文章编号:1000 - 582X(2002)05 - 0033 - 05

现 代 网 络 设 计*

王达恩[1]，李敏基[2]，罗承志[3]
(1.重庆大学 计算机学院,重庆 400044; 2.重庆大学 机械学院,重庆 400044;
3. 深圳华安诚讯科技有限公司,深圳 518000)

摘　要:随着多媒体技术的广泛应用,信息社会迫切需要高速宽带计算机网络。文中讨论了如何利用网络分层设计、地址设计与路由选择来设计企业骨干网;如何利用配置 VPN 相关协议、开凿 VPN 隧道来规划虚拟专用网;如何利用服务运营平台设计、分配内部 IP 地址和配置网络安协议来设计智能小区网。指出利用现代网络设计方法来规划与设计计算机网络,可以满足人们对计算机网络技术向高速化、智能化、宽带化方向发展的需求。

关键词:骨干网; 虚拟专用网; 智能小区网; 网络设计
中图分类号:TP393.03　　**文献标识码**:A

随着因特网络终端数目的急剧增加,因特网信息的瓶颈现象日益严重,现代信息高速公路越来越需要结点少、处理速度高、传输速率快的互联网络中心骨干网;企业、社区、个人都需要宽带接入信息高速公路。

1 企业骨干网、大型 IP 网的设计

1.1 网络设计

1.1.1 网络逻辑结构

从网络拓扑结构上看,一般网络逻辑结构从内到外分为核心骨干层、分布层和接入层 3 大部分。网络与网络之间的不同只在于其规模的大小不同。核心层由核心路由器或第 3 层交换机构成高速干线连接,该层的关键是可靠性和速度;分布层由分布层路由器提供高端口密度,其任务是报文过滤、安全策略、服务质量 QoS 及地址转换等;接入层的路由器实现与其他设备的连接,提供网络访问。核心层一般由 10 ~ 50 个结点构成,应具有可扩展的路由功能和可管理性。在骨干网上实现的功能比较单一,一般采用 1 种路由协议、1 种传输介质,不处理包。核心骨干网仅进行内部连接,无客户接入以保证骨干网的安全[1]。

1.1.2 核心层骨干网设计

核心层骨干网有交换型、路由型(交换路由型)2 种。

对于交换型骨干网,核心的 ATM 或帧中继交换机被路由器包围着,需要维护 2 个层面上的网络。但第 3 层高功能交换机可提供数十至数百 Gbps 交换容量,还可取代传统的中央路由器,这是一种在普通交换机基础上增加了路由功能的第 3 层交换技术。

路由型骨干网只需要维护一个层面上的网络,路由器之间采用 HDLC 或 PPP 链路相连,具有更方便的路由选择和纠错能力,但需要路由器支持更多的端口。

路由型骨干网由若干快速路由交换机通过光纤连接而成,这些路由交换机集第 2 层(数据链路层)的交换技术和第 3 层的路由技术于一体,进行"先寻路后交换,一次路由,多次交换"。这是一种利用第 3 层协议来加强第 2 层交换功能的第 3 层交换技术。并采用多协议标记交换 MPLS(Multi - Protocol label Switching),大大提高路由器的转发速度[1-3]。

目前,核心层骨干网领域内采用第 3 层交换技术占有优势。由于成本高昂,采用 ATM 作为骨干网的企业和事业单位比较少。

核心层骨干网是高可靠的,它通常要考虑冗余部件(路由器/交换机机冗余、链路冗余)。若核心层骨干网是全双工千兆位以太网,应考虑链路聚合,以提供高可靠的链路、提高网络容量和可用性[4]。

核心骨干网的规划设计应与网络的发展现状同步。目前 10 Gb/s 高速路由交换机的标准和产品已出现,光纤网、四层以上交换机、目录服务、智能网管的出现,对网络分层设计产生重大影响。网络的规划设计除了要考虑网络的现状,还要考虑网络的扩展性。

