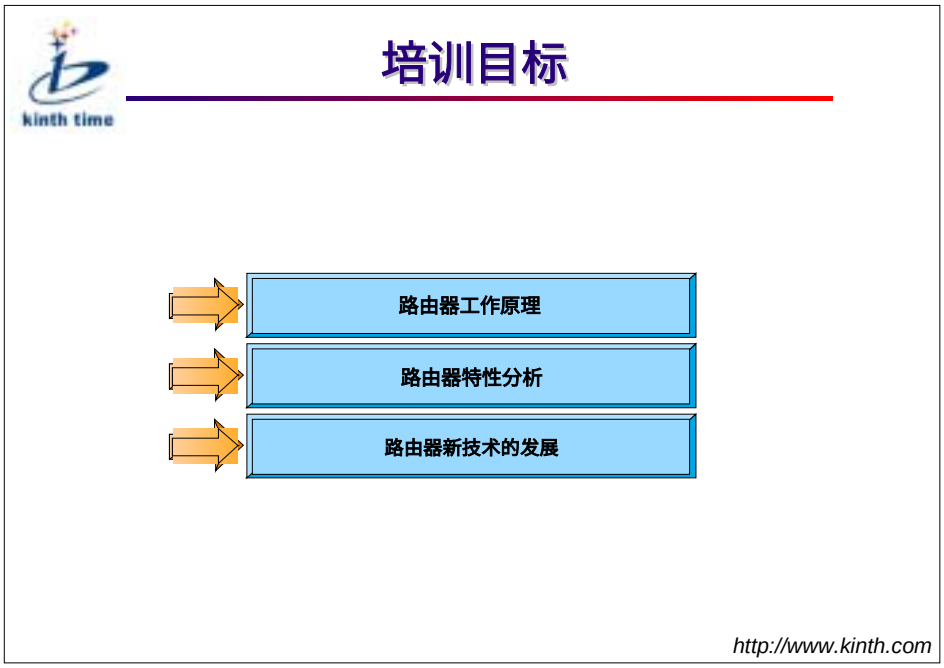
第五章 路由器基础及原理

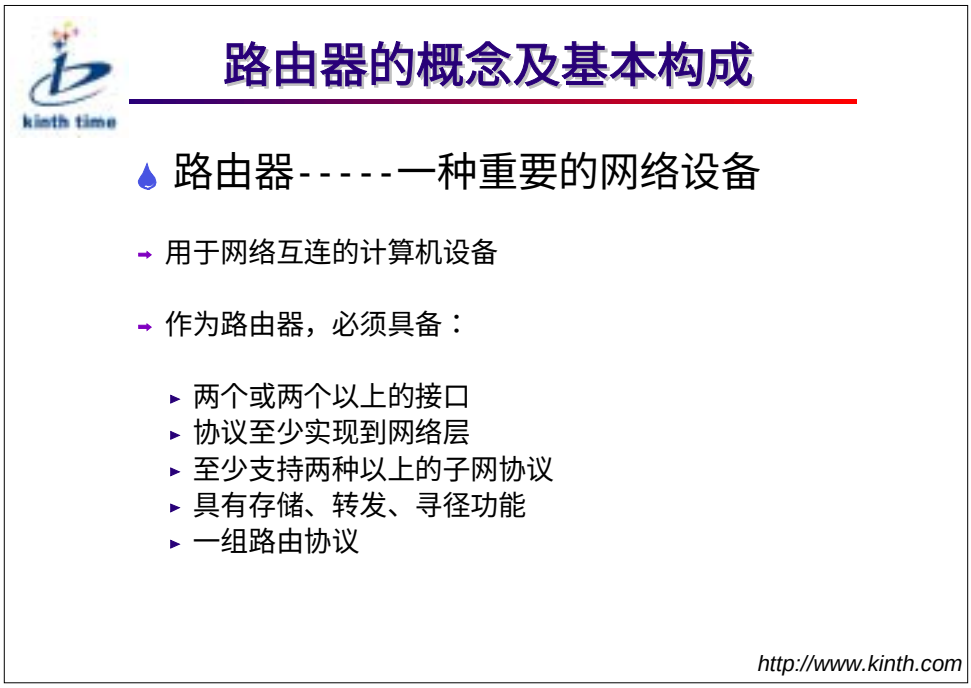
.1 培训目标



本章讨论路由器基础及工作原理，包括路由器工作原理、路由器特性分析及
路由器新技术的发展。

.2 路由器工作原理

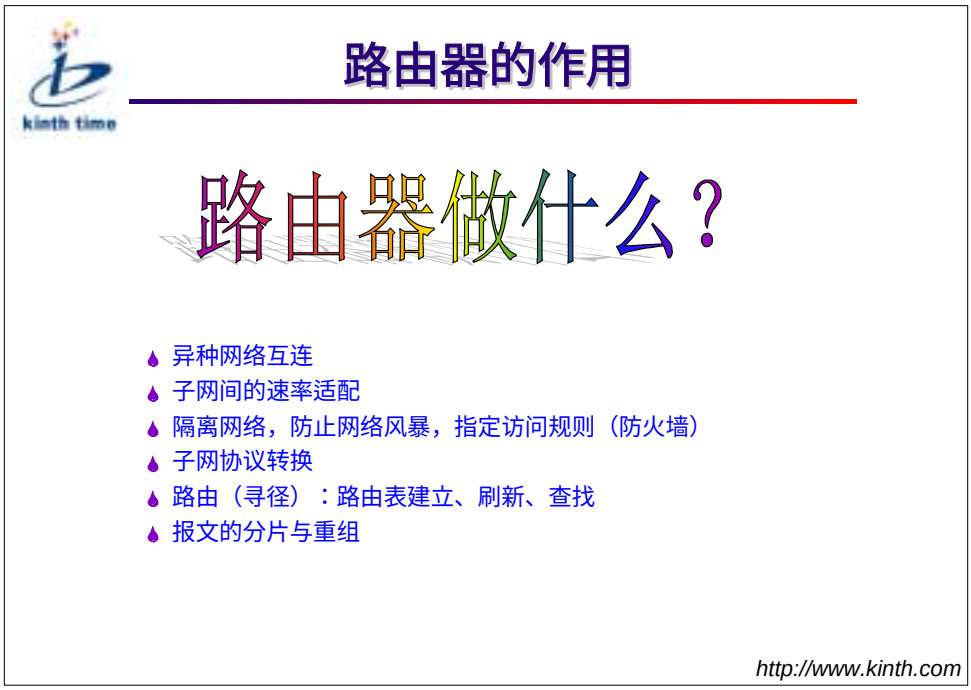
.2.1 路由器的概念及基本构成



路由器是一种用于网络互连的计算机设备，它工作在 OSI 参考模型的第三层（网络层），为不同的网络之间报文寻径并存储转发。
作为路由器，必须具备：

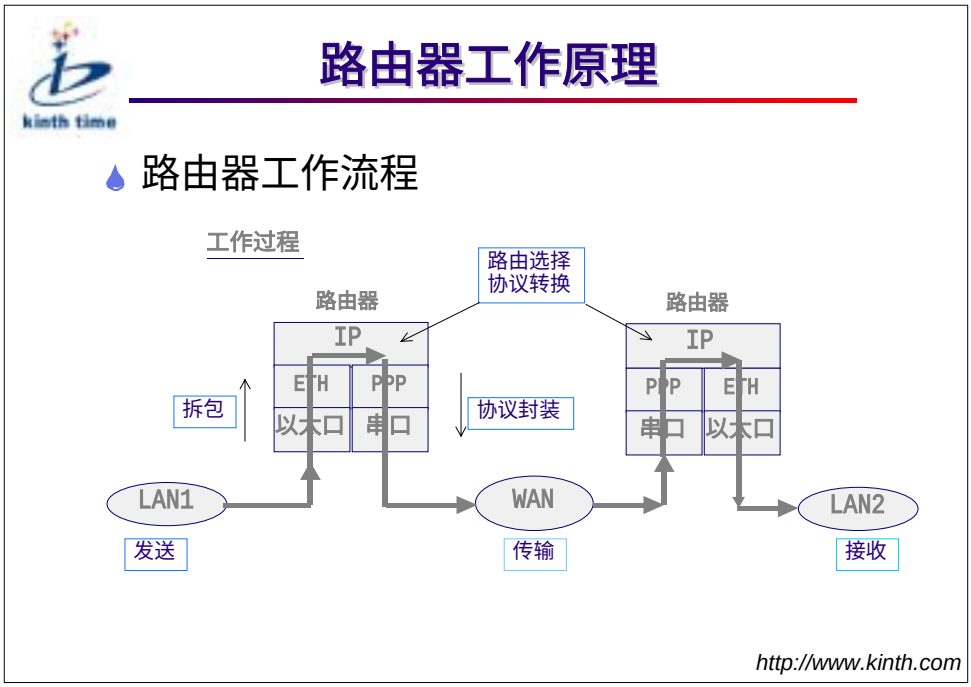
- 两个或两个以上的接口：用于连接不同的网络。
- 协议至少实现到网络层：只有理解网络层协议才能与网络层通讯。
- 至少支持两种以上的子网协议：异种子网互联。
- 具有存储、转发、寻径功能 ：实现速率匹配与路由寻径。
- 一组路由协议：包括域内路由协议、域间路由协议。

.2.2 路由器的作用



- 异种网络互连：主要是具有异种子网协议的网络互连。
- 子网协议转换：不同子网间包括局域网和广域网间协议转换。
- 路由（寻径）：路由表建立、刷新、查找。
- 速率适配：不同接口具有不同的速率，路由器可以利用自己 缓存及流控协议适配。
- 隔离网络：防止广播风暴，网络安全（防火墙）。
- 报文分片与重组：接口的 MTU 不同，超过接口的 MTU 的报文会被分片，到达目的地的报文会被重组。
- 备份、流量流控：主备线路的切换及复杂的流量控制。

