ZIDONGHUA JIANKONGXITONG
SHICAOJINENG JINGSAI SHILI JIEXI

自动化监控系统
实操技能竞赛实例解析

上海市电力公司　组编

中国电力出版社
CHINA ELECTRIC POWER PRESS

ZIDONGHUA JIANKONGXITONG
SHICAOJINENG JINGSAI SHILI JIEXI

自动化监控系统
实操技能竞赛实例解析

上海市电力公司　组编

中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

本书阐述了电网调度自动化系统基本原理与技术，并结合历年自动化专业竞赛经验，详细讲解了目前较有代表性的RCS-9700、NS2000、CSC2000三套厂站端监控系统的构成原理及各环节调试方法，还分别对各自系统的常见故障进行了分析，以满足现场调试与竞赛培训的需要。

本书可供电网及厂站端调度自动化专业的人员学习参考。

图书在版编目（CIP）数据

自动化监控系统实操技能竞赛实例解析 / 上海市电力公司组编. —北京：中国电力出版社，2013.9

ISBN 978-7-5123-4549-2

Ⅰ. ①自… Ⅱ. ①上… Ⅲ. ①电气设备－自动化监测系统 Ⅳ. ①TM76

中国版本图书馆CIP数据核字（2013）第121019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）

北京市同江印刷厂印刷

各地新华书店经售

*

2013年9月第一版 2013年9月北京第一次印刷

880毫米×1230毫米 16开本 20印张 632千字

印数 0001—2000册 定价 **65.00** 元（含1DVD）

编　委　会

序

电力系统是迄今为止人类发明的最庞大、最复杂的人工智能系统。特别是以特高压、大容量、远距离甚至超远距离电力传输为特征，高度依赖各种自动监视和控制手段，并逐渐具备大规模清洁能源接入能力，向智能电网时代过渡的现代电力系统的运行更是瞬息万变，相应的电网运行风险也不断增大。近10年来，在世界上一些工业化与发展中国家，大停电事故此起彼伏，如2003年美加大停电、2012年印度大停电，使当地的工农业生产停滞、社会秩序一度陷入混乱，人民生活极其不便。事后寻找这些大停电事故的深层次的原因，除了常规的电力系统网架固有缺陷、设备故障、自然灾害等因素外，关键时刻电力调度实时信息缺失，电力调度水平落后也有一定的关系。

为打造统一坚强的智能电网，我们需要构建精益专业的设备运维体系，对电网重要资源实现全面监控与管控，以保证设备的安全稳定运行。自动化监控系统是作为电网一线主设备信号采集，集成、上送与远方控制后最终执行的系统，这些系统的运行状态与运行水平直接影响到电网的监控与调度水平。为使电网内运行的自动化监控系统充分发挥作用，培养一支内功深厚的自动化专业人才队伍已是当务之急，这些专业人员要熟悉并掌握自动化监控系统的性能，正确合理地配置系统内各环节的装置，发现问题故障能在最短时间内排除，这样才能最大限度地保障系统的安全稳定运行。

本书的出版正是基于上述目的，望能为自动化工作提供一定借鉴。

藉此受托之际，欣然作序，以与广大共建坚强智能电网同仁共勉。

上海市电力公司副总经理

前 言

当前，电网调度自动化系统对保障电网的安全稳定运行发挥着日益重要的作用。随着大运行体系的深入，电网智能化的发展，调度自动化系统的更新换代，如何对现有系统进行高效、可靠的运行维护与检修调试，成为当务之急。为了提高从业人员专业素养，加快自动化专业与其他技术专业的融合，特编写此书。

本书阐述了电网调度自动化系统的基本原理与技术，并结合历年自动化专业竞赛经验，详细介绍了目前较有代表性的RCS-9700、NS2000、CSC2000三套厂站端监控系统，对其构成原理及各环节调试方法进行了范例演示，还分别对各自系统的常见故障进行了总结，以满足现场调试与竞赛培训的需要。