大型 IP 网络设计与其类似,它可以作为 IDC (Internet Data Center)、ISP、ICP 等,向用户提供接入、宽

* 收稿日期:2002 - 01 - 10
作者简介:王达恩(1948 -),男,重庆人,重庆大学副教授,主要从事计算机网络领域研究工作。

带租用、服务器托管及其增值服务。建立大型 IP 网还需要考虑可靠性与成本的均衡,包括骨干网在内,从分布层到接入层、WAN 的链路、接入设备、服务层协议。

1.1.3 地址设计

IP 网络地址分为注册地址和非注册地址。如果要和 Internet 相连,则一定要用注册地址。在 IP 地址分配过程中要考虑如何分配用户地址、基础设施地址。一定要把基础设施地址段与用户地址段严格区分开来,否则会在管理过程中出现混乱。此外骨干网主机的 IP 地址前缀(网络号,子网号)应相同,属于同一子网[4]。

Internet 上的路由信息膨涨越来越快,约每 6 个月增加 1 倍,因此在路由过程中必须采用集中地址,合并路由项。对 IP 网络而言,对内对外都要有这种合并路由表项的能力。

如果用户想要更换 Internet 服务商,那么必须注意地址问题,因为不同的 Internet 服务商所提供的 IP 地址段不同,他们会根据地址过滤掉一些信息以免网络负担过重。

1.1.4 路由选择

路由协议分为内部路由协议和外部路由协议。内部路由协议 RIP 用于处理基础设施的路由,作用范围在一个自治域内,能够自动发现所有采用内部路由协议的路由器的信息,并且能够动态获得路由信息;外部路由协议 ERP(如 BGP)解决用户路由和 Internet 路由,用于在不同的自治域之间沟通路由信息,需要进行专门的配置。

在大型 IP 网络中一定需要外部路由协议,通过它可以实现层次化设计,并可限制故障波及的范围。通常易出现的错误是,在路由器上将这两种路由协议都配置上去,使得外部可以获得内部的路由信息,而内部又将外部的机器误认为在内部。因而最重要的一个原则是不要与他人分享你的内部路由协议。

路由过滤也很重要,没有必要向所有知道的地方发送广播消息,内部应用也没有必要让外部知道。通过路由过滤控制哪些内部信息可以传播出去,哪些外部信息可以传到内部。

1.2 **设计实例**[3,4,6]

某公司共有 3 个分公司,其中第 3 个分公司在其它地方有办事处,要求总公司与 3 个公司之间以 622 M 相连,分公司之间 155 M 相连,在总公司要求与 CHINANET、CNC 相连,总公司及其各分公司要求能提供 VPN 服务。其规划图如图 1。