.2.3 路由器工作原理



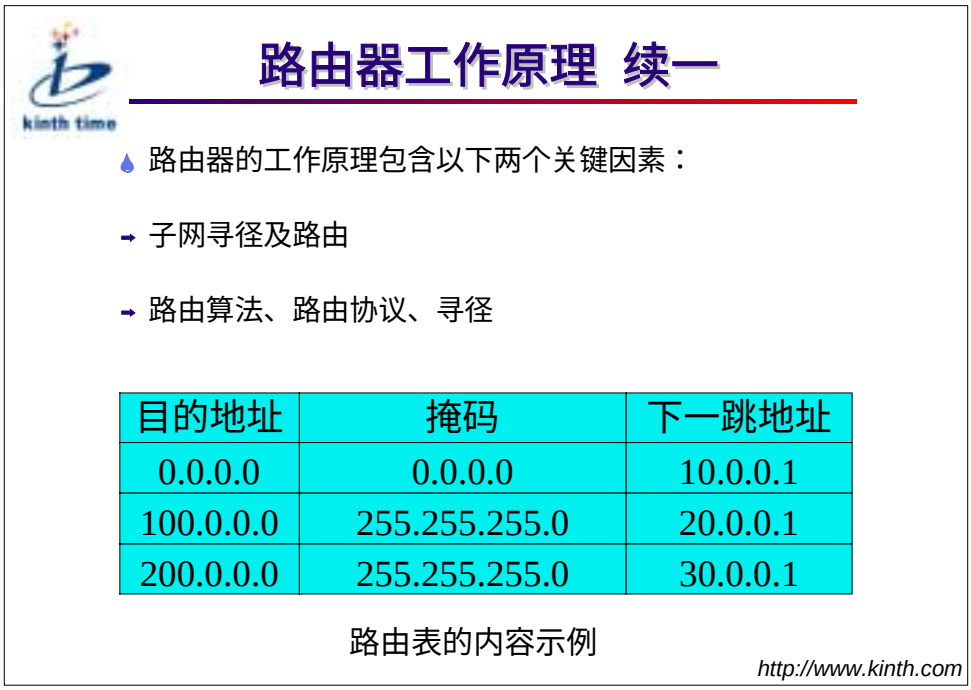
路由器中时刻维持着一张路由表，所有报文的发送和转发都通过查找路由表从相应端口发送。这张路由表可以是静态配置的，也可以是动态路由协议产生的。

物理层从路由器的一个端口收到一个报文，上送到数据链路层。

数据链路层去掉链路层封装，根据报文的协议域上送到网络层。

网络层首先看报文是否是送给本机的，若是，去掉网络层封装，送给上层。若不是，则根据报文的目的地址查找路由表，若找到路由，将报文送给相应端口的数据链路层，数据链路层封装后，发送报文。若找不到路由，报文丢弃。

路由器工作原理（续一）



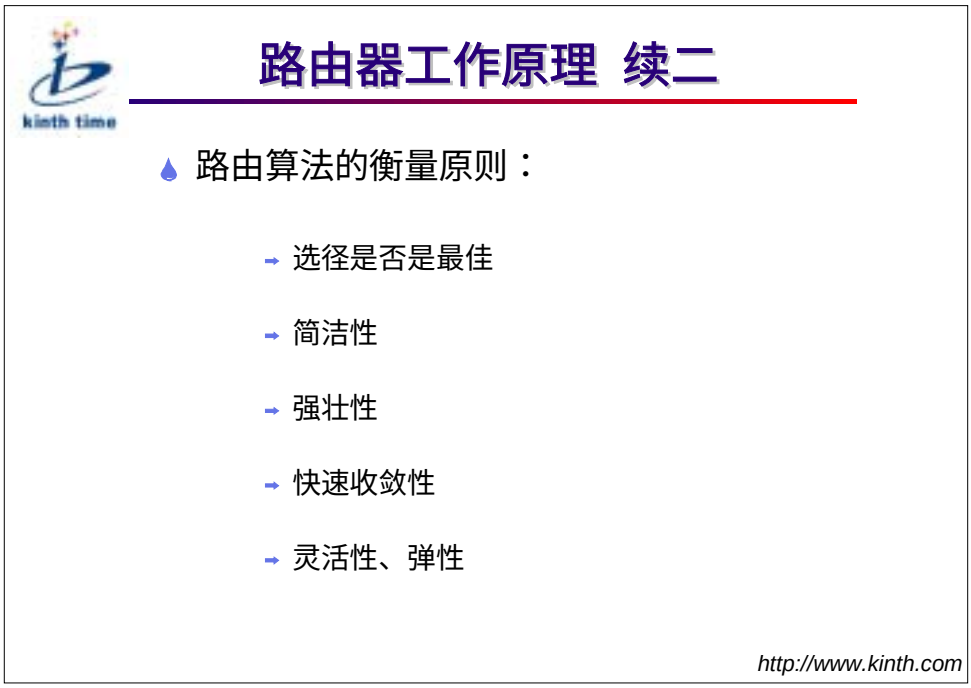
● 子网寻径及路由

标准的寻径表表目是一个二维组（信宿网络地址，下一驿站地址），其中不携带子网信息，不能满足子网寻径。引入子网编址以后，子网寻径表的每一表目中加入子网模，于是子网寻径表表目变为三维组：子网模、信宿网络地址、下一驿站地址。

