华为网络工程师培训

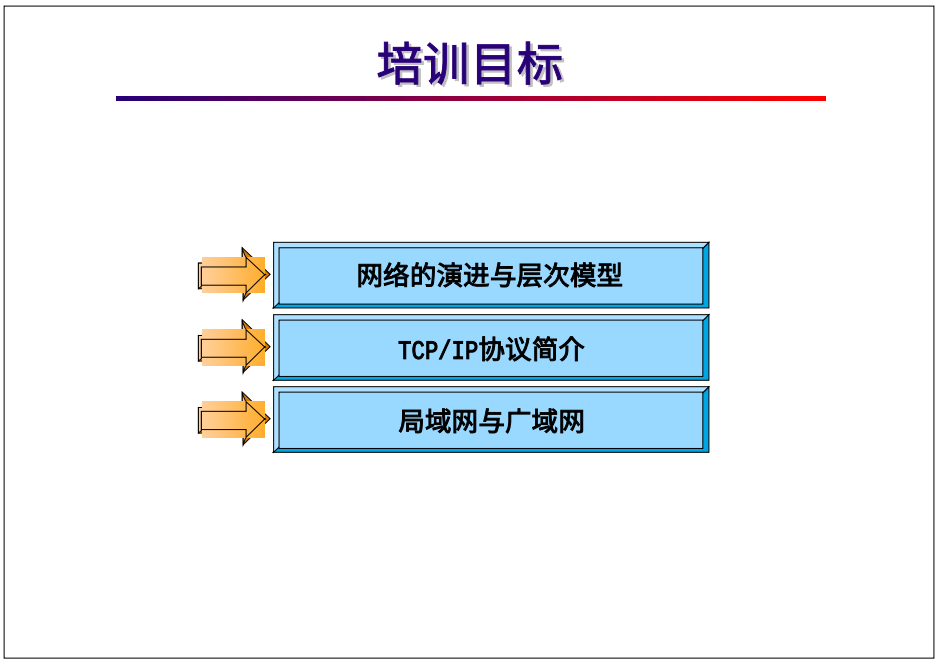
基础教程

西南师范大学网络技术室整理

2005.5

第一章 网络基础知识

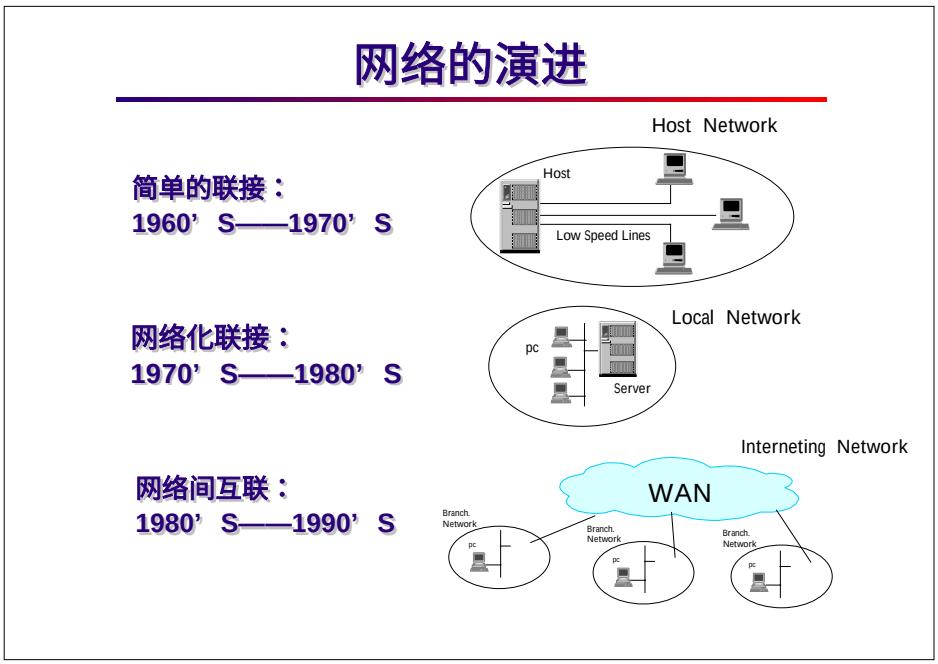
.1 培训目标



本章介绍网络的基础知识，包括网络的演进和层次化模型、TCP/IP 协议简介、局域网和广域网的定义及常用设备原理、常用协议原理与常用组网方式、一些协议特性的比较、以及不同的费用和性能需求下网络组网方式的选用。

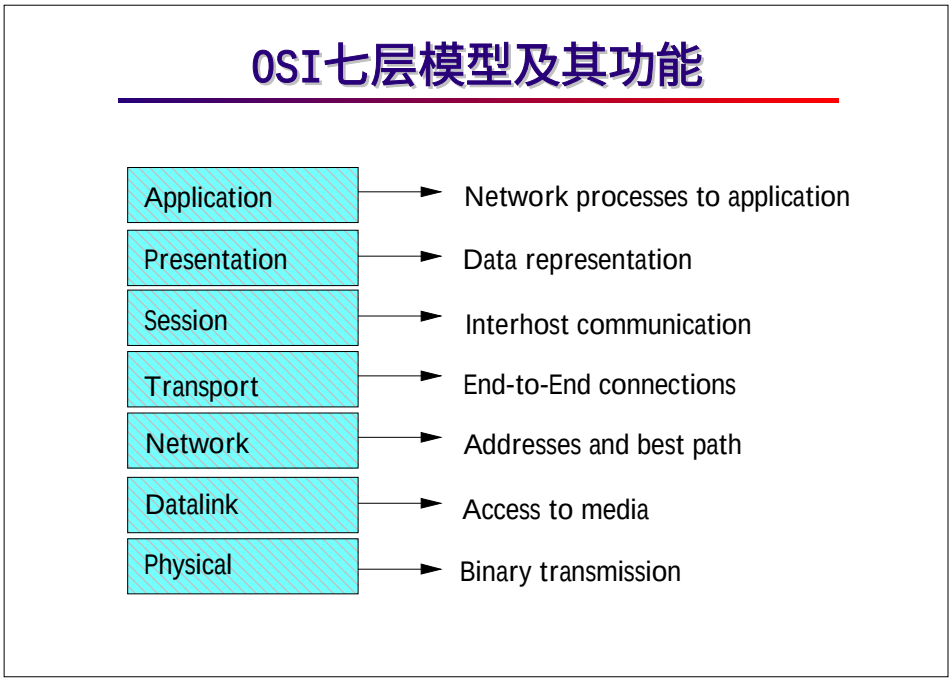
.2　网络的演进与层次模型

.2.1　网络的演进



六十至七十年代，网络的概念主要是基于主机架构的低速串行联接，提供应用程序执行、远程打印和数据服务功能。IBM 的 SNA 架构与非 IBM 公司的 X.25 公用数据网络是这种网络的典型例子。
七十至八十年代，出现了以个人电脑为主的商业计算模式。最初，个人电脑是独立的设备，由于认识到商业计算的复杂性，局域网产生了。局域网的出现，大大降低了商业用户打印机和磁盘昂贵的费用。
八十年代至九十年代，远程计算的需求不断地增加，迫使计算机界开发出多种广域网络协议，满足不同计算方式下远程联接的需求，网间网的互联极大程度地发展起来。

.2.2　OSI 七层模型及其功能



在七十年代末，国际标准化组织 ISO 提出了开放系统互连参考模型。协议分层大大简化了网络协议的复杂性，这实际也是自顶向下、逐步细化的程序设计方法的很好的应用。网络协议按功能组织成一系列“层”，每一层建筑在它的下层之上。分成的层数，每一层的名字、功能，都可以不一样，但是每一层的目的都是为上层提供一定的服务，屏蔽低层的细节。

物理层涉及到通信在信道上传输的原始比特流，它实现传输数据所需要的机械、电气、功能性及过程等手段。

数据链路层的主要任务是提供对物理层的控制，检测并纠正可能出现的错误，使之对网络层显现一条无错线路；并且进行流量调控。

网络层检查网络拓扑，以决定传输报文的最佳路由，其关键问题是确定数据包从源端到目的端如何选择路由。

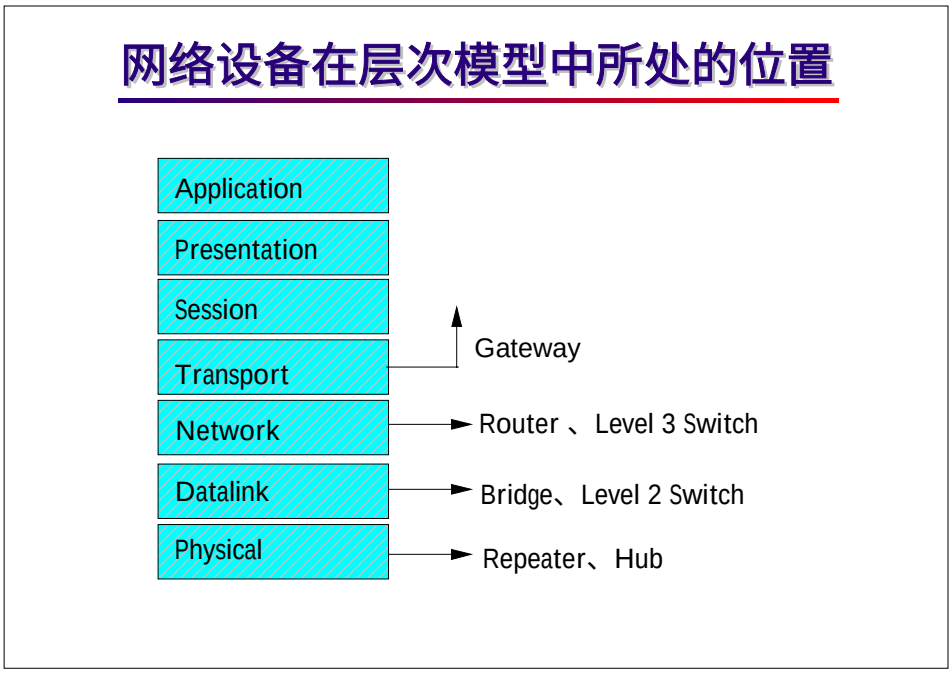
传输层的基本功能是从会话层接受数据，并且在必要的时候把它分成较小的单元，传递给网络层，并确保到达对方的各段信息正确无误。

会话层允许不同机器上的用户建立会话关系，在协调不同应用程序之间的通信时要涉及会话层，该层使每个应用程序知道其它应用程序的状态。

表示层关注于所传输的信息的语法和意义，它把来自应用层与计算机有关的数据格式处理成与计算机无关的格式。

应用层包含大量人们普遍需要的协议，并且具有文件传输功能。其任务是显示接收到的信息，把用户的新数据发送到低层。

.2.3　网络设备在层次模型中所处的位置

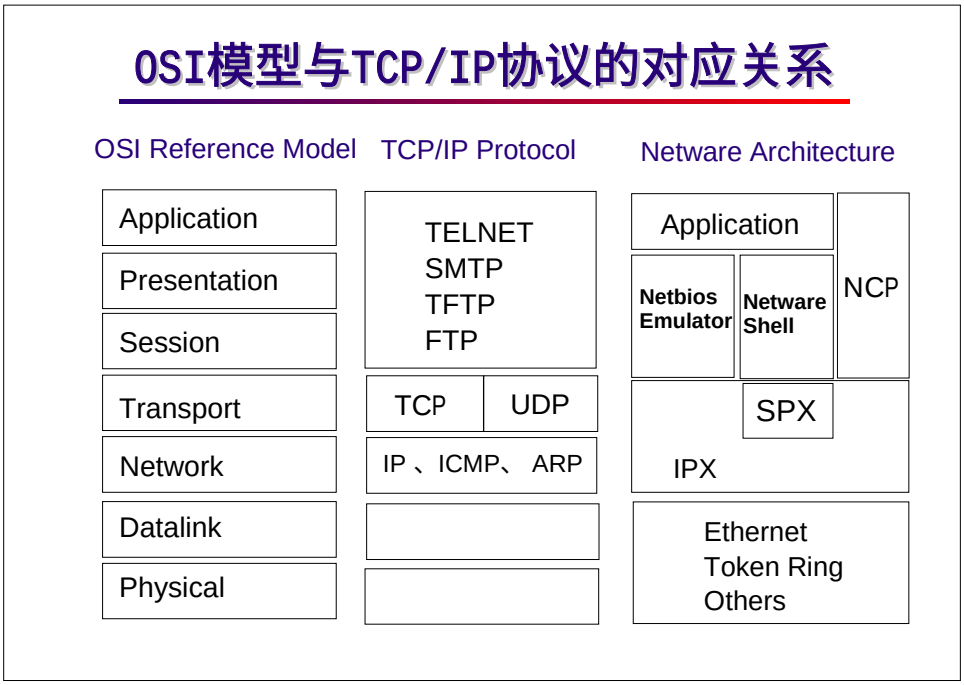


在分层模型中，对等是一个很重要的概念，因为只有对等层才能相互通信，一方在某层上的协议是什么，对方在同一层次上也必须是什么协议。理解了对等的含义，则很容易把网络互连起来：
两个网络在物理层就相同，使用中继器就可以连起来；如果两个网络物理层不同，链路层相同，使用桥接器可以连起来；如果两个网络物理层、链路层都不同，而网络层相同，使用路由器可以互连；如果两个网络协议完全不同，使用协议转换器（网关）可以互连。
上面提到的设备分别是：

- ☞ 中继器（Repeater）：工作在物理层，在电缆之间逐个复制二进制位（bit）；
- ☞ 桥接器（Bridge）：工作在链路层，在 LAN 之间存储和转发帧（frame）；
- ☞ 路由器（Router）：工作在网络层，在不同的网络之间存储和转发分组（packet）。
- ☞ 协议转换器（Gateway）：工作在三层以上，实现不同协议的转换。

Internet 中通常把路由器也叫网关（Gateway）。

.2.4　OSI 模型与TCP/IP 协议的对应关系



今世界上最流行的 TCP/IP 协议的层次并不是按 OSI 参考模型来划分的，只跟它有一种大致的对应关系。

网络层协议主要包括 IP 协议，实现 IP 包的封装和发送，分组路由和避免阻塞是这里的关键设计问题。

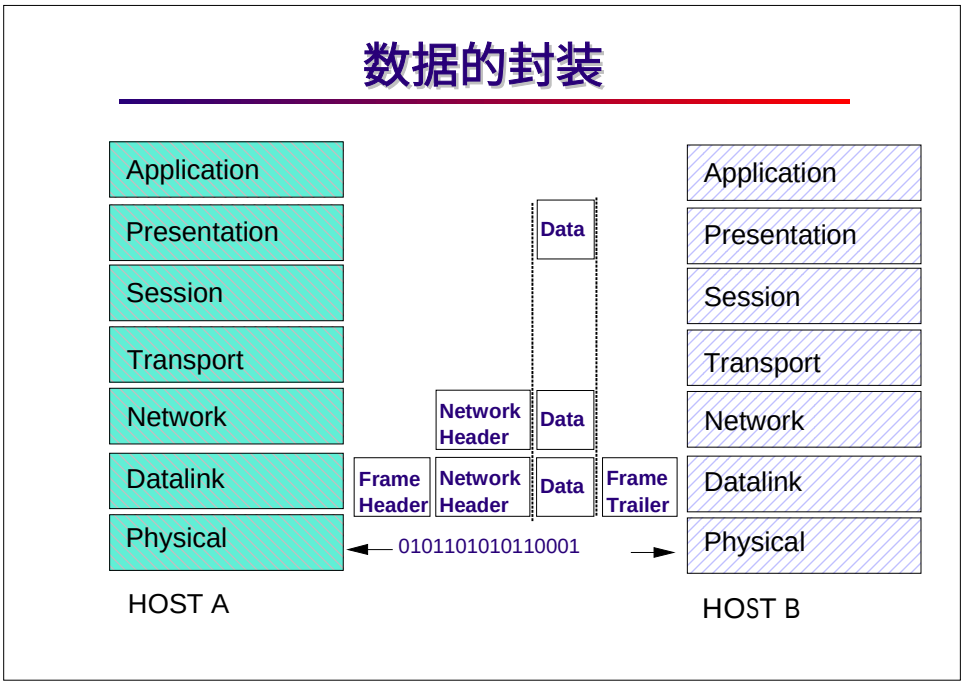
传输层定义了两个端到端的协议：传输控制协议 TCP 和用户数据报协议 UDP。

TCP/IP 不涉及会话层和表示层。

应用层含有所有的高层协议，如虚拟终端协议 Telnet、文件传输协议 FTP 和 电子邮件协议 SMTP。

另有 NOVELL 公司的 SPX/IPX　协议以供参照。

.2.5　数据的封装

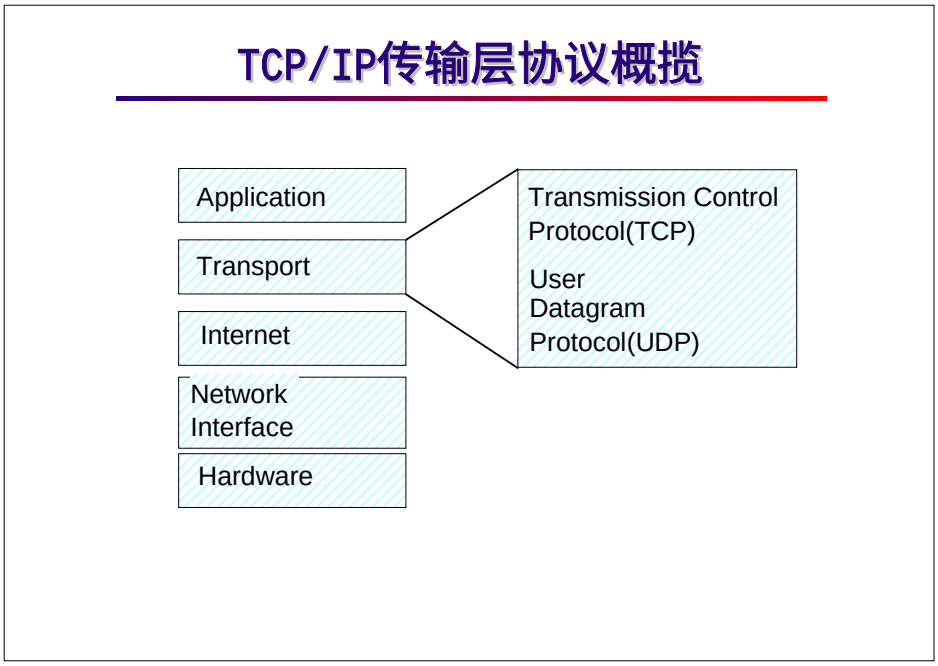


信息交换的过程发生在对等层之间，源系统中的每一层把控制信息附加在数据中，而目的系统的每一层则对接收到的信息进行分解，并从数据中移去控制信息。

高层的协议将数据传递到网络层后，形成标准的数据包，而后传送到数据链路层，添加链路层的控制信息，形成帧，再传递到物理层，在物理层网络传送原始的比特流。

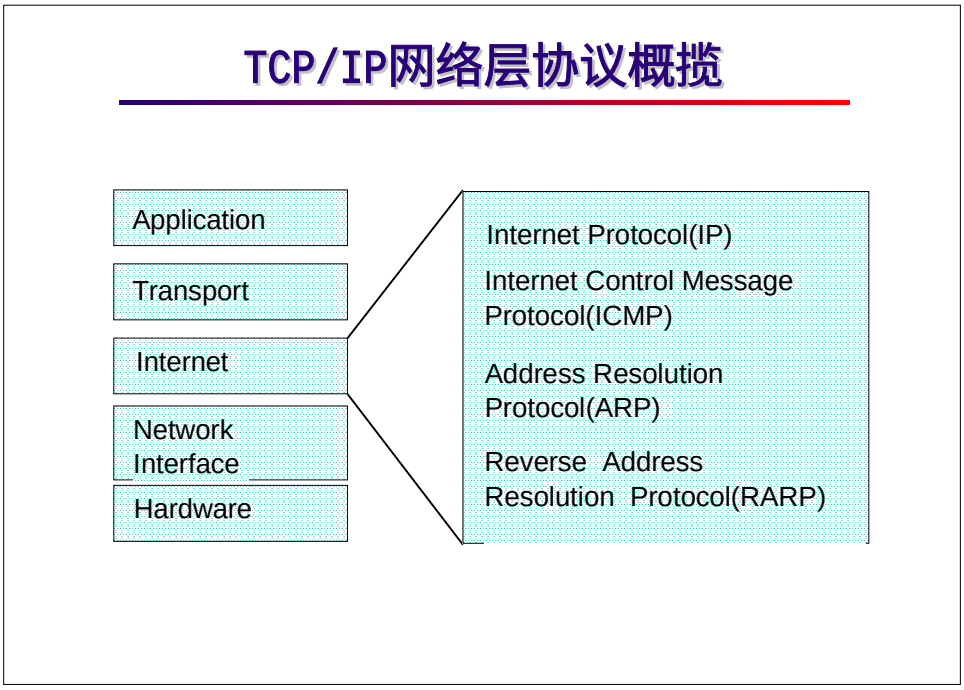
.3　TCP/IP 协议简介

.3.1　TCP/IP 传输层协议概揽



传输控制协议 TCP 是一个面向联接的协议，允许从一台机器发出的字节流无差错地发往到互联网上的其他机器。
用户数据报协议 UDP 是一个不可靠的无联接的协议，用于不需要排序和流量控制能力而是自己完成这些功能的应用程序。

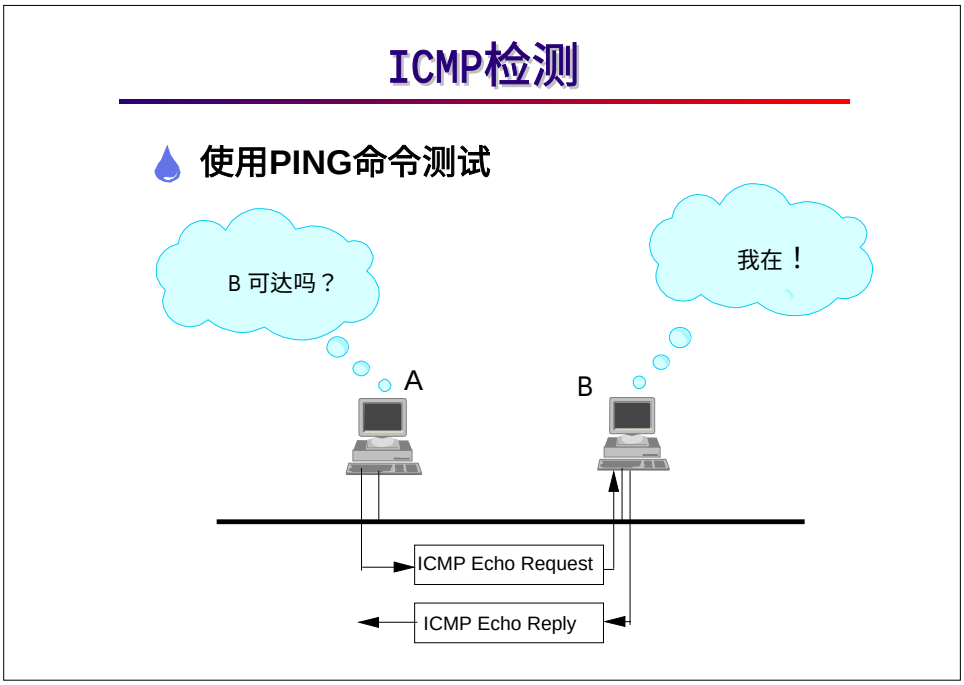
.3.2　TCP/IP 网络层协议概揽



网络层的 IP 协议，实现了 IP 包的封装和寻径发送，它的功能是主机可以把分组发往任何网络并使分组独立地传向目标。这些分组到达的顺序和发送的顺序可能不同。

另外，TCP/IP 的网络层还包括了 互联网络控制消息协议 ICMP、地址解析协议 ARP、反向地址解析协议 RARP。

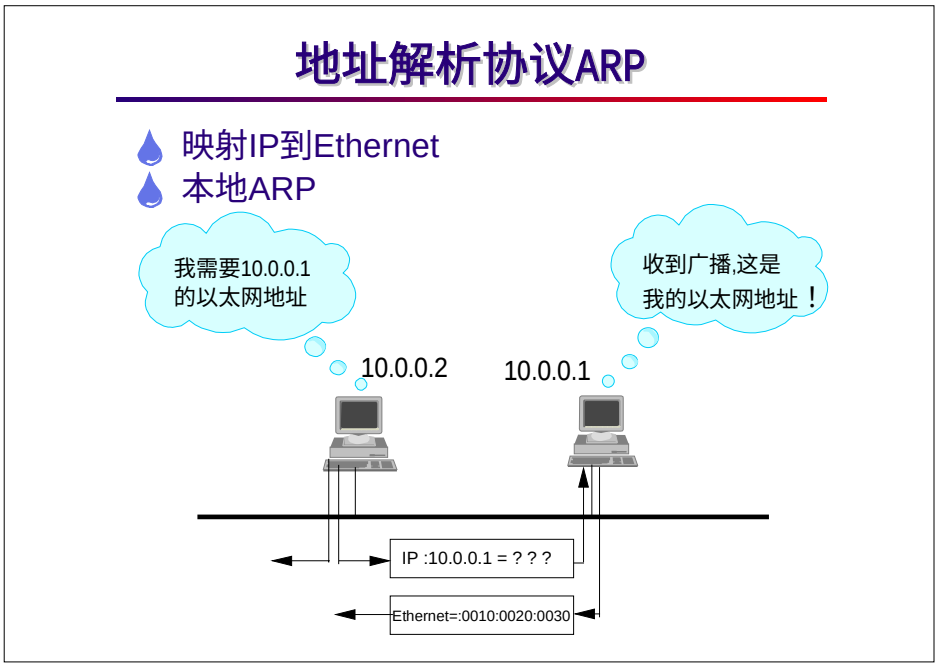
.3.3　ICMP 检测



互联网络控制消息协议 ICMP 是一个网络层的协议，它提供了错误报告和其它回送给源点的关于 IP 数据包处理情况的消息，RFC 792 中有关于 ICMP 的详细说明。

ICMP 包含几种不同的消息，其中 Echo Request 由 Ping 命令产生，主机可通过它来测试网络的可达性，ICMP Echo Reply 消息表示该节点是可达的。

.3.4　地址解析协议 ARP



地址解析协议 ARP 是一种广播协议，主机通过它可以动态地发现对应于一个特殊 IP 网络层地址的 MAC 层地址。

主机 A 发送的 ARP 请求报文中，带有自己的 IP 地址到 MAC 地址的映射。主机 B 收到请求报文后，将其中的地址映射存到自己的 ARP 高速缓存中，并把自己的 IP 地址到 MAC 地址的映射作为响应发回主机 A。

.4　局域网与广域网

.4.1　LAN 定义

LAN 是一个覆盖地理范围相对较小的高速容错数据网络，它包括工作站、个人计算机、打印机和其它设备。
LAN 为计算机用户提供了资源共享的设备访问，如打印、文件交换、电子邮件交换等等。
在这种环境中，LAN 定义了一系列的协议支持局域网网络设备的顺利运行。

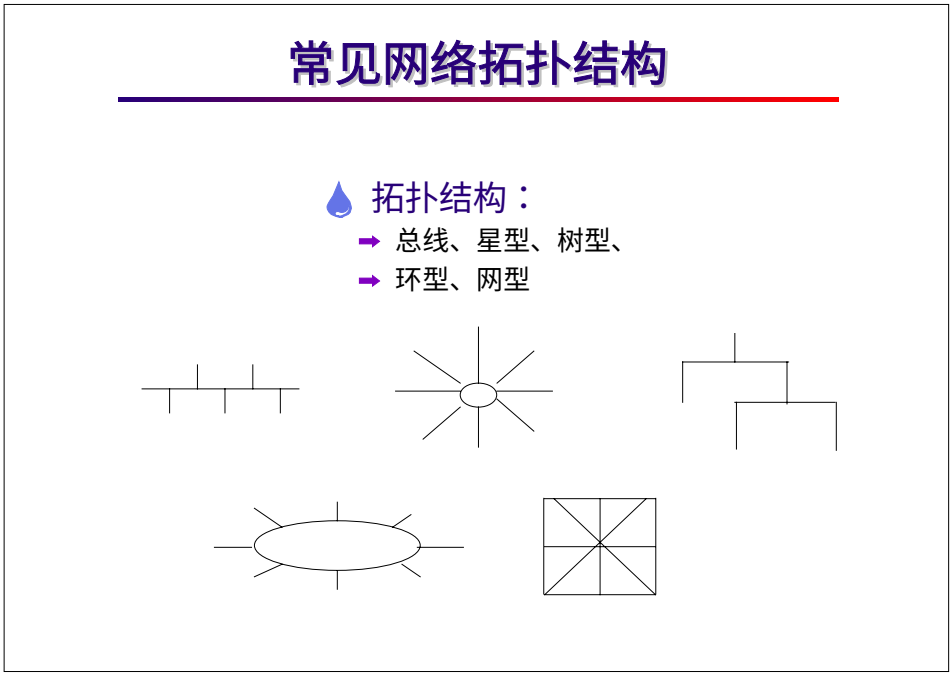
.4.2　LAN 及其常用设备

LAN 的设计目标主要面对有限的地理区域，它允许同时访问高带宽的介质。

LAN 主要通过局部管理控制网络的私有权利，提供全时的局部服务，其连接物理设备一般在相对较近的环境中。

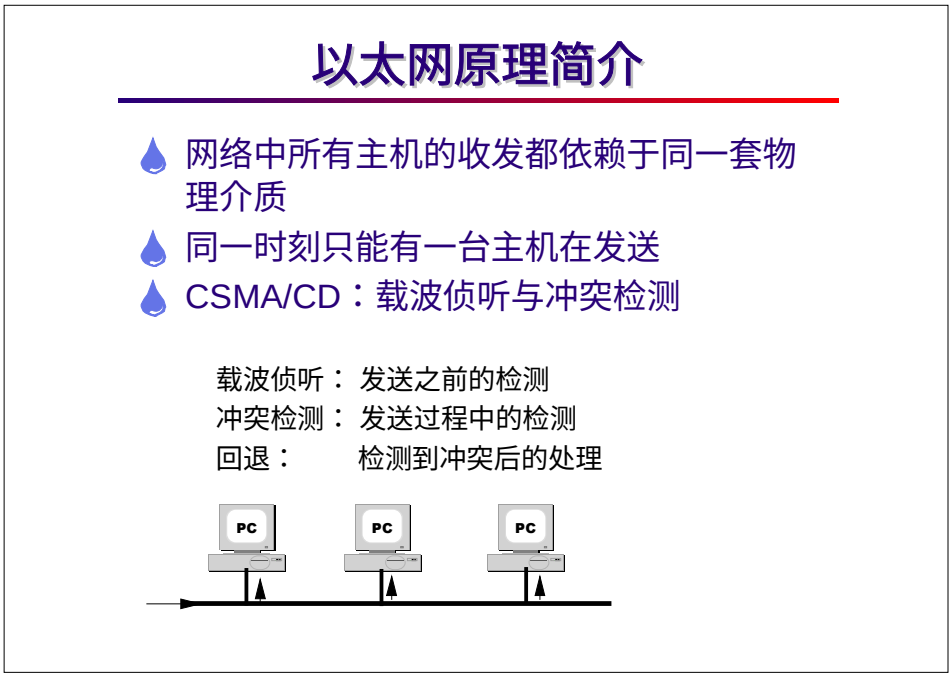
LAN 的传输形式一般以总线型为主，最常见的以太网采用了载波侦听与冲突检测 CSMA/CD 协议以支持总线型的结构。

.4.3　常见网络拓扑结构



LAN 的拓扑结构定义了组织网络设备的方法，LAN 有总线型、星型、树型环型和网型等多种拓扑结构。
这些拓扑结构是逻辑结构，和实际的物理设备的构型没有必然的关系，如逻辑总线型和环型拓扑结构通常表现为星型的物理网络组织。

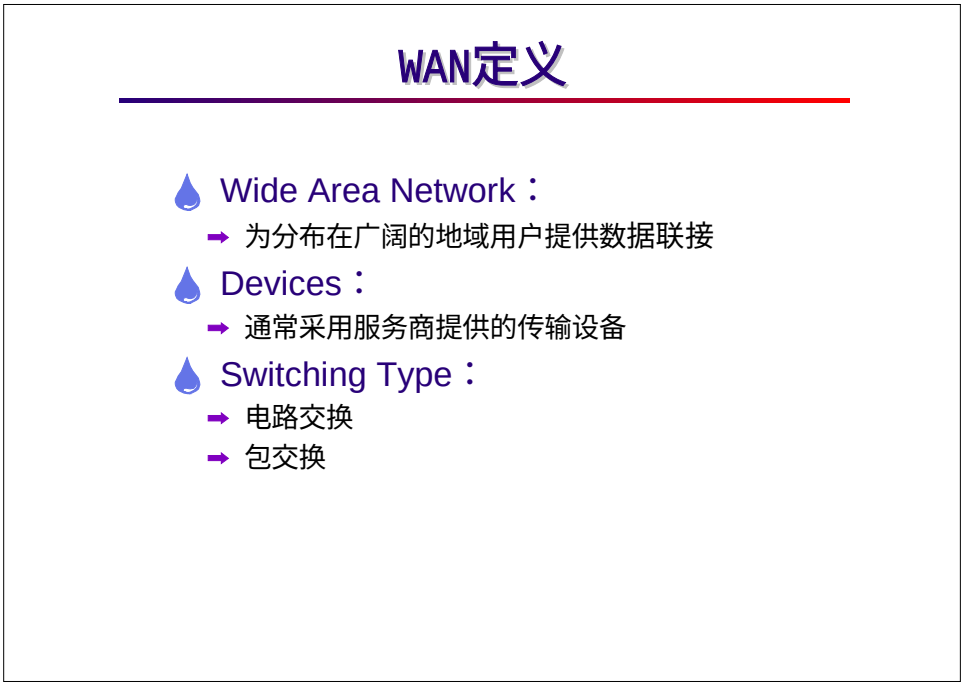
.4.4　以太网原理简介



基于广播的以太网中，所有的工作站都可以接收到发送到网上的广播帧，每个工作站都要经过判断确认信息帧是否是发给自己的，如是，则转到高层的协议层去。

采用了载波侦听与冲突检测 CSMA/CD 协议的以太网中，工作站在发送数据之前，要侦听网络是否空闲，只有在网络不阻塞时，工作站才能发送数据。

.4.5　WAN 定义



WAN 是覆盖地理范围相对较广的数据通信网络，它通常利用公共载波公司提供的便利条件进行传输。

WAN 技术在 OSI 参考模型的下三层（即物理层、数据链路层和网络层）发挥作用。

WAN 通常采用两种交换模式运行，即电路交换和分组交换技术。

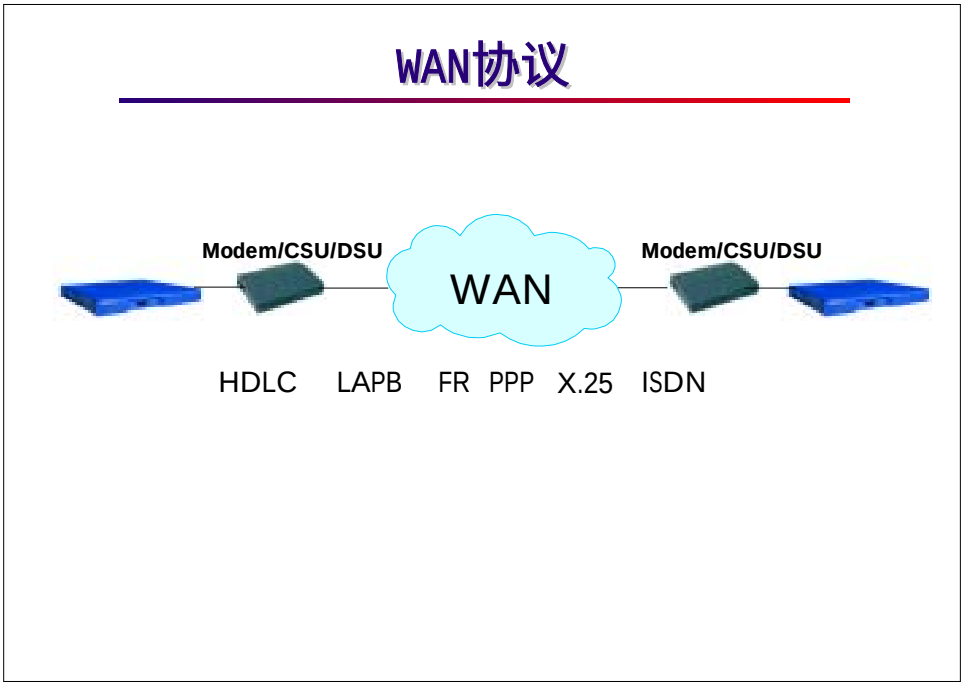
电路方式是基于电话网电路交换的原理，当用户要求发送数据时，交换机就在主叫用户和被叫用户之间接通一条物理的数据传输通路。特点是时延小、“透明”传输（即传输通路对用户数据不进行任何修正或解释）、信息传输的吞吐量大。缺点是所占带宽固定，网络资源利用率低。

分组方式是一种存储转发的交换方式。它是将需要传输的信息划分为一定长度的包（分组），以分组为单位进行存储转发的。每个分组信息都载有接收地址和发送地址的的标识，在传送分组之前必须首先建立虚电路，然后依序传送。分组方式在线路上采用动态复用的技术来传送各个分组，带宽可以复用。缺点是实时性不好。

.4.6　WAN 及其常用设备

常用的 WAN 设备有 Modem /CSU/DSU、路由器、广域网交换机、接入服务器、ATM 交换机等。

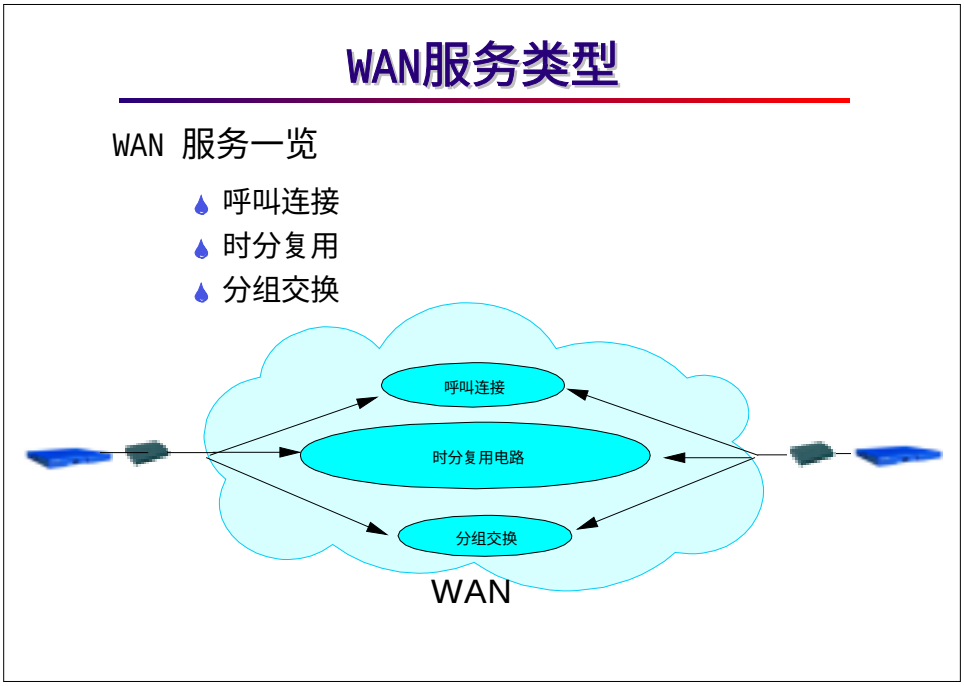
.4.7　WAN 协议



常用的广域网协议有：

- HDLC：高级数据链路控制，ISO 标准的链路层协议；
- LAPB：平衡型链路访问规程，增强了错误检测和更正；
- PPP：点到点协议，有丰富功能的同异步链路层协议；
- X.25：分组交换协议，定义了终端和分组交换网络的连接规程；
- FR：帧中继，在 X.25 基础上发展起来的简洁高效的分组交换协议；
- ISDN：语音数据共享的数字化链路。