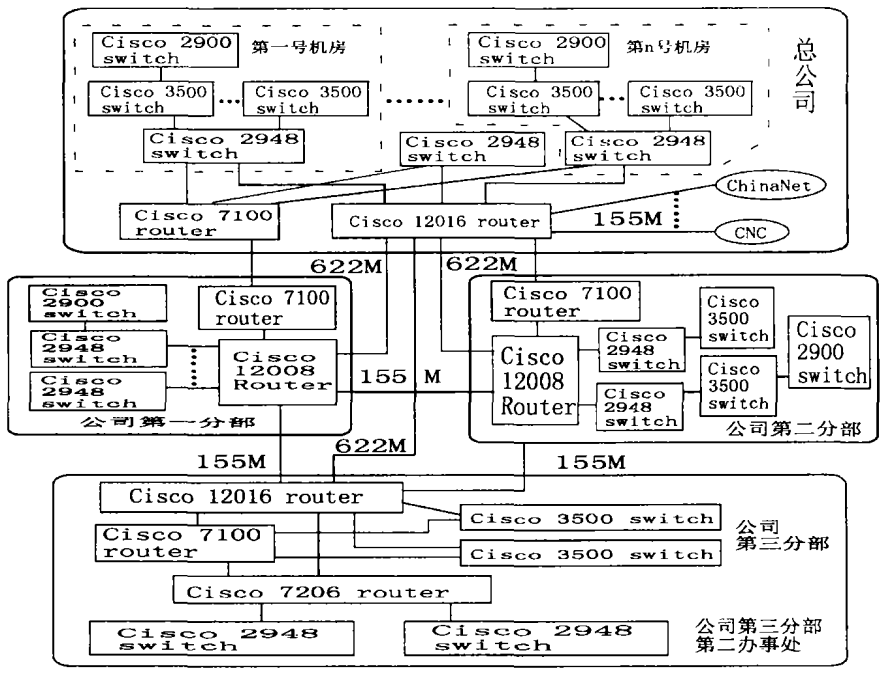

图 1 骨干网、IP 大型网规划图

因其地址设计可能涉及有关法律冲突,所以在本设计中不涉及地址设计。

在选用路由器时,考虑到现代信息及其速度要求,选用 Cisco 12000 系列路由器。它是当代路由器中的高档千兆位服务供应路由平台,为满足数据流量的高速增长提供了一个可靠的和具有良好的扩展性的系统,能很方便的实现路由控制,流量检测。

在路由器与路由器的连接全采用光纤(光缆)连

接，在总公司、分公司与分公司之间的光纤连接可采用租用电信、网通等通信营运商的频带，以此减少初期投入。在路由器以后的系统中采用超五类双绞线进行连接，可达 155 M。

方案的特点：扩充能力强，以上设备的选取，在一定程度上考虑冗余，其支持的协议及服务具有一定的先进性。在经济实力允许的情况下可在很大程度上的提速，不需加任何其它设计，只需增添设备模块，便可加速。再加上软件上对路由器、交换机配置等，可为用户提供诸多的服务，如防黑客、网络增值服务、负载均衡、管理防火墙等服务。

2　VPN 方案设计

2.1　VPN 及其技术实现[2-3]

虚拟专用网络 VPN(Virtual Private Network)是利用接入服务器(Access Server)、路由器及 VPN 专用设备，采用"隧道"技术在公用广域网上为企业建立自己的专用通信网。用于构建 VPN 的公用网络包括 Internet、FR、DDN、X.25、PSTN、ATM、IP 等。在公用网络上组建的 VPN 象企业内部网一样提供安全性、可靠性、可管理性。VPN 具有内部网络广域化、降低运行管理费等优势。

VPN 技术主要有：隧道技术、加密技术、密钥管理技术、身份验证技术。采用的协议：

· PPTP(Point to Point Tunnel Protocol) 点对点隧道协议。

· L2TP(Layer2 Tunneling Protocol) 第 2 层隧道协议。

·IPSec (Internet Protocol Security) 因特网安全协议。

·SOCKS 网络连接的代理协议，将连接请求进行鉴别和授权，常用作网络防火墙。

在 VPN 技术实现中 关键在于以下几个问题：

1) 如何在整个网络范围内定义各 VPN 中的成员；

2) 如何在多个交换设备之间传递 VPN 成员信息；

3) VPN 配置的自动化应达到何种程度以及何种方式进行配置；

4) VPN 之间的通讯如何进行。

在 VPN 交换技术中，在本 VPN 中 ATM 交换机上实现信元交换，一个或多个互连的 ATM 交换机组成网络的核心系统。ATM 交换机端口上接收到信元后，正确地转发到输出端口，此传输速率能达到 155 Mb/s 甚至更高。

2.2　方案设计实现及方案举例[3,4,6]