● 路由算法、路由协议、寻径

路由器依据路由表来为报文寻径，路由表由路由协议建立和维护。路由协议的设计则是依据某种路由算法。

路由器工作原理（续二）



- 选径是否是最佳：

以什么参数来衡量路由，如时延、距离、中间网关数等。

- 简洁性：

路由算法应设计的尽可能简洁。

- 强壮性：

路由算法必须具有鲁棒性，应经得起各种网络环境的考验。

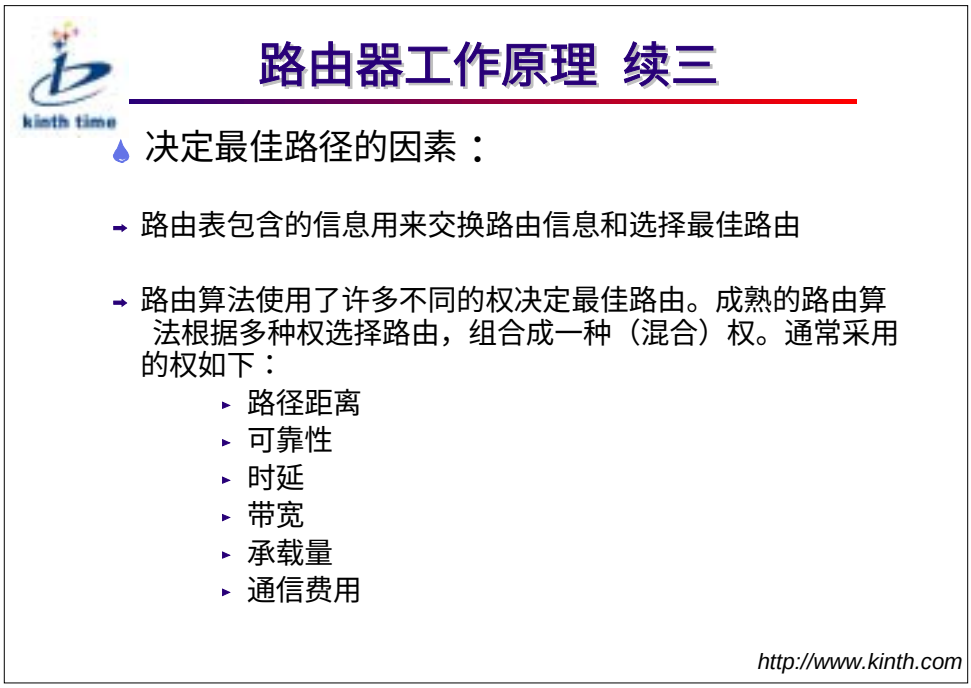
- 快速收敛性：

即所有路由器就最优路径达成一致的过程路由算法如果收敛的慢，就会引起路径循环或网络消耗。

- 灵活性、弹性：

路由算法能否适应网络环境的各种变化，例如网络带宽、路由器的缓存、网络时延等发生变化，路由算法能否根据这些变化做出调整。

路由器工作原理（续三）



● 路由表包含的信息用来交换路由信息和选择最佳路由

路由表是路由器的核心，其中的路由信息来源有两种：一种是手动添加的静态路由，另外一种是路由器运行过程中由动态路由协议学习而得来。

● 路由算法使用了许多不同的权决定最佳路由。通常采用的权如下：

☞ 路径距离：指所经过的每条链路的权值之和，有的路由协议指节点数目；

☞ 可靠性：指网络链路是否容易出故障；

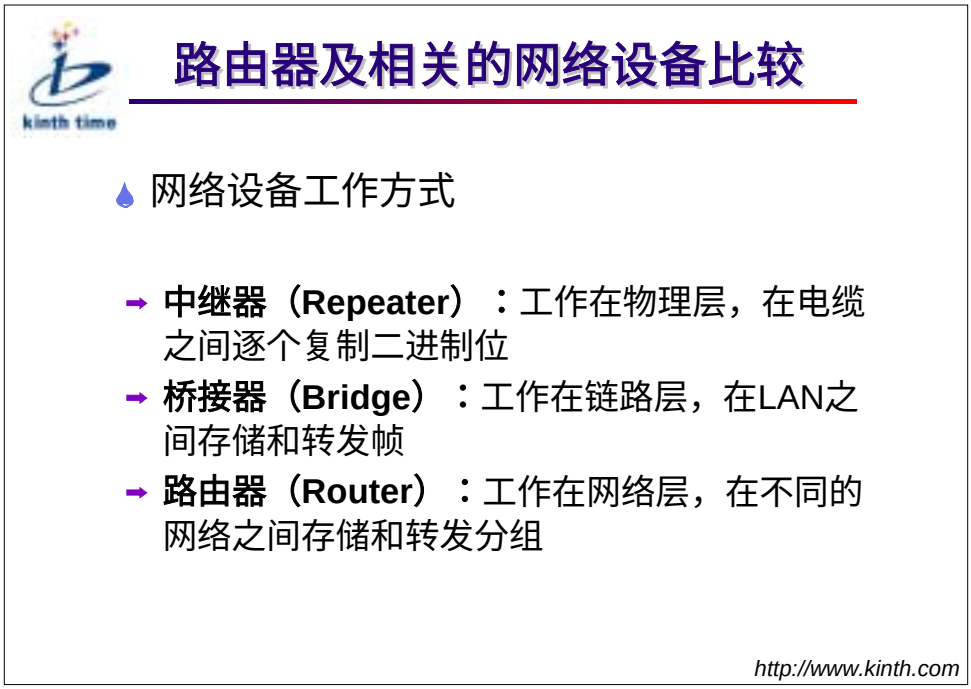
☞ 时延：指网络链路造成的网络延时；

☞ 带宽：指链路传输信息流容量的能力；

☞ 承载量：指网络资源如路由器的繁忙程度；

☞ 通信费用。

.2.4 路由器与相关网络设备的比较

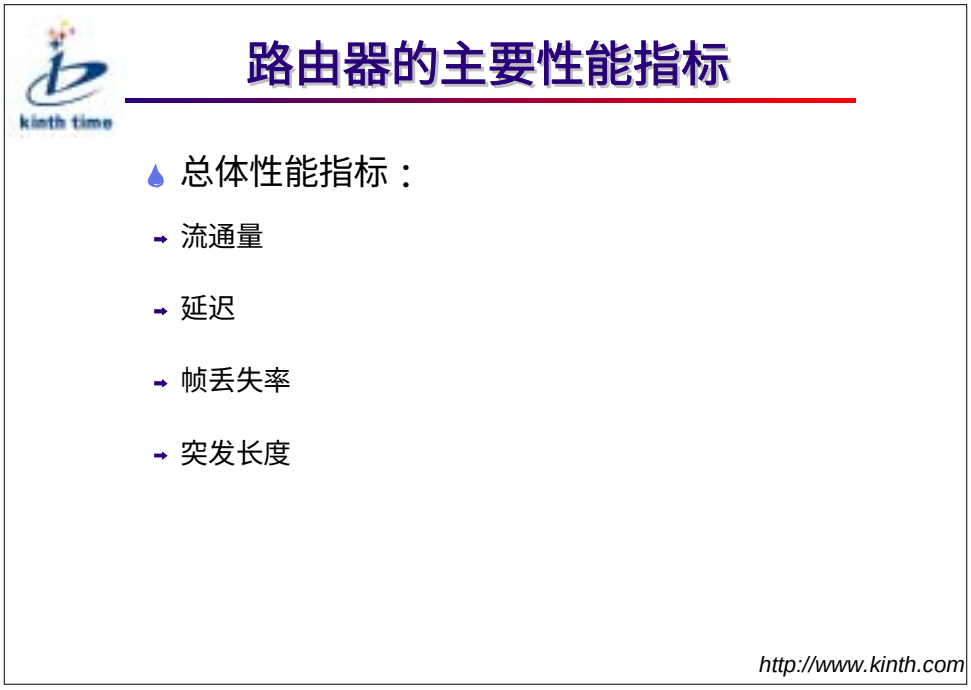


Hubs（中继器）：对应 7 层模型的物理层，它的作用是放大电信号。主要用于连接具有相同物理层的 LAN。Hubs 还将以太网的总线结构变成星状结构。

Bridges（Switches）：是一种在数据链路层实现互连的存储转发设备，广泛用于局域网的扩展。Bridges 从一个网段接收完整的数据帧，进行必要的比较和验证，然后决定是丢弃还是发送给另外一个网段。Bridges 具有隔离网段的作用。在网络上适当地使用 Bridges 可以调整网络负载，提高传输性能。

Router（路由器）：与 Bridges 相比，路由器实现网络互连是发生在网络层，它实现了相对复杂的功能：路由选择、多路重发、错误检测等。路由器的异构网互连能力、阻塞控制能力和网段的隔离能力要强于 Bridges。路由器可以阻止网络风暴、支持多协议、提供多种接口。

.2.5 路由器的主要性能指标 *



☞ 流通量

流通量是指系统在不丢帧的条件的最高接收速率。

☞ 延迟

从接收到某一报文的最后一个比特至该报文第一个比特被发送出来的时间差。

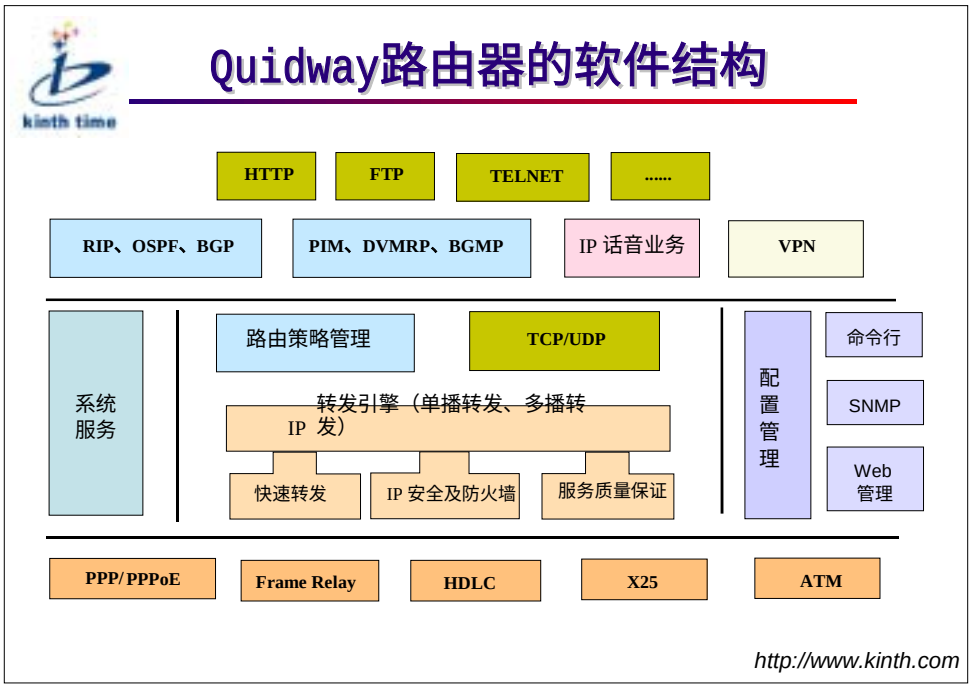
☞ 帧丢失率

在恒定的负载下，由于资源缺乏而不能转发的报文的比例。

☞ 突发长度

以最短间隔连续发送报文，不丢失报文条件下，系统所能处理最大报文数量。

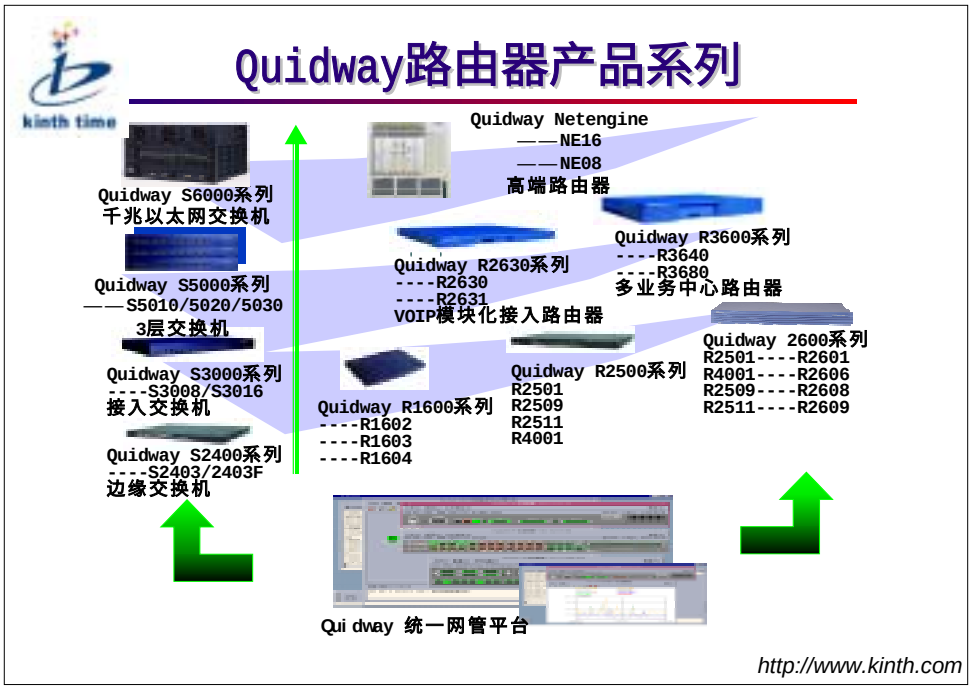
.2.6 Quidway 路由器的软件结构 *



VRP（Versatile Routing Platform）：即通用路由平台，是华为公司在网络领域多年成功探索和应用的基础上发展起来的，是华为公司具有完全自主知识产权的网络操作系统，可支持华为公司的多种网络设备。它以功能强大的 IP 转发引擎为核心，将实时操作系统技术、设备及网络管理技术和各种网络应用技术等通过先进的体系结构设计，完美地融合为一体。它支持丰富的协议和特性，具有很强的可伸缩性、可配置性，并且接口开放，是一个可不断丰富和持续发展的系统平台。利用 VRP 系统可以为您组建一个端到端、安全、高效、高智能化、易于管理的网络。