成书仓促，不足之处，敬请批评指正。

编 者

2013 年 5 月

目 录

第四部分 CSC2000 型综合自动化系统

第一部分

网络与传动

本部分介绍了网络基础知识，并结合一个简化的电力系统主站—厂站网络拓扑实例，简要介绍了常用的远动通信规约：IEC60870-5-101、IEC 60870-5-104 以及 CDT 规约，使大家能够对这些规约报文进行简单的阅读及分析。通过介绍国电南瑞科技公司 NSC300 总控、南瑞继保公司 RCS-9798 通信装置及北京四方公司 CSC1320 远动装置的参数配置，使读者对网络在电力系统中的应用有一定的了解，以便能更好地进行后续章节的阅读。

1 网络基础知识介绍

1.1 网络模型

1.1.1 OSI 参考模型

OSI（Open System Interconnection，开放式系统互联）参考模型是一个逻辑上的定义、一个规范，它把网络从逻辑上分为了 7 层。每一层都有相关、相对应的物理设备，如路由器、交换机。

OSI 参考模型通过 7 个层次化的结构模型使不同系统不同网络之间实现可靠的通信，因此其最主要的功能使就是帮助不同类型的主机实现数据传输。OSI 7 层模型由下至上分别为物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。

物理层：主要定义物理设备标准，如网线的接口类型、光纤的接口类型、各种传输介质的传输速率等。它的主要作用是传输比特流（就是由 1、0 转换为电流强弱来进行传输，到达目的地后再转换为 1、0，即模数转换与数模转换）。这一层的数据叫做比特。

数据链路层：主要将从物理层接收的数据进行 MAC 地址（网卡的地址）的封装与解封装。在这一层工作的设备叫做二层设备（如交换机），常把这一层的数据叫做帧。

网络层：主要将从下层接收到的数据进行 IP 地址（例 192.168.0.1）的封装与解封装。在这一层工作的设备叫做三层设备（如路由器），常把这一层的数据叫做数据包。

传输层：定义了一些传输数据的协议和端口号，如：TCP（Transmission Control Protocol，传输控制协议）、UDP（User Datagram Protocol，用户数据包协议）。主要将从下层接收的数据进行分段进行传输，到达目的地址后再进行重组。常把这一层数据叫做段。

会话层：通过传输层建立数据传输的通路，主要在系统之间发起会话或接受会话请求（设备之间需要互相认识，可以是 IP 也可以是 MAC 或是主机名）。

表示层：主要对接收的数据进行解释、加密与解密、压缩与解压缩等（也就是把计算机能够识别的东西转换成人能够能识别的东西，如图片、声音等）。

应用层：主要是一些终端的应用，如 FTP（各种文件下载）、WEB（IE 浏览）、QQ 等。

1.1.2 TCP/IP 参考模型

OSI 是最早提出的理论标准，但是实际中多采用 TCP/IP 协议分层标准。TCP/IP 通常被认为是一个 4 层协议系统，是一组不同协议组合在一起构成的协议族。表 1.1.1 为 TCP/IP 协议族与 OSI 7 层协议的对应关系。

表 1.1.1　　TCP/IP 协议族与 OSI 7 层协议的对应关系

OSI 模型	TCP/IP 模型	常用协议
应用层	应用层	HTTP，FTP
表示层		
会话层		
传输层	传输层	TCP，UDP
网络层	互联网络层	IP，ICMP
数据链路层	链路层	PPP
物理层		

1.2 IP 地址简介及计算方法

1.2.1 IP 地址的组成及分类

Internet 上的每台主机都有一个唯一的 IP 地址，IP 协议就是使用这个地址在主机之间传递信息，这

是 Internet 能够运行的基础。目前常用的 IP 长度为 32 位，包括网络号和主机号两部分。网络号对于连接到网络上的所有设备来说是公共的，它唯一地标识了数据链路（即网络），而主机号唯一地标识了连接到网络上的特殊设备。

IP 地址可分为五类：

A 类地址：网络号为第一个 8 位数组，第一个字节以“0”开始，因此 A 类地址的范围为 1.0.0.0～126.255.255.255，其中网络号为 127 的地址留作他用。一般 A 类地址用于大型互联网络。

B 类地址：网络号为前两个 8 位数组，第一个字节以“10”开始，因此 B 类地址的范围为 128.0.0.0～191.255.255.255。一般 B 类地址用于中型互联网络。