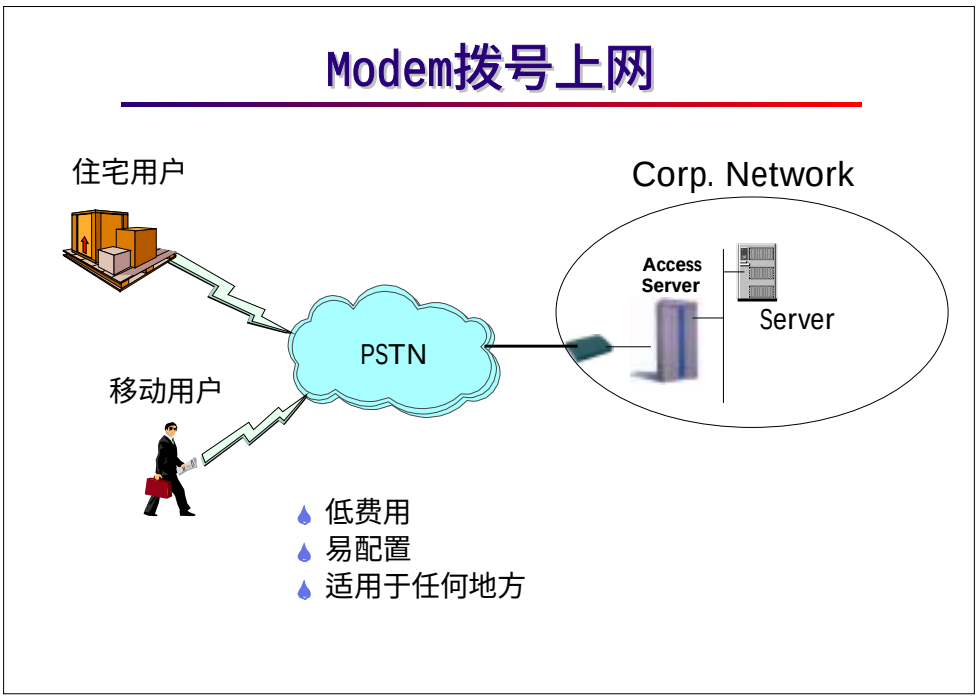
.4.8　WAN 服务类型



常用的广域网服务类型可分为：

- 呼叫连接：通过信令如 SS7 建立连接所成网络，例如 Modem 拨号；
- 时分复用：利用时分复用设备连接的网络，如专用线路；
- 分组交换：利用分组交换网络连接的网络，如帧中继、X.25。

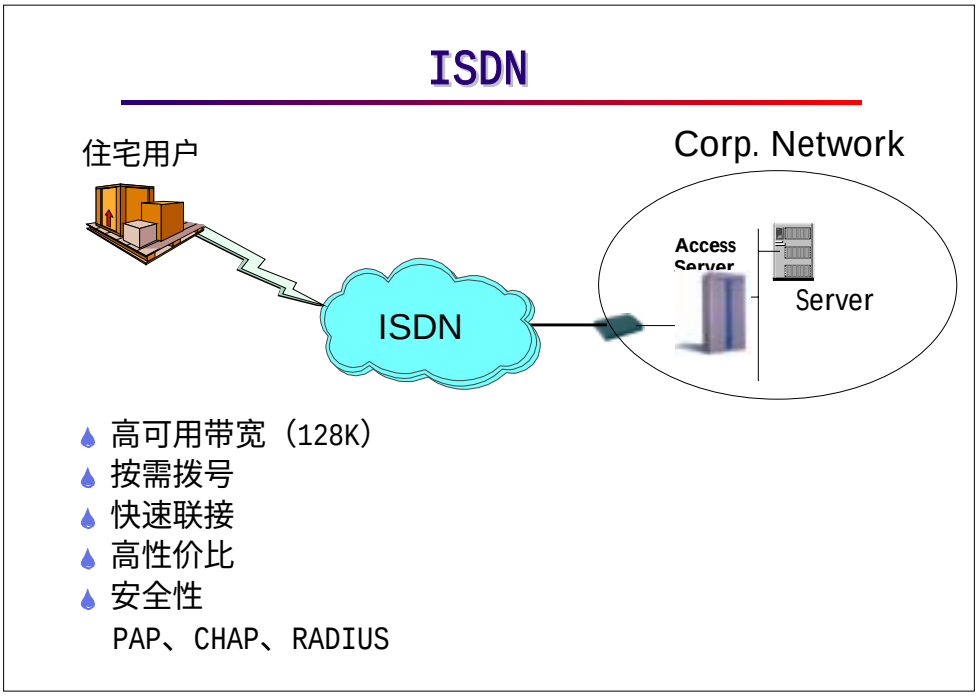
.4.9　Modem 拨号上网



异步 Modem 使用传统的电话网络，并且工作于异步传输模式，传统的电话网络有以下优势：

- 任何地方的可用性：由于传统电话网络的性质决定；
- 容易配置：易于配置，只需简单的参数配置；
- 按需拨号：只在所需要的时候进行联接；
- 低费用：没有其它网络昂贵的设备和运行费用。

.4.10　ISDN 简介

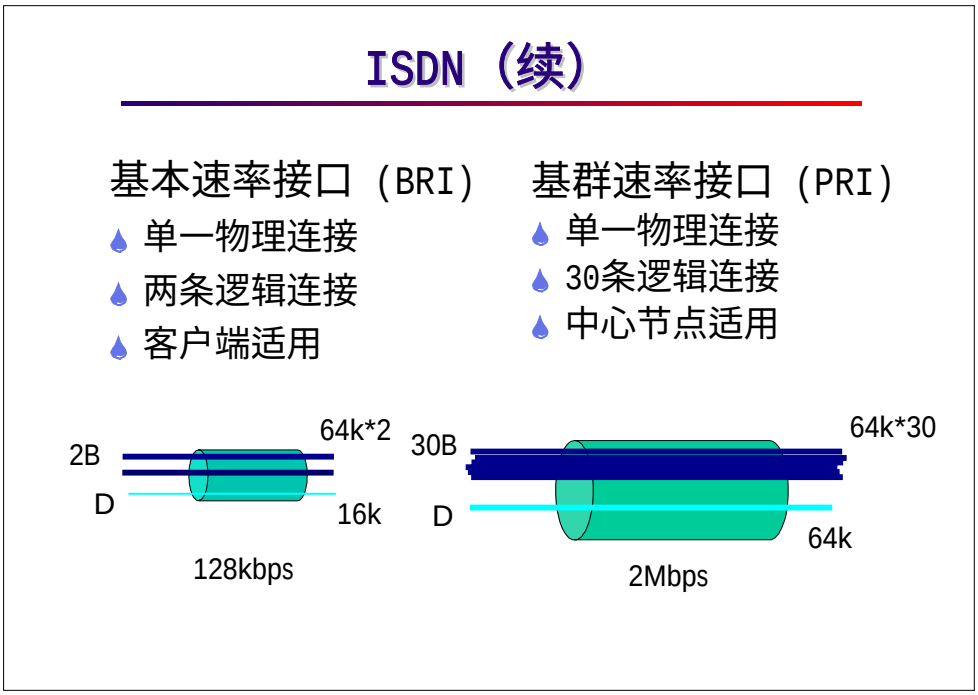


ISDN 是一种标准化的数字服务。ISDN 可以在现有的铜线上传输语音、数据、视频。ISDN 不同于专线连接模式，它是拨号激活的，相对于昂贵的专用线路，可以很大程度的节省费用。

ISDN 提供多种安全措施：

- 呼叫链路识别：此功能由服务商提供；
- PAP：明文传送的密码验证；
- CHAP：密文传送的密码验证；
- RADIUS：工业标准的 Client/Server 结构安全访问协议。

ISDN 简介（续）



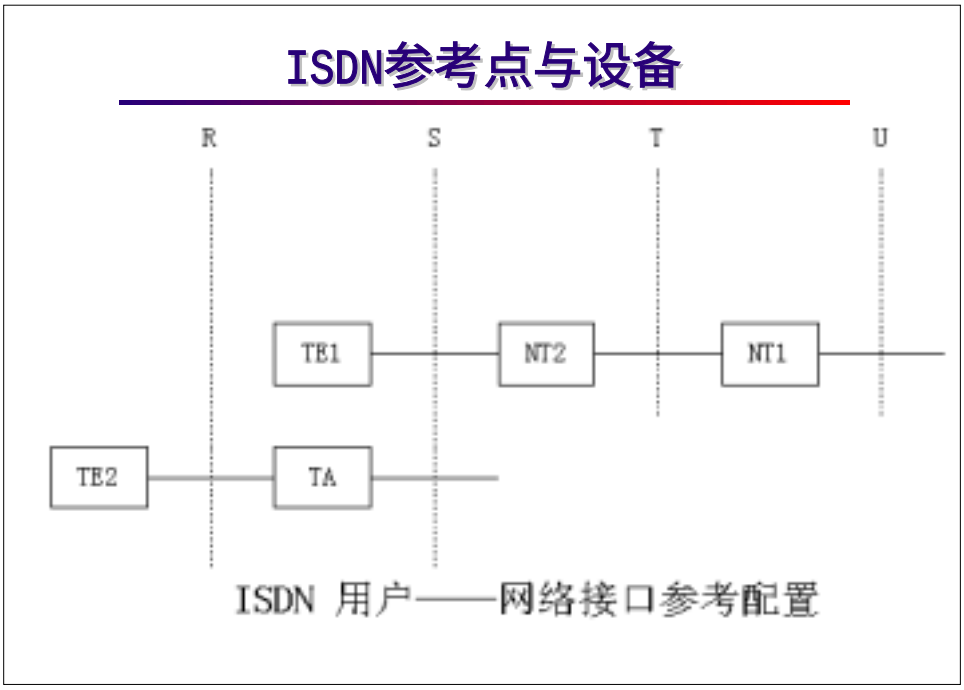
ISDN 的两种信道：

- B 信道（64Kbps）；
- D 信道（16 或 64Kbps）。

ISDN 用户接口类型：

- 基本速率接口（BRI）：2B+D（192Kbps）；
- 基群速率接口（PRI）：30B+D（2048Kbps）。

ISDN 简介（续）



功能群和参考点概念的提出是为了定义 ISDN 用户——网络接口上的配置和建立接口标准。功能群是指用户接入 ISDN 所需的一组功能，而参考点是用来分割功能群的概念上的点。

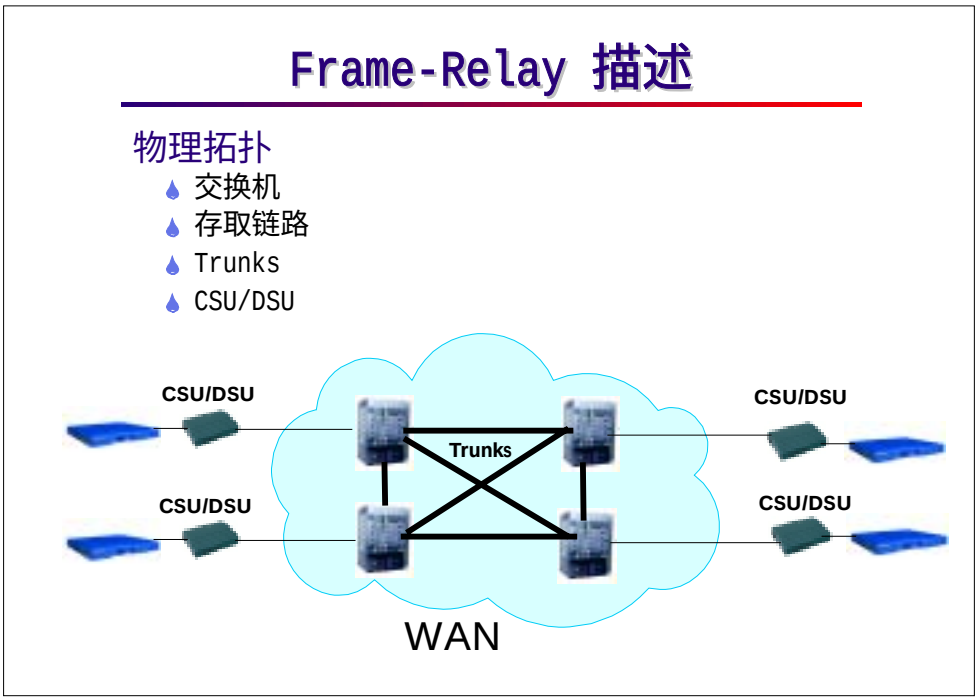
用户接入 ISDN 的功能可以划分为以下功能群：

- 网络终端 1（NT1）：包含 OSI 第一层的功能，ISDN 在用户处的物理和电器终端装置，在 NT1 上要处理 D　　信道竞争的问题；
- 网络终端 2（NT2）：包含 OSI　一到三层的功能；
- 1 类终端设备（TE1）：ISDN　标准终端设备；
- 2 类终端设备（TE2）：非 ISDN　标准终端设备；
- 终端适配器（TA）：完成将 TE2 接入 ISDN 的速率和协议等方面的适配功能。

参考点：

- T 参考点：NT1 与 NT2 之间，是用户和网络之间的分界点（NT1 属于网管部门，NT2 属于用户；
- S 参考点：TE1 和 NT2 之间，对应于单个 ISDN 终端设备接入网络的接口，将用户终端和与网络有关的功能分开；
- U 参考点：对应于用户线，用来描述用户线上的双向数据信号；
- R 参考点：位于 TE2 和 TA 之间，用于提供非标准 ISDN 标准终端的入网接口。

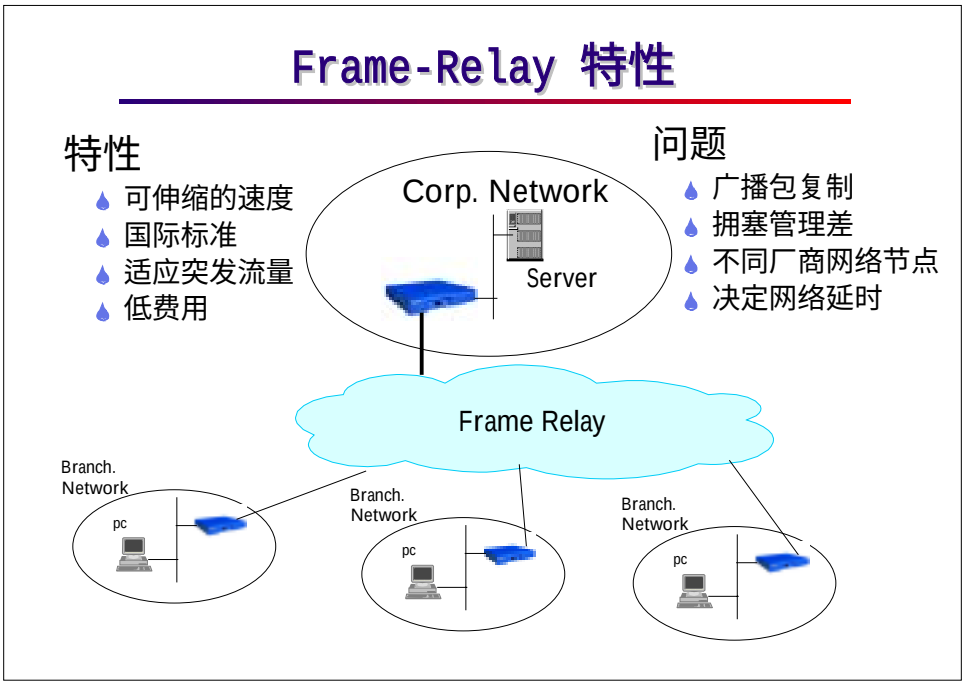
.4.11　Frame-Relay 描述



帧中继技术是在数据链路层用简化的方法传送和交换数据单元的快速分组交换技术。帧中继技术是在分组交换技术充分发展、数字与光纤传输线路逐渐代替已有的模拟线路、用户终端日益智能化的条件下诞生并发展起来的。

帧中继仅完成 OSI 物理层和链路层核心层的功能，将流量控制、纠错等留给智能终端完成，大大简化了节点机之间的协议；同时，帧中继采用虚电路技术，能充分利用网络资源，因此帧中继具有吞吐量高、时延低、适合突发性业务等特点。帧中继对于 ATM 网络，是一个重要的可选项。帧中继作为一种附加于分组方式的承载业务引入 ISDN，其帧结构与 ISDN 的 LAPD 结构一致，可以进行逻辑复用。

.4.12　Frame-Relay 特性



帧中继技术主要有以下几点特性：

在链路层完成统计复用、帧透明传输和错误检测，但不提供发现错误后的重传操作。省去了帧编号、流量控制、应答和监视等机制，大大节省了交换机的开销，提高了网络吞吐量、降低了通信时延。一般帧中继用户的接入速率在 64Kbps-2Mbps，具有可伸缩的速度。

帧中继是一种国际标准，并日益得到广泛地应用。

交换单元——帧的信息长度比分组长度要长，预约的最大帧长度至少要达到 1600 字节/帧，适合封装局域网的数据单元。用户能有效地利用预约的带宽，即承诺的信息速率（CIR），还允许用户的突发数据占用未预定的带宽，以提高网络资源的利用率。

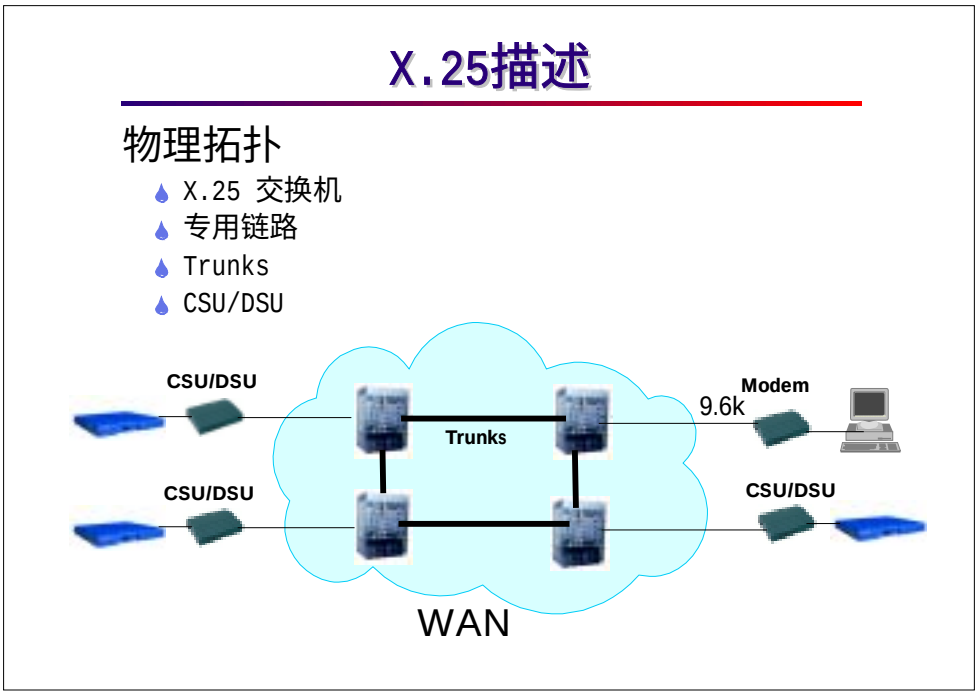
帧中继协议简化了 X.25 的第三层功能，使网络节点的处理大大简化，提高了网络对信息的处理效率。帧中继传送数据使用的传输链路是逻辑连接，而不是物理连接，在一个物理连接上可以复用多个逻辑连接，可以实现带宽的复用和动态分配，降低了网络联接的费用。

由于帧中继协议的非广播特性，广播包的传递必须靠路由器的复制，会降低有效带宽的利用率并降低网络设备的性能。

提供一套带宽管理和防止拥塞的机制，但这种机制需要端设备协议的配合，包括路由器、广域网交换机等，否则没有良好的拥塞管理。

不同厂商的设备互操作性的问题，可能导致帧中继网络的延迟很大。

.4.13　X.25 描述



X.25 协议是数据终端设备（Data Terminal Equipment，DTE）和数据电路终接设备（Data Circuit_terminating Equipmert，DCE）之间的接口规程，其主要功能是描述如何在 DTE 和 DCE 之间建立虚电路、传输分组、建立链路、传输数据、拆除链路、拆除虚电路， 同时进行差错控制、流量控制、情况统计等，并且为用户提供了一些可选的业务功能和配置功能。

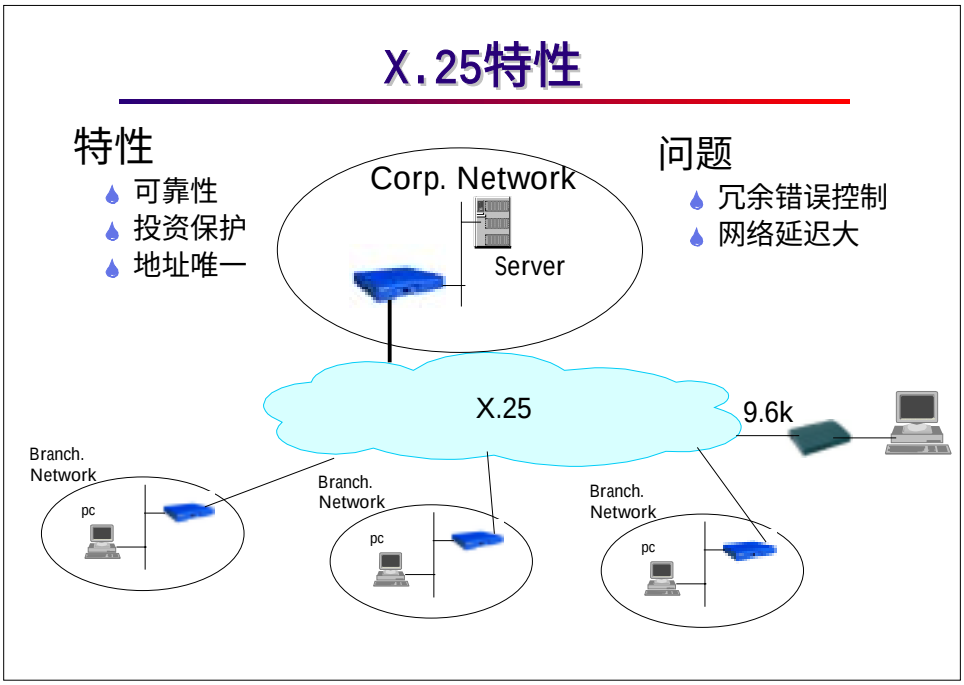
X.25 协议包含了三层：分组层、数据链路层、物理层，是和 OSI 参考模型的下三层一一对应的，它们的功能也是一致的：

☞ 物理层：物理层定义了 DTE 和 DCE 之间的电气接口和建立物理的信息传输通路的过程，可采用 X.21 建议、X.21bis 建议、V 建议等接口标准；

☞ 数据链路层：数据链路层采用平衡型链路访问规程 LAPB，LAPB 定义了 DTE--DCE 链路之间的帧交换的过程及帧格式；

☞ 分组层：分组层则定义了分组的格式和在分组层实体之间交换分组的过程，同时也定义了如何进行流控，差错处理等规程。X.25 的分组层利用链路层提供的服务在 DTE 和 DCE 之间传递分组。它将一条逻辑链路按照动态时分复用的方法划分为多个子逻辑信道。这样就可以允多个用户同时使用数据通道，大大地提高了资源的利用率和效率。

.4.14　X.25 特性



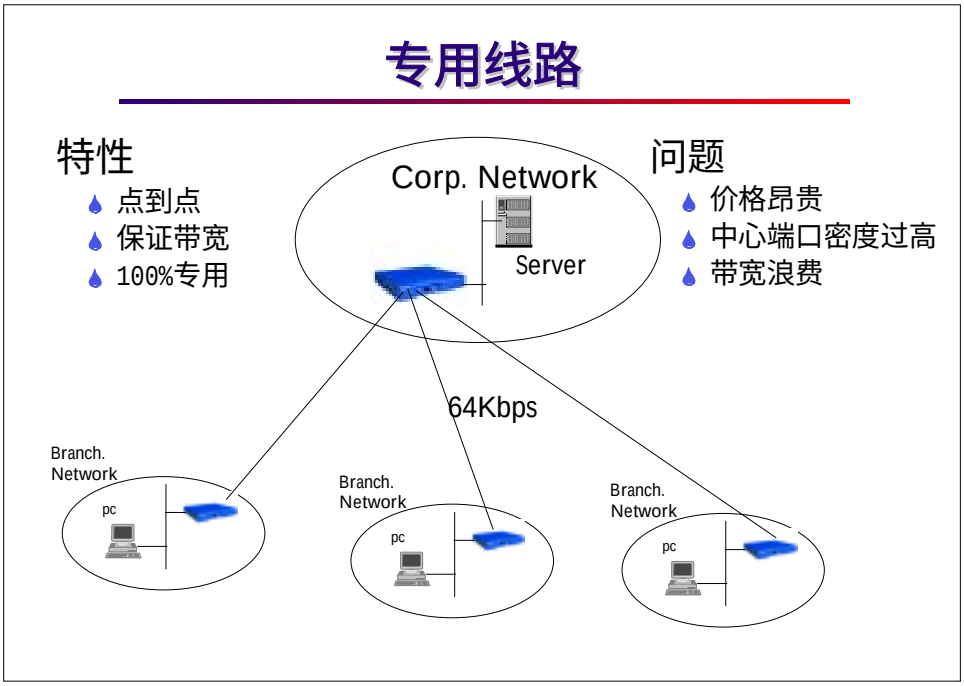
为了适应早期并不可靠的有大量误码的模拟电路，X.25 是一种含有冗余错误控制的可靠传送协议。

X.25 提供了偏远地区可用的庞大的公用分组交换网络，因此可以到达遥远的地域，确保商业用户的网络互联。

X.25 网络采用了标准的地址识别，这种地址是唯一的。

由于高度的可靠传输、过于冗余的错误控制，导致了网络效率较低、延时较大，可能成为网络性能的瓶颈。

.4.15　专用线路

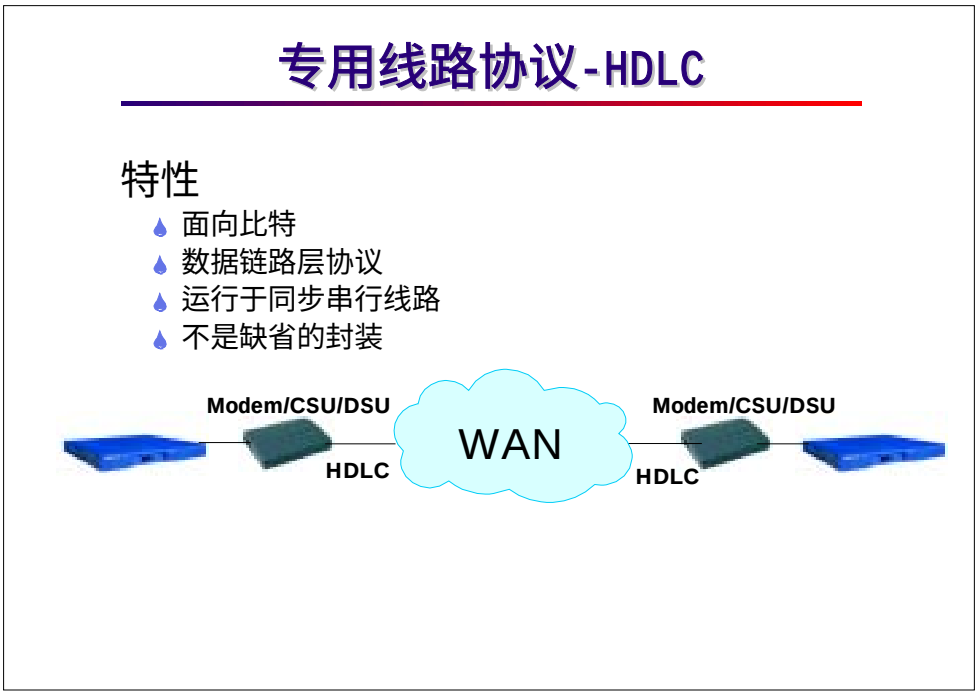


专用线路是透明的物理传输信道，由于它使用简便、覆盖面广，被广泛应用于企业网互联、专线 Internet 接入等。专用线路的明显缺陷是：由于采用点到点通信，对于复杂网络的分支点间的互通，必须通过中心转发。速率以 64K 为主，大于 64K 的线路，费用较贵。

专用线路是点对点连接的，它给予用户访问整个链路带宽的可能性。在某一时刻，带宽的可用率为 100%。然而，在专用线路上，在一段平均时间内，典型的线路利用率只有可用带宽的 30% 至 40%，这是专用线路主要的缺点。但是，由于它是一直联接的，所以不必建立为新的联接而花费等待的时间。

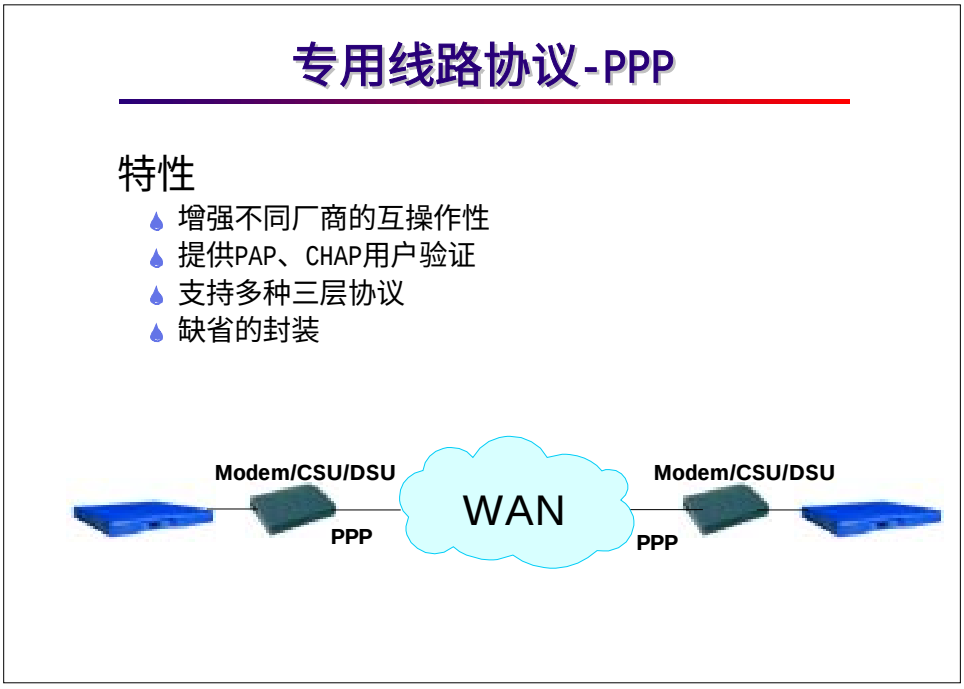
另一方面，专用线路解决方案要求中心端口的高密度，包括通信设备如 DSU/CSU，相对于帧中继等分组交换网络，这将导致网络设备的成本大幅上升。

.4.16　专用线路协议 - HDLC



HDLC 是一种面向比特的、 用于专用线路的数据链路层协议，它提供了一种在同步串行链路的、带有 32 位校验和的封装机制。
HDLC 只运行于同步链路上，它提供的是一种对物理层的面向比特的通明的封装。

.4.17　专用线路协议 - PPP



PPP 协议，其全称为 Point-To-Point Protocol（点到点协议）。它作为一种提供在点到点链路上传输、封装多种不同类型的网络层数据包的数据链路层协议，处于 TCP/IP 协议栈的第二层，主要被设计用来在支持全双工的同异步链路上进行点到点之间的数据传输。

PPP 主要由三类协议组成：链路层控制协议族（LCP）、网络层控制协议族（NCP）和 PPP 扩展协议族。其中，链路控制协议主要用于建立、拆除和监控 PPP 数据链路；网络层控制协议族主要用于协商在该数据链路上所传输的数据包的格式与类型；PPP 扩展协议族主要用于提供对 PPP 功能的进一步支持。

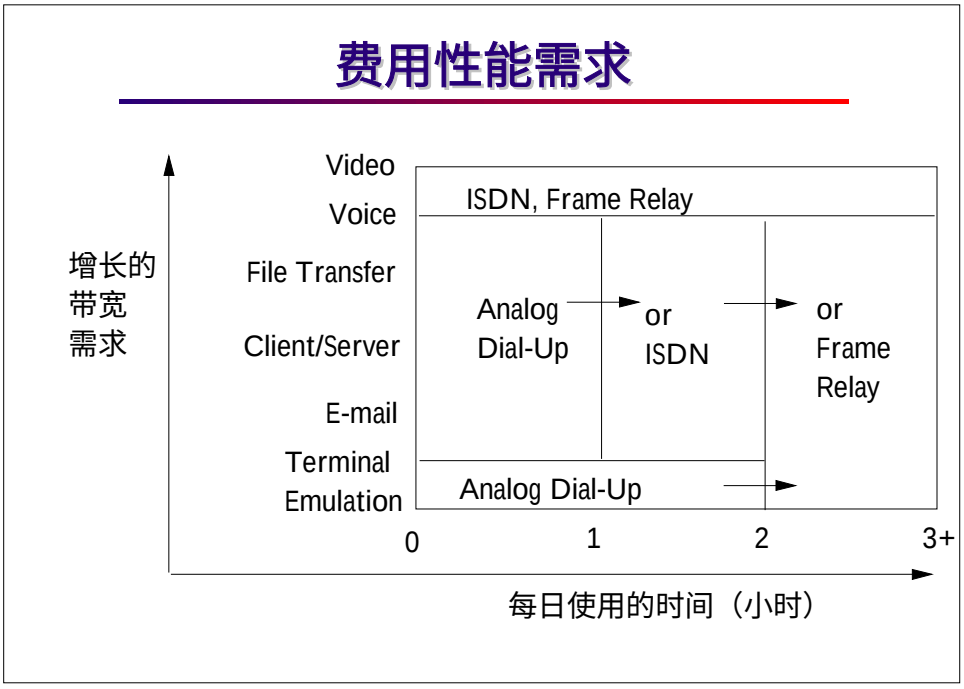
同时，PPP 还提供了用于网络安全方面的验证协议族（PAP 和 CHAP）。

.4.18　X.25 与 Frame-Relay 的比较

由于早期广域网络链路的特点：链路的不可靠性、高误码率，因此 X.25 协议设计成为一种结构严谨，面向连接的协议，它在整个传输过程中，逐段地纠错与进行流量控制，其最大帧长 256 字节，对于 IP 协议效率较低。

在后期由于广域网链路的质量大大提高，光纤的广泛应用，帧中继协议简化了 X.25 的第三层功能，采用物理层和链路层的两级结构，在链路层也只保留了核心子集部分，简化了 X.25 复杂的纠错和重传机制，实现了链路层的高效封装，加大了最大帧传输长度至 1600 比特，适合 IP 报文的传输，提高了网络的对信息的处理效率。

.4.19　费用性能需求



网络的费用性能需求，涉及网络的选型，相对是一个比较模糊的问题，主要是由于它涉及较多的因素，在不同情况下，有不同的选择。
一般来说，首先要考虑的是服务可否提供。在不同的地区，有较大的差异，例如 ISDN 服务并非随处可得 。
其次，从性能与费用方面考虑以下因素：

- ☞ 用户的类别，即什么样的用户需要访问网络资源；
- ☞ 平均每天需要访问的时间；
- ☞ 运行的网络应用以及它所需的带宽；
- ☞ 广域网服务的性能是否满足要求。

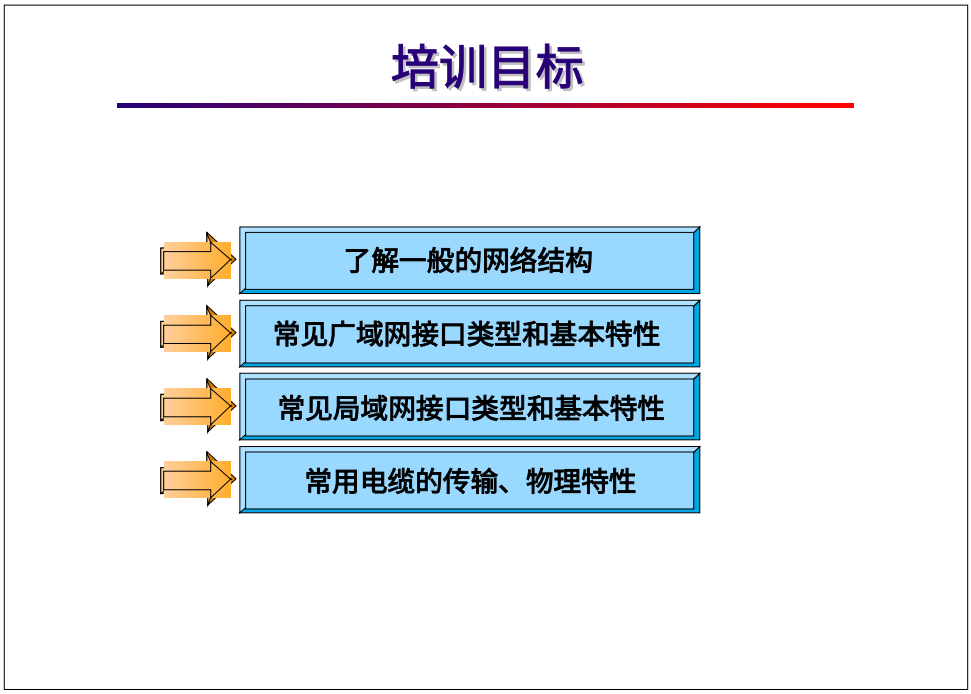
.5 小结

小结

- 学习网络演进与层次化模型的概念
- 了解常用网络设备的工作原理
- 了解TCP/IP 协议族的基本概念
- 了解常用的局域网组网与协议
- 了解常用的广域网组网与协议
- 了解不同网络协议的特性