VPN 网络路由器可选用 Cisco7100 系列的 7120 或 7140 路由器。7100 系列路由器集成 VPN 的关键特性：包括隧道、数据加密、安全、防火墙、高级带宽管理和服务级确认；高性能处理器提供高速可靠、可伸缩的 VPN 服务和路由吞吐量，并为 VPN 服务交付提供扩展的内存和大量接口。Cisco7120 专为大型分支机构和中央站点 VPN 和广域网部署而设计的低端路由器。Cisco7140 为中央站点远程访问、内部和外部网应用寻找高端 VPN 平台的客户提供卓越的路由、广域网的 VPN 服务性能、双广域网接口。其方位设计如图 1。实用范围：

·IT、证卷、金融、保险、教育、媒体等一切有远程局域网互连要求的客户

·有宽带需求的二次运营商；有远程 Extranet 建网要求的客户；有移动办公需求的客户

2.2.1　客户需求

总部在重庆、北京、上海、广州设立分公司，现在是以 DDN 连接，构筑公司内部网 Intranet。原有网络存在以下缺点：

a.所有连接都是点对点的，中心是重庆。两地通信需经重庆转发，重庆通信负担重。

b.网络存在单点故障，如果重庆设备出故障，会影响到所有的连接。

c.设备复杂，不易管理；扩展性不好，如专线带宽不易更改。

d.异地专线费用较高，公司每月所租用的带宽相当高的费用，成本昂贵。

现建立虚拟专用 Intranet 网络 VPN 取代 DDN，在传输信息的两地间建立传输通道，保证该通道带宽，采用用户认证的加密技术，实现高速、安全的信息传输。带宽需求如下表 1：

表 1　数据传输速率表　　kb/s

	重庆	北京	上海	广州
重庆	—	—	—	—
北京	512	—	—	—
上海	512	128	—	—
广州	512	128	128	—

2.2.2　实际互连解决方案

1)各地接入方案：

用 DDN、xDSL、Cable、无线、以太网、拨号、ATM、FR、FTTx 等实现接入，在公司采用本地 DDN 专线接入到提供 VPN 的 ISP 或 IDC，ISP 或 IDC 整合电信本地线路工作。

重庆中心：2 Mb/s 本地 DDN 到 ISP 或 IDC 重庆机房

北京分公司：256 kb/s 本地 DDN 到 ISP 或 IDC 北京机房

上海分公司：256 kb/s 本地 DDN 到 ISP 或 IDC 上海机房

广州分公司：256 kb/s 本地 DDN 到 ISP 或 IDC 广州机房

2)骨干 VPN 方案

·建立二层隧道。根据用户带宽和网络连接需求,在重庆、北京、上海、广州之间建立相应带宽的二层隧道,主要采用 L2TP,同时可以支持 PPTP、L2F 等相关的隧道协议。

·数据端到端加密。通过 IPSec 获得安全保证。这是一个适用于数据加密、主机鉴别、密钥交换的不断演进的 Internet 协议。IPS 提供了访问控制、无连接完整性、数据源鉴别、载荷机密性等安全服务。弥补了由于 TCP/IP 协议体系自身带来的安全漏洞。

·用户身份认证。可通过认证服务器进行 3A 认证,支持基于 MD5/SHA1 身份认证和 RSA 算法的数字签名认证方式。可以采用 ISP 或 IDC 提供认证服务器。

·统一地址管理。接入 ISP 或 IDC 的 VPN 网络可同时实现 Internet 访问、允许用户在 VPN 内使用私有地址,访问 Internet 时进行地址转换。

·通过各种连接方式(DDN、FR、xDSL、ISDN、FTTx、微波等)接入各个结点;

·根据宽带需求开设 VPN 隧道(Tunnel),提供点到点、点到多点和网状的 VPN 网络。采用 CBQ 等流量管理技术提供每条隧道端到端的最小带宽和突发带宽的 QoS 保证。