C 类地址：网络号为前 3 个 8 位数组，第一个字节以“110”开始，因此 C 类地址的范围为 192.0.0.0～223.255.255.255。一般 C 类地址用于小型互联网络系统。

D 类地址：第一个 8 位数组以“1110”开始，因此 D 类地址的范围为 224.0.0.0～239.255.255.255，通常 D 类地址作为组播地址。

E 类地址：第一个 8 位数组以“11110”开始，E 类地址一般用于科学研究。

IP 地址划分方法如图 1.1.1 所示。

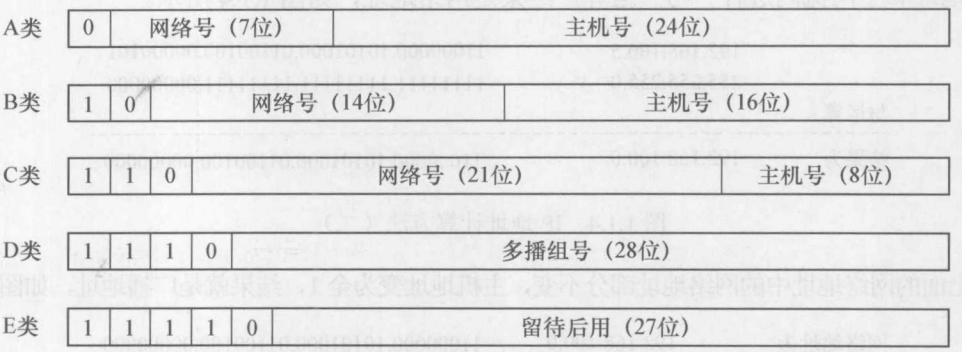

图 1.1.1 IP 地址划分方法

为了解决 IP 地址的不足和在一定程度上保障网络的安全，因特网域名分配组织 IANA 规定了 3 个内部保留地址段：10.0.0.0～10.255.255.255、172.16.0.0～172.31.255.255、192.168.0.0～192.168.255.255。

IP 地址用于唯一标识一台网络设备，但并不是每一个 IP 地址都是可以使用的。一些特殊的 IP 地址被用于各种各样的用途。主机号全为“0”的 IP 地址称为网络地址，用来标识一个网段，例如，C 类地址 192.168.1.0 表示的是网络号为 192.168.1 的网段。主机号全为“1”的 IP 地址称为网段广播地址，标识一个网络的所有主机，广播地址用与向本网段的所有节点发送数据包。例如，192.168.1.255、10.255.255.255 等，路由器可以在 192.168.1.0 及 10.0.0.0 等网段转发广播包。全“0”的 IP 地址 0.0.0.0 代表所有的主机，路由器用 0.0.0.0 地址指定默认路由。全“1”的 IP 地址 255.255.255.255 也是广播地址，但 255.255.255.255 代表所有主机，用于向网络的所有节点发送数据包，但这样的广播不能被路由器转发。

1.2.2 子网划分

每一个设备和接口都将被分配一个唯一的、主机号明确的地址，同时还要确定它所属的网络，这就是子网掩码的作用。子网掩码是一个 32 位的字串，与 IP 地址的每一位对应。A 类地址的默认子网掩码为 255.0.0.0，B 类地址的默认子网掩码为 255.255.0.0，C 类地址的默认子网掩码为 255.255.255.0。

为了提高 IP 地址的利用率，可将网络分成多个不同大小的子网，每个子网可以使用不同长度的子网掩码，即可变长子网掩码（Variable Length Subnet Mask，VLSM），它将一个 IP 地址划分为网络号、子网号、主机号。VLSM 的作用就是在 IP 地址的基础上，从它们的主机号部分借出相应的位数来做子网号，也就是增加网络号的位数，如图 1.1.2 所示。

各类网络可以用来再划分子网的位数为：A 类 24 位，B 类 16 位，C 类 8 位。可以再划分的位数就是主机号的位数，实际上是不能都借出来，因为 IP 地址中必须要有主机号的部分，而且主机号部分剩下一位是没有意义的。所以，在实际中可以借的位数是上面所写的各类网络地址位数再减去 2（如 A 类网