第二章　　常见网络接口与线缆

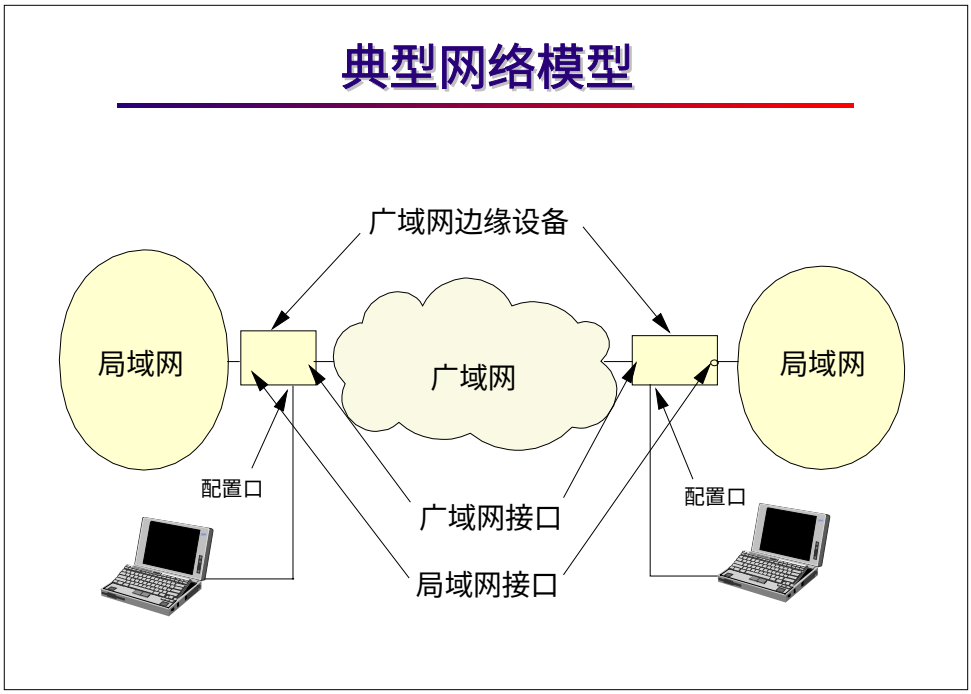
.1　培训目标



本章将围绕 Quidway 系列路由器讨论各种常见网络物理接口与线缆的相关内容，包括常见的接口规范、线缆的类型以及其一般机械特性、电气特性、传输特性以及使用注意事项等等。

.2　典型网络模型

.2.1　网络模型



一个简单明了的网络模型：一个局域网中的某个用户希望利用已有的公共网络资源，与远端的另一个局域网中的某台主机通信时，通过与本局域网相连的广域网边缘设备进入广域网，经由广域网到达与另一台主机所在的局域网相连的边缘设备，从而与目的主机之间建立通信。这里我们关注的重点就是这种广域网边缘设备。
常见的广域网边缘设备包括各类路由器、ATM 接入交换机等等。

.2.2　广域网边缘设备

广域网边缘设备承担着连接局域网与广域网的重要任务，它将同时属于局域网和广域网，可知，就边缘设备而言，局域网接口，广域网接口这二者缺一不可。另外，出于此种设备应用的灵活性，其本地配置接口也是不可缺少的。下面的内容中我们将逐一进行讨论。

.3　局域网

.3.1　常见局域网类型

局域网，Local Area Network ，简称 LAN，和广域网区别有如下三个方面的特征：

（ 1 ） 范围
（ 2 ） 传输技术
（ 3 ） 拓扑结构

就范围来讲，局域网一般覆盖的范围较小，通常是处于同一建筑，同一所大学或方圆几公里以内的专用网络。

就传输技术而言，LAN 通常使用这样一种传输技术，所有的机器连接到一条电缆上，通过广播的方式进行通信。广播式 LAN 有多种拓扑结构，一般多数网络使用以下两种：

总线型网络：突出的例子就是以太网和令牌总线网。这种网络中，任意时刻都只有一台机器是主站并可进行发送，其他机器则不能发送。当两台或更多机器都想发送信息时，就需要一种仲裁机制来解决冲突，这种机制可以是集中式的，也可以是分布式的。不同的网络使用的机制和实现方法不尽相同。

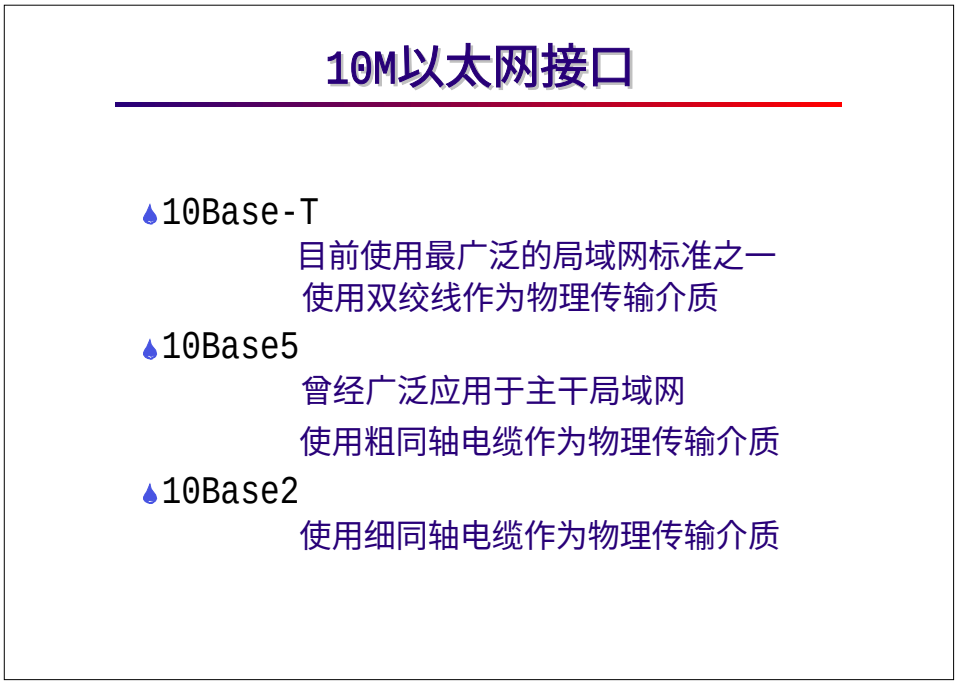
环网：突出的例子就是 IBM 令牌环网。在环中，每个比特独自在网内传播而不必等待他所在的分组里的其他比特。也需要某种机制来仲裁对网络的同时访问。

另外， 目前正迅速发展的交换式 LAN 采用了星型拓扑结构。

.3.2　以太网的物理接口类型

以太网是一种基于总线型拓扑结构的网络，使用分布式仲裁机制来解决冲突。速度有 10Mbps、100Mbps 和 1000Mbps 三种。
IEEE 802.3 主要确定了以太网各项标准及规范。
以太网上的计算机任何时候都可以发送信息，但发送之前都需先检测网络是否空闲，即“侦听”，如果某时刻有两个或者更多的分组发生冲突，则检测到冲突欲发送数据的计算机就都需等待一段时间，即“回退”，然后再次试图发送。这就是以太网技术必须提到的 CSMA/CD（载波侦听多路访问/冲突检测）机制。
显然，随着同一网络上的计算机数目的增加，以太网的效率会降低。同时，随着网络带宽的增大和电缆长度值的增大，（在帧长度不变的条件下）以太网的效率也会降低。

.3.3　10M 以太网



10Mbps 以太网即标准以太网，由 IEEE 802.3 定义，同一公共通信信道上的所有用户共享这个带宽，这个公共信道称为总线。在交换式 LAN 中，每个交换式端口都是一个以太网总线，采用星型拓扑结构。这种连接方式下将有可能提供全双工的连接，此时，将提供 20Mbps 的 总带宽。

根据 IEEE 802.3 的规定，10M 以太网目前广泛使用的线缆有：10Base -T 双绞线、10Base5 粗同轴电缆以及 10Base2 细同轴电缆。

10Base5 粗同轴电缆采用插入式分接头，表示的意思是：工作速率为 10Mb/s，采用基带信号，最大支持段长为 500m，最多段数为 100。10Base5 粗同轴电缆线径较粗，不易弯曲，安装非常不便。

10Base2 细同轴电缆接头采用工业标准的 BNC 连接器组成 T 型插座，使用灵活可靠性高，价格也较便宜，但使用范围只有 200 米，每一段内仅能使用 30 台计算机，段数最高为 30。

10Base-T 是目前使用最为广泛的一种以太网电缆标准。它具有一个显著优势就是易于扩展，维护简单，价格低廉，一个集线器加上几根 10Base-T 电缆，就能构成一个实用的小型局域网（当然还得有计算机），10Base-T 的缺点是：电缆的最大有效传输距离是距集线器 100m，即使是高质量的 5 类双绞线也只能达到 150m 。

10Base-T 的物理介质

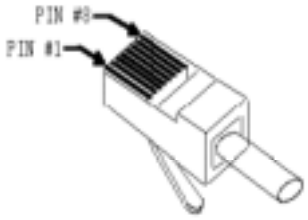
双绞线（Twisted pair），收发各由两条拧在一起并相互绝缘的铜线组成。两条线拧在一起可以减少线间的电磁干扰。

3 类到 6 类双绞线在塑料外壳内均有这样的四对线缆，区别主要在于类数越高的双绞线，单位长度内的绞环数越多，拧得越紧，这使得 5 类或者 6 类双绞线的交感更少并且在更长的距离上信号质量更好，更适用于高速计算机通信。

双绞线连接器

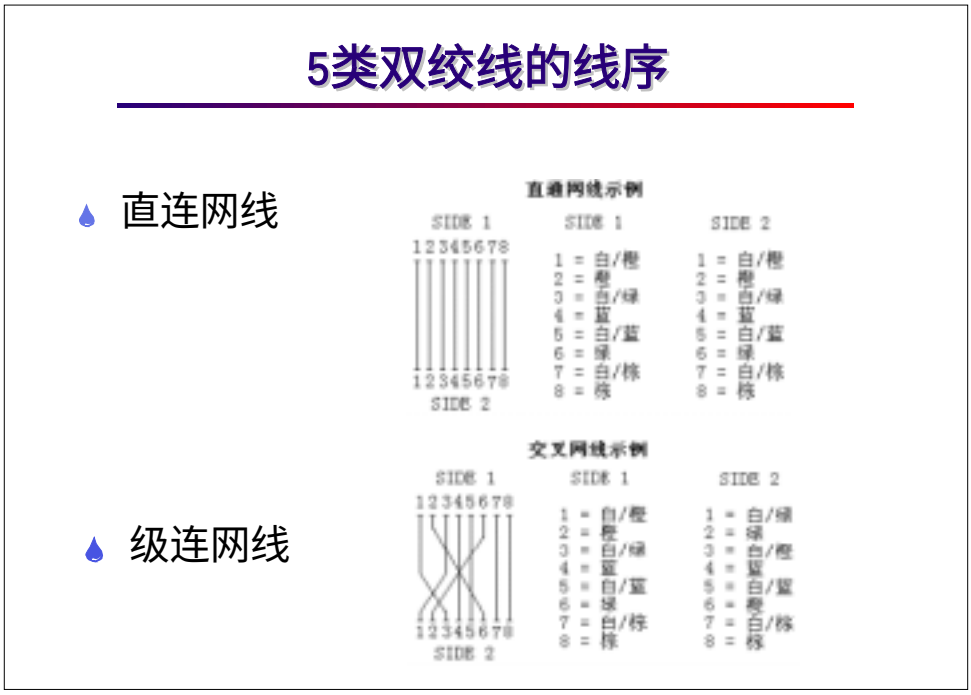
双绞线连接器

- 双绞线的连接器均使用RJ-45水晶头



双绞线连接器一般都使用 RJ-45 连接器（如图）。

5 类双绞线的线序

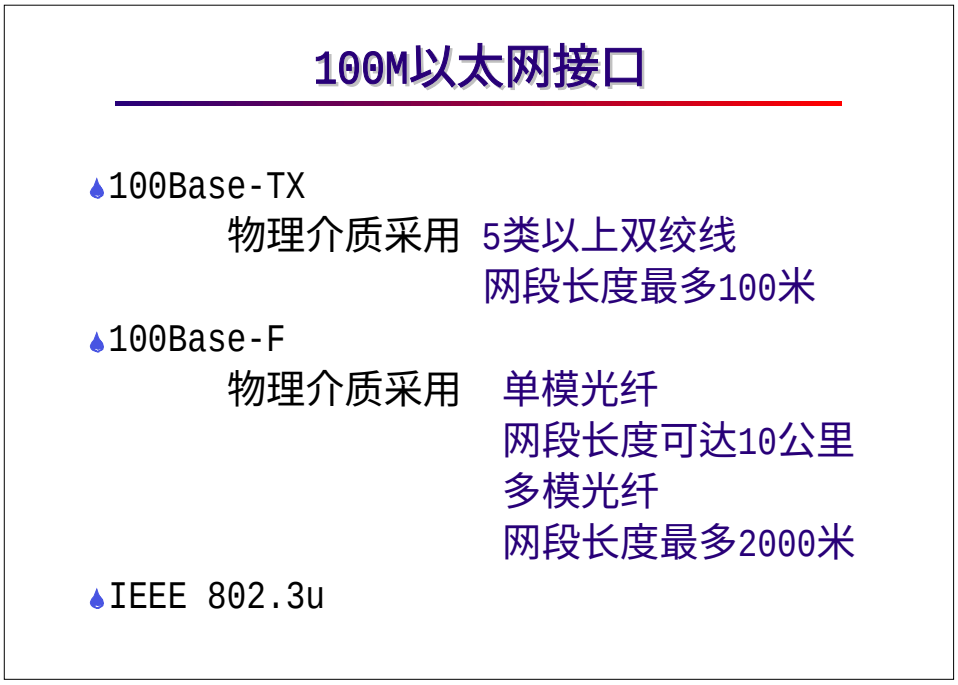


5 类双绞线由 8 芯细线组成，利用细线外绝缘层上的颜色进行分组标识。通常利用单色和单色加上白色作为成对标识，也有利用色点成对进行标识的。

直连网线和级连网线的线序如图所示。

图中各线画法仅为说明两端的线序关系，实际双绞电缆线芯都是成对拧绞在一起的。

.3.4　快速以太网



快速以太网由 IEEE 802.3u 标准定义，基本与标准以太网相同，但速度比标准以太网快十倍。快速以太网的速度是通过提高时钟频率和使用不同的编码方式获得的。其传输方案最常用的便是 100Base-T，100Base-T 又包括 100Base-TX 和 100Base-T4，100Base-T4 是一种 3 类双绞线方案，不支持全双工，目前最广泛使用的都是 100Base-TX，此方案需使用 5 类以上双绞线，时钟信号处理速率高达 125MHz。本书以后内容中提到的快速以太网双绞线方案在不进行特殊说明的情况下均指 100Base-TX 方案。

100Base-FX 使用一对多模或者单模光纤，使用多模光纤的时候，计算机到集线器之间的距离最大可到两公里，使用单模光纤时最大可达十公里。

快速以太网还提供全双工通信，总带宽达到 200Mbps 。全双工快速以太网仅在使用光纤或某些双绞线介质的点对点链路有效，因为每个带宽为 100Mbps 的信道都需要独立的线来支持。

快速以太网有自动协商的功能，能够自动适应电缆两端最高可用的通信速率，能方便的与 10M 以太网连接通信。

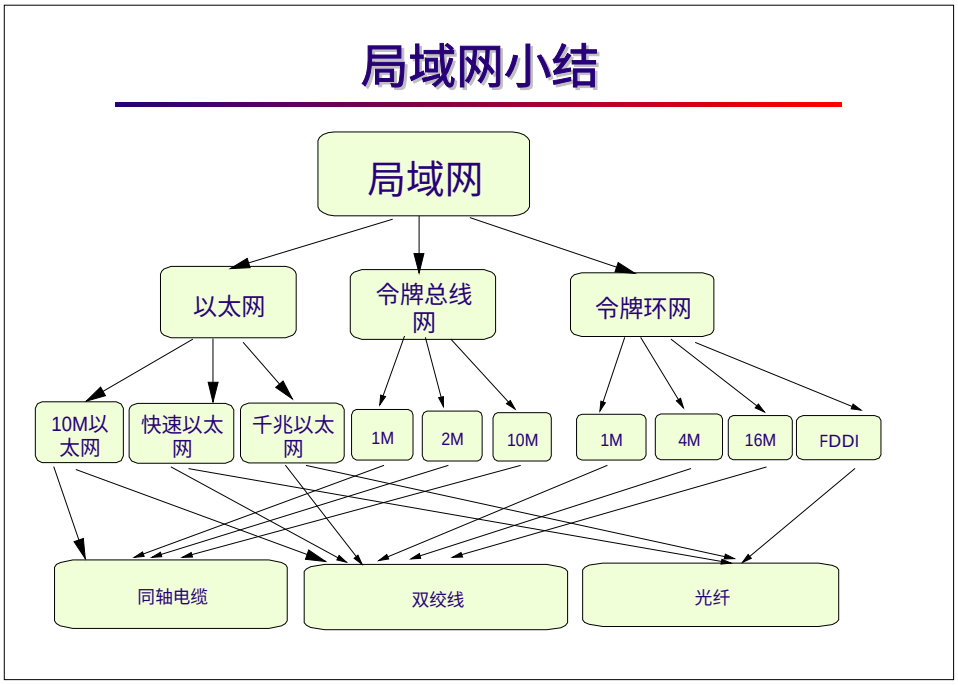
.3.5　千兆以太网

千兆以太网保留了传统以太网的大部分简单特征，以 1000Mbps /2000Mbps 的带宽提供半双工/全双工通信。千兆以太网对电缆的长度的要求更为严厉，多模光纤的长度至多为 500 米，5 类双绞线为 100 米。IEEE 802.3z 标准定义了千兆以太网，IEEE 802.3ab 标准专门定义了双绞线上的千兆以太网规范，两者都是 802.3 标准的补充。

由于高速数据速率定时的限制，在同一冲突域中，千兆以太网不允许中继器的互连。

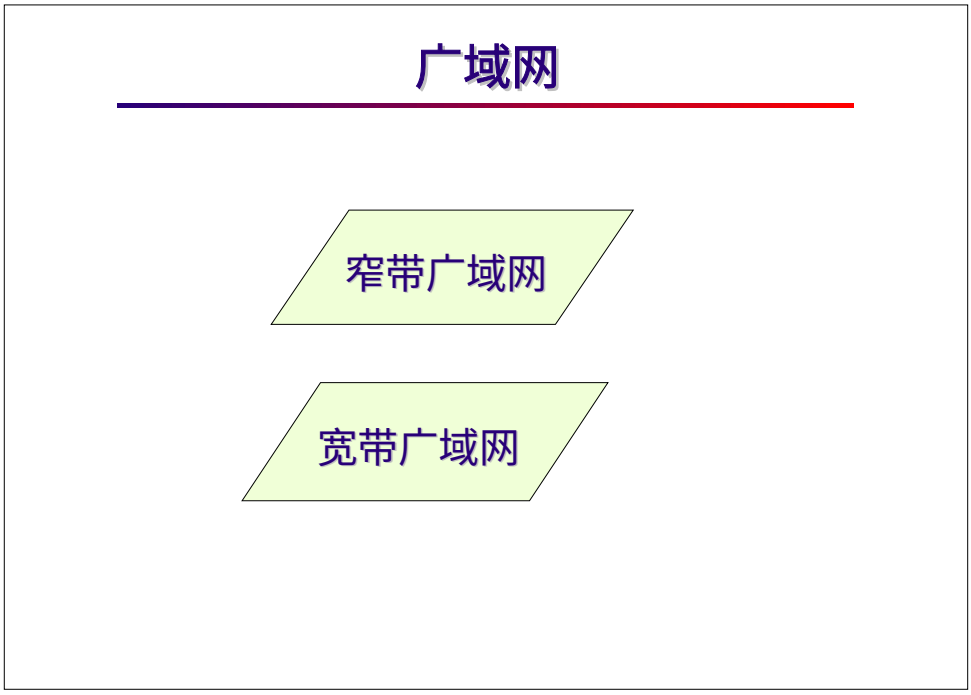
千兆以太网有自动协商的功能，但仅限于协商半双工或全双工流量控制，确定是否支持控制帧，不能与低速以太网之间协商速率。

.3.6　局域网小结


局域网小结
局域网
以太网
令牌总线网
令牌环网
10M以太网
快速以太网
千兆以太网
1M
2M
10M
1M
4M
16M
FDDI
同轴电缆
双绞线
光纤

.4　广域网

.4.1　广域网的类型



广域网（ Wide Area Network ）是一种跨越大的地域的网络。目前有多种公共广域网络，按其提供业务的带宽的不同，可简单的分为窄带广域网和宽带广域网两大类。

窄带广域网的类型

现有的窄带公共网络包括 PSTN 公共交换电话网、ISDN 综合数字业务网、DDN、X.25 网、Frame Relay 帧中继网等。

PSTN 可能是我们接触最多的公共窄带网络，目前主要提供电话和传真业务，通过调制解调器可以完成一些有限的数据传输业务。

ISDN 综合业务数字网将在本章后面小节专门介绍。

DDN 即数字数据网，是一种广泛使用的基于点对点连接的窄带公共数据网络。

X.25 网是一种国际通用的标准广域网，在很多地区，X.25 是唯一可用的 WAN 技术，在欧洲非常流行。内置的差错纠正、流量控制和丢包重传机制，使之具有高度的可靠性，适于长途噪声线路。最大速率仅为有限的 64Kbps ，使之可提供的业务非常有限。沿途每个节点都要重组包，使得数据的吞吐率很低，包时延较大。X.25 显然不适于传输质量好的信道。

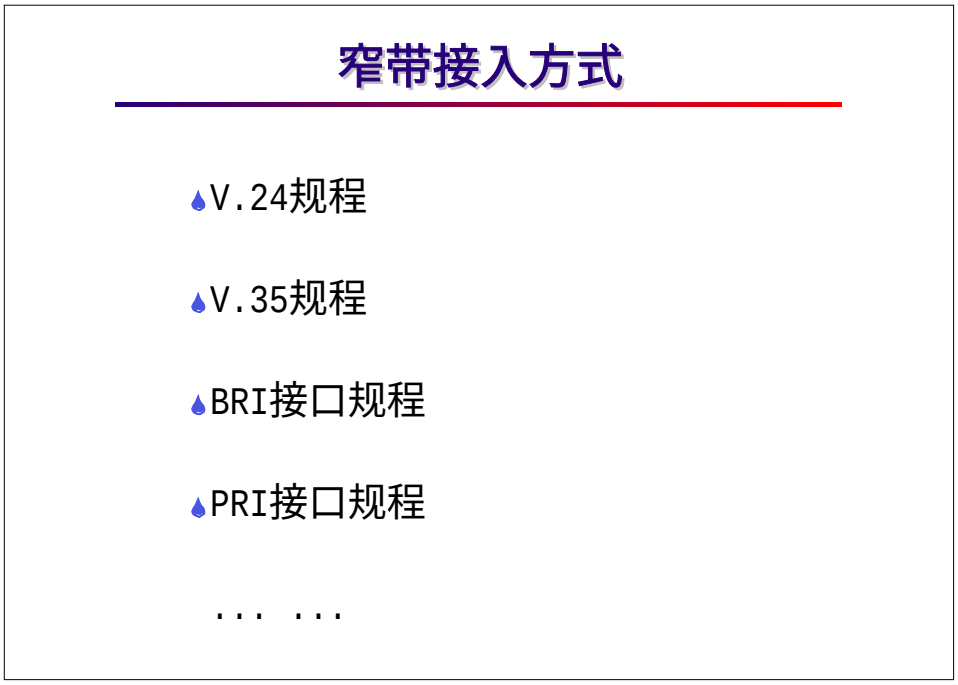
Frame Relay 帧中继是一种应用很广的服务，采用 E-1 电路，速率可从 64K 到 2 兆，速率较快，它减少了差错检测，充分利用了如今广域网连接中比较简洁的信令。中间节点的延迟比 X.25 网小得多。帧中继的帧长度可变，可以方便的适应 LAN 中的任何包或帧，提供了对用户的透明性。帧中继容易受到网络拥挤的影响，对于时间敏感的实时通信没有特殊的保障措施，当线路收到噪声干扰时，将引起包的重传。

宽带广域网的类型

ATM 即异步传输模式，为在交换式 WAN 或 LAN 骨干网以及高速传输数据提供了通用的通信机制，它同时支持多种数据类型（话音、视频、文本等）。与传统 WAN 不同，ATM 是一种面向连接的技术，在开始通信之前，将首先建立端到端的连接。ATM 一个最突出的优势之一，就是支持 QoS (Quality of Service) 。

SDH 是目前应用最广的光传输网络，带宽宽，抗干扰性强，可扩展性较强。

.4.2　窄带接入方式

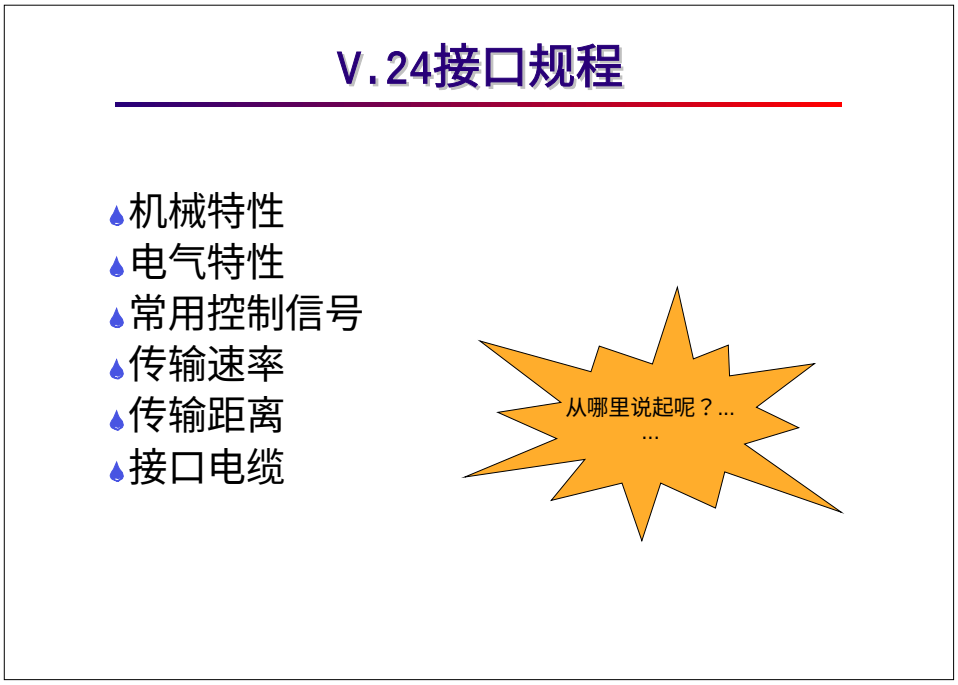


在以下的窄带 WAN 接入方式内容中，我们将介绍以下几种接口规程：

V.24 规程
V.35 规程
BRI 接口规程
PRI 接口规程

以上是目前使用最多的窄带接口规程。

.4.3　V.24 接口规程

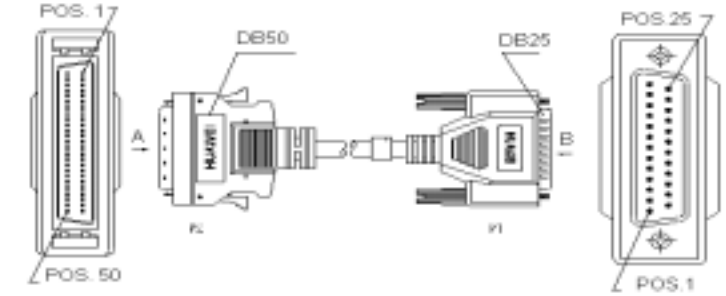


V.24 接口规程的介绍中，将以 Quidway 系列路由器的常用接口为例从机械特性、电气特性、常用控制信号、传输速率、传输距离和接口电缆六个方面来讲解。这几个方面也是其它规程所关心的重要内容之一。

V.24 接口规程的机械特性

V.24规程的机械特性

- DB50（路由器端）--DB25（外接网络端）



V.24DTE电缆　　针型插头

机械规程包括对接口的物理管脚数目、排列定义以及标准尺寸等方面的定义。

Quidway 系列路由器使用 V.24 接口电缆外观如图所示，路由器端为 DB50 专用插头，外接端是标准 DB25 接头，符合 EIA-RS-232 接口标准，电缆可以工作在同步和异步两种方式下，所以既可以与普通的模拟 Modem、ISDN 终端适配器等以拨号方式进行异步连接，也可以连接基带 Modem 进行同步连接。异步工作方式下，封装链路层协议 PPP ，支持网络层协议 IP 和 IPX ，最高传输速率是 115200bps，同步方式下，可以封装 X.25、帧中继、PPP、HDLC、SLIP 和 LAPB 等链路层协议，支持 IP 和 IPX ，而最高传输速率仅为 64000bps 。

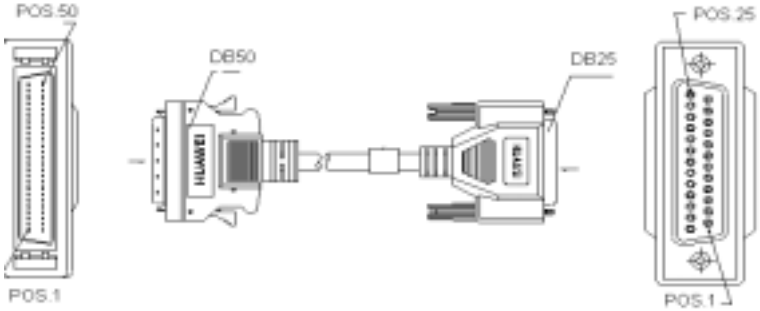
V.24 电缆接口分 DCE 和 DTE 两侧，分别对应数据电路端接设备（网络侧）和数据终端设备（用户侧）。对应的 DCE 侧为插座（25 孔），DTE 侧为插头（25 针）。通信的双方相对而言，路由器属于 DTE 侧设备，各种 Modem 、ISDN 终端适配器等则属于 DCE 设备。

本图所示为 Quidway 系列路由器 V.24 DTE 广域网电缆。

V.24 接口规程的机械特性（续）

V.24规程的机械特性

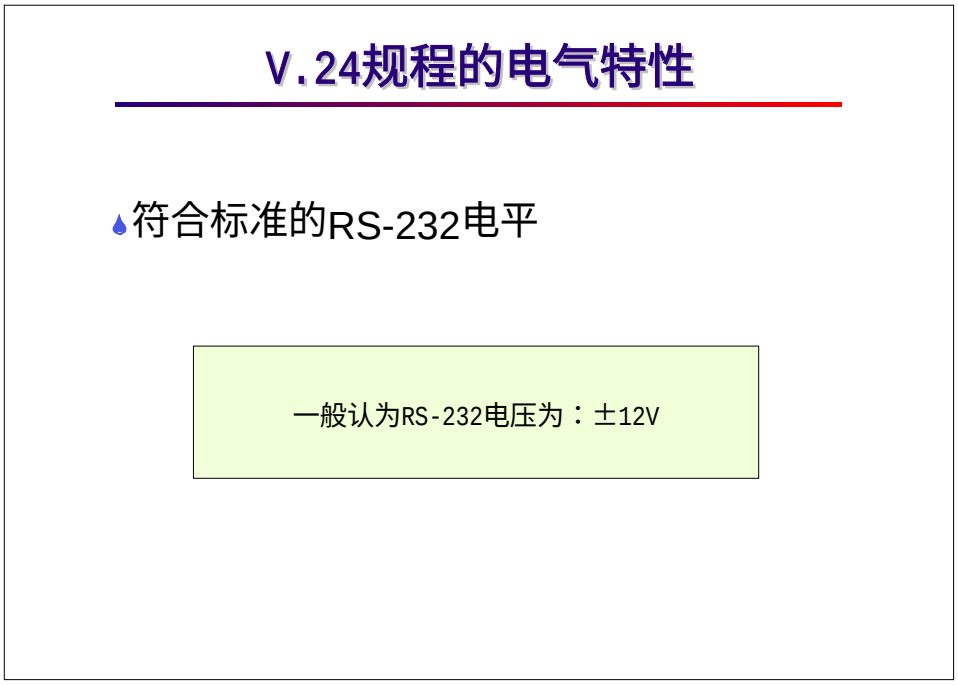
- DB50（路由器端）--DB25（外接网络端）



V.24 DCE电缆　　孔型插头

本图所示为 Quidway 系列路由器 V.24 DCE 广域网电缆，外接网络端为 25 孔插头。

V.24 接口规程的电气特性



V.24 规程所规定的接口的电气特性需符合 EIA- RS-232 电气标准，其电平定义如下：

在 TxD 和 RxD 数据上：

逻辑 1 (MARK) = -3 ~ -15 伏；

逻辑 0 (SPACE) = +3 ~ +15 伏；

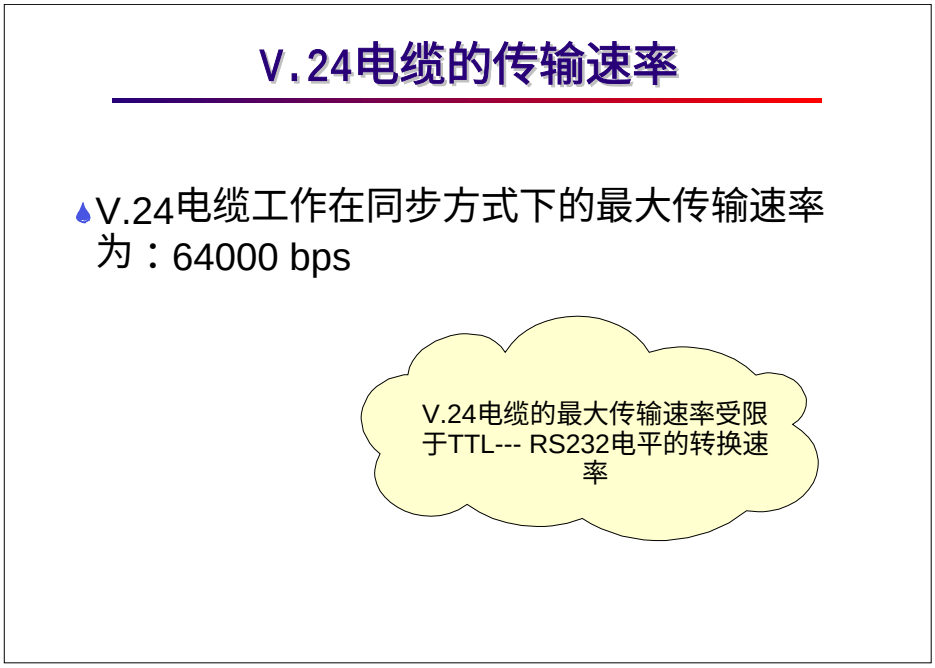
在 RTS、CTS、DSR、STR 和 DCD 等控制线上：

信号有效（接通、ON 状态、正电压）= +3 ~ +15 伏；

信号无效（断开、OFF 状态、负电压）= -3 ~ -15 伏；

一个明显的区别，RS-232 电平标准使用了较 TTL 电平高得多的电压值，在收发数据引脚上使用了负逻辑。

V.24 电缆的传输速率



V.24 电缆在同步工作方式下的最大传输速率为：64000bps；异步工作方式下，最大传输速率为 115200bps。

从前面的介绍可以看到，RS-232 电平与普通 TTL 电平存在很大的区别，快速的电平转换成为一个问题。目前，硬件的电平转换速率主要限制了其最大传输速率。

V.24 电缆的传输距离

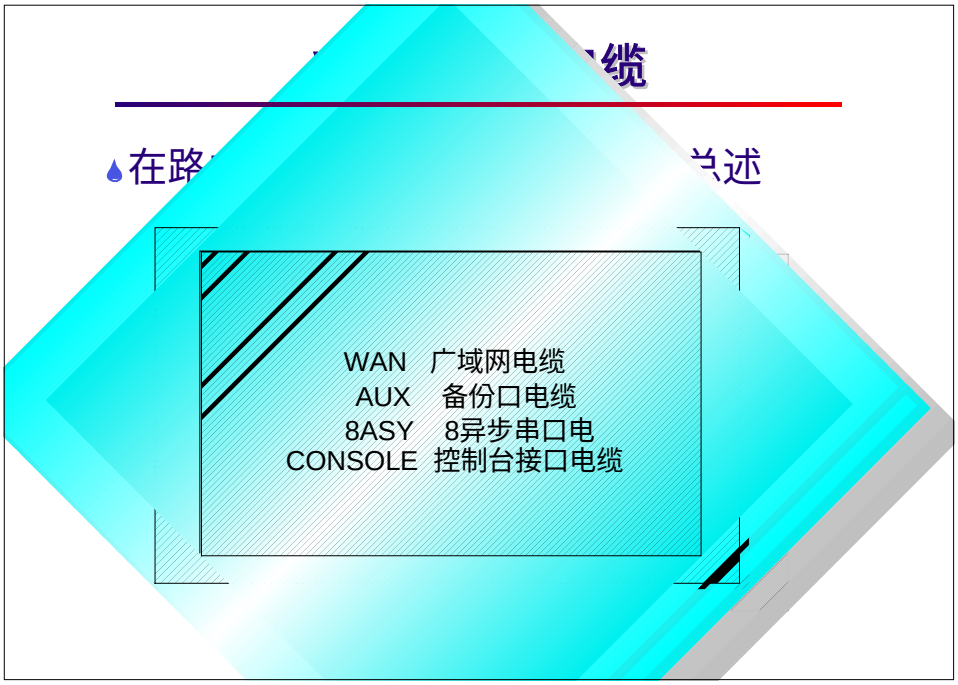
V.24电缆的传输距离

- EIA/TIA-232 电缆的速率和传输距离

波特率（bps）	最大传输距离（米）
2400	60
4800	60
9600	30
19200	30
38400	20
64000	20
115200	10

以上图示为 IEEE（电气与电子工程师协会）提供的 V.24 电缆异步方式下以各种波特率传输数据的标准传输距离，实际情况中，由于使用环境的差别，其传输距离的极限将不尽相同，实际测试表明，本表所给出的数据略偏保守。

