可以从该页直接访问这些设备，或将这些设备添加到收藏列表中。

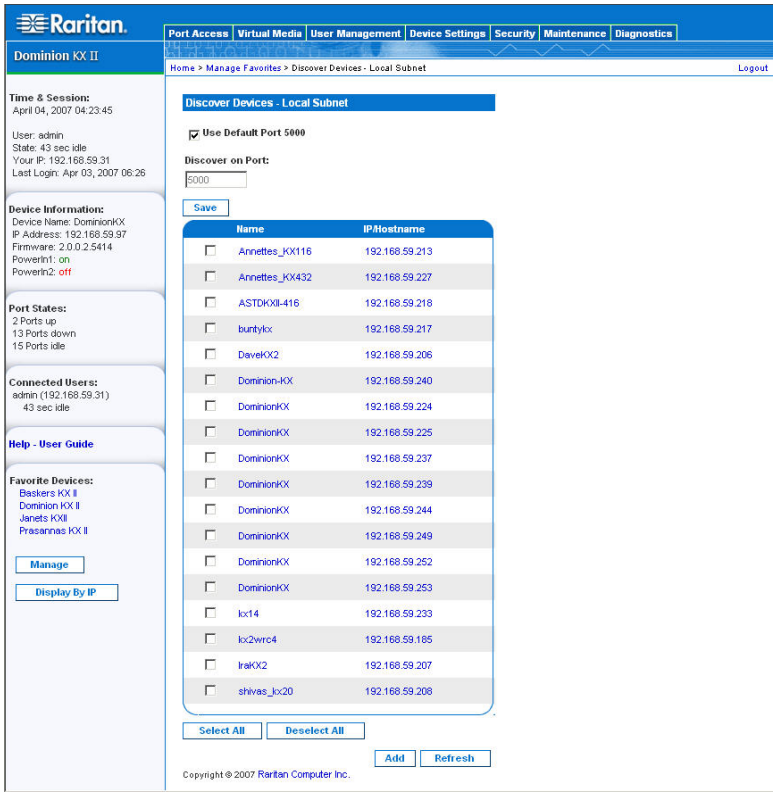


图 20：发现设备 - 本地子网

发现本地子网上的设备：

1. 选择“收藏夹”**(Favorites) >**“发现设备 — 本地子网”**(Discover Devices - Local Subnet)**。将打开“发现设备 — 本地子网”(Discover Devices - Local Subnet) 页。
2. 选择适当的发现端口（有关发现端口的信息，请参阅其它网络杂项设置）：
   - 要使用默认的发现端口，请选中“使用默认端口 5000”**(Use Default Port 5000)** 选项。
   - 要使用其它发现端口，请执行以下操作：
     a. 清除“使用默认端口 5000”**(Use Default Port 5000)** 选项。
     b. 在“发现端口”**(Discover on Port)** 字段中键入端口号。
     c. 单击“保存”**(Save)**。
3. 单击“刷新”**(Refresh)**。本地子网上的设备列表将刷新。

将设备添加到“收藏列表”(Favorites List)：

1. 选中设备名称/IP 地址旁的复选框。
2. 单击“添加”**(Add)**。

*提示：可以使用“全选”**(Select All)** 和“取消全选”**(Deselect All)** 按钮快速选择（或取消选择）远程控制台子网中的所有设备。*

访问发现的设备：

单击该设备的设备名称或 IP 地址。将为该设备打开一个新的浏览器。

发现设备 － KX 子网

该选项用于发现 KX 设备子网（即 Dominion KX II 设备 IP 地址自身的子网）上的设备。可以从该页直接访问这些设备，或将这些设备添加到收藏列表中。

该功能允许多个 Dominion KX II 设备相互作用并自动伸缩。Dominion KX II 远程控制台会自动发现 Dominion KX II 子网中的 Dominion KX II 设备。

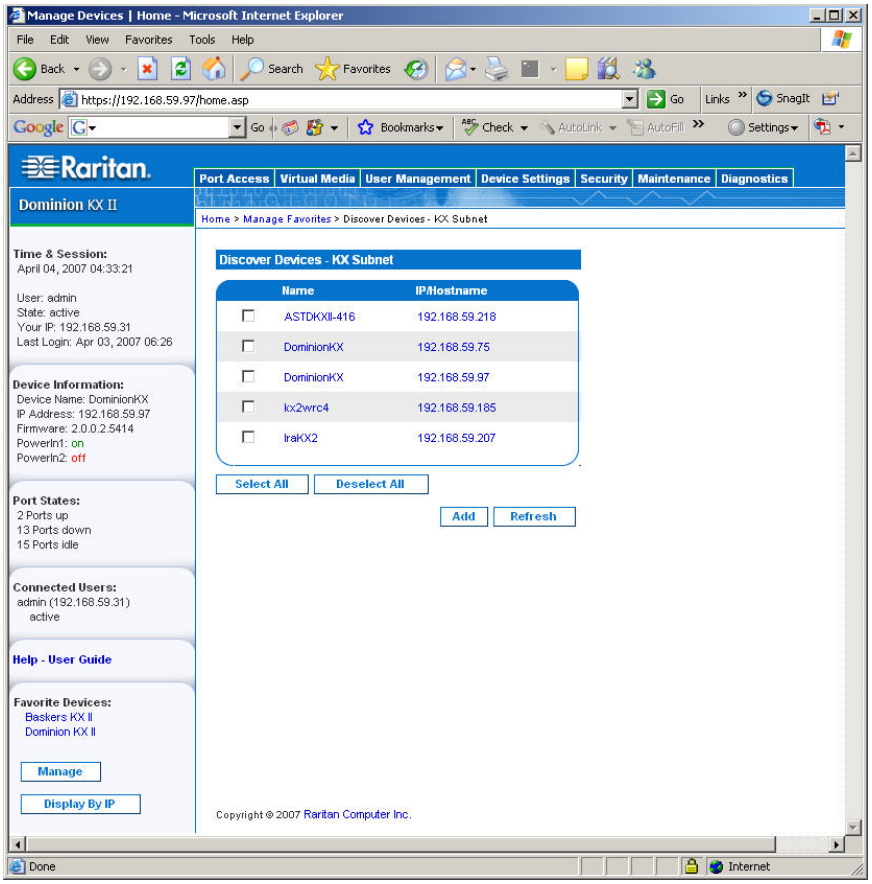


图 21：发现设备 - KX 子网

发现 KX 设备子网上的设备：

1. 选择“收藏夹”**(Favorites) >**“发现设备 － **KX** 子网”**(Discover Devices - KX Subnet)**。将打开“发现设备 － **KX** 子网”(Discover Devices - KX Subnet) 页。
2. 单击“刷新”**(Refresh)**。本地子网上的设备列表将刷新。

将设备添加到“收藏列表”(Favorites List)：

1. 选中设备名称/**IP** 地址旁的复选框。
2. 单击“添加”**(Add)**。

*提示：可以使用“全选”**(Select All)** 和“取消全选”**(Deselect All)** 按钮快速选择（或取消选择）Dominion KX II 设备子网中的所有设备。*

访问发现的设备：

单击该设备的设备名称或 IP 地址。将为该设备打开一个新的浏览器。

添加新收藏

将设备添加到“收藏列表”(Favorites List)：

1. 选择“管理收藏夹”**(Manage Favorites)** > “将新设备添加到收藏夹”**(Add New Device to Favorites)**。将打开“添加新收藏”页：

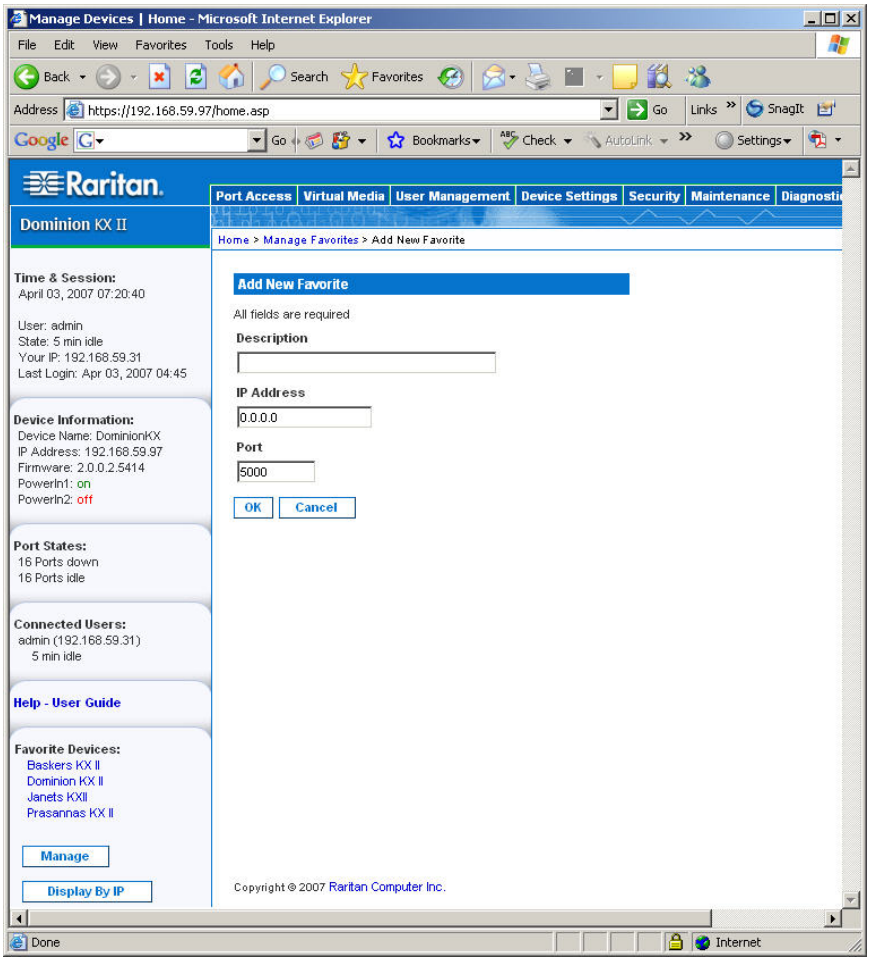


图 22：添加新收藏

2. 键入有意义的“说明”**(Description)**。
3. 键入该设备的“IP 地址”**(IP Address)**。
4. 更改发现“端口”**(Port)**（如有必要）。
5. 单击“确定”**(OK)**。该设备将添加到收藏列表中。

第 5 章：访问目标服务器

“端口访问”页

成功登录 Dominion KX II 远程控制台后，将打开“端口访问”(Port Access) 页。该页中列出了所有 Dominion KX II 端口、连接的目标服务器及其状态和可用性。“端口访问”(Port Access) 页提供了对与 Dominion KX II 相连的目标服务器的访问。目标服务器即要通过 Dominion KX II 设备控制的服务器，它们连接到设备背面的 Dominion KX II 端口上。

***注意：**对于每个目标服务器连接，将打开一个**新的**“虚拟 KVM 客户机”(Virtual KVM Client) 窗口。*

使用“端口访问”(Port Access) 页：

1. 在 KX II 远程控制台中，单击“端口访问”**(Port Access)** 选项卡以打开它。将打开“端口访问”(Port Access) 页：

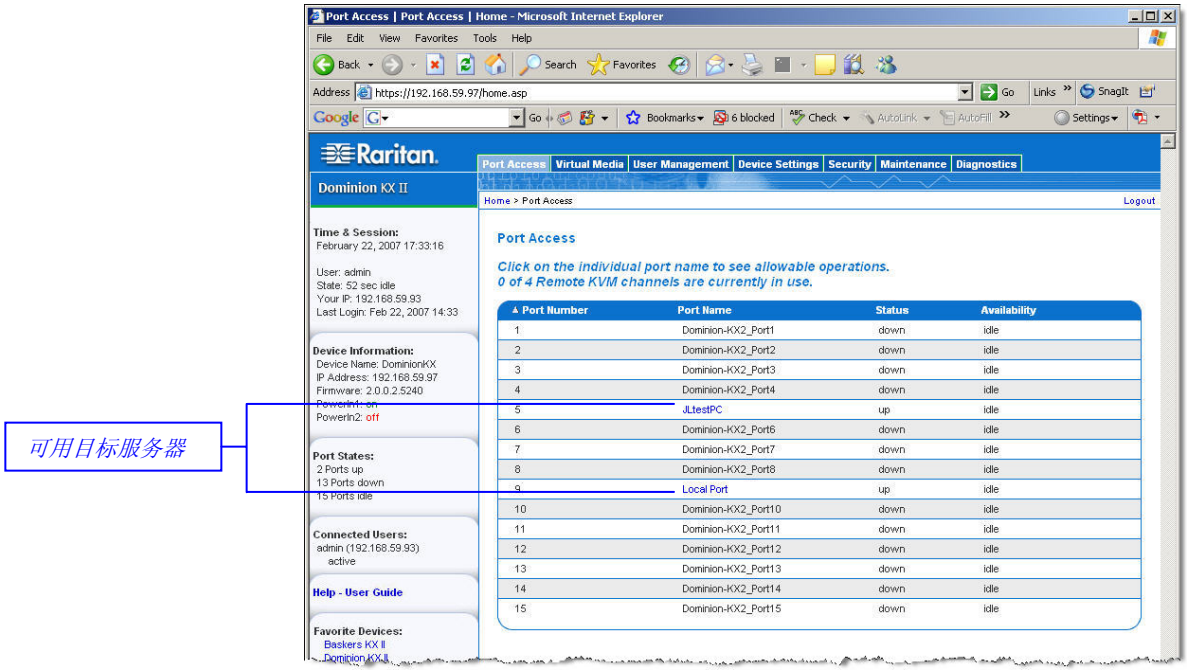


图 23：端口访问

目标服务器最初按端口号排序；您可以更改显示方式，按以下任一列进行排序。

- **端口号 (Port Number)**。从 1 开始编号，直到 Dominion KX II 设备可用的端口总数。请注意，与电源板相连的端口将*不会*在这里列出，这就导致端口号序列中缺少一些编号。
- **端口名称 (Port Name)**。Dominion KX II 端口的名称；最初设置为 Dominion-KX2-Port#，但您可以将此名称更改为某个更具说明性的名称。单击端口号链接时，将打开“端口操作”(Port Action) 菜单。
- **状态 (Status)**。“状态”(Status) 为“打开”(up) 或“关闭”(down)。
- **可用性 (Availability)**。可用性可以为“空闲”(Idle)、“已连接”(Connected)、“忙碌”(Busy) 或“不可用”(Unavailable)。

2. 单击要访问的目标服务器的“端口名称”**(Port Name)**。将显示“端口操作”**(Port Action)** 菜单。有关可用的菜单选项的详细信息，请参阅“端口操作”菜单。
3. 从“端口操作”**(Port Action)** 菜单中选择所需的菜单选项。

更改显示排序顺序：

单击要作为排序依据的列标题。目标服务器列表将按该列进行排序。

“端口操作”菜单

1. 在“端口访问”**(Port Access)** 列表中单击“端口名称”**(Port Name)** 时，将显示“端口操作”**(Port Action)** 菜单。请注意，“端口操作”**(Port Action)** 菜单中只列出可用于所选端口的选项：
   - **连接 (Connect)**。创建与目标服务器的新连接。对于 KX II 远程控制台，将打开新的“虚拟 KVM 客户机”(Virtual KVM Client) 窗口。对于 KX II 本地控制台，显示将从本地用户界面切换到目标服务器。在本地端口上，KX II 本地控制台界面必须可见，才能执行切换。

     ***注意：**如果所有连接都忙，则对于可用端口不能从 KX II 远程控制台使用该选项。*

   - **切换自 (Switch From)**。从现有连接切换到所选端口（目标服务器）。该菜单项可用于每个打开的连接（对于具有 4 个远程用户的设备，最多 4 个连接；对于具有 2 个远程用户的设备，最多 2 个连接；对于具有 1 个远程用户的设备，最多 1 个连接）。该选项仅当一个或多个虚拟 KVM 客户机打开时才可见。

     ***注意：**KX II 本地控制台中未提供该菜单项。*

   - **断开连接 (Disconnect)**。断开该端口的连接，并关闭该目标服务器的“虚拟 KVM 客户机”(Virtual KVM Client) 窗口。该菜单项仅当端口状态为打开及已连接或打开及忙碌时才可用。

     ***注意：**KX II 本地控制台中未提供该菜单项。在本地控制台中，从切换的目标服务器断开连接的唯一方式是使用热键。*

   - **开启电源 (Power On)**。通过相连的插座接通目标服务器的电源。仅当此目标服务器有一个或多个相连的电源、目标服务器关闭（端口处于关闭状态）且用户有权使用该服务时，该选项才可见。
   - **关闭电源 (Power Off)**。通过相连的插座断开目标服务器的电源。仅当此目标服务器有一个或多个相连的电源、目标服务器电源打开（端口处于打开状态）且用户有权使用该服务时，该选项才可见。
   - **电源循环 (Power Cycle)**。通过相连的插座实现目标服务器电源循环。仅当此目标服务器有一个或多个相连的电源且用户有权使用该服务时，该选项才可见。
2. 为要执行操作的端口选择所需的菜单选项。

连接到目标服务器

连接到目标服务器：

1. 在 KX II 远程控制台中，单击“端口访问”**(Port Access)** 选项卡以打开它。将打开“端口访问”**(Port Access)** 页。
2. 单击要访问的目标的“端口名称”**(Port Name)**。将显示“端口操作”**(Port Action)** 菜单：

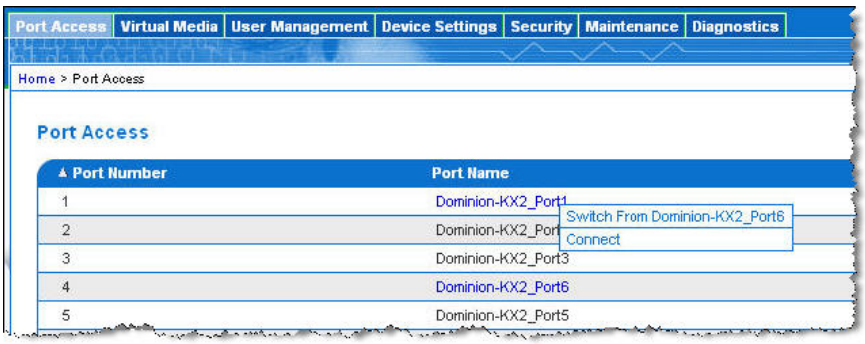


图 24：“端口操作”菜单

3. 选择“连接”**(Connect)**。对于连接到该端口的目标服务器，将打开一个“虚拟 KVM 客户机”(Virtual KVM Client) 窗口。

在目标服务器之间切换

通过 Dominion KX II，您可以访问多台目标服务器。Dominion KX II 提供了从一台目标服务器切换到另一台的功能。

注意：*只有 Dominion KX II 远程控制台提供该功能。*

在目标服务器之间切换：

1. 如果已经在使用目标服务器，请访问 Dominion KX II“端口访问”(Port Access) 页。
2. 单击要立即访问的目标服务器的“端口名称”**(Port Name)**。将显示“端口操作”**(Port Action)** 菜单。
3. 从“端口操作”**(Port Action)** 菜单中选择“切换自”**(Switch From)** 选项。“虚拟 KVM 客户机”(Virtual KVM Client) 窗口切换到刚刚选择的新目标服务器。

断开目标服务器的连接

注意：*KX II 本地控制台中未提供该项。在本地控制台中，从切换的目标服务器断开连接的唯一方式是使用热键。*

断开目标服务器的连接：

1. 单击要断开连接的目标服务器的“端口名称”**(Port Name)**。将显示“端口操作”**(Port Action)** 菜单。
2. 从“端口操作”**(Port Action)** 菜单中选择“断开连接”**(Disconnect)** 选项。“虚拟 KVM 客户机”(Virtual KVM Client) 窗口关闭目标窗口。

---

*提示：您还可以通过从“虚拟 KVM”(Virtual KVM) 菜单中选择“连接”**(Connection)** > “退出”**(Exit)** 来关闭“虚拟 KVM”(Virtual KVM) 窗口。*

对目标服务器进行电源控制

注意：这些功能仅当有相连的电源时才可用。有关详细信息，请参阅电源控制。

实现目标服务器的电源循环

实现目标服务器的电源循环：

1. 在 **KX II** 远程控制台中，单击“端口访问”**(Port Access)** 选项卡以打开它。将打开“端口访问”**(Port Access)** 页。
2. 单击适当目标服务器的“端口名称”**(Port Name)**。将显示“端口操作”**(Port Action)** 菜单。

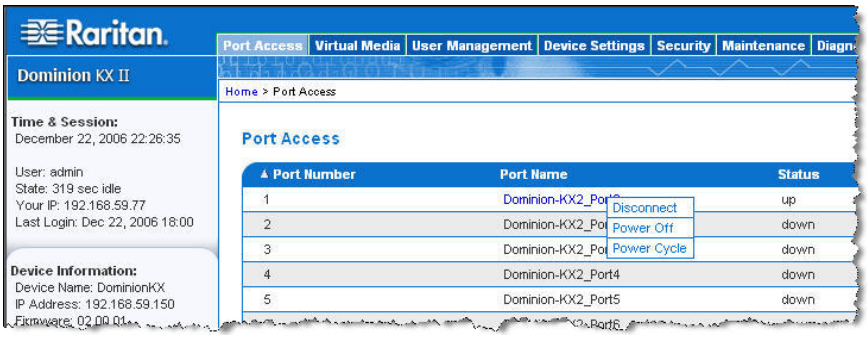


图 25：“端口操作”菜单（电源选项）

3. 选择“电源循环”**(Power Cycle)**。将显示一条消息，确认所采取的操作。

接通目标服务器的电源

接通目标服务器的电源：

1. 在 KX II 远程控制台中，单击“端口访问”**(Port Access)** 选项卡以打开它。将打开“端口访问”(Port Access) 页。
2. 单击适当目标服务器的“端口名称”**(Port Name)**。将显示“端口操作”(Port Action) 菜单。
3. 选择“开启电源”**(Power On)**。

断开目标服务器的电源

断开目标服务器的电源：

1. 在 KX II 远程控制台中，单击“端口访问”**(Port Access)** 选项卡以打开它。将打开“端口访问”(Port Access) 页。
2. 单击适当目标服务器的“端口名称”**(Port Name)**。将显示“端口操作”(Port Action) 菜单。
3. 选择“关闭电源”**(Power Off)**。

第 6 章：虚拟 KVM 客户机

当您使用 KX II 远程控制台访问目标服务器时，将打开一个“虚拟 KVM 客户机”(Virtual KVM Client) 窗口。*每个* 目标服务器都有一个连接的虚拟 KVM 客户机；这些窗口可以通过 Windows 任务栏访问。

“虚拟 KVM 客户机”(Virtual KVM Client) 窗口可以最小化、最大化，以及在计算机桌面上四处移动。

注意：*刷新 HTML 浏览器将关闭虚拟 KVM 客户机连接，因此请谨慎行事。*

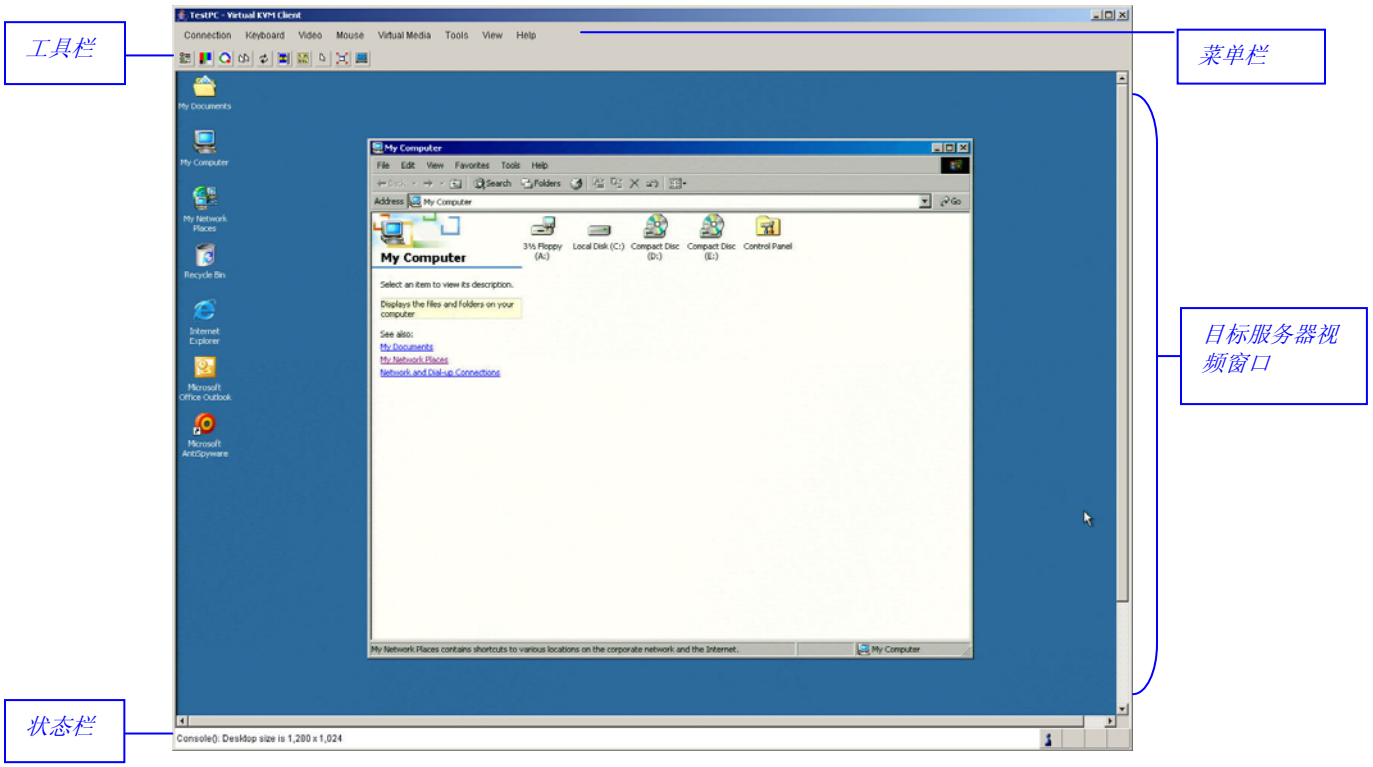


图 26：“虚拟 KVM 客户机”窗口

虚拟 KVM 客户机中的可用功能可通过菜单和工具栏访问。

功能	说明
菜单栏	命令和设置的下拉菜单。
工具栏	常用功能和命令的快捷按钮。
目标服务器视频窗口	目标设备显示。
状态栏	有关连接参数、目标服务器窗口大小、并发连接、Caps Lock 指示器和 Num Lock 指示器的实时信息。

选项

菜单树

下图显示了虚拟 KVM 客户机中的所有可用菜单选项。

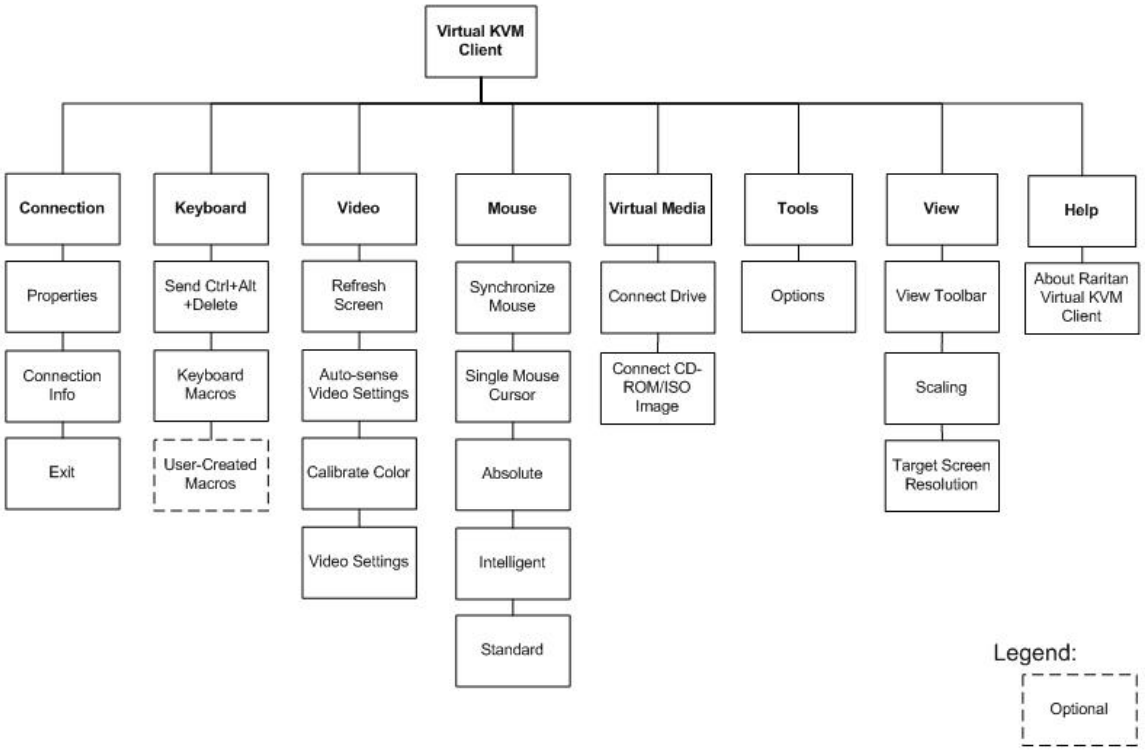


图 27：虚拟 KVM 客户机菜单树

工具栏

按钮	说明
	属性
	视频设置
	校准颜色
	同步客户机与目标服务器鼠标光标
	刷新屏幕
	自动感应视频
	发送 **Ctrl+Alt+Delete**
	切换单/双鼠标模式
	全屏
	调整视频大小以适合屏幕

鼠标指针同步

在远程查看使用鼠标的目标服务器时，您会看到两个鼠标指针：一个属于远程客户机工作站，另一个属于目标服务器。当鼠标指针位于虚拟 KVM 客户机目标服务器窗口*之内*时，鼠标的运动和点击将直接传输到相连的目标服务器。由于鼠标加速设置的缘故，客户机的鼠标指针在运动过程中会稍微领先于目标服务器的鼠标指针。

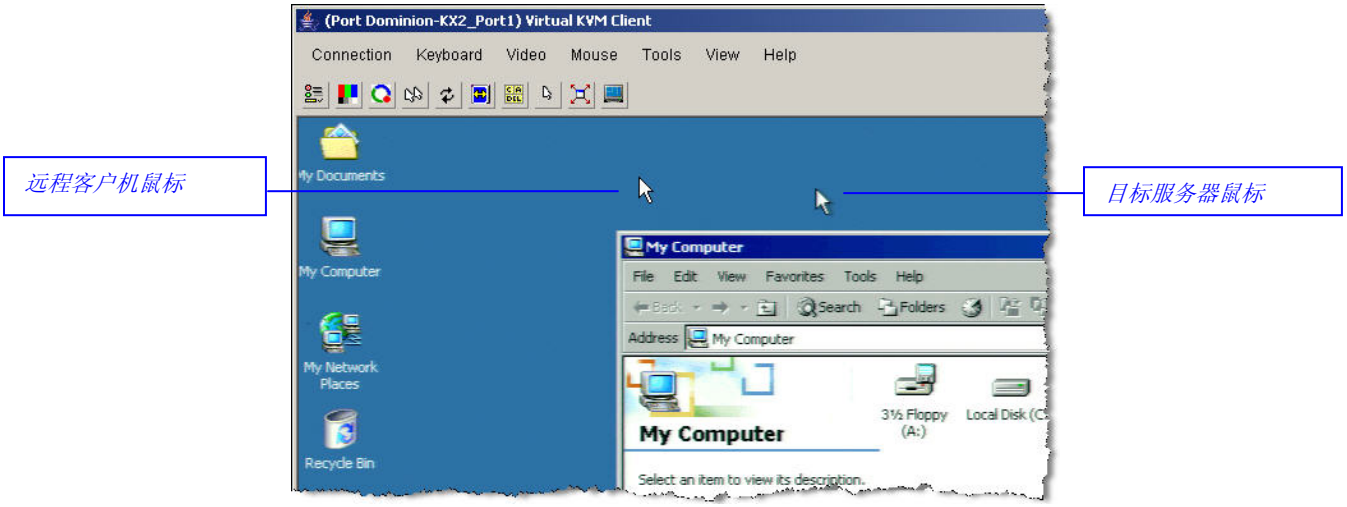


图 28：双鼠标光标

在快速 LAN 连接中，您可能希望禁用虚拟 KVM 客户机的鼠标指针，只查看目标服务器的指针。您可以在这两种模式（单鼠标和双鼠标）之间切换。有关可用鼠标模式的详细信息，请参阅“鼠标”菜单。

“连接”菜单

“属性”对话框

Dominion KX II 动态视频压缩算法保持了 KVM 控制台在不断变化的带宽约束下的可用性。Dominion KX II 设备不仅可以针对 LAN，还可以针对 WAN 和拨号对 KVM 输出进行优化。此外，该设备还能控制颜色深度并限制视频输出，在任意带宽条件下均能在视频质量与系统响应度之间取得最佳平衡。

	连接属性	手动调整与带宽有关的选项（连接速度、颜色深度等）。

对于不同的操作环境，可以根据您的需要对“属性”(Properties) 对话框中的参数进行优化。

设置连接属性：

1. 选择“连接”**(Connection)** >“属性”**(Properties)**。将打开“属性”**(Properties)** 对话框。

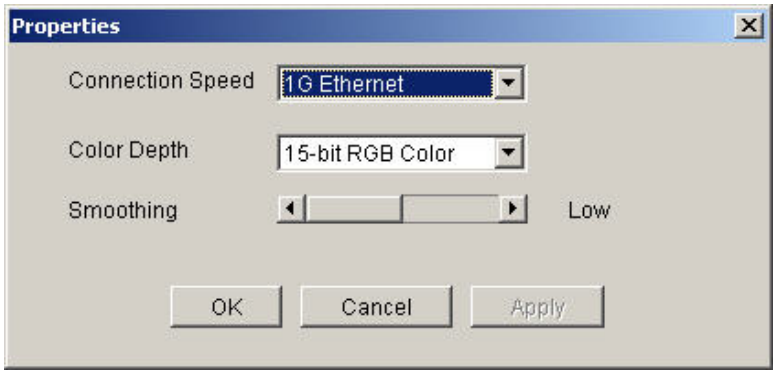


图 29：“属性”对话框

2. 从下拉列表中选择“连接速度”**(Connection Speed)**。Dominion KX II 可以自动检测可用带宽，并且不限制带宽，不过您也可以根据带宽限制调整该使用情况。

自动 (Auto)
1G 以太网 (1G Ethernet)
100 Mb 以太网 (100 Mb Ethernet)
10 Mb 以太网 (10 Mb Ethernet)
1.5 Mb（高速 DSL/T1）(1.5 Mb (MAX DSL/T1))
1 Mb（快速 DSL/T1）(1 Mb (Fast DSL/T1))
512 Kb（中速 DSL/T1）(512 Kb (Medium DSL/T1))
384 Kb（慢速 DSL/T1）(384 Kb (Slow DSL/T1))
256 Kb（电缆）(256 Kb (Cable))
128 Kb（双 ISDN）(128 Kb (Dual ISDN))
56 Kb（ISP 调制解调器）(56 Kb (ISP Modem))
33 Kb（快速调制解调器）(33 Kb (Fast Modem))
24 Kb（慢速调制解调器）(24 Kb (Slow Modem))

请注意，这些设置是针对特定条件而不是确切速度的优化。无论当前网络速度和编码设置如何，客户机和服务器总是会尝试以尽可能快的速度在网络上传递视频。但是如果设置与真实环境相吻合，系统将达到最快的响应速度。

3. 从下拉列表中选择“颜色深度”**(Color Depth)**。Dominion KX II 能动态调整传输到远程用户的颜色深度，以最大化所有带宽条件下的可用性。

15 位 RGB 颜色 (15-bit RGB Color)
8 位 RGB 颜色 (8-bit RGB Color)
4 位彩色 (4-bit Color)
4 位灰度 (4-bit Gray)
3 位灰度 (3-bit Gray)
2 位灰度 (2-bit Gray)
黑白

重要事项：对于大多数管理任务（如服务器监视、重新配置等），不一定需要大多数调制解调器视频图形卡所具备的 24 位或 32 位全色色谱。尝试传输如此高的颜色深度，只会浪费网络带宽。

4. 使用滑块选择所需的“平滑”**(Smoothing)** 级别（仅针对 15 位彩色模式）。平滑级别决定了将具有较小色差的屏幕调和为平滑单色的程度。平滑功能通过降低所显示的视频噪声，改进目标服务器视频的外观。
5. 单击“确定”**(OK)** 设置以上属性。

要取消而不保存更改，请执行以下操作：

单击“取消”**(Cancel)**。

连接信息

获得有关虚拟 KVM 客户机连接的信息：

选择“连接”**(Connection)** >“连接信息”**(Connection Info)**。将打开“连接信息”(Connection Info) 窗口：

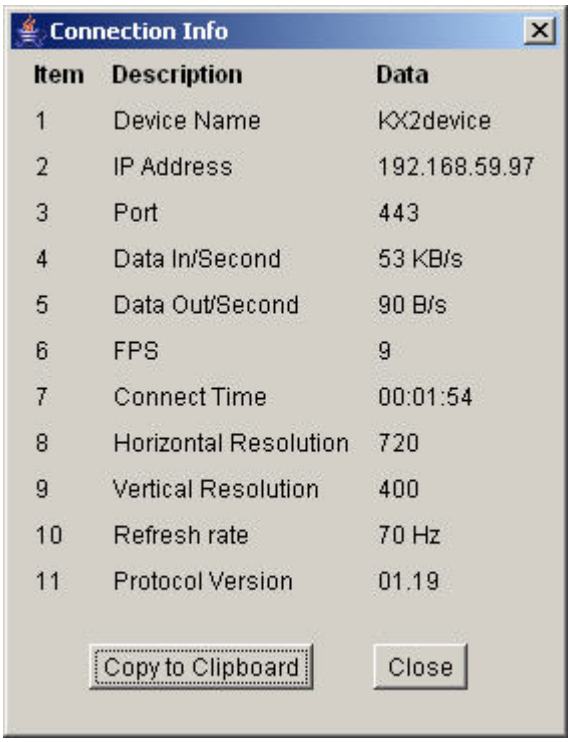


图 30：连接信息

其中显示了有关当前连接的以下信息：

- **设备名称 (Device Name)**。Dominion KX II 设备的名称。
- **IP 地址（IP Address）**。Dominion KX II 设备的 IP 地址。
- **端口（Port）**。用于访问目标服务器的 KVM 通信 TCP/IP 端口。
- **传入的数据/秒 (Data In/Second)**。传入的数据率。
- **传出的数据/秒 (Data Out/Second)**。传出的数据率。
- **连接时间 (Connect Time)**。连接的持续时间。
- **FPS**。每秒传输的视频帧。
- **水平分辨率 (Horizontal Resolution)**。屏幕水平方向上的分辨率。
- **垂直分辨率 (Vertical Resolution)**。屏幕垂直方向上的分辨率。
- **刷新率 (Refresh Rate)**。屏幕的刷新率。
- **协议版本 (Protocol Version)**。RFB 协议版本。

复制该信息：

单击“复制到剪贴板”**(Copy to Clipboard)**。信息可粘贴到您选择的程序中。

退出

关闭虚拟 KVM 客户机（当前访问的目标服务器）：

选择“连接”**(Connection)** >“退出”**(Exit)**。

“键盘”菜单

发送 Ctrl+Alt+Delete

由于 **Ctrl+Alt+Delete** 使用颇为频繁，因此虚拟 KVM 客户机中预先编制了 **Ctrl+Alt+Delete** 宏。

该键序列将发送到当前连接的目标服务器。相反，如果您在使用虚拟 KVM 客户机时按 **Ctrl+Alt+Delete** 键，由于操作系统结构的原因，该命令将首先被您自己的 PC 截取，而不是按照预期的那样将该键序列发送到目标服务器。

	发送 **Ctrl+Alt+Delete**	将 **Ctrl+Alt+Delete** 键序列发送到目标服务器。

将 **Ctrl+Alt+Delete** 键序列发送到目标服务器：

- 选择“键盘”**(Keyboard)** > “发送 Ctrl+Alt+Delete”**(Send Ctrl+Alt+Delete)**，或
- 在工具栏中单击“发送 Ctrl+Alt+Delete”**(Send Ctrl+Alt+Delete)** 按钮。

键盘宏

键盘宏可确保计划用于目标服务器的击键组合被发送到目标服务器，并且只由目标服务器截取。否则，这些击键组合可能会被运行虚拟 KVM 客户机的计算机（您的客户机 PC）截获。

宏存储在客户机 PC 上，并且是该 PC 所专有的；因此，如果您使用其它 PC，将看不到您的宏。此外，如果其他人使用您的 PC 并以不同的用户名登录，则该用户将看到您的宏，因为宏是针对整个计算机的。在虚拟 KVM 客户机中创建的键盘宏可用于 MPC，反之亦然。

创建键盘宏

创建键盘宏（添加宏）：

1. 选择“键盘”**(Keyboard)** > “键盘宏”**(Keyboard Macros)**。将打开“键盘宏”(Keyboard Macros) 窗口：