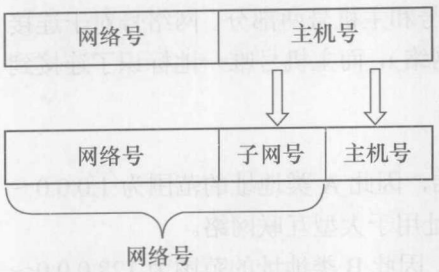

图 1.1.2 子网划分

络实际可借的位数为 22 位），借的位作为子网部分。

1.2.3 IP 地址的计算方法

通过前面的介绍，可以知道，一个唯一的网络地址应该由 IP 地址和子网掩码组成，才能确定这个地址的网络号、主机号。下面通过一个实例来介绍 IP 地址的计算方法。

例：IP 地址为 192.168.100.5，子网掩码是 255.255.255.0（也可表示为 192.168.100.5/24，即子网掩码为 24 位），请算出网络地址、广播地址、地址范围、主机数。

（1）将 IP 地址和子网掩码换算为二进制，子网掩码连续全 1 的是网络号，后面的是主机号。虚线前为网络号，虚线后为主机号，如图 1.1.3 所示。

```
192.168.100.5      11000000.10101000.01100100.00000101
255.255.255.0      11111111.11111111.11111111.00000000
```

图 1.1.3 IP 地址计算方法（一）

（2）IP 地址和子网掩码进行“与”运算，结果是网络地址，如图 1.1.4 所示。

```
                192.168.100.5      11000000.10101000.01100100.00000101
                255.255.255.0      11111111.11111111.11111111.00000000
与运算
-------------------------------------------------------------------------
结果为          192.168.100.0      11000000.10101000.01100100.00000000
```

图 1.1.4 IP 地址计算方法（二）

（3）将上面的网络地址中的网络地址部分不变，主机地址变为全 1，结果就是广播地址，如图 1.1.5 所示。

```
网络地址为          192.168.100.0      11000000.10101000.01100100.00000000
-------------------------------------------------------------------------
将主机地址变为全1
广播地址为          192.168.100.255    11000000.10101000.01100100.11111111
```

图 1.1.5 IP 地址计算方法（三）

（4）地址范围就是含在本网段内的所有主机，网络地址+1 即为第一个主机地址，广播地址–1 即为最后一个主机地址。由此可以看出，地址范围是 192.168.100.1～192.168.100.254，即这些地址都是一个网段的。

（5）主机的数量：主机的数量=$2^{\text{二进制的主机位数}}$–2，减 2 是因为主机不包括网络地址和广播地址。本例中二进制的主机位数是 8 位，则主机的数量=2^8–2=254。

1.3 路由技术基础

1.3.1 路由的概念和分类

路由就是通过互联的网络把信息从源地址传输到目的地址的过程。路由发生在 OSI 参考模型的第三层即网络层、TCP/IP 模型的互联网络层。路由规定了把信息包从一个地址发送到另外一个地址的路径。一条路由仅仅规定了主机到网关的一条路径，然后由网关把信息包转发到目的地的主机或者另一个网关。路由选择是指选择一条发送信息包的路径，而网关是指任何能够完成路由选择功能的网络设备，用来连接不同的网络。一个包从源地址到达目的地址的距离取决于它必须经过的网关跳（hop）数。一台主机到它直联网的跳数为零，如果通过一个网关就能就能到达指定的网络，则它到该网络的跳数为 1，依此类推。

路由分为直连路由、静态路由和动态路由三种。

直连路由是由链路层协议发现的，一般是指去往路由器的接口地址所在网段的路径，该路径信息不需要网络管理员维护，也不需要路由器通过某种算法进行计算获得，只要该接口处于活动状态（active），路由器就会把通向该网段的路由信息填写到路由表中去，直连路由无法使路由器获取与其不直接相连的路由信息。

静态路由是由管理员在路由器进行手工配置的固定的路由，允许对路由的行为进行精确的控制，减少了网络流量，单向以及配置简单，但不能及时反应网络拓扑的变化。通常情况下的静态路由的优先级最高。

