供电企业
信息网络实验案例

陈锡祥　主　编
宋金根　姚冰峰　副主编

中国电力出版社
CHINA ELECTRIC POWER PRESS

供电企业
信息网络实验案例

陈锡祥　主　编
宋金根　姚冰峰　副主编

中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

本书主要讲解供电企业信息网络建设、运行、维护所涉及的各类操作的实验案例，分基础篇和实验篇。基础篇主要介绍信息网络基础知识，信息网络实验平台的发展、特点与应用等；实验篇讲解了与网络交换、路由、安全等技术相关的33个实验案例，详细介绍实验目的、原理、步骤和相关知识点等内容。

本书由浅入深、图文并茂，注重实际操作，可作为信息网络技术基础培训教材和高等院校网络专业实验课的辅导书，还可供网络工程技术专业人员参考使用。

图书在版编目（CIP）数据

供电企业信息网络实验案例/陈锡祥主编. —北京：中国电力出版社，2013.8

ISBN 978-7-5123-4540-9

Ⅰ.①供… Ⅱ.①陈… Ⅲ.①供电-工业企业-信息网络-研究 Ⅳ.①F416.61-39

中国版本图书馆CIP数据核字（2013）第120284号

中国电力出版社出版、发行

（北京市东城区北京站西街19号 100005 http://www.cepp.sgcc.com.cn）

北京丰源印刷厂印刷

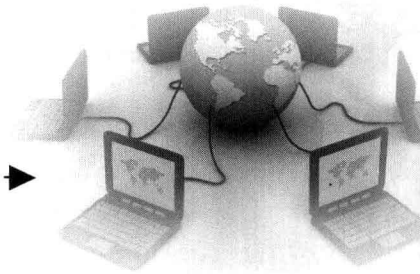
各地新华书店经售

*

2013年8月第一版 2013年8月北京第一次印刷

787毫米×1092毫米 16开本 19印张 467千字

印数0001—3000册 定价**48.00**元



前　言

信息网络是电网企业信息化的基础，在企业的生产、经营管理中发挥着重要作用。为提高信息网络的运行维护技能，保障信息网络的可靠运行，网络运行维护人员不仅需要掌握网络交换、路由、安全等理论知识，而且必须具备熟练的网络设备操作技能。

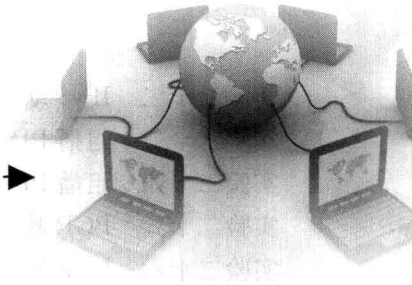
本书是湖州电力局信息网络专业人员多年工作经验的积累与总结，分基础篇和实验篇。基础篇介绍了网络技术的基础知识，包括 VLAN、STP、VTP、HSRP、MPLS（中文）等交换技术，RIP、EIGRP、OSPF、BGP 等路由技术，以及 AAA 认证配置、端口安全配置等网络安全技术。此外，还探讨了组播、IPv6、VOIP、MPLS VPN 等技术的应用以及常见网络实验平台的技术要点，并介绍了本书实验案例所用网络实验平台的架构、功能和使用方法。实验篇精选了 35 个基于思科（Cisco）公司网络产品的实验案例，覆盖交换技术、路由技术和网络安全技术等知识点，每个案例包括实验目的、实验原理、实验场景、实验步骤及参考配置等内容。

本书主要由陈锡祥、宋金根和姚冰峰主持编写。张鹰、楼平、詹辉红、邢建旭、翁时乐、凌红星、吕斌斌、孙卫庆、卢黎明、孙刚、包震斌、杨晔、张云峰、胡天瑜、张明乐、徐晓伟、陈军、吴云鹏、程路明、张骋、张页、徐国华等也参加了相关章节的编写工作。