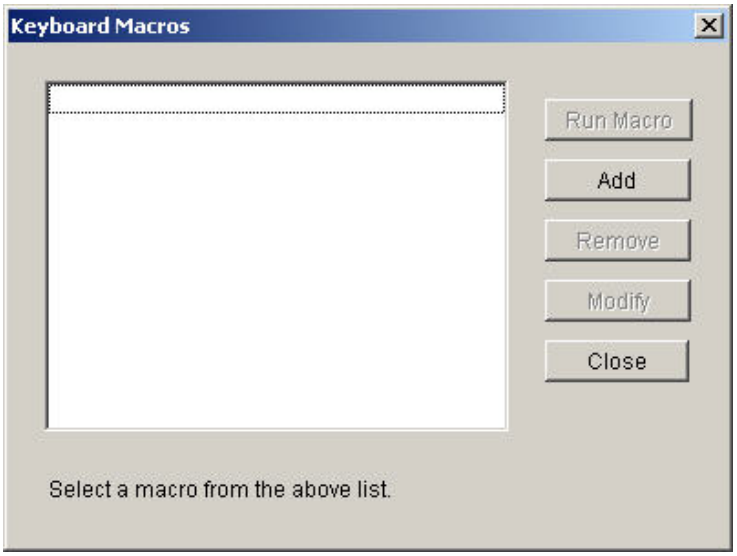


图 31：键盘宏

2. 单击“添加”**(Add)**。将打开“添加键盘宏”**(Add Keyboard Macro)** 窗口：

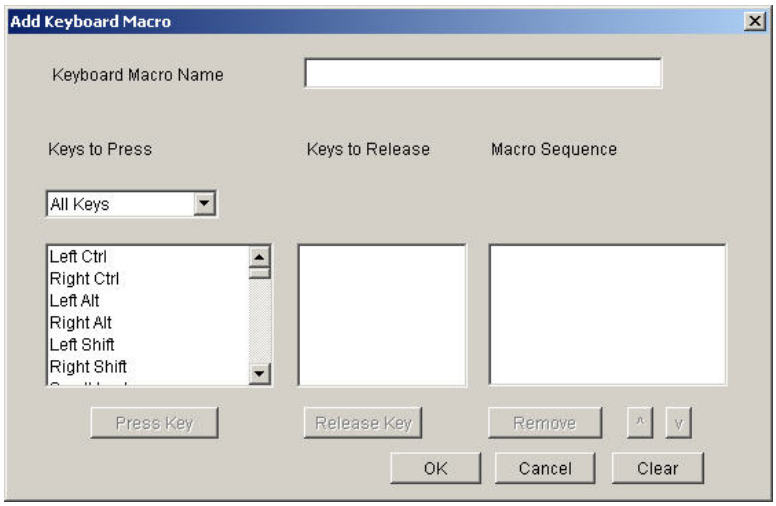


图 32：添加键盘宏

3. 在“键盘宏名称”**(Keyboard Macro Name)** 字段中键入名称。创建宏之后，该名称将显示在虚拟 **KVM** 客户机菜单栏上。在本例中，键入“最小化所有窗口”**(Minimize All Windows)**。
4. 在“要按的键”**(Keys to Press)** 下拉列表中：
   a. 滚动并选择要模拟其按键操作的每个键（按照按下的顺序）。
   b. 每次选择之后单击“按键”**(Press Key)**。选择每个键后，该键将显示在“要松开的键”**(Keys to Release)** 字段中。

   *在本例中，*选择两个键：**Windows** 键和字母 **D** 键。
5. 在“要松开的键”**(Keys to Release)** 字段中：
   a. 选择要模拟其松开键操作的每个键（按照松开的顺序）。
   b. 每次选择之后单击“松开键”**(Release Key)**。

   *在本例中，*按下的两个键还必须松开。

6. 检查“宏序列”**(Macro Sequence)**，该序列是通过选择“要按的键”**(Keys to Press)** 和“要松开的键”**(Keys to Release)** 自动生成的。验证“宏序列”**(Macro Sequence)** 确实是您所需的键序列。（要删除序列中的某个步骤，请选择该步骤并单击“删除”**(Remove)**。）

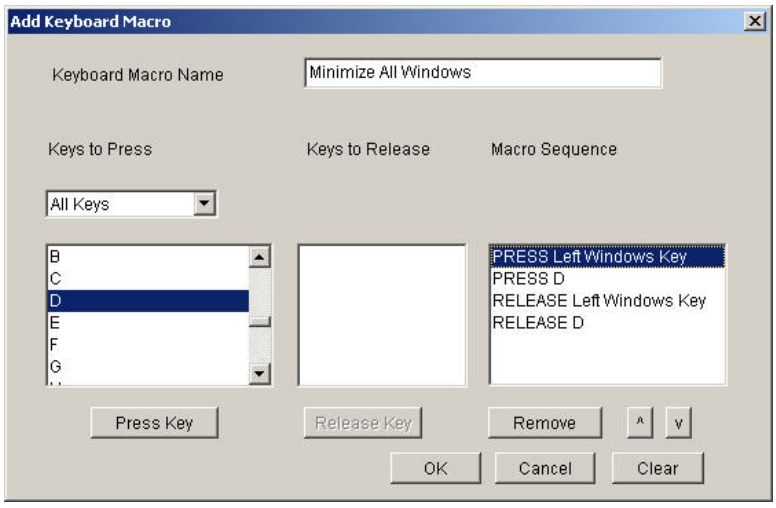


图 33：键盘宏示例

提示：可使用 ∧ 和 ∨ 键对键序列重新排序。

7. 在“添加键盘宏”**(Add Keyboard Macro)** 窗口中单击“确定”**(OK)**，以保存宏。
8. 在“键盘宏”**(Keyboard Macros)** 窗口（图 31）中单击“关闭”**(Close)**。创建的键盘宏现在作为“键盘”**(Keyboard)** 菜单的选项列出：



图 34：“键盘”菜单中的“新建宏”

要取消而不保存更改，请执行以下操作：

单击“取消”**(Cancel)**。

清除所有字段并重新开始：

单击“清除”**(Clear)** 按钮。

运行键盘宏

创建键盘宏之后，可以通过在“键盘”**(Keyboard)** 菜单中单击其名称来执行该键盘宏。

执行宏（使用本例）：

选择“键盘”**(Keyboard)** > “最小化所有窗口”**(Minimize All Windows)**。

还有一种方法是从“键盘宏”**(Keyboard Macros)** 窗口中选择该宏。

执行宏：

1. 选择“键盘”**(Keyboard)** > “键盘宏”**(Keyboard Macros)**。将打开“键盘宏”(Keyboard Macros) 窗口。
2. 从列出的键盘宏中选择宏。
3. 单击“运行宏”**(Run Macro)**。

修改键盘宏

修改宏：

1. 选择“键盘”**(Keyboard)** > “键盘宏”**(Keyboard Macros)**。将打开“键盘宏”(Keyboard Macros) 窗口。
2. 从列出的键盘宏中选择宏。
3. 单击“修改”**(Modify)**。将打开“添加/编辑宏”**(Add/Edit Macro)** 窗口。
4. 进行修改。
5. 单击“确定”**(OK)**。

删除键盘宏

请谨慎删除宏，因为系统不会提示您确认删除。

删除宏：

1. 选择“键盘”**(Keyboard)** > “键盘宏”**(Keyboard Macros)**。将打开“键盘宏”(Keyboard Macros) 窗口。
2. 从列出的键盘宏中选择宏。
3. 单击“删除”**(Remove)**。宏将被删除。

“视频”菜单

视频设置可以通过以下几种方式自动刷新：

- “刷新屏幕”**(Refresh Screen)** 选项会强制刷新视频屏幕。
- “自动感应视频设置”**(Auto-sense Video Settings)** 选项会自动检测目标服务器的视频设置。
- “校准颜色”**(Calibrate Color)** 选项会校准视频，以改善显示的颜色。

此外，您还可以使用“视频设置”**(Video Settings)** 选项手动调整设置。

刷新屏幕

“刷新屏幕”**(Refresh Screen)** 选项会强制刷新视频屏幕。整个视频屏幕将重新绘制。

	“刷新屏幕”(Refresh Screen) 按钮

刷新视频设置：

- 选择“视频”**(Video)** > “刷新屏幕”**(Refresh Screen)**，或
- 在工具栏中单击“刷新屏幕”**(Refresh Screen)** 按钮。

自动感应视频设置

“自动感应视频设置”(Auto-sense Video Settings) 选项会强制重新感应视频设置（分辨率、刷新率），并重新绘制视频屏幕。

	“自动感应视频设置”(Auto-Sense Video Settings) 按钮

自动检测视频设置：

- 选择“视频”**(Video)** > “自动感应视频设置”**(Auto-sense Video Settings)**，或
- 在工具栏上单击“自动感应视频设置”**(Auto-sense Video Settings)** 按钮。

将显示一条消息，表示正在进行自动调整。

校准颜色

可以使用“校准颜色”(Calibrate Color) 命令优化所传输视频图像的颜色级别（色调、亮度、饱和度）。Dominion KX II 颜色设置以目标服务器为基础。

	校准颜色	调整颜色设置以优化视频显示。

***注意：** “校准颜色”(Calibrate Color) 选项仅适用于当前连接。*

校准颜色：

1. 打开运行图形用户界面的任意目标服务器的远程 **KVM** 连接。
2. 选择“视频”**(Video)** > “校准颜色”**(Calibrate Color)**（或单击“校准颜色”**(Calibrate Color)** 按钮）。目标设备将更新其颜色校准。

视频设置

可以使用“视频设置”(Video Setting) 选项手动调整视频设置。

	视频设置	打开“视频设置”(Video Settings) 以手动调整视频参数。

更改视频设置：

1. 选择“视频”**(Video)** >“视频设置”**(Video Settings)**。将打开“视频设置”**(Video Settings)** 窗口，其中显示了当前设置：

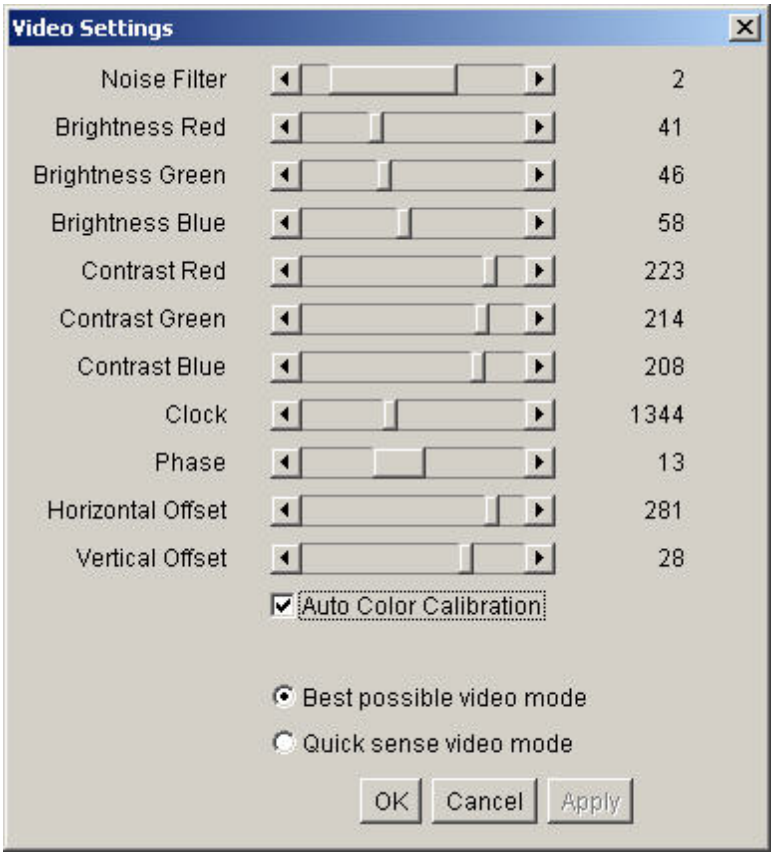


图 35：视频设置

2. 使用滑块调整设置，以获得所需的效果（在调整设置时，效果会立即显现出来）：
   - **噪声过滤 (Noise Filter)**。Dominion KX II 可以过滤掉图形卡视频输出的电子干扰。该功能不仅能优化图片质量，还可减少带宽的使用。如果设置较高，那么只有在与相邻像素存在较大色差时，才传输不同的像素。不过，将阈值设置过高会导致无意中过滤掉想要的屏幕变化。

     如果设置较低，则传输大部分像素变化。将该阈值设置过低会增加带宽的使用量。
   - **亮度 (Brightness)**：该设置用于调整目标服务器显示的亮度。
     - **红 (Red)**。控制红色信号的亮度。
     - **绿 (Green)**。控制绿色信号的亮度。
     - **蓝 (Blue)**。控制蓝色信号的亮度。

– 颜色对比度设置：控制对比度调整。
  - **红色对比度 (Contrast Red)**。控制红色信号。
  - **绿色对比度 (Contrast Green)**。控制绿色信号。
  - **蓝色对比度 (Contrast Blue)**。控制蓝色信号。
– 如果视频图像看起来相当模糊或焦距不实，那么可以调整时钟和相位，直至活动目标服务器上显示出较清晰的图像。

警告：请谨慎更改时钟和相位设置，这么做可能会导致视频丢失或失真，而且您可能无法回到之前的状态。在进行任何更改之前，请与 Raritan 技术支持部门联系。

  - **时钟 (Clock)**。控制视频像素在视频屏幕上的显示速度。更改时钟设置会导致视频图像在水平方向上拉长或缩短。建议采用奇数设置。大多数情况下，不应当更改该设置，因为自动检测通常都非常精确。
  - **相位 (Phase)**。相位值范围为 0 到 31，而且将回绕。请停在为活动目标服务器生成最佳视频图像的相位值处。
– 偏移：控制屏幕的位置：
  - **水平偏移 (Horizontal Offset)**。控制目标服务器显示在您显示器上的水平位置。
  - **垂直偏移 (Vertical Offset)**。控制目标服务器显示在您显示器上的垂直位置。
– **自动颜色校准 (Auto Color Calibration)**。如果希望进行自动颜色校准，选中该选项。
– **视频感应 (Video Sensing)**：选择视频感应模式：
  - **最佳视频模式 (Best possible video mode)**：Dominion KX II 在切换目标服务器或目标分辨率时将执行完整的自动感应过程。选择该选项可校准视频，以获得最佳的图像质量。
  - **快速感应视频模式 (Quick sense video mode)**：使用该选项时，Dominion KX II 将使用快速视频自动感应，以尽快显示目标服务器的视频。如果要在重新引导之后立即进入目标服务器的 BIOS 配置，该选项尤为有用。

3. 单击“应用”**(Apply)**。视频设置将进行更改。

***注意：**某些 Sun 背景屏幕（如带深黑色边框的屏幕）在某些 Sun 服务器上可能无法准确居中。可以使用其它背景或在屏幕的左上角放置一个浅颜色的图标。*

保存更改同时取消：

单击“取消”**(Cancel)**。

“鼠标”菜单

在控制目标服务器时，KX II 远程控制台显示两个鼠标光标：一个属于客户机工作站，另一个属于目标服务器。您既可以在单鼠标模式下，也可以在双鼠标模式下操作。如果采用双鼠标模式且配置正确，那么这两个鼠标光标将一致。如果在鼠标同步方面遇到问题，请参阅配置目标服务器。

当有两个鼠标光标时，Dominion KX II 提供了以下几种鼠标模式：

- 绝对（鼠标同步）
- 智能（鼠标模式）
- 标准（鼠标模式）

同步鼠标

在双鼠标模式下，“同步鼠标”(Synchronize Mouse) 会强制目标服务器的鼠标指针与虚拟 KVM 客户机的鼠标指针重新取得一致。

	同步鼠标

同步鼠标：

- 选择“鼠标”**(Mouse) >**“同步鼠标”**(Synchronize Mouse)**，或
- 在工具栏中单击“同步鼠标”(Synchronize Mouse) 按钮。

单鼠标光标

“单鼠标光标”(Single Mouse Cursor) 将进入单鼠标模式，在该模式下只显示目标服务器鼠标光标，本地 PC 的鼠标指针不再显示在屏幕上。当处于单鼠标模式下时，“同步鼠标”(Synchronize Mouse) 选项不再可用（无需同步单个鼠标光标）。

	单鼠标光标

进入单鼠标模式：

- 选择“鼠标”**(Mouse) >**“单鼠标光标”**(Single Mouse Cursor)**，或
- 在工具栏中单击“单/双鼠标光标”(Single/Double Mouse Cursor) 按钮。

退出单鼠标模式：

1. 进入单鼠标模式时，会显示以下消息：单击“确定”**(OK)**。

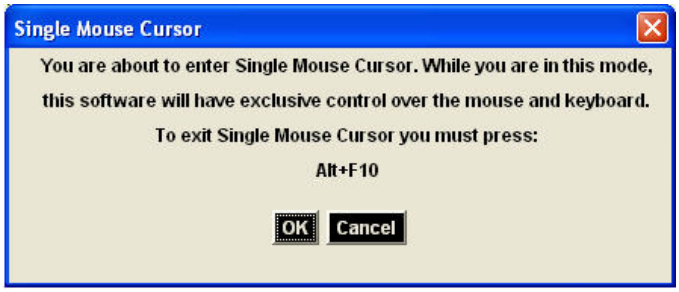


图 36：单鼠标光标消息

2. 在键盘上按 **Alt+F10** 可退出单鼠标模式。

标准

这是采用相对鼠标位置的标准鼠标同步算法。标准鼠标模式要求禁用加速并正确设置其它鼠标参数，以使客户机和服务器鼠标能够保持同步。标准鼠标模式为默认的鼠标模式。

进入标准鼠标模式：

选择“鼠标”**(Mouse) >**“标准”**(Standard)**。

智能

在智能鼠标模式下，Dominion KX II 可以检测目标鼠标设置，并据此同步鼠标指针，同时允许目标服务器上启用鼠标加速。在该模式下，鼠标光标在屏幕的左上角“舞动”，并计算加速。要使该模式正确运行，必须满足某些条件。

有关智能鼠标模式的其它信息，请参阅“*Raritan Multi-Platform Client 用户指南*”*(Raritan Multi-Platform Client User Guide)*（*附录 B：智能鼠标同步条件*），可在 Raritan 网站 http://www.raritan.com/support/productdocumentation 或 Dominion KX II 附带的“*Raritan 用户手册和快速设置指南 CD ROM*”上找到。

进入智能鼠标模式：

选择“鼠标”**(Mouse) >**“智能”**(Intelligent)**。

绝对

注意：*绝对鼠标同步仅用于支持虚拟媒体的 USB CIM (D2CIM-VUSB)。*

在该模式下，采用绝对坐标来保持客户机与目标服务器的指针同步，即使目标服务器鼠标设置为不同的加速或速度时也如此。带 USB 端口的服务器可支持该模式。鼠标将移动到目标服务器上的确切位置。

进入绝对鼠标模式：

选择“鼠标”**(Mouse) >**“绝对”**(Absolute)**。

虚拟媒体

有关设置和使用虚拟媒体的完整信息，请参阅有关虚拟媒体的章节。

“工具”菜单

选项

在“工具”(Tools) 菜单中，可以指定用于虚拟 KVM 客户机的某些选项：处于双鼠标模式时同步鼠标、启用日志记录、键盘类型以及退出目标屏幕分辨率模式的热键。

设置工具选项：

1. 选择“工具”**(Tools) >**“选项”**(Options)**。将打开“选项”(Options) 窗口：

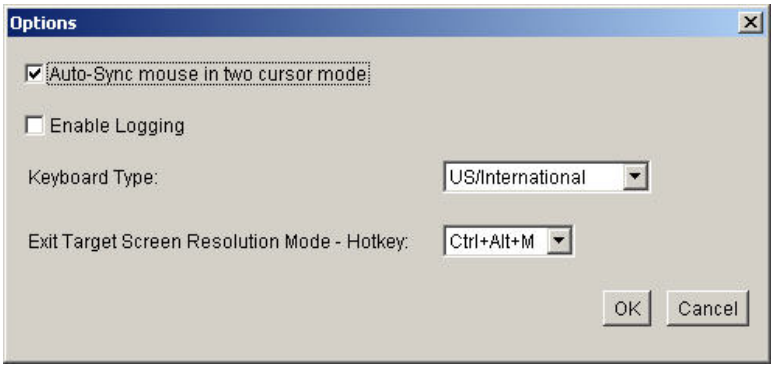


图 37：（工具）选项

2. 选中要启用的选项旁的复选框：
   - **在双光标模式下自动同步鼠标 (Auto Sync Mouse in Two Cursor Mode)**。选中该选项可在双鼠标模式下操作时自动同步鼠标光标。
   - **启用日志记录 (Enable Logging)**。该选项必须在技术支持部门的指导下使用。该选项会在您的主目录中创建一个日志文件。
3. 如果必要，从下拉列表中选择“键盘类型”**(Keyboard Type)**。这些选项包括：
   - 美国英语/国际 (US/International)
   - 法语（法国）(French (France))
   - 德语（德国）(German (Germany))
   - 日语 (Japanese)
   - 英国 (United Kingdom)
   - 朝鲜语（韩国）(Korean (Korea))
4. **退出目标屏幕分辨率模式—热键 (Exit Target Screen Resolution Mode - Hotkey)**。进入目标屏幕分辨率模式时，目标服务器的显示将变为全屏，并获得与目标服务器同样的分辨率。这是用于退出该模式的热键。从下拉列表中进行选择。
5. 单击“确定”**(OK)**。

“视图”菜单

查看工具栏

您可以在显示或不显示工具栏的情况下使用虚拟 KVM 客户机。

切换工具栏的显示（打开和关闭）：

选择“视图”**(View) >**“查看工具栏”**(View Toolbar)**。

缩放

通过缩放目标窗口，可以查看目标服务器窗口的整个内容。该功能可扩大或缩小目标视频的大小，使之适合虚拟 KVM 客户机窗口的大小，并保持长宽比不变以便您使用滚动条查看整个目标服务器桌面。

切换缩放（打开和关闭）：

选择“视图”**(View) >**“缩放”**(Scaling)**。

目标屏幕分辨率

进入目标屏幕分辨率模式时，目标服务器的显示将变为全屏，并获得与目标服务器同样的分辨率。用于退出该模式的热键在“选项”(Options) 对话框中指定（默认热键为 **Ctrl+Alt+M**）。

进入目标屏幕分辨率：

选择“视图”**(View) >**“目标屏幕分辨率”**(Target Screen Resolution)**。

退出目标屏幕分辨率模式：

按下在图 37 中配置的热键。默认热键为 **Ctrl+Alt+M**。

“帮助”菜单

关于 Raritan 虚拟 KVM 客户机

当您需要从 Raritan 技术支持部门获得帮助时，该菜单选项提供了有关虚拟 KVM 客户机的版本信息。

获得版本信息：

选择“帮助”**(Help) >**“关于 Raritan 虚拟 KVM 客户机”**(About Raritan Virtual KVM Client)**。

第 7 章：虚拟媒体

概要

虚拟媒体通过允许目标服务器远程访问客户机 PC 和网络文件服务器的媒体，扩展了 KVM 功能。借助该功能，安装在客户机 PC 和网络文件服务器上的媒体基本上可由目标服务器*虚拟安装*。随后，目标服务器可以对该媒体进行读写，就好像该媒体是物理连接到目标服务器本身一样。虚拟媒体可以包括内部和 USB 安装的 CD 和 DVD 驱动器、USB 大容量存储设备、PC 硬盘驱动器和 ISO 映像（磁盘映像）。

虚拟媒体提供了远程执行更多任务的能力，如：

- 传输文件
- 运行诊断
- 安装或修补应用程序
- 使用可从客户机访问的可启动的 CD ISO 映像重新引导网络上的目标服务器
- 完成操作系统的安装

该 KVM 控制功能扩展功能可以节省来回数据中心的旅途，并节省时间与金钱，从而使得虚拟媒体功能非常强大。

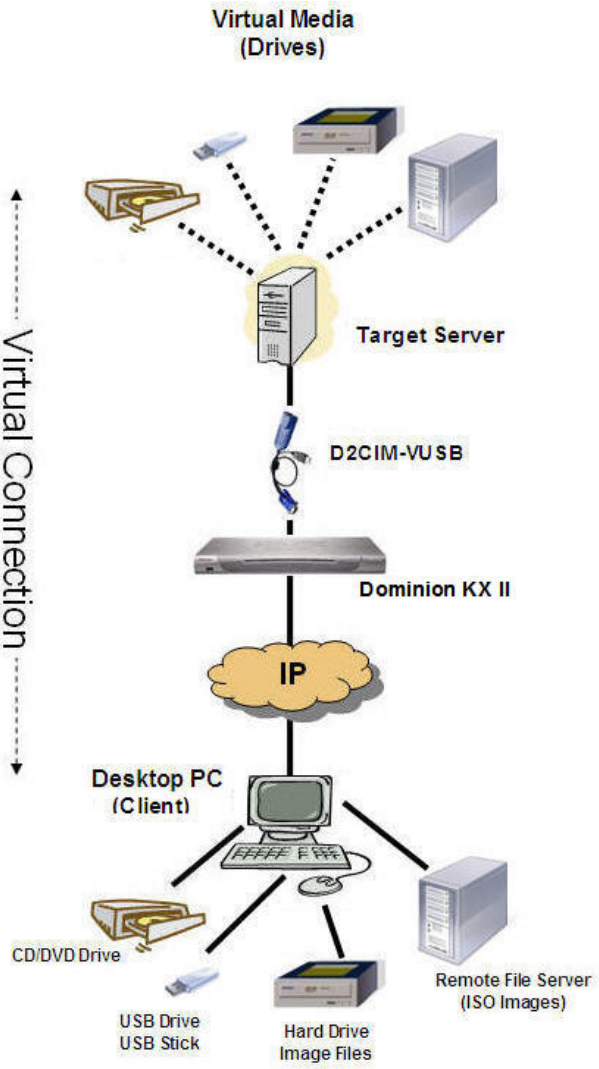


图 38：虚拟媒体连接

使用虚拟媒体的先决条件

要使用虚拟媒体，必须满足以下条件：

Dominion KX II

- 对于需要访问虚拟媒体的用户，必须设置 KX 权限以允许访问相关的端口，同时还必须设置这些端口的虚拟媒体访问权限（“VM 访问”(VM Access) 端口权限）。端口权限在组级别设置。有关详细信息，请参阅设置端口权限。
- （可选）如果要使用 PC 共享，那么还必须在“安全设置”(Security Settings) 页中启用 VM 共享模式。

客户机 PC

- 某些虚拟媒体选项需要对客户机 PC 具有管理权限（例如，整个驱动器的驱动器重定向）。

  注意：*在 Microsoft Vista 中，必须**关闭**用户帐户控制：“控制面板”**(Control Panel)** > “用户帐户”(User Accounts) > “用户帐户控制”(User Account Control) > “关闭”(turn off)。*

- USB 2.0 端口速度更快，是首选端口。

目标服务器

- 目标服务器必须支持 USB 连接的设备。
- 运行 Windows 2000 的目标服务器必须安装了最近所有的修补程序。

使用虚拟媒体

借助 Dominion KX II 虚拟媒体功能，您可以安装最多两个（不同类型的）驱动器。在 KVM 会话期间，可访问这些驱动器。

例如，您可以安装并使用特定 CD-ROM，然后在完成后断开其连接。不过，CD-ROM 虚拟媒体“通道”将保持打开状态，以便您能虚拟安装另一个 CD-ROM。这些虚拟媒体“通道”的打开状态将保持到 KVM 会话结束为止。

使用虚拟媒体：

1. 将媒体连接到要从目标服务器访问的客户机或网络文件服务器。该步骤并不一定是第一步，但必须在尝试访问该媒体**之前**完成。
2. 检验是否满足了适当的先决条件。
3. *（仅针对文件服务器 **ISO** 映像）*如果计划访问文件服务器 **ISO** 映像，请通过 **Dominion KX II** 远程控制台“文件服务器设置”(File Server Setup) 页确认这些文件服务器和映像。
4. 用适当的目标服务器打开一个 KVM 会话。
5. 连接到虚拟媒体。

对于：	选择该 VM 选项：
本地驱动器	连接驱动器（Connect Drive）
本地 CD/DVD 驱动器	连接 CD-ROM/ISO 映像 (Connect CD-ROM/ISO Image)
ISO 映像	连接 CD-ROM/ISO 映像 (Connect CD-ROM/ISO Image)
文件服务器 ISO 映像	连接 CD-ROM/ISO 映像 (Connect CD-ROM/ISO Image)

6. 完成任务之后，断开虚拟媒体。

打开 KVM 会话

打开 KVM 会话：

1. 从 **Dominion KX II** 远程控制台打开“端口访问”**(Port Access)** 页。

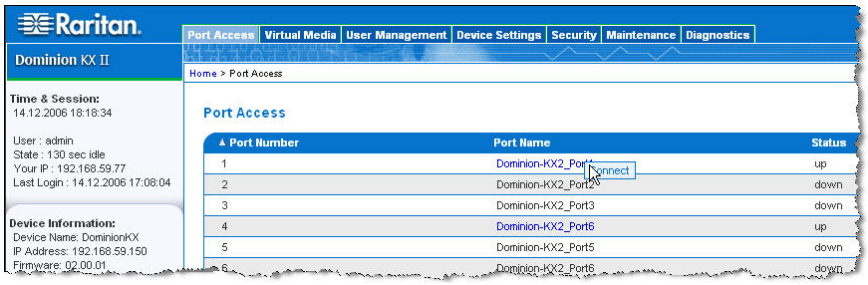


图 39：打开 KVM 会话

2. 从“端口访问”(Port Access) 页连接到目标服务器：
   a. 单击适当服务器的“端口名称”**(Port Name)**。
   b. 从“端口操作”(Port Action) 菜单中选择“连接”**(Connect)** 选项。

该目标服务器在“虚拟 KVM 客户机”(Virtual KVM Client) 窗口中打开。

连接到虚拟媒体

本地驱动器

该选项安装*整个* 驱动器。整个磁盘驱动器*虚拟安装* 到目标服务器上。该选项只能用于硬盘驱动器和外部驱动器，不包括网络驱动器、CD-ROM 或 DVD-ROM 驱动器。只有该选项提供了**读写**功能。

***注意：**在 NTFS 格式的分区（如本地 C 盘驱动器）重定向至新的大容量存储连接之后，运行某些 Windows 操作系统版本的目标服务器可能无法接受这些连接。如果发生这种情况，请关闭 KX II 远程控制台，并重新连接，然后再重定向其它虚拟媒体设备。如果还有其他用户连接到同一台目标服务器，那么该用户也必须关闭与目标服务器的连接。*

访问客户机计算机上的驱动器：

1. 在虚拟 KVM 客户机中，选择“虚拟媒体”**(Virtual Media)** >“连接驱动器”**(Connect Drive)**。将打开“映射虚拟媒体驱动器”**(Map Virtual Media Drive)** 对话框：

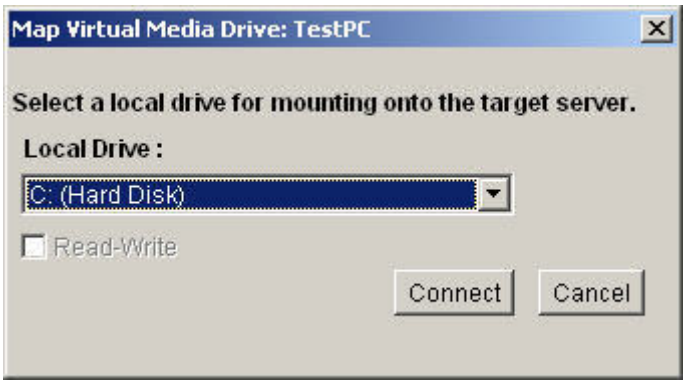


图 40：映射虚拟媒体驱动器

2. 从“本地驱动器”**(Local Drive)** 下拉列表中选择驱动器。
3. 如果需要读写功能，请选中“读-写”**(Read-Write)** 选项复选框。对于固定驱动器，该选项是禁用的。有关详细信息，请参阅什么情况下读写不可用。选中该选项后，便可以读或写所连接的 **USB** 磁盘。

警告：启用读写访问可能很危险！从多个实体同时访问同一个驱动器可能会导致数据损坏。如果您不需要写访问，请不要选中该选项。

4. 单击“连接”**(Connect)**。媒体将虚拟安装在目标服务器上。您可以像访问其它任何驱动器一样访问该媒体。

什么情况下读写不可用

虚拟媒体读写在以下情况下不可用：

- 对于所有硬盘驱动器。
- 驱动器具有写保护时。
- 用户没有读写权限时：
- “访问”**(Access)** 端口权限设置为“无”(None) 或“查看”(View)。
- “VM 访问”**(VM Access)** 端口权限设置为“只读”(Read-Only) 或“拒绝”(Deny)。

CD-ROM/DVD-ROM/ISO 映像

该选项安装 CD-ROM、DVD-ROM 和 ISO 映像。

访问 CD-ROM、DVD-ROM 或 ISO 映像：

1. 在虚拟 **KVM** 客户机中，选择“虚拟媒体”**(Virtual Media)** >“连接 **CD-ROM/ISO** 映像”**(Connect CD-ROM/ISO Image)**。将打开“映射虚拟媒体 CD/ISO 映像”(Map Virtual Media CD/ISO Image) 对话框：

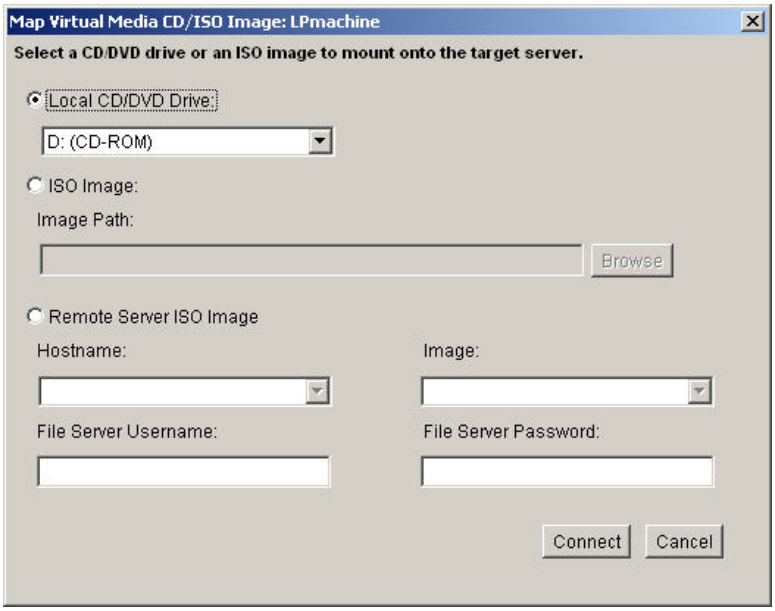


图 41：映射虚拟媒体 CD/ISO 映像

2. 对于内部和外部 CD-ROM 或 DVD-ROM 驱动器：
   a. 选择“本地 CD/DVD 驱动器”**(Local CD/DVD Drive)** 选项。
   b. 从“本地 CD/DVD 驱动器”**(Local CD/DVD Drive)** 下拉列表中选择驱动器。所有可用的内部和外部 CD 和 DVD 驱动器名称将填充到该下拉列表中。
   c. 单击“连接”**(Connect)**。
3. 对于 **ISO** 映像：
   a. 选择“ISO 映像”**(ISO Image)** 选项。如果要访问 CD、DVD 或硬盘驱动器的磁盘映像，可使用该选项。ISO 格式是唯一支持的格式。
   b. 单击“浏览”**(Browse)** 按钮。
   c. 导航至包含要使用的磁盘映像的路径，然后单击“打开”**(Open)**。该路径将填充到“映像路径”**(Image Path)** 字段中。
   d. 单击“连接”**(Connect)**。
4. 对于文件服务器上的远程 ISO 映像：
   a. 选择“远程服务器 ISO 映像”**(Remote Server ISO Image)** 选项。
   b. 从下拉列表中选择“主机名”**(Hostname)** 和“映像”**(Image)**。可用的文件服务器和映像路径是使用“文件服务器设置”(File Server Setup) 页配置的服务器和路径。下拉列表中只包含使用 Dominion KX II“文件服务器设置”**(File Server Setup)** 页配置的项。
   c. **文件服务器用户名 (File Server Username)**。访问文件服务器所需的用户名。
   d. **文件服务器密码 (File Server Password)**。访问文件服务器所需的密码（当您输入时该字段将屏蔽）。
   e. 单击“连接”**(Connect)**。

媒体将虚拟安装在目标服务器上。您可以像访问其它任何驱动器一样访问该媒体。

断开虚拟媒体

断开虚拟媒体：

- 对于本地驱动器，选择“虚拟媒体”**(Virtual Media)** > “断开驱动器”**(Disconnect Drive)**。
- 对于 CD-ROM、DVD-ROM 和 ISO 映像，选择“虚拟媒体”**(Virtual Media)** > “断开 CD-ROM/ISO 映像”**(Disconnect CD-ROM/ISO Image)**。

注意：*除了使用“断开连接”(Disconnect) 选项断开虚拟媒体之外，仅仅关闭 KVM 连接也可关闭虚拟媒体。*

文件服务器设置（仅针对文件服务器 ISO 映像）

注意：仅当使用虚拟媒体访问文件服务器 ISO 映像时，才需要该功能。

可以使用 Dominion KX II 远程控制台“文件服务器设置”(File Server Setup) 页指定要使用 Dominion KX II 虚拟媒体访问的文件服务器和映像路径。此处指定的文件服务器 ISO 映像将成为**“远程服务器 ISO 映像主机名”(Remote Server ISO Image Hostname)** 和“映像”(Image) 下拉列表（位于“映射虚拟媒体 ISO 映像”(Map Virtual Media CD/ISO Image) 对话框中）中的可选项。

指定用于虚拟媒体访问的文件服务器 ISO 映像：

1. 从 Dominion KX II 远程控制台中选择“虚拟媒体”**(Virtual Media)**。将打开“文件服务器设置”(File Server Setup) 页：

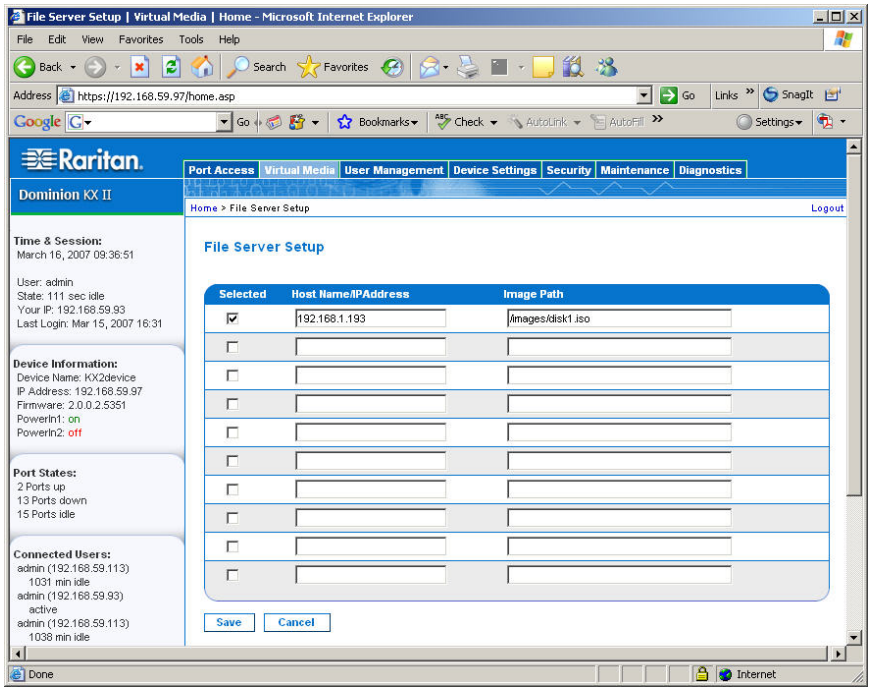


图 42：文件服务器设置

2. 输入有关要访问的文件服务器 ISO 映像的信息：
   - **主机名/IP 地址 (Host Name/IP Address)**。文件服务器的主机名或 IP 地址。
   - **映像路径 (Image Path)**。ISO 映像位置的完整路径名。
3. 选中要作为虚拟媒体访问的所有媒体的“选定”**(Selected)** 复选框。
4. 单击“保存”**(Save)**。此处指定的所有媒体现在可作为“映射虚拟媒体 CD/ISO 映像”(Map Virtual Media CD/ISO Image) 对话框中的选择项。

不保存而取消：

单击“取消”**(Cancel)**。

第 8 章：用户管理

“用户管理”(User Management) 菜单按以下各项进行组织：“用户列表”(User List)、“添加新用户”(Add New User)、“用户组列表”(User Group List)、“添加新用户组”(Add New User Group)、“更改密码”(Change Password) 和“认证设置”(Authentication Settings)。

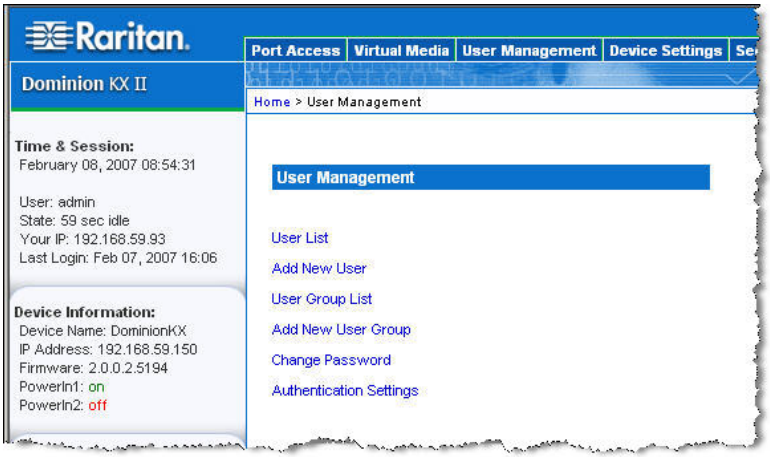


图 43：用户管理菜单

使用：	目的：
用户列表	显示所有用户的字母顺序列表；添加、修改或删除用户。
添加新用户	添加新用户；修改用户信息。
用户组列表	显示所有用户组的字母顺序列表；添加、修改或删除用户组。
添加新用户组	添加新用户组；修改用户组信息。
更改密码	更改特定用户的密码。
认证设置	配置用于访问 Dominion KX II 的认证的类型。