动态路由是网络中的路由器之间根据实时网络拓扑变化，相互通信传递路由信息，利用收到的路由信息通过路由选择协议计算，及时更新路由表的过程。动态路由减少了管理任务，但对网络设备资源的消耗较大。

1.3.2 路由协议

路由可以静态配置（静态路由），也可以通过路由协议自动生成。路由协议能够自动发现和计算路由，并在拓扑变化时自动更新，无需人工维护，适用于复杂的网络。

路由协议的基本原理是：

（1）网络中所有路由器须实现相同的某种路由协议并已经启动该协议；

（2）邻居发现：路由器通过发送广播报文或发送给指定路由器邻居以主动把自己介绍给网段内的其他路由器；

（3）路由交换：每台路由器将自己已知的路由相关信息发送给相邻的路由器；

（4）路由计算：每台路由器运行某种算法，计算出最终的路由；

（5）路由维护：路由器之间通过周期性地发送协议报文来维护邻居信息。

路由协议分为内部网关协议（IGP）和外部网关协议（EGP）两种。在同一自治域（AS）内部使用的路由协议称为内部网关协议；在不同的自治域使用的路由协议称为外部网关协议（EGP），其关系如图 1.1.6 所示。这里的自治域是指一个具有统一管理机构、统一路由策略的网络。常用的内部网关协议有 RIP、OSPF、IS-IS、IGRP 等，常用的外部网关协议是 BGP 和 BGP-4。

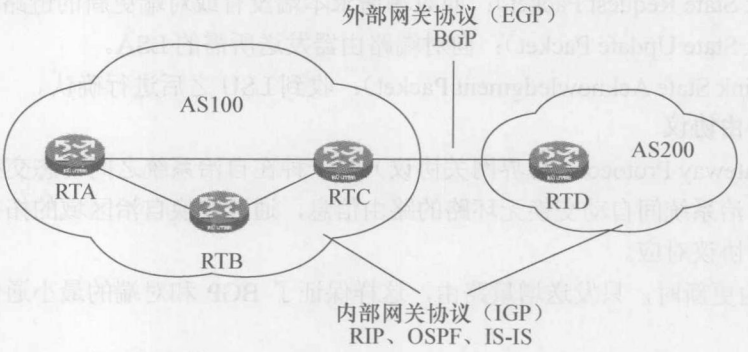

图 1.1.6 路由协议关系图

1.3.2.1 RIP 路由协议

RIP（Routing Information Protocol，路由信息协议）是一种基于距离矢量算法的路由协议，它通过 UDP 交换路由信息，每隔 30s 向外发送一次更新报文，如果在 180s 内没有收到来自对端的路由更新报文，则将所有来自次路由器的路由信息标识为不可达；如果在其后 120s 内仍未收到更新报文，则将该条路由从路由表中删除。RID 是一种相对简单的动态路由协议，在实际中应用广泛。RIP 协议有以下技术特点：

（1）选用跳数作为唯一的路由选择度量标准；

（2）跳数允许的最大值是 15，如果路由器收到了一个跳数值为 16 的路由更新信息，则其目标网络是不可达的；

（3）缺省情况下，每 30s 广播一次路由更新数据。

1.3.2.2 OSPF 路由协议

OSPF（Open Shortest Path First，开放最短路径优先）是一种内部网关协议，它通过路由器之间通告网络接口的状态来建立链路状态数据库，生成最短路径树，每个 OSPF 路由器使用这些最短路径构造路由表。OSPF 是 Internet 路由选择协议的一种，也是目前构建大型网络最常用的路由选择协议，并且不容易受到有害路由信息的影响。