路由器上使用的 V.24 规程电缆总述



符合 V.24 规程的接口及电缆在通信、计算机系统中使用的非常广泛，从计算机串口到路由器的广域网口，都有它的身影。在路由器上，主要出现在以下几种接口电缆之中：

WAN 广域网接口

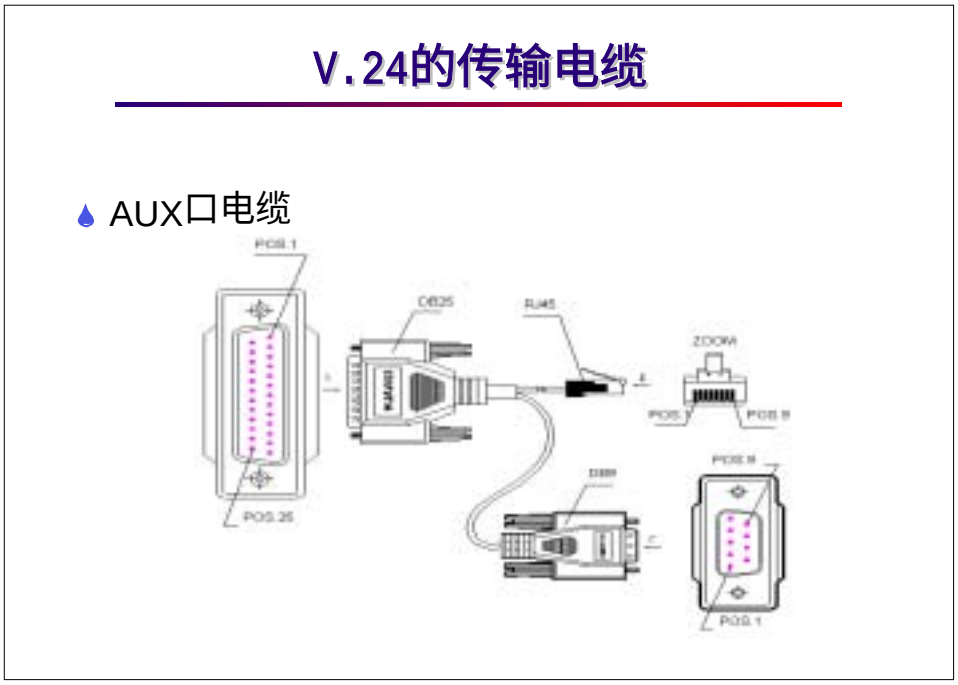
AUX 备份接口

8AS 八异步串行接口

Console 控制台接口

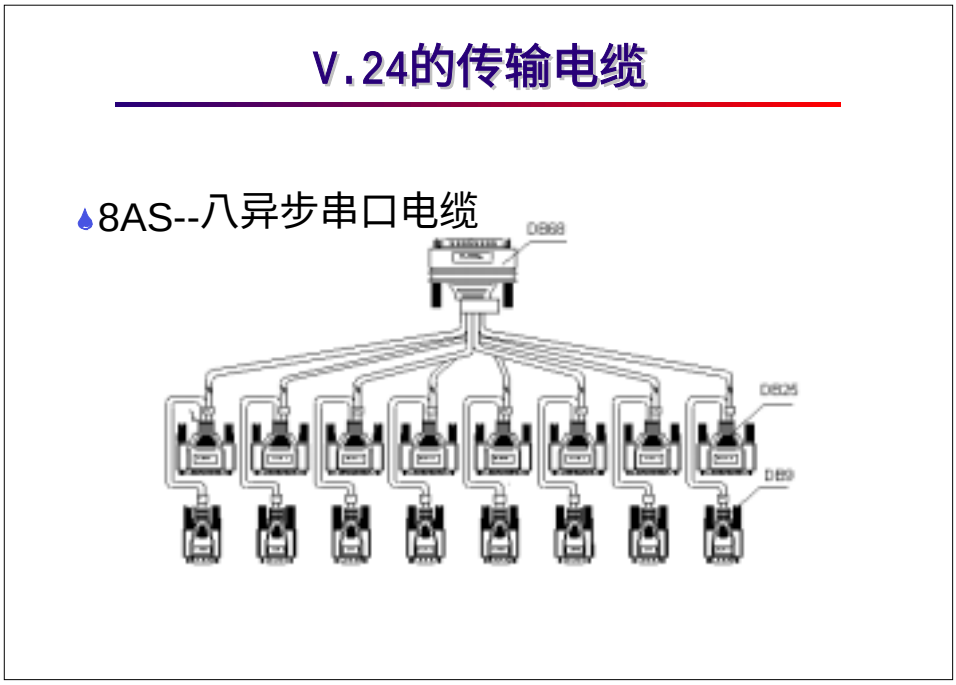
应用于广域网口的 V.24 电缆在前面的内容中已经介绍过了，下面将介绍其他三种接口电缆。

AUX 口电缆



备份接口（AUX）电缆，路由器作为 DTE 设备，采用标准 RS-232 电平，路由器端采用 RJ-45 插座，与 Modem 的 DB-25 或 DB-9 插座相连。连接电缆与控制台接口电缆相同；是一根 8 芯的屏蔽双绞线，一端压接的是 RJ-45 水晶插头；另一端分别是一个 DB-25（针）插头和一个 DB-9（针）插头，与 DCE 设备的 DB-25（孔）或 DB-9（孔）插座对应。AUX 口是一个标准异步口，通常用于连接 Modem 或 ISDN 终端适配器作为备份接口使用，也可以接一个 Modem，作为一个远程配置接口。

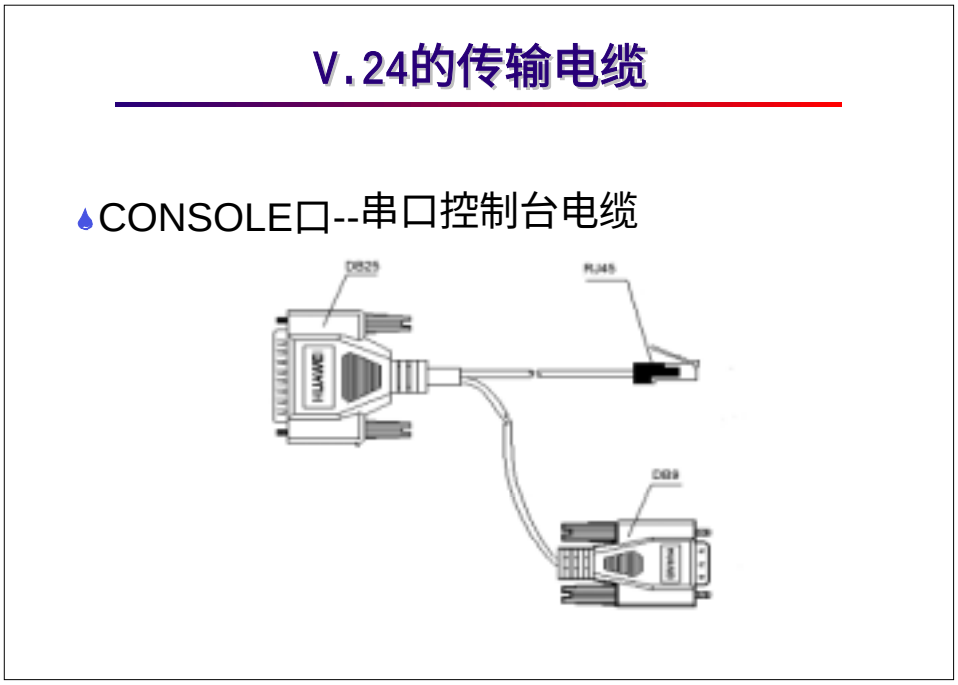
8AS —— 八异步串行口电缆



八异步串口是 Quidway R2509/2511 以及华为公司其他中/高端路由器可选的接口，配合该接口的电缆俗称“八爪鱼”，路由器端为一 68 针插头，外接端被分为八个标准 RS-232 异步串行口，如果与八个模拟 Modem 配合，连接八根电话线，就可以组建一个小型的接入服务网络，可以允许八个用户使用 Modem 通过 PSTN 拨号同时登录到本地路由器所在的局域网，或者经由此路由器访问外部的 Internet。

另外，注意到每个串行口均为标准的 RS-232 接口，联系到很多其它网络设备的配置口一般也为 RS-232 串行口，不难想到，用一台 Quidway R2509/2511 作为其它网络设备的远程带外配置中心也是个不错的网管方案。

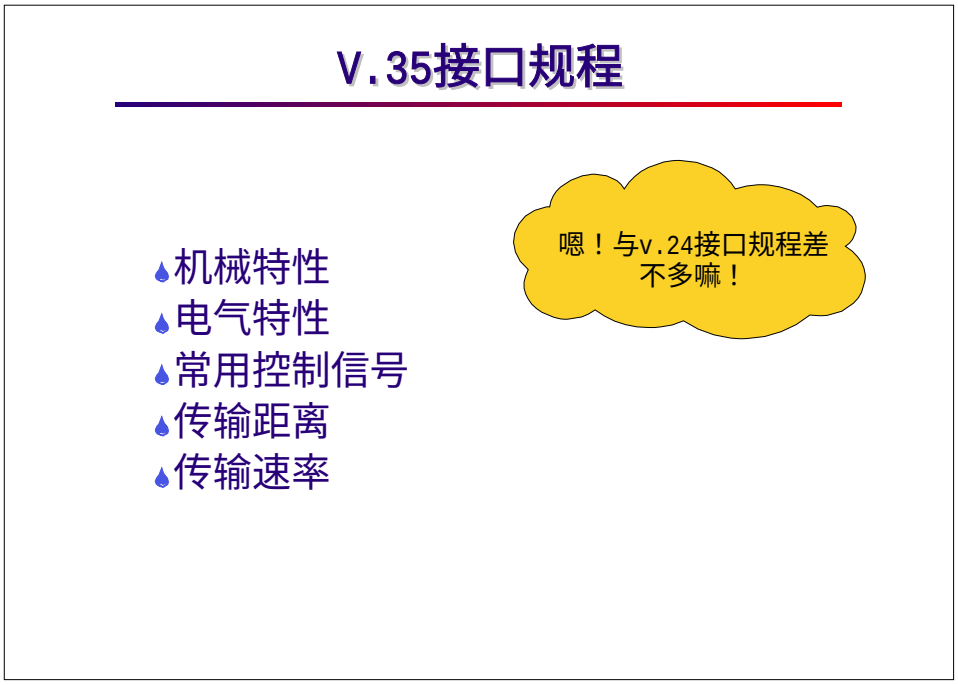
Console 口 —— 串口控制台电缆



控制台接口，即 Console 口，路由器作为 DCE 设备，采用标准 RS-232 电平，路由器端采用 RJ-45 插座，与计算机 25 芯或 9 芯串行口相连。连接电缆采用一根 8 芯的屏蔽双绞线，一端是压接的是 RJ-45 水晶插头；另一端与计算机串口相连，分别有一个 DB-9（孔）和 DB-25（孔）RS-232 插头。

Console 口是对路由器进行配置使用的主要接口。

.4.4　V.35 接口规程

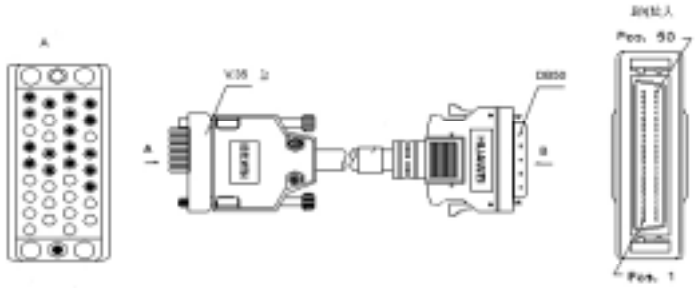


V.35 接口规程的介绍中，同样的将以 Quidway 系列路由器的常用接口为例，从其机械特性、电气特性、常用控制信号、传输速率、传输距离和接口电缆六个方面来讲解。

V.35 规程的机械特性

V.35规程的机械特性

- DB34（外接网络端）--DB50（路由器端）



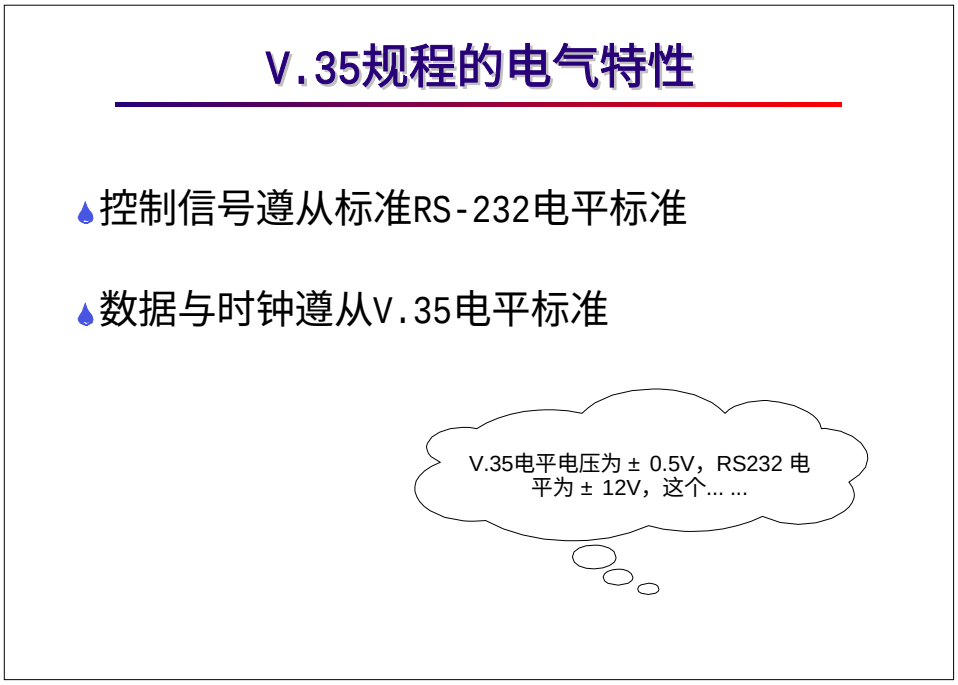
- DTE端为34针型插头
- DCE端为34孔型插头

V.35 电缆的接口特性严格遵照 EIA/TIA-V.35 标准。路由器端为 DB50 接头，外接网络端为 34 针接头，也分 DCE 和 DTE 两种，对应的 DCE 侧为插座（34 孔），DTE 侧为插头（34 针）。

V.35 电缆一般只用于同步方式传输数据，可以在接口封装 X.25、帧中继、PPP、SLIP、LAPB 等链路层协议，支持网络层协议 IP 和 IPX。V.35 电缆通常用于路由器与基带 Modem 的连接之中，此方式下，与使用 V.24 电缆相同，路由器总是处在 DTE 侧。

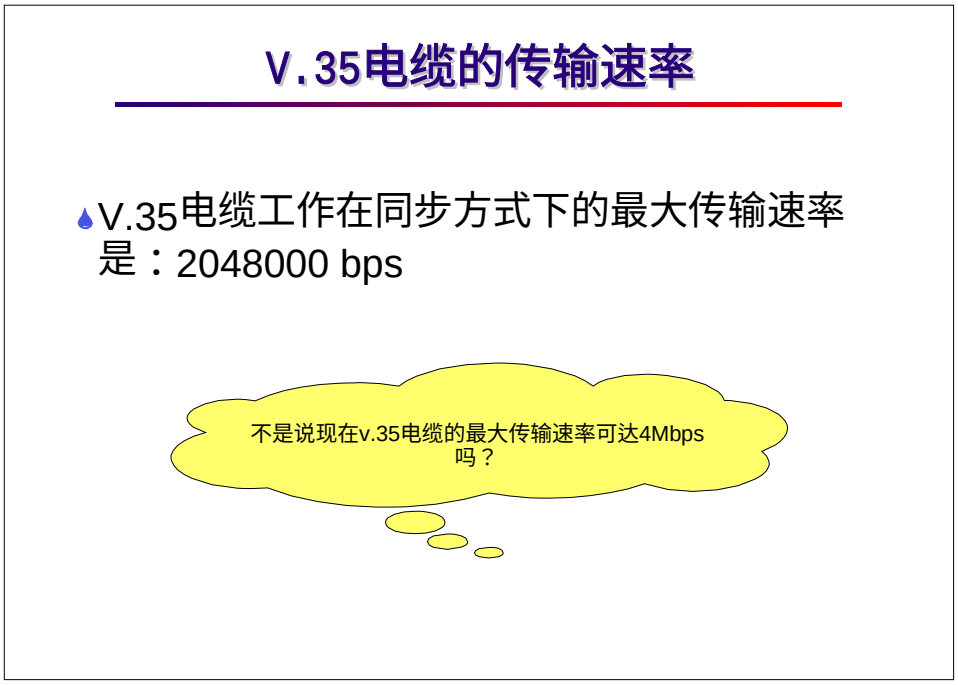
本图所示为 DTE 电缆示意，DCE 电缆示意图略。

V.35 规程的电气特性



V.35 规程定义了 V.35 电缆接口的电气特性。就电平标准而言，V.35 接口同时符合 EIA-RS-232 电平和 V.35 电平标准。在 V.35 电缆接口上，不同功能定义的引脚的电气特性是不一样的，其中，控制信号电平符合 RS-232 电平，数据与时钟电平则符合 V.35 电平。
一般认为，V.35 电平的标准电压使用±0.5 伏，RS-232 电平的电压使用±12V，对重要的但相对速率要求不是很高的控制信号使用幅值更高更不易出错的电平，对要求速率第一的数据等采用幅值低得多的电平，这是 V.35 接口规程考虑网络的速率和稳健性时的一个巧妙而折衷的办法。

V.35 电缆的传输速率



V.35 电缆传输（同步方式下）的公认最高速率是 2048000bps（2Mbps）。与 V.24 规程不同，V.35 电缆的最高传输速率主要受限于广泛的使用习惯，虽然从理论上 V.35 电缆速率可以超过 2M 到 4M 或者更高，但就目前来说，没有网络营运商在 V.35 接口上提供这种带宽的服务。

V.35 电缆的传输距离

V.35电缆的最大传输距离

- EIA/TIA-V.35 电缆的速率和传输距离

波特率（bps）	最大传输距离（米）
2400	1250
4800	625
9600	312
19200	156
38400	78
56000	60
64000	50
2048000	30

以上图示为 IEEE 提供的 V.35 电缆在同步工作方式下以各种波特率传输数据的标准传输距离，实际情况中，由于使用环境的差别，其传输距离的极限将不尽相同，实际测试表明，本表所给出的数据略偏保守。

V.35/V.24 的主要控制信号

以下是 V.24 及 V.35 规程中几个常见然而重要的控制信号的说明：

DTR（Data terminal ready，数据终端准备好）

DSR（Data Set Ready 数据准备好）

主要用于传输设备之间的协商信息。

DCD（Data Carrier Detect 数据载体检测）

用于设备检测当前的链路状态。

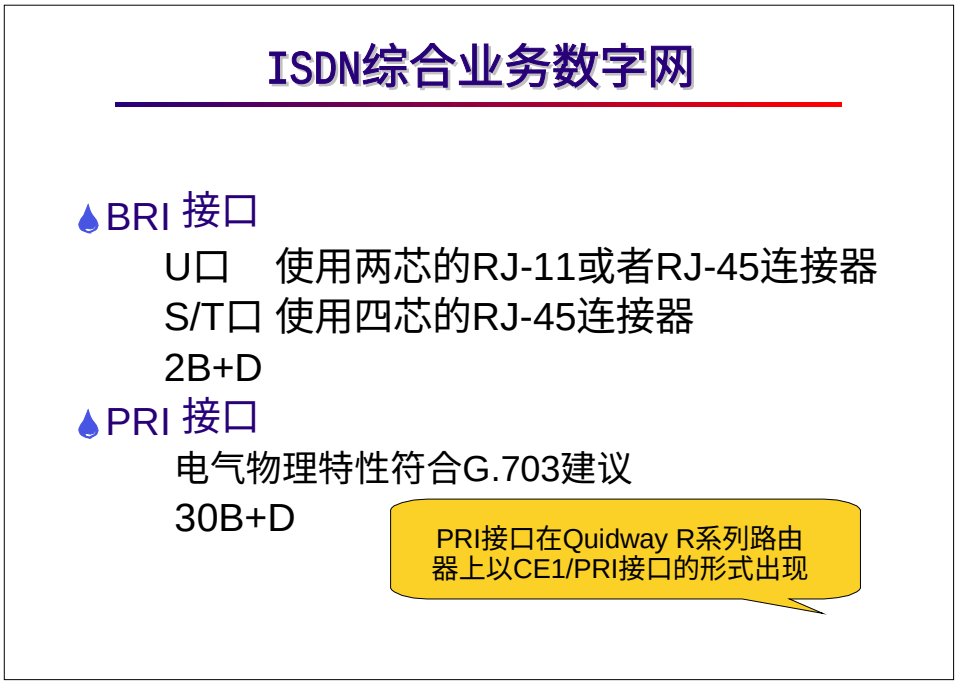
RTS（request to send 请求发送）

CTS（clear to send 清除发送）

非常重要的数据流控信号，在很多接口规程中都可以看到。

无论是在 V.24 还是 V.35 接口规程中，这些控制信号对应的引脚都遵从 RS-232 电平标准。

.4.5　ISDN 综合业务数字网



综合业务数字网（Integrated Services Digital Network，简称 ISDN）是自 70 年代发展起来的一种新兴技术。提供从终端用户到终端用户的全数字服务，实现了语音、数据、图形、视频等综合业务的一个全数字化传递方式。

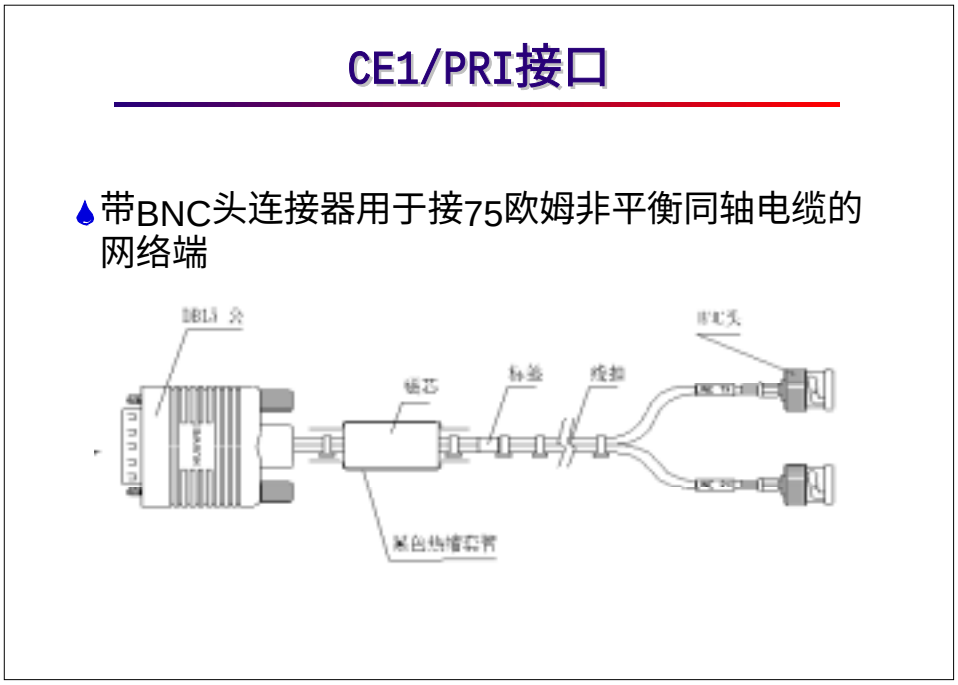
Quidway R1600 系列路由器各提供了一个 BRI 接口，相当于内置了一个 ISDN 终端适配器，可以方便的通过 ISDN 专线与远端进行通信，也可以作为一个桥梁将一个局域网接入到 Internet。Quidway R1600 系列路由器中包括 Quidway R1603 S/T 接口路由器和 Quidway R1604 U 接口路由器，分别适应不同电信网络的规范。在中国采用 S/T 接口规范，所以中国用户应选用 Quidway R1603 路由器。连接时，S/T 口的 R1603 路由器需通过一个 NT1 再与 ISDN 线相连，U 口的 R1604 则可以直接连接 ISDN 线路使用。BRI 接口（S/T）也使用 RJ-45 水晶头连接器，但实际只使用了其中的四芯，U 口的 R1604 可不通过 NT1，直接与两芯的 ISDN 用户线相连。

BRI 接口规程定制的带宽为 2B+D，共 128Kbps。

ISDN BRI 接口缺省封装链路层协议为 PPP，支持 IP 和 IPX 等网络层协议。

Quidway R4000 系列路由器（其他中高端路由器选配）各提供了一个 CE1/PRI 接口，下面将对这种接口进行介绍。

CE1/PRI 接口

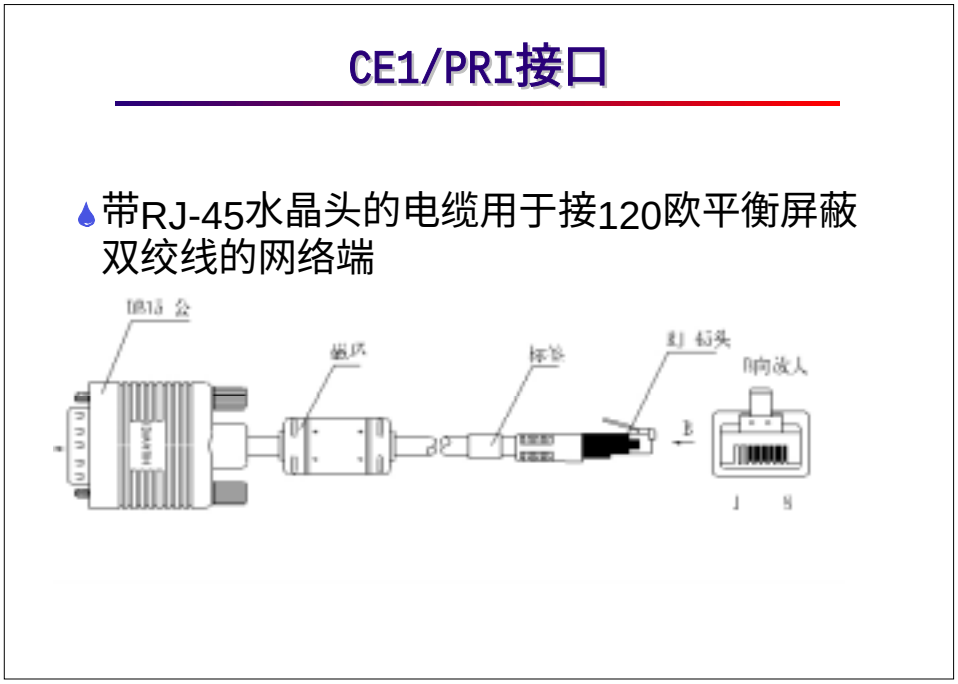


CE1/PRI 接口在华为 Quidway 系列路由器中一般可见于 R4001 或各种中高端路由器的接口配置中。从 CE1/PRI 接口的这个名字就不难推断，该接口可以承载 CE1 和 PRI 这两种不同接口规程的数据传输任务。

对应于 CE1 封装，大多数用于与 DDN 节点机的连接，最多可以支持同时划分为 31 个 64K 的逻辑接口，用于 DDN 连接，当然，按照实际需要，也可以通过捆绑多个时隙作为一个接口使用（channel-group）的方法，这样可以灵活的配置每条连接的带宽（必然是 64K 的整数倍）。可以使用的时隙范围为 1~31，时隙 0 用于系统同步，不能用于数据传输。每一个逻辑接口特性均与同步串口相同，支持 PPP、帧中继、LAPB 和 X.25 等链路层协议，支持 IP 和 IPX 等网络层协议。

对应于 PRI 封装，主要用于作为 ISDN 用户的接入服务，PRI 接口最多可以同时接入 30 位 ISDN 单 B 用户，或者 15 位双 B 用户。与 R2509 或 R2511 对应，R4001 可以作为一个经济的小型数字用户接入服务器使用。

CE1/PEI 接口（续）



PRI 能使用 32 个时隙中的 30 个，另外的 0 时隙用于系统同步，15 时隙用作 D 信道传输信令，不能随便使用。需要注意的是，PRI 封装只能捆绑出一个接口（PRI-GROUP），此接口未捆绑的时隙将不能使用。PRI-GROUP 的逻辑特性与 ISDN 拨号口相同，支持 PPP 链路层协议和 IP/IPX 等网络层协议，可以封装 DDR 等参数。

路由器 CE1/PRI 接口端为 DB-15（针式）连接器，在网络端分别是 BNC 头或 RJ-45 水晶头连接器。上页图示为网络端为 BNC 头的 CE1/PRI 电缆。

PRI 接口能提供的总带宽为 30B+D，共 2048Kbps。

本页图示为外接网络端为 RJ-45 连接器的 CE1/PRI 电缆。

介质电缆使用 120 欧平衡屏蔽双绞线。

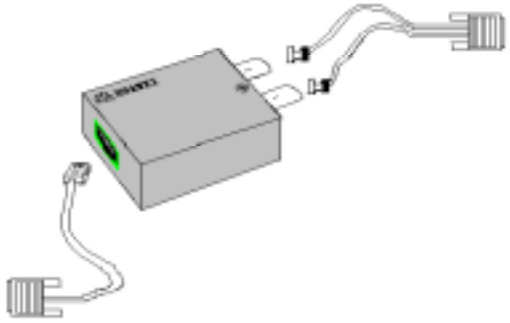
注：配置 CE1/PRI 接口时，需注意其帧校验方式、线路编解码格式和线路时钟的设置应与对端保持一致。

现在，一般都使用下图所示的 75 欧铜轴电缆到 120 欧屏蔽双绞线的转换适配器来连接使用 RJ-45 连接器的 CE1/PRI 电缆。

CE1/PEI 接口（续）

CE1/PRI接口

- 75欧BNC同轴电缆到120欧平衡屏蔽双绞线的转接器



本图为 75 欧 BNC 同轴电缆到 120 欧平衡屏蔽双绞线的转接适配器示意。

.4.6　宽带接入方式

ATM 接口是 Quidway 系列高端路由器才具有的特殊接口，用以连接基于 ATM 传输技术的宽带网络。ATM 即 Asynchronous Transfer Mode 异步传输模式的英文缩写。ATM 接口一般使用带宽 155Mbps（OC-3）或 622M（OC-12）的单/多模光纤作为传输介质，具有带宽宽（还可以成倍扩展），传输距离远，不易受电磁干扰等多方面的优点，发展潜力巨大。
ATM 接口在 Quidway 系列高端路由器中以可选模块的方式出现。
SDH —— Synchronous Digital Hierarchy 同步数字系列的英文缩写，现多用于底层物理传输，是目前使用最多的光传输网络。

.5　本章重点

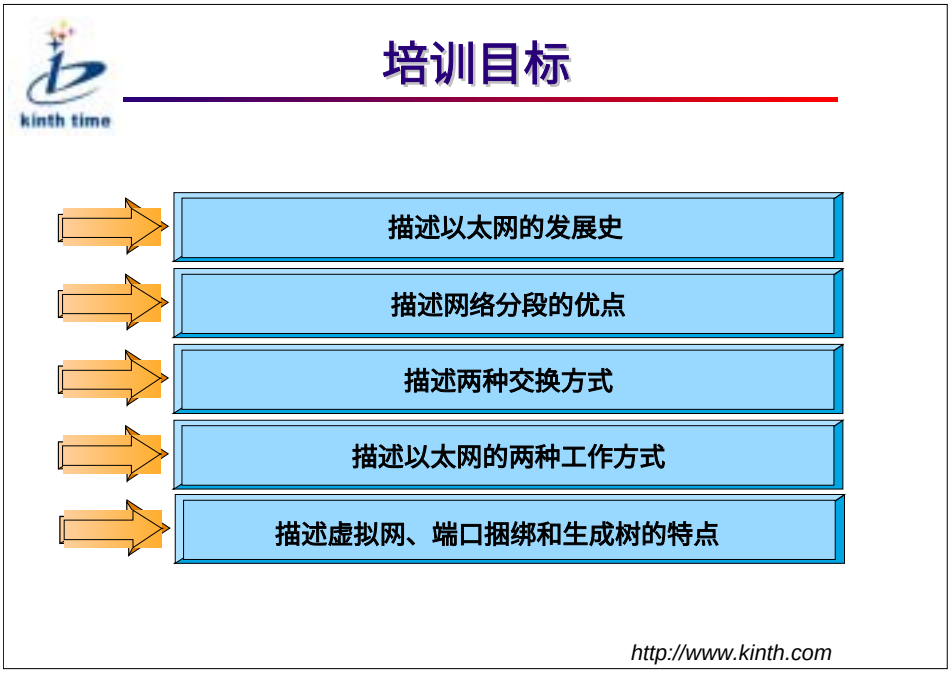
本章重点

- 常见局域网：以太网，令牌环网使用的传输介质类型；
- V.24，V.35 接口规程定义的物理特性，传输特性；
- V.24，V.35 接口几种常见控制信号的作用与意义；

本章掌握的重点如下：
常见局域网：以太网，令牌环网使用的传输介质类型；
V.24、V.35 接口规程定义的物理特性，传输特性；
V.24、V.35 接口几种常见控制信号的作用与意义；
Quidway 系列路由器各接口使用的电缆类型。

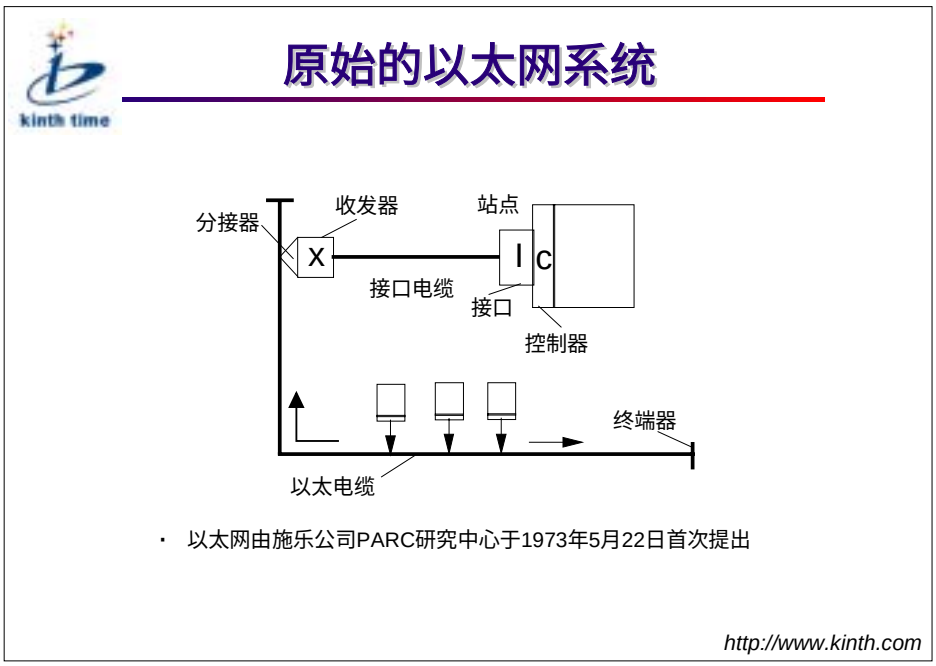
第三章　　以太网交换机基础

.1　培训目标



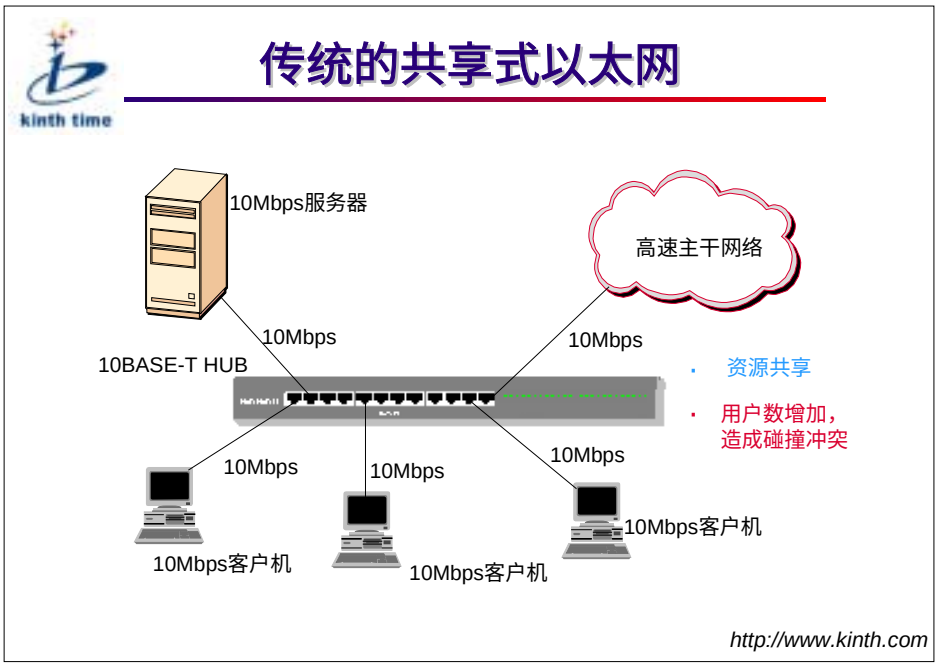
.2　以太网发展及原理

.2.1　原始的以太网系统



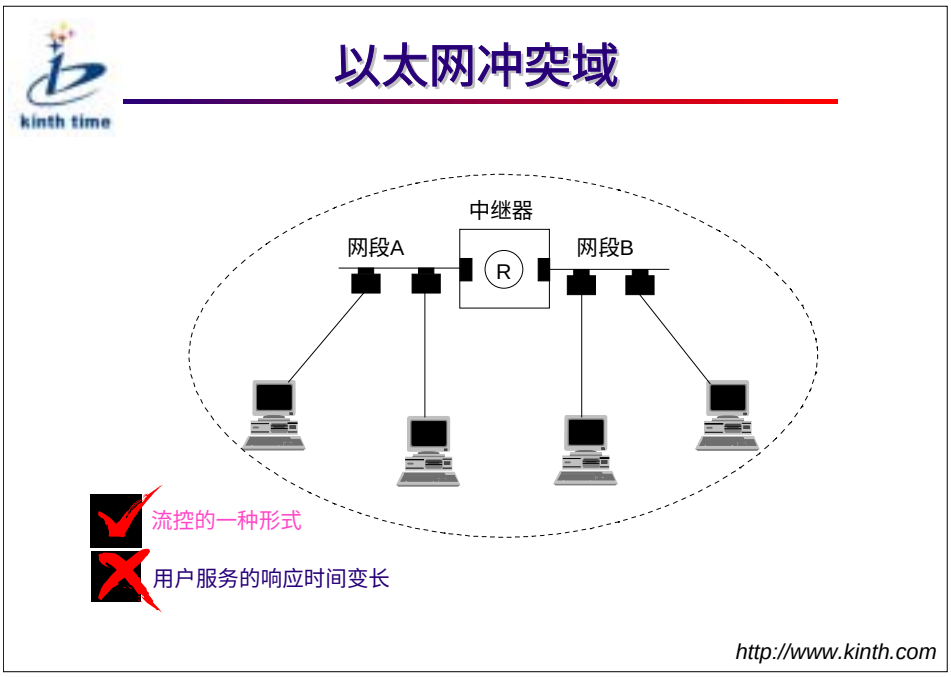
以太网由施乐公司 PARC 研究中心的 Bob Metcalfe 于 1973 年 5 月 22 日首次提出，至 1999 年已经有了 26 年的历史。在这 26 年中，以太网技术如同计算机技术一样， 不断创新，不断发展，成为世界上最流行的局域网。