用户列表

“用户列表”(User List) 页显示所有用户的列表，包括其用户名、全名和用户组。单击列名可按任何列对该列表进行排序。在“用户列表”(User List) 页中，还可以添加、修改或删除用户。

要查看用户列表，请执行以下操作：

选择“用户管理”**(User Management)** > “用户列表”**(User List)**。将打开“用户列表”(User List) 页：

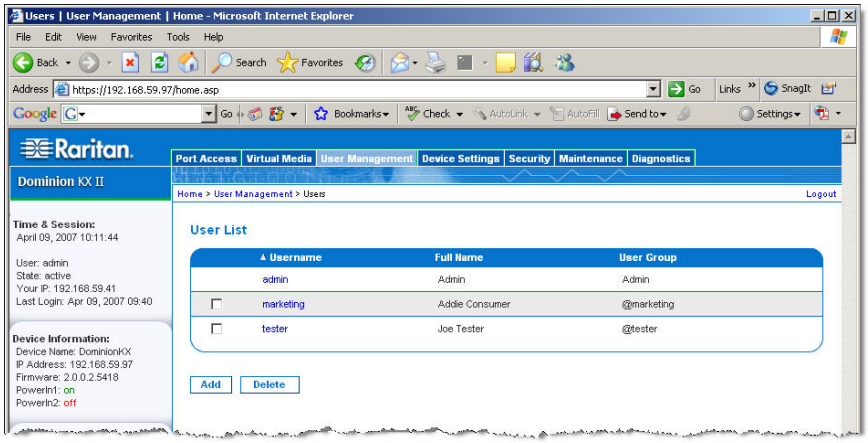


图 44：用户列表

要添加新用户，请执行以下操作：

单击“添加”**(Add)** 按钮。将打开“用户”**(User)** 页。有关“用户”(User) 页的完整信息，请参阅添加新用户。

要修改现有用户，请执行以下操作：

1. 在列出的用户中查找该用户。
2. 单击“用户名”**(Username)**。将打开“用户”**(User)** 页。有关编辑用户的完整信息，请参阅修改现有用户。

要删除用户，请执行以下操作：

1. 选中“用户名”**(Username)** 左侧的复选框，从列出的用户中选择用户。
2. 单击“删除”**(Delete)**。
3. 系统将提示您确认删除。单击“确定”**(OK)**。

添加新用户

在创建 Dominion KX II 用户*之前* 最好先定义用户组，原因在于，在添加用户时，必须将该用户分配到*现有的* 用户组。从“用户”(User) 页中，可以添加新用户、修改用户信息以及重新激活已停用的用户。

注意：*当失败的登录尝试次数超过“安全设置”屏幕上设置的最大登录尝试次数时，可以停用用户名（清除“活动”(Active) 复选框）。有关更多信息，请参阅*安全设置*。*

要添加新用户，请执行以下操作：

1. 使用下列方法之一打开“用户”**(User)** 页：
   - 选择“用户管理”**(User Management) >** “添加新用户”**(Add New User)**，或者
   - 在“用户列表”**(User List)** 页中单击“添加”**(Add)** 按钮

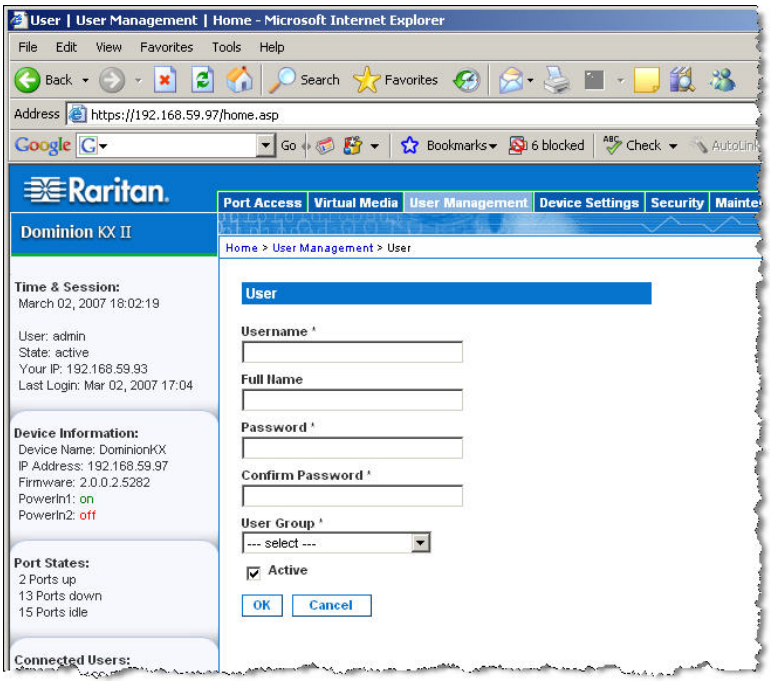


图 45：“用户”页

2. 在“用户名”**(Username)** 字段中键入一个唯一用户名（最长 16 个字符）。
3. 在“全名”**(Full Name)** 字段中键入该用户的全名（最长 64 个字符）。
4. 在“密码”**(Password)** 字段中键入密码，在“确认密码”**(Confirm Password)** 字段中重新键入密码（最长 64 个字符）。
5. 从“用户组”**(User Group)** 下拉列表中选择组。除系统提供的默认组（**<**未知**>**（默认设置）、**Admin**、单个组）外，该列表中包含已创建的所有组。如果不需要将此用户与现有“用户组”**(User Group)** 建立关联，请从下拉列表中选择“单个组”**(Individual Group)**。

   有关“单个组”**(Individual Group)** 的权限的更多信息，请参阅设置单个组的权限。
6. 要激活此用户，请选中“活动”**(Active)** 复选框。该复选框在默认情况下处于激活（启用）状态。
7. 单击“确定”**(OK)**。

修改现有用户

要修改现有用户，请执行以下操作：

1. 从“用户”(User) 页（图 45）中，更改相应的字段。（有关如何访问“用户”**(User)** 页的信息，请参阅添加新用户。）
2. 单击“确定”**(OK)**。

用户组列表

用户组与本地和远程认证一起使用（通过 RADIUS 或 LDAP）。在创建单个用户*之前* 最好先定义用户组，原因在于，在添加用户时，必须将该用户分配到*现有的* 用户组。

“用户组列表”(User Group List) 页显示所有用户组的列表，通过单击“组名”(Group Name) 列标题，可按升序或降序对该列表进行排序。从“用户组列表”(User Group List) 页中，还可以添加、修改或删除用户组。

要列出用户组，请执行以下操作：

选择“用户管理”**(User Management)** >“用户组列表”**(User Group List)**。将打开“用户组列表”(User Group List) 页：

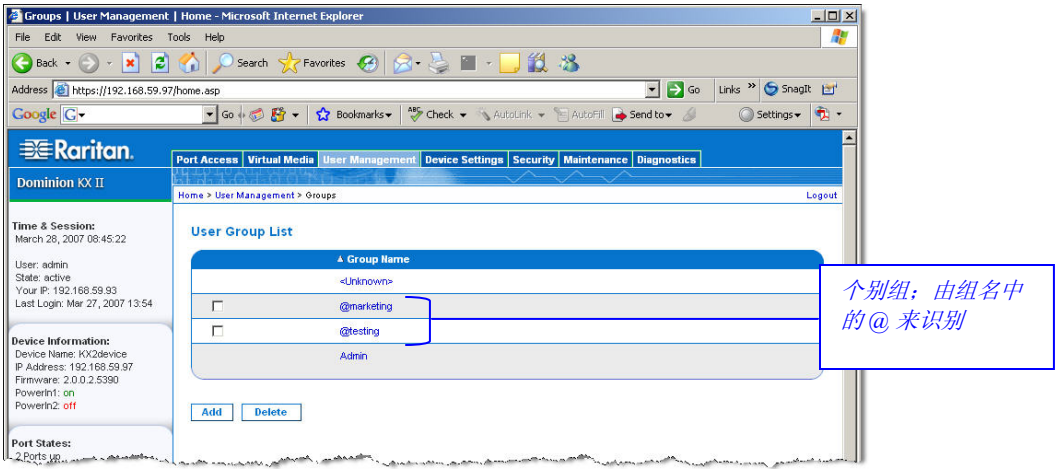


图 46：用户组列表

要添加新用户组，请执行以下操作：

单击“添加”**(Add)** 按钮。将打开“组”(Group) 页。有关“组”(Group) 页的完整信息，请参阅添加新用户组。

要修改现有用户组，请执行以下操作：

1. 在列出的用户组中查找该用户组。
2. 单击“组名”**(Group Name)**。将打开“组”(Group) 页。有关编辑组的完整信息，请参阅修改现有用户组。

要删除用户组，请执行以下操作：

重要事项：删除组之前，要确保未向其分配任何用户，否则这些用户也将一同被删除。

提示：要确定属于某一特定组的用户，必须按“用户组”(User Group) 对“用户列表”(User List)（图 44）进行排序。

1. 选中“组名”**(Group Name)** 左侧的复选框，从列出的组中选择组。
2. 单击“删除”**(Delete)**。
3. 系统将提示您确认删除。单击“确定”**(OK)**。

添加新用户组

要添加新用户组，请执行以下操作：

1. 使用下列方法之一打开“组”**(Group)** 页：
   - 选择“用户管理”**(User Management) >** “添加新用户组”**(Add New User Group)**，或者
   - 在“用户组列表”**(User Group List)** 页中单击“添加”**(Add)** 按钮

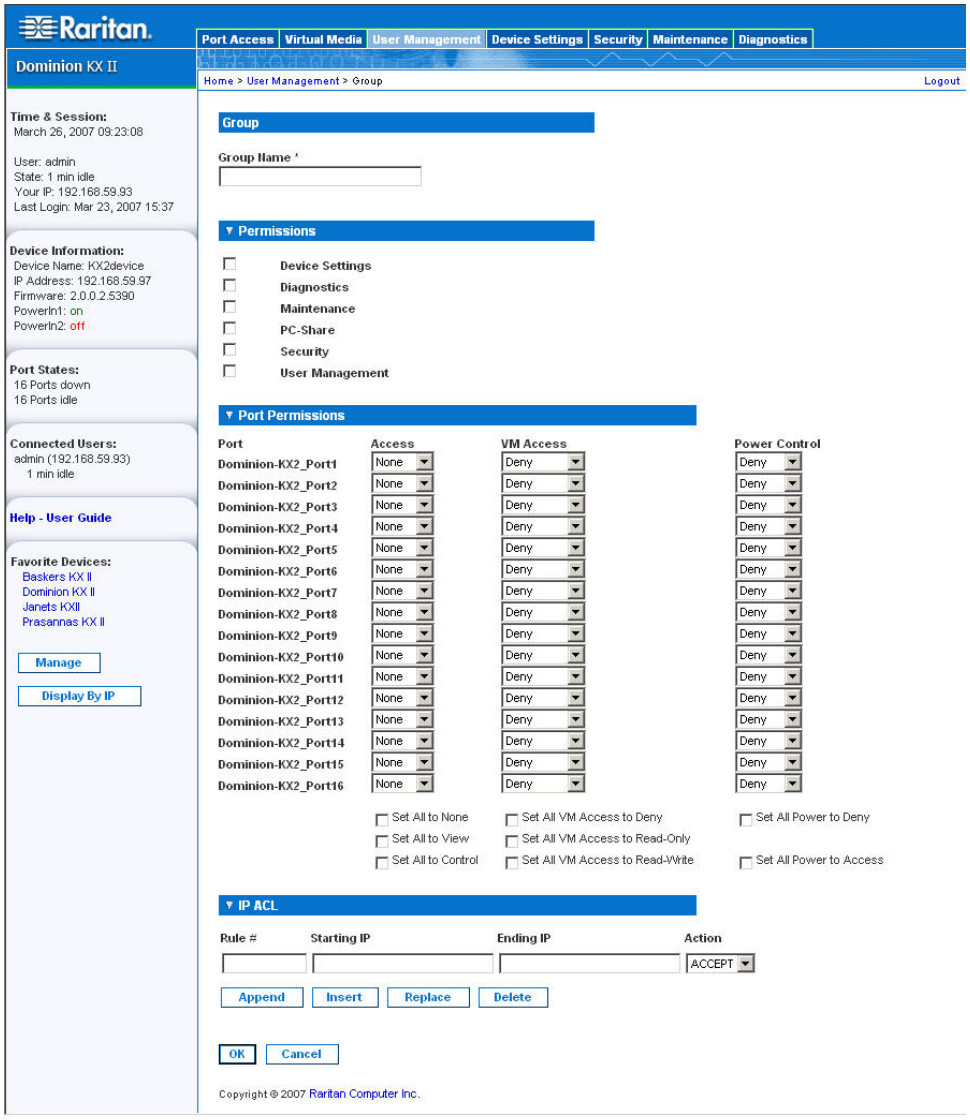


图 47：“组”页

应将“组”(Group) 页按以下类别进行组织：组、权限、端口权限和 IP ACL。

2. 将新用户组的说明性名称键入“组名”**(Group Name)** 字段。
3. 设置组的“权限”**(Permissions)**。选中要分配给属于此组的所有用户的权限前边的复选框。有关更多信息，请参阅设置权限。
4. 设置“端口权限”**(Port Permissions)**。指定属于此组的用户可以访问的服务器端口（及访问类型）。有关更多信息，请参阅设置端口权限。

5. 设置 IP ACL（可选）。通过指定 IP 地址，此功能限制对 Dominion KX II 设备的访问，与适用于对设备的所有访问尝试的 IP 访问控制列表功能不同，此功能仅适用于属于特定组的用户。
6. 单击“确定”**(OK)**。

注意：*MPC 和 Dominion KX II Local Console 中提供了几项管理功能；只有默认 ADMIN 组中的成员才能使用这些功能。*

设置权限

重要事项：通过选中“用户管理”(User Management) 复选框，组成员可以更改所有用户的权限，包括他们的自己的权限。授予这些权限时要仔细斟酌。

权限	说明
设备设置	网络设置、日期/时间设置、端口配置（通道名称、电源关联）、事件管理 (SNMP 和 Syslog)，虚拟媒体文件服务器设置
诊断	网络接口状态、网络统计信息、ping 主机、跟踪到主机的路由、KX 诊断
维护	备份和还原数据库、固件升级、出厂复位、重新引导
PC 共享	多个用户同时访问同一个目标
安全性	SSL 证书、安全设置（VM 共享和 PC 共享）、IP ACL
用户管理	用户和组管理、远程认证 (LDAP/RADIUS)、登录设置

设置端口权限

对于每个服务器端口，可以指定访问类型、对虚拟媒体的访问类型以及电源控制。请注意，所有权限的默认设置都将禁用。

访问 (Access)		VM 访问		电源控制	
选项	**说明**	**选项**	**说明**	**选项**	**说明**
无 (None)*	完全拒绝访问	**拒绝 (Deny)***	完全拒绝端口的虚拟媒体权限	**拒绝 (Deny)***	完全拒绝访问
查看 (View)	查看视频（但不与所连接的目标服务器交互）	**只读 (Read-Only)**	虚拟媒体访问仅限于读访问	**访问 (Access)**	完全访问
控制 (Control)	控制所连接的目标服务器	**读写 (Read-Write)**	对虚拟媒体进行完全访问（读、写）		

* 默认设置

提示：使用复选框可快速设置每个端口的所有相同权限。

基于组的 IP ACL（访问控制列表）

重要事项：使用基于组的 IP 访问控制时，须格外小心。如果您的 IP 地址处于已拒绝访问的范围内，则有可能被锁在 Dominion KX II 之外。

此功能限制选定组中的用户对特定 IP 地址的 Dominion KX II 设备的访问。与适用于对设备的所有访问尝试的“IP 访问控制列表”(IP Access Control List) 功能不同，此功能仅适用于属于特定组的用户，它将被优先处理。有关更多信息，请参阅 IP 访问控制。

重要事项：IP 地址 127.0.0.1 由 Dominion KX II 本地端口使用。创建“访问控制列表”(IP Access Control List) 时，如果 127.0.0.1 处于被阻止的“IP 地址”(IP Address) 范围内，则您将无权访问 Dominion KX II 本地端口。

使用“组”(Group) 页中的 IP ACL 部分，基于组级别添加、插入、替换和删除 IP 访问控制规则。

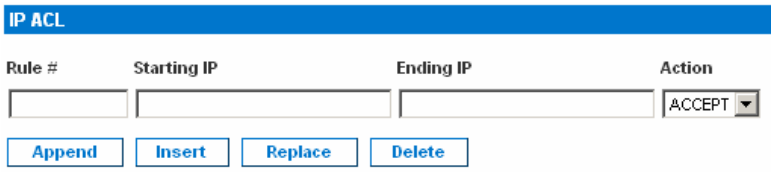


图 48：基于组的 IP 访问控制列表

要添加（追加）规则，请执行以下操作：

1. 在“起始 IP”**(Starting IP)** 字段中键入起始 IP 地址。
2. 在“结束 IP”**(Ending IP)** 字段中键入结束 IP 地址。
3. 从可用的选项中选择“操作”**(Action)**：
   - 接受 **(Accept)**。允许指定为“接受”的“IP 地址”**(IP Address)** 访问 Dominion KX II 设备。
   - 放弃 **(Drop)**。拒绝指定为“放弃”的“IP 地址”**(IP Address)** 访问 Dominion KX II 设备。
4. 单击“追加”**(Append)**。规则将添加到规则列表的底部。
5. 对于要输入的每一条规则，都要重复步骤 1 到步骤 4。

要插入规则，请执行以下操作：

1. 键入一个“规则号”**(Rule #)**。使用“插入”**(Insert)** 命令时，“规则号”**(Rule #)** 是必填的。
2. 填充“起始 IP”**(Starting IP)** 和“结束 IP”**(Ending IP)** 字段。
3. 从下拉列表中选择“操作”**(Action)**。
4. 单击“插入”**(Insert)**。如果刚才键入的“规则号”(Rule #) 等于现有的“规则号”(Rule #)，则新规则将放在现有规则的前面，同时列表中的所有规则都将下移。

要替换规则，请执行以下操作：

1. 指定要替换的“规则号”**(Rule #)**。
2. 填充“起始 **IP**”**(Starting IP)** 和“结束 **IP**”**(Ending IP)** 字段。
3. 从下拉列表中选择“操作”**(Action)**。
4. 单击“替换”**(Replace)**。新规则将替换具有相同“规则号”(Rule #) 的原始规则。

要删除规则，请执行以下操作：

1. 指定要删除的“规则号”**(Rule #)**。
2. 单击“删除”**(Delete)**。
3. 系统将提示您确认删除。单击“确定”**(OK)**。

重要事项：将按照 ACL 规则的列出顺序对这些规则进行评估。例如，在此处显示的示例中，如果两个 ACL 规则颠倒了，则 Dominion 将不会接受任何通信。



图 49：IP ACL 示例

提示：通过规则号，可以更好地控制规则的创建顺序。

修改现有用户组

***注意：**对于 Admin 组启用了所有权限，您无法对此进行更改。*

要修改现有用户组，请执行以下操作：

1. 从“组”(Group) 页中，更改相应的字段，然后选择相应的权限。

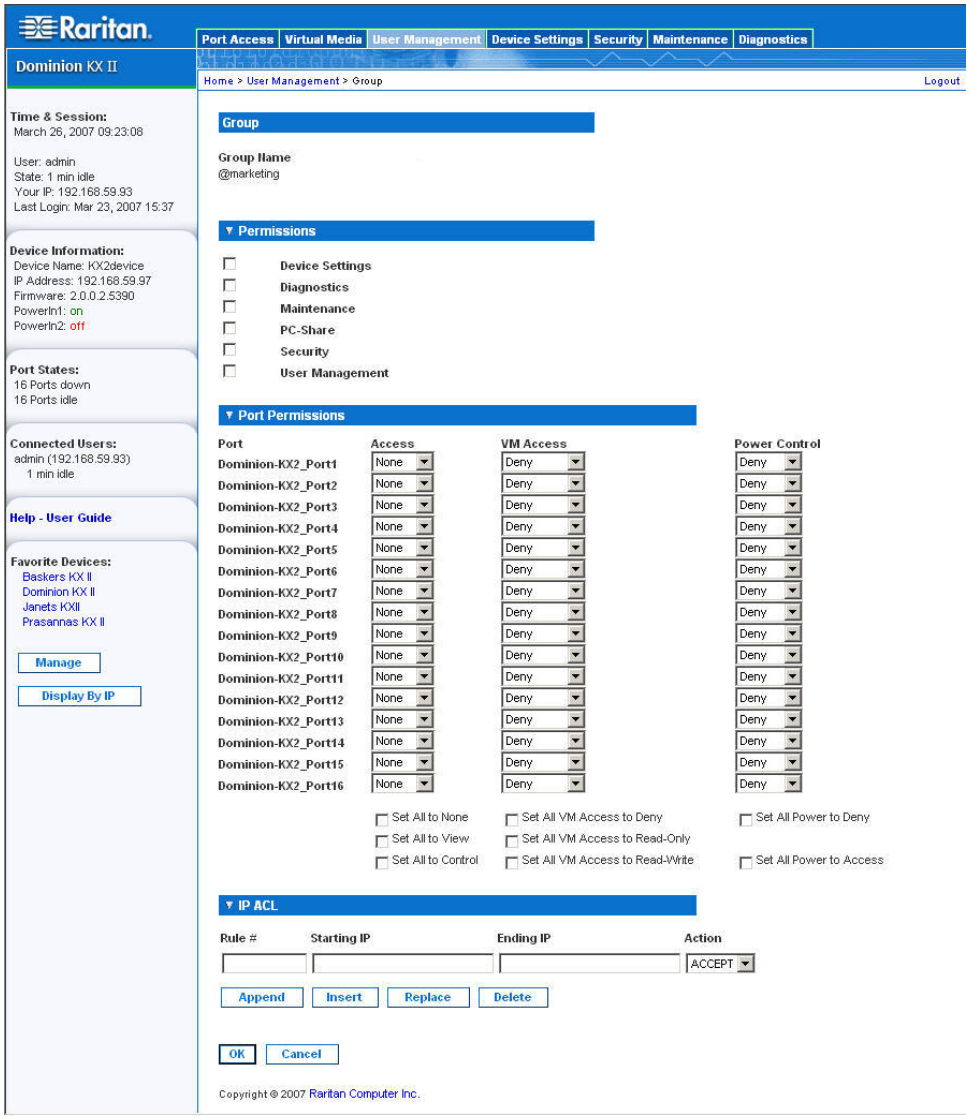


图 50：修改组

2. 设置组的“权限”**(Permissions)**。选中要分配给属于此组的所有用户的权限前边的复选框。有关更多信息，请参阅设置权限。
3. 设置“端口权限”**(Port Permissions)**。指定属于此组的用户可以访问的服务器端口（及访问类型）。有关更多信息，请参阅设置端口权限。
4. 设置 **IP ACL**（可选）。通过指定 IP 地址，此功能限制对 Dominion KX II 设备的访问。有关更多信息，请参阅基于组的 IP 访问控制。
5. 单击“确定”**(OK)**。

设置单个组的权限

要设置单个用户组的权限，请执行以下操作：

1. 在所列出的组中查找该用户。可以通过“组名”**(Group Name)** 中的 @ 来识别单个组。
2. 单击“组名”**(Group Name)**。将打开“组”(Group) 页（图 50）。
3. 选择相应的权限。
4. 单击“确定”**(OK)**。

更改密码

要更改密码，请执行以下操作：

1. 选择“用户管理”**(User Management)** >“更改密码”**(Change Password)**。将打开“更改密码”(Change Password) 页：

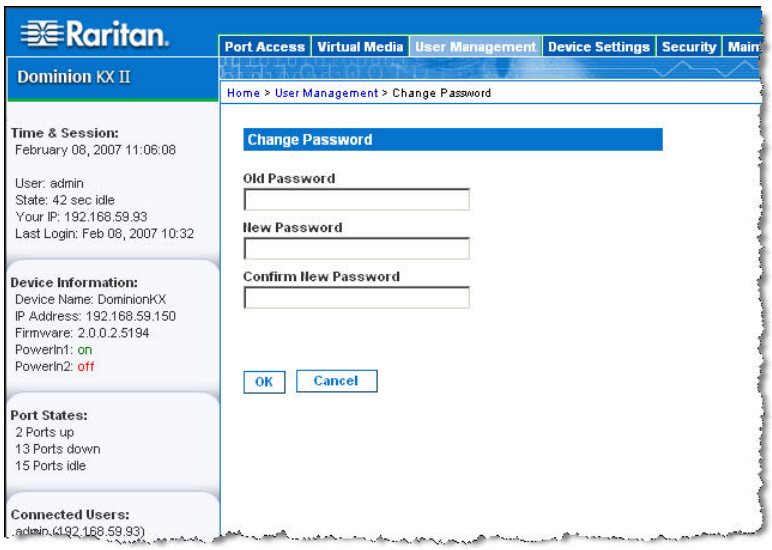


图 51：更改密码

2. 在“旧密码”**(Old Password)** 字段中键入当前的密码。
3. 在“新密码”**(New Password)** 字段中键入新密码，然后在“确认新密码”**(Confirm New Password)** 字段中重新键入新密码。密码最长可达 64 个字符，可以由英文字母数字字符和特殊字符组成。
4. 单击“确定”**(OK)**。
5. 此时将收到密码更改成功的确认。单击“确定”**(OK)**。

***注意：**如果使用的是复合密码，则此页将显示有关这种密码所要求格式的信息。有关密码和复合密码的更多信息，请参阅安全设置 – 复合密码。*

认证设置

从“认证设置”(Authentication Settings) 页中，可以配置用于访问 Dominion KX II 的认证类型。有关认证和授权的操作方式以及二者之间差异的信息，请参阅认证与授权。

***注意：**即使选择远程认证（LDAP 或 RADIUS），仍要使用本地认证。*

要配置认证，请执行以下操作：

1. 选择“用户管理”**(User Management)** >“认证设置”**(Authentication Settings)**。将打开“认证设置”(Authentication Settings) 页：

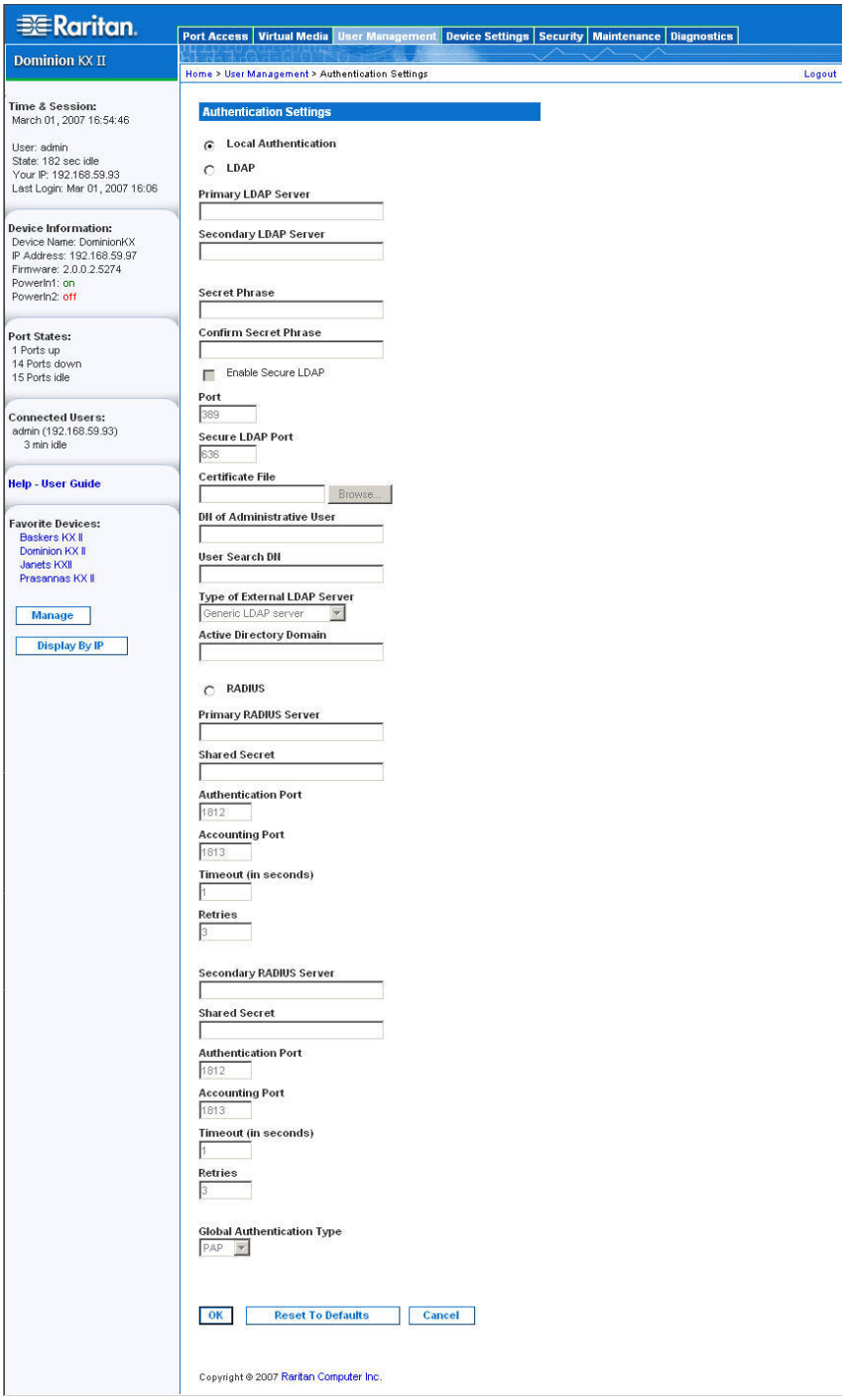


图 52：认证设置

2. 选择要使用的认证协议选项（“本地认证”**(Local Authentication)**、“**LDAP**”或“**RADIUS**”）。选择 **LDAP** 选项将启用其余的 **LDAP** 字段，选择 **RADIUS** 选项将启用其余的 **RADIUS** 字段。
3. 如果选择了“本地认证”**(Local Authentication)**，请继续步骤 **6**。
4. 如果选择了“**LDAP**”，请阅读标题为实现 LDAP 远程认证的一节，以了解有关填写“认证设置”**(Authentication Settings)** 页中 **LDAP** 部分的字段的信息。
5. 如果选择了“**RADIUS**”，请阅读标题为实现 RADIUS 远程认证的一节，以了解有关填写“认证设置”**(Authentication Settings)** 页中 **RADIUS** 部分的字段的信息。
6. 完成后，单击“确定”**(OK)** 保存。

要取消而不保存更改，请执行以下操作：

单击“取消”**(Cancel)**。

要返回到出厂默认值，请执行以下操作：

单击“复位为默认值”**(Reset to Defaults)** 按钮。

实现 LDAP 远程认证

轻量级目录访问协议 (LDAP) 是用于查询和修改运行在 TCP/IP 上的目录服务的网络协议。客户机通过连接到 LDAP 服务器（默认 TCP 端口为 389）来启动 LDAP 会话。然后客户机向服务器发送操作请求，而服务器发送响应。

提示：Microsoft Active Directory 实质上是充当 LDAP 认证服务器。

要使用 LDAP 认证协议，请输入以下信息：



图 53：认证设置 (LDAP)

1. 在“主 **LDAP** 服务器”**(Primary LDAP Server)** 字段中键入 **LDAP** 远程认证服务器的 **IP** 地址或 **DNS** 名称。如果“启用安全 LDAP”(Enable Secure LDAP) 选项处于选中状态，则必须使用 DNS 名称。
2. （可选）在“备用 **LDAP** 服务器”**(Secondary LDAP Server)** 字段中键入备份 **LDAP** 服务器的 **IP** 地址或 **DNS** 名称。如果“启用安全 LDAP”(Enable Secure LDAP) 选项处于选中状态，则必须使用 DNS 名称。请注意，其余字段将共享带有“主 **LDAP** 服务器”**(Primary LDAP Server)** 字段的相同设置。
3. 在“密码”**(Secret Phrase)** 字段中，键入根据远程认证服务器进行认证所需的服务器密码，然后再次在“确认密码”**(Confirm Secret Phrase)** 字段中键入此密码。
4. 如果要使用 **SSL**，请选中“启用安全 **LDAP**”**(Enable Secure LDAP)** 复选框；此时将启用“安全 **LDAP** 端口”**(Secure LDAP Port)** 字段。安全套接字层 **(SSL)** 是一个加密协议，**Dominion KX II** 可以使用它与 **LDAP** 服务器安全地通信。
5. 默认端口为 **389**。使用标准 **LDAP TCP** 端口或指定其它端口。
6. 默认的“安全 **LDAP** 端口”**(Secure LDAP Port)** 为 **636**。使用默认端口或指定其它端口。选中“启用安全 **LDAP**”**(Enable Secure LDAP)** 复选框时将启用此字段。

7. 证书文件 **(Certificate File)**。要获取 LDAP 服务器的 **Base64** 编码 **X-509** 格式的 **CA** 证书文件，请咨询认证服务器管理员。使用“浏览”**(Browse)** 按钮定位到该证书文件。选中“启用安全 **LDAP**”**(Enable Secure LDAP)** 选项时将启用此字段。
8. 管理性用户的 **DN (DN of administrative User)**。管理性用户的辨别名；要了解要在此字段中键入的相应值，请咨询认证服务器管理员。管理性用户 **DN** 的示例值可能如下：“cn=Administrator,dc=Users=,dc=testradius,dc=com”。
9. 用户搜索 **DN (User Search DN)**。它说明要与 LDAP 绑定的名称，以及从数据库中何处开始搜索指定的基础 DN。“基础搜索”(Base Search) 的示例值可能如下：“cn=”Users,dc=raritan,dc=com”。要了解要在这些字段中输入的相应值，请咨询认证服务器管理员。
10. 外部 LDAP 服务器的类型 **(Type of external LDAP server)**。从可用的选项中进行选择：
    - **常规 LDAP 服务器 (Generic LDAP Server)**。
    - **Microsoft Active Directory**。Active Directory 是 Microsoft 对 LDAP 目录服务的实现，以便在 Windows 环境中使用。
11. **Active Directory** 域 **(Active Directory Domain)**。键入 **Active Directory** 域的名称。

从 Active Directory 服务器返回用户组信息

Dominion KX II 支持用户认证到 Active Directory (AD)，而且*不*要求在 KX II 上本地定义这些用户。这样一来就可以在 AD 服务器上*独占地* 维护 Active Directory 用户帐户和密码。授权和 AD 用户权限是通过标准 KX II 策略和用户组权限（本地应用到 AD 用户组）受到控制和管理的。

注意：*如果您现在是 Raritan, Inc. 客户，而且已经通过更改 AD 架构配置了 Active Directory 服务器，则 Dominion KX II 仍然支持此配置，您也不必执行下列操作。有关更新 AD LDAP 架构的信息，请参阅附录 B：更新 LDAP 架构。*

在 Dominion KX II 上启用 AD 服务器：

1. 使用 Dominion KX II 创建特殊组，并将合适的权限分配到这些组。例如，创建这些组：KVM_Admin、KVM_Operator。
2. 在 Active Directory 服务器上，以和上一步**相同** 的组名创建新组。
3. 在 AD 服务器上，将创建的组分配给将要使用 Dominion KX II 的用户。
4. 从 Dominion KX II 正确启用和配置 AD 服务器。请参阅实现 LDAP 远程认证。

重要注意事项：

- 组名称是区分大小写的。
- Dominion KX II 提供下列不能更改或删除的默认组：Admin 和 <未知>。请验证您的 Active Directory 服务器没有使用相同的组名。
- 如果从 Active Directory 服务器返回的组信息与 KX II 组配置不匹配，则 Dominion KX II 会自动将 <未知> 组分配给成功认证的用户。

实现 RADIUS 远程认证

远程认证拨号用户服务 (RADIUS) 是一个适用于网络访问应用程序的 AAA（认证、授权和帐户）协议。

要使用 RADIUS 认证协议，请执行以下操作：



图 54：认证设置 (RADIUS)

1. 分别在“主 **Radius** 服务器”**(Primary Radius Server)** 和“备用 **Radius** 服务器”**(Secondary Radius Server)** 字段中键入主和（可选）备用远程认证服务器的 **IP** 地址。
2. 键入用于进行认证的服务器密码（在“共享机密” **(Shared Secret)** 字段中）。共享机密是 Dominion KX II 和 RADIUS 服务器双方都必须知道的一个字符串，可以使用它进行安全的通信。共享机密实质上就是一个密码。
3. 认证端口 **(Authentication Port)**。默认认证端口为 1812，可以按需更改。
4. 帐户端口**(Accounting Port)**。默认帐户端口为 1813，可以按需更改。
5. 超时 **(Timeout)**（秒）。默认超时值为 1 秒，可以按需更改。超时就是在发送另一个认证请求之前 Dominion KX II 等待来自 RADIUS 服务器的响应的时间长度。
6. 重试次数 **(Retries)**。默认重试次数为 3，可以按需更改。这是 Dominion KX II 向 RADIUS 服务器发送认证请求的次数。

7. 全局认证类型 (Global Authentication Type)。从下拉列表中的选项中进行选择：
   - **PAP**。使用 PAP，密码将以纯文本形式发送。PAP 不是交互式的；建立连接之后用户名和密码将在一个数据包中发送，而不是服务器先发送登录提示然后等待响应。
   - **CHAP**。使用 CHAP，服务器可以随时请求认证。CHAP 提供的安全性比 PAP 高。

通过 RADIUS 返回用户组信息

在 RADIUS 认证尝试成功时，Dominion KX II 设备将基于用户组的权限确定给定用户的权限。

通过返回一个以 RADIUS *FILTER-ID* 形式实现的属性，您的远程 RADIUS 服务器可以提供这些用户组名。*FILTER-ID* 的格式应如下：

```
Raritan:G{GROUP_NAME}
```

其中 `GROUP_NAME` 是一个字符串，表示用户所属组的名称。

RADIUS 通信交换规范

Dominion KX II 设备向您的 RADIUS 服务器发送以下 RADIUS 属性。

属性	数据
登录	
访问请求 (1)	
NAS 端口类型 (61)	用于网络连接的 VIRTUAL (5)。
NAS IP 地址 (4)	Dominion KX II 设备的 IP 地址。
用户名 (1)	在登录屏幕上输入的用户名。
帐户会话 ID (44)	帐户的会话 ID。
用户密码 (2):	经过加密的密码。
帐户请求 (4)	
帐户状态 (40)	Start(1) – 启动帐户。
NAS 端口类型 (61)	用于网络连接的 VIRTUAL (5)。
NAS 端口 (5)	始终为 0。
NAS IP 地址 (4)	Dominion KX II 设备的 IP 地址。
用户名 (1)	在登录屏幕上输入的用户名。
帐户会话 ID (44)	帐户的会话 ID。
注销	
帐户请求 (4)	
帐户状态 (40)	Stop(2) – 停止帐户
NAS 端口类型 (61)	用于网络连接的 VIRTUAL (5)。
NAS 端口 (5)	始终为 0。
NAS IP 地址 (4)	Dominion KX II 设备的 IP 地址。
用户名 (1)	在登录屏幕上输入的用户名。
帐户会话 ID (44)	帐户的会话 ID。

第 9 章：设备管理

“设备设置”(Device Settings) 菜单按以下各项进行组织：“网络”(Network)、“日期/时间”(Date/Time)、“事件管理 – 设置”(Event Management - Settings)、“事件管理 – 目标”(Event Management - Destinations)、“电源设置”(Power Supply Setup)、“端口配置”(Port Configuration) 以及“本地端口设置”(Local Port Settings)（仅限 Dominion KX II Local Console）。

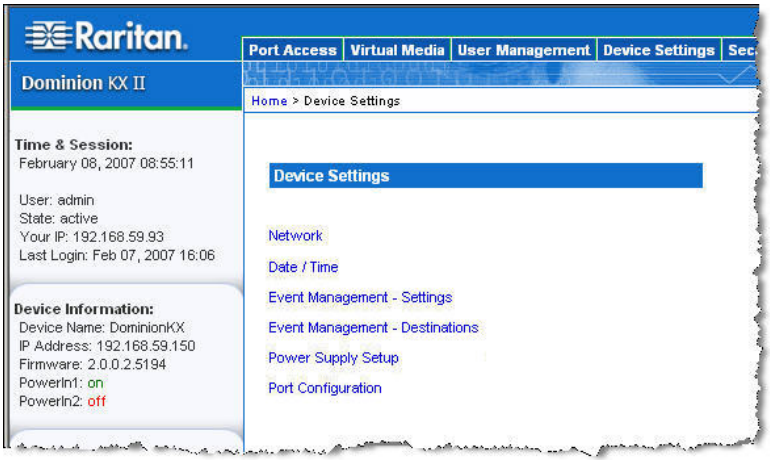


图 55：“设备设置”菜单

使用：	目的：
网络 (Network)	自定义 Dominion KX II 的网络配置。
日期/时间 (Date/Time)	设置日期、时间、时区和网络时间协议 (NTP)。
事件管理 – 设置 (Event Management - Settings)	配置 SNMP 和 Syslog。
事件管理 – 目标	选择要跟踪的系统事件以及要将此信息发送到的位置。
电源设置	配置 Dominion KX II 电源的自动检测。
端口配置	配置 KVM 端口、电源 CIM 和插座。
本地端口设置	配置本地端口；*仅限 Dominion KX II Local Console*。