·使用 IPSec 和 L2TP 安全协议,提供 64 位 DES 数据加密、MD5/SHA1 身份认证服务、IKE/PKI 密钥管理。

·实现远程 VPN(Remote VPN)服务。

·实现 VPN 管理服务,包括隧道的建立、带宽的变更、流量的监控和管理,安全认证的管理、密钥的管理等。

3 智能小区方案设计

目前,智能化社区建设逐渐成为热门话题。由于 Internet 的信息和服务内容极大丰富,使得用户入网需求急剧增加。住宅社区的智能化、网络化给社区开发商带来新的商机,不但可以利用网络对社区进行现代化的内部管理,还可以为社区用户提供增值服务,如 Internet 访问,网上社区,网上超市,视频点播等社区服务。智能化社区网络属于园区网络,但它是公用的运营网络。其物理网络传输技术可以采用以太网等局域网络技术,又可以采用有线电视网数字传输、xDSL、FTTx 等广域宽带接入技术[5]。智能化社区网络设计包括:

·保护模式基础物理传输网络设计,包括物理线路、传输协议等。

·网络逻辑设计,包括路由服务、网络流量控制等。

·网络运营管理平台设计,包括基于用户的认证、计费、网络安全服务质量等。

·Internet 服务平台设计,包括防火墙等。

3.1 设计实现[4-6]

在住户的家中添加以太网 RJ45 插座作为接入网络接口,可接 100 M b/S 的网络速率,采用以太网技术,其基础网络设计方案和技术实现比较成熟,包括以下两点:

1)园区数据网络结构化布线。采用 FTTx(光纤到....)+超五类双绞线到每户的方案。

2)以太网络设计与实现。网络结构基本上分为核心和边缘。网络核心即社区网络管理中心,在此为 Cisco 12008,通过光纤实现与 Internet 互连;如果广域出口接防火墙是 Ethernet 形式,应采用第 3 层交换机,既便宜又好。网络边缘即各个建筑物内,可采用工作组级以太网交换机 Cisco 2948 再下级连 Cisco Catalyst 3500 及 2912。可根据每个建筑物内用户数量来确定交换机端口的数量。从而决定交换机的数量。

·服务运营平台实现。社区网络作为一个公用的提供接入服务的运营网络,其运营服务管理应特别考虑用户认证与计费和网络安全两方面问题。由于以太网技术本身的一些弱点,如广播、SPT 等,对整个网络的服务可靠性造成威胁。如果不采取措施,以太网内的用户将面临本地黑客从网络第 2 层次的直接窃听甚至攻击。对于以上问题,一般采用虚拟局域网络 VLAN 技术从用户端口到网络出口建立专用逻辑通路。但由于一般网络将承载数以百计的用户,网络管理员通过静态设置,管理同样数量的虚拟网和路由,其繁杂程度和不灵活性可想而知。同时还要考虑此种设置方案下,网络设备的承载能力。由此可见,社区网络设计中网络运营管理平台设计建设与接入网相配套是非常关键的。

·Internet 多功能服务平台设计实现。除了基础物理网和网络运营管理平台的设计,围绕 Internet 应用服务实现,也应该是网络设计者需要考虑的重点。如 DHCP 服务器、DNS 服务器、防火墙系统、WWW Server、Mail Server 和文件访问服务器等。面对以上诸多的 Internet 服务,对于不同的应用、不同规模的网络环境有不同的解决方案。

·其它设计实现。包括网络线路冗余设计、网络地址分配与管理、服务质量的实现等。

3.2 硬件选择(可参阅图 2)

网线选择:超五类双绞线、多模光纤。

防火墙的选择:有 2 种方式,一种是在计算机内部安装住留防火墙,如 Norton 防火墙。另一种选择专用防火墙,原理上由堡垒主机后加一包过滤等功能软件。在这里可以选用 Cisco Secure PIx 防火墙,是高速专用防火墙设备,能在不影响网络性能的情况下提供强大的安全性,最多支持 250 000 个同时连接,URL 过滤,