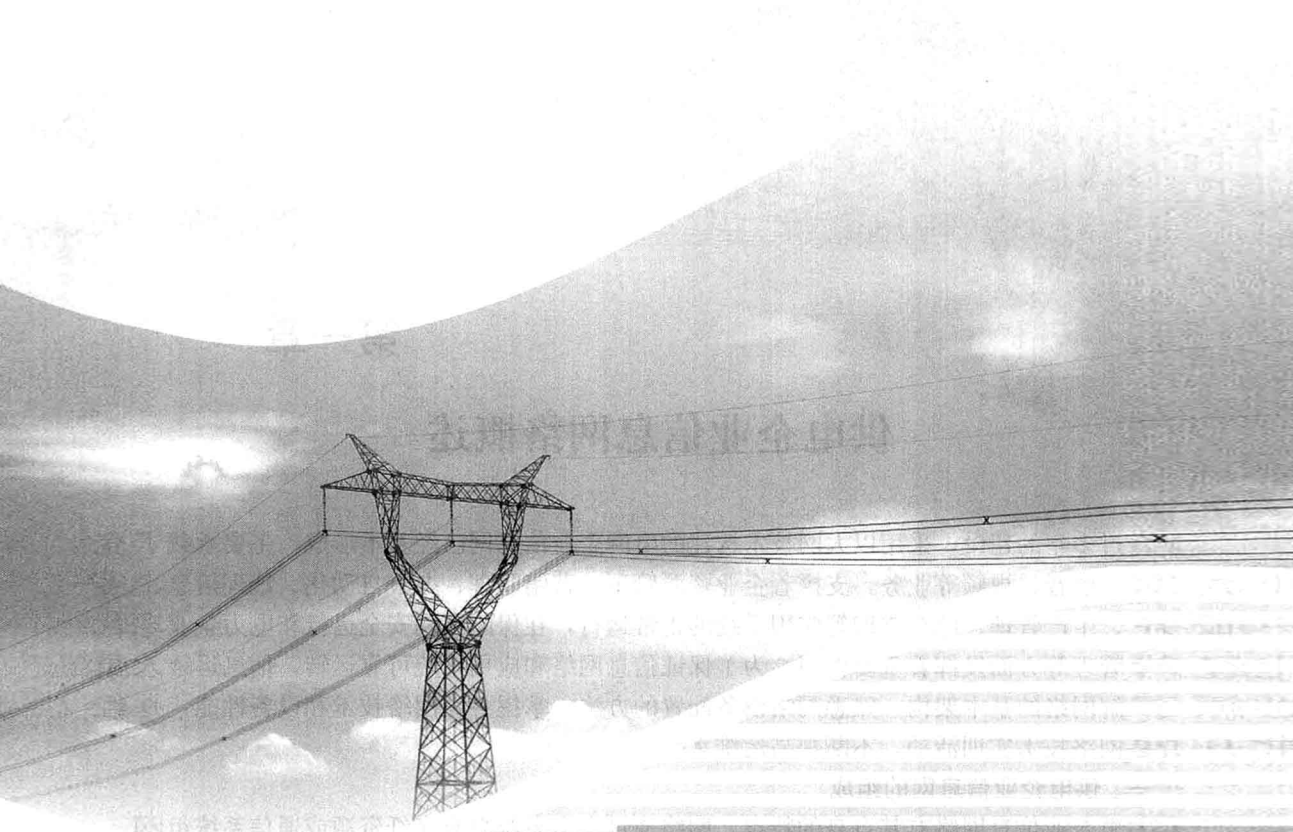
限于编者水平，书中难免存在疏漏和不足之处，恳请读者批评指正。

编　者

2013 年 5 月



目　录



第一篇 基 础 篇

第一章

供电企业信息网络概述

经过多年的建设，采用以太网技术构建的电网企业信息网已经基本形成，主要承载了企业数据、语音、视频等业务，支撑着企业资源管理、营销管理、办公自动化、地理信息、客户服务、生产管理、综合查询等应用系统的正常运行，在保障电网安全运行和电力企业现代化经营管理等方面发挥着重要作用。为了保证信息网络和应用系统可靠运转，信息运维人员必须了解网络的基本架构，熟悉网络设备配置的方法，掌握各类网络技术和设备性能，并经常开展网络技术实训活动，不断提高运维水平。

一、供电企业信息网的组成

供电企业信息网络有其自身的特点，网络通过电力系统自有光纤资源或通信系统组网。

根据信息网络的业务类型，电网企业网络主要分为信息内网和信息外网，信息内网和信息外网之间一般通过 MPLS VPN 技术进行逻辑强隔离。信息内网是公司内部信息业务应用承载网络和内部办公网络。信息外网是公司对外业务应用承载网络和访问互联网用户终端网络。同时电网企业中的电力调度、电量采集等各类业务形成了不同规模的业务系统专用信息网络，这些网络通过各种隔离方式与信息内/外网进行受控的数据交换。

二、网络架构

在电网信息网络的构建中，合理划分网络层次结构是网络稳定、高效运行的保证。为减少网络各部分的相关性，便于网络的实施及管理，应对网络进行层次化设计。

供电企业信息网的组成按架构层级分为骨干网和本地网，骨干网是用于连接公司各区域本地网的高速信息网，按连接区域分为一级、二级和三级骨干网。一级骨干网连接公司总部与各省（自治区、直辖市）电力公司；二级骨干网连接各省（自治区、直辖市）电力公司至所属地市公司；三级骨干网连接地市公司至所属县公司。本地网，是指各单位本部办公区所在地的局域网和城域网。本地网按其所在地域分为总部本地网、省本地网、地市本地网和县本地网；按组网结构又分为核心层、汇聚层和接入层。

如图 1-1-1 所示，骨干信息网络之间通过路由器进行连接，本地信息网大多数采用三层网络架构，核心层由两台核心交换机组成，并配置成双设备冗余模式，分别连接到骨干网路由器，通过 OSPF（最短路径优先）动态路由实现与上级设备的互联互通。两台核心交换机之间互联通过 CISCO 的 PORT Channel 技术，实现两条线路的捆绑，中心采用 Trunk 二层方式接入核心设备上。两台核心设备采用 HSRP 技术实现网关的冗余备份，由核心设备负责全网数据的路由处理及转发，链路上与核心交换机之间形成一个环路，以保证链路的冗余。