OSPF 被设计为运行在一个单独的自治系统（AS）内部，每个 OSPF 路由器维持一个相同的数据库

描述自治系统的拓扑。通过这个数据库，一个路由表通过创建一个最短路径树来计算得到。OSPF 在拓扑变化时会利用路由协议流量的最小值很快地重新计算路径。

OSPF 协议的特点是：

（1）可适应大规模网络，OSPF 支持各种规模的网络，最多可支持几百台路由器。

（2）路由变化收敛速度快，如果网络的拓扑结构发生变化，OSPF 立即发送更新报文，使这个变化在自治系统中同步。

（3）无路由自环，由于 OSPF 通过收集到的链路状态用最短路径树算法计算路由，因此算法本身不会产生自环路由。

（4）对可变长子网掩码提供很好的支持。

（5）支持到同一目的地址的多条等值路由。

（6）允许自治系统的网络被划成区域来管理。

（7）提供路由分级管理，OSPF 使用 4 类不同的路由，按优先顺序来说分别是区域内路由、区域间路由、第一类外部路由、第二类外部路由。

（8）支持基于接口的报文验证以保证路由计算的安全性。

（9）支持以组播地址发送协议报文，既起到了广播的作用，又最大限度地减少了对其他网络设备的干扰。

OSPF 协议有五种协议报文，分别是 HELLO 报文、DD 报文、LSR 报文、LSU 报文和 LSAck 报文。

HELLO 报文：用来发现及维持邻居关系，选举指定路由器（DR）、备用指定路由器（BDR）。

DD 报文（Database Description Packet）：用来描述本地链路状态数据库（LSDB）的情况。

LSR 报文（Link State Request Packet）：向对端请求本端没有或对端更新的链路状态广播（LSA）。

LSU 报文（Link State Update Packet）：向对端路由器发送所需的 LSA。

LSAck 报文（Link State Acknowledgment Packet）：收到 LSU 之后进行确认。

1.3.2.3 BGP 路由协议

BGP（Border Gateway Protocol，边界网关协议）是一种在自治系统之间动态交换路由信息的路由协议，它的功能是在自治系统间自动交换无环路的路由信息，通过交换自治区域的拓扑图，从而消除路由环路并使内部运行的协议对应。

BGP 协议在路由更新时，只发送增量路由，这样保证了 BGP 和对端的最小通信量，但同时增加了 BGP 的复杂程度。

BGP 相邻路由器之间的会话是建立在 TCP 协议之上的。TCP 协议提供一种可靠的传输机制，支持以下两种类型的会话：

- 外部 BGP（EBGP）：是在属于两个不同的自治系统的路由器之间的会话。这些路由器是毗邻的，共享相同的介质和子网。
- 内部 BGP（IBGP）：是在一个自治系统内部路由器之间的会话。它被用来在自治系统内部协调和同步寻找路由的进程。BGP 路由器可以在自治系统的任何位置，甚至中间可以相隔数个路由器。

BGP 有四种报文类型，分别是 Open 报文、KeepAlive 报文、Update 报文和 Notification 报文。通过 TCP 建立 BGP 连接时，发送 Open 报文；建立连接后，如果有路由需要发送或路由变化时，发送 Update 报文通告对端路由信息；稳定后，需要定时发送 KeepAlive 报文以保持 BGP 连接的有效性；当本地 BGP 在运行中发现错误时，要发送 Notification 报文通告 BGP 对端。

1.3.2.4 MPLS

MPLS（Multi-Protocol Label Switching，多协议标签交换）是一种用于快速数据包交换和路由的体系，它为网络数据流量提供了目标、路由、转发和交换等能力。与传统 IP 路由方式相比，它在数据转发时，只在网络边缘分析 IP 报文头、而不用在每一跳都分析 IP 报文头，从而节约了处理时间。

MPLS 的标签转发，通过 LDP（Label Distribution Protocol，标签分发协议）事先分配好的标签，为报文建立了一条 LSP（Label Switching Path，标签转发通道）。在通道经过的每一台设备处，只需要进行快速的标签交换即可（一次查找），如图 1.1.7 所示。