HP Openview 网管平台集成等。

3.3 软件选择

网络操作系统可选用 Win2000 Server、WinNt Server、Linux，数据库选用 SQL Server7.0、My SQL 等；服务器软件选用 IIS(Internet Information Server)4.0 以上。IIS 的标准组成：

1) Internet 服务，包括 WWW 服务，FTP 服务，Gopher 服务。

2) Internet 服务管理器。管理 Internet 服务的工具。

3) 数据库管理器。向数据库发布查询的组件。

4) 密钥管理器。安装安全套接字层(SSL)密钥的工具。

3.4 接入 Internet/Intranet/WAN

智能小区与外界连接，可采用拨号、专线、光纤与因特网、外部企业网或城域网相连(最后 1 英里接入问题)：

1)在智能小区的中心机房，12008 路由器通过单模尾纤与 ISP 相连，由 ISP 统一规划分配 IP 地址。

2)在小区内部，个人用户可选择几种入网方式：一是通过网卡与小区网络相连。由小区分配的内部 IP 地址通过内部网与外部网连接。二是单独的与外部连接，及通过调制解调器、ISDN、DDN、Cable、xDSL、FTTh 等上网。

3.5 内部 IP 地址分配

在智能小区内部，采用内部 IP 地址分配方法，即在网络中心 12008 路由器处设置好在互连网外部唯一的 IP 地址后高置内部 IP，比如 12008 内部 IP 可设置为 192.168.0.1，子网掩码根据内部网络规模设定，在小区内部电脑数目相当多的情况下，如达到 256x64，则子网掩码可设为 255.255.192.0。内部电脑通过内部网络上网时，IP 的选取又可有 2 种，即自动获取 IP 地址和按小区中心机房统一规划来设定。比如某住户 IP 地址是 192.168.1.25，子网掩码为 255.255.192.0，其内部网关统一设定为 12008 的内部 IP 地址，即 192.168.0.1。

DNS 的选择，在内部网络提供 DNS 的情况下，如 192.168.0.3 是 DNS 服务器，内部网的 DNS 可设置为 192.168.0.3，亦可选取 ISP 提供的专业 DNS，如设置为 202.96.134.133。

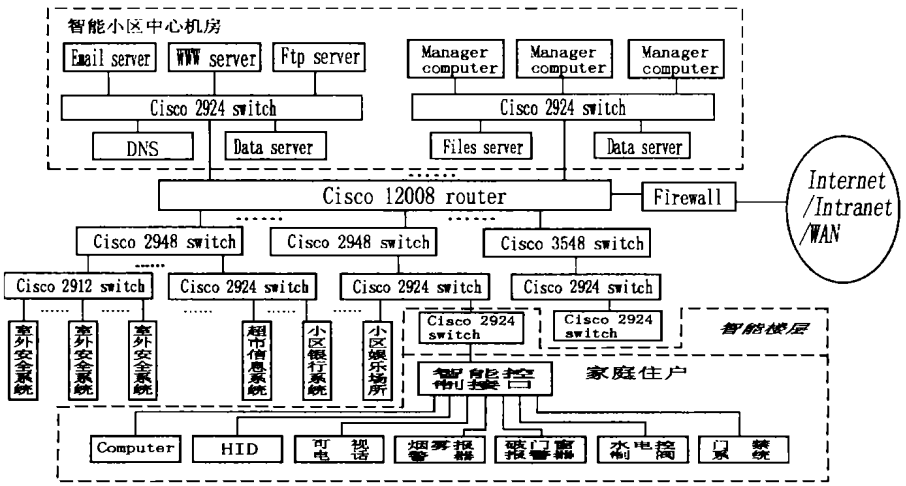

图 2　智能小区整体设计图

4 结　语

运用现代网络设计方法设计规划计算机网络是一个复杂的系统工程问题，要有前瞻性，应与当前网络的发展同步。目前 10Gbps 标准的产品已经出现，光纤网、四层以上交换机、目录服务、智能网管的出现，对网络分层设计产生重大影响。网络的规划设计除了要考虑现状还要考虑扩展性问题。

参考文献：

[1] [美]WEBB K 著. 组建 Cisco 多层交换网络[M]. 李逢天，张帆 译. 北京：人民邮电出版社. 2000.