各级本地网络划分为核心层、汇聚层、接入层三个层次，虚拟分层示意图如图 1-1-2 所示。

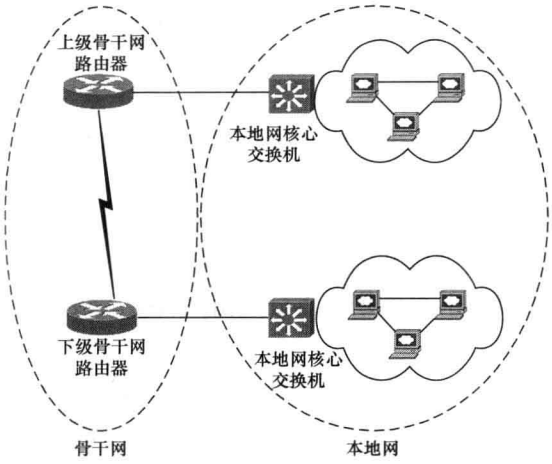


图 1-1-1　供电企业网络架构

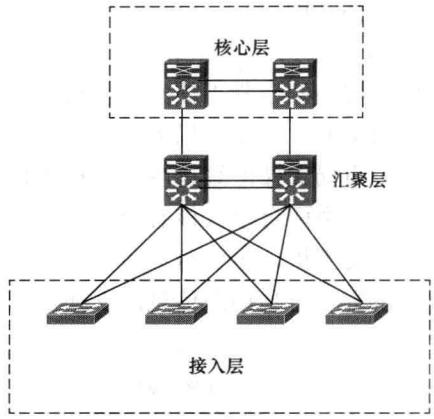


图 1-1-2　虚拟分层示意图

1. 核心层

核心层主要功能是给下层各业务汇聚节点提供 IP 业务平面高速承载和交换通道，负责进行数据的高速转发，同时实现与上级网络的互联，提供高速 IP 数据出口。核心层完成高速数据转发，结构重点考虑可靠性和可扩展性。城域信息应根据业务流向、流量、光纤资源等情况综合考虑核心层节点的数量和位置，同时应保证本地区数据中心和电力骨干广域网的高速接入。

核心层设备主要选择思科（Cisco）65、华为的 NE20 等系列。

为保证安全性和可靠性，核心层节点设备应该实现关键部件（包括引擎、电源和风扇等）冗余配置，必须采用无源背板，以避免机箱出现单点故障；所有单板和电源模块支持热插拔功能，必须能够支持防火墙、IPS 等安全业务板卡。在系统软件及硬件的支持下，关键部件在发生故障时能自动启动备份系统，而且主备部件之间的切换要能够实时热倒换，即运行中即使发生设备故障切换也不会对网络业务造成影响。核心层设备必须采用分布式体系架构，能够实现业务的快速无阻塞转发。无论这台设备的管理单元、交换转发单元，还是单一接口是否出现故障，都可以保证至少有部分路径是连通的，以降低设备故障带来的网络中断风险。

2. 汇聚层

汇聚层主要完成的任务是对各业务接入节点的业务汇聚、管理和分发处理。汇聚层起着承上启下的作用，对上连接至核心层，对下将各种宽带数据业务分配到各个接入层的业务节点。

汇聚层设备主要选择思科（Cisco）的 45、37，华为的 S5700 系列。

汇聚层节点的数量和位置应根据业务和光纤资源情况来选择。核心层节点与汇聚层节点可采用环行连接，每个汇聚层节点采用手拉手方式保证与两个不同的节点连接，形成自愈路由。

3. 接入层

接入层主要利用多种接入技术，迅速覆盖至用户节点，将不同地理分布的用户快速有效地接入到地区城域信息网骨干。对上连接至汇聚层和核心层，对下进行带宽和业务分配，实现用户的接入。

接入层设备主要选择思科的 29、36，华为的 S2700 系列。

三、供电企业信息网常见网络拓扑结构

供电企业信息网常见的网络拓扑结构有口字形、环形、树形，供电企业一般按照电力系

统光纤资源，综合利用这些拓扑结构，保证网络的冗余和可靠。下面介绍常见的供电企业信息网络拓扑结构。

1. 口字形网络拓扑结构

核心层为两台骨干核心交换机，负责各汇聚层间、与 Internet、省电力公司和兄弟单位间的路由交换。下接市局大楼汇聚节点、生产单位汇聚节点、变电站汇聚节点、县局汇聚节点。其中市局大楼汇聚点由两台接入核心交换机组成，主要负责市区范围内信息的交换。郊区汇聚节点由两台接入核心交换机组成，主要负责郊区范围内信息的交换。变电站汇聚点为接入核心交换机，主要负责各变电站信息的交换。县局汇聚节点分别由两台接入核心交换机组成，负责各自县局内信息的交换。

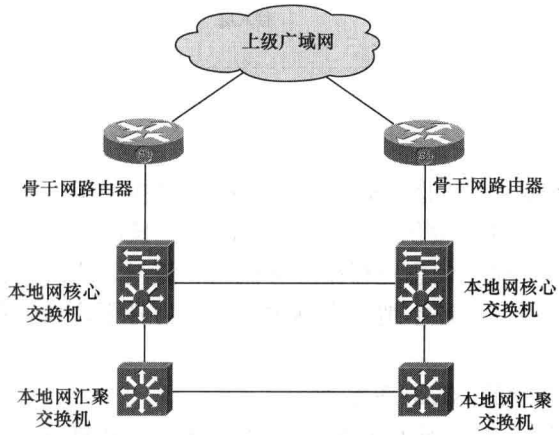


图 1-1-3 口字形网络拓扑结构图

核心层通过骨干路由器与 Internet、省电力公司和兄弟单位互联，在核心层设备骨干核心交换机和骨干路由器间安装两台防火墙，这两台防火墙工作在热备用方式。口字形网络拓扑结构如图 1-1-3 所示。