.2.2　传统的共享式以太网



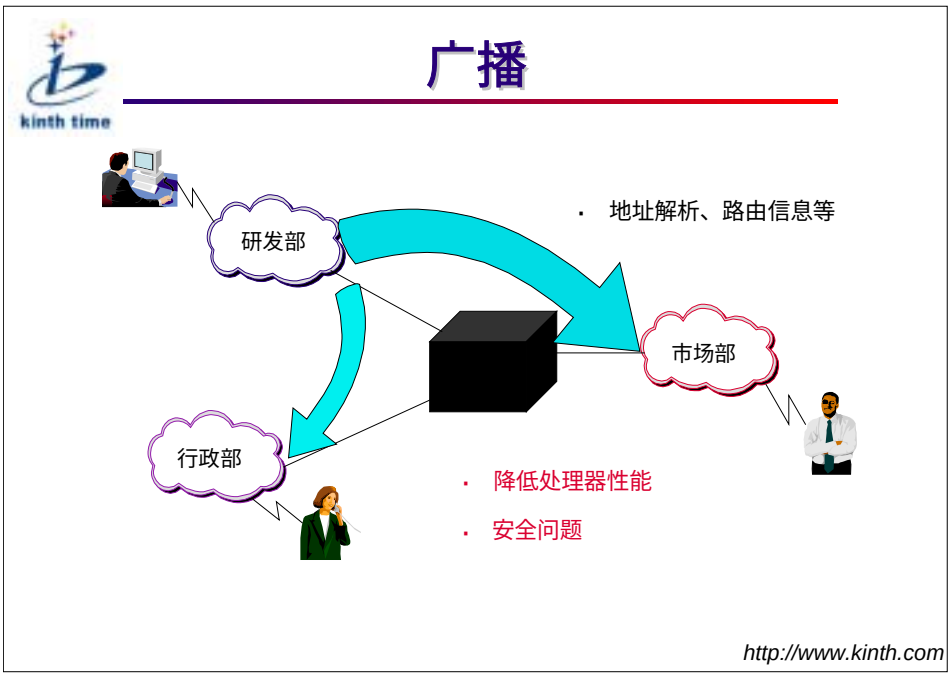
传统的共享式以太网通过将用户连接到中继器实现资源共享，但是随着通信量和用户数的增加，超出一定数量时会造成碰撞冲突。

.2.3　以太网冲突域



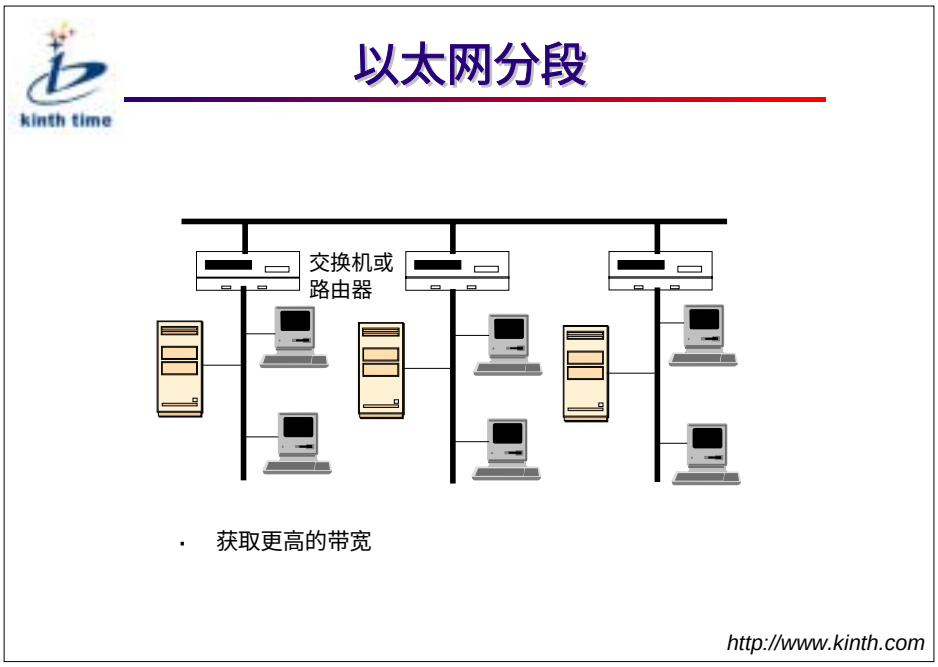
冲突不是以太网中的故障，而是作为流控的一种形式成为以太网操作的正常组成部分，它带来快速而又自动的重新发送调整。然而随着通信量和用户数的增加，冲突率也不断地增加，这样有效带宽减少，网络性能降低，导致用户服务的响应时间变长。

.2.4　广播



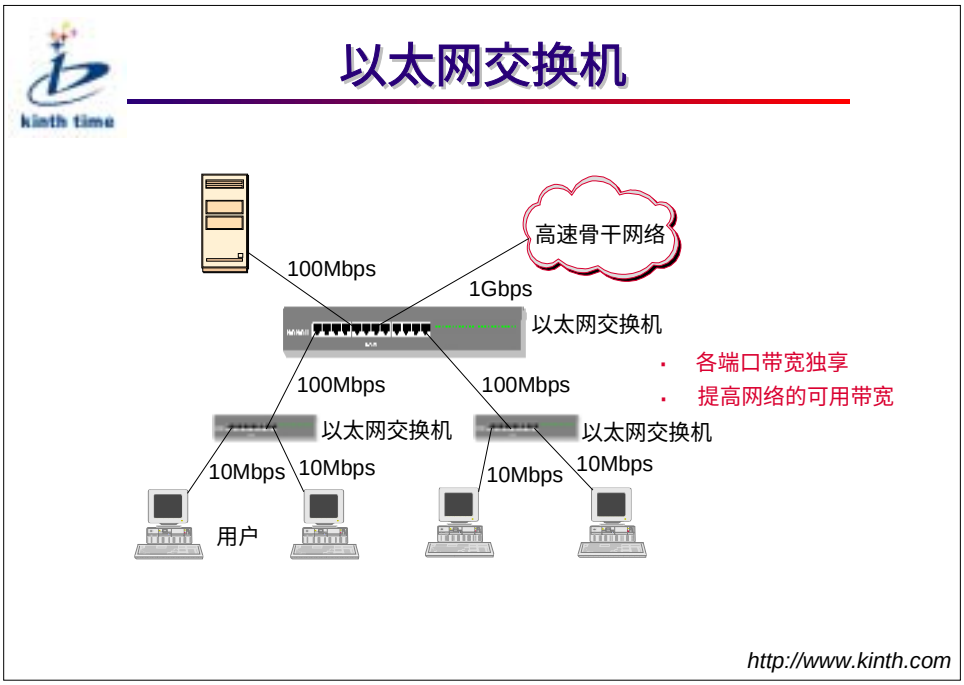
大多数网络协议都利用广播来提供网络信息，而广播包到达所有的计算机，计算机必须处理这些广播包，大大降低了处理器的性能。另外，在共享式网络中，安全问题得不到保证，由于所有数据包到达中继器后往所有端口广播，这样信息很容易被窃取。

.2.5　以太网分段



随着技术的更新，网络也在不断地发展，性能更优的计算机产生了。网络不再仅仅用于发送电子邮件，声音、图象伴随着数据在网络上应运而生，此时对网络带宽的需求越来越高。对网络分段便是获得高带宽的一种有效途径。目前主要用路由器和以太网交换机完成以太网分段。

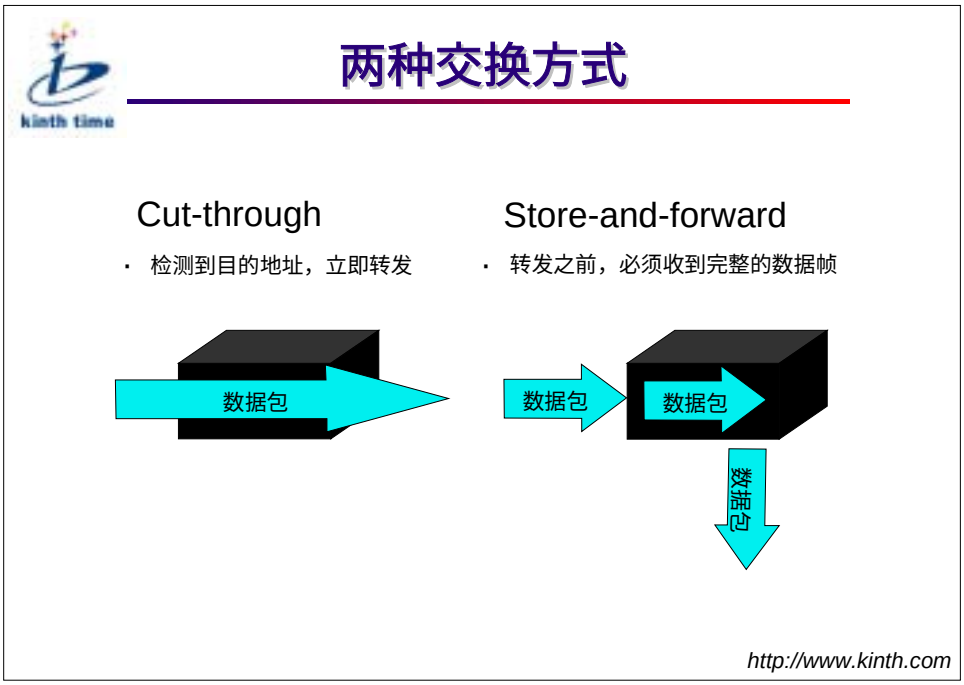
.2.6　以太网交换机



以太网交换机是较经济实用的一种以太网分段的技术。以太网交换机能够实现高速数据交换，各个端口完全独享带宽，这样网络的可用带宽有了很大的提高。

以太网交换机价格低廉，易于安装和操作。

.2.7　两种交换方式

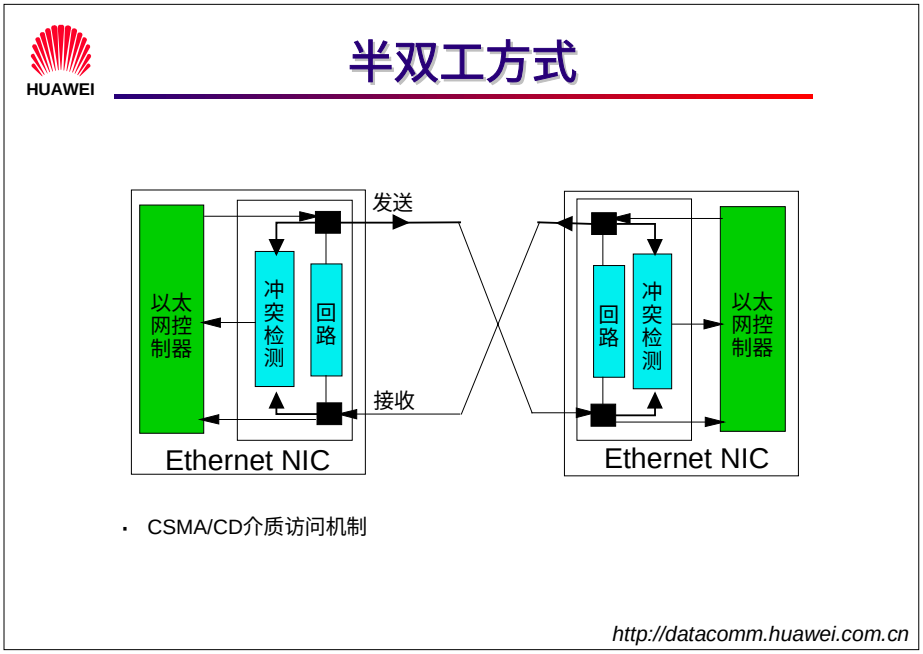


帧交换的方式主要有两种：

☞ Cut-through：交换机一旦接收到帧头便检查目的地址，并且立即转发该帧。

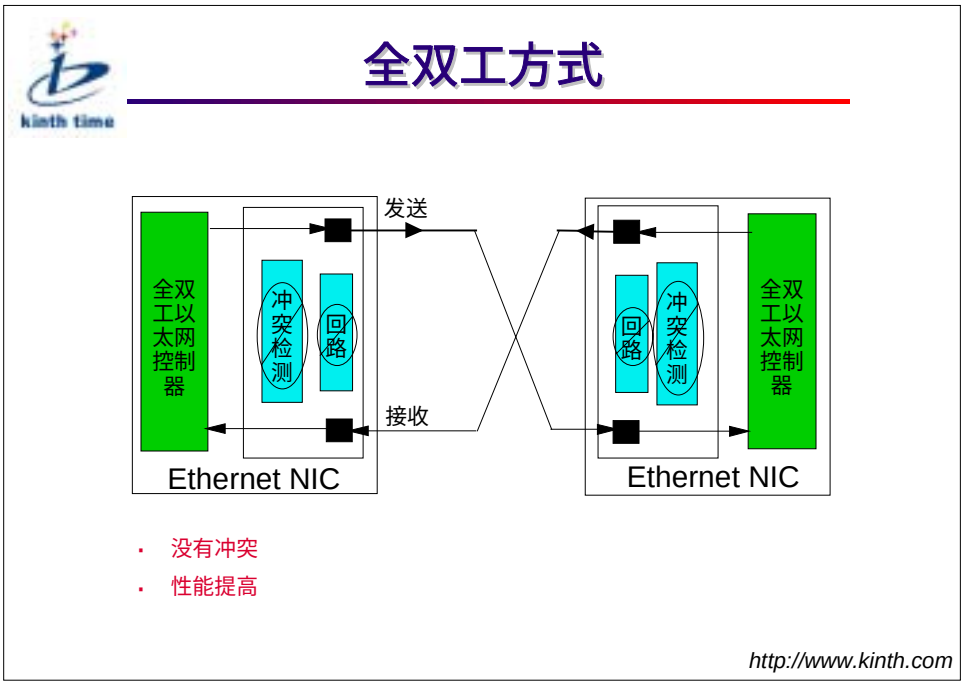
☞ Store-and-forward：在转发之前，交换机必须接收到完整的数据帧，读取目的和源地址，进行CRC校验，并作相应的过滤。这样，加长了交换延时，但保证数据的准确性。

.2.8　半双工方式



以太网利用CSMA/CD介质访问机制实现半双工流量控制。

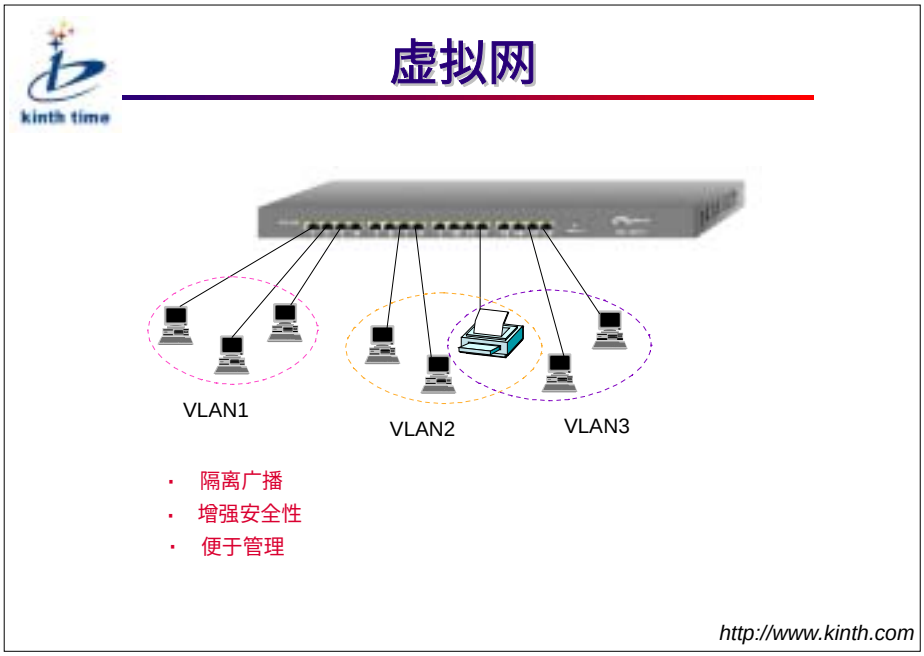
.2.9　全双工方式



全双工以太网技术为发送电路和接收电路提供了直接的连接，这样没有了冲突，消除了竞争，性能也得到了很大的提高。

.3 以太网扩展功能

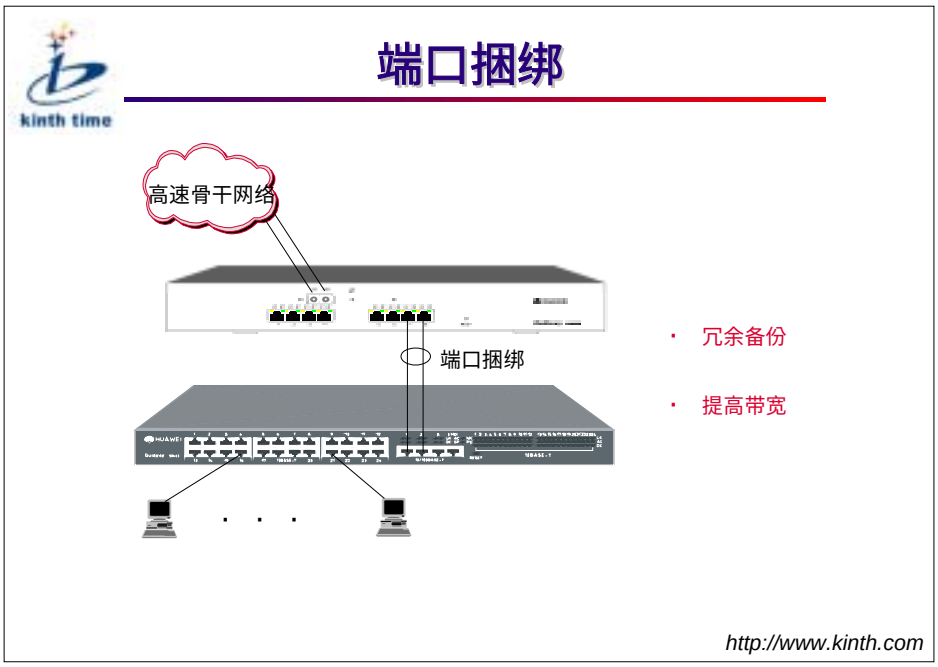
.3.1 虚拟网



虚拟网将连接在同一个物理网络上的主机分组，使它们看起来就象连接在不同的网络上。

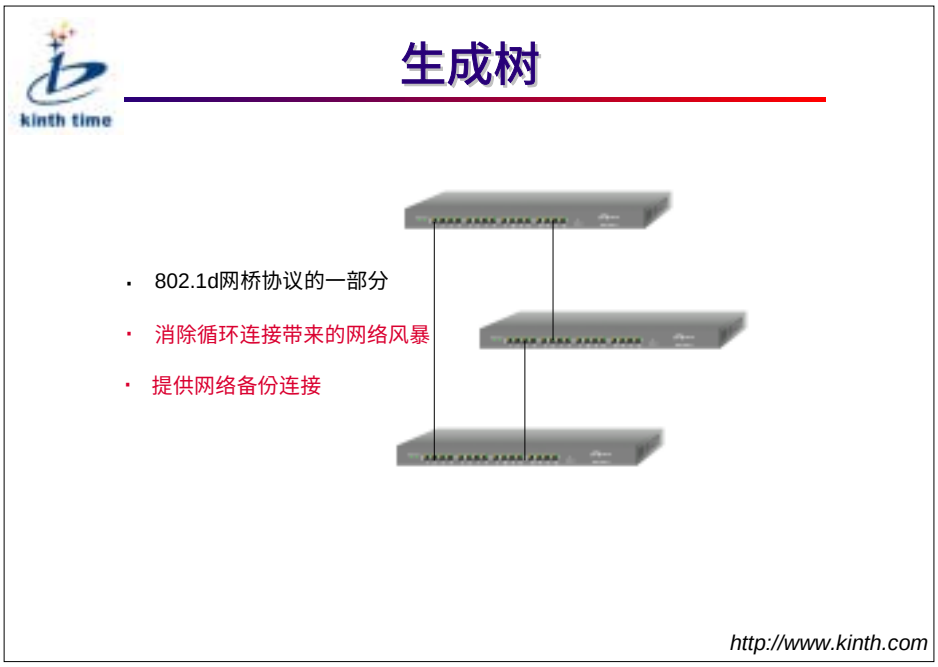
使用虚拟网，可以限制网上的计算机互相访问的权限，各个网段可以共用同一套网络设备，节约了网络硬件的开销，同时也便于迁移，从而降低了成本。

.3.2　端口捆绑



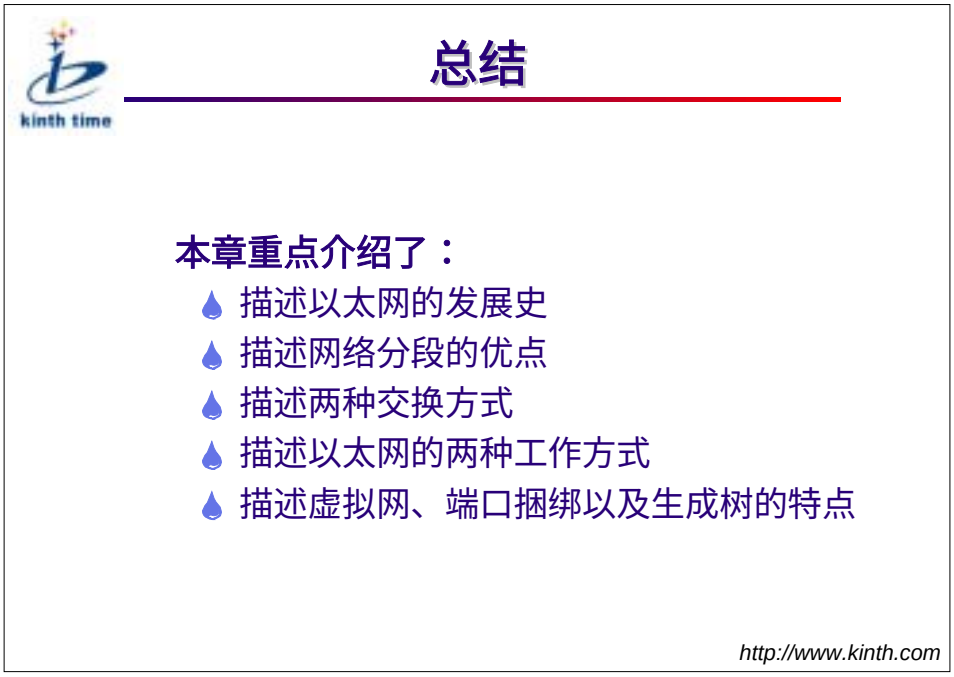
端口捆绑是将多个端口设为一组，这样既提高了带宽，又提供端口备份功能。

.3.3　生成树



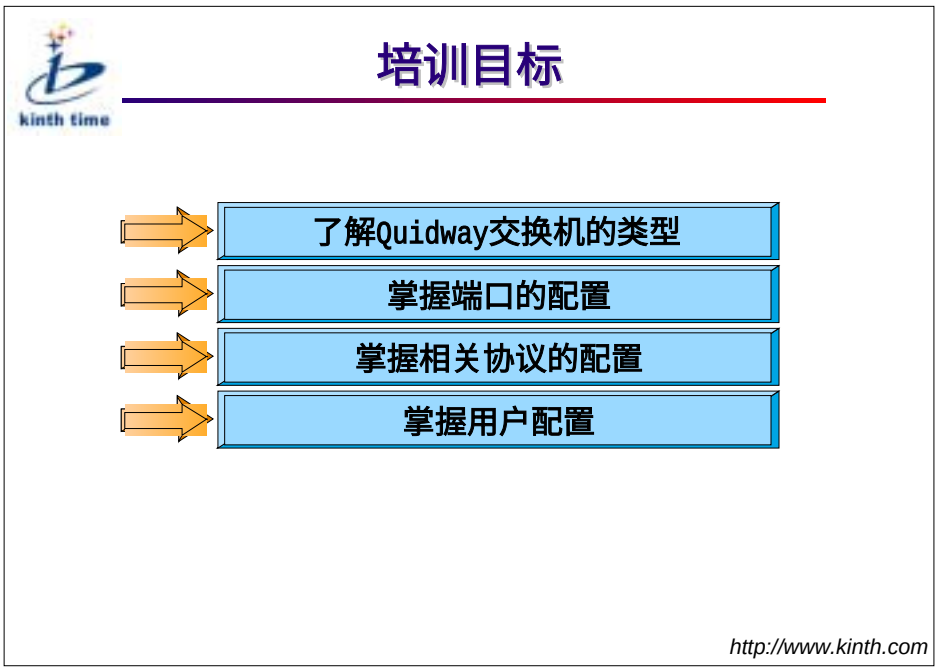
生成树协议是 IEEE 802.1D 网桥协议的一部分。标准的生成树可以消除因网络循环连接造成的网络风暴，同时也为网络备份提供了可能。

.4 小结


kinth time
总结
本章重点介绍了：
描述以太网的发展史
描述网络分段的优点
描述两种交换方式
描述以太网的两种工作方式
描述虚拟网、端口捆绑以及生成树的特点
http://www.kinth.com

第四章 LAN Switch 配置

.1 培训目标



.2 Quidway S2403 交换机

Quidway S2403 以太网交换机端口及性能参数如下：

提供 24 个 10Base-T 以太网端口；

提供 3 个 100Base-T 以太网端口（其中第27号端口同时提供 MDI 和 MDIX 两种接口，但同时只能使用其中之一）；

最多可支持 2048 个 MAC 地址；

交换方式同时支持 Cut-through 和 Store-and-forward；

支持 MIB-II，可通过 Console 或 Telnet 进行管理。

.3 Quidway S3016 交换机

Quidway S3016 以太网交换机端口及性能参数如下：

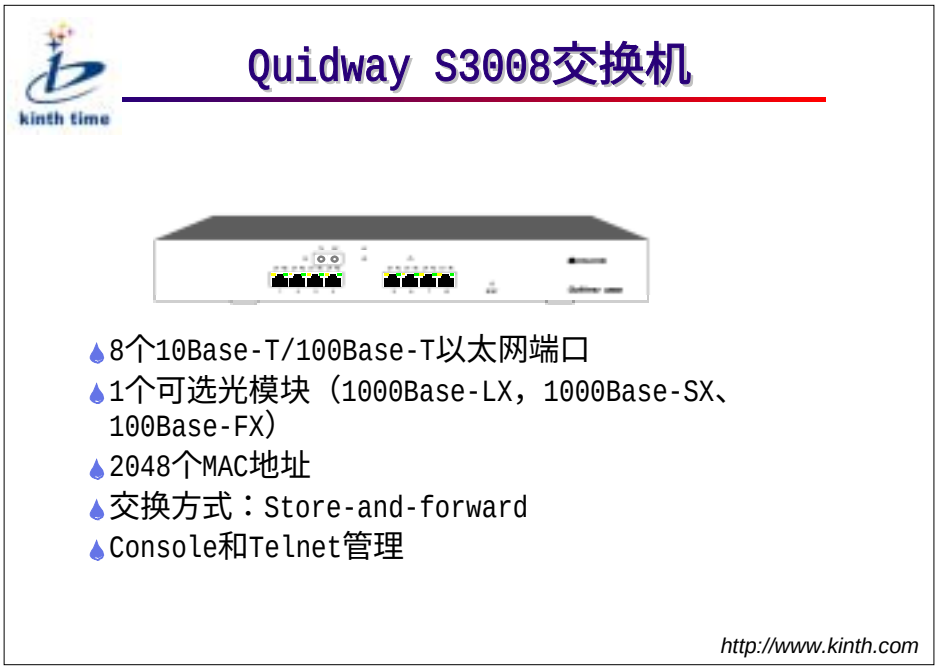
提供16个10Base-T/100Base-T 自适应以太网端口；

最多可支持 4096 个 MAC 地址；

交换方式：Store-and-forward ；

支持 MIB-II，可通过 Console 或 Telnet 进行管理。

.4 Quidway S3008 交换机



Quidway S3008 以太网交换机端口及性能参数如下：

提供8个10Base-T/100Base-T 自适应以太网端口；

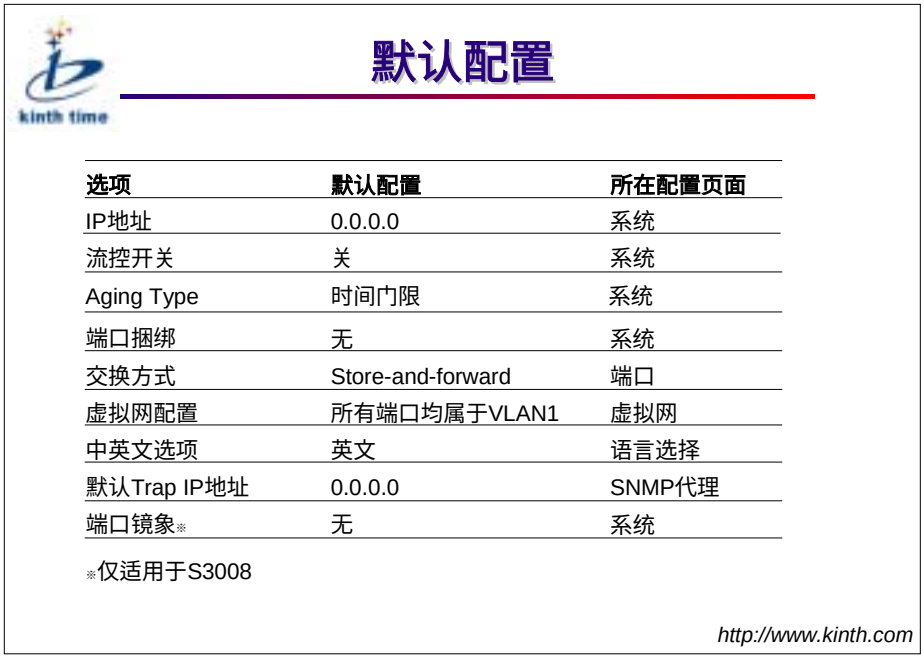
提供1个可选光纤模块：可在1000Base-LX，1000Base-SX，1000Base-FX 三种模块中选择；

最多可支持 2048 个MAC地址；

交换方式：Store-and-forward ；

支持MIB-II，可通过 Console 或 Telnet 进行管理。

.5　默认配置



默认配置

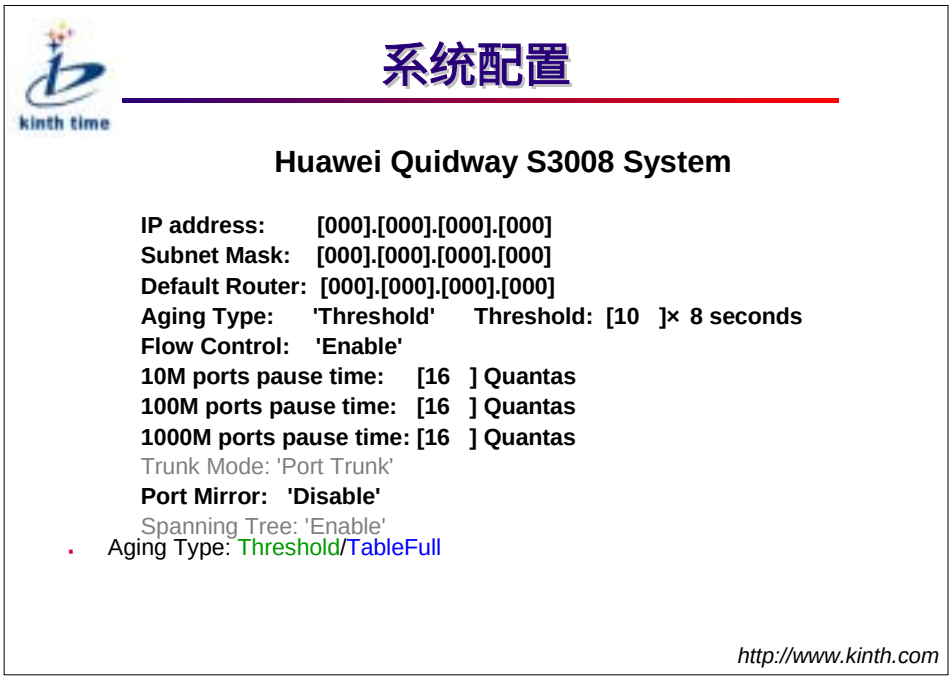
选项	默认配置	所在配置页面
IP地址	0.0.0.0	系统
流控开关	关	系统
Aging Type	时间门限	系统
端口捆绑	无	系统
交换方式	Store-and-forward	端口
虚拟网配置	所有端口均属于VLAN1	虚拟网
中英文选项	英文	语言选择
默认Trap IP地址	0.0.0.0	SNMP代理
端口镜象※	无	系统

※仅适用于S3008

http://www.kinth.com

上图显示为三种交换机的默认设置，基于这些默认配置，交换机便可正常工作。

.6 系统配置



本页上图以 Quidway S3008 的系统配置页面为例显示了Quidway 系列以太网交换机的系统配置项目。

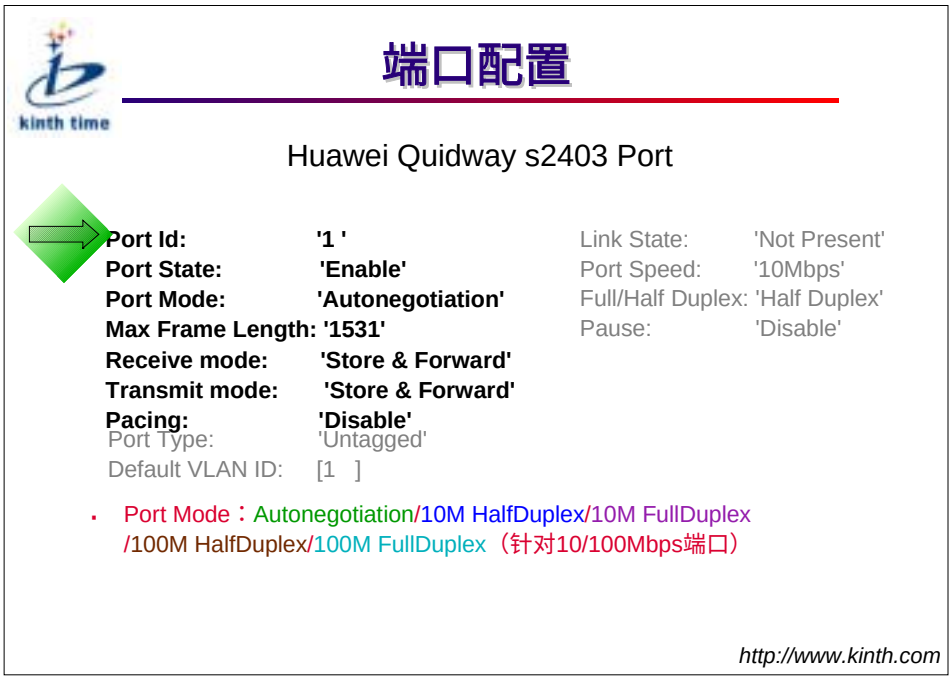
前三项为交换机的 IP 地址、子网掩码及其默认网关。不配置 IP 地址，将不能使用 SNMP 和 Telnet 管理交换机。

Aging Type 项设置 MAC 地址表的地址删除管理方式：Threshold Aging 和 TableFull Aging。

Threshold Aging 是指地址表中的地址项的时间戳增长到一定数值时，将它从地址表中删除；TableFull Aging 是指地址表填满时将时间戳最大的地址项删除。

Flow control 项设置允许/ 禁止启动流量控制。半双工方式下，以太网的流量控制是基于 CSMA/CD 算法的；全双工方式下，以太网的流量控制采用符合802.3x 的基于 PAUSE 的流量控制策略。

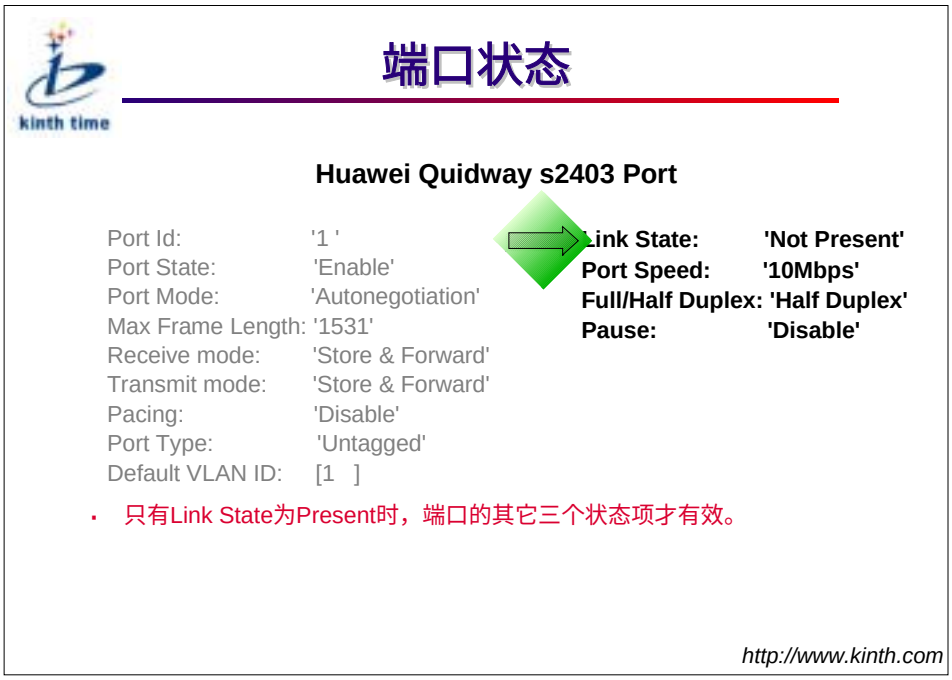
.7 端口配置



端口配置页面中，Port State 项为端口的管理状态，可设置为允许/ 禁止。

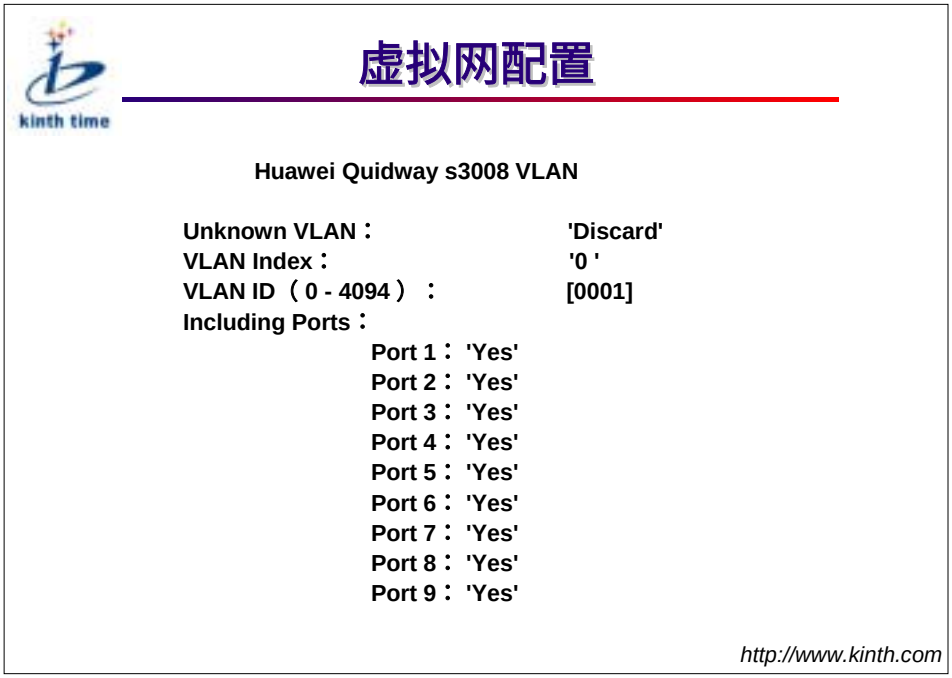
Port Mode 项可将本端口设置为自动协商方式，也可设置为固定工作模式（包括端口的工作速率和双工方式）。