网络设置

使用“网络设置”(Network Settings) 页，可以为 Dominion KX II 设备自定义网络配置（如 IP 地址、发现端口和 LAN 接口参数）。

重要事项：必须重新引导 Dominion KX II 才能使新的网络设置生效。更改网络配置之前，要确保当前没有到该设备的任何其它用户连接；KX II 设备重新引导时，所有的连接都将断开。

设置“IP 配置”(IP Configuration) 主要用两种方法：

- **无 (None)**。此选项是建议的选项（静态 IP）。由于 Dominion KX II 是网络基础结构的一部分，因此您很有可能不希望其 IP 地址频繁更改。可以使用此选项设置网络参数。
- **DHCP**。IP 地址由 DHCP 服务器自动分配。

要更改网络配置，请执行以下操作：

1. 选择“设备设置”**(Device Settings)** > “网络”**(Network)**。将打开“网络设置”(Network Settings) 页。

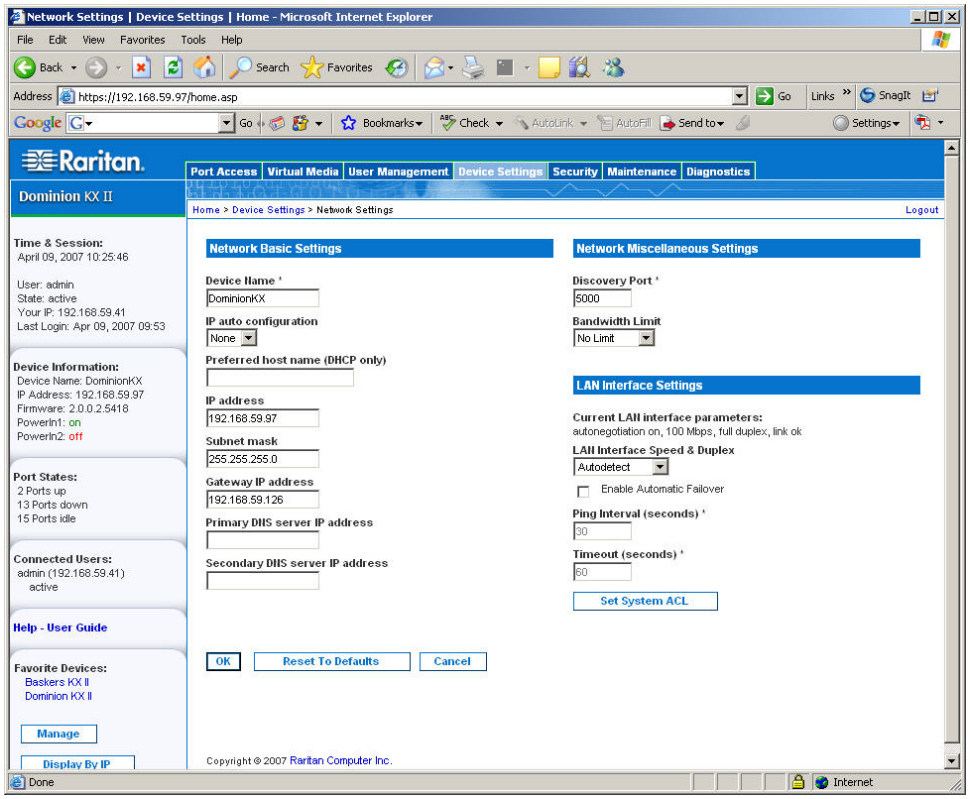


图 56：网络设置

2. 更新网络基本设置。有关每个字段的更多信息，请参阅网络基本设置。
3. 更新其它网络设置。有关每个字段的更多信息，请参阅其它网络设置。
4. 更新 LAN 接口设置。有关每个字段的更多信息，请参阅 LAN 接口设置。
5. 单击“确定”**(OK)** 设置这些配置。如果所做的更改需要重新引导设备，则将显示一条重新引导消息。

要取消而不保存更改，请执行以下操作：

单击“取消”**(Cancel)**。

要复位为出厂默认值，请执行以下操作：

单击“复位为默认值”**(Reset to Defaults)**。

网络基本设置



图 57：网络设置（网络基本设置）

- **设备名称 (Device Name)**。为设备键入一个唯一的名称（最长 16 个字符，不允许空格）。命名您的设备，使其容易识别。Dominion KX II 设备的默认名称为：**“DominionKX”**。远程用户也将看到此名称。但是，如果 MPC 用户已经为该设备创建了“连接配置文件”(Connection Profile)，则该用户将看到的是连接配置文件中的“说明”**(Description)** 字段。
- **IP 自动配置 (IP auto configuration)**。从下拉列表中的可用选项中进行选择：
  - **无 (None)**。如果不需要自动 IP 配置而更喜欢自己设置 IP 地址（静态 IP），请使用此选项。此选项是默认选项，建议您使用。

*如果选择此选项作为“IP 自动配置”**(IP auto configuration)**，则将启用以下“网络基本设置”(Network Basic Settings) 字段，从而允许手动设置 IP 配置。*

- **IP 地址 (IP Address)**。默认 IP 地址为 192.168.0.192。
- **子网掩码 (Subnet Mask)**。默认子网掩码为 255.255.255.0。
- **网关 IP 地址 (Gateway IP Address)**。网关的 IP 地址（如果使用的话）。
- **主 DNS 服务器 IP 地址 (Primary DNS Server IP Address)**。用于将名称转换为 IP 地址的主“域名服务器”(Domain Name Server)。
- **备用 DNS 服务器 IP 地址 (Secondary DNS Server IP Address)**。用于将名称转换为 IP 地址的备用“域名服务器”(Domain Name Server)（如果使用的话）。

– **DHCP**。联网的计算机（客户机）使用“动态主机配置协议”(Dynamic Host Configuration Protocol) 从 DHCP 服务器获取唯一的 IP 地址和其它参数。

- 如果使用了 DHCP，请输入**“首选主机名”(Preferred host name)**（仅限 DHCP）。最长 63 个字符。

其它网络设置

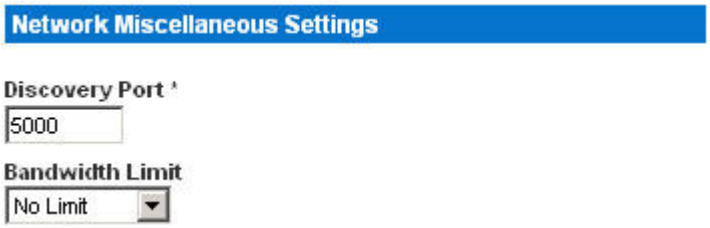


图 58：网络设置（网络杂项设置）

- **发现端口 (Discovery Port)**。Dominion KX II 发现功能在单个可配置的 TCP 端口上进行。默认值是“端口 5000”(Port 5000)，但是可将其配置为使用除 80 和 443 之外的任何 TCP 端口。要从防火墙外部访问 KX II 设备，则防火墙设置必须允许通过默认端口 5000 或此处配置的非默认端口进行双向通信。有关更多信息，请参阅配置网络防火墙设置。
- **带宽限制 (Bandwidth Limit)**。默认值为“无限”(no limit)。从下拉列表的选项中进行选择，以设置此 Dominion KX II 设备可占用的最大带宽数量（供所有会话使用）。这些选项包括：无限 (No Limit)、100 Mb、10 Mb、5 Mb、2 Mb、512 Kb、256 Kb 和 128 Kb。

***注意：**带宽越窄，性能可能就越低。*

LAN 接口设置

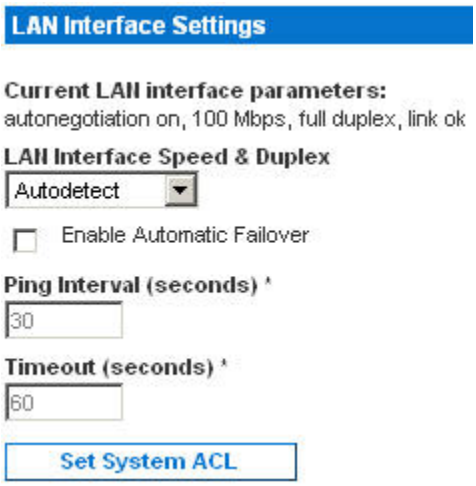


图 59：网络设置（LAN 接口设置）

- 当前的参数设置标识在**“当前的 LAN 接口参数”(Current LAN interface parameters)**字段中。
- **LAN 接口速度与双工 (LAN Interface Speed & Duplex)**。从可用的速度与双工组合中进行选择。

自动检测	*默认选项*
10 Mbps/半 (10 Mbps/Half)	
10 Mbps/全 (10 Mbps/Full)	
100 Mbps/半 (100 Mbps/Half)	
100 Mbps/全 (100 Mbps/Full)	
1000 Mbps/全 (1000 Mbps/Full)	*Gb*

  - **“半双工”(Half-duplex)** 提供双向通信，但某一时刻只允许在一个方向上进行通信（而不允许在两个方向上同时通信）。
  - **“全双工”(Full-duplex)** 允许同时进行双向通信。

***注意：**在半双工或全双工通信中，以 10 Mbps 运行时偶尔也会出现问题。如果遇到问题，请尝试其它速度和双工。*

- **启用自动故障切换 (Enable Automatic Failover)**。选中此复选框，可在活动网络端口出现故障时允许 Dominion KX II 使用第二网络端口自动恢复其网络连接。启用此选项时，将使用以下两个字段：
  - **Ping 间隔 (Ping Interval)（秒）**。“Ping 间隔”(Ping Interval) 确定 Dominion KX II 多长时间检查一次网络连接状态（如果此值设置得太小，可能会产生过大的网络流量）。默认“Ping 间隔”(Ping Interval) 为 30 秒。
  - **超时 (Timeout)（秒）**。“超时”(Timeout) 确定在进行切换之前网络端口必须停止工作时间。两个网络端口都必须连接到网络，而且必须选中此选项才能使“自动故障切换”(Automatic Failover) 起作用。默认超时值为 60 秒。

***注意：**默认“Ping 间隔”和“超时”会产生以下情况，即当 KX 设备尝试进行切换时，远程会话将被终止，然后必须重新建立。将这些间隔减到非常小的值可使远程会话保持连接状态，但会使网络流量增加。*

- **设置系统 ACL (Set System ACL)**。单击此按钮为 Dominion KX II 设置全局级别的“访问控制列表”(Access Control List)，这样可确保设备不响应从禁止的 IP 地址发送的封包。将打开 IP 访问控制页。

***注意：**这些 ACL 值是全局性的，会对整个 Dominion KX II 设备产生影响。您还可以基于组级别创建 ACL。例如，可以创建“外包供应商”用户组，只允许该组从给定的 IP 地址范围访问 Dominion KX II（有关如何创建组专用的“访问控制列表”的更多信息，请参阅基于组的 IP ACL）。*

日期/时间设置

使用“日期/时间设置”(Date/Time Settings) 页，可以指定 Dominion KX II 的日期和时间。执行此操作有两种方法：

- 手动设置日期和时间，或者
- 与网络时间协议 (NTP) 服务器保持同步。

要设置日期和时间，请执行以下操作：

1. 选择“设备设置”**(Device Settings) >**“日期/时间”**(Date/Time)**。将打开“日期/时间设置”**(Date/Time Settings)** 页：

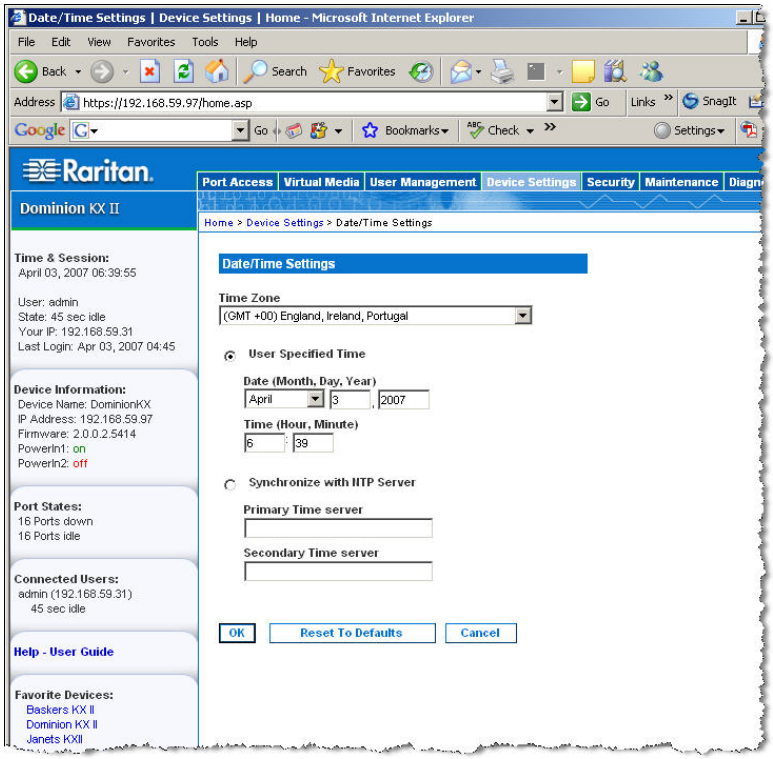


图 60：日期/时间设置

2. 从“时区”**(Time Zone)** 下拉列表中选择**时区。**
3. 选择要用于设置日期和时间的方法：
   - **用户指定的时间 (User Specified Time)**。选择此选项可手动输入日期和时间。
   - **与 NTP 服务器同步 (Synchronize with NTP Server)**。选择此选项可与网络时间协议 (NTP) 服务器同步日期和时间。
4. 对于“用户指定的时间”**(User Specified Time)** 选项，应如下输入日期和时间：
   a. 从下拉列表中选择“月”**(Month)**。
   b. 键入月中的“日”**(Day)**。
   c. 以 yyyy 格式键入“年”**(Year)**。
   d. 以 hh:mm 格式输入“时间”**(Time)**（采用 24 小时制）。

5. 对于“与 **NTP** 服务器同步”**(Synchronize with NTP Server)** 选项：
   a. 输入“主时间服务器”(Primary Time server) 的 IP 地址。
   b. （可选）输入“备用时间服务器”**(Secondary Time server)** 的 IP 地址。
6. 单击“确定”**(OK)**。

事件管理

Dominion KX II 事件管理功能提供了一组屏幕，用于允许和禁止向 SNMP 管理器、Syslog 和审计日志分发系统事件。这些事件都进行了分类，对于每个事件都可以确定是否需要将其发送到一个或多个目标。

事件管理 — 设置

SNMP 配置

简单网络管理协议 (SNMP) 是一个调控网络管理和监控网络设备及其功能的协议。Dominion KX II 通过“事件管理”(Event Management) 提供 SNMP 代理支持。有关 SNMP 代理和 SNMP 陷阱的更多信息，请参阅 SNMP 代理配置和 SNMP 陷阱配置。

要配置 SNMP（启用 SNMP 记录），请执行以下操作：

1. 选择“设备设置”**(Device Settings)** >“事件管理 – 设置”**(Event Management – Settings)**。将打开“事件管理 – 设置”**(Event Management – Settings)** 页：

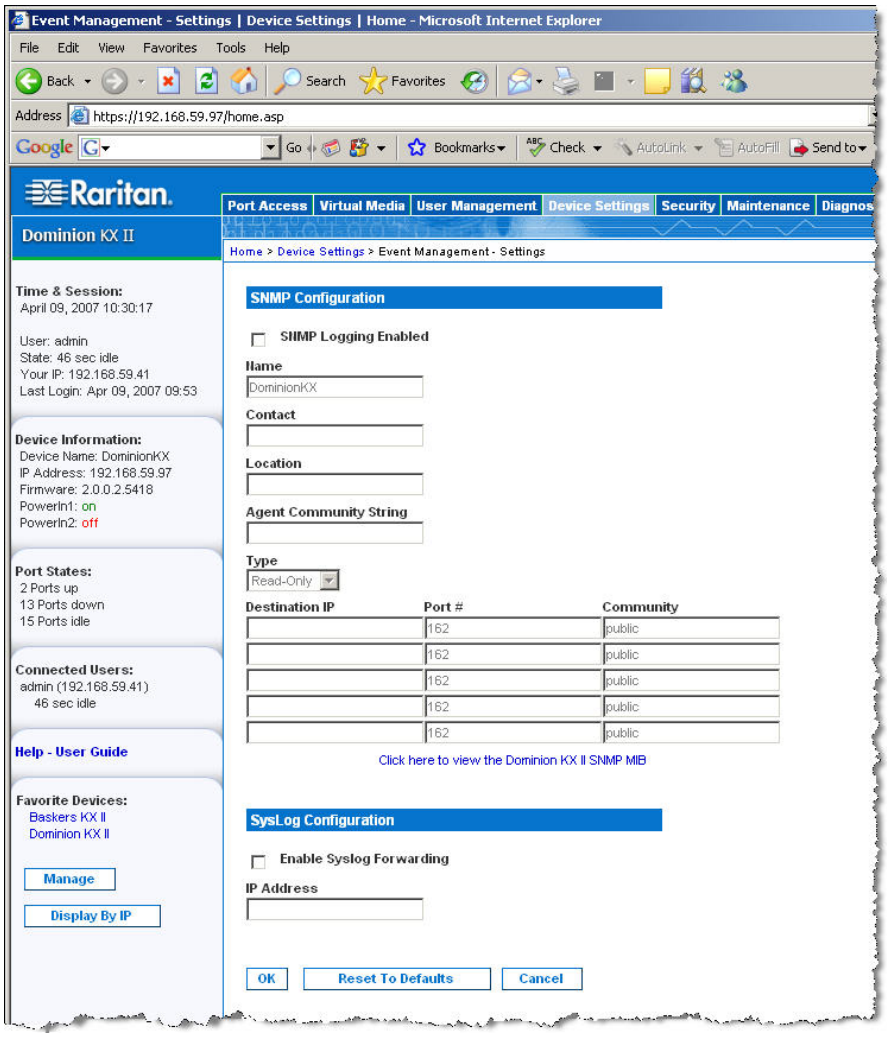


图 61：事件管理 – 设置

2. 选中“启用 **SNMP** 记录”**(Enable SNMP Logging)** 选项，此时将启用其余的 SNMP 字段。
3. 在“名称”**(Name)**、“联系人”**(Contact)** 和“位置”**(Location)** 三个字段中，分别键入 SNMP 代理的（此 Dominion 设备的）名称（如 KX II Console 界面上所显示的），与此设备有关的联系人姓名，以及此 Dominion 设备的物理位置。
4. 键入“代理社区字符串”**(Agent Community String)**（**Dominion** 设备的字符串）。SNMP 社区是运行 SNMP 的设备和管理站所属的组；它帮助定义信息的发送位置。社区名用于标识该组；一个 SNMP 设备或代理可以属于多个 SNMP 社区。
5. 使用“类型”**(Type)** 下拉列表指定社区是“只读”还是“读写”。
6. 通过指定其“目标 **IP**”**(Destination IP)**、“端口号”**(Port #)** 和“社区”**(Community)**，最多可以配置 5 个 SNMP 管理器。
7. 单击链接“单击此处查看 **Dominion-KX2 SNMP MIB**”**(Click here to view the Dominion-KX2 SNMP MIB)**，可访问“**SNMP** 管理信息库”(SNMP Management Information Base)。
8. 单击“确定”**(OK)**。

Syslog 配置



图 62：Syslog 配置

要配置 Syslog（启用 Syslog 转发），请执行以下操作：

1. 选中“启用 Syslog 转发”**(Enable Syslog Forwarding)** 选项可将设备的消息记录到远程 Syslog 服务器上。
2. 在“IP 地址”**(IP Address)** 字段中键入 Syslog 服务器的 IP 地址。
3. 单击“确定”**(OK)**。

要取消而不保存更改，请执行以下操作：

单击“取消”**(Cancel)**。

要复位为出厂默认值，请执行以下操作：

单击“复位为默认值”**(Reset to Defaults)** 按钮。

事件管理 — 目标

如果启用，则系统事件可以生成 SNMP 通知事件（陷阱），还可以将系统事件记录到 Syslog 或审计日志中。使用“事件管理 – 目标”(Event Management - Destinations) 页，可以选择要跟踪的系统事件和此信息的发送位置。

注意：*仅当选中“启用 SNMP 记录”选项时，才会生成 SNMP 陷阱；仅当选中“启用 Syslog 转发”选项时，才会生成 Syslog 事件。这两个选项都位于事件管理 – 设置页中。*

要选择事件及其目标，请执行以下操作：

1. 选择“设备设置”**(Device Settings)** >“事件管理 – 目标”**(Event Management – Destinations)**。将打开“事件管理 – 目标”(Event Management – Destinations) 页：

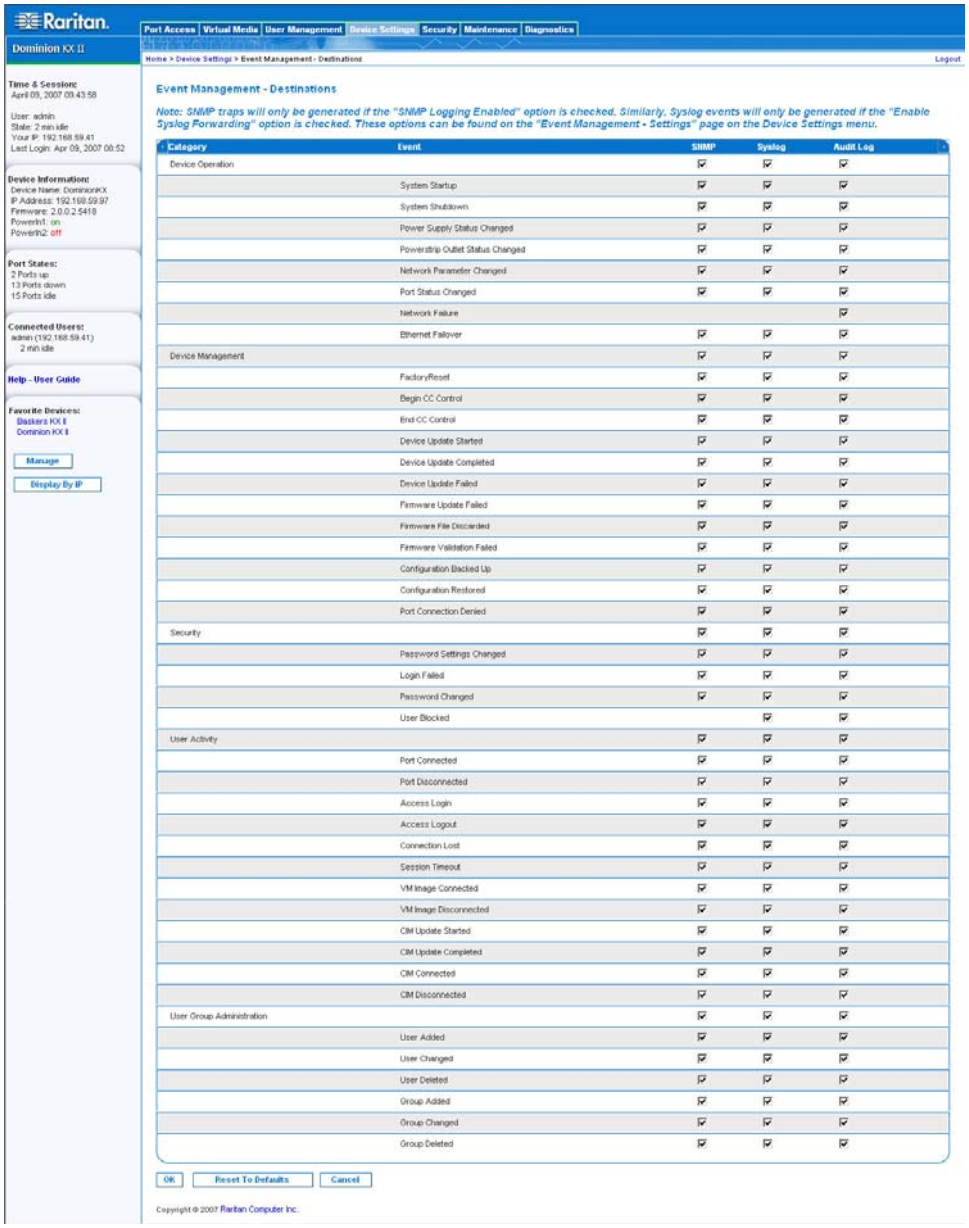


图 63：事件管理 – 目标

系统事件将按以下各项加以分类，设备操作、设备管理、安全性、用户活动，以及用户组管理。

2. 选中要启用或禁用的那些“事件”**(Event)** 行项目对应的复选框，需要在这些位置发送信息。

提示：分别选中或清除“类别”行复选框，可以启用或禁用整个“类别”。

3. 单击“确定”**(OK)**。

要取消而不保存更改，请执行以下操作：

单击“取消”**(Cancel)**。

要复位为出厂默认值，请执行以下操作：

单击“复位为默认值”**(Reset to Defaults)** 按钮。

SNMP 代理配置

称作代理的 SNMP 兼容设备在管理信息库 (MIB) 中存储有关其自身的数据，然后将这些数据返回给 SNMP 管理器。使用“事件记录”(Event Logging) 页可以配置 Dominion KX II（SNMP 代理）和 SNMP 管理器之间的 SNMP 连接。

SNMP Trap 配置

使用 SNMP 可以发送陷阱或通知，以便在一个或多个条件得到满足时通知管理员。下表列出的是 Dominion KX II SNMP 陷阱：

陷阱名称	说明
cimConnected	将 CIM 插入 Dominion KX II 端口。
cimDisconnected	将 CIM 从 Dominion KX II 端口拔出或关闭其电源。
cimUpdateCompleted	CIM 固件更新过程已完成。
cimUpdateStarted	CIM 固件更新过程已开始。
configBackup	设备配置已备份。
configRestore	设备配置已恢复。
deviceUpdateFailed	设备更新失败。
deviceUpgradeCompleted	Dominion KX II 已通过 RFP 文件完成更新。
deviceUpgradeStarted	Dominion KX II 已通过 RFP 文件开始更新。
ethernetFailover	检测到以太网故障切换，已在新的以太网接口上恢复。
factoryReset	设备已复位到出厂默认值。
firmwareFileDiscarded	固件文件已被丢弃。
firmwareUpdateFailed	固件更新失败。
firmwareValidationFailed	固件确认失败。
groupAdded	组已添加到 KX II 系统中。
groupDeleted	组已从系统中删除。
groupModified	组已修改。
ipConflictDetected	检测到 IP 地址冲突。
ipConflictResolved	IP 地址冲突已解决。
networkFailure	该产品的以太网接口无法再在网络上通信。
networkParameterChanged	已对网络参数进行更改。
passwordSettingsChanged	复合密码设置已更改。
portConnect	以前谁认证的用户已开始 KVM 会话。
portConnectionDenied	到目标端口的连接被拒绝。
portDisconnect	参与 KVM 会话的用户正确关闭该会话。
portStatusChange	端口已不可用。
powerNotification	电源插座状态通知：1=活动、0=非活动。
powerOutletNotification	电源板设备插座状态通知。
rebootCompleted	KX 已完成其重新引导。
rebootStarted	KX 已通过向系统循环电源或从 OS 热重新引导开始重新引导。
securityViolation	安全冲突。
startCCManagement	设备已置于 CommandCenter 管理下。
stopCCManagement	设备已从 CommandCenter 管理中删除。
userAdded	用户已添加到系统中。
userAuthenticationFailure	用户尝试使用不正确的用户名和/或密码进行登录。
userConnectionLost	活动会话中的用户遇到了异常会话终止。
userDeleted	用户帐户已删除。
userLogin	用户已成功登录到 KX II 并且已通过认证。
userLogout	用户正确 注销 KX II 成功。
userModified	用户帐户已修改。
userPasswordChanged	修改设备的*任何*用户的密码时，都将触发此事件。
userSessionTimeout	活动会话中的用户遇到了由超时造成的会话终止。
vmImageConnected	用户尝试使用“虚拟媒体”在目标上安装设备或图像。对于设备/图像映射（安装）的每一次尝试，都将生成此事件。
vmImageDisconnected	用户尝试使用“虚拟媒体”在目标上卸载设备或图像。

“电源设置”页

Dominion KX II 提供了双电源，可以自动进行检测并提供有关这些电源的状态的通知。使用“电源设置”(Power Supply Setup) 页，可指定是使用一个电源还是使用两个电源。正确的配置可确保在电源出现故障时 Dominion KX II 能发送相应的通知。例如，如果电源 1 出现故障，则设备前端的电源指示灯将变成红色。

要针对所使用的电源启用自动检测功能，请执行以下操作：

1. 选择“设备设置”**(Device Settings) >**“电源设置”**(Power Supply Setup)**。将打开“电源设置”(Power Supply Setup) 页。

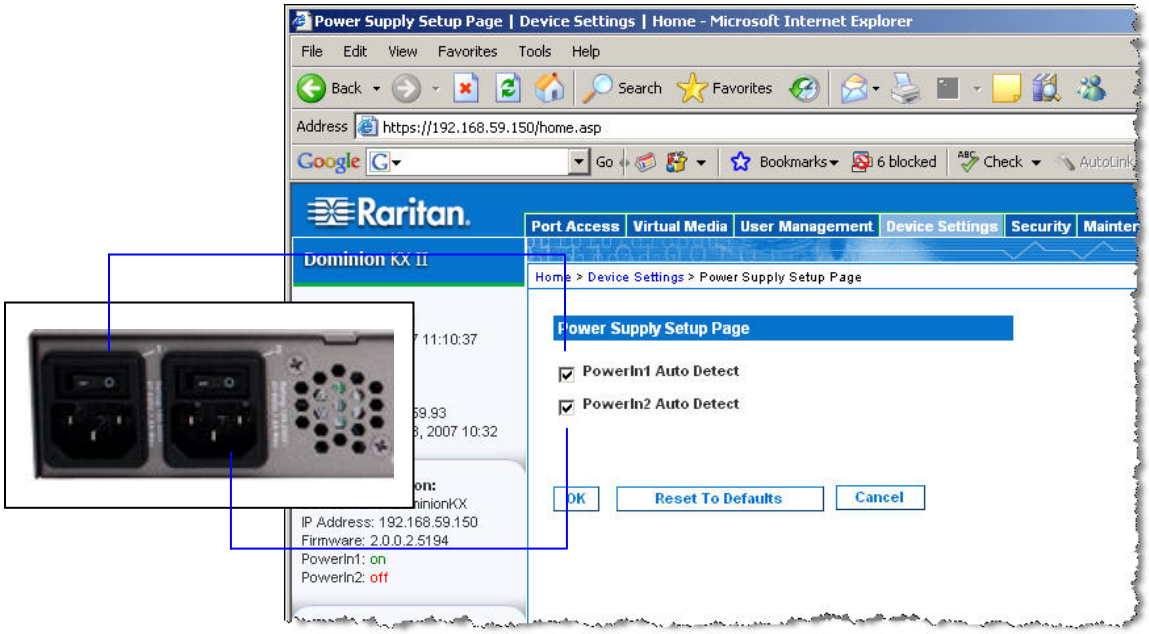


图 64：电源设置

2. 如果要将输入电源插入电源 1 中（设备背面最左边的电源），然后选中“电源 1 自动检测”**(PowerIn1 Auto Detect)** 选项。
3. 如果要将电源的输入端插入电源 2 中（设备背面最右边的电源），然后选中“电源 2 自动检测”**(PowerIn1 Auto Detect)** 选项。
4. 单击“确定”**(OK)**。

注意：*如果这两个复选框中的任意一个处于选中状态，而且实际上没有连接输入电源，则设备前面的电源指示灯会显示为红色。*

要关闭自动检测，请执行以下操作：

清除相应电源前面的复选框。

要复位为出厂默认值，请执行以下操作：

单击“复位为默认值”**(Reset to Defaults)** 按钮。

要取消而不保存更改，请执行以下操作：

单击“取消”**(Cancel)** 按钮。

注意：*Dominion KX II 不向 CommandCenter 报告电源状态。然而，Dominion I（1 代）却向 CommandCenter 报告电源状态。*

“端口配置”页

“端口配置”(Port Configuration) 页显示的是 Dominion KX II 端口的列表。连接到目标服务器或电源板的端口显示为蓝色，您可以对这些端口进行编辑。对于未连接 CIM 的端口或 CIM 名称为空白的端口，将分配默认端口名称 **Dominion-KX2_Port#**，其中 **Port#** 是 Dominion KX II 物理端口的编号。

要更改端口配置，请执行以下操作：

1. 选择“设备设置”**(Device Settings)** >“端口配置”**(Port Configuration)**。将打开“端口配置”(Port Configuration) 页：

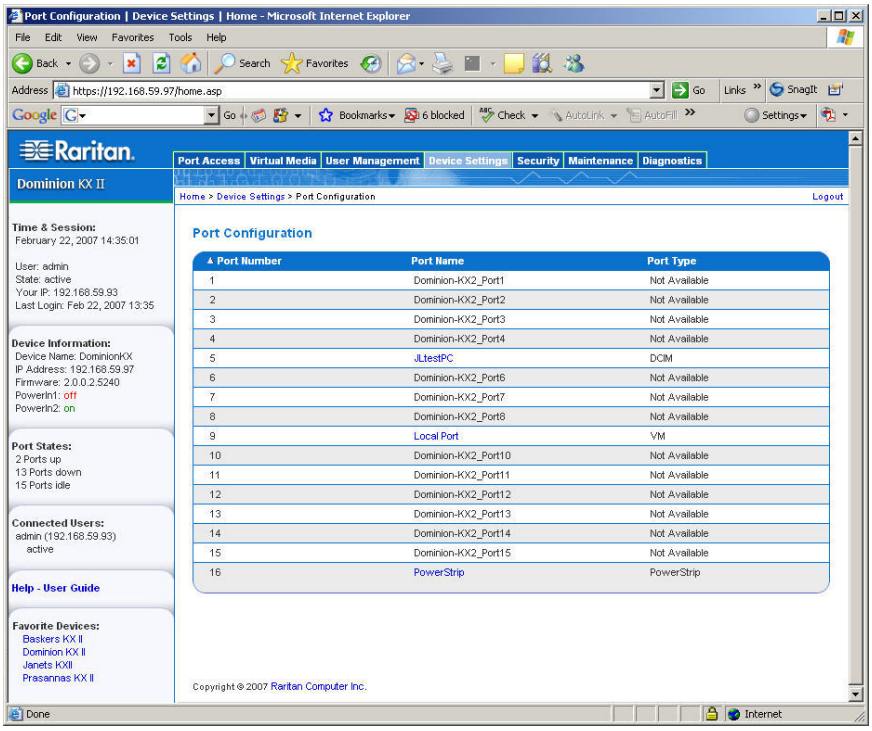


图 65：端口配置

此页最初按端口号顺序显示，不过可以通过单击列标题按任一字段排序。

- **端口号 (Port Number)**。从 1 开始编号，直到 Dominion KX II 设备可用的端口总数。
- **端口名称 (Port Name)**。分配给端口的名称。如果端口名称显示为空白，则表示端口名称不能更改，而且端口无法编辑；如果端口名称显示为蓝色，则表示端口是可以编辑的。
- **端口类型 (Port Type)**。连接到端口的 CIM 的类型：

端口类型	说明
DCIM	Dominion CIM
不可用	未连接 CIM
PCIM	Paragon CIM
PowerStrip	电源 CIM
VM	虚拟媒体 CIM (D2CIM-VUSB)

2. 单击要编辑的端口对应的“端口名称”**(Port Name)**。
   - 对于 KVM 端口，将打开“端口”(Port) 页。在此页中，可以命名端口和创建电源关联。
   - 对于电源板，将打开电源板的“端口”(Port) 页。在此页中，可以命名电源板及其插座。

电源控制

Dominion KX II 提供对目标服务器的远程电源控制。要利用此功能，必须有一个 Raritan 远程电源板和 D2CIM-PWR 计算机接口模块 (CIM)。进行电源分配之后，就可以对目标服务器进行远程电源管理了。

要使用 Dominion KX II 电源控制功能，请执行以下操作：

1. 连接电源板到目标服务器。
2. 命名电源板
3. 在电源板中关联插座至目标服务器。
4. 从“端口访问”(Port Access) 页中利用目标服务器的远程电源管理

连接电源板

下图中的编号对应于如下步骤的步骤编号。

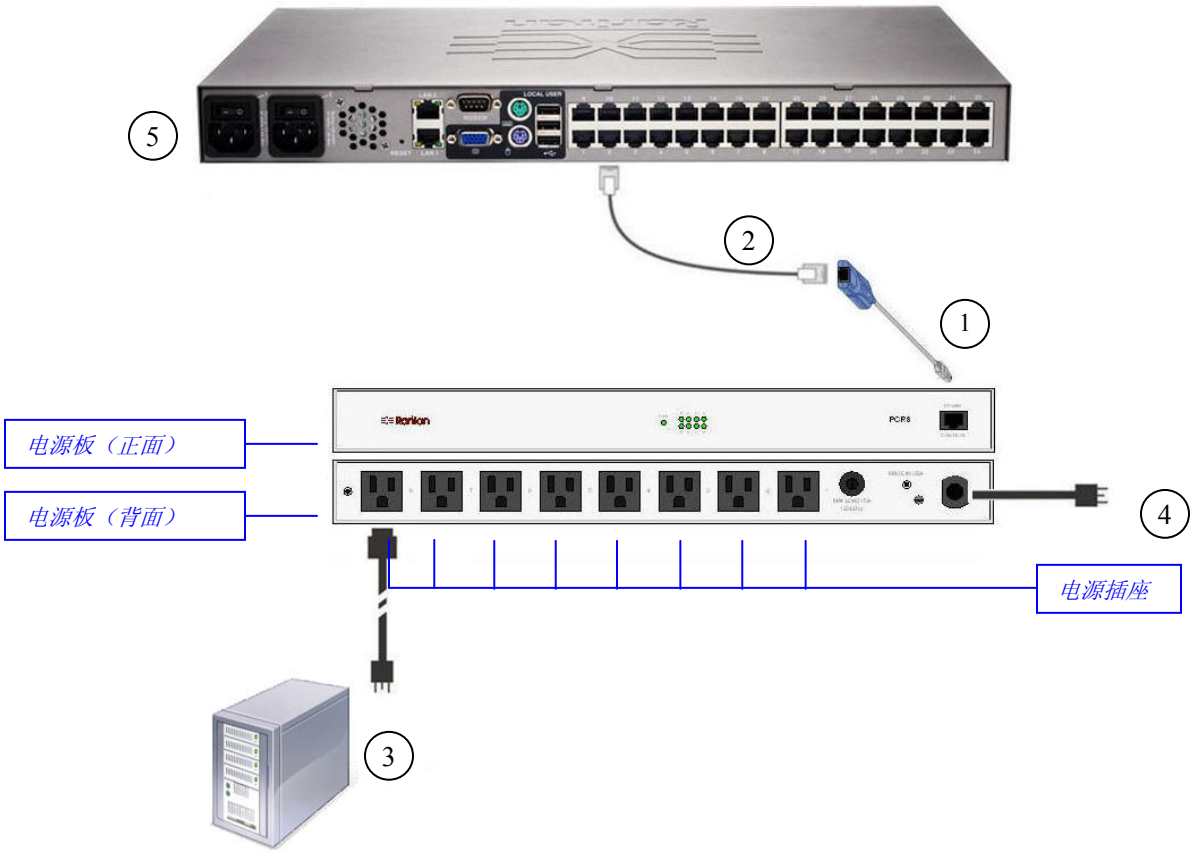


图 66：电源板连接

要连接电源板，请执行以下操作：

1. 将 D2CIM-PWR 的插针 RJ-45 连接到电源板上的插孔 RJ-45 连接端。
2. 使用直通 Cat 5 线缆将 D2CIM-PWR 的插孔 RJ-45 连接端连接到 Dominion KX II 上的任何可用插孔系统端口连接端。
3. 将交流电源线连接到目标服务器和可用的电源板插座。
4. 将电源板连接到交流电源。
5. 打开 Dominion KX II 设备的电源。

命名电源板（电源板的“端口”页）

当在端口配置页中选择连接到 Raritan 远程电源板的端口时，将打开此“端口”(Port) 页。“类型”(**Type**) 和“名称”(**Name**) 字段是预先填充的；请注意，您*不能* 更改 (CIM) “类型”(**Type**)。将显示电源板中每个插座的以下信息：插座“编号”(**Number**)、“名称”(**Name**) 和“端口关联”(**Port Association**)。