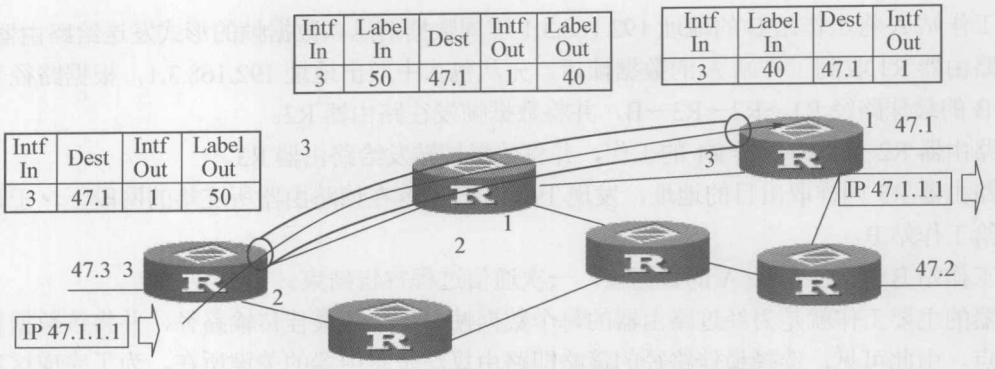

图 1.1.7 MPLS 标签转发

1.3.3 VPN 技术

VPN（Virtual Private Network）即为虚拟专用网络，定义为通过一个公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。使用这条隧道可以对数据进行几倍加密达到安全使用互联网的目的。VPN 是对企业内部网的扩展，可以帮助远程用户建立可信的安全连接，并保证数据的安全传输。图 1.1.8 为电力系统中 VPN 的应用。

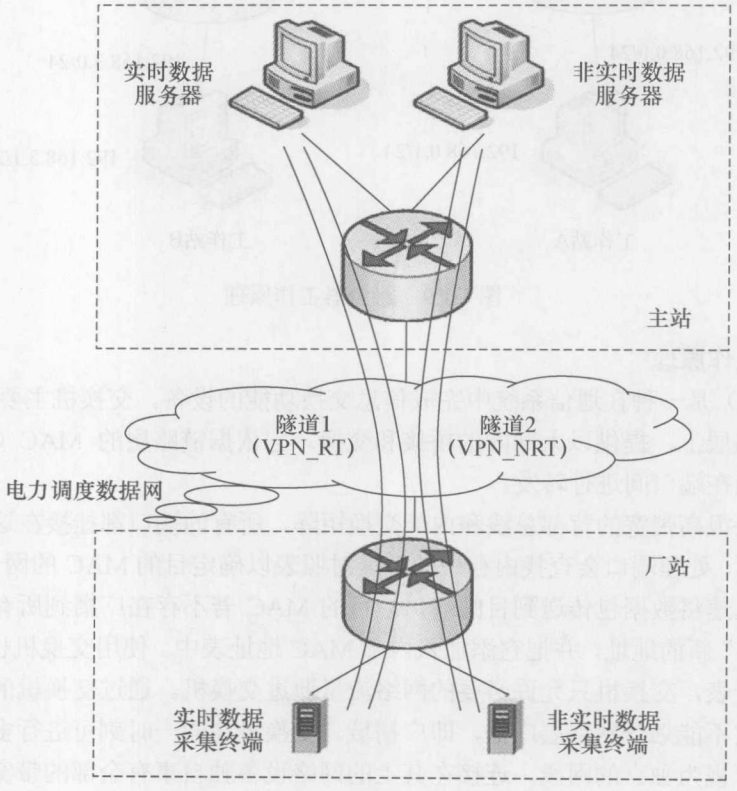

图 1.1.8 电力系统中 VPN 的应用

1.4 路由器、交换机及其操作系统介绍

1.4.1 路由器工作原理

路由器（Router）用于连接多个逻辑上分开的网络，所谓逻辑网络是代表一个单独的网络或者一个子网。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、交换和维护路由信息。路由器主要工作在 OSI 参考模型的物理层、数据链路层和网络层，根据网络层信息进行路由转发。同时，路由器提供丰富的接口类型，并支持多种链路层协议和路由协议。

其工作原理如图 1.1.9 所示，具体解释如下：

（1）工作站 A 将工作站 B 的地址 192.168.3.1 连同数据信息以数据帧的形式发送给路由器 R1。

（2）路由器 R1 收到工作站 A 的数据帧后，先从包头中取出地址 192.168.3.1，根据路径表计算出发往工作站 B 的最佳路径 R1→R2→R3→B，并将数据帧发往路由器 R2。