华为公司通过其网络产品在网上的大规模应用，获得了丰富的网络运行经验，也充分了解了各种各样的用户需求，所有这些，都作为设计 VRP 系统的输入，VRP 系统通过对丰富的协议和特性的支持，能适应目前绝大多数网络应用环境的需求。

.2.7 Quidway 路由器产品系列



按照路由器的接口、处理能力、吞吐量、提供的路由协议、功能等可以把路由器分成高、中、低各种档次。

高端路由器 GSR12000、 NetEngine 08/16 位于 WAN 骨干网的中心或骨干位置，构成整个 IP 网络的核心。

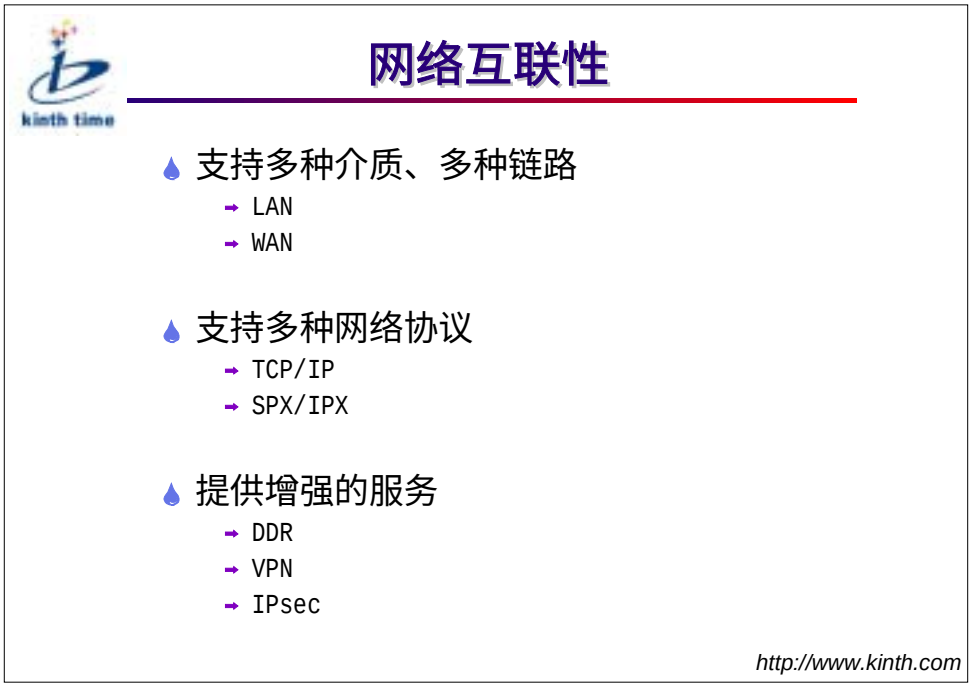
中端路由器 Quidway 2630/2631/3680/3640 适合于有分支机构的中小型企业，一般位于路由中心位置上，互连企业网的各个分支机构，并作为企业网的出口，上行接入高端路由器中。中端路由器边缘可以接入 1600、2500、4001 等低端路由器。对于中小型企业来说，中端路由器是其网络中心。

低端路由器 Quidway 1600 系列、2500 系列、4000 系列主要针对小的分支机构，接口少，处理能力相对较低。

安全加密路由器 Quidway2601/2606/2608/2609 系列是在华为 Quidway2500 系列路由器基础上发展起来的新一代的远程分支路由器。其内置一个接口插槽，可以插入 128 位以上硬件序列码加密的加密板，升级为一台高性能加密路由器。也可支持硬件压缩、硬件防火墙等内置模块，成为满足特殊功能需求的边缘路由器。

.3 路由器的软件特性

.3.1 网络互联性



☞ 局域网支持的介质与协议：

Ethernet、 FastEthernet

☞ 广域网支持的介质与协议：

Serial、 ATM、 ADSL、 PPP、 HDLC、 ISDN、 X25、 FR

☞ 支持多种网络协议

TCP/IP：TCP/IP 协议族

SPX/IPX：Novell 协议族

☞ 提供增强的服务

DDR：按需拨号

VPN：虚拟专用网

IPSec：VPN 加密标准

.3.2 IP 服务特性

- HSRP —— Hot Standby Router Protocol（热备份路由器协议）

它的作用是能够把一台或多台路由器用来做备份。所谓热备份是指当使用的路由器不能正常工作时，候补的路由器能够实现平滑的替换。主机使用缺省网关；实现容错功能，并不是一种动态路由协议；适用于支持多播或广播的局域网。

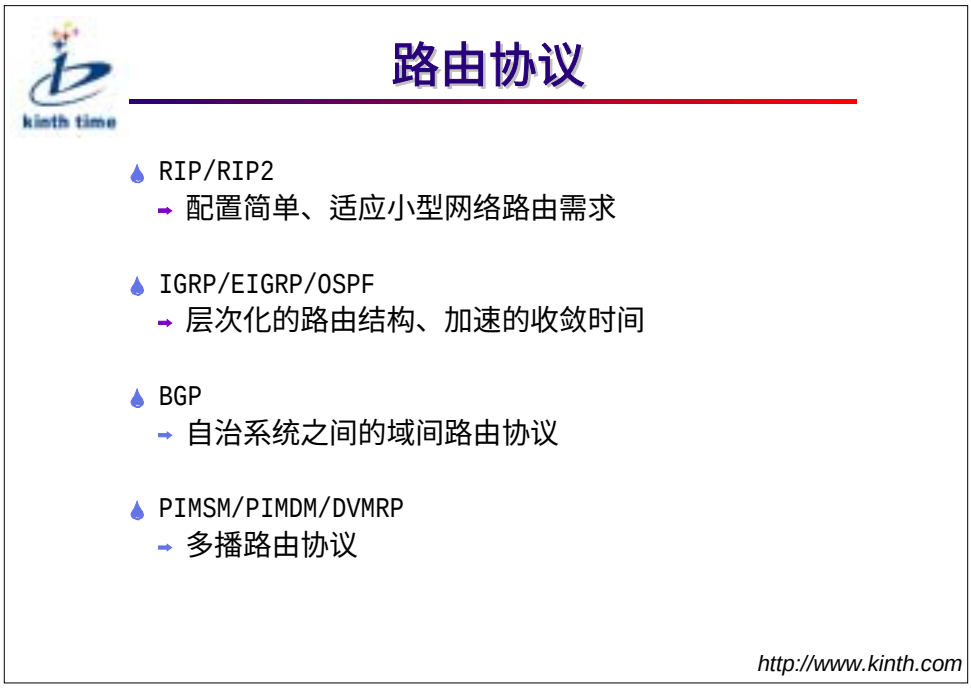
- NAT —— Network Address Translation（地址转换）

地址转换，又称地址代理，用来实现私有网络地址与公有网络地址之间的转换。内部网络的主机可以通过该功能访问网外资源；为内部主机提供了“隐私”（privacy）保护。

- Policy（策略（路由））*

为了确保两个私有网段间的任何通信都必须通过隧道进行传输，我们使用策略路由技术（Policy Routing）。通常的路由技术是通过检查 IP 包的目的地址来选择路由的，而策略路由可以根据 IP 包的更多信息来进行路由的选择，这些信息除了目的地址外，还可以是数据包的源 IP 地址甚至可以根据应用的类型来做路由的选择。Quidway 路由器提供灵活的路由策略机制，针对复杂的大型网络提供高效灵活的路由策略的定制功能。主要提供了管理路由选择决定以及手工调整特定路由器上发生的路由更新报文的机制。

.3.3 路由协议



RIP（Route Information Protocol）协议是基于 D-V 算法（又称为 Bellman-Ford 算法）的内部动态路由协议，简称 IGP（Interior Gateway Protocol）。D-V 是 Distance-Vector 的缩写，因此 D-V 算法又称为距离向量算法。 RIP 协议是最广泛使用的 IGP 之一。

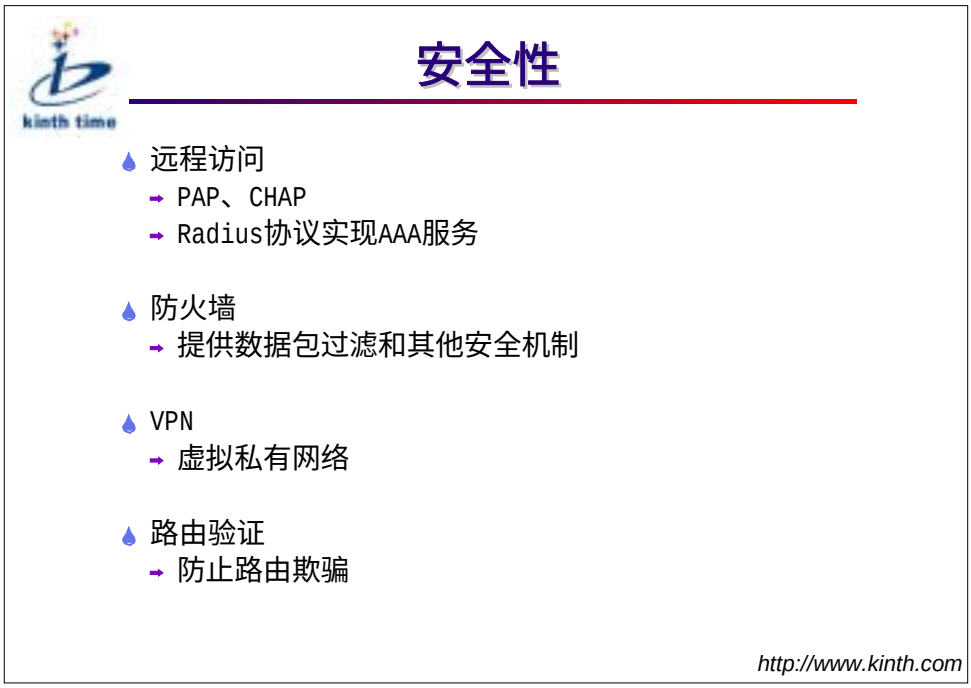
IGRP 是一个基于 D-V（Distance Vector）算法的路由协议，运行 IGRP 的路由器通过和相邻路由器之间相互交换路由信息来建立路由表。IGRP 是从 RIP 基础之上发展而来的。EIGRP 在其基础上进行了大量的改进，具有链路状态协议的某些特征，有快速的路由收敛能力。