2. 环形网络拓扑结构

核心层为两台核心交换机，负责各汇聚层间、与 Internet、地市局和下属单位间的路由交换。网络拓扑成环状，同时有链路和子环，下接市局大楼汇聚节点、生产单位汇聚节点。其中，市局大楼汇聚点由楼层交换机组成，主要负责市局大楼范围内信息的交换。生产单位汇聚节点由两台楼层交换机组成，主要负责生产单位内信息的交换。环形网络拓扑结构如图 1-1-4 所示。

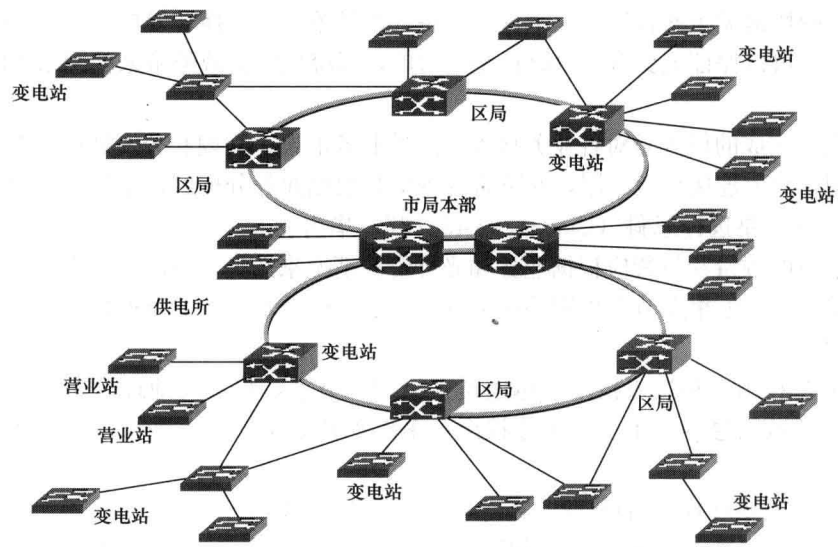


图 1-1-4 环形网络拓扑结构图

3. 星形网络拓扑结构

市局和县局主站配置各 1 台核心路由器和 1 台核心交换机，市局和县局的核心路由器采用传输的 155Mb/s POS 端口互连形成主干数据网，核心路由器和核心交换机采用千兆网互连。市局主站配置网管电脑 1 台，网管软件 1 套，对整个地区调度数据网进行监控和管理。

每个变电站配置 1 台路由器和 1 台 24 端口二层交换机，一个机柜，24 端口网配以及电源等附件。变电站路由器通过传输的 2Mb/s 链路与主站核心路由器互连，与变电站的调度数据网相联。变电站的路由器和交换机采用百兆网互连。星形网络拓扑结构如图 1-1-5 所示。