（3）路由器 R2 重复路由器 R1 的工作，并将数据帧转发给路由器 R3。

（4）路由器 R3 同样取出目的地址，发现 192.168.3.1 就在该路由器所连接的网段上，于是将该数据帧直接交给工作站 B。

（5）工作站 B 收到工作站 A 的数据帧，一次通信过程宣告结束。

路由器的主要工作就是为经过路由器的每个数据帧寻找一条最佳传输路径，并将该数据有效地传送到目的站点。由此可见，选择最佳路径的策略即路由算法是路由器的关键所在。为了完成这项工作，在路由器中保存着各种传输路径的相关数据——路由表（Routing Table），供路由选择时使用。路径表中保存着子网的标志信息、网上路由器的个数和下一个路由器的名字等内容。

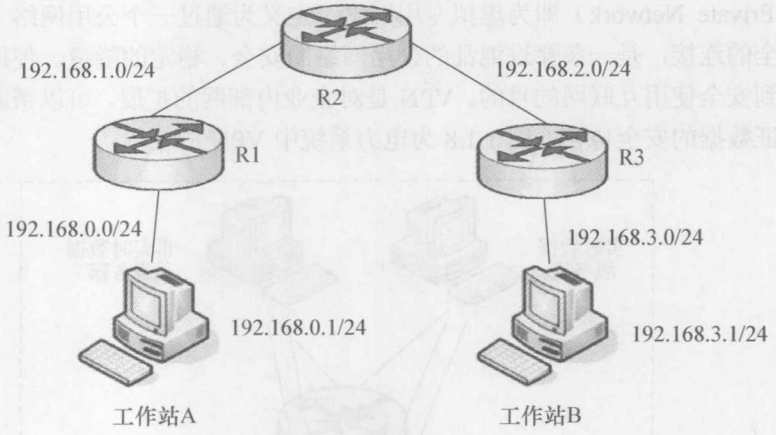

图 1.1.9　路由器工作原理

1.4.2　交换机工作原理

交换机（Switch）是一种在通信系统中完成信息交换功能的设备。交换机主要工作在 OSI 参考模型的物理层、数据链路层上，提供以太网间的桥接和交换。它依据链路层的 MAC（网卡的硬件地址）地址，将以太网数据帧在端口间进行转发。

交换机拥有一条很高带宽的背部总线和内部交换矩阵，所有的端口都挂接在这条背部总线上，控制电路收到数据包以后，处理端口会查找内存中的地址对照表以确定目的 MAC 的网卡挂接在哪个端口上，通过内部交换矩阵迅速将数据包传送到目的端口。目的 MAC 若不存在广播到所有的端口，接收端口回应后交换机会“学习”新的地址，并把它添加入内部 MAC 地址表中。使用交换机也可以把网络“分段”，通过对照 MAC 地址表，交换机只允许必要的网络流量通过交换机。通过交换机的过滤和转发，可以有效减少冲突域，但它不能划分网络层广播，即广播域。交换机在同一时刻可进行多个端口对之间的数据传输。每一端口都可视为独立的网段，连接在其上的网络设备独自享有全部的带宽，无须同其他设备竞争使用。总之，交换机是一种基于 MAC 地址识别，能完成封装转发数据包功能的网络设备。

交换机的主要功能包括物理编址、网络拓扑结构、错误校验、帧序列及流控。目前交换机还具备了一些新的功能，如对 VLAN（虚拟局域网）的支持、对链路汇聚的支持，甚至有的还具有防火墙。

虚拟局域网（Virtual Local Area Network，VLAN）是交换机一种比较常用的技术，是一组逻辑上的设备和用户。这些设备和用户不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样，由此得名虚拟局域网。VLAN 是一种比较新的技术，工作在 OSI 参考模型的第 2 层和第 3 层。一个 VLAN 就是一个广播域，VLAN 之间的通信是通过第 3 层的路由器来完成的。例如，在图 1.1.10 中，几个终端可能组成一个部分，其中可能包括实时数据服务器或非实时数据服务器。当终端的实际物理位置比较相近，可以组成一个局域网（LAN）；如果它们在不同的建筑物中，就可以通过 VLAN 将其聚合在一起。同一个 VLAN 中的端口可以接受