OSPF 路由协议：Open Shortest Path First，即最短路径优先协议。OSPF 是一个基于链路状态的动态路由协议。路由器计算出以自己为根、其它网络节点为叶的一根最短的路径树，从而计算出自己到达系统内部可定点的最佳路由。

BGP 是一种自治系统间的动态路由发现协议，它的基本功能是在自治系统间自动交换无环路的路由信息。

PIMDM/PIMSM/DVMRP 是多播路由协议，在一些应用中，源主机需要将信息发送到许多主机。比如，天气预报的广播、股票市场的实时更新和在线广播等。多播（Multicast）是实现这类应用的一种十分高效的方法。

.3.4 安全性



PAP 为两次握手协议，它通过用户名及口令来对用户进行验证。PAP 的特点是在网络上以明文的方式传递用户名及口令。CHAP 为三次握手协议。它的特点是，只在网络上传输用户名，而并不传输用户口令，因此它的安全性要比 PAP 高。

AAA 是验证、授权和记账（Authentication, Authorization, and Accounting）的简称。它是运行于 NAS 上的客户端程序。它提供了一个用来对验证、授权和记账这三种安全功能进行配置的一致的框架。AAA 的实现可采用 RADIUS 协议。RADIUS 是 Remote Authentication Dial In User Service 的简称，用来管理使用串口和调制解调器的大量分散用户。

防火墙一方面阻止来自因特网的对受保护网络的未授权或未验证的访问，另一方面允许内部网络的用户对因特网进行 Web 访问或收发 E-Mail 等。防火墙也可以作为一个访问因特网的权限控制关口，如允许组织内的特定的人可以访问因特网。现在的许多防火墙同时还具有一些其他特点，如进行身份鉴别，对信息进行安全（加密）处理等等。

虚拟私有网（Virtual Private Network，VPN），是近年来随着 Internet 的发展而迅速发展起来的一种技术。许多企业趋向于利用 Internet 来替代它们私有数据网络。这种利用 Internet 来传输私有信息而形成的逻辑网络就称为虚拟私有网。

防止路由欺骗技术可以防止内部路由信息的泄露和外部非法路由信息的传入。

.3.5 可靠性

可靠性

- HSRP
  - 热备份路由器协议
- EIGRP
  - 快速、层次化的域内路由协议
- 备份中心
  - 强大灵活的备份解决方案

http://www.kinth.com

EIGRP 是增强版的 IGRP。它仍然使用 V-D 算法，而且下层的距离向量没有改变。但它的收敛特性和操作效率比以前有显著的提高。EIGRP 的收敛特性是基于 DUAL（Distributed Update Algorithm）算法的。DUAL 算法使得路径在路由计算中根本不可能形成环路。它的收敛时间可以与已存在的其他任何路由协议相匹敌。

为了提高网络的可靠性，Quidway 系列路由器的备份中心提供了完善的备份功能：可为路由器上的任意接口提供备份接口。路由器上的任一接口可以作为其它接口（或逻辑链路）的备份接口。可对接口上的某条逻辑链路提供备份。备份接口可以是一个接口，也可以是接口上的某条逻辑通道（这里所指的逻辑通道可以是 X.25、帧中继、ATM 或 ADSL 的虚电路，也可以是拨号口的某一条 dialer map）。对一个主接口，可为它提供多个备份接口。当主接口出现故障时，多个备份接口可以根据优先级来决定使用顺序。对于具有多个物理通道的接口（如 BRI 和 PRI 接口），可为多个主接口提供备份。主接口和备份接口可以进行负载分担。当主接口的流量达到设定的门限时，启动备份接口。当主备流量和小于设定的另一门限时，关闭备份接口。

.3.6 可管理性 *

命令行接口包括一系列命令，用户通过该接口可以配置和管理路由器。也可通过 Modem 拨号进行远程配置，或通过哑终端、Reverse Telnet 等灵活多样的终端接入方式配置令，提供全中文的提示和帮助信息和网络测试命令，如 Tracert、Ping 等。

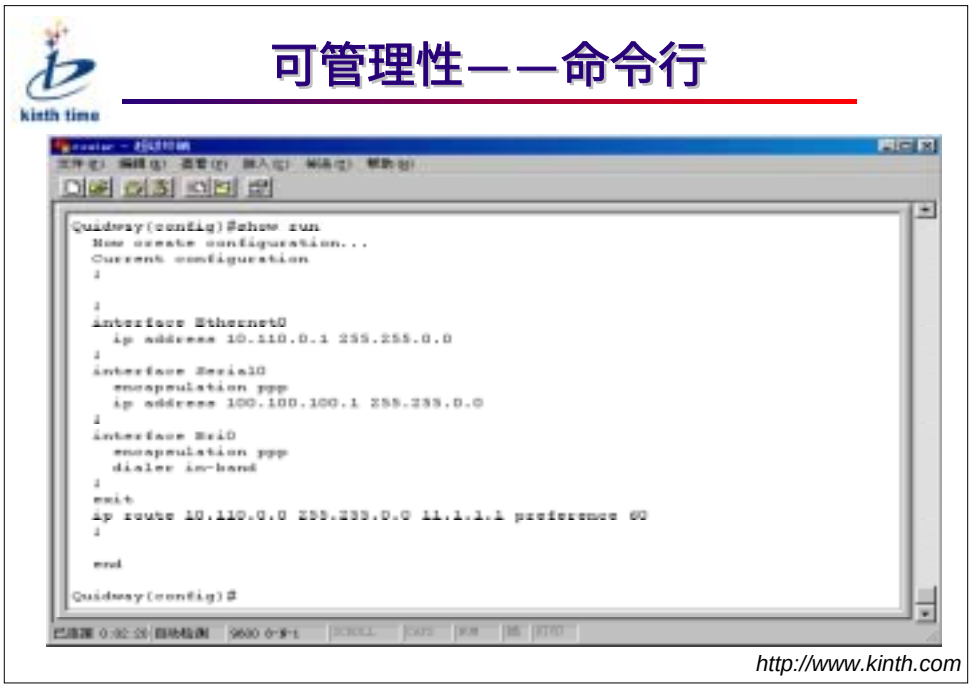
EasyConfig 是图形化易用的配置管理工具，运行在 Windows95/98 或 Windows NT 操作系统的 PC 机上，可以方便地绘制组网图、按照模块配置模块化路由器、进行路由器的配置、打开/保存图形化配置文件、保存普通配置文件、传送路由器配置文件到本地或远程路由器。

QuidView 网管系统是华为公司采用最新的网管技术为路由器量身定制的新一代网管系统。QuidView 系统既可以作为设备级的应用程序集成到已有的网管平台中进行网络级管理，又可以作为独立的应用程序执行设备级管理。

QuidView 系统基于 Web 的扩展允许网络管理人员使用任一种浏览器在网络的任何节点上方便迅速地配置、控制及监视网络，其它网管机器不用预装网管软件，只要有 Web 浏览器且设备能上网，就能使用 QuidView 系统管理网络。

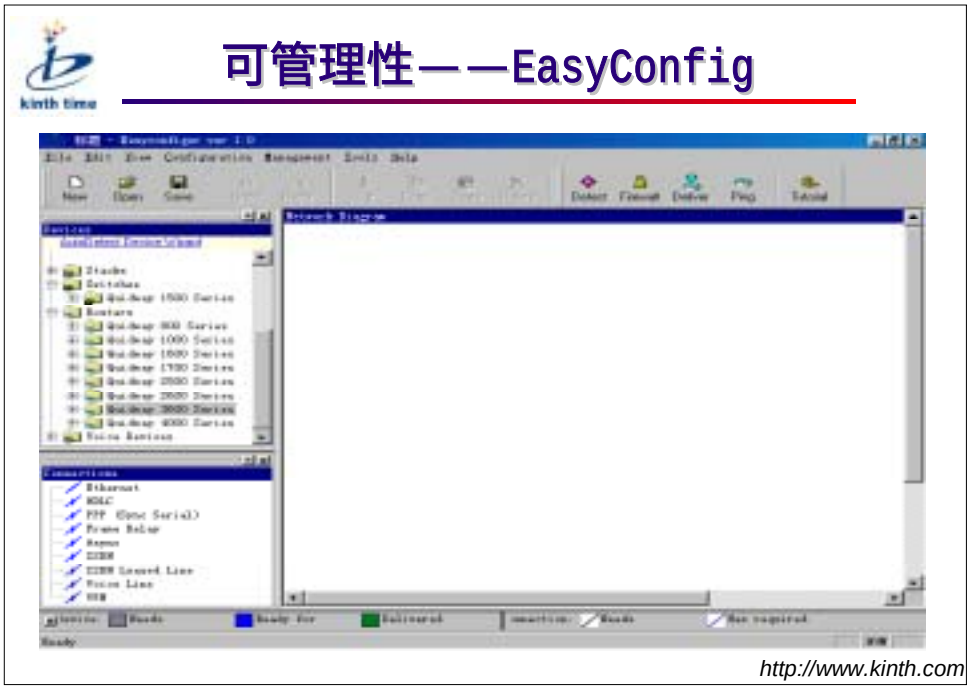
RadiumNMS 数据通信综合网管系统是华为公司自主开发的、管理华为的各类数据通信设备的统一的网络管理系统，它实现在统一用户界面下完成对华为公司的系列交换机、接入服务器、路由器、宽带接入设备、LAN Switch 等的集成管理，功能包括拓扑管理、配置管理、性能管理、故障管理、日志管理、安全管理、系统管理等。