.8 端口状态



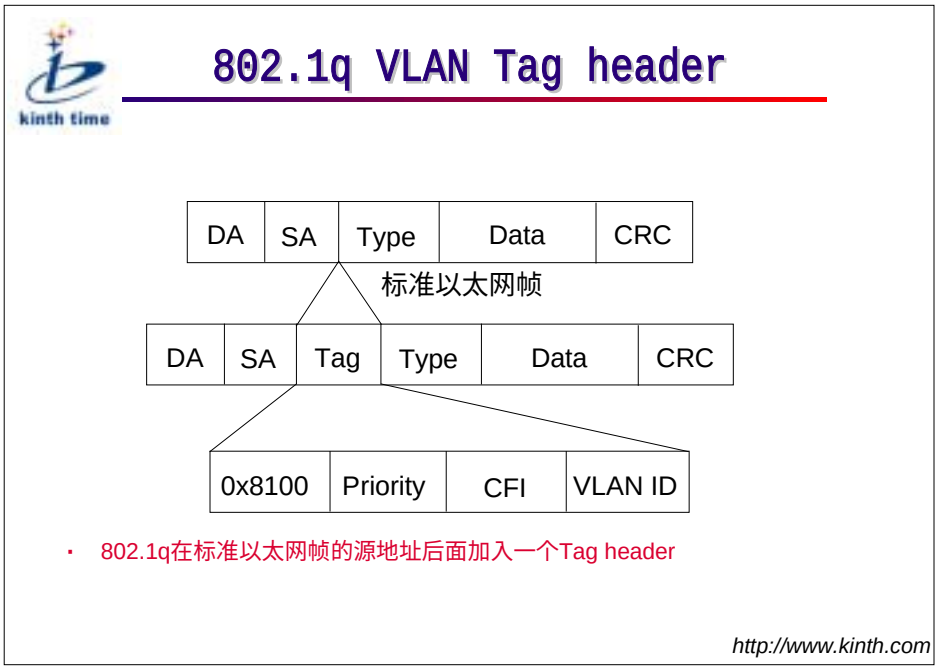
状态项 Link State 用以表明端口是否连接设备，该状态也可通过交换机前面板的指示灯查看，橘黄灯亮表示有连接，灭表示没有连接。只有端口连接了设备，其它状态才起作用。

.1 虚拟网配置



VLAN 通过广播域的设置实现主机分组。

.2 802.1q VLAN Tag header



IEEE 802.1q 是新的虚拟局域网标准，符合 IEEE 802.1q 标准的以太网交换机实现的虚拟局域网之间可以互通。

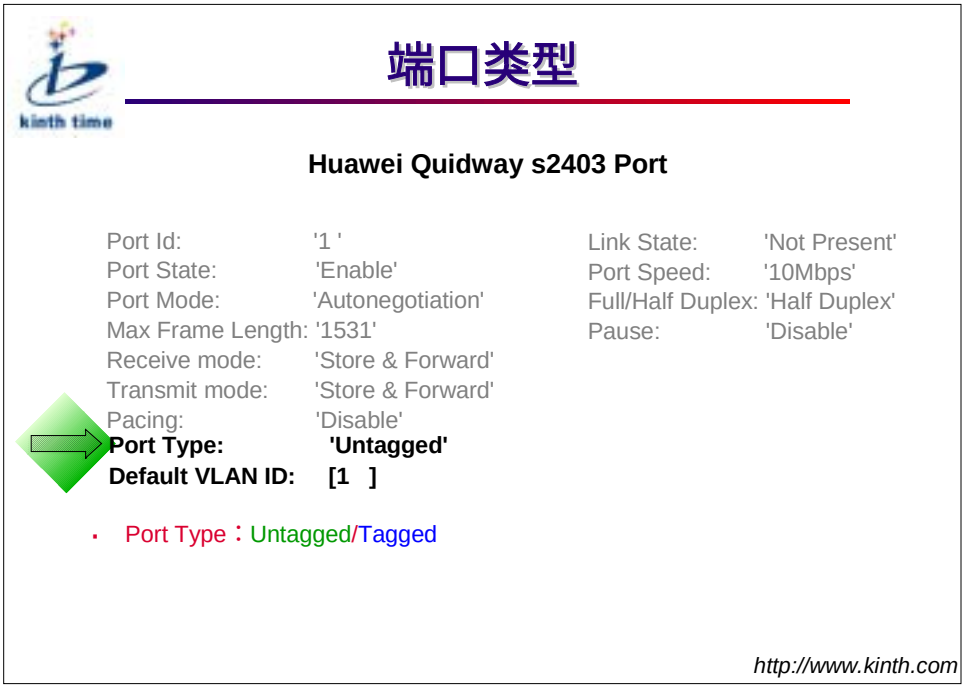
配置 VLAN 时，需要考虑三项配置：

端口类型（Untagged/Tagged）：标志端口所连接的设备是否支持带有802.1q Tag header的帧；

端口的缺省 VLAN ：当交换机不能从一个帧的 Tag header 中识别该帧属于哪一个 VLAN 时，就指定其属于接收端口的缺省 VLAN ；

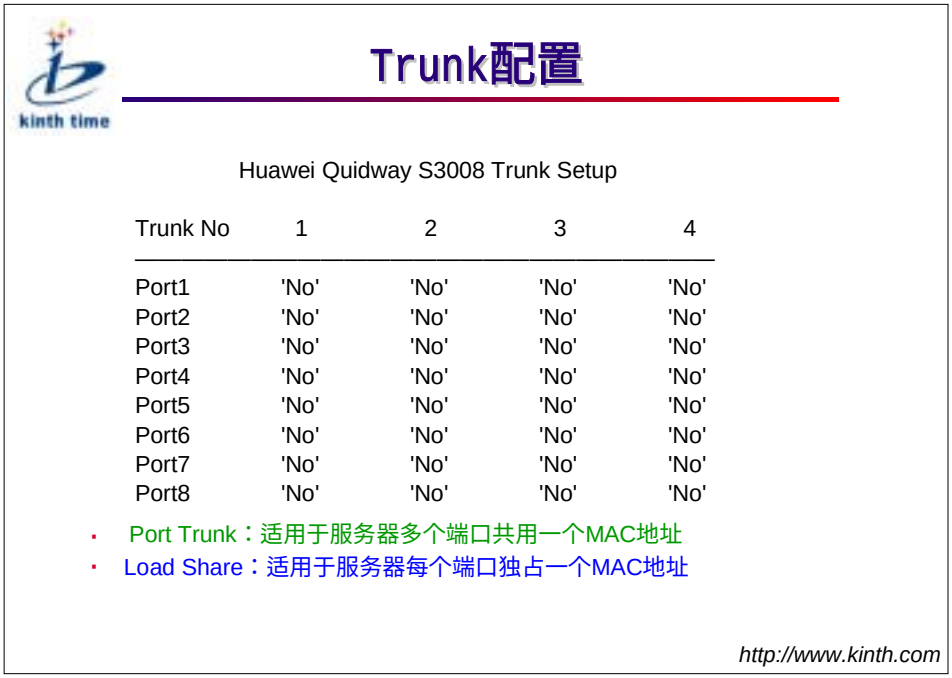
VLAN 广播域：用于界定属于该 VLAN 的帧的转发范围。

.3 端口类型



端口类型（虚拟局域网）设置如上图示。

.4 Trunk 配置



在配置Trunk 端口时，需要注意：

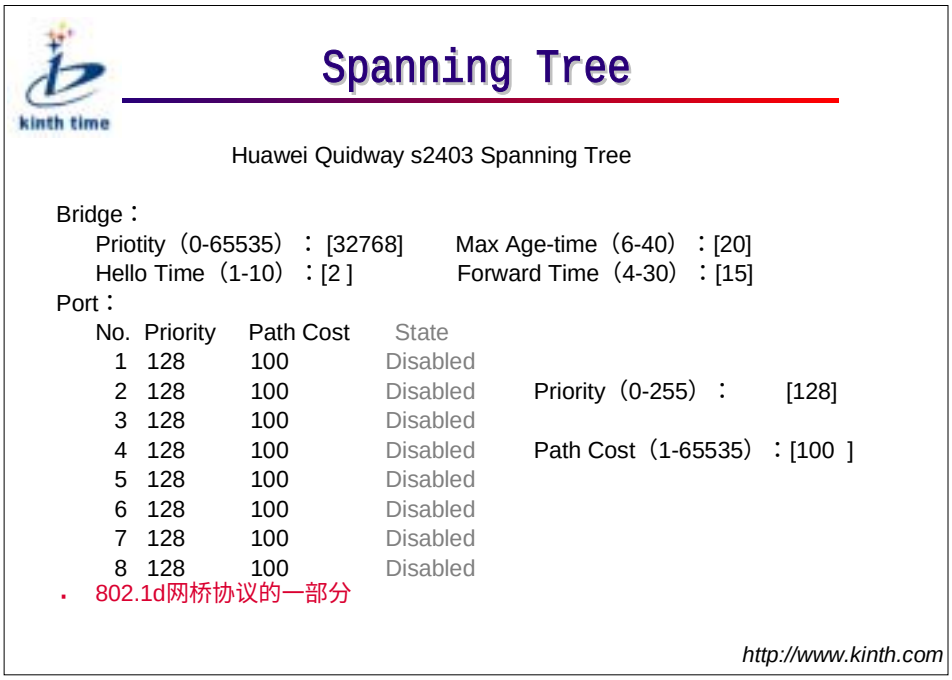
Trunk 线路两端的端口都应设置为 Trunk 方式；

所有 Trunk 端口的 VLAN 设置应该保持一致；

建议所有 Trunk 端口的其它设置也保持一致；

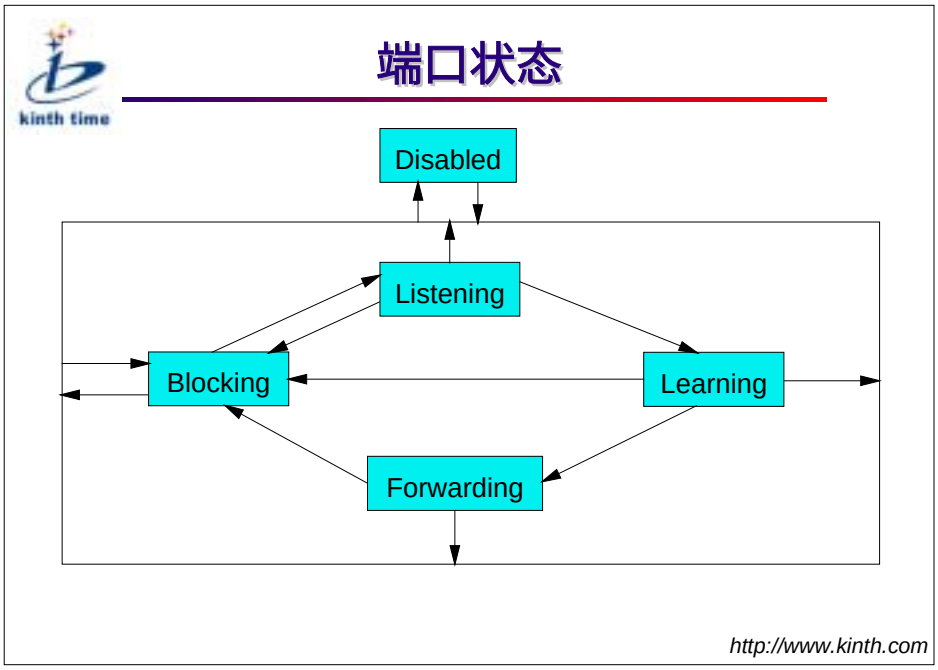
所有 Trunk 端口的工作速率应保持一致。

.5 Spanning Tree



Spanning Tree 算法通过将导致循环连接的端口（如果处于活动状态）设置为阻塞状态，来保证网络拓扑中没有环路存在。

.6 端口状态



以上五种端口状态的含义如下：

Disabled：端口不参加生成树协议的计算；

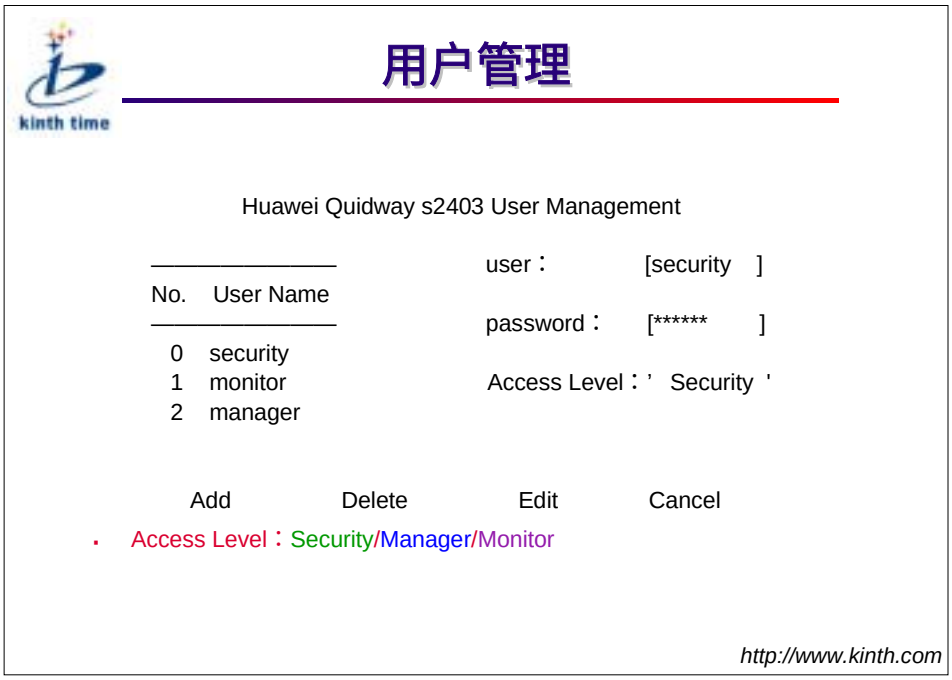
Blocking：经协议计算端口被阻塞。该状态下，端口除可以接收 BPDU（桥协议数据单元）外不能收发任何帧；

Listening：经协议计算阻塞端口应该打开。由于网络中所有交换机端口状态不能全部立即计算完成，为防止计算过程中出现循环，增加了 Listening 和 Learning 两个状态。Listening 状态下端口的收发工作状态同 Blocking 状态一致；

Learning：该状态下，端口即将转变为 Forwarding 状态，端口开始学习地址，但收发工作状态仍然不变；

Forwarding：端口正常转发数据帧。

.7 用户管理



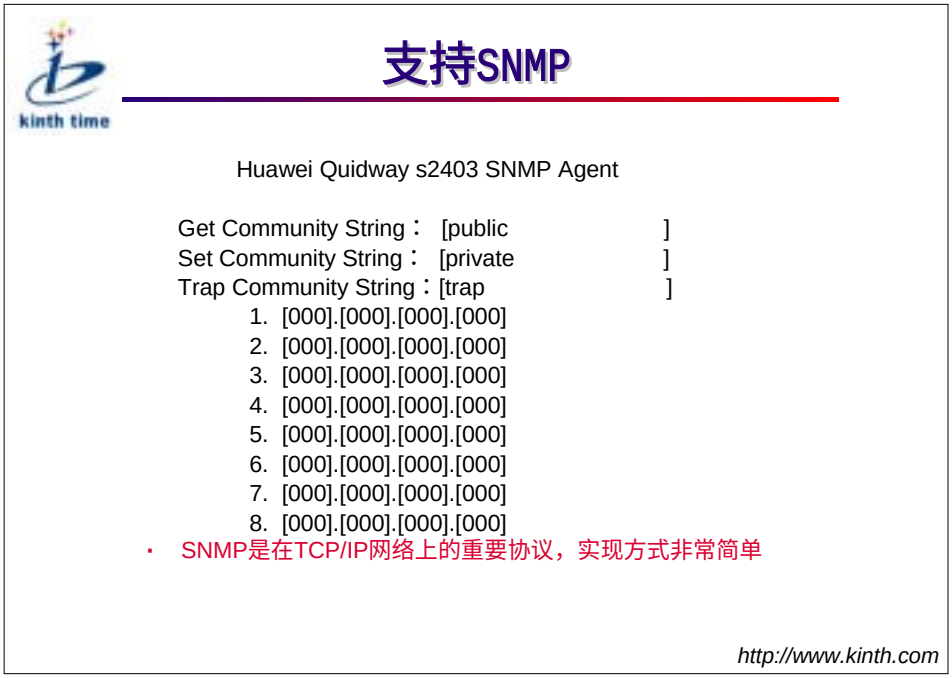
Quidway S2403/3016/3008 以太网交换机系统的用户有3个级别：

Security：用户拥有最高权限，可以访问系统提供的所有功能；

Manager：用户拥有次高级权限，除不能修改软件下载口令，拥有其它所有访问权限。

Monitor：用户拥有最低的权限，可以查看系统配置和状态，但不能作任何修改操作。

.8 支持SNMP



SNMP协议给大型网络的集中管理提供了可能。

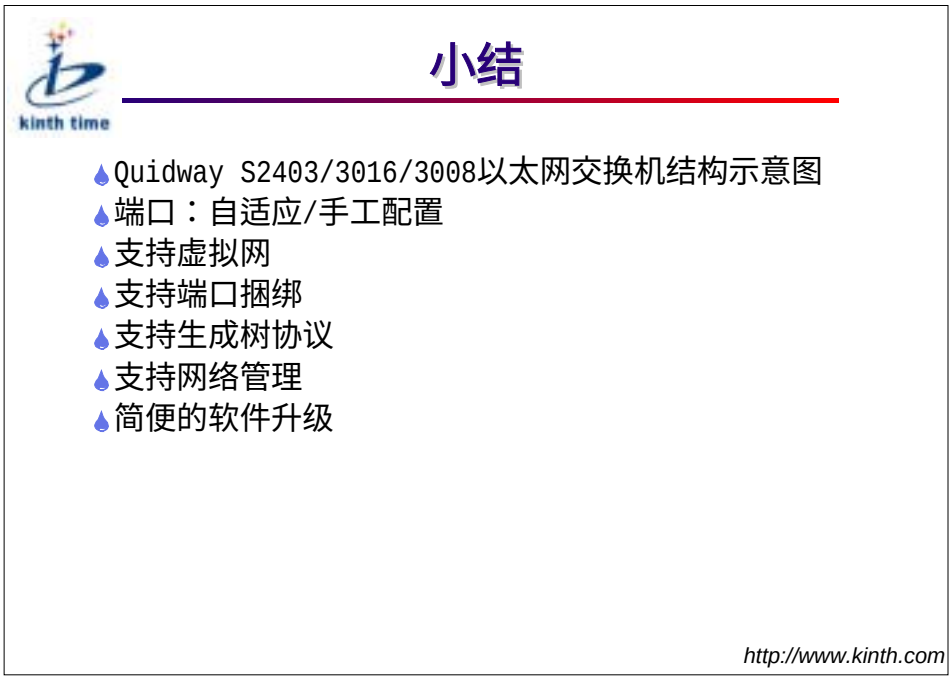
上图显示为SNMP 命令设置页面。

以太网交换机的SNMP Agent 解析出网管站的管理请求，采集信息给出回应或同时产生相应的操作。

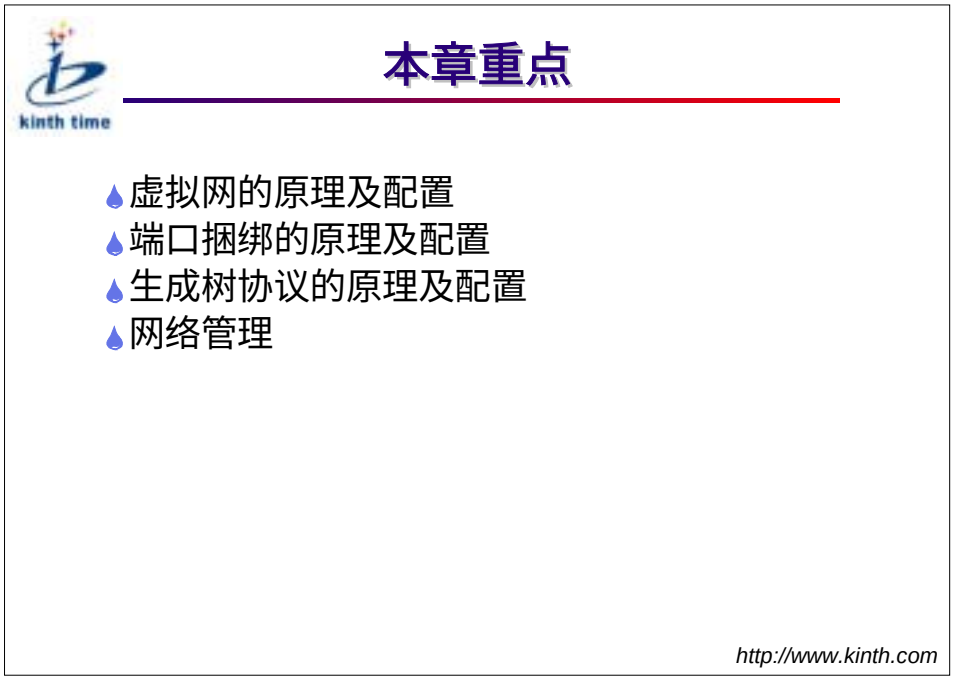
.9 软件升级管理

Quidway S2403/3016/3008 以太网交换机的软件初始阶段提供了程序下载功能，在口令正确的情况下，可以根据提示信息简单完成软件升级工作。

.10 小结

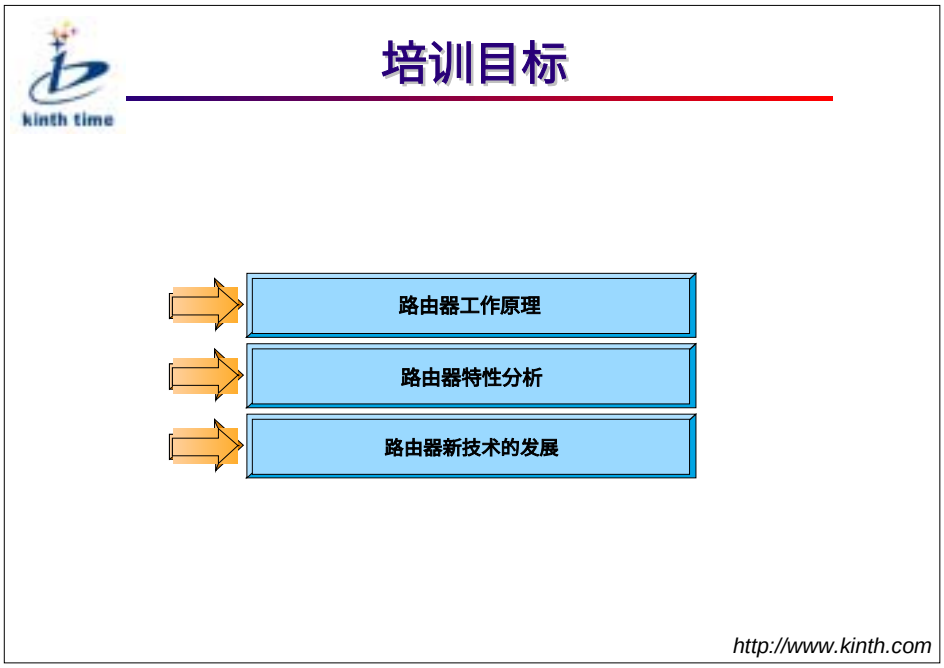

小结
Quidway S2403/3016/3008以太网交换机结构示意图
端口：自适应/手工配置
支持虚拟网
支持端口捆绑
支持生成树协议
支持网络管理
简便的软件升级
http://www.kinth.com

.11 本章重点


kinth time
本章重点
虚拟网的原理及配置
端口捆绑的原理及配置
生成树协议的原理及配置
网络管理
http://www.kinth.com

第五章　　路由器基础及原理

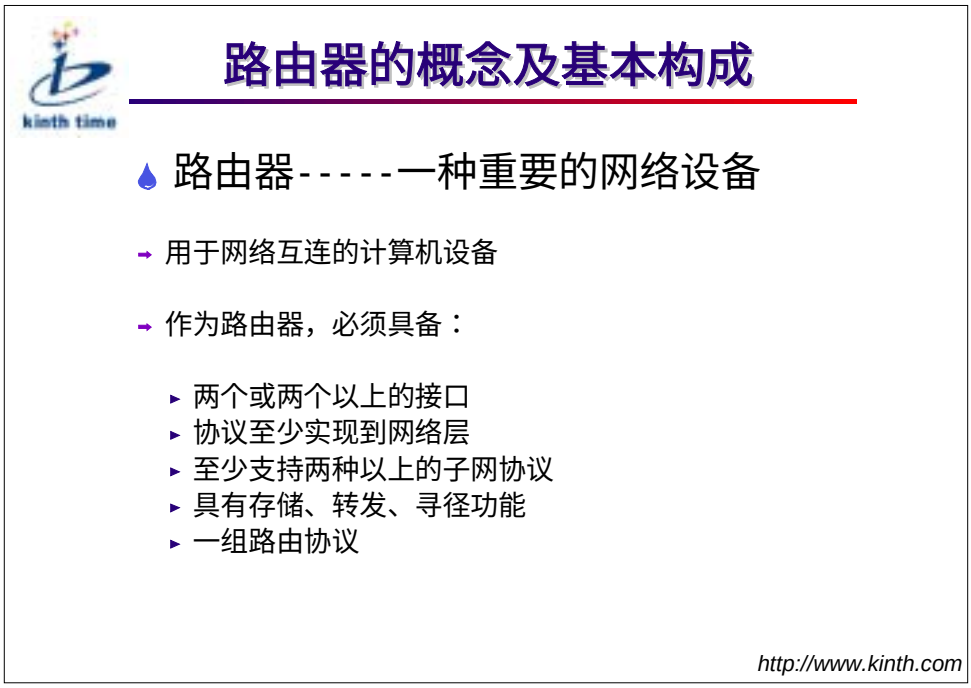
.1　培训目标



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

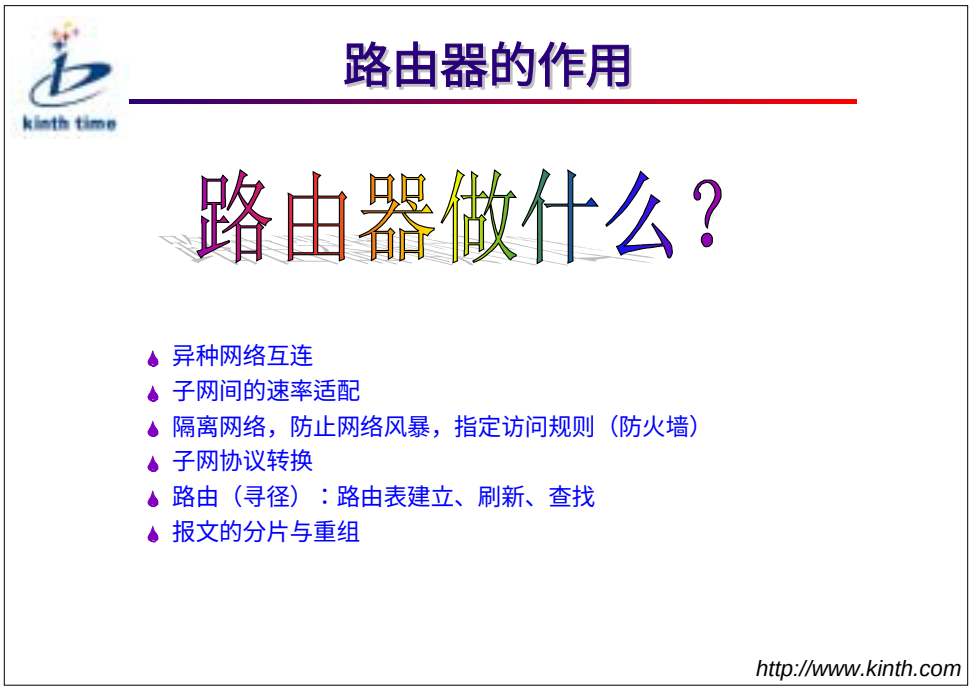
.2.1 路由器的概念及基本构成



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：

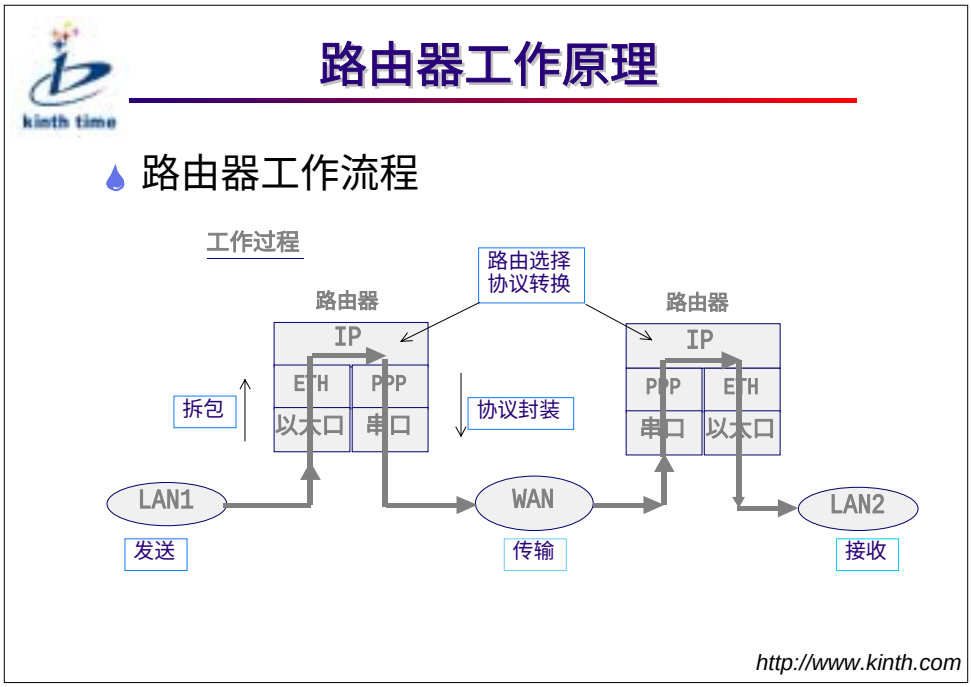
- 两个或两个以上的接口：用于连接不同的网络。
- 协议至少实现到网络层：只有理解网络层协议才能与网络层通讯。
- 至少支持两种以上的子网协议：异种子网互联。
- 具有存储、转发、寻径功能 ：实现速率匹配与路由寻径。
- 一组路由协议：包括域内路由协议、域间路由协议。

.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



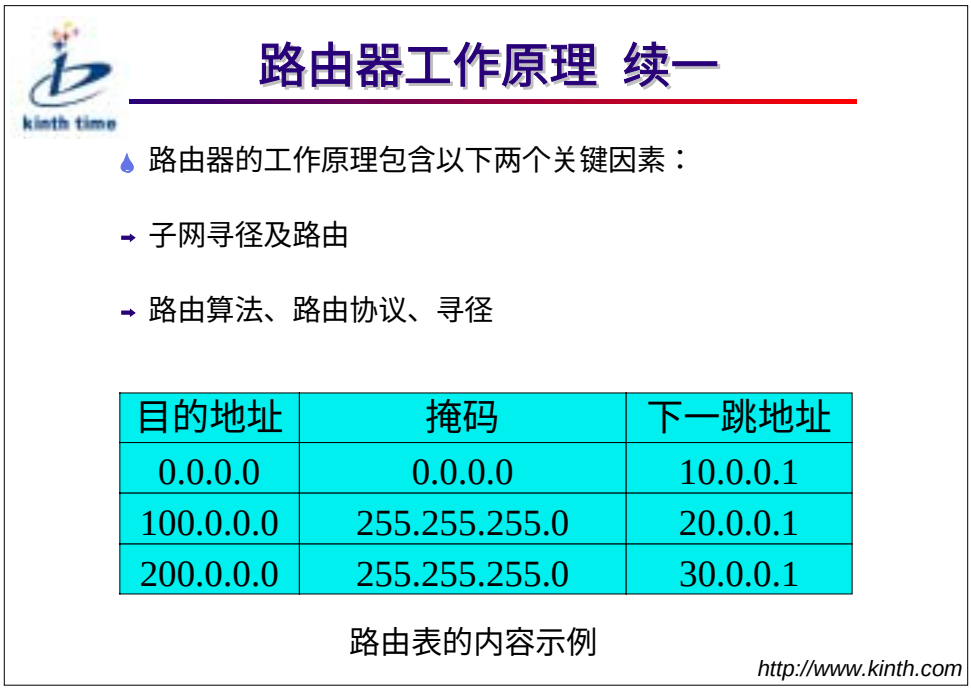
路由器中时刻维持着一张路由表，所有报文的发送和转发都通过查找路由表从相应端口发送。这张路由表可以是静态配置的，也可以是动态路由协议产生的。