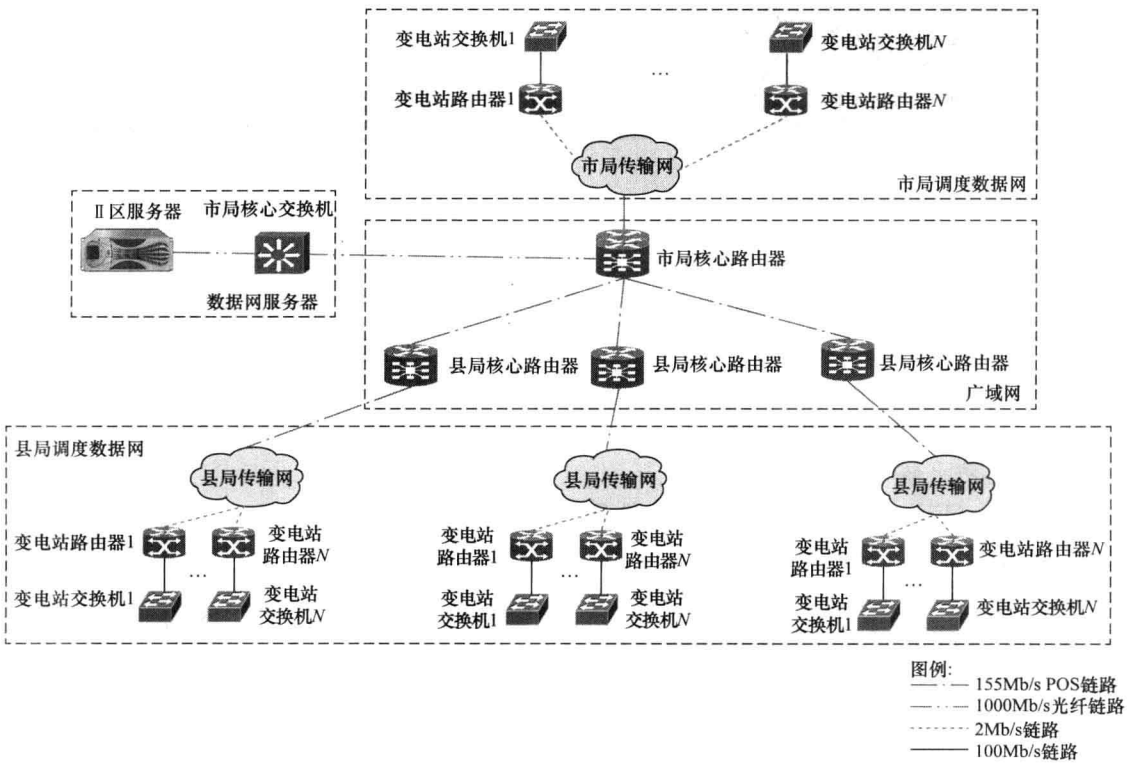


图 1-1-5　星形网络拓扑结构

四、供电企业信息网常用网络设备简介

1. 交换机

交换机（Switch）也称交换式集线器，是一种工作在 OSI 第二层（数据链路层）上的、基于 MAC（网卡的介质访问控制地址）识别、能完成封装转发数据包功能的网络设备。它通过对信息进行重新生成，并经过内部处理后转发至指定端口，具备自动寻址能力和交换作用。

（1）核心交换机。核心层交换机全部采用机箱式模块化设计，已经基本上设计了与之相配备的 1000Base-T 模块，同时带有路由功能，数据交换能力非常强。核心交换机如图 1-1-6 所示。

（2）接入交换机。接入层支持 1000Base-T 的以太网交换机基本上是固定端口式交换机，

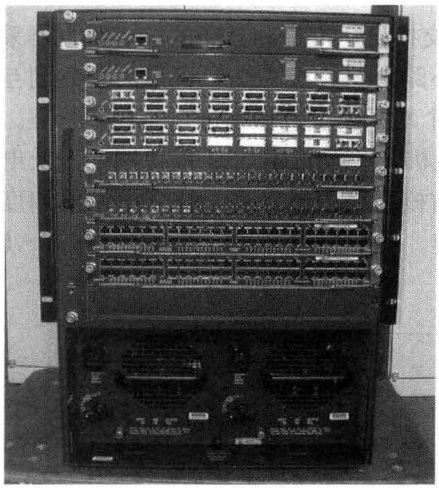


图 1-1-6 核心交换机

以 10/100Mb/s 端口为主，并且以固定端口或扩展槽方式提供 1000Base - T 的上联端口。汇聚层 1000Base - T 交换机同时存在机箱式和固定端口式两种设计，可以提供多个 1000Base - T 端口，一般也可以提供 1000Base - *X* 等其他形式的端口。接入层和汇聚层交换机共同构成完整的中小型局域网解决方案。接入交换机如图 1-1-7 所示。

2. 路由器

路由器（Router）是用于连接多个逻辑上分开的网络，逻辑网络是代表一个单独的网络或者一个子网。

图 1-1-7 接入交换机

当数据从一个子网传输到另一个子网时，可通过路由器来完成。因此，路由器具有判断网络地址和选择 IP 路径的功能，它能在多网络互联环境中建立灵活的连接，可用完全不同的数据分组和介质访问方法连接各种子网，路由器只接受源站或其他路由器的信息，属网络层的一种互联设备。它不关心各子网使用的硬件设备，但要求运行与网络层协议相一致的软件。一般核心层交换机都具备路由功能。

3. 网络防火墙

防火墙（Firewall）是指一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障。它是一种获取安全性方法的形象说法，它是一种计算机硬件和软件的结合，使 Internet 与 Intranet 之间建立起一个安全网关（Security Gateway），从而保护内部网免受非法用户的入侵。防火墙主要由服务访问规则、验证工具、包过滤和应用网关四部分组成。防火墙就是一个位于计算机和它所连接的网络之间的软件或硬件，该计算机流入流出的所有网络通信和数据包均要经过此防火墙。网络防火墙实物如图 1-1-8 所示。