可管理性 —— 命令行



命令行接口包括一系列命令，用户通过该接口可以配置和管理路由器。命令行接口有如下特性：通过 Console 口、Telnet、 Modem 拨号进行本地或远程配置； 提供哑终端、Reverse Telnet 等灵活多样的终端接入方式；配置命令分级保护，确保未授权用户无法侵入路由器；用户可以随时键入“?”而获得在线帮助；提供全中文的提示和帮助信息。
提供网络测试命令，如 Tracert、Ping 等，迅速诊断网络是否正常；用 Telnet 命令直接登录并管理其它路由器；提供种类丰富、内容详尽的调试信息，帮助诊断网络故障；提供 FTP 服务，方便用户上、下载路由器软件及配置文件；可以执行某条历史命令；命令行解释器对关键字采取不完全匹配的搜索方法，用户只需键入无冲突关键字即可解释。

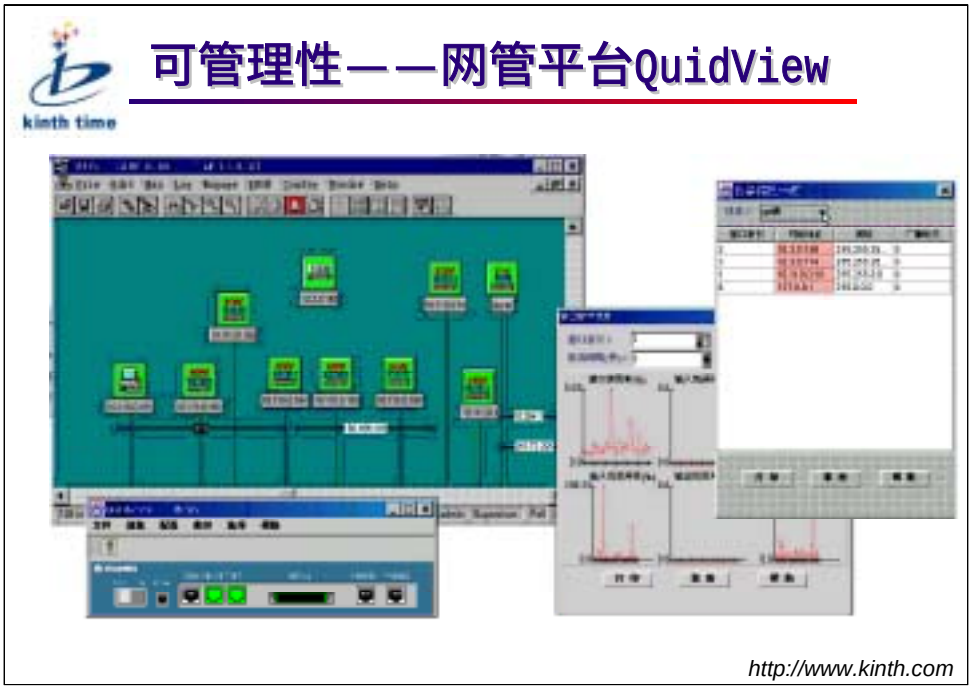
可管理性 —— EasyConfig *



命令行配置方式的使用者往往是专业人员，他们追求的是效率和速度。而图形化配置工具的使用者更多的是普通用户，他们没有多少配置经验，他们希望通过图形化配置工具得到帮助。这就要求图形化配置工具从用户的角度来分析和处理问题，既要对配置命令集覆盖面广，又能为使用者提供清晰的配置思路和流畅的配置向导。此外，图形化配置工具的界面应力求美观，用户操作方法力求简单方便。

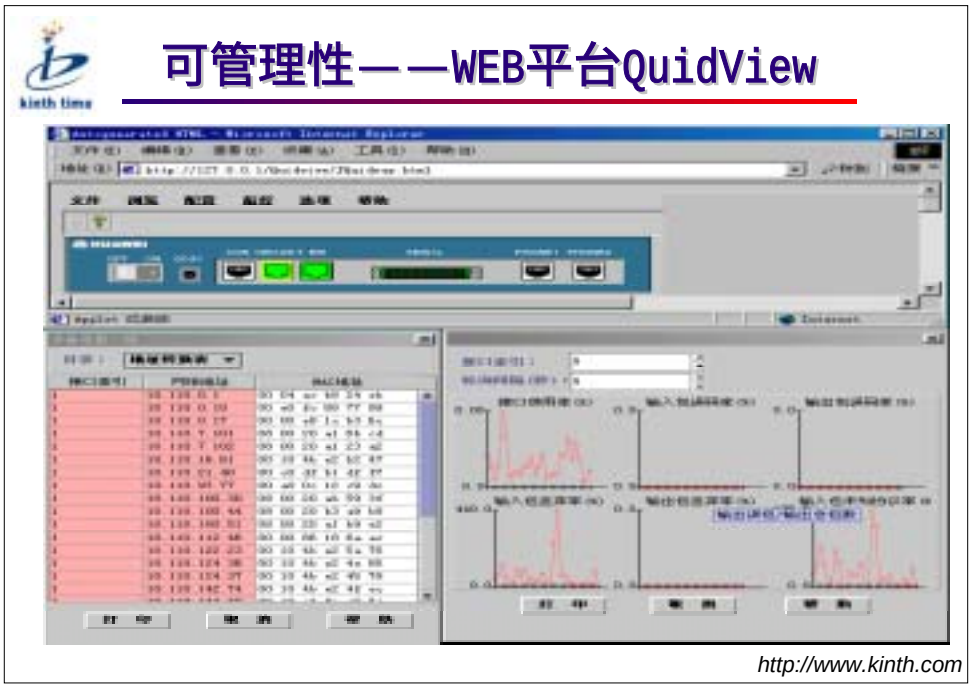
EasyConfig 是图形化易用的配置管理工具，运行在 Windows95/98 或 Windows NT 操作系统的 PC 机上，它的主要功能包括绘制组网图、按照模块配置模块化路由器、进行路由器的配置、打开/保存图形化配置文件、保存普通配置文件、传送路由器配置文件到本地或远程路由器。

可管理性 —— 基于网管平台的 QuidView *



QuidView 网管系统是华为公司采用最新的网管技术为路由器量身定制的新一代网管系统。遵守标准的 SNMP 协议（RFC1157），有投资省、使用灵活、易于移植等特点。QuidView 系统既可以作为设备级的应用程序集成到已有的网管平台（如 SNMPC）中进行网络级管理，又可以作为独立的应用程序执行设备级管理。

可管理性 —— 基于 Web 平台的 QuidView *



QuidView 系统基于 Web 的扩展允许网络管理人员使用任一种浏览器在网络的任何节点上方便迅速地配置、控制及监视网络。在 Web Server 上安装了网管软件后，其它网管机器不用预装网管软件，只要有 Web 浏览器且设备能上网，就能使用 QuidView 系统管理网络。

可管理性 —— 电信级的网络管理 NMS *

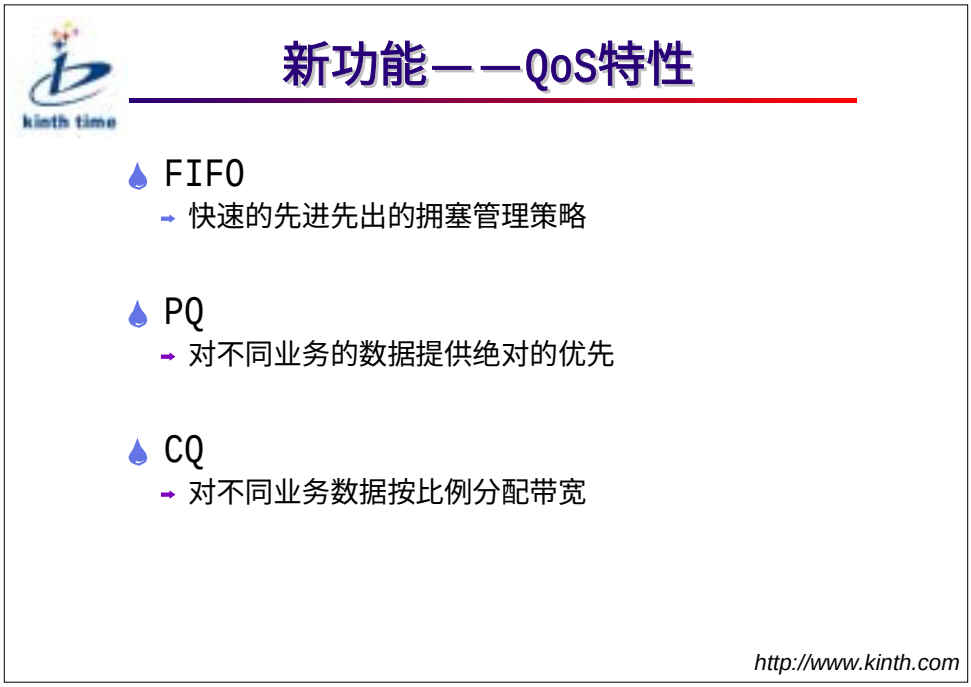
RadiumNMS 数据通信综合网管系统是华为公司自主开发的、管理华为的各类数据通信设备的统一的网络管理系统，它实现在统一用户界面下完成对华为公司的 ATM 系列交换机、A8010 接入服务器、Quidway 系列路由器、MUSA 系列宽带接入设备、Quidway 以太网交换机等的集成管理，功能包括拓扑管理、配置管理、性能管理、故障管理、日志管理、安全管理、系统管理等。