使用此页可命名电源板及其插座，所有名称最长可以为 32 个字母数字字符，可以包含特殊字符。

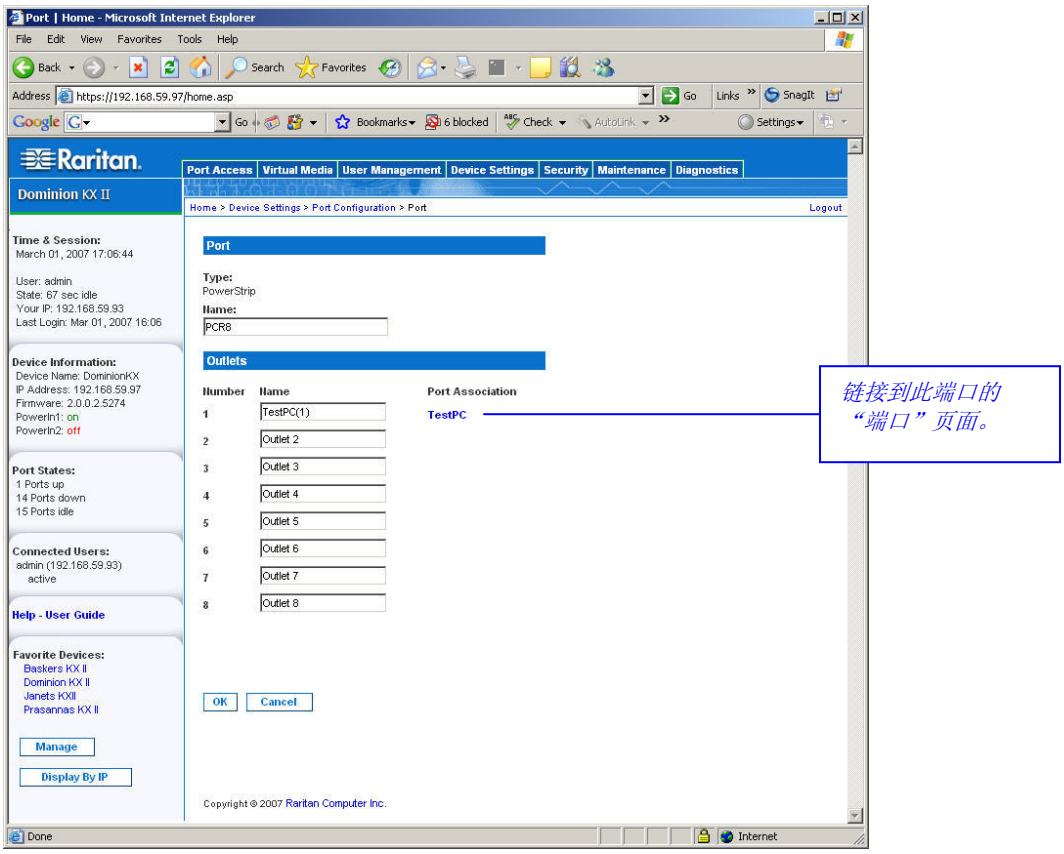


图 67：“端口”页（电源板）

***注意：**将电源板关联到目标服务器（端口）时，插座名称将替换为目标服务器的名称（即使为该插座分配了其它名称也是如此）。*

要命名电源板（及插座），请执行以下操作：

***注意：** CommandCenter Service Gateway 无法识别包含空格的电源板名称。*

1. 将电源板的“名称**(Name)** 更改为便于记忆的名称。
2. 如果需要，请更改（插座）“名称”**(Name)**。（插座名称默认为“插座编号”**(Outlet #)**。）
3. 单击“确定”**(OK)**。

要取消而不保存更改，请执行以下操作：

单击“取消”**(Cancel)** 按钮。

将目标服务器关联到插座（“端口”页）

当在端口配置页中选择连接到目标服务器的端口时，将打开此“端口”(Port) 页。在此页中，可以进行电源关联，将“端口名称”(Port Name) 更改为更具说明性的名称，以及更新目标服务器设置（如果使用的是 D2CIM-VUSB CIM）。(CIM)“类型”（**Type**）和（端口）“名称”（**Name**）字段是预先填充的；请注意，您*不能* 更改 CIM“类型”(Type)。

一台服务器最多可以有 4 个电源插头，每个插头均可关联不同的电源板。在此页中可以定义这些关联，以便可以从“端口访问”(Port Access) 页中打开服务器电源、关闭服务器电源和为服务器循环加电。

要使用此项功能，将需要：

- Raritan 远程电源板
- 电源 CIM (D2CIM-PWR)

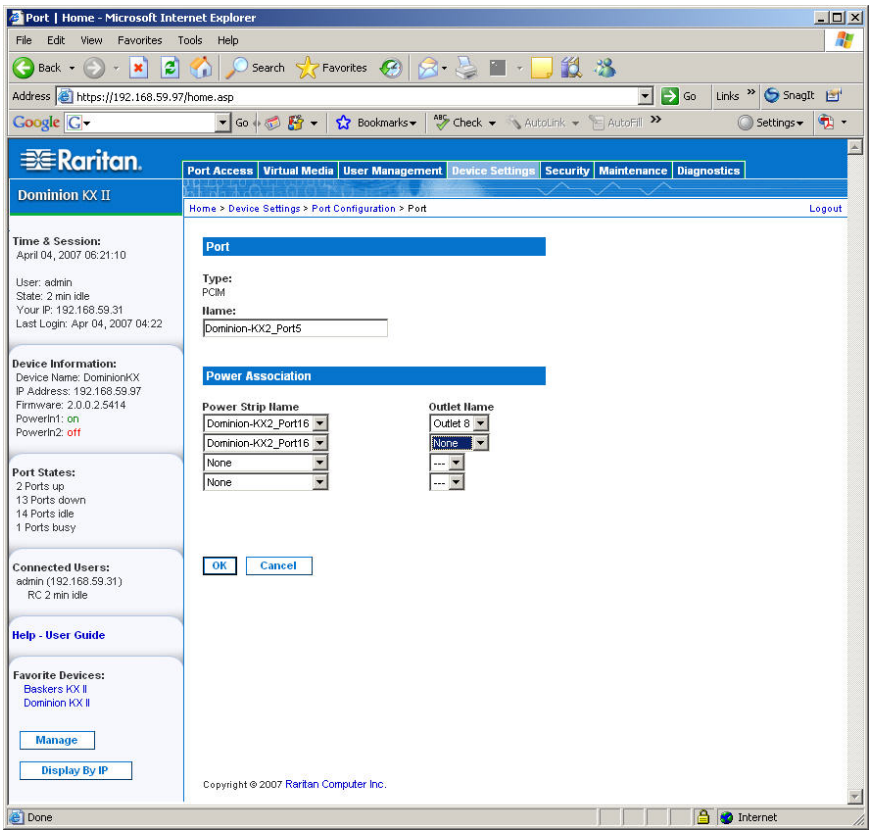


图 68：“端口”页（KVM 端口）

要进行电源关联（电源板插座与目标服务器关联），请执行以下操作：

***注意：**将电源板关联到目标服务器（端口）时，插座名称将替换为目标服务器的名称（即使为该插座分配了其它名称也是如此）。*

1. 从“电源板名称”**(Power Strip Name)** 下拉列表中选择所需的电源板。
2. 对于该电源板，从“插座名称”**(Outlet Name)** 下拉列表中选择所需的插座。
3. 对于全部所需的电源关联，重复步骤 1 和步骤 2。
4. 单击“确定”**(OK)**。将显示一条确认消息。

要更改端口名称，请执行以下操作：

1. 在“名称”**(Name)** 字段中键入具有说明性的名称。例如，目标服务器的名称就是可能的候选名称。该名称最长可以为 32 个字母数字字符，可以包含特殊字符。
2. 单击“确定”**(OK)**。

要取消而不保存更改，请执行以下操作：

单击“取消”**(Cancel)** 按钮。

要删除电源板关联，请执行以下操作：

1. 从“电源板名称”**(Power Strip Name)** 下拉列表中选择相应的电源板。
2. 对于该电源板，从“插座名称”**(Outlet Name)** 下拉列表中选择相应的插座。
3. 从“插座名称”**(Outlet Name)** 下拉列表中选择“无”**(None)**。
4. 单击“确定”**(OK)**。电源板/插座关联将被删除。将显示一条确认消息。

D2CIM-VUSB CIM 使用须知

如果使用的是 D2CIM-VUSB，则“端口”（Port）页上会显示有助于提高性能的附加设置。

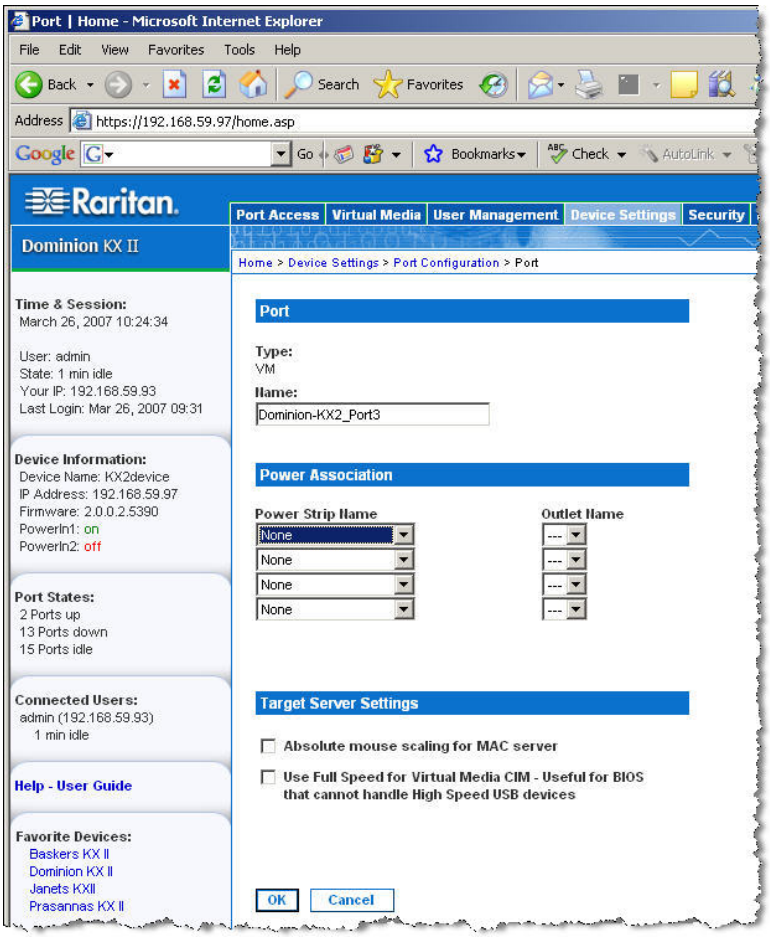


图 69：“端口”页（D2CIM-VUSB 的目标服务器设置）

如果遇到同步问题，而且针对 Mac 目标服务器使用的是 D2CIM-VUSB CIM，请选中“MAC 服务器的绝对鼠标缩放”**(Absolute mouse scaling for MAC server)** 选项。

某些特定的 BIOS 不支持 USB 高速功能，而且“自动尝试协商”功能也不起作用。如果目标服务器遇到 BIOS 问题，请选中“针对虚拟媒体 CIM 使用全速”**(Use Full Speed for Virtual Media CIM)** 选项。

注意：*对于 SUSE 9.2 目标服务器，请对目标服务器端口启用（选中）“针对虚拟媒体 CIM 使用全速”**(Use Full Speed for Virtual Media CIM)** 选项。当协商高速时，SUSE 9.2 不能与虚拟媒体 CIM 协同工作。*

第 10 章：安全设置

“安全”(Security) 菜单按以下各项进行组织：“安全设置”(Security Settings) 和“IP 访问控制”(IP Access Control)。

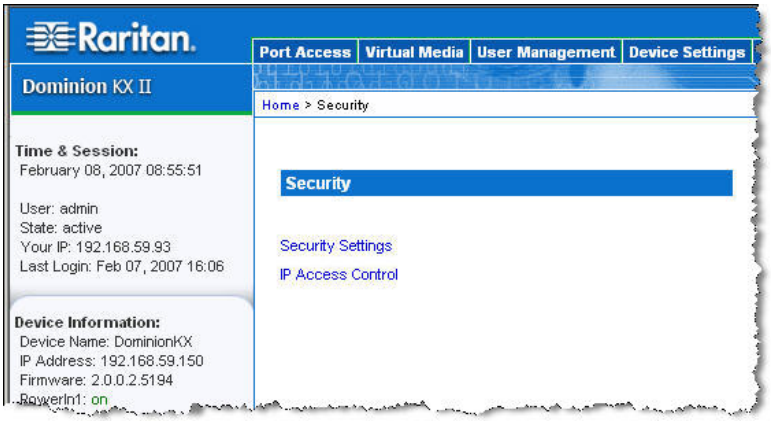


图 70：“安全”菜单

使用：	目的：
安全设置	配置登录限制、复合密码、用户阻止以及加密与共享等安全设置。
IP 访问控制	控制对 Dominion KX II 设备的访问。通过设置全局访问控制列表，可确保设备不响应从禁止的 IP 地址发送的封包。

安全设置

在“安全设置”(Security Settings) 页中，可以指定登录限制、用户阻止、密码规则，以及加密与共享。

Raritan SSL 证书可用于公用密钥和私有密钥交换，并提供额外的安全级别。Raritan 网络服务器证书是自签名证书；Java Applet 证书要由 VeriSign® 证书来签名。通过加密可以使信息免遭窃听，同时这些证书可确保您可以相信该实体就是 Raritan, Inc.。

要配置安全设置，请执行以下操作：

1. 选择“安全”**(Security)** >“安全设置”**(Security Settings)**。将打开“安全设置”(Security Settings) 页。

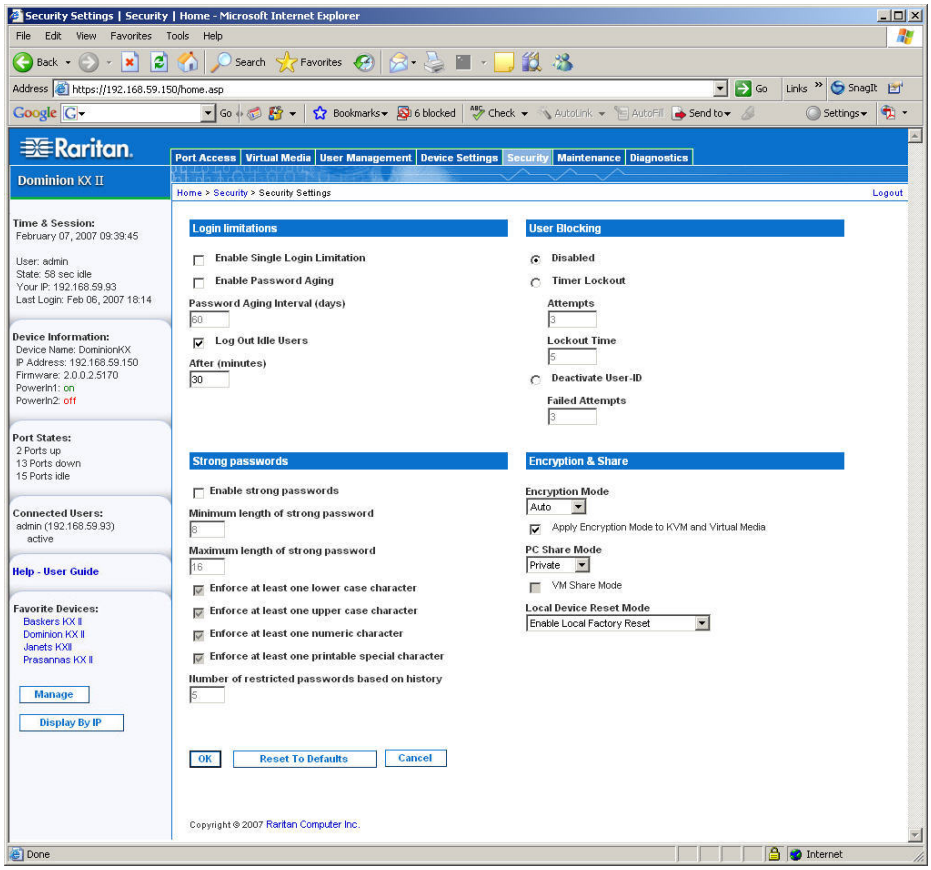


图 71：安全设置

这些字段应组织为以下几组：登录限制、复合密码、用户阻止，以及加密与共享。

2. 根据需要更新登录限制设置。
3. 根据需要更新复合密码设置。
4. 根据需要更新用户阻止设置。
5. 根据需要更新加密与共享设置。
6. 完成后单击“确定”**(OK)**。

要关闭此页且不保存任何更改，请执行以下操作：

单击“取消”**(Cancel)**。

要复位为默认值，请执行以下操作：

单击“复位为默认值”**(Reset to Defaults)**。

登录限制

使用“登录限制”(Login Limitations)，可以指定单点登录、密码过期以及空闲用户注销等方面的限制。

- **启用单点登录限制 (Enable Single Login Limitation)**。当该选项处于选中状态时，任何时候只允许每个用户名有一个登录。当该选项处于清除状态时，给定的用户名/密码组合可以从多个客户机工作站同时连接到设备。
- **启用密码过期 (Enable Password Aging)**。当该选项处于选中时，所有用户都需要基于“密码过期间隔”(Password Aging Interval) 字段中指定的天数定期更改其密码。
  - **密码过期间隔 (Password Aging Interval)**（天）。在选中“启用密码过期”(Enable Password Aging) 复选框时将启用此字段，此字段是必填的。输入需要在多少天之后更改密码。默认值为 60 天。
- **注销空闲用户 (Log Out Idle Users)**。如果选中此复选框，则可在经过特定的一段不活动时间之后自动取消用户会话的连接。在“之后”(After) 字段中键入所需的时间长度。如果没有来自键盘或鼠标的活动，则所有 KVM 会话和所有 KVM 资源都将注销。然而，如果正在进行“虚拟媒体”(Virtual Media) 会话，则该会话不会超时。
  - **之后 (After)（分钟）**。在经过多长时间之后空闲用户将被注销（分钟）。选中“注销空闲用户”**(Log Out Idle Users)** 选项时将启用此字段。

复合密码

复合密码为系统提供更为安全的本地认证。使用“复合密码”(Strong Passwords)，可以指定用来为 KX II 有效本地密码定义格式的标准，例如，最小和最大长度、所需的字符以及密码历史记录保留天数。

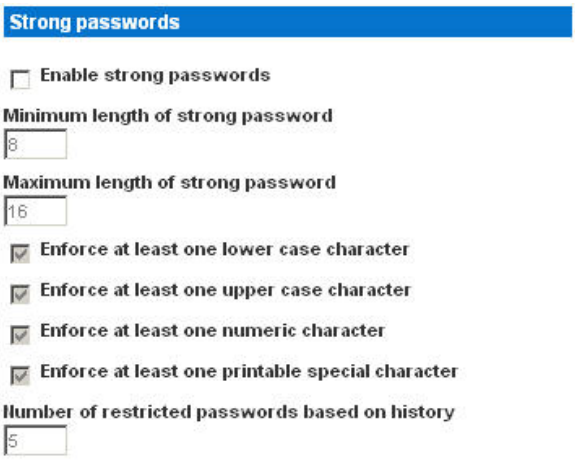


图 72：安全设置（复合密码）

- **启用复合密码（Enable strong passwords）**。复合密码要求用户创建的密码至少有 8 个字符，其中至少包含一个字母字符和一个非字母字符（标点字符或数字）。此外，密码和用户名的前 4 个字符不能相同。

  当该选项处于选中状态时，将实施复合密码规则。将自动要求密码不符合复合密码标准的用户在下次登录时更改其密码。当该选项处于清除状态时，仅实施标准格式验证。选中该选项时，将启用以下必填选项：

- **最小复合密码长度 (Minimum length of strong password)**。密码必须至少 8 个字符长。默认为 8 个字符，不过可以多达 63 个字符。
- **最大复合密码长度 (Maximum length of strong password)**。默认为 16 个字符，不过可以多达 64 个字符长。
- **强制至少包含一个小写字符 (Enforce at least one lower case character)**。当该选项处于选中状态时，要求密码中至少包含一个小写字符。
- **强制至少包含一个大写字符 (Enforce at least one upper case character)**。当该选项处于选中状态时，要求密码中至少包含一个大写字符。
- **强制至少包含一个数字字符 (Enforce at least one numeric character)**。当该选项处于选中状态时，要求密码中至少包含一个数字字符。
- **强制至少包含一个可打印特殊字符 (Enforce at least one printable special character)**。当该选项处于选中状态时，要求密码中至少包含一个（可打印的）特殊字符。
- **基于历史记录的限制密码个数 (Number of restricted passwords based on history)**。此字段表示密码历史记录深度；即不能重复的优先密码个数。范围是 1-12；默认为 5。

用户阻止

“用户阻止”(User Blocking) 选项指定如下标准：在达到指定的失败登录尝试次数之后阻止用户访问系统。以下三个选项相互排斥：

- **禁用 (Disabled)**。默认选项；无论用户认证失败多少次，都不阻止该用户。
- **计时器锁定 (Timer Lockout)**。在超过指定的失败登录尝试次数之后的指定时间段内拒绝用户访问系统。当该选项处于选中状态时，将启用以下字段：
  - **尝试次数 (Attempts)**。在登录尝试失败多少次之后将锁定用户。有效范围是 1 – 10；默认为尝试 3 次。
  - **锁定时间 (Lockout Time)**。将要使用户处于锁定状态的时间长度。有效范围是 1 – 1440 分钟；默认为 5 分钟。
- **停用用户 ID (Deactivate User-ID)**。当该选项处于选中状态时，将指定在达到“失败尝试次数”(Failed Attempts) 字段中指定的失败登录尝试次数之后，用户将被系统锁定：
  - **失败尝试次数 (Failed Attempts)**。在登录尝试失败多少次之后停用用户的“用户 ID”(User-ID)。选中“停用用户 ID”(Deactivate User-ID) 选项时将启用此字段。有效范围是 1 – 10。

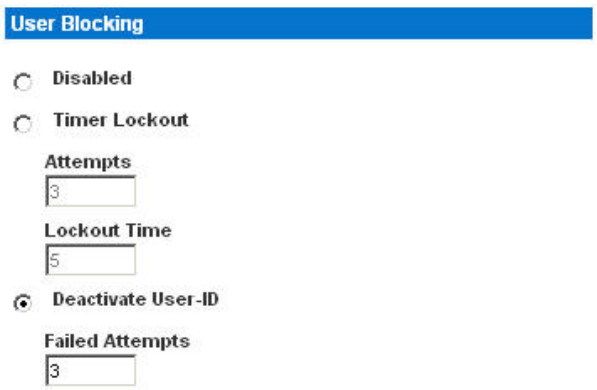


图 73：安全设置（用户阻止）

在达到指定的失败尝试次数之后停用用户 ID 时，管理员必须更改用户密码，然后在“用户”(User) 页上选中“活动”(Active) 复选框来激活用户帐户。

加密与共享

使用“加密与共享”(Encryption & Share) 设置，可以指定使用的加密类型、PC 和 VM 共享模式，以及在按下 Dominion KX II 复位按钮时要执行的复位类型。

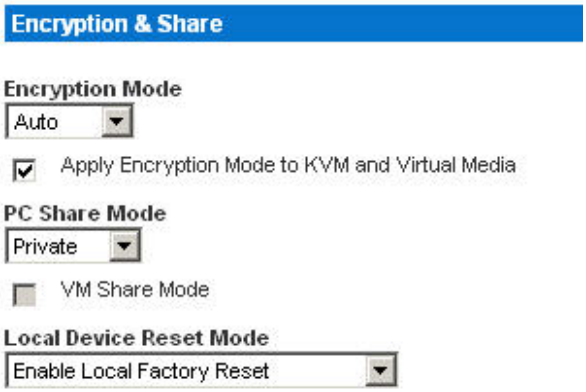


图 74：安全设置（加密与共享）

- **加密模式 (Encryption Mode)**。选择下拉列表中的选项之一。选择加密模式后将显示一条警告，即如果浏览器不支持所选模式，则将无法连接到 Dominion KX II：

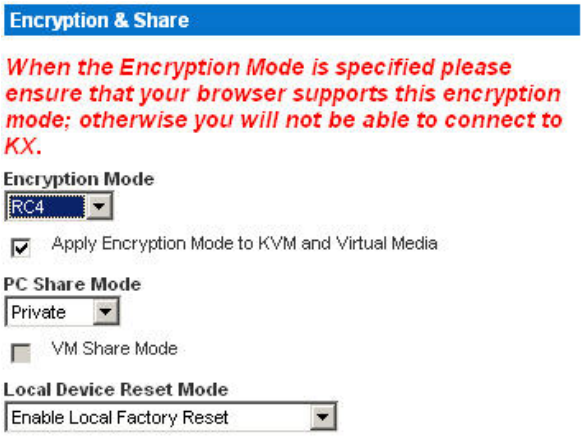


图 75：安全设置（加密模式警告消息）

  - **自动 (Auto)**。这是建议的选项；Dominion KX II 将自动协商到可能的最高加密级别。
  - **RC4**。使用 RSA RC4 加密方法来保护用户名、密码以及 KVM 数据（包括所传输的视频）。这是一个 128 位的安全套接字层 (SSL) 协议，在进行初始连接认证期间，该协议将在 Dominion KX II 设备与远程 PC 之间提供专用的通信通道。
  - **AES-128**。高级加密标准 (AES) 是美国国家标准与技术研究院提供的电子数据加密规范；128 是密钥长度。指定 AES-128 时，请确保浏览器支持它，否则将无法连接。有关更多信息，请参阅检查浏览器是否使用 AES 加密。
- **将加密模式应用于 KVM 和虚拟媒体 (Apply Encryption Mode to KVM and Virtual Media)**。当该选项处于选中状态时，会将所选加密模式应用于 KVM 和虚拟媒体。认证之后，KVM 和虚拟媒体数据也以 128 位加密方式进行传送。

- **PC 共享模式 (PC Share Mode)**。确定*全局*并发远程 KVM 访问，最多允许八个远程用户同时登录到一个 Dominion KX II 设备，可通过该设备同时查看和控制同一个目标服务器。单击下拉列表可选择下列选项之一：
  - **专用 (Private)**：禁止 PC 共享；这是默认模式。在某一时刻，每个目标服务器只能由一个用户*以独占方式访问*。
  - **PC 共享 (PC-Share)**：在某一时刻，目标服务器最多可以由 8 个用户（管理员或非管理员）访问。每个远程用户都有同等的键盘和鼠标控制权，不过请注意，如果某一用户不停止键入或移动鼠标，则会出现非均等控制权。
- **VM 共享模式 (VM Share Mode)**。仅当启用了“PC 共享模式”(PC-Share Mode) 时，才能启用该选项。当该选项处于选中状态时，允许在多个用户间共享虚拟媒体，即多个用户可访问同一个虚拟媒体会话。该选项在默认情况下处于禁用状态。
- **本地设备复位模式 (Local Device Reset Mode)**。此选项指定在按下硬件复位按钮（在设备的背面）时要执行的操作。有关更多信息，请参阅复位按钮。可选择以下选项之一：
  - **启用本地出厂复位 (Enable Local Factory Reset)**（默认设置）。Dominion KX II 设备将返回到出厂默认值。
  - **启用本地管理员密码复位 (Enable Local Admin Password Reset)**。仅复位本地管理员密码。密码将复位为 **raritan**。
  - **禁用所有本地复位 (Disable All Local Resets)**。禁止执行任何复位操作。

检查浏览器是否使用 AES 加密

如果不清楚浏览器是否使用 AES，请与浏览器厂商核对，或者在使用要核对的加密方法的浏览器中导航到以下网站：https://www.fortify.net/sslcheck.html。此网站将检测该浏览器使用的加密方法并显示一份报告。

IP 访问控制

使用“IP 访问控制”(IP Access Control)，可以控制对 Dominion KX II 设备的访问。通过设置全局访问控制列表 (ACL)，可确保设备不响应从禁止的 IP 地址发送的封包。“IP 访问控制”(IP Access Control) 是全局性的，会对整个 KX 设备产生影响。但是您也可以在组级别控制对设备的访问。有关组级别控制的更多信息，请参阅基于组的 IP 访问控制。

重要事项：IP 地址 127.0.0.1 由 Dominion KX II 本地端口使用。创建 IP 访问控制列表时，如果 127.0.0.1 处于被阻止的 IP 地址范围之内，您将无权访问 Dominion KX II 本地端口。

要使用 IP 访问控制，请执行以下操作：

1. 可使用下列方法之一打开“IP 访问控制”(IP Access Control) 页：
   - 选择“安全”**(Security) >**“IP 访问控制”**(IP Access Control)**，或者
   - 在“网络设置”(Network Settings) 页中单击“设置系统 ACL”**(Set System ACL)** 按钮
   - 将打开 IP 访问控制页：

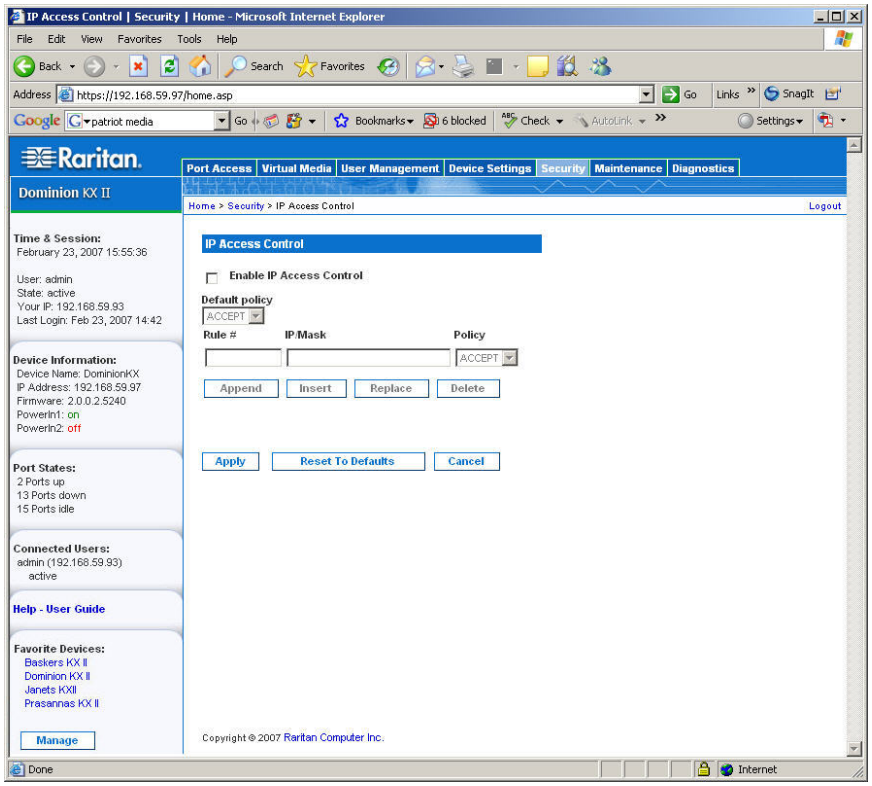


图 76：IP 访问控制

2. 在该页上选中“启用 **IP** 访问控制”**(Enable IP Access Control)** 复选框，以启用 IP 访问控制及其余的字段。
3. 选择“默认策略”**(Default Policy)**。对于不在指定范围内的 IP 地址，会执行此操作。
   - 接受 **(Accept)**。允许 IP 地址访问 Dominion KX II 设备。
   - 放弃 **(Drop)**。拒绝 IP 地址访问 Dominion KX II 设备。

要添加（追加）规则，请执行以下操作：

1. 在“**IP/**掩码”**(IP/Mask)** 字段中键入 IP 地址和子网掩码。
2. 从下拉列表中选择“策略”**(Policy)**。
3. 单击“追加”**(Append)**。规则将添加到规则列表的底部。
4. 对于要输入的每一条规则，都要重复步骤 1 到步骤 3。

要插入规则，请执行以下操作：

1. 键入一个“规则号”**(Rule #)**。使用“插入”**(Insert)** 命令时，“规则号”(Rule #) 是必填的。
2. 在“**IP/**掩码”**(IP/Mask)** 字段中键入 IP 地址和子网掩码。
3. 从下拉列表中选择“策略”**(Policy)**。
4. 单击“插入”**(Insert)**。如果刚才键入的“规则号”(Rule #) 等于现有的“规则号”(Rule #)，则新规则将放在现有规则的前面，同时列表中的所有规则都将下移。

要替换规则，请执行以下操作：

1. 指定要替换的“规则号”**(Rule #)**。
2. 在“**IP/**掩码”**(IP/Mask)** 字段中键入 IP 地址和子网掩码。
3. 从下拉列表中选择“策略”**(Policy)**。
4. 单击“替换”**(Replace)**。新规则将替换具有相同“规则号”**(Rule #)** 的原始规则。

要删除规则，请执行以下操作：

1. 指定要删除的“规则号”**(Rule #)**。
2. 单击“删除”**(Delete)**。
3. 系统将提示您确认删除。单击“确定”**(OK)**。

提示：通过规则号，可以更好地控制规则的创建顺序。

第 11 章：维护

“维护”(Maintenance) 菜单包括以下这些选项：“审计日志”(Audit Log)、“设备信息”(Device Information)、“备份/恢复”(Backup/Restore)、“CIM 固件升级”(CIM Firmware Upgrade,)、“固件升级”(Firmware Upgrade)、“出厂复位”(Factory Reset)（仅限 Dominion KX II Local Console）、“升级报告”(Upgrade Report) 以及“重新引导”(Reboot)。

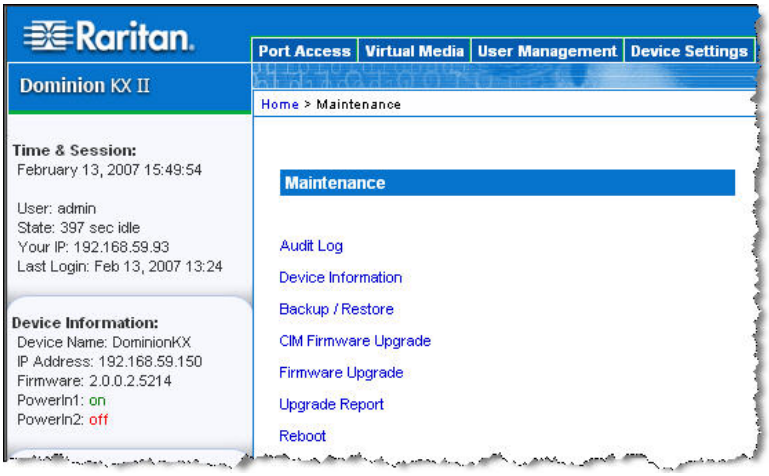


图 77：“维护”菜单

使用：	目的：	本地	远程
审计日志	查看按日期和时间排序的 Dominion KX II 事件。	✓	✓
设备信息	查看有关 Dominion KX II 及其 CIM 的信息。	✓	✓
备份/恢复	备份和恢复 KX II 配置。		✓
CIM 固件升级 (CIM Firmware Upgrade)	使用 Dominion KX II 内存中存储的固件版本升级 CIM。	✓	✓
固件升级	升级 Dominion KX II 固件。		✓
出厂复位 (Factory Reset)	执行出厂复位。	✓	
升级报告	查看有关最近执行的升级的信息。	✓	✓
重新引导	重新引导 Dominion KX II 设备。	✓	✓

审计日志

为 Dominion KX II 系统事件创建的日志。

要查看 Dominion KX II 设备的审计日志，请执行以下操作：

选择“维护”**(Maintenance)** >“审计日志”**(Audit Log)**。将打开“审计日志”**(Audit Log)** 页：

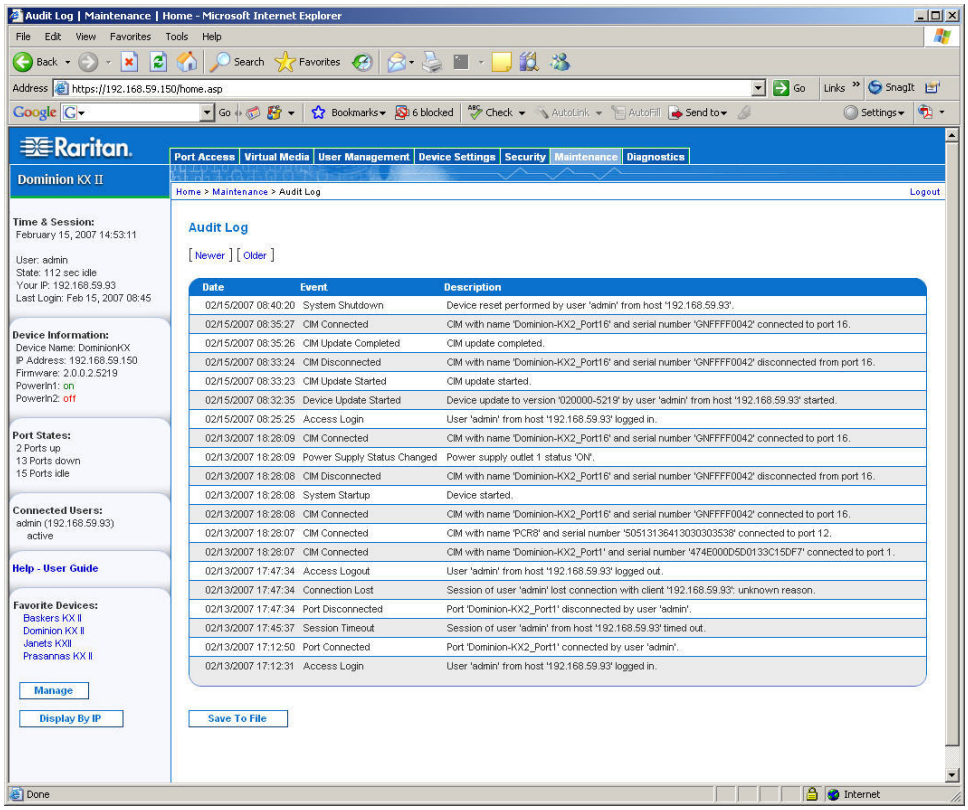


图 78：审计日志

“审计日志”(Audit Log) 页按日期和时间显示事件（最近的事件首先列出）。“审计日志”(Audit Log) 提供以下信息：

- **日期 (Date)**。事件发生的日期和时间（采用 24 小时制）。
- **事件 (Event)**。列在“事件管理”(Event Management) 页中的事件名称。
- **说明 (Description)**。事件的详细说明。

要保存审计日志，请执行以下操作：

***注意：** “审计日志”的保存操作只能在 Dominion KX II Remote Console 上执行，而不能在 Local Console 上执行。*

1. 单击“保存到文件”**(Save to File)** 按钮。将打开“保存文件”(Save File) 对话框。
2. 选择所需的文件名和位置，然后单击“保存”**(Save)**。审计日志将以指定的名称和位置保存到*本地*客户机上。

要遍历审计日志，请执行以下操作：

请使用“[更旧]”**([Older])** 和“[更新]”**([Newer])** 链接。

设备信息

“设备信息”(Device Information) 页提供有关所使用的 Dominion KX II 设备和 CIM 的详细信息。在需要与 Raritan 技术支持部门联系时，此信息将有很大帮助。

要查看有关 Dominion KX II 和 CIM 的信息，请执行以下操作：

选择“维护”**(Maintenance)** >“设备信息”**(Device Information)**。将打开“设备信息”(Device Information) 页：

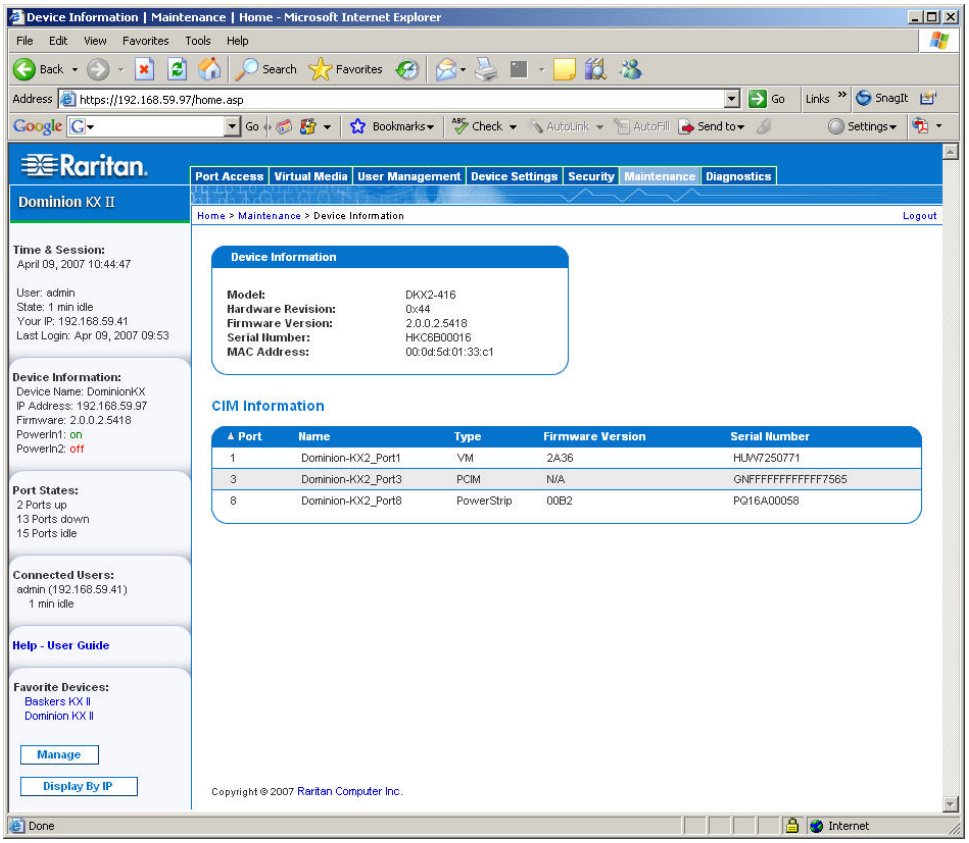


图 79：设备信息

该页中提供有关 Dominion KX II 的以下信息：“型号”**(Model)**、“硬件修订版”**(Hardware Revision)**、“固件版本”**(Firmware Version)**、“序列号”**(Serial Number)**以及“MAC 地址”**(MAC Address)**。