网络防火墙部署示意如图 1-1-9 所示。

图 1-1-8 网络防火墙

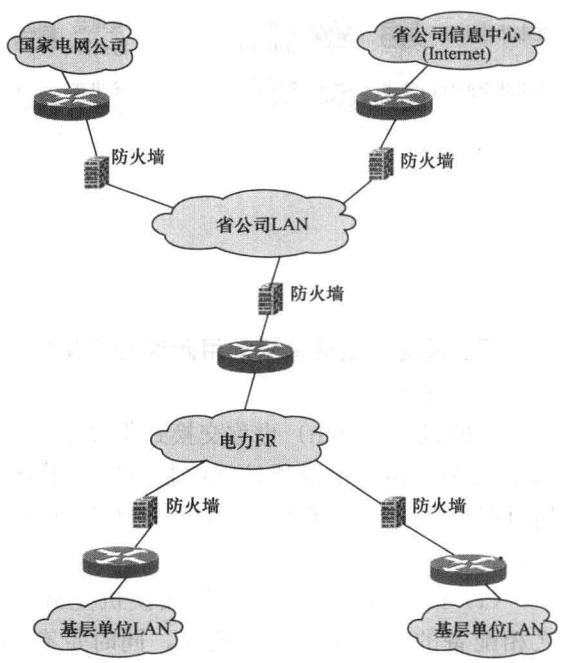


图 1-1-9 网络防火墙部署示意

4. 物理隔离装置

物理隔离装置就是现在所说的网闸。安全隔离网闸是一种由带有多种控制功能专用硬件在电路上切断网络之间的链路层连接，并能够在网络间进行安全适度的应用数据交换的网络安全设备。它与防火墙的区别是，防火墙一般在进行 IP 包转发的同时，通过对 IP 包的处理，实现对 TCP 会话的控制，但是对应用数据的内容不进行检查。这种工作方式无法防止泄密，也无法防止病毒和黑客程序的攻击。无论从功能，还是实现原理上来说，安全隔离网闸和防火墙是完全不同的两个产品，防火墙是保证网络层安全的边界安全工具（如通常的非军事化区），而安全隔离网闸重点是保护内部网络的安全。因此两种产品由于定位的不同，不能相互取代。物理隔离装置主要用于供电企业信息网不同区之间的隔离，实际上是专用的防火墙，因为它具有不公开性，所以很难被黑客攻击。实物及部署示意图如图 1-1-10 和图 1-1-11 所示。

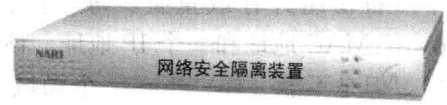


图 1-1-10　物理隔离装置

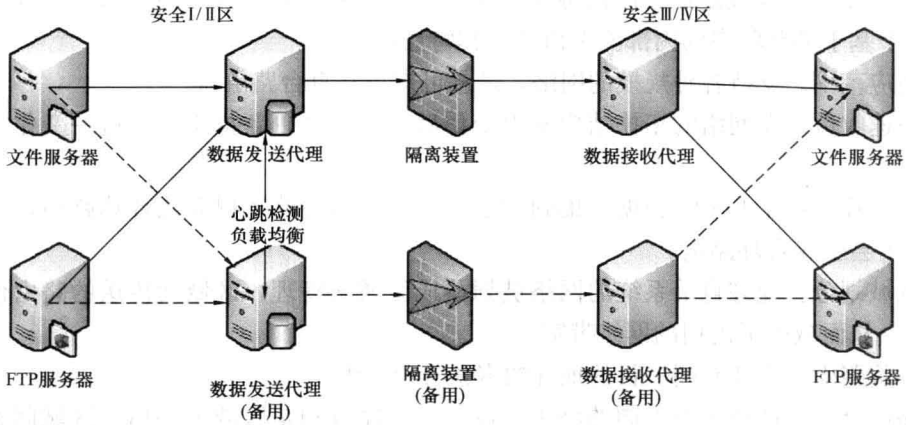


图 1-1-11　物理隔离装置的部署

五、网络技术简介

1. 交换技术在供电企业信息网中的应用

(1) STP 环网自愈技术。所有的楼层交换机和两个核心交换机都由两条链路连接，每个楼层交换机和两个核心交换机之间形成一个环形拓扑结构。在正常情况下，2 层环形结构容易形成广播风暴，造成整个网络的瘫痪，通过 Spanning Tree 生成树技术，自动在环形网络结构中选择一条最优化的路径作为传输数据的路径，状态为 Forwarding；另外一条通路作为备用，状态为 Blocking。当正常线路出故障时，状态为 Blocking 的线路可以马上切换为 Forwarding 状态，接管所有的数据通信，实现冗余功能。

(2) 双链路通道技术。两台核心交换机之间采用两条千兆线路连接，通过 Port Channel 技术，可以实现两条线路的捆绑，在正常情况下提供全双工千兆速率。可以实现冗余的技术，在其中一条线路出故障时，不会影响整个系统的运行，从而提高系统的可靠性。

(3) HSRP。热备份路由器协议（Hot Standby Router Protocol，HSRP），是 Cisco 平台的一种特有技术，是 Cisco 的私有协议。

实现 HSRP 的条件是系统中有多台路由器，它们组成一个“热备份组”，这个组形成一个虚拟路由器。在任一时刻，一个组内只有一个路由器是活动的，并由它来转发数据包，如果活动路由器发生了故障，将选择一个备份路由器来替代活动路由器，但是在本网络内的主机看来，虚拟路由器没有改变。所以主机仍然保持连接，没有受到故障的影响，这样就较好地解决了路由器切换的问题。为了减少网络的数据流量，在设置完活动路由器和备份路由器之后，只有活动路由器和备份路由器定时发送 HSRP 报文。如果活动路由器失效，备份路由器将接管成为活动路由器。如果备份路由器失效或者变成了活跃路由器，将由另外的路由器取代备份路由器。在一个实际的特定的局域网中，可能有多个热备份组并存或重叠。每个热备份组模仿一个虚拟路由器工作，它有一个 Well-known - MAC 地址和一个 IP 地址。该 IP 地址、组内路由器的接口地址、主机在同一个子网内，但是不能一样。当在一个局域网上有多个热备份组存在时，把主机分布到不同的热备份组，可以分担负载。

2. 路由、组播技术的应用

(1) OSPF。开放最短路径优先协议（Open Shortest Path First，OSPF）是 IETF 组织开发的一个基于链路状态的内部网关协议。其特性如下：