RadiumNMS 的特点：

- 采用 Client/Server 的体系结构，支持多个客户同时登录到网管 Server 上运行；
- 可以对网络进行集中管理或分级管理，以适应不同规模网络的管理需要；
- 采用标准的简单网络管理协议 SNMP ；
- 采用标准 SYSLOG 日志协议收集、管理设备日志；
- 具有严格的用户登录安全检查和权限检查机制，保证系统的安全可靠；
- 内嵌 WWW Server，用户可通过浏览器登录到网管 Server，实时查询各类故障、性能、设备日志及报表数据；
- 可与当前流行的几种通用网管平台集成运行，如 HP 的 OpenView、IBM 的 NetView；
- 具有中文图形界面，并支持多种语言环境。

.4 新功能软件特性

.4.1 QoS 特性



随着计算机网络的高速发展，人们对网络的要求也越来越高。越来越多的对带宽、延迟、抖动敏感、实时性强的语音、图象、重要数据在网上传输，这极大地扩展了网络的能力和资源，同时引入了如何保证服务质量的问题。 Quidway 系列路由器实现了多种拥塞管理策略，能够在一定程度上满足不同业务对不同服务质量需求。

先进先出队列（First In, First Out （FIFO） Queueing）

分组按照到达的先后顺序进入先进先出队列（以后简称 FIFO），出队列的顺序与进队列的顺序一致，即先到达的分组先发送，后到达的分组后发送。FIFO 不对分组进行裁决，分组到达的顺序决定了网络带宽和资源的分配。

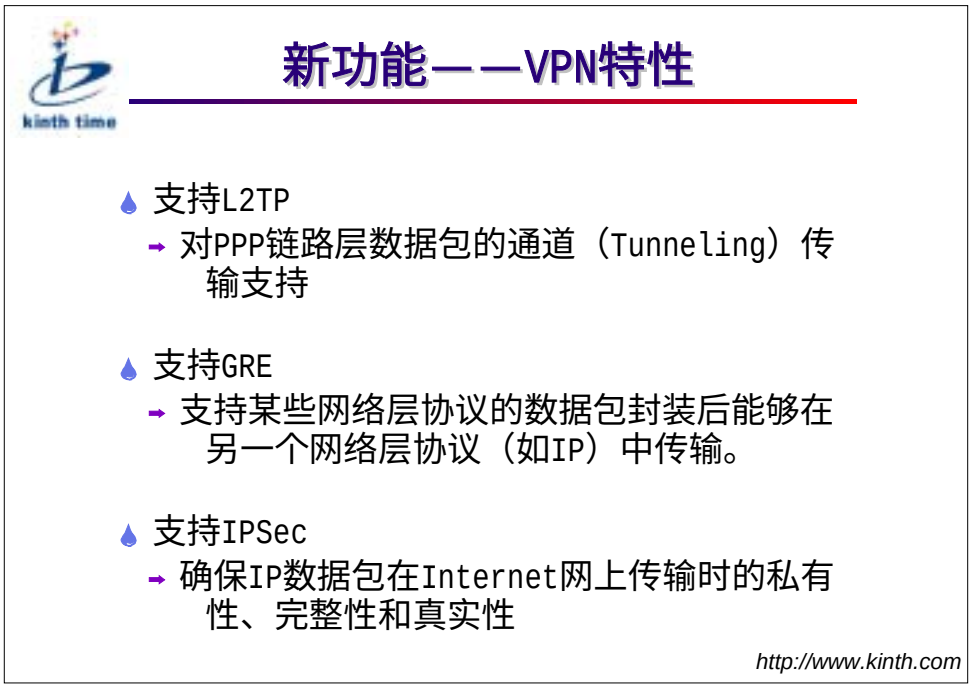
优先队列（Priority Queueing, PQ）

优先队列（以后简称 PQ）按照一定的规则将分组分成四类（对应于 PQ 的四个队列），分组根据自己的类别按照先进先出的策略进入相应的队列。按照优先级从高到低的次序，PQ 的四个队列依次为高优先级队列（High）、中优先级队列（Medium）、正常优先级队列（Normal）和低优先级队列（Low）。在队列调度时，PQ 严格按照优先级从高到低的次序优先发送较高优先级队列中的分组。

定制队列（Custom Queueing, CQ）

定制队列（以后简称 CQ）按照一定的规则将分组分成 17 类（对应于 CQ 的 17 个队列），分组根据自己的类别按照先进先出的策略进入相应的 CQ 队列。在 CQ 的 17 个队列中，0 号队列是系统队列，1 到 16 号队列是用户队列。用户可以配置各个用户队列之间占用接口带宽的比例关系。

.4.2 VPN 特性



虚拟私有网（Virtual Private Network）简称为 VPN，是近年来随着 Internet 的发展而迅速发展起来的一种技术。现代企业越来越多地利用 Internet 资源来进行促销、销售、售后服务、培训和合作等活动。许多企业趋向于利用 Internet 来替代它们私有数据网络。这种利用 Internet 来传输私有信息而形成的逻辑网络就称为虚拟私有网。

虚拟私有网实际上就是将 Internet 看作一种公用数据网（Public Data Network），这种公用网和 PSTN 网在数据传输上没有本质的区别。因为从用户观点来看，数据都被正确传送到了目的地。相对地，企业在这种公共数据网上建立的用以传输企业内部信息的网络被称为为私有网。

L2TP：

L2TP（Layer 2 Tunneling Protocol ）协议提供了对 PPP 链路层数据包的通道（Tunneling）传输支持，它结合了另外两个通道协议 —— Cisco 的 L2F 和 Microsoft 的 PPTP —— 的各自优点，逐渐成为 IETF 有关 2 层通道协议的工业标准。L2TP 还具有适用于 VPN 服务的以下几个特性：

- 灵活的身份验证机制以及高度的安全性

L2TP 可以选择多种身份验证机制（CHAP、PAP 等），具有 PPP 所具有的所有安全特性。L2TP 还可以对通道端点进行验证，这使得通过 L2TP 所传输的数据更加难以被攻击。而且根据特定的网络安全要求还可以方便地在 L2TP 之上采用通道加密、端对端数据加密或应用层数据加密等方案来提高数据的安全性。

支持 RADIUS 服务器的验证，LAC 端通过用户名和密码向 RADIUS 服务器要求验证。

- 内部地址分配支持

LNS 可以放置于企业网的防火墙之后，它可以对远端用户的地址进行动态的分配和管理，可以支持 DHCP 和私有地址应用（RFC1918）等方案。远端用户所分配的地址不是 Internet 地址而是企业内部的私有地址，这样方便了地址的管理并可以增加安全性。

- 网络计费的灵活性

可以在 LAC 和 LNS 两处同时计费，即 ISP 处（用于产生帐单）及企业处（用于付费及审记）。L2TP 能够提供数据传输的出入包数、字节数以及连接的起始、结束时间等计费数据，还可以根据这些数据方便地进行网络计费。

- 可靠性

L2TP 协议支持备份 LNS。当一个主 LNS 不可达之后，LAC（接入服务器）可以重新与备份 LNS 建立连接，这样增加了 VPN 服务的可靠性和容错性。

- 统一的网络管理

L2TP 协议将很快成为标准的 RFC 协议，有关 L2TP 的标准 MIB 也将很快得到制定，这样可以统一地采用 SNMP 网络管理方案进行方便的网络维护与管理。

GRE：

GRE（Generic Routing Encapsulation）即基本路由封装协议是对某些网络层协议（如：IP 和 IPX 等）的数据报进行封装，使这些被封装的数据报能够在另一个网络层协议（如 IP）中传输。GRE 是 VPN（Virtual Private Network ）的第三层隧道协议，即在协议层之间采用了一种被称之为 Tunnel（隧道）的技术。Tunnel 是一个虚拟的点对点的连接，在实际中可以看成仅支持点对点连接的虚拟接口。这个接口提供了一条通路使封装的数据报能够在这个通路上传输，并且在一个 Tunnel 的两端分别对数据报进行封装及解封。