该页中提供有关所使用的 CIM 的以下信息：“端口”**(Port)**（号）、“名称”**(Name)**、“类型”**(Type)**（适用于 CIM：DCIM、PCIM、电源板或 VM）、“固件版本”**(Firmware Version)**以及“序列号”**(Serial Number)**。

备份和恢复

从“备份/恢复”(Backup/Restore) 页中，可以备份和恢复 Dominion KX II 的设置和配置。备份和恢复功能除了用于使业务连续，还可以省时。例如，您可以从另一个 Dominion KX II 快速提供对您的团队的访问，方法是从所使用的 KX II 设备备份用户配置并将这些配置恢复到新的 KX II。还可以先设置一个 Dominion KX II，然后将其配置复制到多个 KX II 设备。

要访问“备份/恢复”(Backup/Restore) 页，请执行以下操作：

选择“维护”**(Maintenance)** >“备份/恢复”**(Backup/Restore)**。将打开“备份/恢复”(Backup/Restore) 页：

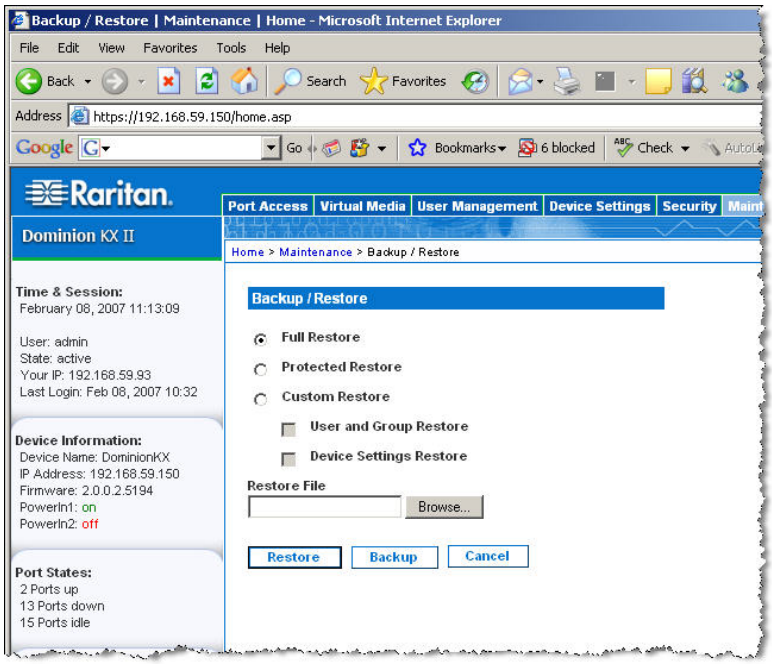


图 80：备份/恢复

***注意：**备份总是以完整的系统备份形式进行，恢复可以是完整恢复，也可以是部分恢复，具体情况取决于您的选择。*

要备份 Dominion KX II，请执行以下操作：

1. 单击“备份”**(Backup)**。将打开“文件下载”(File Download) 对话框。
2. 单击“保存”**(Save)**。将打开“另存为”(Save As) 对话框。
3. 选择所需的位置，指定文件名，然后单击“保存”**(Save)**。将打开“下载完成”(Download Complete) 对话框。
4. 单击“关闭”**(Close)**。备份文件将以指定的名称和位置保存到*本地*客户机上。

要恢复 Dominion KX II，请执行以下操作：

警告：将 Dominion KX II 恢复到较早版本时，须格外小心。在对备份进行恢复时，必须知道用户名和密码。如果忘了旧的管理用户名和密码，则 KX II 将被锁定。

此外，如果在备份时使用了不同的 IP 地址，则该 IP 地址也将被恢复。如果配置使用的是 DHCP，那么，只有当您有权访问本地端口以在更新后检查 IP 地址时，才可能需要执行此操作。

1. 选择要运行的恢复类型：
   - **完全恢复 (Full Restore)**。完整地恢复整个系统；通常用于进行传统的备份和恢复。
   - **受保护的恢复 (Protected Restore)**。恢复除 特定于设备的信息（如序列号、MAC 地址、IP 地址、名称、端口名等）以外的所有配置。使用该选项，可以对一个 Dominion KX II 设备进行设置并将其配置复制到多个 KX II 设备。
   - **自定义恢复 (Custom Restore)**。使用此选项，可以选择“用户和组恢复”(User and Group Restore)、“设备设置恢复”(Device Settings Restore) 或两者都选择。选中相应的复选框：
     - **恢复用户和组 (User and Group Restore)**。此选项仅包括用户和组信息。使用此选项可以在另一个 Dominion KX II 设备上快速设置用户。
     - **恢复设备配置 (Device Settings Restore)**。此选项仅包括设备设置。使用此选项可以快速复制设备信息。
2. 单击“浏览”**(Browse)** 按钮。将打开“选择文件”(Choose file) 对话框。
3. 定位到相应的备份文件并选中该文件，然后单击“打开”**(Open)**。所选文件将在“恢复文件”**(Restore File)** 字段中列出。
4. 单击“恢复”**(Restore)**。基于所选恢复类型的配置将会恢复。

CIM 升级

通过此过程，可以使用存储在 Dominion KX II 设备内存中的固件版本来升级 CIM。一般情况下，当使用固件升级页升级设备固件时，所有的 CIM 都将会升级。使用“CIM 升级”(CIM Upgrade) 页可升级新的 CIM。

注意：从该页只能升级 D2CIM-VUSB 和 D2CIM-PWR。

要使用 Dominion KX II 内存升级 CIM，请执行以下操作：

1. 选择“维护”**(Maintenance)** > “**CIM** 固件升级”**(CIM Firmware Upgrade)**。将打开“从 KX 闪存升级 CIM”(CIM Upgrade from KX Flash) 页：

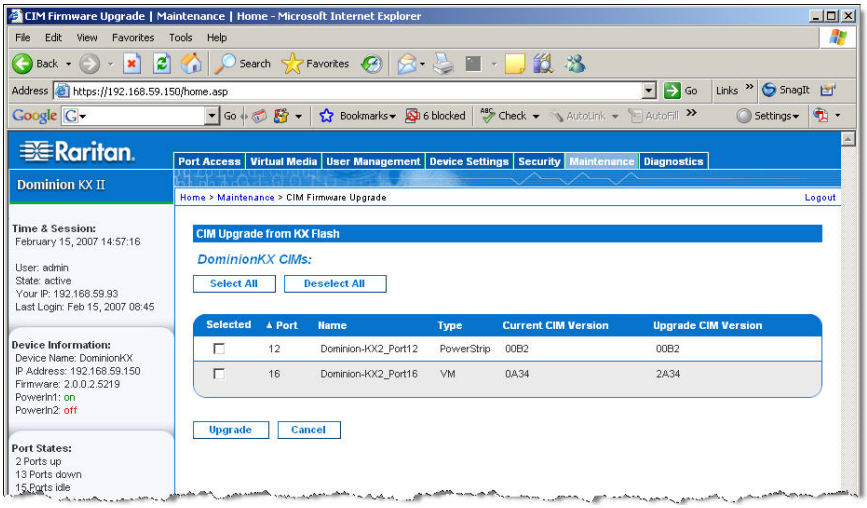


图 81：从 KX 闪存升级 CIM

2. 将显示“端口”**(Port)**（号）、“名称”**(Name)**、“类型”**(Type)**、“当前的 **CIM** 版本”**(Current CIM Version)** 和“升级 **CIM** 版本”**(Upgrade CIM Version)**，以便容易识别 CIM。
3. 选中与要升级的每个 CIM 相对应的“选中”(Selected) 复选框。

*提示：使用“全选”**(Select All)** 和“取消全选”**(Deselect All)** 按钮，可以快速选择全部（或取消选择全部）CIM。*

4. 单击“升级”**(Upgrade)** 按钮。系统将提示您确认升级。
5. 单击“确定”**(OK)** 继续升级。升级过程中将显示进度条。每个 CIM 的升级时间大约为 2 分钟（或不到 2 分钟）。

要退出而不升级，请执行以下操作：

单击“取消”**(Cancel)** 按钮。

固件升级

使用“固件升级”(Firmware Upgrade) 页，可以升级 Dominion KX II 设备的固件以及它所连接的全部 CIM。只有在 *KX II Remote Console 中才提供此页。*

重要事项：在升级过程中请勿关闭 Dominion KX II 设备或断开 CIM 的连接，这样很可能会对该设备或 CIM 造成损坏。

要升级 Dominion KX II 设备，请执行以下操作：

1. 在 Raritan 固件升级网页（网址是 http://www.raritan.com/support/firmwareupgrades）上找到相应的 Raritan 固件分发文件（*.RFP 格式）并下载该文件。
2. 解压缩该文件。升级前请先仔细阅读该固件 ZIP 文件中包含的所有说明。

***注意：**上载前请先将固件更新文件复制到本地 PC。请不要从网络驱动器加载文件。*

3. 选择“维护”**(Maintenance)** >“固件升级”**(Firmware Upgrade)**。将打开“固件升级”(Firmware Upgrade) 页：

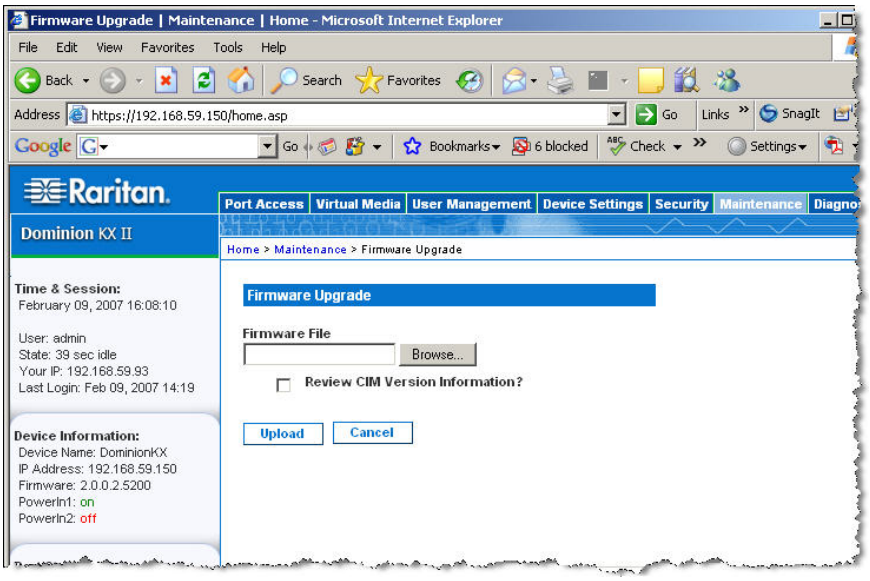


图 82：固件升级

4. 单击“浏览”**(Browse)** 按钮定位到解压缩升级文件所在的目录。
5. 如果希望显示有关所使用的 CIM 版本的信息，请选中“是否查看 **CIM** 版本信息?”**(Review CIM Version Information?)**复选框。
6. 在“固件升级”(Firmware Upgrade) 页中单击“上载”**(Upload)**。将显示有关升级和版本号的信息供您确认（如果选择查看 CIM 信息，则还将显示该信息）：

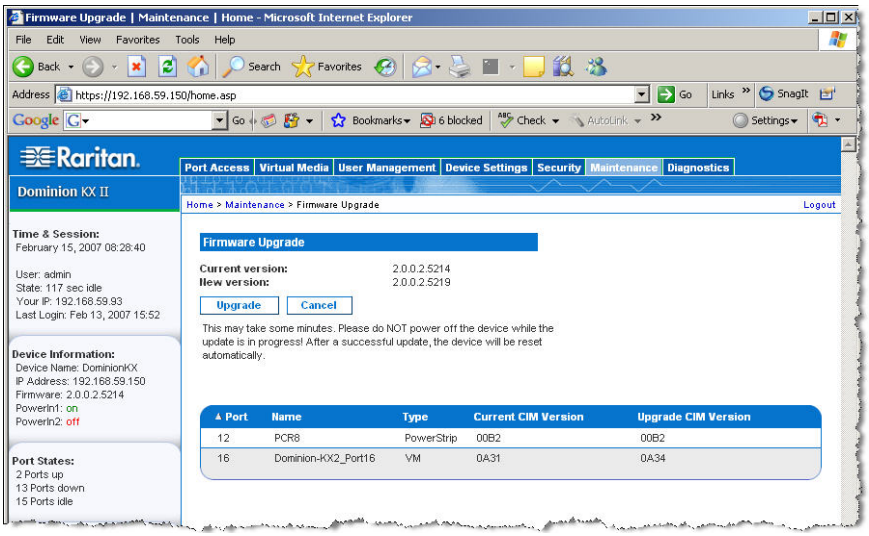


图 83：固件升级查看

***注意：**此时，已连接的用户都将被注销，新的登录尝试都将被阻止。*

7. 单击“升级”**(Upgrade)**。请等候升级完成。升级过程中将显示状态信息和进度条。升级一完成，设备就会重新引导（以一声“嘟”音发出重新引导信号）。

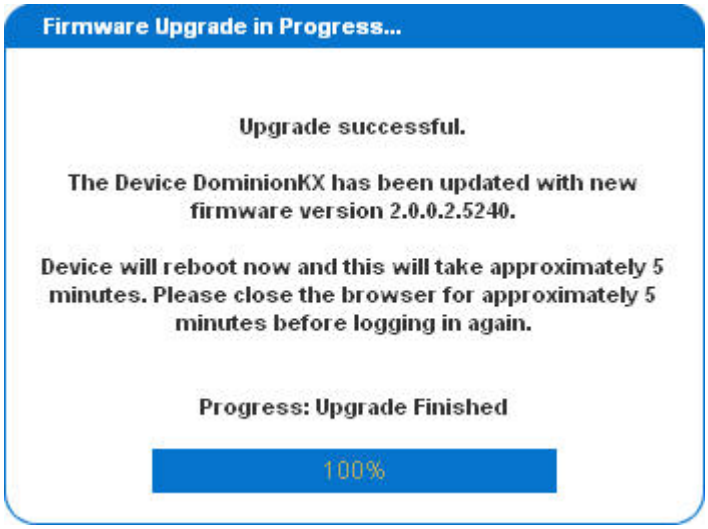


图 84：固件升级成功

8. 出现提示时关闭浏览器，大约等待 5 分钟，之后再次登录到 Dominion KX II。

有关使用 Multi-Platform Client 升级设备固件的信息，请参阅《Raritan Multi-Platform Client (MPC) 和 Raritan Remote Client (RRC) 用户指南》(Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide)。

升级报告

Dominion KX II 提供有关对 KX II 设备和它所连接的 CIM 所执行升级的信息。

要查看升级报告，请执行以下操作：

选择“维护”**(Maintenance)** >“升级报告”**(Upgrade Report)**。将打开“升级报告”(Upgrade Report) 页：

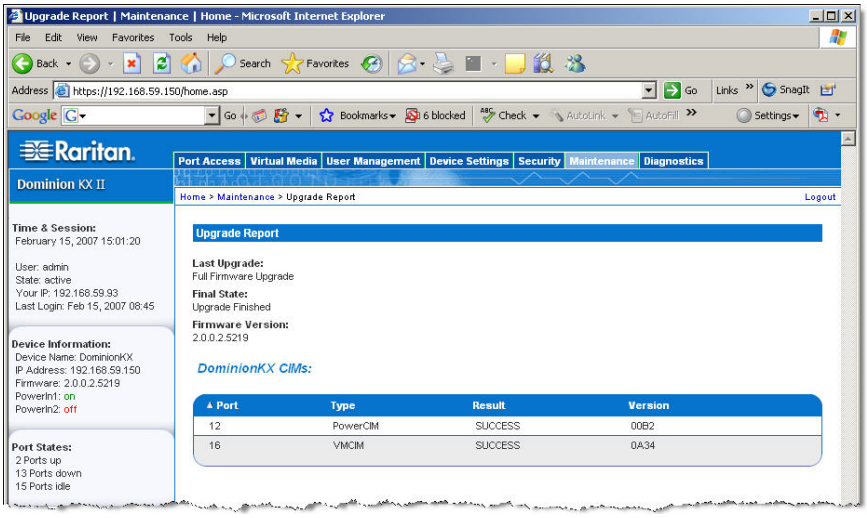


图 85：升级报告

报告中提供有关上次运行的 Dominion KX II 升级、该升级的最终状态以及固件版本的信息，同时还将提供有关 CIM 的信息：

- **端口 (Port)**。CIM 所连接到的端口。
- **类型 (Type)**。CIM 的类型。
- **结果 (Result)**。升级的结果（成功还是失败）。
- **版本 (Version)**。CIM 固件版本。

重新引导

“重新引导”(Reboot) 页提供了一种安全可控的方法来重新引导 Dominion KX II 设备，这是建议的重新引导方法。

重要事项：所有的 KVM 连接都将被关闭，所有用户都将被注销。

要重新引导 Dominion KX II，请执行以下操作：

1. 选择“维护”**(Maintenance)** > “重新引导”**(Reboot)**。将打开“重新引导”(Reboot) 页：

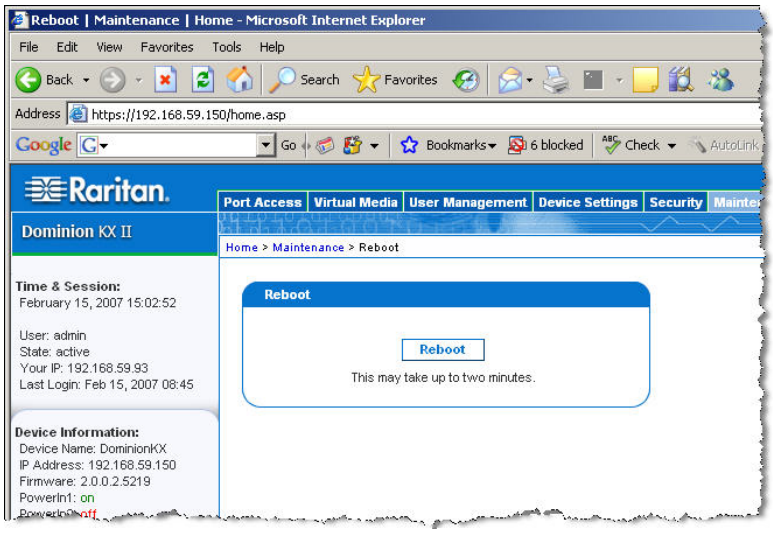


图 86：重新引导

2. 单击“重新引导”**(Reboot)** 按钮。系统将提示您确认该操作：

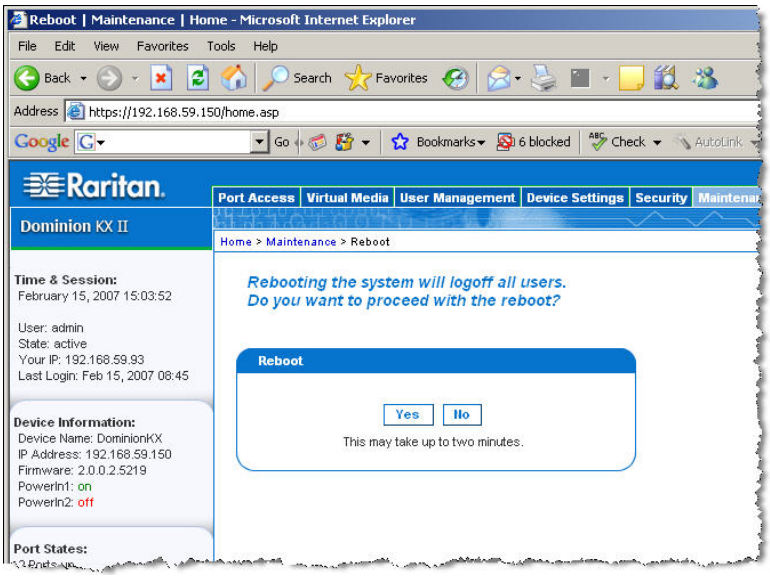


图 87：重新引导确认

3. 单击“是”**(Yes)** 继续重新引导。

要退出而不重新引导，请执行以下操作：

单击“否”**(No)**。

第 12 章：诊断

“诊断”菜单

“诊断”(Diagnostics) 页用于疑难排解，主要供 KX II 设备的管理员使用。所有的“诊断”(Diagnostics) 页（KX 诊断除外）均运行标准网络命令；所显示的信息是这些命令的输出。

“诊断”(Diagnostics) 页上的下列选项可帮助调试和配置网络设置：

- 网络接口
- 网络统计信息 (Network Statistics)
- Ping 主机
- 跟踪到主机的路由

“KX 诊断”(KX Diagnostics) 选项应在 Raritan 技术支持人员的指导下使用。

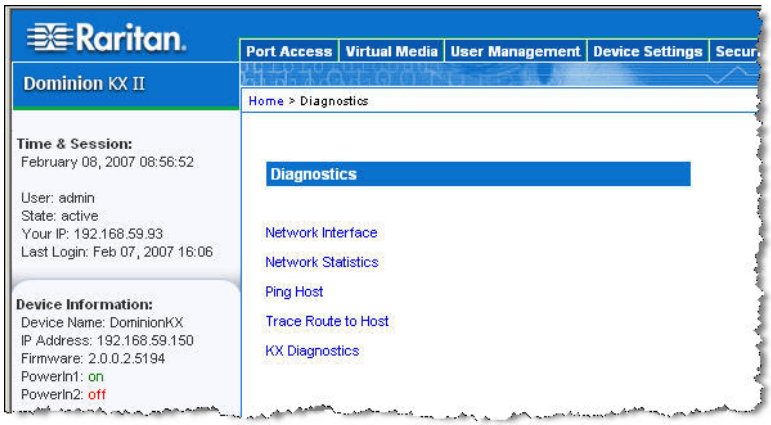


图 88：“诊断”菜单

使用：	目的：
网络接口	获取网络接口的状态。
网络统计信息 (Network Statistics)	获取有关网络的统计信息。
Ping 主机	确定是否可以通过 IP 网络与特定主机联系。
跟踪到主机的路由	确定到达所选主机所经过的整个路由。
KX 诊断	应在 Raritan 技术支持人员的指导下使用*（仅限 Remote Console）*。

“网络接口”页

Dominion KX II 提供有关网络接口状态的信息。

要查看有关网络接口的信息，请执行以下操作：

选择“诊断”**(Diagnostics)** >“网络接口”**(Network Interface)**。将打开“网络接口”(Network Interface) 页：

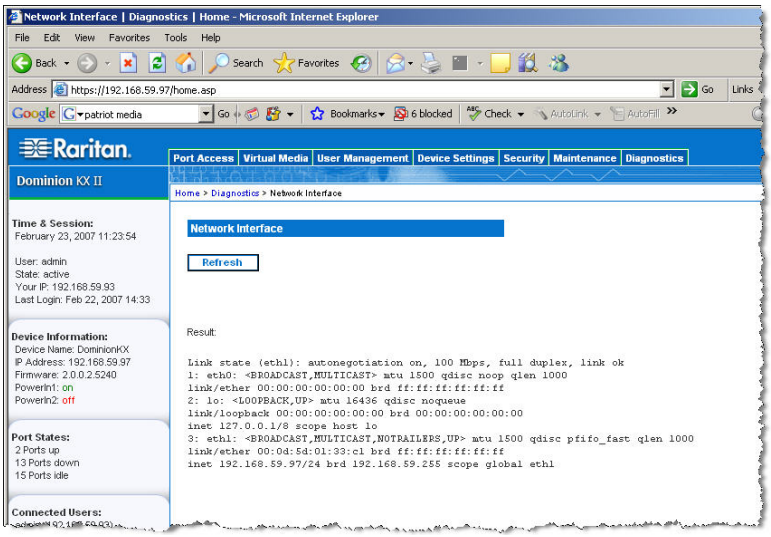


图 89：网络接口

显示以下信息：

- 以太网接口是处于打开还是关闭状态。
- 能否 ping 到网关。
- 当前处于活动状态的 LAN 端口。

要刷新此信息，请执行以下操作：

单击“刷新”**(Refresh)** 按钮。

“网络统计信息”页

Dominion KX II 提供有关您的网络接口的统计信息。

要查看有关网络接口的统计信息，请执行以下操作：

1. 选择“诊断”**(Diagnostics)** >“网络统计信息”**(Network Statistics)**。将打开“网络统计信息”**(Network Statistics)** 页。
2. 从“选项”**(Options)** 下拉列表中选择适当的选项：
   - **统计信息 (Statistics)**。将生成类似如下的页面：

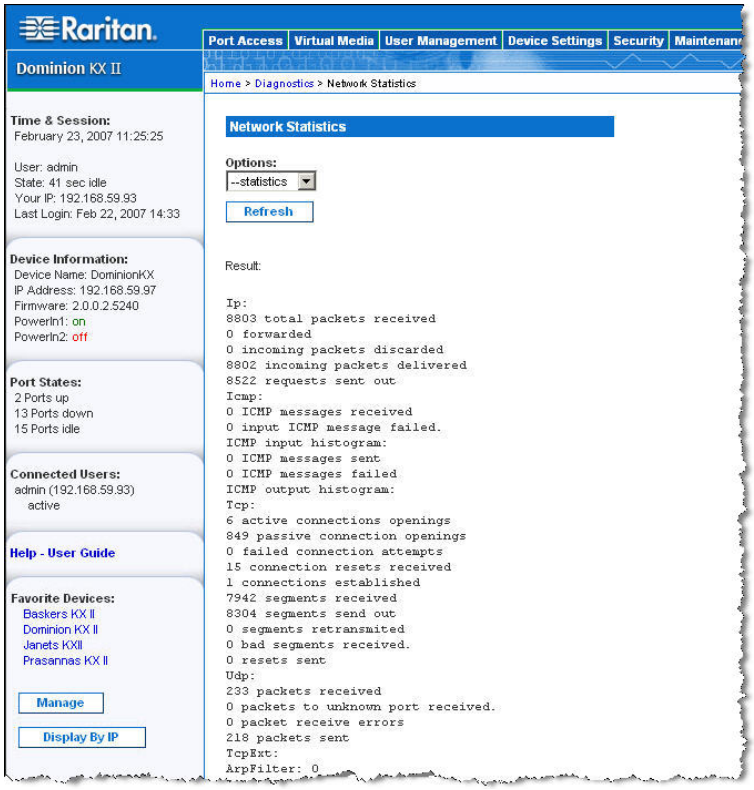


图 90：网络统计信息（统计信息）

   - **接口 (Interfaces)**。将生成类似如下的页面：

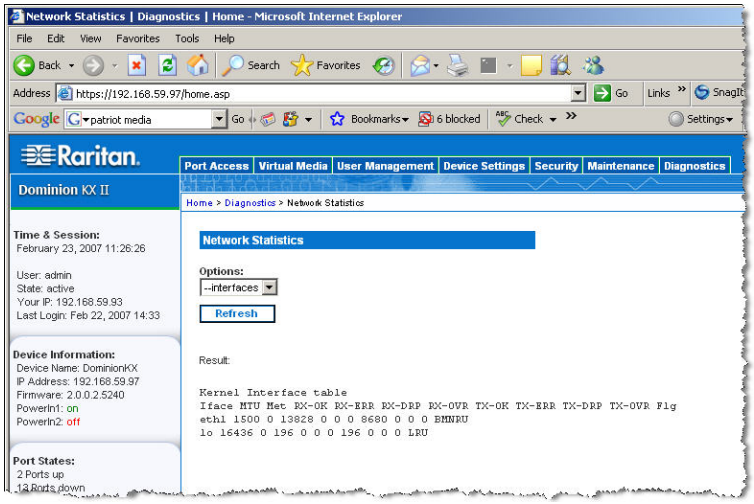


图 91：网络统计信息（接口）

- **路由 (Route)**。将生成类似如下的页面：

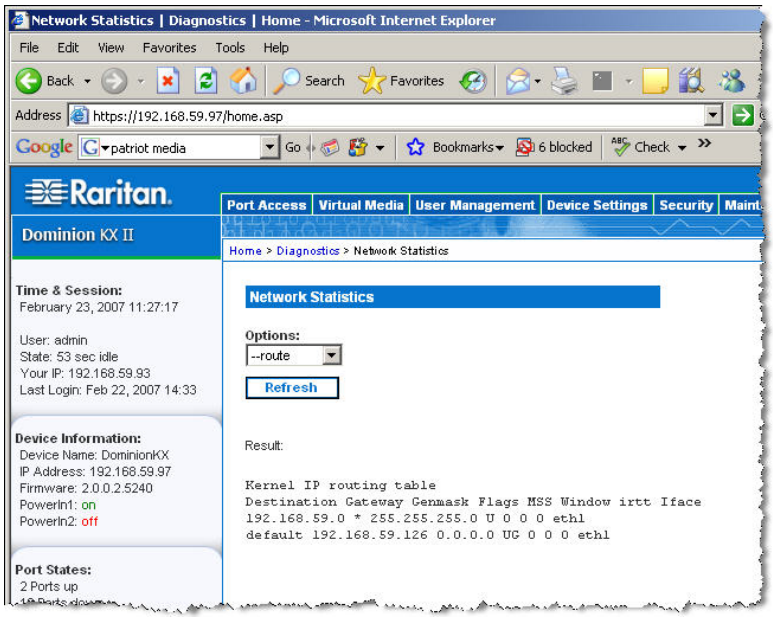


图 92：网络统计信息（路由）

3. 单击“刷新”**(Refresh)** 按钮。

“结果”**(Result)** 字段中将显示相关信息。

“Ping 主机”页

Ping 是一种网络工具，用于测试是否可以通过 IP 网络与特定主机或 IP 地址联系。使用“Ping 主机”(Ping Host) 页可以确定是否可以访问某个目标服务器或另一个 Dominion KX II 设备。

要 ping 主机，请执行以下操作：

1. 选择“诊断”**(Diagnostics) >** “**Ping** 主机”**(Ping Host)**。将打开“**Ping** 主机”(Ping Host) 页。

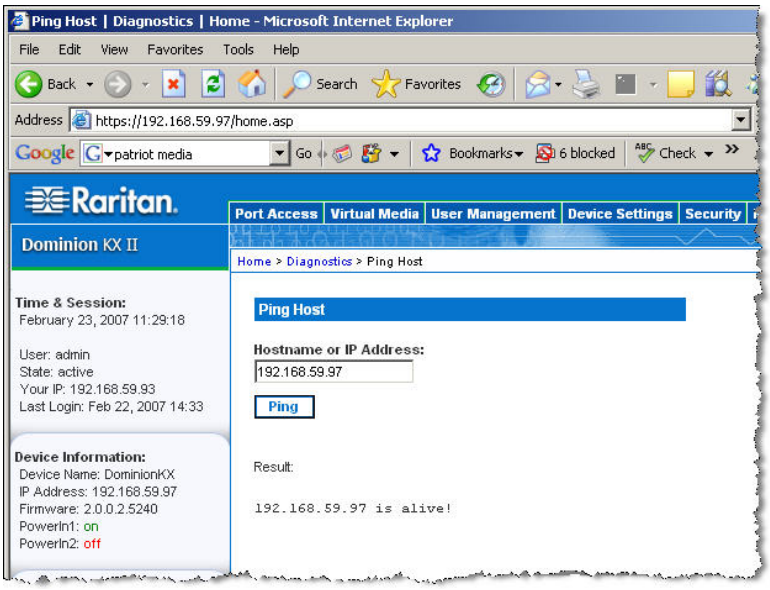


图 93：Ping 主机

2. 在“主机名”(Hostname) 或“**IP** 地址”**(IP Address)** 字段中键入主机名或 IP 地址。
3. 单击“**Ping**”。Ping 的结果显示在“结果”**(Result)** 字段中。

“跟踪到主机的路由”页

跟踪路由是一种网络工具，用于确定到达所提供的主机名或 IP 地址所经过的整个路由。

要跟踪到主机的路由，请执行以下操作：

1. 选择“诊断”**(Diagnostics)** >“跟踪到主机的路由”**(Trace Route to Host)**。将打开“跟踪到主机的路由”(Trace Route to Host) 页：

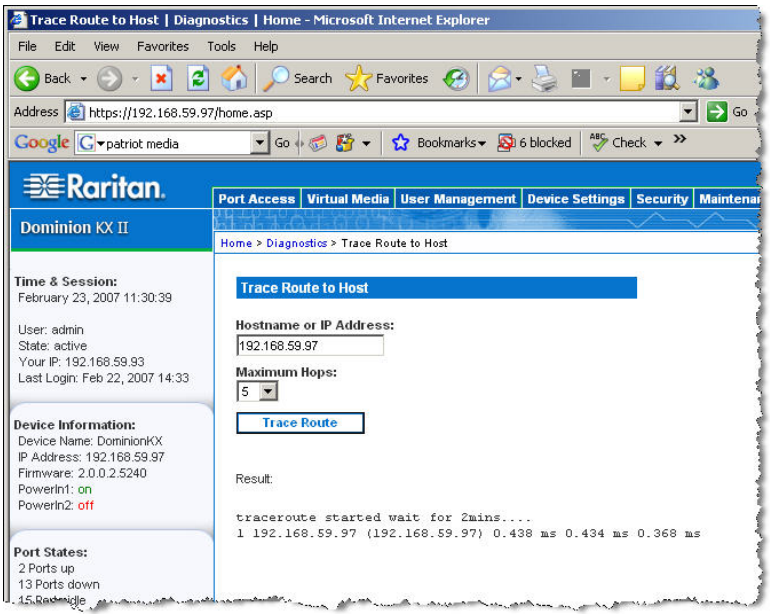


图 94：跟踪到主机的路由

2. 在“主机名”**(Hostname)** 或“**IP** 地址”**(IP Address)** 字段中键入主机名或 IP 地址。
3. 从下拉列表中选择“最大跃点数”**(Maximum Hops)**（5 或 10）。
4. 单击“跟踪路由”**(Trace Route)** 按钮。针对给定的主机名或 IP 地址，并根据最大跃点数来执行跟踪路由命令。跟踪路由的输出显示在“结果”**(Result)** 字段中。

KX 诊断

***注意：**本页供 Raritan 现场工程师使用，或者在 Raritan 技术支持人员的指导下使用。*

“KX 诊断”(KX Diagnostics) 可以将 Dominion KX II 中的诊断信息下载到客户机。在本页上可以执行以下三种功能：

- **命令行接口**。启用或禁用命令行接口功能。通过此功能，Raritan 技术支持工程师可以打开一个标准的 SSH 客户机，连接到相应设备，并远程执行诊断功能。
- **诊断脚本**。在关键错误调试会话过程中执行由 **Raritan** 技术支持部门提供的特殊脚本。此脚本上载到设备并加以执行。一旦执行了该脚本，您就可以通过“保存到文件”**(Save to File)** 按钮下载诊断消息。
- **KX 诊断日志**。将 **KX II** 设备中的诊断消息快照下载到客户机。该加密文件随后被发送到 **Raritan** 技术支持部门；只有 **Raritan** 可以对该文件进行解密。

***注意：**只有具有管理权限的用户才能访问本页。*

要运行 KX II 系统诊断，请执行以下操作：

1. 选择“诊断”**(Diagnostics) >**“**KX** 诊断”**(KX Diagnostics)**。将打开“**KX** 诊断”(KX Diagnostics) 页。

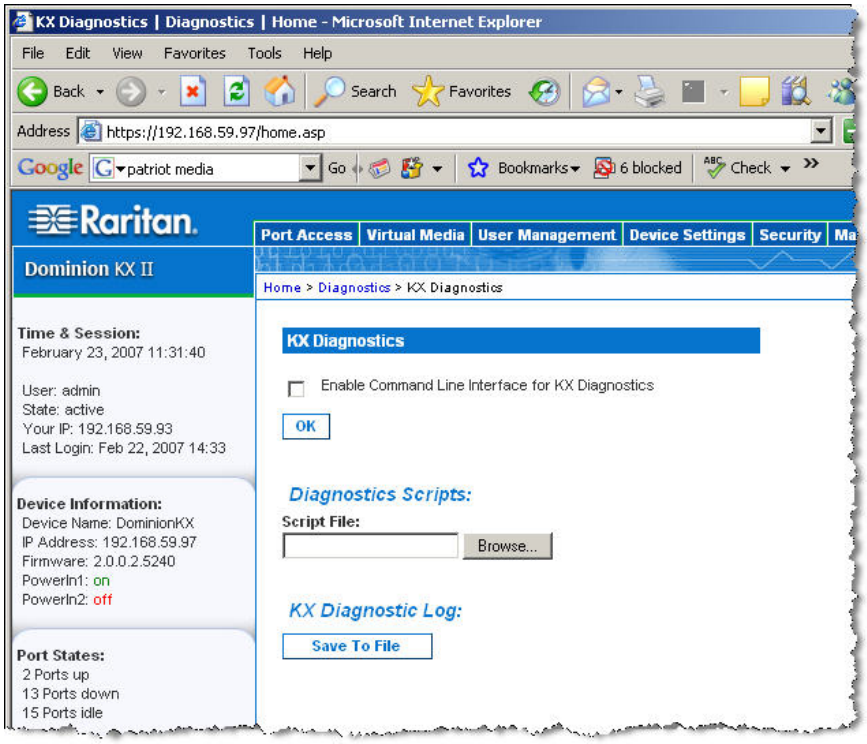


图 95：KX 诊断

2. 要启用命令行接口以供 **Raritan** 技术支持人员使用，请执行以下操作：

***注意：**要使用该功能，需要 UDP 端口 21。*

a. 单击“为 KX 诊断启用命令行接口”(Enable Command Line Interface for KX Diagnostics) 复选框。

b. 单击“确定”**(OK)**。

c. UDP 端口 21 必须打开，并且可供 Raritan 技术支持人员使用。

d. Raritan 技术支持部门还需要知道 KX II 的管理密码。

e. 一旦 Raritan 技术支持人员完成了测试，请将 UDP 端口 21 返回到其初始状态。

3. 要执行由 **Raritan** 技术支持部门通过电子邮件发送给您的诊断脚本文件，请执行以下操作：

a. 检索由 Raritan 提供的诊断文件并解压缩 (如果需要)。

b. 使用“浏览”**(Browse)** 按钮。将打开“选择文件”**(Choose file)** 对话框。

c. 定位到该诊断文件并选择它。

d. 单击“打开”**(Open)**。此文件将在“脚本文件”**(Script File)** 字段中显示：

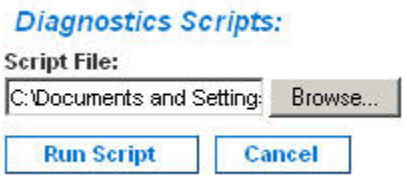


图 96：诊断脚本

e. 单击“运行脚本”**(Run Script)**。

f. 按步骤 4 所述将该文件发送到 Raritan 技术支持部门。

4. 要创建诊断文件以发送给 Raritan 技术支持部门，请执行以下操作：

a. 单击“保存到文件”**(Save to File)** 按钮。将打开“文件下载”(File Download) 对话框：

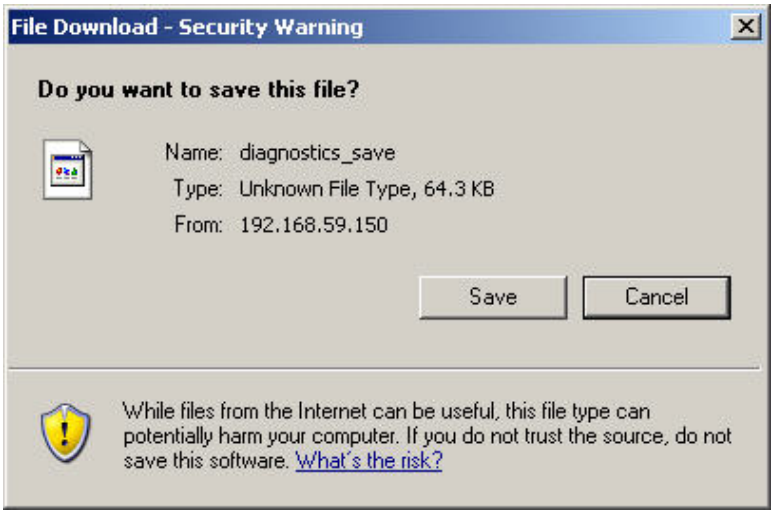


图 97：文件下载

b. 单击“保存”**(Save)**。将打开“另存为”(Save As) 对话框。

c. 定位到所需的目标并单击“保存”**(Save)**。

d. 根据 Raritan 技术支持人员的指示通过电子邮件发送该文件。

第 13 章：KX II Local Console

KX II Local Console

Dominion KX II 通过其本地端口提供机架访问和管理，使用其基于浏览器的图形用户界面，可以在服务器之间快速、方便地切换。Dominion KX II Local Console 提供了与您所连接的服务器的直接模拟连接；其性能就像您直接连接到服务器的键盘、鼠标和视频端口时的性能一样。KX II Local Console 与 Dominion KX II Remote Console 提供相同的管理功能。