1) 适应范围。支持各种规模的网络，最多可支持几百台路由器。

2) 快速收敛。在网络的拓扑结构发生变化后立即发送更新报文，使这一变化在自治系统中同步。

3) 无自环。由于 OSPF 根据收集到的链路状态用最短路径树算法计算路由，从算法本身保证了不会生成自环路由。

4) 区域划分。允许自治系统的网络被划分成区域来管理，区域间传送的路由信息被进一步抽象，从而减少了占用的网络带宽。

5) 等价路由。支持到同一目的地址的多条等价路由。

6) 路由分级。使用 4 类不同的路由，按优先顺序分别是区域内路由、区域间路由、第一类外部路由、第二类外部路由。

7) 支持验证。支持基于接口的报文验证，以保证路由计算的安全性。

8) 组播发送。协议报文支持以组播形式发送。

(2) EIGRP。Enhanced Interior Gateway Routing Protocol，增强内部网关路由线路协议也称加强型内部网关路由协议。EIGRP 是 Cisco 公司的私有路由协议。Cisco 公司是该协议的发明者和唯一具备该协议解释和修改权的厂商。EIGRP 结合了链路状态和距离矢量型路由选择协议的 Cisco 专用协议，采用弥散更新算法（Diffusing Update Algorichi，DUAL）来实现快速收敛，可以不发送定期的路由更新信息以减少带宽的占用，支持 Appletalk、IP、Novell 和 NetWare 等多种网络层协议。它综合了距离矢量和链路状态两者的优点，其特点包括快速收敛、减少带宽占用、支持多种网络层协议、无缝连接数据链路层协议和拓扑结构。

(3) ISIS。中间系统到中间系统（Intermediate System to Intermediate System，IS - IS）是一种内部网关协议，是电信运营商普遍采用的内部网关协议之一，也是一个分级的链接状态路由协议。它基于 DECnet PhaseV 路由算法，实际上与 OSPF 非常相似，使用 Hello 协议寻找毗邻节点，使用一个传播协议发送链接信息。ISIS 可以在不同的子网上操作，包括

广播型的 LAN、WAN 和点到点链路。但是标准的 IS－IS 协议是为无连接网络服务（CLNS）设计的，并不直接适合于 IP 网络，因此互联网工程任务组制定了适用于 IP 网络的集成化的 IS－IS 协议，称为集成 IS－IS，它由 RFC 1195 等 RFC 文档所规范。由于 IP 网络的普遍存在，一般所称的 IS－IS 协议通常是指集成 IS－IS 协议。

（4）RIP。路由信息协议（RIP）是一种在网关与主机之间交换路由选择信息的标准。RIP 是一种内部网关协议。在国家性网络中如当前的因特网，拥有很多用于整个网络的路由选择协议。作为形成网络的每一个自治系统，都有属于自己的路由选择技术，不同的自治系统，路由选择技术也不同。RIP 的特点：①仅和相邻的路由器交换信息。如果两个路由器之间的通信不经过另外一个路由器，那么这两个路由器是相邻的。RIP 协议规定，不相邻的路由器之间不交换信息。②路由器交换的信息是当前路由器所知道的全部信息，即自己的路由表。③按固定时间交换路由信息，如每隔 30s，然后路由器根据收到的路由信息更新路由表（也可进行相应配置使其触发更新）。

（5）BGP。边界网关协议（BGP）是运行于 TCP 上的一种自治系统的路由协议。BGP 是唯一一个用来处理像因特网大小的网络协议，也是唯一能够妥善处理好不相关路由域间的多路链接的协议。BGP 构建在 EGP 经验之上。BGP 系统的主要功能是和其他的 BGP 系统交换网络可达信息。网络可达信息包括列出的自治系统（AS）的信息。这些信息有效地构造了 AS 互联的拓扑图并由此清除了路由环路，同时在 AS 级别上可实施策略决策。

（6）组播。（Multicast）传输：在发送者和每一接收者之间实现点对多点网络连接。如果一台发送者同时给多个接收者传输相同的数据，也只需复制一份相同的数据包。它提高了数据传送效率，减少了骨干网络出现阴塞的可能性。主机之间“一对一组”的通信模式，也就是加入了同一个组的主机可以接收到此组内的所有数据，网络中的交换机和路由器只向有需求者复制并转发其所需数据。主机可以向路由器请求加入或退出某个组，网络中的路由器和交换机有选择地复制并传输数据，即只将组内数据传输给那些加入组的主机。这样既能一次将数据传输给多个有需要（加入组）的主机，又能保证不影响其他不需要（未加入组）的主机的其他通信。

3. 安全技术在网络中的应用

（1）虚拟网技术。虚拟网技术主要基于近年来发展的局域网交换技术（ATM 和以太网交换）。交换技术将传统的基于广播的局域网技术发展为面向连接的技术。因此，网管系统有能力限制局域网通信的范围而无需通过路由器。由以上运行机制带来的网络安全的好处是显而易见的：信息只到达应该到达的地点。因此，防止了大部分基于网络监听的入侵手段。通过虚拟网设置的访问控制，使在虚拟网外的网络节点不能直接访问虚拟网内节点。但是，虚拟网技术也带来了新的安全问题：执行虚拟网交换的设备越来越复杂，从而成为被攻击的对象。基于网络广播原理的入侵监控技术在高速交换网络内需要特殊的设置。基于 MAC 的 VLAN 不能防止 MAC 欺骗攻击。以太网从本质上基于广播机制，但应用了交换器和 VLAN 技术后，实际上转变为点到点通信，除非设置了监听口，信息交换也不会存在监听和插入（改变）问题。但是，采用基于 MAC 的 VLAN 划分将面临假冒 MAC 地址的攻击。因此，VLAN 的划分最好基于交换机端口。但这要求整个网络桌面使用交换端口或每个交换端口所在的网段机器均属于相同的 VLAN。网络层通信可以跨越路由器，因此攻击可以从远方发起。IP 协议族各厂家实现的不完善，因此，在网络层发现的安全漏洞相对更多，