GRE 提供了以下几种服务类型：

- 多协议的本地网通过单一协议的骨干网传输的服务；
- 扩大了网络的工作范围，包括那些路由网关有限的协议；
- 将一些不能连续的子网连接起来。

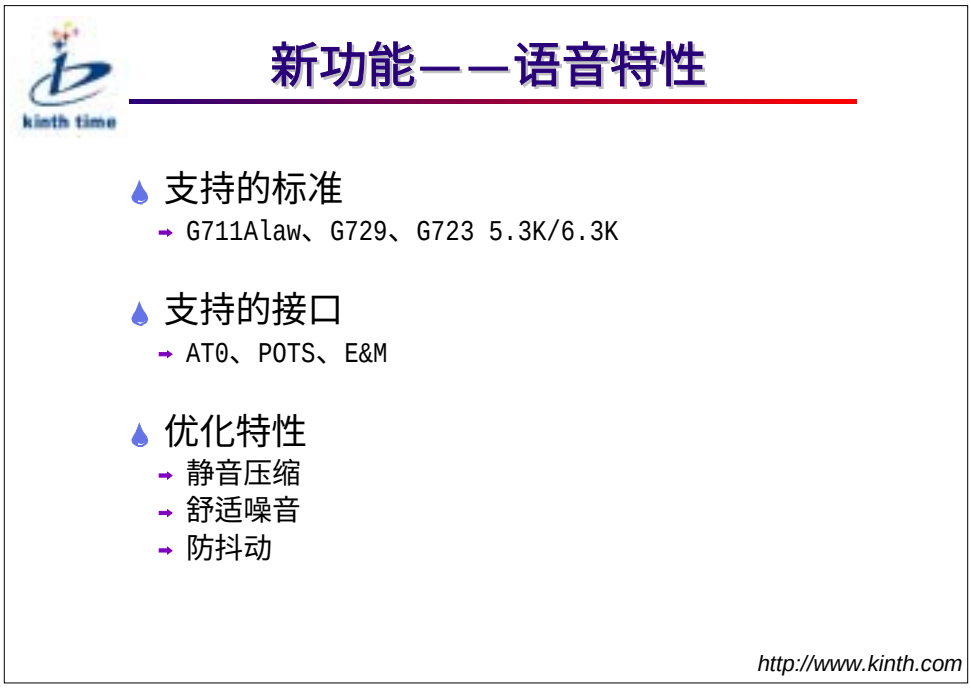
IPSec：

IPSec（IP Security）是 IETF 制定的为了保证在 Internet 上传送数据的安全保密性能的一系列协议。IPSec 包括 AH 和 ESP 两个协议，AH（Authentication Header）是报文验证头协议，主要提供的功能有数据源验证、数据完整性校验和防报文重放功能；ESP（Encapsulating Security Payload）是报文安全封装协议，在 AH 协议的功能之外再提供对 IP 报文的加密功能。IPSec 在 IP 层对 IP 报文提供安全服务，对 IP 层以上的各种协议和应用是透明的，几乎不需要网络基础设施做任何附加的改动，只要在安全隧道两端的两台路由器或主机具有 IPSec 功能即可。此外，因特网密钥交换协议（Internet Key Exchange —— IKE）为 IPSec 提供了自动协商交换密钥、建立安全联盟的服务，能够简化 IPSec 的使用和管理。IPSec 将成为 Internet 的安全基石。

通过 IPSec，数据流能够穿过公共网而不用担心被偷窥或修改。它的最

典型的应用就是通过 Intranets、Extranets、以及远程拨号用户建立 VPN（Virtual Private Network）。

.4.3 语音特性



VoIP 的主要目的是为企业降低高昂的长话费用及简化网络的构建和管理，通过统一的网络平台，提供话音与数据的集成应用。下面我们针对企业采用华为公司的 VoIP 产品实现具体的组网方案，一般来说，WAN 网络应该有足够的带宽，最好有 QoS 保障。

标准支持

支持 G711Alaw、G729、G723 5.3K/6.3K、H225.0、H245、RFC1889、RFC1890；严格按照 ITU 和 IETF 的系列标准，能够同所有遵从国际通用标准的路由器语音设备、IP 网关设备、电信级语音设备等互通，具有良好的互通性和兼容性。另一方面，还积极参与和跟踪新标准的制定，保持技术领先者的优势。

接口丰富

支持 POTS、AT0、E&M、E1 等；能够支持国内外绝大部分主流 PSTN 设备的接口，丰富的接口支持能够有效的保护商家在 PSTN 上的已有投资，实现传统电话同 IP 电话的无缝连接，使商家能够逐步实现从传统话音业务到完全的语音业务的过渡。

提供好的话音质量是语音技术应用的基础，Quidway 路由器解决了 VoIP 的几个关键技术，使语音质量达到普通电话的效果：

- 时延

影响时延的因素有多个方面，编解码、网络、防抖动缓冲、报文队列等都影响时延。其中有些是固定时延，如编解码网络速率等；有些是

变化的，如防抖动缓冲和队列调度等。固定的时延可以通过改变编解码方式和提高网络速率来改善，而变化的时延通常采用提高转发效率来改善。目前华为主要通过快速转发的技术来提高报文的转发效率。

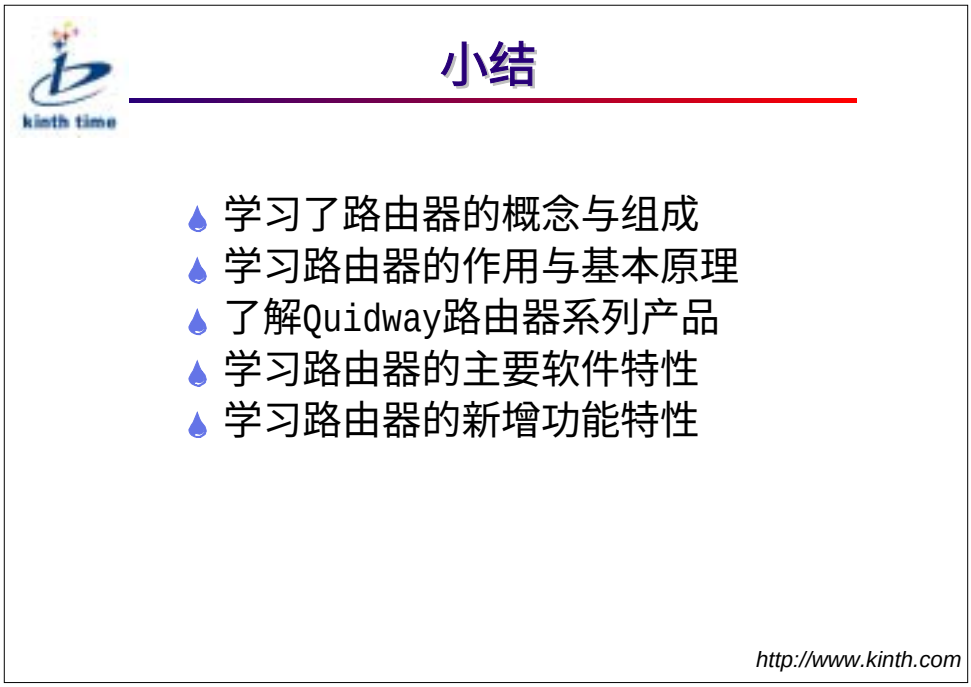
- 抖动

影响抖动的因素通常与网络的拥塞程度相关。由于语音与数据在同一条物理线路上传输，语音数据通常会由于数据报文占用了物理线路而导致阻塞。解决抖动通常采用缓冲队列来解决，另外提供 QoS 和资源预留使语音数据获得优先发送和获得固定的带宽也是解决抖动问题的主要手段。目前华为主要采用 QoS 队列调度和缓冲队列的方式解决抖动问题。

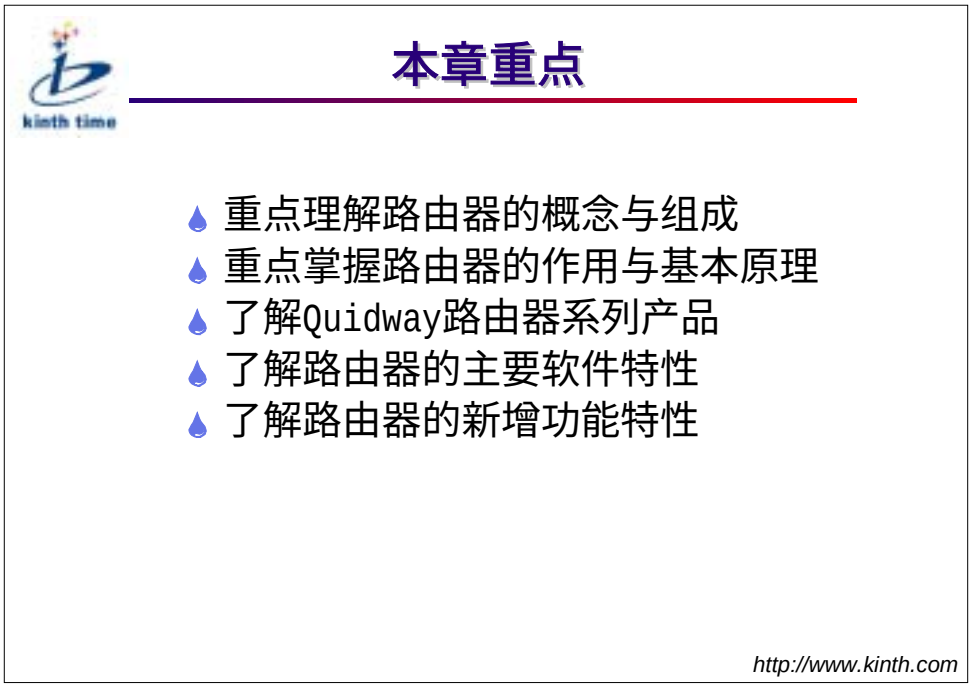
- 话音质量

质量问题是 VoIP 要解决的主要问题。话音质量除了与编解码方式有关外，与网络的拓扑结构、拥塞程度等都有很大的关系。现在解决网络引起话音质量的技术已经有很多，主要从两个方面来解决：一种方式是采用资源预留策略（RSVP），预先为语音数据保留一部分带宽；另一种方式是为语音数据设立高优先级队列或定制队列（PQ/CQ），当有语音数据时，优先发送语音数据。两种策略各有优缺点，都可以解决话音质量问题。

.5 小结


kinth time
小结
学习了路由器的概念与组成
学习路由器的作用与基本原理
了解Quidway路由器系列产品
学习路由器的主要软件特性
学习路由器的新增功能特性
http://www.kinth.com

.6 本章重点


kinth time
本章重点
重点理解路由器的概念与组成
重点掌握路由器的作用与基本原理
了解Quidway路由器系列产品
了解路由器的主要软件特性
了解路由器的新增功能特性
http://www.kinth.com