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）



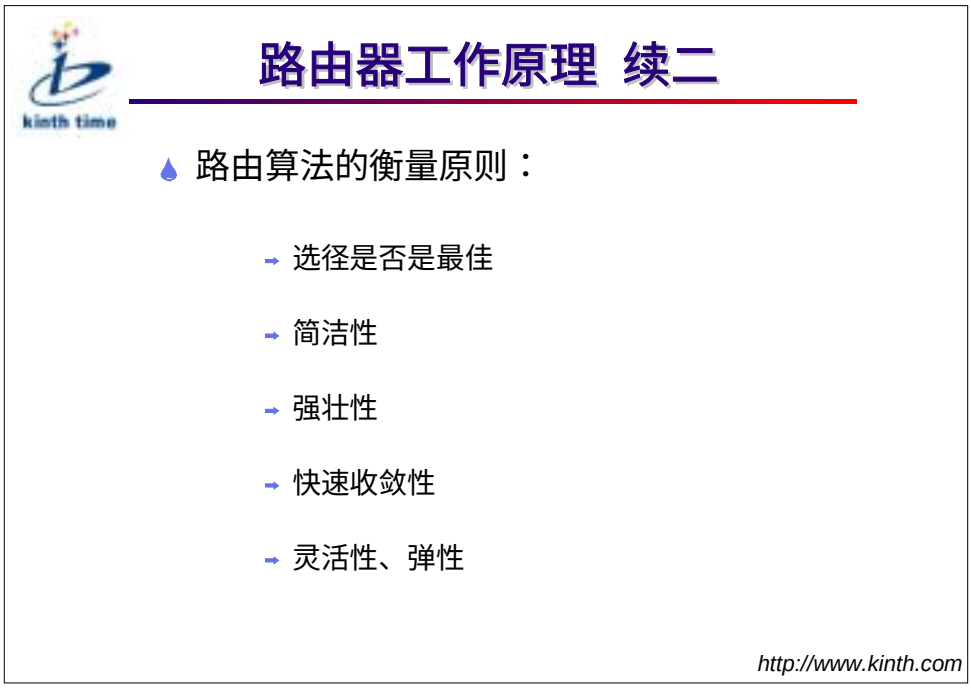
● 子网寻径及路由

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。

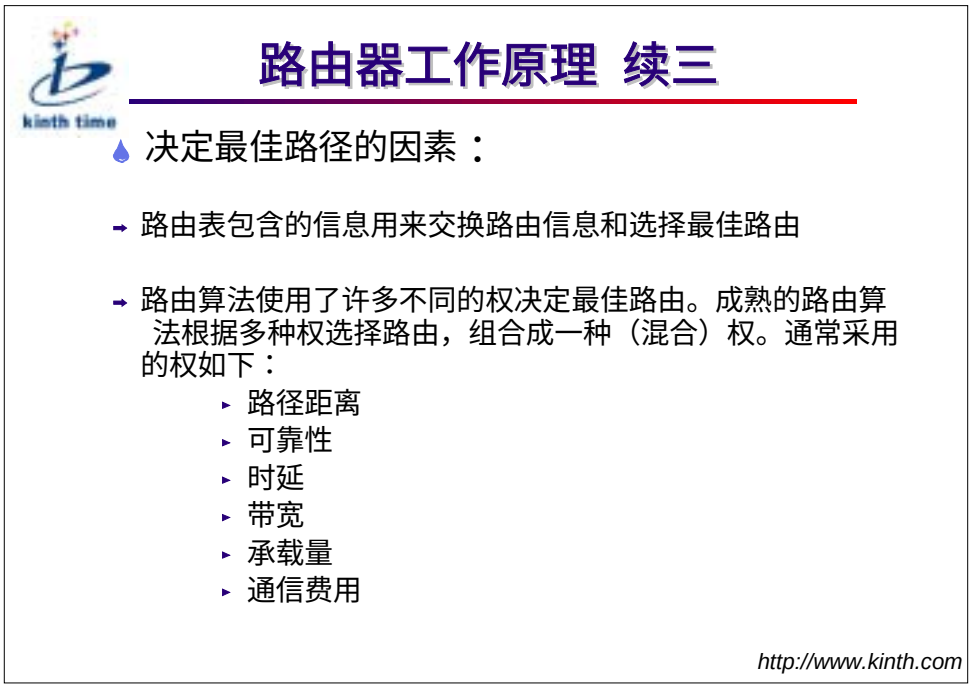
- 快速收敛性：

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；

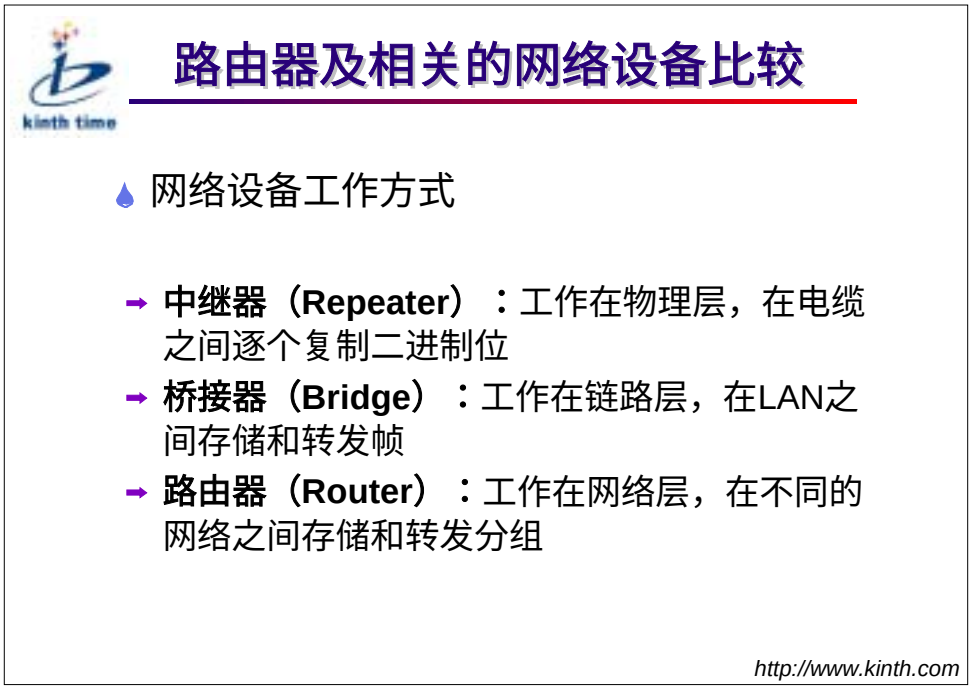
☞ 时延：指网络链路造成的网络延时；

☞ 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

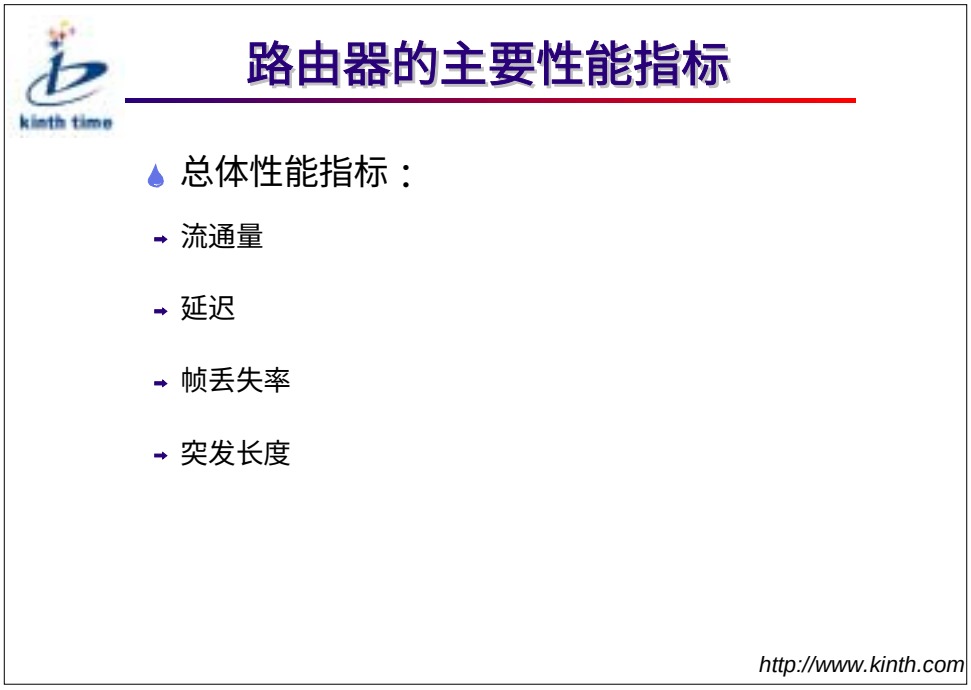


Hubs（中继器）：对应 7 层模型的物理层，它的作用是放大电信号。主要用于连接具有相同物理层的 LAN。Hubs 还将以太网的总线结构变成星状结构。

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。

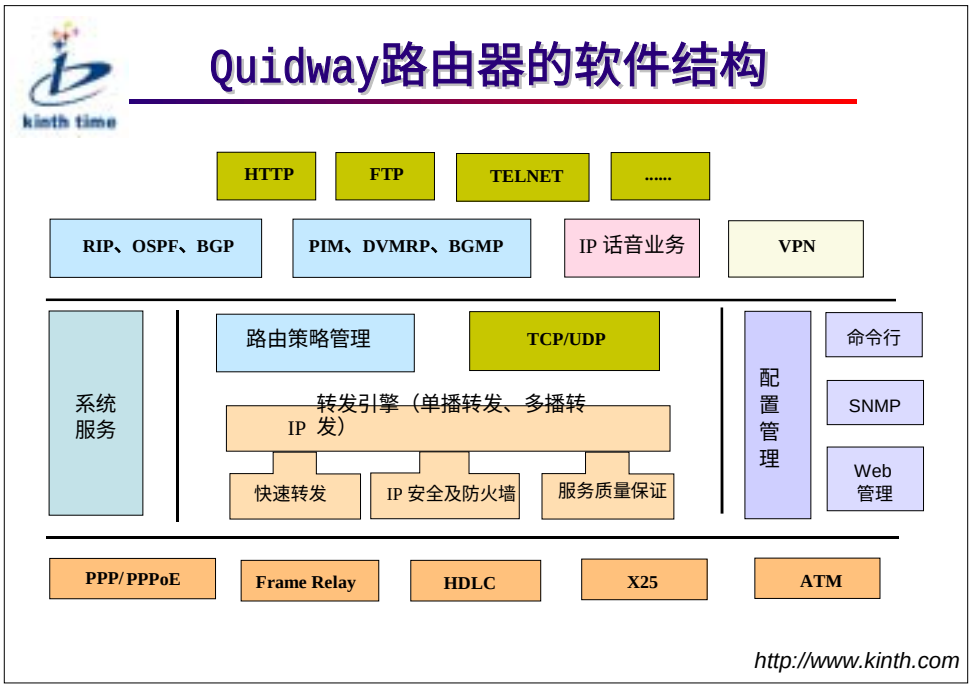
☞ 帧丢失率

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。

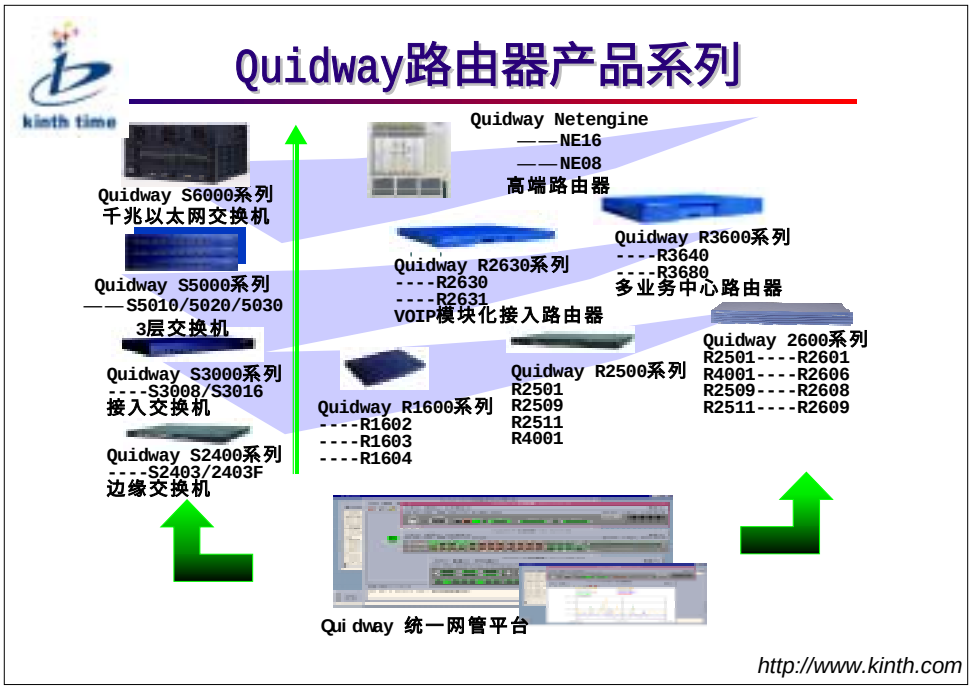
.2.6　Quidway 路由器的软件结构 *



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。

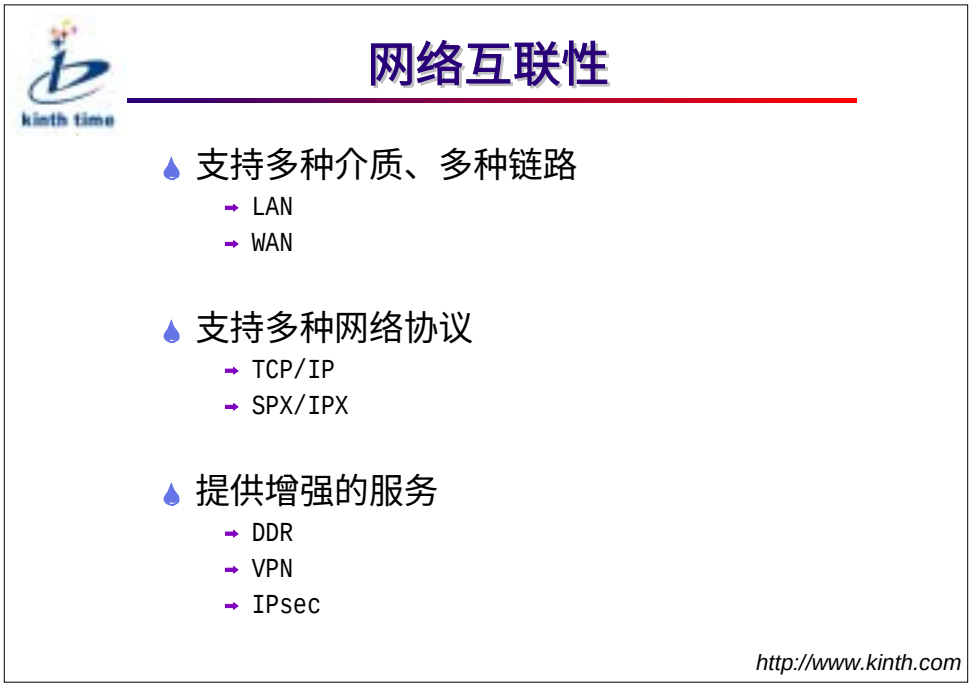
中端路由器 Quidway 2630/2631/3680/3640 适合于有分支机构的中小型企业，一般位于路由中心位置上，互连企业网的各个分支机构，并作为企业网的出口，上行接入高端路由器中。中端路由器边缘可以接入 1600、2500、4001 等低端路由器。对于中小型企业来说，中端路由器是其网络中心。

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。

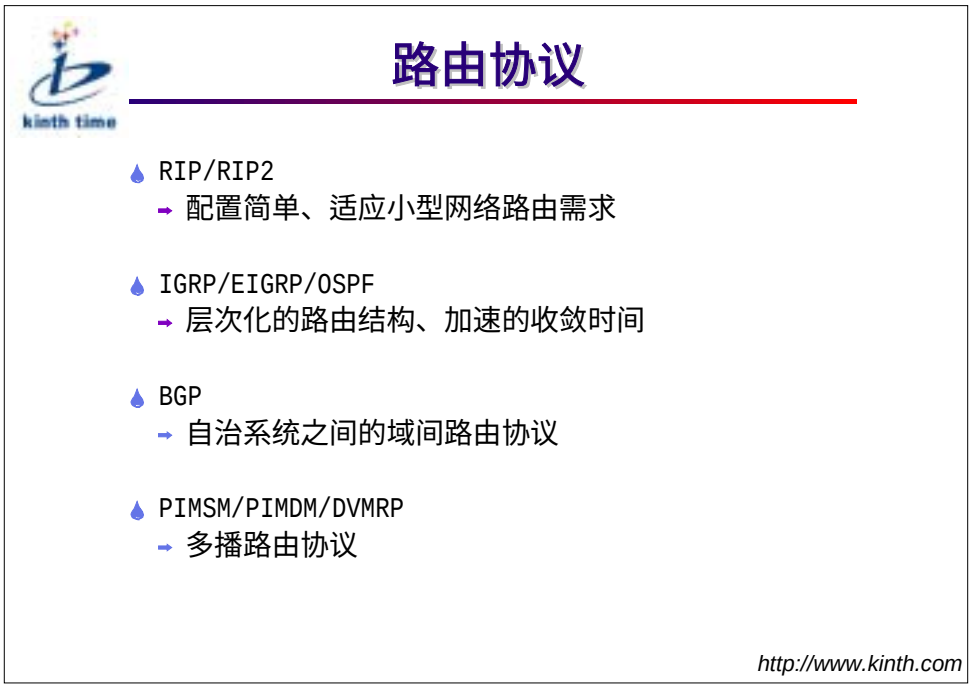
- NAT —— Network　Address Translation（地址转换）

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。

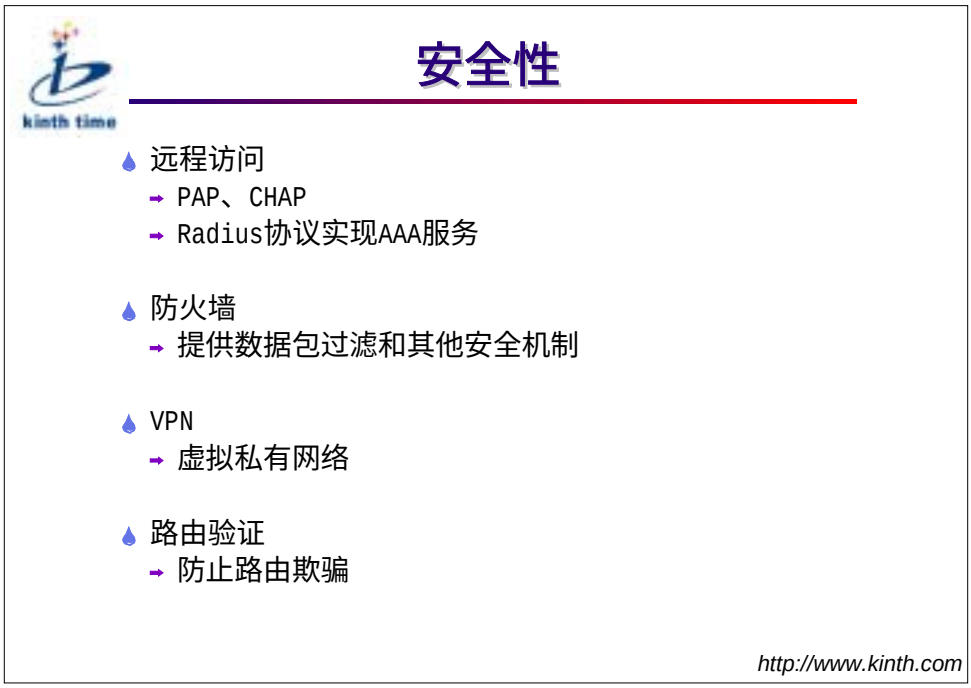
IGRP 是一个基于 D-V（Distance Vector）算法的路由协议，运行 IGRP 的路由器通过和相邻路由器之间相互交换路由信息来建立路由表。IGRP 是从 RIP 基础之上发展而来的。EIGRP 在其基础上进行了大量的改进，具有链路状态协议的某些特征，有快速的路由收敛能力。

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。

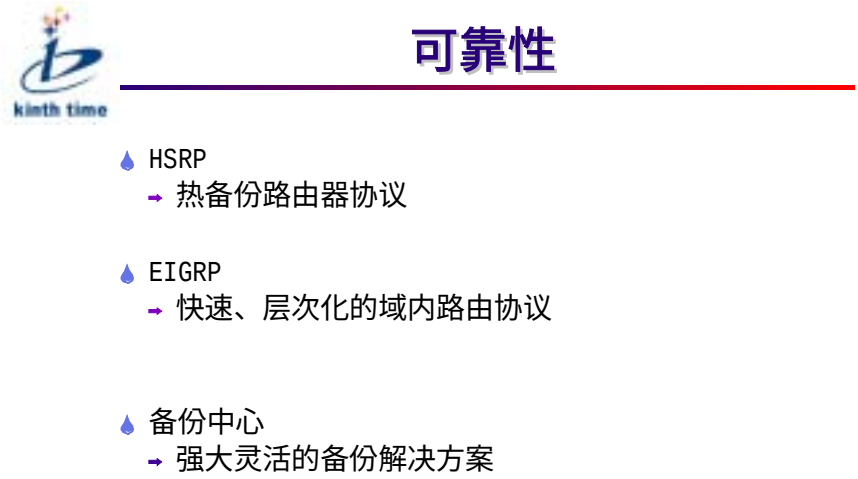
AAA 是验证、授权和记账（Authentication, Authorization, and Accounting）的简称。它是运行于 NAS 上的客户端程序。它提供了一个用来对验证、授权和记账这三种安全功能进行配置的一致的框架。AAA 的实现可采用 RADIUS 协议。RADIUS 是 Remote Authentication Dial In User Service 的简称，用来管理使用串口和调制解调器的大量分散用户。

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



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。

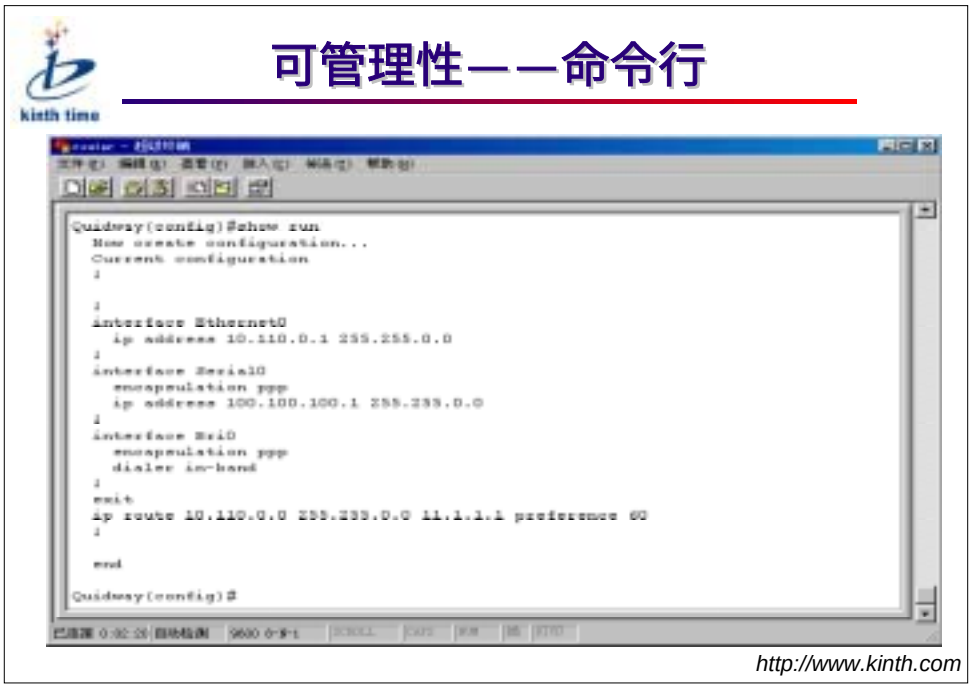
EasyConfig 是图形化易用的配置管理工具，运行在 Windows95/98 或 Windows NT 操作系统的 PC 机上，可以方便地绘制组网图、按照模块配置模块化路由器、进行路由器的配置、打开/保存图形化配置文件、保存普通配置文件、传送路由器配置文件到本地或远程路由器。

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。

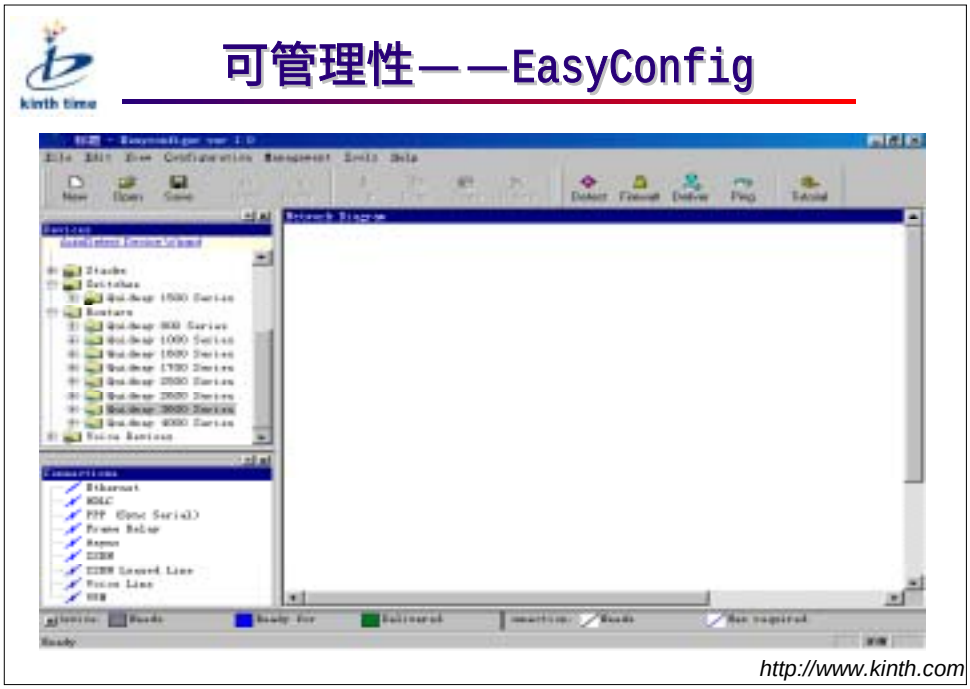
RadiumNMS 数据通信综合网管系统是华为公司自主开发的、管理华为的各类数据通信设备的统一的网络管理系统，它实现在统一用户界面下完成对华为公司的系列交换机、接入服务器、路由器、宽带接入设备、LAN Switch 等的集成管理，功能包括拓扑管理、配置管理、性能管理、故障管理、日志管理、安全管理、系统管理等。

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。

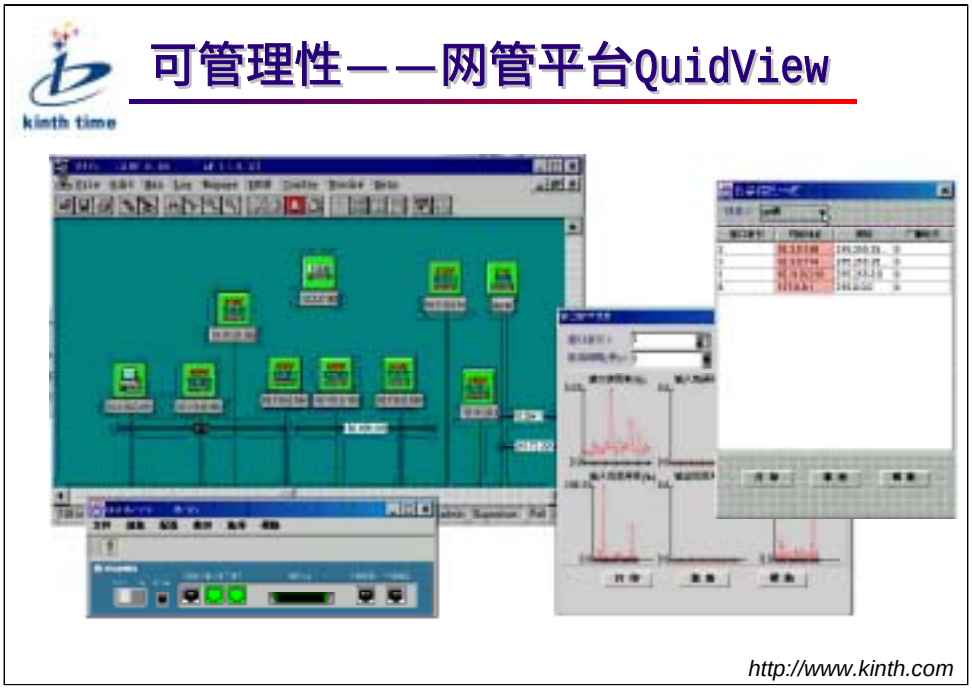
可管理性 —— EasyConfig *



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。

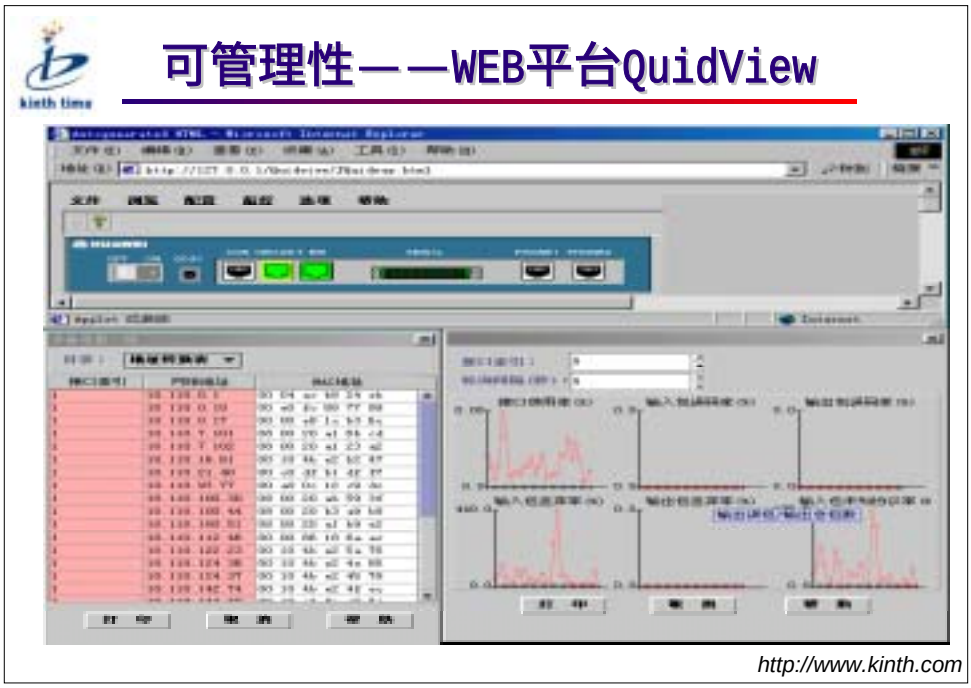
EasyConfig 是图形化易用的配置管理工具，运行在 Windows95/98 或 Windows NT 操作系统的 PC 机上，它的主要功能包括绘制组网图、按照模块配置模块化路由器、进行路由器的配置、打开/保存图形化配置文件、保存普通配置文件、传送路由器配置文件到本地或远程路由器。

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 *

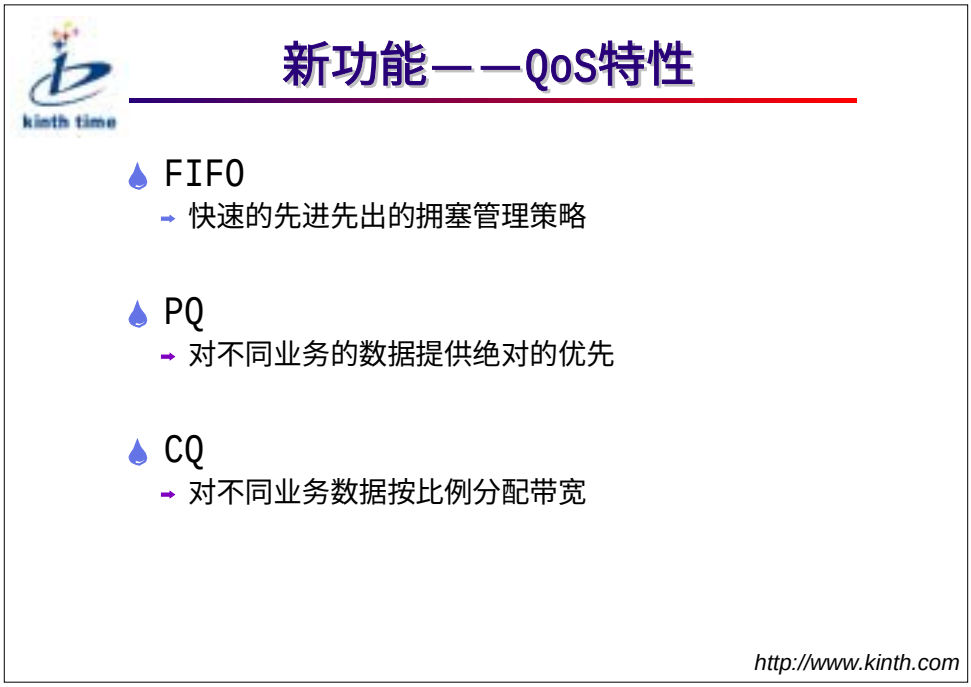
RadiumNMS 数据通信综合网管系统是华为公司自主开发的、管理华为的各类数据通信设备的统一的网络管理系统，它实现在统一用户界面下完成对华为公司的 ATM 系列交换机、A8010 接入服务器、Quidway 系列路由器、MUSA 系列宽带接入设备、Quidway 以太网交换机等的集成管理，功能包括拓扑管理、配置管理、性能管理、故障管理、日志管理、安全管理、系统管理等。

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。

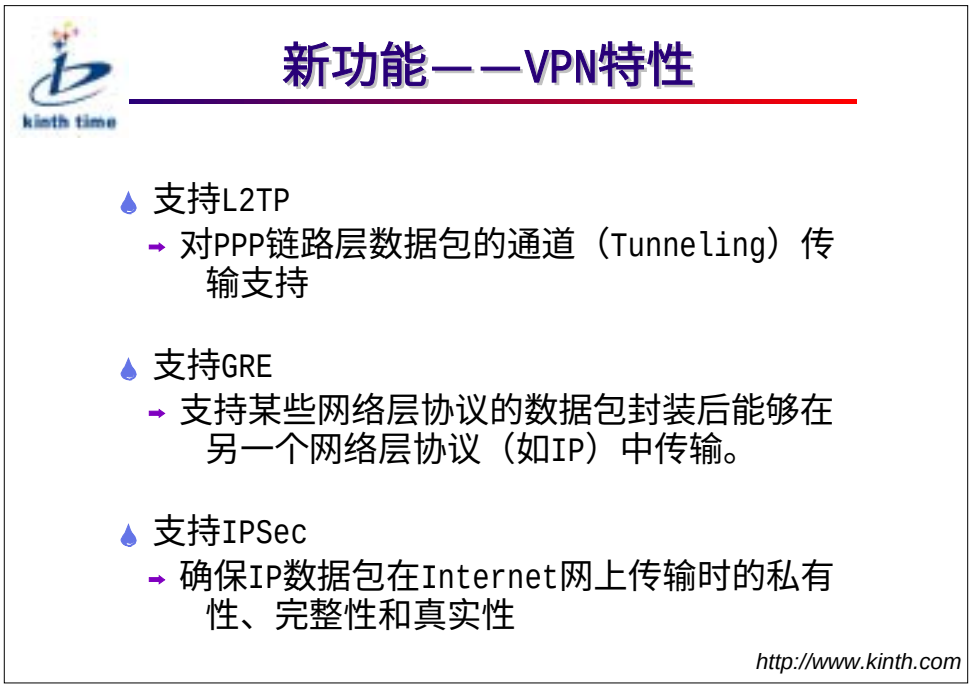
优先队列（Priority Queueing, PQ）

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。

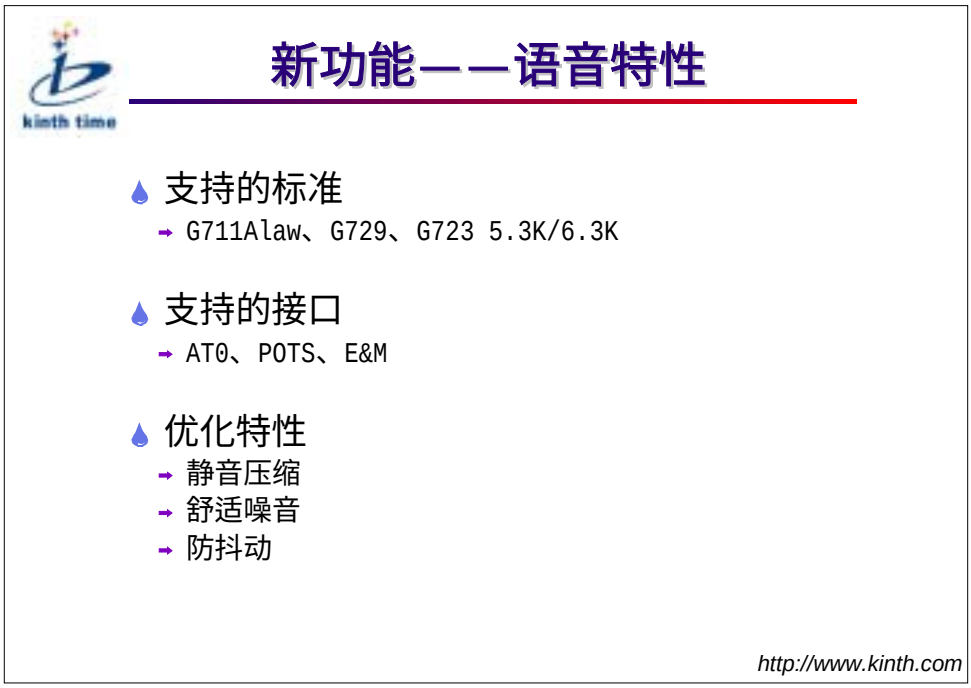
IPSec：

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。

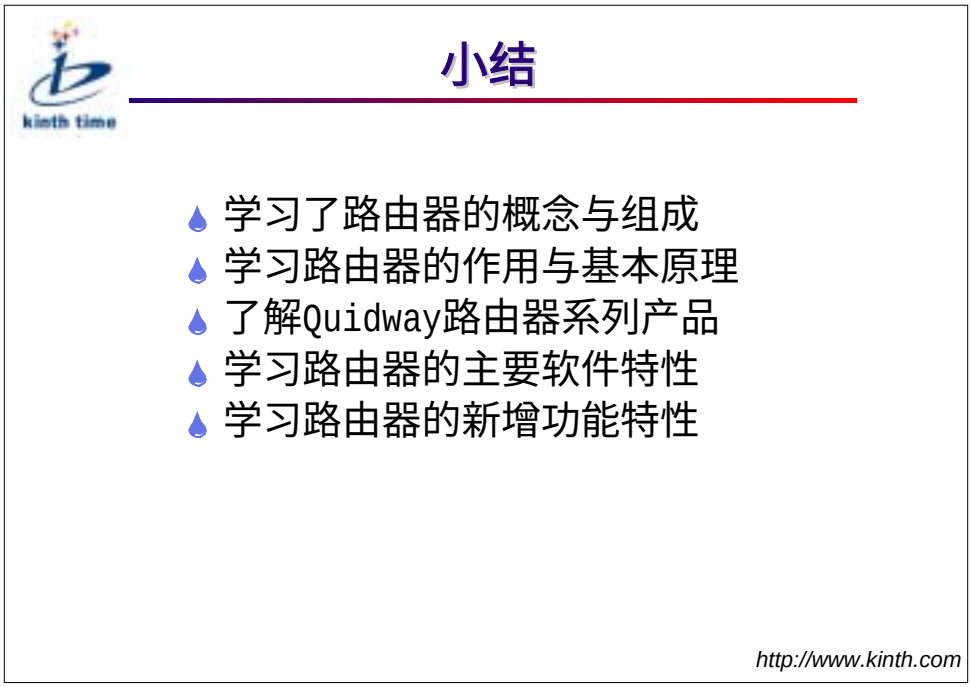
- 抖动

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。

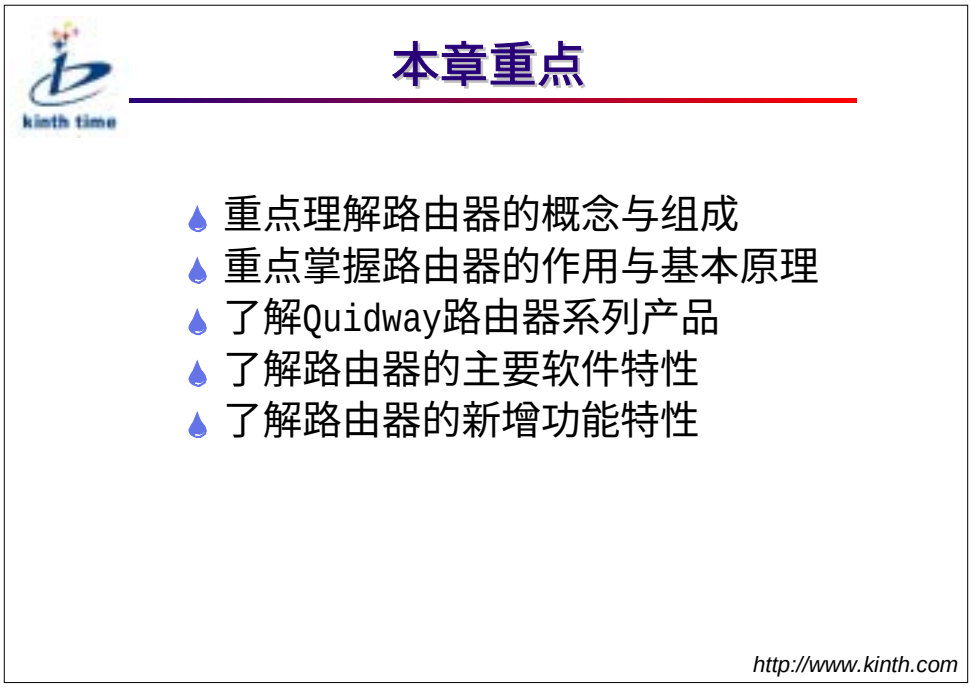
- 话音质量

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

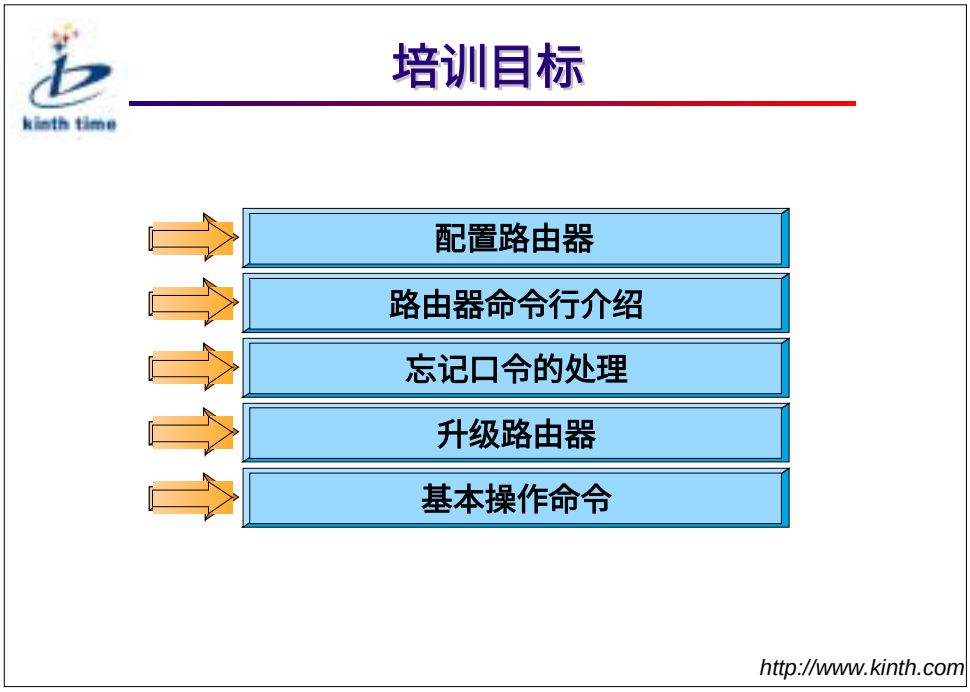

小结
学习了路由器的概念与组成
学习路由器的作用与基本原理
了解Quidway路由器系列产品
学习路由器的主要软件特性
学习路由器的新增功能特性
http://www.kinth.com