如 IP sweep、teardrop、sync-flood、IP spoofing 攻击等。

(2) 防火墙技术。网络防火墙技术是一种用来加强网络之间访问控制，防止外部网络用户以非法手段通过外部网络进入内部网络，访问内部网络资源，保护内部网络操作环境的特殊网络互联设备。它对两个或多个网络之间传输的数据包如链接方式按照一定的安全策略来实施检查，以决定网络之间的通信是否被允许，并监视网络运行状态。防火墙产品主要有堡垒主机、包过滤路由器、应用层网关（代理服务器）、电路层网关、屏蔽主机防火墙及双宿主机等类型。虽然防火墙是保护网络免遭黑客袭击的有效手段，但也有明显不足：无法防范通过防火墙以外的其他途径的攻击，不能防止来自内部变节者和不经心的用户带来的威胁，也不能完全防止传送已感染病毒的软件或文件，以及无法防范数据驱动型的攻击。防火墙处于 5 层网络安全体系中的最底层，属于网络层安全技术范畴。在这一层上，所有的 IP 是否都能访问到企业的内部网络系统。如果是，则说明企业内部网还没有在网络层采取相应的防范措施。作为内部网络与外部公共网络之间的第一道屏障，防火墙是最先受到人们重视的网络安全产品之一。虽然从理论上看，防火墙处于网络安全的最底层，负责网络间的安全认证与传输，但随着网络安全技术的整体发展和网络应用的不断变化，现代防火墙技术已经逐步走向网络层之外的其他安全层次，不仅要完成传统防火墙的过滤任务，同时还能为各种网络应用提供相应的安全服务。另外，还有多种防火墙产品正朝着数据安全与用户认证，防止病毒与黑客入侵等方向发展。

(3) 病毒防护技术。病毒历来是信息系统安全的主要问题之一。由于网络的广泛互联，病毒的传播途径和速度加快。病毒的途径主要通过 FTP、电子邮件、移动介质、Web 浏览等传播。

病毒防护的主要技术如下：

1) 阻止病毒的传播。在防火墙、代理服务器、SMTP 服务器、网络服务器、群件服务器上安装病毒过滤软件。在桌面个人计算机（Personal Computer，PC）上安装病毒监控软件。

2) 检查和清除病毒。使用防病毒软件检查和清除病毒。

3) 病毒数据库的升级。病毒数据库应不断更新，并下载到桌面系统。

4) 在防火墙、代理服务器及 PC 上安装 Java 及 ActiveX 控制扫描软件，禁止未经许可的控件下载和安装。

(4) 入侵检测技术。利用防火墙技术，经过仔细地配置，通常能够在内外网之间提供安全的网络保护，降低网络安全风险。但是，仅仅使用防火墙、网络安全还远远不够。入侵检测系统是近年来出现的新型网络安全技术，目的是提供实时的入侵检测及采取相应的防护手段，如记录证据用于跟踪和恢复、断开网络连接等。实时入侵检测能力之所以重要，是因为它能够对付来自内部网络的攻击，并能够缩短发现黑客入侵的时间。

(5) 安全扫描技术。网络安全技术中，另一类重要技术为安全扫描技术。安全扫描技术与防火墙、安全监控系统互相配合能够提供很高安全性的网络。安全扫描工具源于发现黑客在入侵网络系统时采用的工具。商品化的安全扫描工具为网络安全漏洞的发现提供了强大的支撑。安全扫描工具通常也分为基于服务器和基于网络的扫描器。基于服务器的扫描器主要扫描服务器相关的安全漏洞，如密码文件、目录和文件权限、共享文件系统、敏感服务、软件、系统漏洞等，并给出相应的解决办法和建议。通常，与相应的服务器操作系统紧密相

关。基于网络的安全扫描主要扫描设定网络内的服务器、路由器、网桥、变换机、访问服务器、防火墙等设备的安全漏洞，并可设定模拟攻击，以测试系统的防御能力。

(6) 认证和数字签名技术。认证技术主要解决网络通信过程中通信双方的身份认可，数字签名作为身份认证技术中的一种具体技术，同时数字签名还可用于通信过程中的不可抵赖要求的实现。认证技术将应用到企业网络中的以下方面：

1) 路由器认证。路由器和交换机之间的认证。

2) 操作系统认证。操作系统对用户的认证。

3) 网管系统对网管设备之间的认证。

4) VPN 网关设备之间的认证。

5) 拨号访问服务器与客户间的认证。

6) 应用服务器（如 Web Server）与客户的认证。

7) 电子邮件通信双方的认证。

(7) VPN 技术。企业总部和各分支机构之间采用 Internet 网络进行连接，由于 Internet 是公用网络，因此，必须保证其安全性。我们将利用公共网络实现的私用网络称为虚拟私用网（VPN)。因为 VPN 利用了公共网络，所以其最大的弱点在于缺乏足够的安全性。企业网络接入 Internet，主要的危险是来自 Internet 的未经授权的对企业内部网信息的存取，信息可能受到窃听和非法修改。