Dominion KX II Local Console 支持以下语言的键盘：美国英语、英国英语、德文、法文、日文、韩文、简体中文和繁体中文。

注意：*用于中文、日语和朝鲜语的键盘仅供显示；目前，KX II Local Console 功能不支持本地语言输入。*

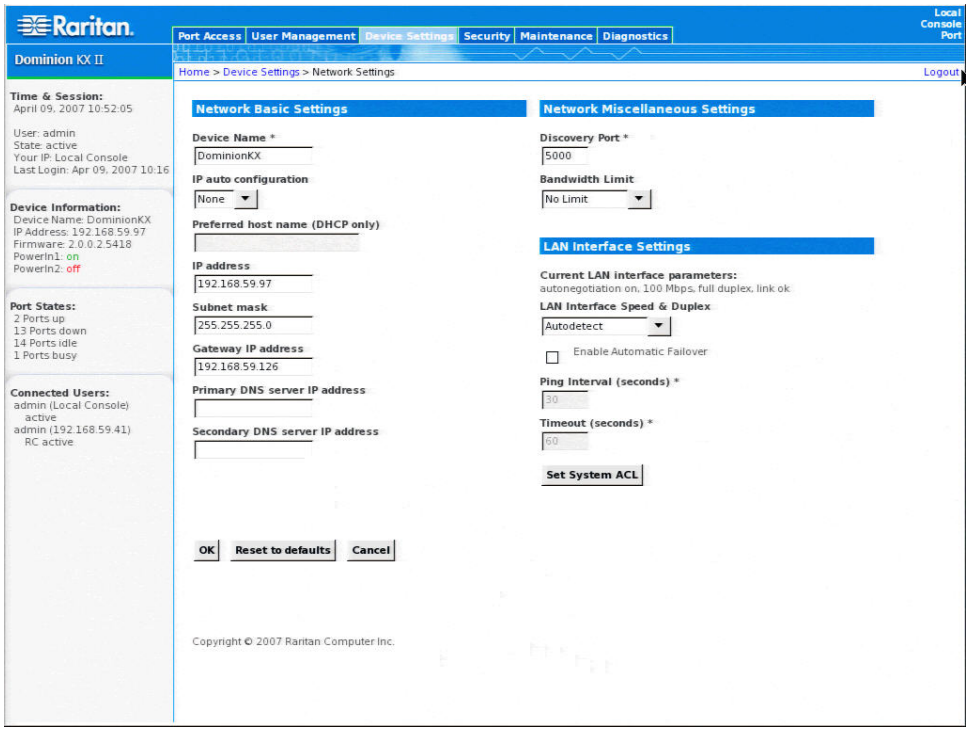


图 98：Dominion KX II Local Console

实际连接

可以在 Dominion KX II 的后面板上找到本地端口的实际连接：



图 99：Dominion KX II 上的本地面板

显示器：将标准多同步 VGA 显示器连接到 HD15（插孔）视频端口。

键盘：将一个标准 PS/2 键盘连接到微型 DIN6（插孔）键盘端口，*或者* 将一个标准 USB 键盘连接到 USB A（插孔）端口之一。

鼠标：将一个标准 PS/2 鼠标连接到微型 DIN6（插孔）鼠标端口，*或者* 将一个标准 USB 鼠标连接到 USB A（插孔）端口之一。

“复位”按钮

Dominion KX II 设备的背面有一个“复位”(Reset) 按钮。它凹入面板中，以避免不小心按下（需要使用尖头物按下该按钮)。



图 100：“复位”按钮（设备背面）

按下复位按钮时执行的操作在图形用户界面中定义。有关更多信息，请参阅安全设置、加密和共享。

***注意：**建议在执行出厂复位之前保存审计日志。执行出厂复位时，将删除审计日志，且审计日志中不会记录复位事件。有关保存审计日志的更多信息，请参阅审计日志。*

要复位设备，请执行以下操作：

1. 关闭 Dominion KX II 设备的电源。
2. 使用尖头物按下复位按钮。
3. ***继续按住复位按钮，***重新打开 Dominion KX II 设备的电源。
4. 按住复位按钮约 5-10 秒钟。一旦设备复位完毕，将响两下短促的嘟声，表示复位完成。

启动 KX II Local Console

同时连接的用户

Dominion KX II Local Console 提供对所连接的目标服务器的独立访问途径。使用 Local Console 不会阻止其他用户通过网络同时连接。即使当远程用户连接到 Dominion KX II 时，您仍可以通过 Local Console 从机架同时访问您的服务器。

安全和认证

要使用 Dominion KX II Local Console，必须先使用有效的用户名和密码进行认证。Dominion KX II 提供了完全集成的认证和安全架构，无论您通过网络还是本地端口访问都适用。在任何一种情况下，Dominion KX II 都只允许用户访问其具有访问权限的服务器（有关指定服务器访问和安全设置的其它信息，请参阅用户管理）。

如果已针对外部认证服务（LDAP、RADIUS、Active Directory 或 Raritan 的 CC-SG）配置了您的 Dominion KX II，还会针对外部认证服务对 Local Console 的认证尝试进行认证。

***注意：**您也可以指定对 Local Console 访问不进行认证；仅在安全的环境中建议使用此选项。*

要使用 KX II Local Console，请执行以下操作：

1. 需要将键盘、鼠标和视频显示连接到 Dominion KX II 设备背面的本地端口上。有关本地端口连接的更多信息，请参阅实际连接。
2. 启动 Dominion KX II 设备，这将显示 KX II Local Console 界面。

KX II Local Console 界面

KX II Local Console 界面与 KX II Remote Console 界面几乎完全相同。本用户手册中介绍了二者的不同之处。有关其它信息，请参阅用户界面、KX II 控制台和 KX II 控制台菜单树。

可用分辨率

KX II Local Console 提供下列分辨率以支持各种显示器：

- 800x600
- 1024x768
- 1280x1024

其中每一种分辨率都支持 60 和 75 赫兹的刷新率。

访问目标服务器

服务器显示

登录 KX II Local Console 之后，将打开“端口访问”(Port Access) 页。该页中列出了所有 Dominion KX II 端口、连接的目标服务器及其状态和可用性。

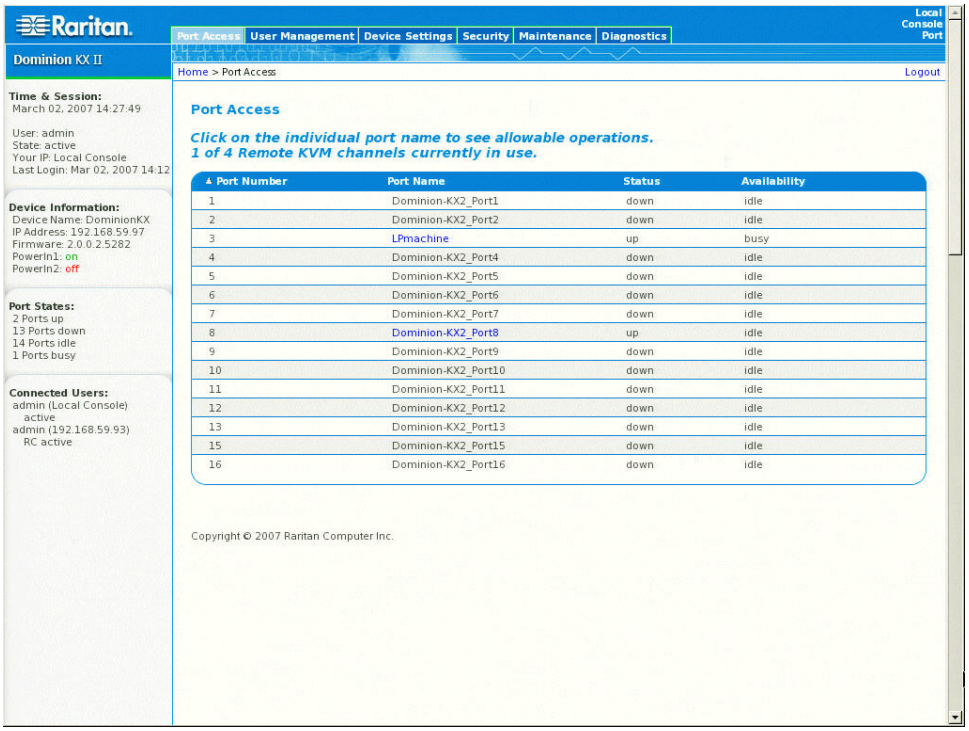


图 101：Local Console 端口访问

目标服务器最初按端口号排序；您可以更改显示方式，按以下任一列进行排序。

- **端口号 (Port Number)**。从 1 开始编号，直到 Dominion KX II 设备可用的端口总数。请注意，与电源板相连的端口将不会 在这里列出，这就导致端口号序列中缺少一些编号。
- **端口名称 (Port Name)**。Dominion KX II 端口的名称；最初设置为 Dominion-KX2-Port#，但您可以将此名称更改为某个更具说明性的名称。单击“端口名称”(Port Name) 链接时，将打开“操作菜单”(Action Menu)。有关可用的菜单选项的更多信息，请参阅端口操作菜单 (Port Action Menu)。
- **状态 (Status)**。“状态”(Status) 为“打开”(up) 或“关闭”(down)。
- **可用性 (Availability)**。有效值包括“空闲”(Idle)、“已连接”(Connected)、“忙碌”(Busy) 或“不可用”(Unavailable)。

要更改排序顺序，请执行以下操作：

单击要作为排序依据的列标题。目标服务器列表将按该列进行排序。

热键

由于 Dominion KX II Local Console 的界面完全被您所访问的目标服务器的界面替代，因此采用了热键，以便您可以在这些界面之间切换。

正在查看目标服务器时，可以使用本地端口热键快速访问 KX II Local Console 用户界面。默认热键是快速连按两下 **Scroll Lock** 键，但您可以将（“本地端口设置”(Local Port Settings) 页中的）任意组合键指定为热键。有关更多信息，请参阅本地端口设置。

访问目标服务器

要访问目标服务器，请执行以下操作：

1. 单击要访问的目标的“端口名称”**(Port Name)**。将显示“端口操作”**(Port Action)** 菜单。
2. 从端口操作菜单 (Port Action Menu) 中选择“连接”(Connect)。视频显示将切换到目标服务器界面。

返回 KX II Local Console 界面

重要事项：KX II Local Console 的默认热键是快速连按两下 Scroll Lock 键。可以在本地端口设置 (Local Port Settings) 页中更改此组合键。

要从目标服务器返回 KX II Local Console，请执行以下操作：

快速按两下热键（默认热键为 **Scroll Lock**）。视频显示将从目标服务器界面切换到 Dominion KX II Local Console 界面。

本地端口管理

Dominion KX II 可以通过 KX II Local Console 或 KX II Remote Console 进行管理。请注意，KX II Local Console 还提供对以下管理功能的访问：

- 本地端口设置
- 出厂复位 (Factory Reset)

***注意：**只有具有管理权限的用户才能访问这些功能。*

本地端口设置（仅限 KX II Local Console）

从“本地端口设置”(Local Port Settings) 页可以自定义 KX II Local Console 的许多设置，包括键盘、本地端口热键、视频切换延迟、节电模式、本地用户界面分辨率设置和本地用户认证。

***注意：**此功能仅在 Dominion KX II Local Console 上可用。*

要配置本地端口设置，请执行以下操作：

1. 选择“设备设置”**(Device Settings) >**“本地端口设置”**(Local Port Settings)**。将打开“本地端口设置”(Local Port Settings) 页。

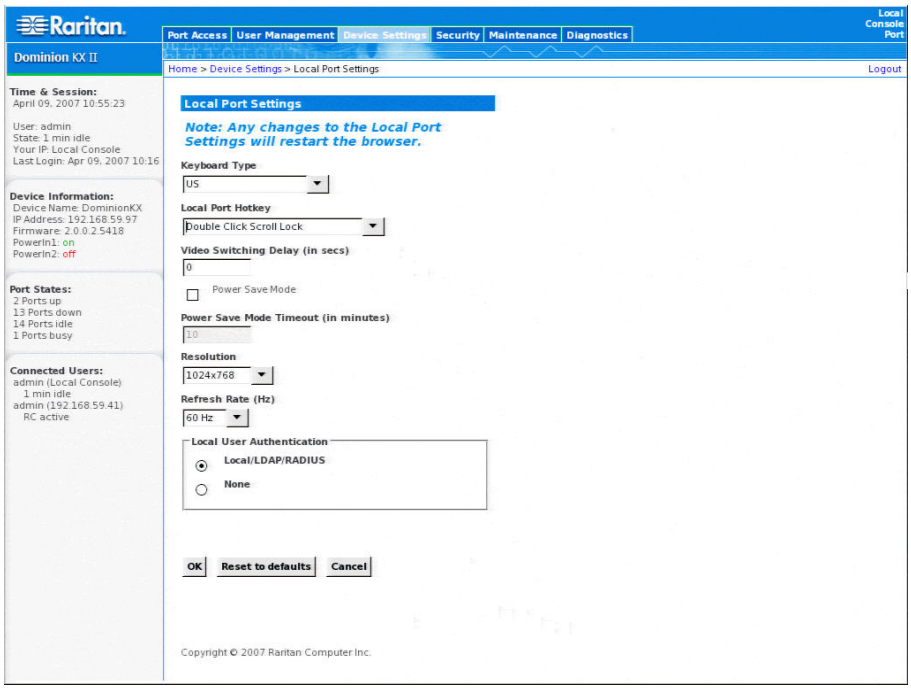


图 102：本地端口设置

2. 从下拉列表选项中选择适当的“键盘类型”(Keyboard Type)。
   - 美国英语 (US)
   - 美国英语/国际 (US/International)
   - 英国英语 (UK)
   - 法文 (French)
   - 德文 (German)
   - 日本工业标准 (JIS, Japanese Industry Standard)
   - 简体中文 (Simplified Chinese)
   - 繁体中文 (Traditional Chinese)
   - 韩文 (Dubeolsik Hangul (Korean))
3. 选择“本地端口热键”**(Local Port Hotkey)**。本地端口热键用于在查看目标服务器界面时返回到 KX II Local Console 界面。默认热键是“双击 **Scroll Lock**”**(Double Click Scroll Lock)**，但您可以从下拉列表中选择任意组合键：

热键：	执行此操作：
双击 Scroll Lock (Double Click Scroll Lock)	快速按两下 **Scroll Lock** 键
双击 Num Lock (Double Click Num Lock)	快速按两下 **Num Lock** 键
双击 Caps Lock (Double Click Caps Lock)	快速按两下 **Caps Lock** 键
双击左 Alt 键 (Double Click Left Alt key)	快速按两下**左 Alt** 键
双击左 Shift 键 (Double Click Left Shift key)	快速按两下**左 Shift** 键
双击左 Ctrl 键 (Double Click Left Ctrl key)	快速按两下**左 Ctrl** 键

4. 根据需要，将“视频切换延迟”**(Video Switching Delay)** 设置为 0 – 5 秒。通常使用 0 秒，除非需要更长时间（某些显示器需要用更长的时间来切换视频）。
5. 如果要使用节电功能，请执行以下操作：
   a. 选中“节电模式”(Power Save Mode) 复选框。
   b. 设置一段时间（以分钟为单位），超过该段时间将启动节电模式。
6. 从 **KX II Local Console** 的下拉列表中选择“分辨率”**(Resolution)**：
   - 800x600
   - 1024x768
   - 1280x1024
7. 从下拉列表中选择“刷新率”**(Refresh Rate)**：
   - 60 赫兹
   - 75 赫兹

8. 选择“本地用户认证”**(Local User Authentication)** 的类型：
   - **本地/LDAP/RADIUS (Local/LDAP/RADIUS)**。这是建议的选项；有关认证的更多信息，请参阅远程认证和认证与授权。
   - **无（None）**。对 Local Console 访问不进行认证。*仅在安全的环境中* 建议使用此选项。
9. 单击“确定”**(OK)**。

要关闭此页且不保存任何更改，请执行以下操作：

单击“取消”**(Cancel)**。

要复位为默认值，请执行以下操作：

单击“复位为默认值”**(Reset to Defaults)**。

出厂复位（仅限 KX II Local Console）

***注意：**此功能仅在 Dominion KX II Local Console 上可用。*

Dominion KX II 从 Local Console 用户界面提供了若干类型的复位模式。

***注意：**建议在执行出厂复位之前保存审计日志。执行出厂复位时，将删除审计日志，且审计日志中不会记录复位事件。有关保存审计日志的更多信息，请参阅审计日志。*

要执行出厂复位，请执行以下操作：

1. 选择“维护”**(Maintenance)** >“出厂复位”**(Factory Reset)**。将打开“出厂复位”(Factory Reset) 页：

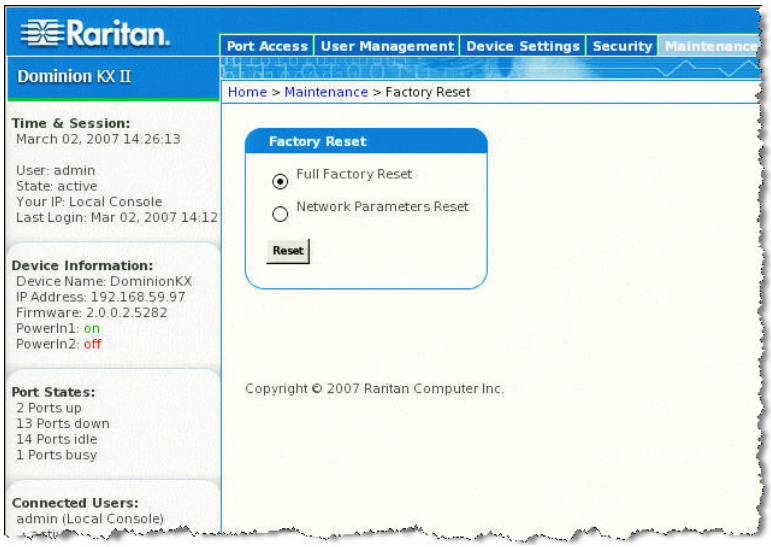


图 103：出厂复位（仅限 Local Console）

2. 选择适当的复位选项。
   - **完全出厂复位 (Full Factory Reset)**：删除整个配置，将设备完全复位到出厂默认设置。请注意，与 CommandCenter 的任何管理关联将中断。鉴于这种复位模式的彻底性，您将得到确认出厂复位的提示。
   - **网络参数复位 (Network Parameter Reset)**：（从“设备设置”(Device Settings) > “网络设置”(Network Settings)）将设备的网络参数复位为默认值：

IP 自动配置 (IP auto configuration)
IP 地址 (IP Address)
子网掩码 (Subnet Mask)
网关 IP 地址 (Gateway IP address)
主 DNS 服务器 IP 地址 (Primary DNS server IP address)
备用 DNS 服务器 IP 地址 (Secondary DNS server IP address)
搜索端口 (Discovery Port)
带宽限制 (Bandwidth Limit)
LAN 接口速度和双工 (LAN Interface Speed & Duplex)
启用自动故障切换 (Enable Automatic Failover)
Ping 时间间隔 (秒) (Ping Interval (seconds))
超时 (秒) (Timeout (Seconds))

将提示您确认此操作，因为所有网络设置将永久丢失。

3. 单击“复位”**(Reset)** 继续操作。将提示您确认执行出厂复位。
4. 单击“确定复位”**(Really Reset)** 按钮继续。完成后，Dominion KX II 设备将自动重新启动。

第 14 章：取消对 CC 的管理

概要

如果某个 Dominion KX II 设备处于 CommandCenter Secure Gateway 的控制下，那么，当您尝试使用 Dominion KX II 远程控制台直接访问该设备时，在您输入有效的用户名和密码之后，将显示以下消息：



图 104：“设备由 CC-SG 管理”消息

从 CC-SG 管理中删除 Dominion KX II

除非解除 CC-SG 对 Dominion KX II 的控制，否则您将无法直接访问该设备。但是，如果 KX II 从 CommandCenter 收不到检测信号消息（例如，CommandCenter 不在网络中），则您可以解除 CC-SG 对 KX II 的控制，以访问该设备。这是使用“取消 CC 的管理”(CC Unmanage) 功能完成的。

***注意：**要使用该功能，需要维护权限。*

如果收不到检测信号消息，则尝试直接访问设备时将显示以下消息：

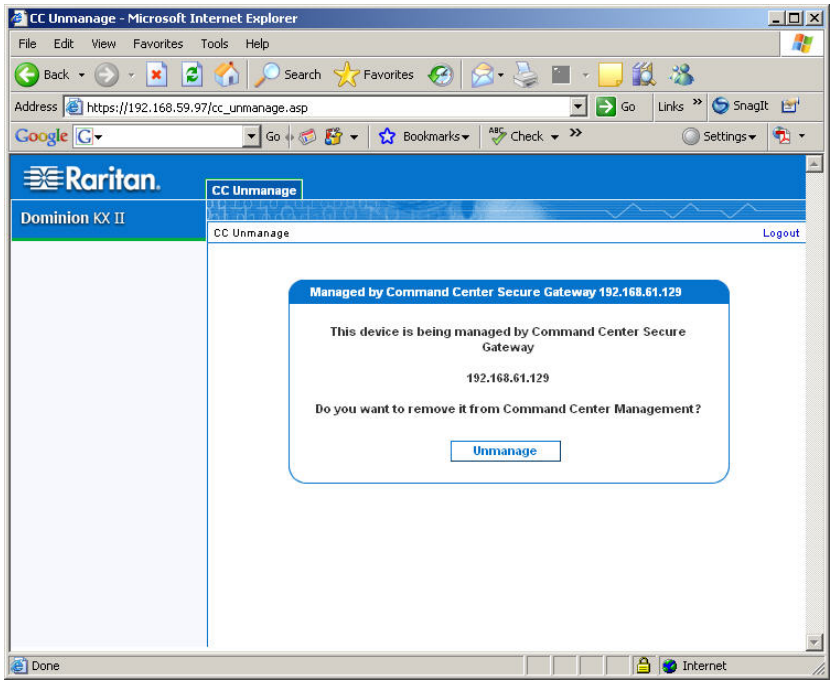


图 105：从 CC-SG 管理中删除

要从 CC-SG 管理中删除设备（以使用“取消 CC 的管理”(CC Unmanage)），请执行以下操作：

1. 单击“取消管理”**(Unmanage)** 按钮。系统将提示您确认该操作：



图 106：确认取消 CC 的管理

2. 单击“确实要取消管理”**(Really Unmanage)** 按钮。将显示一则消息，确认该设备已不处于 CC 管理之下：

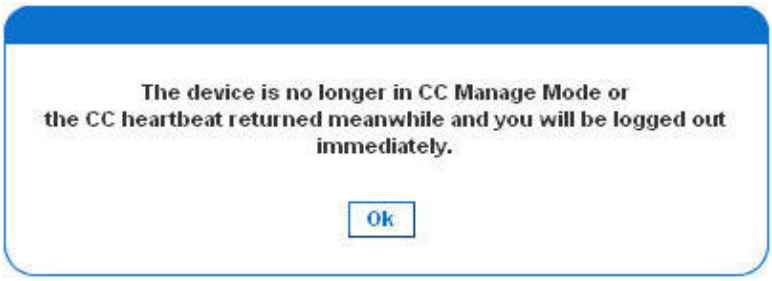


图 107：设备已从 CC 管理中取消

3. 单击“确定”**(OK)**。将打开“端口访问”(Port Access) 页。

附录 A：规格

环境要求

操作时	
温度	0℃- 40℃ (32℉-104℉)
湿度	20% - 85% RH
海拔高度	无
振动	5-55-5 赫兹，0.38 毫米，每个周期 1 分钟； 每个轴（X、Y、Z）30 分钟
电击	无
非操作时	
温度	0℃- 50℃ (32℉-122℉)
湿度	10% - 90% RH
海拔高度	无
振动	5-55-5 赫兹，0.38 毫米，每个周期 1 分钟； 每个轴（X、Y、Z）30 分钟
电击	无

物理规格

部件号	DKX2-116	DKX2-132	DKX2-216	DKX2-232	DKX2-416	DKX2-432
明细说明	具有本地端口、允许 1 个用户进行网络访问的 16 端口 Dominion KX II；虚拟媒体，双电源	具有本地端口、允许 1 个用户进行网络访问的 32 端口 Dominion KX II；虚拟媒体，双电源	具有本地端口、允许 2 个用户进行网络访问的 16 端口 Dominion KX II；虚拟媒体，双电源	具有本地端口、允许 2 个用户进行网络访问的 32 端口 Dominion KX II；虚拟媒体，双电源	具有本地端口、允许 4 个用户进行网络访问的 16 端口 Dominion KX II；虚拟媒体，双电源	具有本地端口、允许 4 个用户进行网络访问的 32 端口 Dominion KX II；虚拟媒体，双电源
重量	8.95 磅； 3.9 公斤	9.0 磅； 4.1 公斤	8.59 磅； 3.9 公斤	9.0 磅； 4.1 公斤	9.04 磅； 4.1 公斤	9.48 磅； 4.3 公斤
产品尺寸（宽 x 深 x 高）	1.75 英寸 x 17.32 英寸 x 11.4 英寸 44 毫米 x 439 毫米 x 290 毫米	1.75 英寸 x 17.32 英寸 x 11.4 英寸 44 毫米 x 439 毫米 x 290 毫米	1.75 英寸 x 17.32 英寸 x 11.4 英寸 44 毫米 x 439 毫米 x 290 毫米	1.75 英寸 x 17.32 英寸 x 11.4 英寸 44 毫米 x 439 毫米 x 290 毫米	1.75 英寸 x 17.32 英寸 x 11.4 英寸 44 毫米 x 439 毫米 x 290 毫米	1.75 英寸 x 17.32 英寸 x 11.4 英寸 44 毫米 x 439 毫米 x 290 毫米
装运重量	14.85 磅； 6.7 公斤	14.9 磅； 6.8 公斤	14.49 磅； 6.6 公斤	14.9 磅； 6.8 公斤	14.94 磅； 6.8 公斤	15.38 磅； 7.0 公斤
装运尺寸（宽 x 深 x 高）	22 英寸 x 16.6 英寸 x 6.5 英寸 559 毫米 x 422 毫米 x 165 毫米	22 英寸 x 16.6 英寸 x 6.5 英寸 559 毫米 x 422 毫米 x 165 毫米	22 英寸 x 16.6 英寸 x 6.5 英寸 559 毫米 x 422 毫米 x 165 毫米	22 英寸 x 16.6 英寸 x 6.5 英寸 559 毫米 x 422 毫米 x 165 毫米	22 英寸 x 16.6 英寸 x 6.5 英寸 559 毫米 x 422 毫米 x 165 毫米	22 英寸 x 16.6 英寸 x 6.5 英寸 559 毫米 x 422 毫米 x 165 毫米
UPC 代码	785813624055	785813624079	785813624086	785813625021	785813625359	785813625380
电源	双电源 100/240 伏 50/60 赫兹 0.6 安 25.4 瓦	双电源 100/240 伏 50/60 赫兹 0.6 安 26 瓦	双电源 100/240 伏 50/60 赫兹 0.6 安 26.3 瓦	双电源 100/240 伏 50/60 赫兹 0.6 安 27 瓦	双电源 100/240 伏 50/60 赫兹 1 安 62 瓦	双电源 100/240 伏 50/60 赫兹 1 安 64 瓦

电气规格

参数		值
输入		
	额定频率	50/60 赫兹
	额定电压范围	100/240 V 伏交流电
	最大交流电流 RMS	最大 0.6 安
	交流电工作范围	100 至 240 伏交流电 (+-10%)，47 至 63 赫兹
输出		
	+5 伏直流，+12 伏直流电	无
	-5 伏直流，-12 伏直流电	无
最大直流电源输出		无
	最大交流电耗电量	无
	最大散热	无
额定伏安		无

计算机接口模块 (CIM)

部件号	D2CIM-VUSB	DCIM-PS2	DCIM-USB	DCIM-SUSB
明细说明	Dominion KX II 计算机接口模块 [具有虚拟媒体的 USB 端口]	Dominion KX I & II 计算机接口模块 [PS/2 端口]	Dominion KX I & II 计算机接口模块 [USB 端口]	Dominion KX I & II 计算机接口模块 [用于 Sun 的 USB 端口]
产品重量	0.2 磅	0.2 磅	0.2 磅	0.2 磅
产品尺寸（宽 x 深 x 高）	1.3 英寸 x 3.0 英寸 x 0.6 英寸	1.3 英寸 x 3.0 英寸 x 0.6 英寸	1.3 英寸 x 3.0 英寸 x 0.6 英寸	1.3 英寸 x 3.0 英寸 x 0.6 英寸
装运重量	0.2 磅	0.2 磅	0.2 磅	0.2 磅
装运尺寸（宽 x 深 x 高）	7.2 英寸 x 9 英寸 x 0.6 英寸	7.2 英寸 x 9 英寸 x 0.6 英寸	7.2 英寸 x 9 英寸 x 0.6 英寸	7.2 英寸 x 9 英寸 x 0.6 英寸
UPC 代码	785813332004	785813338532	785813338518	785813338556

部件号	DCIM-SUN	D2CIM-PWR	D2CIM-VUSB-32PAC	D2CIM-VUSB - 64PAC
明细说明	Dominion KX I & II 计算机接口模块 [Sun 端口，HD15 视频]	用于远程电源板的 Dominion KX II 计算机接口模块	散装 32 D2CIM-VUSB	散装 64 D2CIM-VUSB
产品重量	0.2 磅	0.2 磅	6.4 磅	12.8 磅
产品尺寸（宽 x 深 x 高）	1.3 英寸 x 3.0 英寸 x 0.6 英寸	1.3 英寸 x 3.0 英寸 x 0.6 英寸	（1.3 英寸 x 3.0 英寸 x 0.6 英寸）*32	（1.3 英寸 x 3.0 英寸 x 0.6 英寸）*64
装运重量	0.2 磅	0.2 磅	8.01 磅	18.13 磅
装运尺寸（宽 x 深 x 高）	7.2 英寸 x 9 英寸 x 0.6 英寸	7.2 英寸 x 9 英寸 x 0.6 英寸	21.65 英寸 x 12.20 英寸 x 4.33 英寸	22.64 英寸 x9.45 英寸 x 12.99 英寸
UPC 代码	785813338549	785813332011	785813332028	785813332035

远程连接

网络： 10BASE-T、100BASE-T 和 1000BASE-T（千兆）以太网
协议： TCP/IP、UDP、SNTP、HTTP、HTTPS、RADIUS 和 LDAP

KVM 属性

键盘：PS/2 或 USB
鼠标：PS/2 或 USB
视频：VGA

使用的 TCP 和 UDP 端口

- **HTTP，端口 80** – Dominion KX II 通过 HTTP（端口 80）接收的所有请求都自动转发到 HTTPS，以保证完全的安全性。为方便用户，Dominion KX II 能够响应端口 80，以便用户无需在 URL 字段中显式键入“https://”，但同时仍保持完全的安全性。
- **HTTPS，端口 443** – 此端口仅有一个用途：将 Dominion KX II 可通过 Web 访问的客户机（KX II 控制台，MPC）发送给用户。此端口上不发生其它通信。如果您要使用 Dominion KX II Web 访问功能，并且想要改为使用 CD-ROM 上提供的已安装的客户机软件，可以通过您的防火墙阻止对端口 443 的访问，此时 Dominion KX II 仍然可以工作。
- **Dominion KX II（Raritan 采用 IP 的 KVM）协议，可配置端口 5000** – 除了在上述端口外，所有与 Dominion KX II 进行的通信都可以通过一个可配置的 TCP 端口进行。默认情况下，它设置为端口 5000，但您可以将它配置为使用您选择的任何 TCP 端口（端口 80 和 443 除外）。有关如何配置该设置的详细信息，请参阅网络设置。
- **可配置的 UDP 端口 123 上的 SNTP（时间服务器）（可选）** – Dominion KX II 提供此可选功能，将其内部时钟与中央时间服务器同步。此功能需要使用 UDP 端口 123（SNTP 的标准端口），但也可以配置为使用您指定的任何端口。
- **可配置端口 389 和 636 上的 LDAP（可选）** – 如果 Dominion KX II 配置为通过 LDAP 协议对用户登录进行远程认证，将使用端口 389 和 636，但也可以将系统配置为使用您指定的任何端口。
- **可配置端口 1812 上的 RADIUS（可选）** – 如果 Dominion KX II 配置为通过 RADIUS 协议对用户登录进行远程认证，将使用端口 1812 或 1813，但也可以将系统配置为使用您指定的任何端口。
- **在可配置端口 1813 上的 RADIUS 计费** – 如果 Dominion KX II 配置为通过 RADIUS 协议对用户登录进行远程认证，并且采用 RADIUS 计费来记录事件，将使用端口 1813 或您指定的其它端口来传送日志通知。
- **可配置的 UDP 端口 514 上的 SYSLOG** – 如果 Dominion KX II 配置为向 Syslog 服务器发送消息，则使用指定端口进行通信 – 使用 UDP 端口 514。
- **SNMP 默认 UDP 端口（可选）** – 端口 161 用于入站/出站读/写 SNMP 访问，端口 162 用于 SNMP 陷阱的出站交通。
- **UDP 端口 21** – 端口 21 用于 Dominion KX II 命令行接口（当您与 Raritan 技术支持人员一起工作时）。

目标服务器连接距离和视频分辨率

支持的最大距离取决于许多因素，包括 Cat5 线缆的类型/质量、服务器类型和厂商、视频驱动程序和显示器、环境条件以及用户期望度。下表总结了各种视频分辨率和刷新率的最大目标服务器距离：

视频分辨率	刷新率	最大距离
1600x1200	60	50 英尺（15 米）
1280x1024	60	100 英尺（30 米）
1024x768	60	150 英尺（45 米）

使用 Paragon CIM 不会增加 Dominion KX II 和目标服务器之间的距离。

鉴于服务器厂商和类型、操作系统版本、视频驱动程序等等的多样性，以及视频质量的主观性，Raritan 无法保证在所有环境中所有距离情况下的性能。

有关 Dominion KX II 支持的视频分辨率，请参阅支持的视频分辨率。

附录 B：更新 LDAP 架构

注意：本章中的过程应仅供有经验的用户尝试使用。

返回用户组信息

一旦认证完成，可以参考本章中的信息以返回用户组信息（需要相应的授权）。

从 LDAP

当 LDAP 认证成功之后，Dominion KX II 将根据给定用户所在组的权限来确定该用户的权限。您的远程 LDAP 服务器可以通过返回如有如下名称的属性来提供这些用户组名称：

`rciusergroup` 属性类型：字符串

这可能要求您的 LDAP 服务器上有架构扩展。请咨询您的认证服务器管理员以启用该属性。

此外，还可以使用标准 LDAP `memberOf`。

从 Microsoft Active Directory

注意：仅供有经验的 Active Directory 管理员尝试使用。

从用于 Windows 2000 Server 的 Microsoft Active Directory 返回用户组信息需要更新 LDAP 架构。有关详细信息，请参阅相关 Microsoft 文档。

1. 安装用于 **Active Directory** 的架构插件 – 有关相应的说明，请参阅 **Microsoft Active Directory** 文档。
2. 运行 **Active Directory** 控制台并选择“**Active Directory** 架构”**(Active Directory Schema)**。

设置注册表以允许将操作写入架构

要允许域控制器写入架构，必须设置一个允许进行架构更新的注册表项。

1. 右键单击窗口左窗格中的“**Active Directory** 架构”**(Active Directory Schema)** 根节点，然后单击“操作主体”**(Operations Master)**。
2. 选中“可以在此域控制器上修改架构”**(The Schema may be modified on this Domain Controller)** 前面的复选框。
3. 单击“确定”**(OK)**。

创建新属性

要为 **rciusergroup** 类创建新属性，请执行以下操作：

1. 单击窗口左窗格中“**Active Directory** 架构”**(Active Directory Schema)** 前面的 + 号。
2. 右键单击左窗格中的“属性”**(Attributes)**。
3. 单击“新建”**(New)**，然后选择“属性”**(Attribute)**。出现警告消息时，单击“继续”**(Continue)**。将显示“创建新属性”**(Create New Attribute)** 窗口。

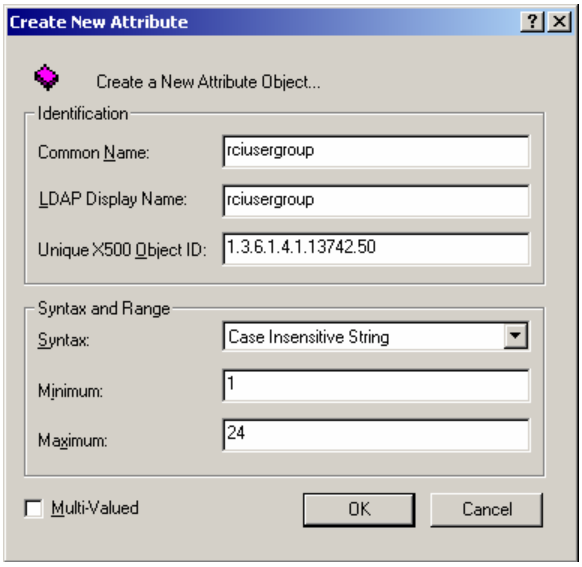


图 108：创建新属性

4. 在“通用名称”**(Common Name)** 字段中键入“**rciusergroup**”。
5. 在“LDAP 显示名称”**(LDAP Display Name)** 字段中键入“**rciusergroup**”。
6. 在“唯一 **x5000** 对象 **ID**”**(Unique x5000 Object ID)** 字段中键入“**1.3.6.1.4.1.13742.50**”。
7. 单击“语法”**(Syntax)** 下拉箭头，并从列表中选择“不区分大小写的字符串”**(Case Insensitive String)**。
8. 在“最小值”**(Minimum)** 字段中键入“**1**”。
9. 在“最大值”**(Maximum)** 字段中键入“**24**”。
10. 单击“确定”**(OK)** 以创建新属性。

向类添加属性

1. 单击窗口左窗格中的“类”**(Classes)**。
2. 在右窗格中滚动到“用户”**(user)** 类，然后右键单击以打开它。
3. 从菜单中选择“属性”**(Properties)**。将显示“用户属性”**(user Properties)** 窗口。
4. 单击“属性”**(Attributes)** 选项卡。
5. 单击“添加”**(Add)**。
6. 从“选择架构对象”**(Select Schema Object)** 列表中选择“**rciusergroup**”。

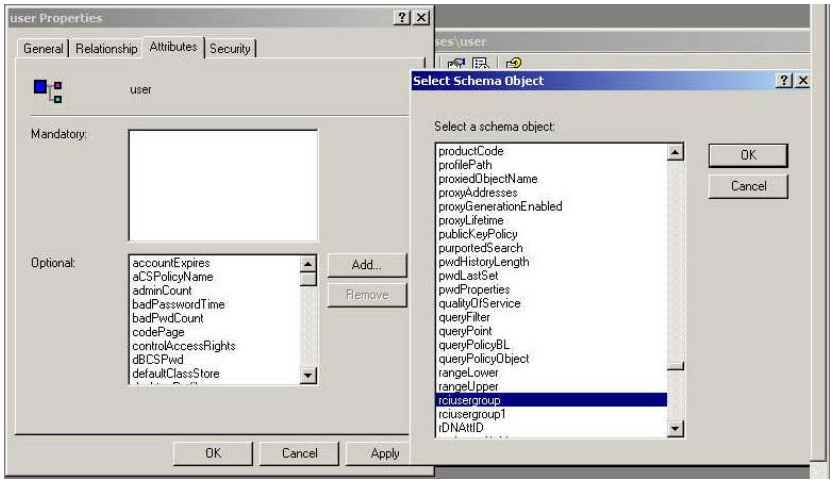


图 109：向类添加属性

7. 单击“确定”**(OK)**。
8. 单击“确定”**(OK)**。

更新架构高速缓存

1. 在窗口左窗格中右键单击“**Active Directory** 架构”**(Active Directory Schema)**，然后从快捷菜单中选择“重新加载架构”**(Reload the Schema)**。
2. 最小化“Active Directory 架构”(Active Directory Schema) MMC 控制台。

编辑用户成员的 RCI 用户组属性

要在 Windows 2003 服务器上运行 Active Directory 脚本，请使用 Microsoft 提供的脚本。这些脚本是在安装 Microsoft Windows 2003 时加载到系统中的。ADSI（(Active Directory 服务接口）充当 Active Directory 的低级别编辑器，允许您使用某个目录服务执行一些常见管理任务，例如添加、删除和移动对象。有关其它信息，请访问 Microsoft 网站：http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/ebca3324-5427-471a-bc19-9aa1decd3d40.mspx。

要编辑组 rciusergroup 中的单个用户属性，请执行以下操作：

1. 在 **Windows**“开始”**(Start)** 菜单上，单击“运行”**(Run)**。
2. 键入“**regsvr adsiedit.msc**”。将显示“ADSI 编辑”(ADSI Edit) 窗口。

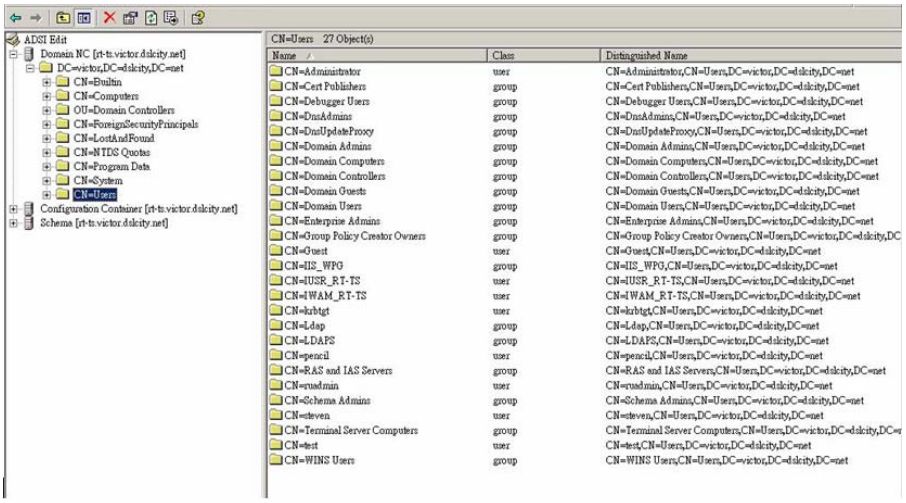


图 110：ADSI 编辑

3. 在窗口左窗格中，选择“**CN=User**”文件夹。
4. 在右窗格中找到要调整其属性的用户名。右键单击该用户名，并选择“属性”**(Properties)**。
5. 单击“属性”**(Attributes)** 选项卡。
6. 单击“选择要查看的属性”**(Select a property to view)** 下拉箭头，并从列表中选择“**rciusergroup**”。