[2] GUICHARD J, PEPELNJAK I. MPLS and VPN Architectures[M]. America: Cisco Press. 2000.

[3] 李津生，洪佩玲. 下一代 Internet 的网络技术[M]. 北京：人民邮电出版社. 2001.

[4] [美]FEIT S 著. 组网用网：高速局域网[M]. 郭幽燕，曲健，张灵欣 译. 北京：电子工业出版社. 2001.

[5] 上海市科学技术委员会. 网络通信技术实用大全[M]. 上海：上海科学技术文献出版社. 1999.

[6] [美]SLATTERY T, BUOTON B. Cisco 网络高级 IP 路由技术(第二版)[M]. 达达翻译组译. 北京：机械工业出版社. 2001.

(下转第 41 页)

参考文献：

[1] OTT E, GREBOGI C, YORKE J A. Controlling Chaos[J]. Phys. Rev. Lett., 1990, 64(11): 1 196 - 1 199.

[2] PECORA L M, CARROLL T L. Synchronization in Chaotic Systems [J]. Phys. Rev. Lett., 1990, 64(8): 821 - 824.

[3] 关新平，唐英干，范正平，等．基于神经网络的混沌系统鲁棒自适应同步[J]．物理学报，2001，50 (11)：2 112 - 2 115.

[4] ZHOU PING. Synchronization of Hyperchaos by Nonlinear Feedback [J]. The Journal of China Universities of Posts and Telecommunications, 1997, 4(2): 57 - 62.

[5] CHEN XI - MING, ZHOU PING. A Design of Observers for a Discrete Chaotic System[J]. The Journal of China Universities of Posts and Telecommunications, 2001, 8(4): 21 - 23.

[6] 周平．控制离散非线性系统中不稳定不动点的一种方法[J]．物理学报，1999，48(10)：1 804 - 1 809.

[7] HE R, VAIDYA D G. Analysis and Synthesis of Synchronous Periodic and Chaotic Systems[J]. Phys. Rev., 1992, A46: 7 387 - 7 392.

Chaos Synchronization of Continuous Systems for Different Systems Parameters

CHEN Xi - ming, ZHOU Ping

(Institute of Electronic Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: Because parameter disturbed exist every practical system, so chaos synchronization for different system parameters is availabe. Chaos synchronization of continuous system for different system parameters is studied with the relation between chaotic synchronization and asymptotic stability, parameter adaptive and driving feedback. Lorenz system is used to verify the effectivenss of the proposed method, and the simulation results confirm it.

Key words: parameter adaptive; driving feedback; chaos synchronization

(责任编辑　吕赛英)

(上接第 37 页)

Modern Network Design

WANG Da - en[1], *LI Min - ji*[2], *LUO Cheng - zhi*[3]

(1. College of Computer Science, Chongqing University, Chongqing 400044;
2. College of Mechanical Engineering, Chongqing University, Chongqing 400044;
3. Shenzhen Huaan Chengxun Science&Technology Co., Ltd, Shenzhen 518000, China)

Abstract: Nowadays the network of high - speed and broadband is required in the application of multimedia technology and information community. Many methods, such as network layering design, address design and routing are introduced to design Enterprise Backbone Network. VPN's interrelation protocol is disposed and VPN tunnel is cut to establish virtual private network. Server and run plane design, bowels IP address distribution and network security advisement to design Intelligent Residential Area Network are given. It is pointed out that the method of modern network designs satisfies high - speed, intelligent and broadband for the developments of network technology.

Key words: enterprise backbone network; virtual private network; intelligent residential area network; network design

(责任编辑　吕赛英)