图 111：用户属性

7. 在窗口的“属性值”**(Attribute Values)** 面板中，在“编辑属性”**(Edit Attribute)** 字段中键入要返回到 **RRC** 的用户名。

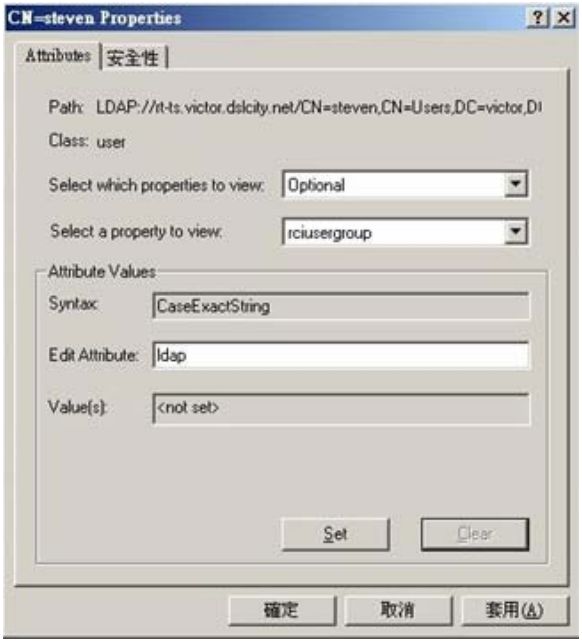


图 112：编辑属性（将用户添加到 KX II 组）

8. 单击“设置”**(Set)**。
9. 单击“确定”**(OK)**。

附录 C：常见问题解答

一般性问题

问题	解答
什么是 Dominion KX II？	Dominion KX II 是第二代数字 KVM（键盘、视频和鼠标）切换器，可允许 IT 管理员利用 BIOS 级功能通过网络访问和控制 16、32 或 64* 台服务器。Dominion KX II 完全独立于硬件和操作系统；即使服务器关闭，用户也可以对服务器进行疑难排解和重新配置。 在机架部分，Dominion KX II 提供与传统的模拟 KVM 切换器相同的功能、便利性，并同样节省空间和成本。但是，Dominion KX II 还集成了业界表现最佳的采用 IP 的 KVM 技术，允许多个管理员从任何联网工作站访问服务器 KVM 控制台。
Dominion KX II 与远程控制软件有哪些不同？	远程使用 Dominion KX II 时，其界面看上去类似远程控制软件，例如 pcAnywhere™、Windows® Terminal Services / Remote Desktop、VNC 等等。但是，由于 Dominion KX II 不是软件，而是一种硬件解决方案，因此功能更强大： • 独立于操作系统和硬件 – Dominion KX II 可用于管理运行许多常用操作系统（包括 Windows、Linux®、Solaris™ 的 Intel®、Sun®、PowerPC 等）的服务器。 • 独立于状态/无代理 – Dominion KX II 不要求运行受管服务器的操作系统，也不要求在受管服务器上安装任何特殊软件。 • 独立于网络外 – 即使受管服务器自己的网络连接不可用，它仍能通过 Dominion KX II 进行管理。 • BIOS 级访问 – 即使服务器开机挂起、要求引导到安全模式或要求改变系统 BIOS 参数，Dominion KX II 仍能顺畅工作，完成这些配置。
Dominion KX II 的新功能与 KX I 相比如何？	Dominion KX II 具有许多引人入胜的新功能，包括虚拟媒体、双电源、双千兆以太网、基于 Web 的公用用户界面、下一代本地端口等等。
如何从 Dominion KX I 迁移到 Dominion KX II？	通常，KX I 客户可以继续使用其现有的切换器许多年。随着客户数据中心的扩张，他们可以购买和使用新的 KX II 型号。Raritan 的集中管理设备 CommandCenter® Secure Gateway 和 Multi-Platform Client (MPC) 均无缝地支持 KX I 和 KX II 切换器。
我现有的 KX I CIM 可以与 Dominion KX II 切换器一起使用吗？	是的，现有的 KX I CIM 可以与 Dominion KX II 切换器一起使用。此外，Paragon CIM 选件也可以与 KX II 一起使用。这样，想要切换到采用 IP 的 KVM 的 Paragon I 客户可以更容易地迁移到 KX II。
是否可以将 Dominion KX II 安装在机架上？	可以。Dominion KX II 标配 19 英寸机架安装托架。还可以进行反向机架安装，使服务器端口面朝前。
Dominion KX II 有多大？	Dominion KX II 仅有 1U 高（KX2-464* 除外，它为 2U 高），可以容纳在一个标准 19 英寸机架中，仅有 11.4 英寸（29 厘米）深。

* KX2-464 可用 2Q07

远程访问

<table>
<tr><th>问题</th><th>解答</th></tr>
<tr><td>多少个用户可以远程访问每台 Dominion KX II 上的服务器？</td><td>Dominion KX II 型号每个通道为最多 8 个用户提供远程连接，允许他们同时访问和控制一台唯一的目标服务器。对于单通道设备，例如 DKX2-116，最多可以有 8 个远程用户访问和控制一台目标服务器。对于双通道设备，例如 DKX2-216，最多可以有 8 个用户访问和控制通道 1 中的服务器，另外最多可以有 8 个用户访问和控制通道 2 中的服务器。对于 4 通道设备，每个通道最多可以有 8 个用户，总共可以有 32 (8 x 4) 个用户以类似的方式访问和控制 4 台服务器。</td></tr>
<tr><td>两个人是否可以同时查看同一台服务器？</td><td>是，实际上，最多可以有 8 个人同时访问和控制任何一台目标服务器。</td></tr>
<tr><td>是否可以一人从远程端口，另一人从本地端口，两人同时访问同一台服务器？</td><td>是，本地端口与远程“端口”完全独立。本地端口可以使用 PC 共享功能访问同一服务器。</td></tr>
<tr><td>要从客户机访问 Dominion KX II，需要哪些硬件、软件或网络配置？</td><td>由于 Dominion KX II 完全可以通过 Web 访问，因此不需要在用于访问的客户机上安装专用软件。（Raritan.com 中提供了一个已安装客户机选件，用于通过调制解调器访问 Dominion KX II）。

可以通过以下主流 Web 浏览器访问 Dominion KX II：Internet Explorer、Mozilla™ 和 Firefox。现在，可以通过 Raritan 的基于 Java 的 Multi-Platform Client (MPC) 和新的 Virtual KVM Client™ 在 Windows、Linux、Sun Solaris 以及 Macintosh® 桌面上访问 Dominion KX II。

Dominion KX II 管理员也可以使用基于浏览器的使用方便的界面执行远程管理（设置密码和安全配置、重命名服务器、更改 IP 地址等）。</td></tr>
<tr><td>用于访问 Dominion KX II 的小程序文件有多大？检索需要多少时间？</td><td>用于访问 Dominion KX II 的 Virtual KVM Client 小程序大小约为 500KB。下图显示了以不同网络速度检索 Dominion KX II 的小程序所需的时间：

<table>
<tr><td>100Mbps</td><td>理论上 100Mbit 网络速度</td><td>0.05 秒</td></tr>
<tr><td>60Mbps</td><td>可能的实际 100Mbit 网络速度</td><td>0.08 秒</td></tr>
<tr><td>10Mbps</td><td>理论上 10Mbit 网络速度</td><td>.4 秒</td></tr>
<tr><td>6Mbps</td><td>可能的实际 10Mbit 网络速度</td><td>.8 秒</td></tr>
<tr><td>512Kbps</td><td>电缆调制解调器下载速度（通常）</td><td>8 秒</td></tr>
</table>
</td></tr>
<tr><td>当网络不可用时，我如何访问与 Dominion KX II 连接的服务器？</td><td>Dominion KX II 提供了一种专用调制解调器端口，用于连接外部调制解调器。即使发生网络紧急情况，仍然可以远程访问外接了调制解调器的服务器。此外，无论网络状况如何，Dominion KX II 的本地端口始终允许从机架访问服务器。</td></tr>
<tr><td>您有非 Windows 客户机吗？</td><td>可以。Virtual KVM Client 和 Multi-Platform Client (MPC) 都允许非 Windows 用户通过 Dominion KX I 和 KX II 切换器连接到目标服务器。MPC 可以通过 Web 浏览器运行，也可以独立运行。有关更多信息，请参阅 Virtual KVM Client 和 MPC/RRC User Guide（MPC/RRC 用户指南）。</td></tr>
</table>

问题	解答
我的调制解调器连接断了，收到错误消息“There was an unexpected communications error – connection terminated.”（发生意外的通信错误 - 连接终止。），我该怎么办？	根据用户尝试通过调制解调器进行连接的频率，可能会发生这种情况。重新引导 KX 设备和调制解调器，并且以后进行连接时，在两次尝试之间等待至少两 (2) 分钟。
有时在虚拟 KVM 会话期间，**Alt** 键好像卡住了一样。我该怎么办？	这种情况通常发生在按住 **Alt** 键但是没有放开的时候。例如，在按空格键的同时连续按 **Alt** 键可能导致焦点从目标服务器移动到客户机 PC。 然后本地操作系统解释此组合键，并在活动窗口（客户机 PC）中触发此组合键的操作。

通用虚拟媒体

问题	解答
哪些型号的 Dominion KX II 支持虚拟媒体？	所有型号的 Dominion KX II 都支持虚拟媒体。可以独立使用虚拟媒体，也可以通过 CommandCenter Secure Gateway（一种集中管理设备）使用虚拟媒体。
Dominion KX II 支持哪些类型的虚拟媒体？	Dominion KX II 支持下列类型的媒体：内置和 USB 连接的 CD/DVD 驱动器、USB 大容量存储设备、PC 硬盘驱动器和远程驱动器。
使用虚拟媒体有什么要求？	要使用虚拟媒体，需要新的 D2CIM-VUSB CIM。它支持与支持 USB 2.0 接口的目标服务器进行虚拟媒体会话。该新的 CIM 在数量为 32 和 64 的经济 CIM 套装中提供，支持绝对鼠标同步以及远程固件更新。
虚拟媒体安全吗？	可以。虚拟媒体会话使用 128 位 AES 或 RC4 加密方法保护。

以太网和 IP 网络

<table>
<tr><th>问题</th><th>解答</th></tr>
<tr><td>Dominion KX II 是否提供双千兆以太网端口以提供冗余故障切换或负载平衡？</td><td>可以。Dominion KX II 配有双千兆以太网端口，以提供冗余故障切换功能。如果主以太网端口（或者与它相连的交换机/路由器）发生故障，Dominion KX II 将故障切换到具有相同 IP 地址的备用网络端口，确保服务器操作不中断。注：管理员必须启用自动故障切换。</td></tr>
<tr><td>Dominion KX II 需要多少带宽？</td><td>Dominion KX II 提供下一代采用 IP 的 KVM 技术，这种技术能提供最好的视频压缩。Raritan 已获得了无数科技成果奖，表彰它的高视频质量传输性能和低带宽利用率。

Raritan 是采用 IP 的 KVM 功能的先驱，用户可以利用这种功能定制他们的视频参数以节约网络带宽。例如，通过拨号调制解调器连接到 Dominion KX II 时，可以将视频传输调整为灰度，以允许用户达到最大产能且确保高性能。

了解这一点以后，以下数据表示使用默认视频设置的 Dominion KX II – 这些设置也可以根据特定环境进行定制。可以提高这些数据，以提供甚至更高质量的视频（色深），或降低这些数据，以优化低速连接。

通常，保守估计的带宽利用率（使用 Dominion KX II 的默认设置）约为每个活动 KVM 用户（已连接并在使用服务器的用户）0.5Mbit/s，很偶尔的情况下可以达到 2MBit/s。这是非常保守的估计，因为带宽利用率通常会更低。

每次视频传输所需的带宽取决于正在受管服务器上执行的任务。屏幕变化的越多，需使用更多的带宽。下表概述了一些使用情况，以及在 10Mbit/s 网络中使用 Dominion KX II 的默认设置时所需的带宽利用率：

<table><tr><td>空闲 Windows 桌面</td><td>0 Mbps</td></tr><tr><td>移动桌面指针</td><td>0.18Mbps</td></tr><tr><td>移动静态 400x600 窗口/对话框</td><td>0.35Mbps</td></tr><tr><td>浏览“开始”菜单</td><td>0.49Mbps</td></tr><tr><td>滚动文本整页</td><td>1.23Mbps</td></tr><tr><td>运行三维迷宫屏幕保护程序</td><td>1.55Mbps</td></tr></table></td></tr>
<tr><td>Dominion KX II 可以运行的最慢连接（最低带宽）是多少？</td><td>通过调制解调器连接时，要获得可接受的 KX 性能，建议使用 33Kbps 或更高的连接速度。</td></tr>
<tr><td>Dominion KX II 的以太网接口的速度是多少？</td><td>Dominion KX II 支持千兆以太网和 10/100 以太网。KX II 支持 10/100/1000 速双以太网接口，以及可配置的速度和双工设置（自动检测或手动设置）。</td></tr>
<tr><td>我是否可以通过无线连接访问 Dominion KX II？</td><td>可以。Dominion KX II 不仅使用标准以太网，而且很节省带宽，同时提供质量非常高的视频。因此，如果无线客户机具有与 Dominion KX II 的网络连接，则可以在 BIOS 级别无线配置和管理服务器。</td></tr>
</table>

问题	解答
是可以通过 WAN (Internet) 使用 Dominion KX II，还是只能通过公司 LAN 使用它？	无论是通过快速的公司 LAN、较不可预测的 WAN (Internet)，还是通过电缆调制解调器或拨号调制解调器进行的连接，Dominion KX II 的采用 IP 的 KVM 技术都能适合。
是否可以通过 VPN 使用 Dominion KX II？	可以。Dominion KX II 使用从第 1 层到第 4 层的标准 Internet 协议 (IP) 技术。通信可以从标准 VPN 轻松通过。
要启用对 Dominion KX II 的网络访问，我的防火墙上必须打开多少 TCP 端口？这些端口是否可以配置？	只需要一个。Dominion KX II 只需访问一个 TCP 端口便可工作，从而保护网络的安全。此端口可以进行完全配置，以获得更高的安全性。 当然，请注意，要使用 Dominion KX II 可选的 Web 浏览器功能，还必须打开标准 HTTPS 端口 443。
Dominion KX II 是否需要外部认证服务器才能运行？	不需要。Dominion KX II 是完全自足的设备。为 Dominion KX II 分配 IP 地址之后，便可以使用它了 – Web 浏览器和认证功能是完全内置的。 Dominion KX II 也允许使用外部认证服务器（例如 LDAP、Active Directory®、RADIUS 等），甚至可以在外部认证服务器不可用的情况下故障切换为其自己的内部认证。这样，Dominion KX II 的设计原理便得以优化，可以提供轻松的安装、与任何外部服务器的完全独立性和最大的灵活性。
是否可以将 Dominion KX II 与 CITRIX 一起使用？	Dominion KX II 可以与经过正确配置的远程访问产品（如 CITRIX）一起使用，但 Raritan 无法保证它工作时能够提供可接受的性能。诸如 CITRIX 的产品利用在概念上与数字 KVM 切换器相似的视频重定向技术，因此，可以同时使用这两种采用 IP 的 KVM 技术。
Dominion KX II 是否可以使用 DHCP？	可以使用 DHCP 寻址，但是，Raritan 建议使用固定地址，因为 Dominion KX II 是一种基础架构设备，通过固定 IP 地址可以更有效地访问和管理 Dominion KX II。
我通过我的 IP 网络连接 Dominion KX II 时有问题，这会是什么问题呢？	Dominion KX II 依赖您的 LAN/WAN 网络。一些可能的问题有： • 以太网自动协商。在某些网络上，10/100 自动协商无法正确工作，且 KX II 设备必须设置为 100MB/全双工或适合其网络的选项。 • IP 地址重复。如果 KX II 与另一个设备的 IP 地址相同，网络连接可能会不一致。 • 端口 5000 冲突。如果另一个设备在使用端口 5000，则必须更改 KX II 的默认端口（或必须更改另一个设备使用的端口）。 • 更改 KX II 的 IP 地址，或者在新的 KX II 中进行交换时，必须留有足够的时间，让整个第 2 层和第 3 层网络知道它的 IP 和 MAC 地址。

服务器

问题	解答
Dominion KX II 必须依赖 Windows 服务器才能工作吗？	完全不是。由于用户要求 KVM 基础架构在任何情况下都始终可用（因为他们可能需要使用 KVM 基础架构来修复问题），因此 Dominion KX II 设计为完全独立于任何外部服务器。 例如，当数据中心受到恶意 Windows 蠕虫或病毒攻击时，管理员需要使用 KVM 解决方案来解决这种情况。因此，为了使 KVM 解决方案有效，KVM 解决方案绝不能依赖这些相同的 Windows 服务器（或对于该情况来说，任何服务器）才能工作。 总而言之，Dominion KX II 是完全独立的。即使用户选择将 Dominion KX II 配置为针对 Active Directory 服务器进行认证时也是如此：如果该 that Active Directory 服务器变为不可用，Dominion KX II 自己的认证将被激活并完全正常工作。
我是否需要安装 Web 服务器（例如 Microsoft Internet 信息服务 (IIS)）才能使用 Dominion KX II 的 Web 浏览器功能？	不需要。Dominion KX II 是完全自足的设备。为 Dominion KX II 分配 IP 地址之后，便可以使用它了 – Web 浏览器和认证功能是完全内置的。
要从特定工作站访问 Dominion KX II，必须安装什么软件？	不需要安装。完全可以通过 Web 浏览器访问 Dominion KX II（不过，为了通过调制解调器访问 Dominion KX II，在 Raritan 的网站 Raritan.com 上提供了一个已安装客户机选件）。现在，非 Windows 用户可以使用基于 Java 的客户机。
要将服务器连接到 Dominion KX II，我需要做哪些准备工作？	只需设置鼠标参数（以便为用户在远程连接期间提供最佳鼠标同步）并关闭影响屏幕显示的电源管理功能。但是，如果使用新的 D2CIM-VUSB 适配器（支持 Absolute Mouse Synchronization™（绝对鼠标同步）），则不需要手动设置鼠标参数。
Dominion KX II 包装盒中都有什么？	包括下列项：(a) Dominion KX II 设备；(b) 快速安装指南；(c) 标准 19 英寸机架安装托架；(d) 用户手册 CD-ROM；(e) 网络电缆；(f) 交叉电缆；(g) 当地的交流电源线；(h) 保修证书和其它文档。

安装

问题	解答
除了设备本身，我还需要从 Raritan 订购哪些组件才能安装 Dominion KX II？	连接 Dominion KX II 的每台服务器需要一个 Dominion 或 Paragon 计算机接口模块 (CIM)，它是一个直接连接到服务器的键盘、视频和鼠标端口的适配器。
安装时应使用哪一种 Cat5 电缆？	Dominion KX II 可以使用任何标准 UTP（非屏蔽双绞线）电缆，包括 Cat5、Cat5e 或 Cat6。为简便起见，在我们的手册和市场宣传文字中，Raritan 通常只提到“Cat5”电缆。实际上，任何品牌的 UTP 电缆都能满足 Dominion KX II。
哪些类型的服务器可以连接到 Dominion KX II？	Dominion KX II 支持任何厂商的服务器。可以连接具有符合标准的键盘、视频和鼠标端口的任何服务器。
如何将服务器连接到 Dominion KX II？	连接到 Dominion KX II 的服务器需要一个 Dominion 或 Paragon CIM，该 CIM 直接连接到服务器的键盘、视频和鼠标端口。然后，使用 Cat5、Cat5e 或 Cat6 等标准 UTP（双绞线）电缆将每个 CIM 连接到 Dominion KX II。
服务器与 Dominion KX II 的距离可以有多远？	通常，服务器与 Dominion KX II 的距离最远可以达 150 英尺（45 米），具体取决于服务器的类型。有关更多信息，请参见 Raritan 网站或目标服务器连接距离。对于支持虚拟媒体和绝对鼠标同步的新 D2CIM-VUSB CIM，建议的距离为 100 英尺（30 米）。
在操作过程中断开键盘或鼠标的连接时，某些操作系统会锁定。当我从连接到 Dominion KX II 的服务器切换出来时，是什么防止了这些服务器的锁定？	每个 Dominion 计算机接口模块 (DCIM) 解密器充当模块所连接的服务器的虚拟键盘和鼠标。这种技术称为 KME（键盘/鼠标仿真）。Raritan 的 KME 技术是数据中心等级的，经过实践测试，比低端 KVM 切换器中使用的 KME 要可靠的多：它融入了超过 15 年的开发经验，已部署在全球数百万台服务器中。
连接到 Dominion KX II 的服务器中必须安装代理吗？	连接到 Dominion KX II 的服务器不需要安装任何软件代理，因为 Dominion KX II 通过硬件直接连接到服务器的键盘、视频和鼠标端口。
每个 Dominion KX II 设备可以连接多少台服务器？	Dominion KX II 在 1U 机架中支持 16 或 32 个服务器端口，在 2U 机架中支持 64 个服务器端口，具体取决于型号。这是业界最高的数字 KVM 切换器端口密度。
如果将服务器与某个 Dominion KX II 设备断开连接，然后将其重新连接到另一个 Dominion KX II 设备，或者将其连接到同一 Dominion KX II 设备的其它端口，会发生什么情况？	服务器从一个端口移至另一个端口时，Dominion KX II 将自动更新服务器端口名称。而且，这种自动更新不仅仅影响本地访问端口，还会传播到所有远程客户机和 CommandCenter Secure Gateway 管理设备选件。

问题	解答
如何将串口控制的 (RS-232) 设备连接到 Dominion KX II，例如 Cisco 路由器/交换机或无头式 Sun 服务器？	如果只有几个串口控制的设备，可以使用 Raritan 的串口适配器 AUATC 或新的 P2CIM-SER 串口转换器将它们连接到 Dominion KX II。 但是，如果有四个或更多串口控制的设备，建议使用 Raritan 的安全控制台服务器的 Dominion SX 产品线。对于多个串口设备，Dominion SX 可提供比 Dominion KX II 更多、价格更经济串行功能。该 SX 易于使用、配置和管理，并且可以与 Dominion 系列部署完全集成。特别是，直接将 SSH 连接到 Dominion SX 设备的功能受许多 UNIX 和网络管理员的青睐。

本地端口

问题	解答
是否可以从机架直接访问我的服务器？	可以。在机架部分，Dominion KX II 就像传统的 KVM 切换器那样工作 – 允许使用一个键盘、显示器和鼠标来控制多达 64 台服务器。
使用本地端口时，会阻止其他用户远程访问服务器吗？	不会。Dominion KX II 本地端口具有对服务器的完全独立的访问路径。这意味着用户可以在机架本地访问服务器，且不会减少可同时远程访问机架的用户数量。
我可以在本地端口使用 USB 键盘或鼠标吗？	可以。Dominion KX II 在本地端口提供了 PS/2 和 USB 键盘及鼠标端口。请注意，USB 端口是 USB v1.1 的，仅支持键盘和鼠标，不支持扫描仪或打印机这样的 USB 设备。
本地机架访问有屏幕显示 (On-Screen Display, OSD) 吗？	有，不过 Dominion KX II 的机架访问提供的不仅仅是传统的 OSD。KX II 的本地端口为机架访问提供了业界第一个基于浏览器的界面，它使用同一界面进行本地和远程访问。此外，在机架提供了大多数管理功能。
使用本地端口时如何选择服务器？	本地端口使用与远程客户机相同的用户界面来显示连接的服务器。只需单击鼠标，便可连接到服务器。
如何确保只有授权用户才能从本地端口访问服务器？	尝试使用本地端口的用户必须通过与远程访问的用户相同的认证级别。这意味着： • 如果 Dominion KX II 配置为与外部 RADIUS、LDAP 或 Active Directory 服务器交互，则尝试访问本地端口的用户将针对同一服务器进行认证。 • 如果外部认证服务器不可用，Dominion KX II 将故障切换到其自己的内部认证数据库。 Dominion KX II 具有其自己的独立认证，以允许即时、随时可以进行的安装。
如果我使用本地端口来更改所连接服务器的名称，该更改会不会还传播到远程访问客户机？该更改会传播到 CommandCenter 设备选件吗？	可以。本地端口显示与远程访问客户机以及 Raritan 的 CommandCenter Secure Gateway 管理设备选件的显示相同且完全同步。进一步说，如果 Dominion KX II 屏幕显示中的服务器名称发生更改，所有远程客户机和外部管理服务器也会相应实时更新。
如果我使用 Dominion KX II 的远程管理工具来更改所连接服务器的名称，该更改会不会还传播到本地端口 OSD？	可以。如果远程更改服务器的名称，或者通过 Raritan 的 CommandCenter Secure Gateway 管理设备选件更改服务器的名称，此更新将立即影响 Dominion KX II 的屏幕显示。
有时候会在本地端口用户界面上看到“阴影”，为什么会这样？	开启了很长时间的 LCD 显示器上可能会出现该阴影/重像效果。屏幕开启了很长时间时，LCD 的性质和电荷/静电充放可能会导致生成这些效果。

电源控制

问题	解答
Dominion KX II 有双电源选件吗？	所有型号的 Dominion KX II 都配有双交流电源输入和具有自动故障切换功能的电源。一旦电源输入或电源之一发生故障，则 KX II 将自动切换到另一个。
Dominion KX II 使用的电源会自动检测电压设置吗？	可以。Dominion KX II 的电源可以在 100-240 伏、50-60 赫兹的交流电压范围内使用。
如果电源或电源输入发生故障，我会得到通知吗？	KX II 前面板 LED 将向用户通知电源故障。还将向审计日志发送一个条目，并在 KX II 远程客户机用户界面中显示该条目。如果管理员进行了相应配置，还将生成 SNMP 或 Syslog 事件。
Dominion KX II 提供什么类型的电源控制功能？	Raritan 的远程电源控制电源板可以连接到 Dominion KX II，以提供对目标服务器的电源控制。经过简单的一次性配置步骤之后，只需右键单击服务器名称即可打开、关闭服务器电源，或恢复使用挂起的服务器。请注意，硬重新引导等效于物理上拔出服务器的交流电源线，然后重新插入。
Dominion KX II 支持具有多个电源的服务器吗？如果每个电源连接到不同的电源板上，会发生什么情况？	可以。可以轻松将 Dominion KX II 配置为支持连接到多个电源板的多个电源。最多可以将八 (8) 个电源板连接到一个 KX II 设备。每个目标服务器可以有四个电源连接到多个电源板。
远程电源控制需要任何特殊服务器配置吗？	某些服务器附带默认 BIOS 设置，使得服务器在断电和恢复供电之后不会自动重新启动。有关更多信息，请参阅服务器用户手册。
Dominion KX II 支持哪些类型的电源板？	为了利用 Dominion KX II 的集成电源控制用户界面，更为重要的是，为了利用它的集成安全性，请使用 Raritan 的远程电源控制 (RPC) 电源板。RPC 具有许多不同的电源插座，连接器和放大器。必须购买 D2CIM-PWR，才能将 RPC 连接到 KX II。

可伸缩性

问题	解答
如何将多个 Dominion KX II 设备一起连接到一个解决方案中？	多个 Dominion KX II 设备不需要物理连接在一起。每个 Dominion KX II 设备连接到网络中之后，它们将自动作为一个解决方案一起工作（如果使用 Raritan 的 CommandCenter Secure Gateway (CC-SG) 管理设备选件进行了部署）。CC-SG 充当远程访问和管理的单一接入点。CC-SG 提供了一组重要的方便工具，例如整合配置、整合固件更新，以及单一认证和授权数据库。 此外，CC-SG 允许复杂的服务器排序、权限和访问。如果无法选择部署 Raritan 的 CC-SG 管理设备，多个 Dominion KX II 设备仍然可以自动互操作和缩放：KX II 的远程用户界面和 Multi-Platform Client 将自动发现 Dominion KX II 设备。未发现的 Dominion KX II 设备可以通过用户创建的配置文件进行访问。
是否可以将现有的模拟 KVM 切换器连接到 Dominion KX II？	可以。模拟 KVM 切换器可以连接到 Dominion KX II 的某个服务器端口。只需将一个 PS/2 计算机接口模块 (CIM) 连接到现有模拟 KVM 切换器的用户端口即可。请注意，各个模拟 KVM 切换器的规格有所不同，Raritan 不能保证与任何特殊的第三方模拟 KVM 切换器的互操作性。有关更多信息，请咨询 Raritan 技术支持部门。Raritan 的 Paragon® 和 Paragon II 模拟切换器通过 IP-Reach® 系列远程访问产品支持 IP。

计算机接口模块 (CIM)

问题	解答
我可以将 Raritan 的模拟矩阵 KVM 切换器 Paragon 的计算机接口模块 (CIM) 用于 Dominion KX II 吗？	可以。某些 Paragon 计算机接口模块 (CIM) 可以用于 Dominion KX II（有关最新的认证 CIM 的列表，请查看网站上的 Raritan Dominion KX II 发布声明）。 但是，由于 Paragon CIM 的成本比 Dominion KX II CIM 高（因为它们采用了视频传输距离最远达 1000 英尺 [300 米] 的技术），通常不建议购买 Paragon CIM 来用于 Dominion KX II。另外请注意，当连接到 Dominion KX II 时，Paragon CIM 的视频传输距离最远达 150 英尺（而不是 1000 英尺 [300 米]），与 Dominion KX II CIM 连接到 Paragon 时的视频传输距离相同。
我可以将 Dominion KX II 计算机接口模块 (CIM) 用于 Raritan 的模拟矩阵 KVM 切换器 Paragon 吗？	不能。Dominion KX II 计算机接口模块 (CIM) 的视频传输距离为 50 至 150 英尺（15 – 45 米），因而不能用于 Paragon，后者需要视频传输距离为 1000 英尺（300 米）的 CIM。为了确保 Raritan 的所有客户都能体验到业界最高质量的视频（这也是 Raritan 一向的特点），Dominion 系列 CIM 不能与 Paragon 互操作。

安全性

<table>
<tr><th>问题</th><th>解答</th></tr>
<tr><td>Dominion KX II 使用什么类型的加密？</td><td>Dominion KX II 在其 SSL 通信和其自己的数据流中均使用业界标准（且极为安全）的 128 位 RC4 或 AES 加密。也就是说，远程客户机和 Dominion KX II 之间不会传输未经加密机制完全保护的数据。</td></tr>
<tr><td>Dominion KX II 支持美国政府的 NIST 和 FIPs 标准推荐的 AES 加密吗？</td><td>Dominion KX II 使用高级加密标准 (AES) 加密以提高安全性。
AES 是美国政府认可的加密算法，美国国家标准与技术研究所 (NIST) 在“FIPS 标准 197”中推荐使用。</td></tr>
<tr><td>Dominion KX II 允许加密视频数据吗？还是仅加密键盘和鼠标数据？</td><td>与仅加密键盘和鼠标数据的竞争解决方案不同，Dominion KX II 不会牺牲安全：它允许加密键盘、鼠标和视频数据。</td></tr>
<tr><td>Dominion KX II 如何与外部认证服务器（例如 Active Directory®、RADIUS 或 LDAP）集成？</td><td>通过非常简单的配置，可以将 Dominion KX II 设置为将所有认证请求转发到外部服务器，例如 LDAP、Active Directory 或 RADIUS。对于每个经过认证的用户，Dominion KX II 会从认证服务器接收该用户所属的用户组。Dominion KX II 随后根据该用户所属的用户组来确定该用户的访问权限。</td></tr>
<tr><td>用户名和密码是如何存储的？</td><td>如果使用 Dominion KX II 的内部认证功能，则所有敏感信息（用户名和密码等）以加密格式进行存储。也就是说，任何人，包括 Raritan 技术支持部门或产品工程部门人员，都无法检索这些用户名和密码。</td></tr>
<tr><td>Dominion KX II 支持复合密码吗？</td><td>可以。Dominion KX II 具有管理员可以配置的复合密码检查，以确保用户创建的密码符合公司和/或政府标准，并能抵御强力黑客行为。</td></tr>
<tr><td>如果 Dominion KX II 加密模式设置为自动，将实现什么级别的加密？</td><td>自动协商的加密级别取决于所使用的浏览器：
<table>
<tr><th>浏览器</th><th>加密级别</th></tr>
<tr><td>Internet Explorer 6</td><td>RC4</td></tr>
<tr><td>Internet Explorer 7</td><td>AES-128</td></tr>
<tr><td>Firefox 1.5</td><td>RC4</td></tr>
<tr><td>Firefox 2.0</td><td>RC4</td></tr>
<tr><td>Mozilla 1.7</td><td>RC4</td></tr>
<tr><td>Safari 2.0.4</td><td>AES-128</td></tr>
</table>
</td></tr>
</table>

易管理性

问题	解答
Dominion KX II 可以通过 Web 浏览器进行远程管理和配置吗？	可以。Dominion KX II 可以通过 Web 浏览器远程进行完全配置。请注意，这并不要求工作站安装适当的 Java Runtime Environment (JRE) 版本。 除了 Dominion KX II 的 IP 地址初始设置外，可以通过网络完全设置有关解决方案的任何内容。（实际上，使用交叉以太网电缆和 Dominion KX II 的默认 IP 地址时，甚至可以通过 Web 浏览器配置初始设置。）
我可以备份和恢复 Dominion KX II 的配置吗？	可以。Dominion KX II 的设备和用户配置可以完全进行备份，以便以后在发生灾难的情况下进行恢复。 可以通过网络远程使用 Dominion KX II 的备份和恢复功能，也可以通过 Web 浏览器使用。
Dominion KX II 提供什么样的审计和记录功能？	为了进行完整的说明，Dominion KX II 记录所有主要用户事件，并附带了日期和时间戳。例如，报告的事件包括（但不限于）：特定服务器的用户登录、注销和访问、不成功的登录、配置更改，等等。
Dominion KX II 可以与 Syslog 集成吗？	可以。除了 Dominion KX II 自己的内部记录功能，Dominion KX II 还可以将所有记录的事件发送到中央 Syslog 服务器。
Dominion KX II 可以与 SNMP 集成吗？	可以。除了 Dominion KX II 自己的内部记录功能，Dominion KX II 还可以将 SNMP 跟踪发送到 SNMP 管理系统，例如 HP Openview 和 Raritan 的 CC-NOC。
Dominion KX II 的内部时钟可以与时间服务器同步吗？	可以。Dominion KX II 支持业界标准的 NTP 协议，用于与公司时间服务器同步或与任何公共时间服务器同步（假设允许出站 NTP 请求通过公司防火墙）。

其它问题

问题	解答
Dominion KX II 的默认 IP 地址是什么？	192.168.0.192
Dominion KX II 的默认用户名和密码是什么？	KX II 的默认用户名和密码是 **admin**/**raritan** [全部小写]。但是，为了实现最高级别的安全，KX II 强制管理员在第一次引导 Dominion KX II 设备时更改其默认管理用户名和密码。
我更改了 Dominion KX II 的管理密码，但后来忘记了；我可以自己检索到它吗？	KX II 包含一个硬件复位按钮，可用于对设备进行出厂复位。出厂复位将复位设备的管理密码。

疑难排解

问题	解答
我使用 Firefox 登录到 Dominion KX II，并打开了另一个 Firefox 浏览器。结果在第二个 Firefox 浏览器窗口中，我自动登录到同一个 Dominion KX II。这是正常的吗？	是，这是正确行为，是浏览器和 cookie 运行所导致的直接结果。
我使用 Firefox 登录到 Dominion KX II，并尝试从同一客户机使用另一个 Firefox 浏览器会话登录另一个 Dominion KX II。结果我从两个 KX II 中都注销了，这是正常行为吗？	是，要访问两个不同的 Dominion KX II 设备，请关闭第一个会话，或者使用另一台客户机。
在我使用 Firefox 作为浏览器运行 KVM 会话时，如果在虚拟 KVM 客户机中打开某些对话框（例如“连接属性”(Connection Properties)、“视频设置”(Video Settings)），似乎会拦截 Firefox 浏览器（甚至其它 Firefox 会话）。我该怎么办？	这是正常现象；使用 Firefox 时，所有会话都是关联的。一旦您关闭虚拟 KVM 客户机对话框，Firefox 就不会再受到拦截了。

255-62-4023-00

全球总部

Raritan, Inc.
400 Cottontail Lane
Somerset, NJ 08873, USA
电话：(732) 764-8886
传真：(732) 764-8887
电子邮件：sales@raritan.com
Web：www.raritan.com

Raritan America

Raritan, Inc.
400 Cottontail Lane
Somerset, NJ 08873, USA
电话：(732) 764-8886
传真：(732) 764-8887
电子邮件：sales@raritan.com
Web：www.raritan.com

亚太区总部

Raritan Asia Pacific, Inc.
5F, 121, Lane 235, Pao-Chiao Road,
Hsin Tien 231,
235 巷 121 号 5 楼
电话：(886) 2 8919-1333
传真：(886) 2 8919-1338
电子邮件：sales.asia@raritan.com
Web：raritan-ap.com

力登大陆代表处

力登北京
中国北京市西城区金融街 35 号
国际企业大厦 C 座 1035 室
邮编 100032
电话：(86) 10-8809-1890
电子邮件：sales.china@raritan.com
Web：raritan.com.cn

力登上海
中国上海市徐汇区零陵路 899 号
飞洲国际大厦 17 楼 E 室（邮编 200030）
电话：(86) 21 5425-2499
传真：(86) 21 5425-3992
电子邮件：sales.china@raritan.com
Web：raritan.com.cn

力登广州
中国广州市天河北路 183 号
大都会广场 1205 室（邮编 510075）
电话： (86) 20 8755-5581
传真： (86) 20 8755-5571
电子邮件：sales.china@raritan.com
Web：raritan.com.cn

Raritan Korea

#3602, Trade Tower, World Trade Center
Samsung-dong, Kangnam-gu
Seoul, Korea
电话：(82) 2 557-8730
传真：(82) 2 557-8733
电子邮件：sales.korea@raritan.com
Web：raritan.co.kr

Raritan Japan

4th Floor, Shinkawa NS Building
1-26-2 Shinkawa, Chuo-ku,
Tokyo 104-0033
电话：(81) 03-3523-5991
传真：(81) 03-3523-5992
电子邮件：sales@raritan.co.jp
Web：raritan.co.jp

Raritan Osaka
3rd Floor,
Osaka Kagaku Sen'I Kaikan Bldg.
4-6-8 Kawara-machi, Chuo-ku,
Osaka 541-0048
电话：(81) 03-3523-5953
传真：(81) 03-3523-5992
Web：raritan.co.jp

Raritan Australia Offices

Raritan Melbourne
Level 2, 448 St Kilda Rd.,
Melbourne, VIC3004
Australia
电话：(61) 3-9866-6887
电子邮件：sales.au@raritan.com
Web：raritan.com.au

Raritan Sydney
PO BOX A386,
Sydney, NSW2000, Australia
电话：(61) 2-9029-2558
电子邮件：sales.au@raritan.com
Web：raritan.com.au

Raritan India

210 2nd Floor Orchid Square
Sushant Lok 1, Block B, Mehrauli Gurgaon
Rd, Gurgaon 122 002
Haryana, India
电话： (91) 124 410-7881
传真：(91) 124 410-7880
电子邮件：enquiry.india@raritan.com
Web：raritan.co.in

力登台湾

中国台湾省台北县新店市
宾桥路
235 巷 121 号 5 楼
电话：(886) 2 8919-1333
传真：(886) 2 8919-1338
电子邮件：sales.taiwan@raritan.com
Web：raritan.com.tw

Raritan Singapore

350 Orchard Road
#11-08, Suite 21, Shaw House
Singapore 238868
电话：(65) 6725 9871
传真：(65) 6725 9872
电子邮件：sales.ap@raritan.com
Web：raritan-ap.com

欧洲总部

Raritan Europe, B.V.
Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands
电话：(31) 10-284-4040
传真：(31) 10-284-4049
电子邮件：sales.europe@raritan.com
Web：www.raritan.fr
www.raritan.de

Raritan France

120 Rue Jean Jaures
92300 Levallois-Perret, France
电话：(33) 14-756-2039
传真：(33) 14-756-2061
电子邮件：sales.france@raritan.com
Web：www.raritan.fr

Raritan Deutschland GmbH

Lichtstraße 2
D-45127 Essen, Germany
电话：(49) 201-747-98-0
传真：(49) 201-747-98-50
电子邮件：sales.germany@raritan.com
Web：www.raritan.de

Raritan Italia

Via dei Piatti 4
20123 Milan
Italy
电话：(39) 02-454-76813
传真：(39) 02-861-749
电子邮件：sales.italy@raritan.com
Web：raritan.it
www.raritan.info

Raritan Canada

Raritan Inc.
4 Robert Speck Pkwy., Suite 1500
Mississauga, ON L4Z 1S1
Canada
电话：1-905-949-3650
电子邮件：sales.canada@raritan.com
Web：raritan.ca

Raritan U.K.

9th Floor, 12-20 Camomile St
London EC3A 7EX, United Kingdom
电话：(44) (0)20-7614-7700
电子邮件：sales.uk@raritan.com
Web：raritan.co.uk