.6 本章重点


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

第六章 路由器配置简介

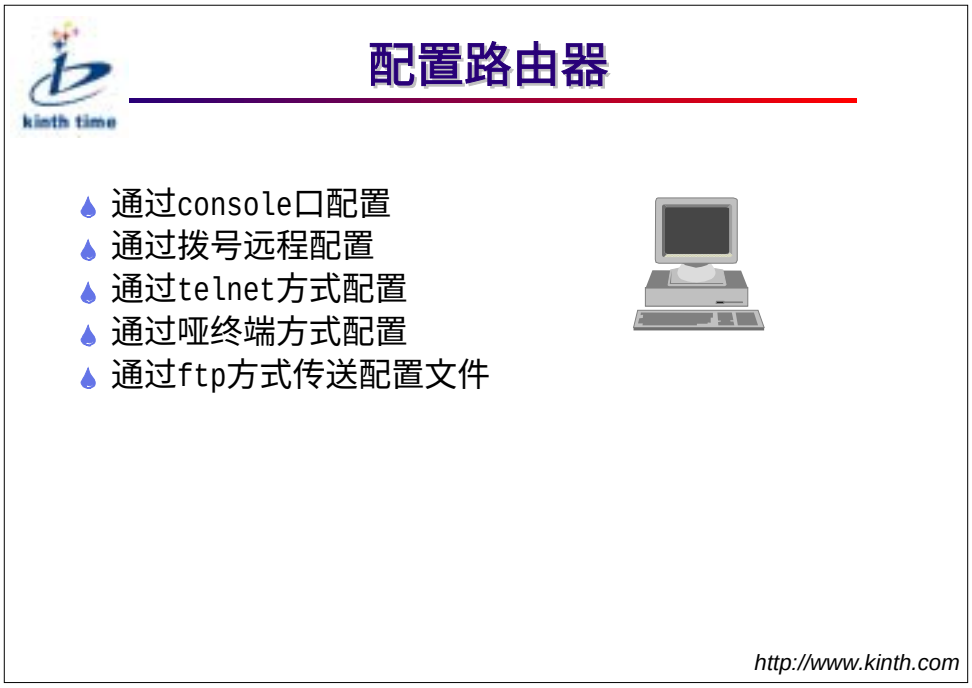
.1 培训目标



本章讨论 Quidway 路由器的配置与升级。本章是后续课程的基础，路由器的各种功能的实现，必须通过对路由器的配置来实现，熟悉路由器的配置方式，根据不同的实际情况采用不同的配置模式，可以大大的提高工作效率，增加对路由器的操作能力。

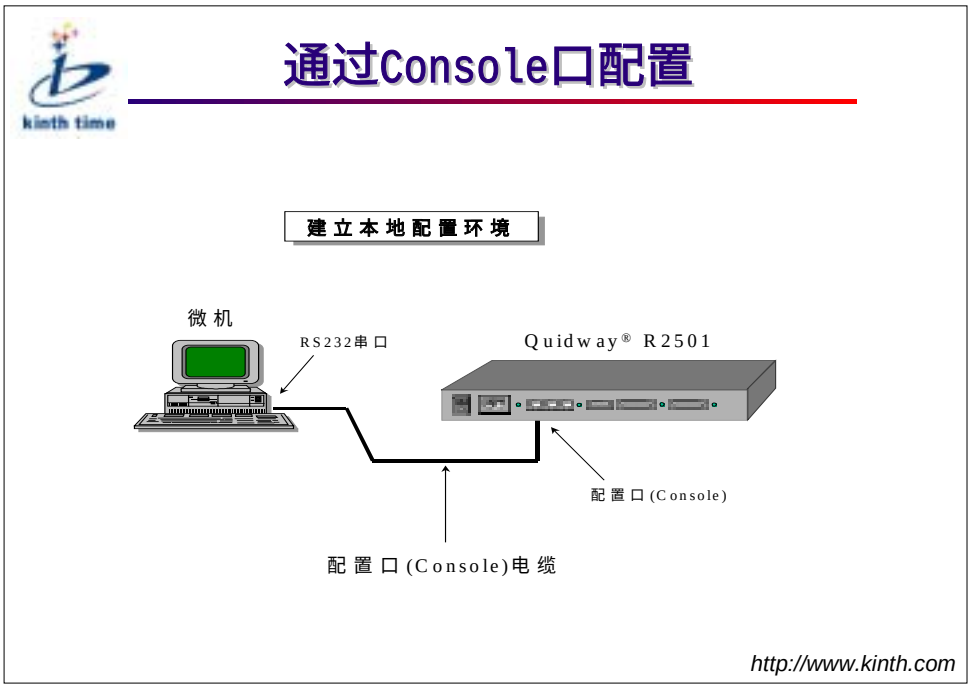
同样，路由器功能的实现很大一部分依赖于路由器的软件，许多新功能的应用是通过软件升级来实现的。因此，掌握路由器升级的方法，有助于您利用路由器软件的新特性来提高网络的性能。

.2 配置路由器



在 Quidway 系列路由器 VRP1.2 版及其后续版本中，可以通过四种方法来配置 Quidway 路由器：Console 终端配置模式、AUX 口远程配置模式、远程 Telnet 配置模式、FTP 下载配置文件模式。而 VRP1.2 版以前的版本中，只能通过前三种模式对路由器进行配置。

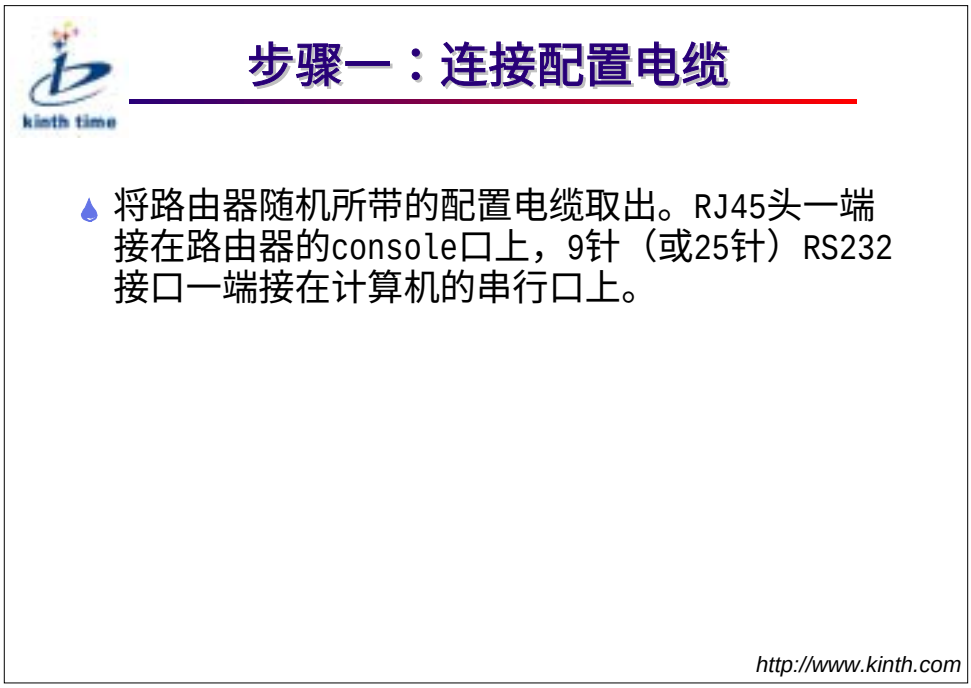
.2.1　通过 Console 配置路由器



在路由器的各种配置模式中，通过 Console 口配置路由器是最常用的一种配置模式，也是最基本的配置模式。

由于 Telnet 配置模式、FTP 配置模式都需要预先对路由器进行相应的配置才能生效，而通过 AUX 口配置模式需要连接 Modem 。所以，当第一次对路由器进行配置时，通过 Console 口配置就是必然的选择。只有先通过 Console 口对路由器进行配置，才能使能其他的配置模式。另外，由于某些原因造成其他几种配置模式不能对路由器进行配置。这样，使用 Console 口对路由器进行配置就成了唯一的选择了。

电缆的连接

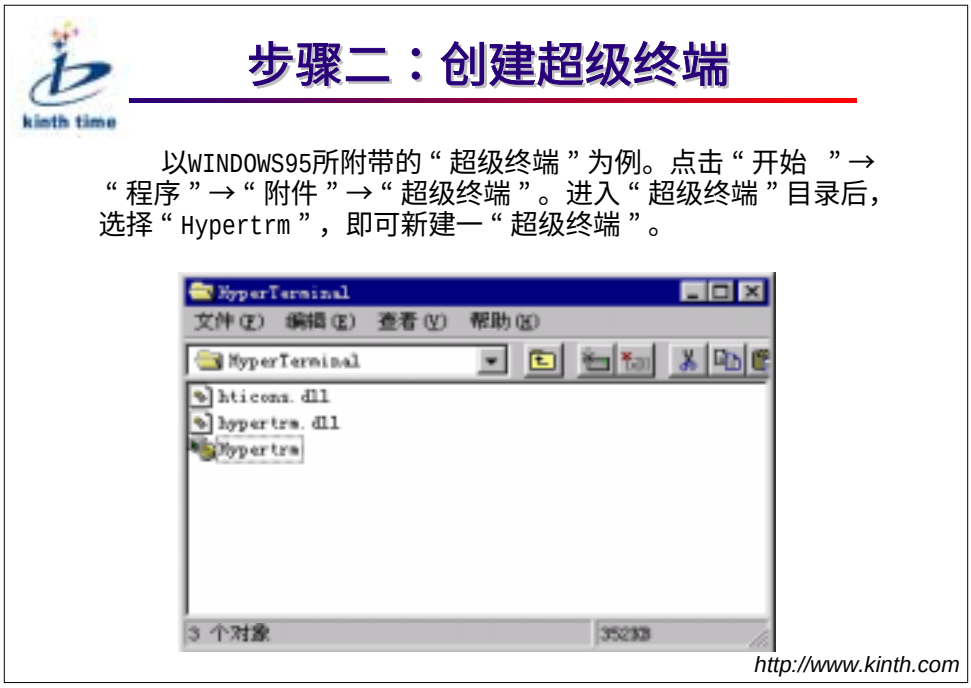


通过 Console 口对路由器进行配置的第一步是建立路由器与终端（通常为计算机）的物理连接。

请您从路由器的包装箱中取出标有“配置电缆”一根墨绿色电缆，它的一端为 RJ45 头，应插入到路由器的 Console 口中；另一端为一个 9 针的串口接头和一个 25 针的串口接头，根据您所用终端的串口的物理特性，您可将合适的接头接到终端的串口上。

注意：应仔细区分“配置电缆”和“备份电缆”。“配置电缆”的串口接头为孔状，而“备份电缆”的串口接头为针状。

创建超级终端



如果您是使用操作系统为 Windows95/Windows98/Windows NT4.0/Windows 2000 的计算机来配置路由器，则通过 Console 口对路由器进行配置的第二步是创建超级终端。

在所有的工作之前，您应确定您的计算机中已经安装了“超级终端”，否则，您应在操作系统中添加“超级终端”。

现在，您就应该创建一个用于配置路由器的“超级终端”了。先运行“HyperTerminal”中的“Hypertrm”文件。

创建超级终端（续1）

第二步：您可以为您创建的“超级终端”取一个好听的名字。如：Router、Mywork 等；同时，还请您为它选择一个漂亮的图标，它们都是根据您的意愿来决定的，对路由器的配置没有影响。

创建超级终端（续2）

第三步：请您选择使用您的计算机的哪个串口与路由器相连。这里的串口是您连接 Console 电缆的接口，它的串口号是固定的，您应确定您的选择是正确的。否则，您在“超级终端”中将看不到任何内容。

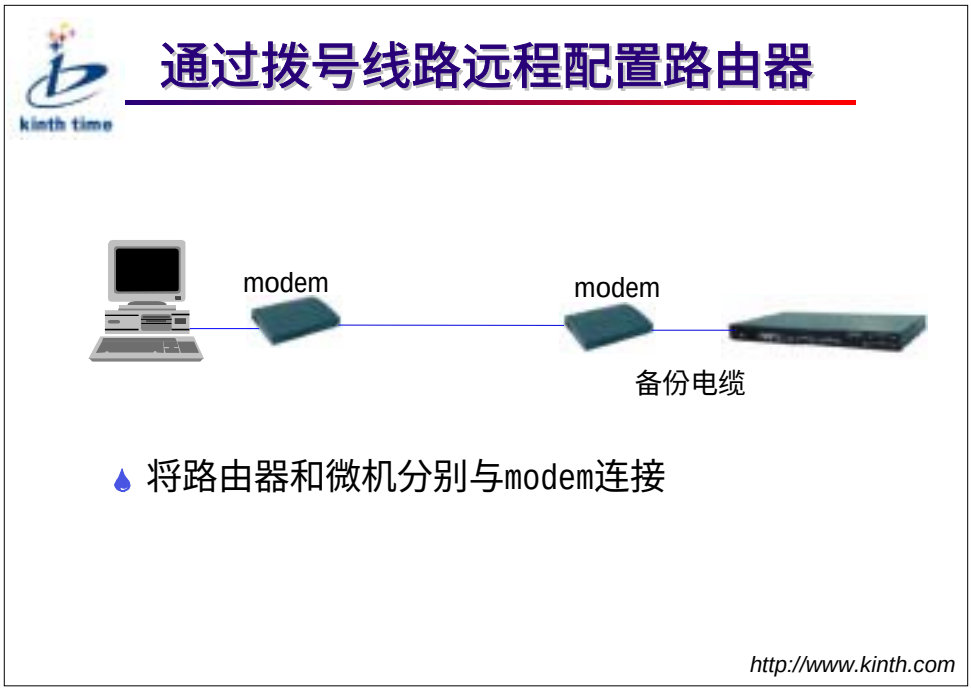
创建超级终端（续3）

第四步：选择串口的属性。为了顺利的配置路由器，您应正确的配置您的计算机的串口的属性，否则，您会在“超级终端”中看不到任何内容，也就无法对路由器进行配置。具体参数为：

- 速率 9600
- 数据位 8 位
- 奇偶校验无
- 停止位 1
- 流控制为“没有”或“硬件”

现在，您已经完成了“超级终端”的创建，系统将自动进入您创建的“超级终端”。启动路由器，看“超级终端”中是否出现了提示信息。若有，则说明一切正常；否则，您只得检查一下您的设置，重新设置。

.2.2　通过拨号线路远程配置路由器

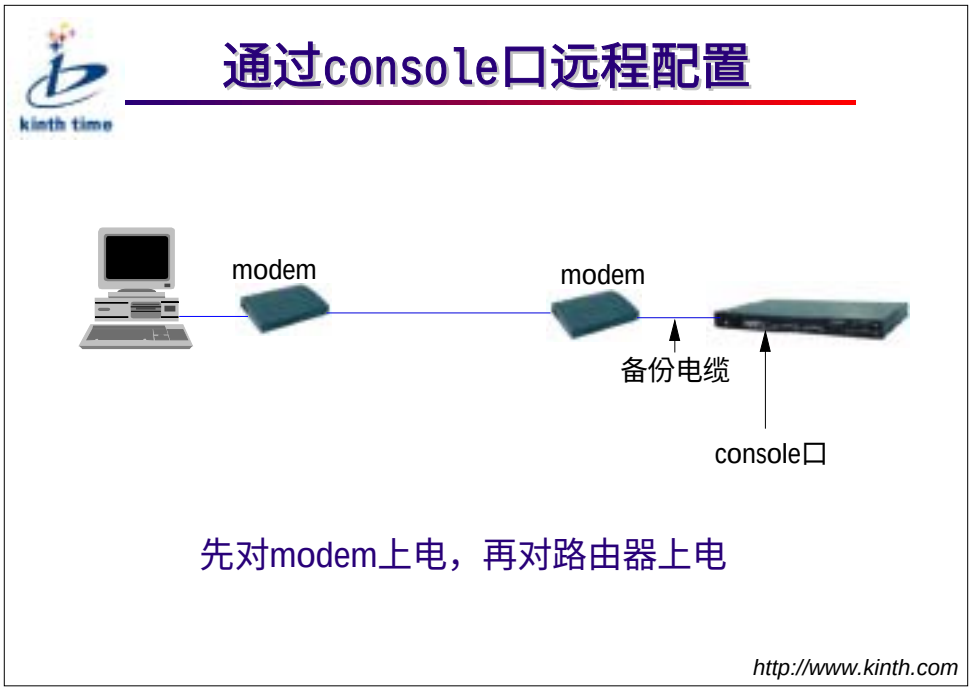


当您需要对远端的路由器进行配置时，可以通过拨号线路连接到需要配置的路由器上。

首先，在配置终端的空闲的串口上连接一模拟 Modem，确保能与其它计算机建立拨号连接。

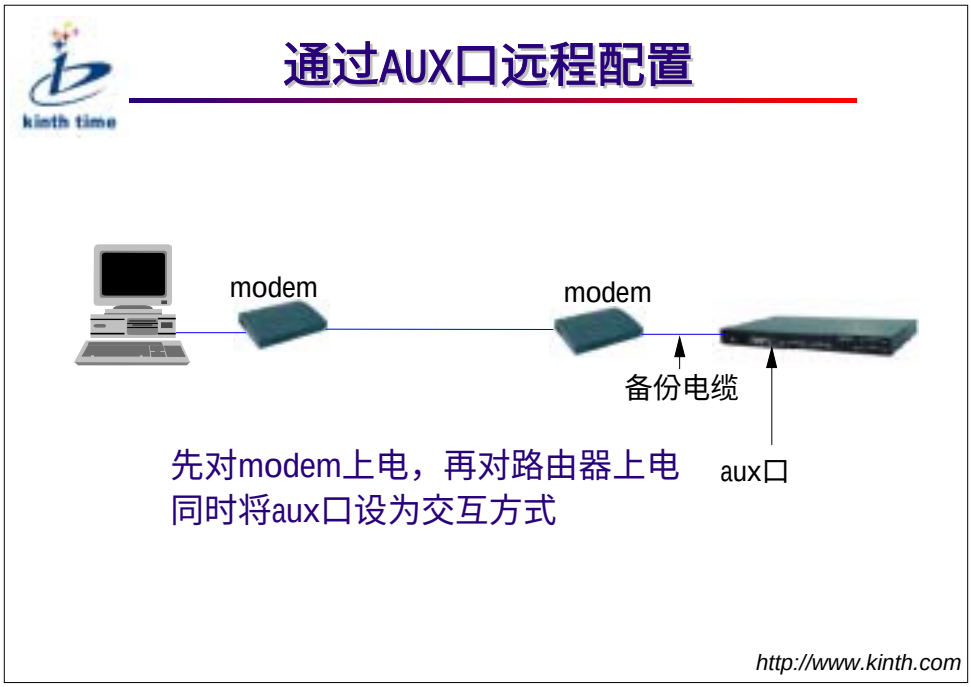
然后，通知对方工程师，将一模拟 Modem 通过“备份电缆”连接到路由器的 Console 口或 AUX 口上。

通过 Console 口远程配置路由器



如果是接在 Console 上，则在路由器上不需作任何配置；只需要通知对方的网络管理员先将 Modem 上电，再对路由器上电。

通过 AUX 口远程配置路由器



如果是接在 AUX 口上，则需要在路由器上配置 AUX 口的模式为交互方式；并通知通知对方的网络管理员先将 Modem 上电，在对路由器上电。

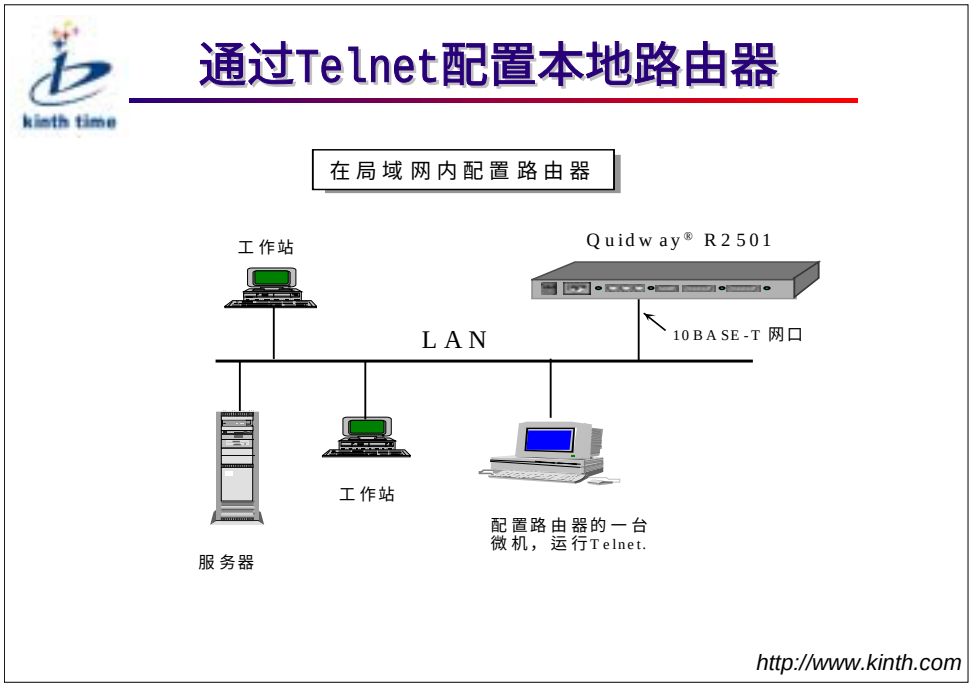
将 AUX 口设置为交互方式：

```
Quidway(config-if-Serial2)# enc ppp
Quidway(config-if-Serial2)# asy mode interactive
```

通过 AUX 口配置路由器（续）

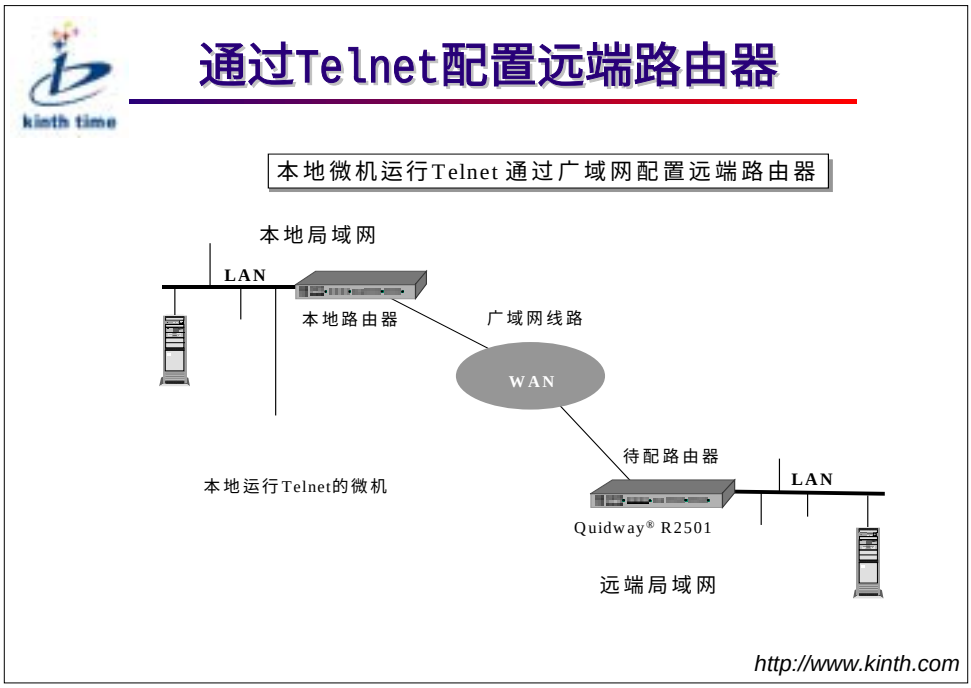
设置好路由器的相关属性，并建立好连接后，就可以通过“超级终端”建立与远端路由器的拨号连接时，并对该路由器进行配置。

.2.3　通过 Telnet 配置同一局域网内的路由器



在本地微机上键入路由器以太网口 IP 地址，与路由器建立连接，然后出现命令行提示符（如 Quidway>），如果出现用户太多的提示，则请稍候再连。

.2.4　通过 Telnet 配置远端路由器



配置远端的路由器，除了前面所介绍的通过拨号线路建立连接外，还可以通过 Telnet 到对方的路由器上进行配置。然而，这有一个前提：即必须能与该路由器建立 Telnet 连接，并拥有合法的用户名和口令。然后，就可以像 Telnet 本地的路由器一样，通过在 Telnet 窗口中输入对端路由器的以太网口地址或广域网地址，登录到对方的路由器进行配置。

.2.5 通过哑终端配置路由器 *

哑终端功能是在一种交互方式下通过异步专线直接登录到路由器的配置接口，提供除 Console 口、Telnet 之外的另一种终端服务。他扩展了路由器的配置通道的选择，使得路由器的同异步口、备份口（AUX 口）、异步串口通过一些简单的设置后，均能对路由器进行配置。对各端口的设置如下：

对同异步口如下配置：

Quidway(config-if-serialx)# physical-layer asyncQuidway

(config-if-serialx)# async mode interactive

对 8/16 异步口如下配置：

Quidway(config-if-async x)# no modem

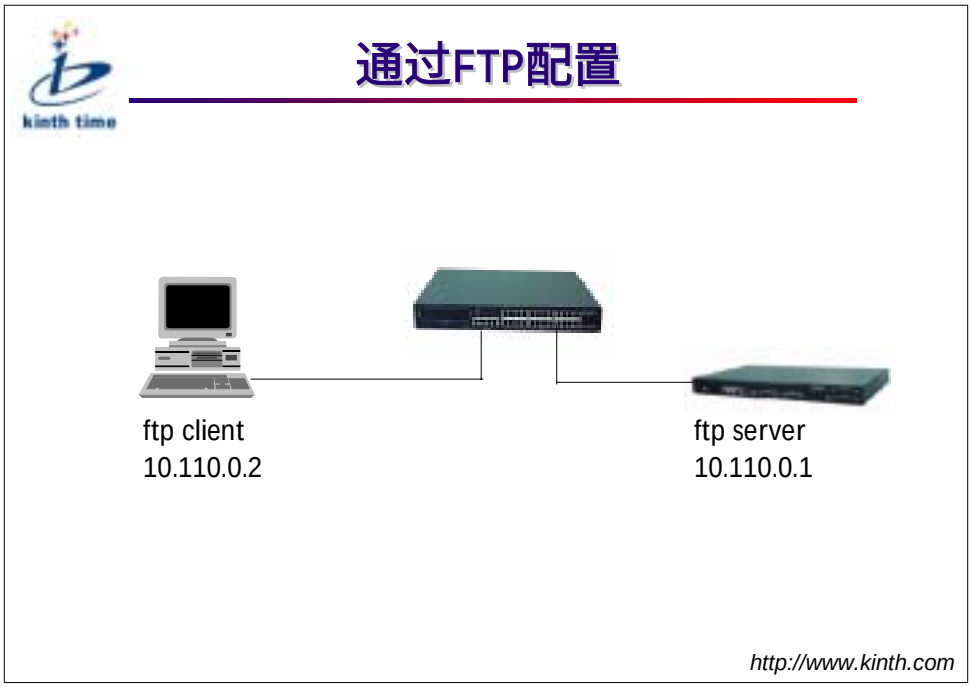
Quidway(config-if-async x)# async mode interactive

对 AUX 口如下配置：

Quidway(config-if-serial2)# no modem

Quidway(config-if-serial2)# async mode interactive

.2.6 通过 FTP 配置路由器 *



Quidway 系列路由器提供 FTP 服务器，该功能提供了另外一种更新配置文件或程序主体的途径。任何 FTP 客户均可连接到路由器上，在通过用户验证后，进行配置文件或程序主体的上传下载。

1. 在路由器上启动 FTP 服务器

（1）设置验证方式

如果在路由器中设置 aaa 验证，需作如下配置：

☞ 在全局配置模式下，键入 aaa-enable 。

☞ 在全局配置模式下，键入 aaa authentication login default local 。

☞ 在全局配置模式下，键入 aaa accounting optional。

如果您不需作 aaa 验证，则不需以上的配置。

（2）添加用户名、密码

在全局配置模式下，如键入 user ftp password 0 123 service-type ftp，表示用户名为 ftp，密码为 123。

（3）启动 FTP 服务器

在全局配置模式下，键入 ftp-server enable 。

经过以上操作，在路由器上已经启动了 FTP 服务器，并设置了用户；任何一个 FTP 客户端程序均可使用该用户名、密码登录 FTP 服务器。

2. 上传配置文件

（1）配置路由器以太网口地址，使运行 FTP 客户端程序的主机与路由器的网络相通。

（2）使用已经在路由器设置好的用户名、密码登录 FTP 服务器，以 Windows 98 所提供的 FTP 客户端程序为例：

☞ 在 DOS 提示符下，键入 FTP A.B.C.D（A.B.C.D 是路由器的以太网 IP 地址）。

☞ 在“username”提示下，键入用户名 ftp。

☞ 在“password”提示下，键入密码 123 ，验证通过后登录成功，显示 FTP 客户端提示符“ FTP > ”。

☞ 在提示符下键入 put。

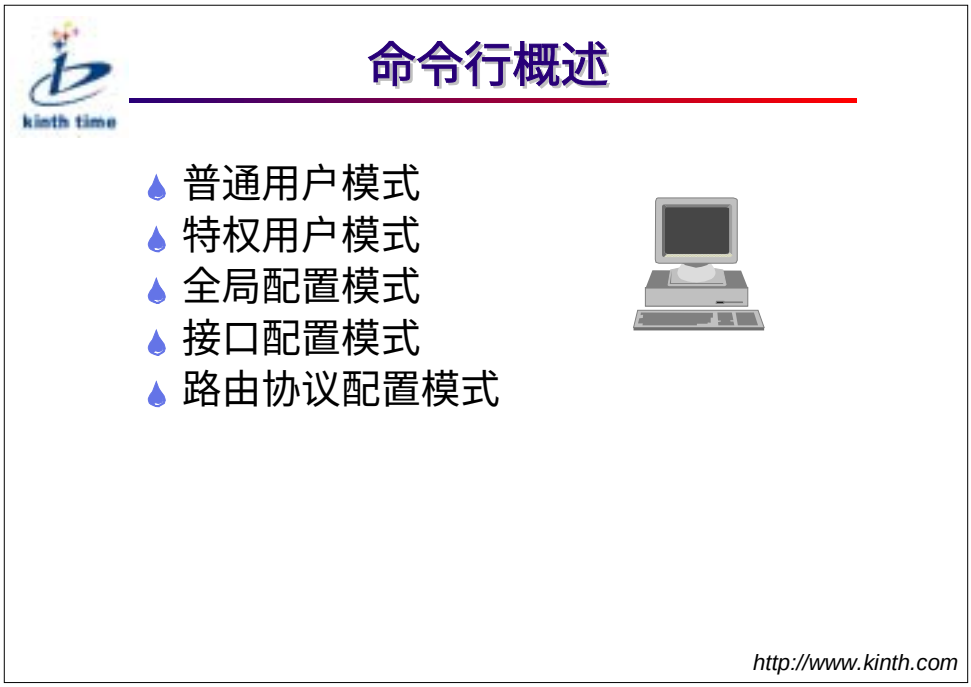
☞ 在“local file”提示下，键入您所要上传的配置文件的名称。

☞ 在“remote file”提示下，键入路由器端上传后所要保存的配置文件名称，该名称在上传操作之前必须在路由器端进行设置，缺省名称为 CONFIG。

☞ 上传文件结束后，重新显示“FTP >”的提示符，键入 dir ，显示路由器上的文件名称和大小，上传成功则配置文件大小与主机上的文件大小一致。

☞ 上传成功后，键入 quit 退出 FTP 客户端程序。

.3 路由器命令行介绍



Quidway 路由器的命令行分为两种用户模式：普通用户模式和特权用户模式。

☞ 普通用户模式：只能执行一些常用的状态查看命令；

☞ 特权用户模式：可以对路由器进行查看、配置和修改。

从命令本身的类型、属性来看，Quidway 路由器的命令配置分为如下三种模式：

☞ 全局配置模式：命令执行的效果和影响对路由器来说是全局性的；

☞ 接口配置模式：命令执行只对某个接口本身有意义；

☞ 路由协议配置模式： 动态路由协议的参数配置。

.3.1　进入路由器配置界面

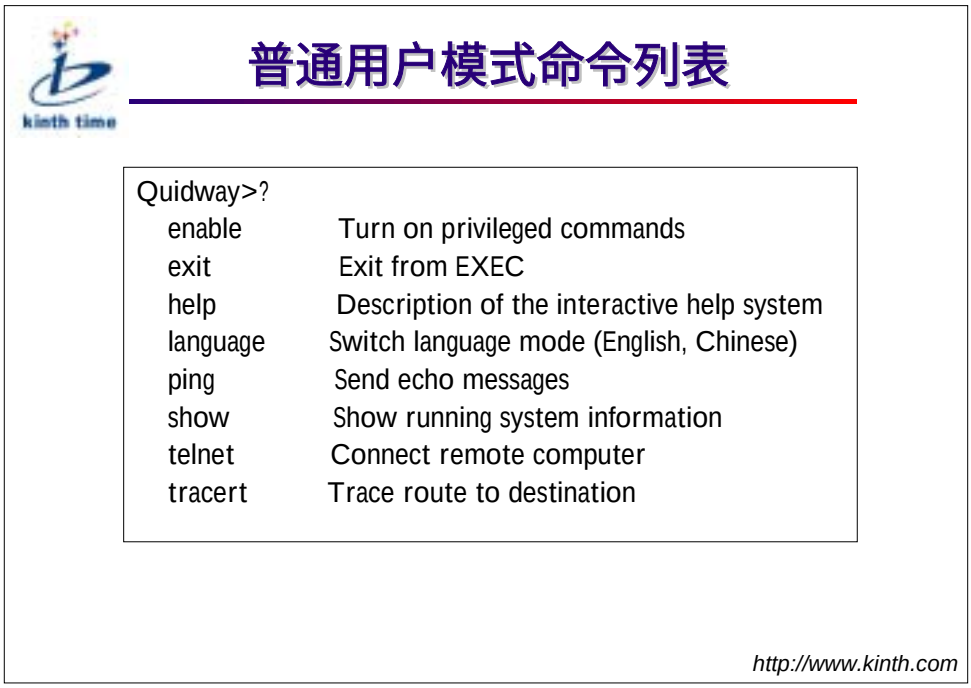
从超级终端中进入路由器配置界面，对路由器进行命令操作：

☞ 路由器启动完成后，根据提示敲入回车键，系统自动进入到普通用户模式界面，提示符为大于号（>）；

☞ 在普通用户命令行模式下，如果想进入到特权用户命令行界面，执行 Enable 命令，此时系统提示输入 Password ，如果是新买的路由器，系统默认没有特权用户口令，直接敲回车就可以进入到特权用户命令行模式，命令提示符由 > 变为 #。

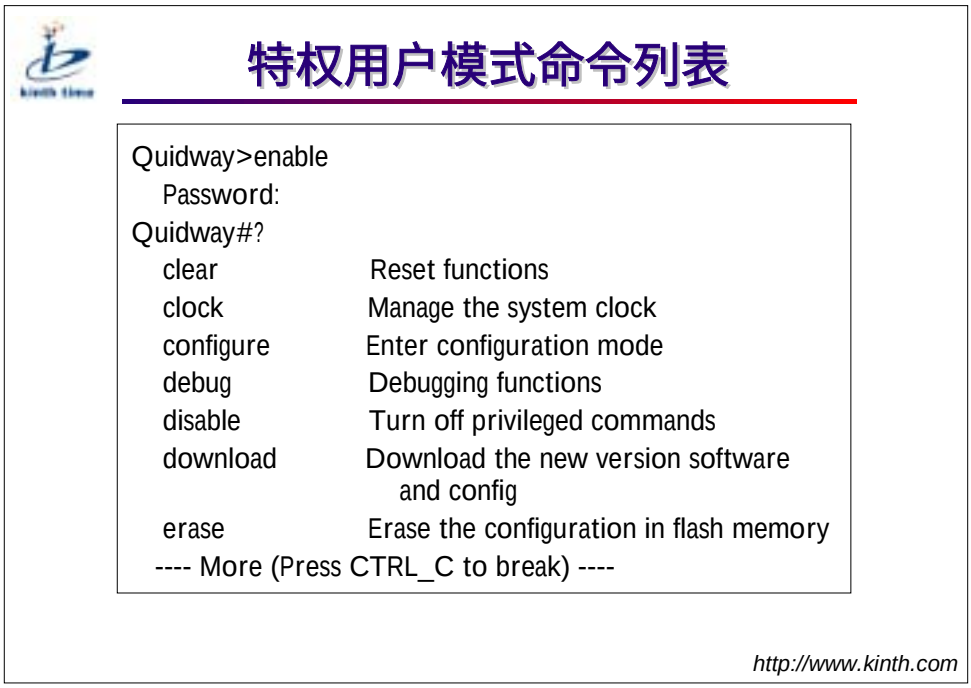
☞ 要退出特权命令模式，只用键入“disable”即可。

.3.2　普通用户模式



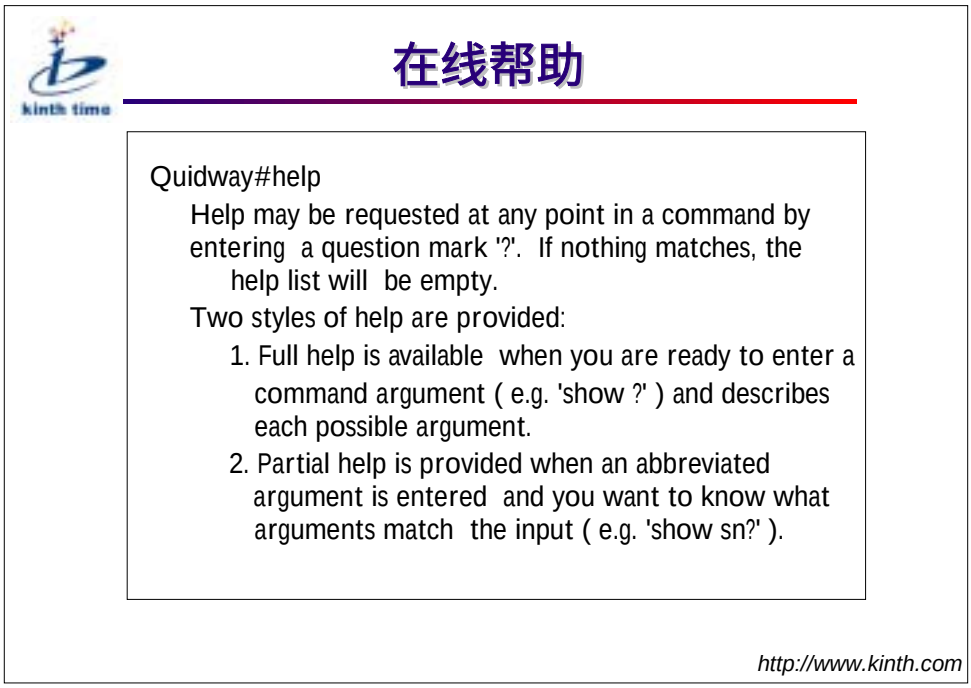
路由器启动后，将默认进入普通用户模式。在该模式中，只能对路由器进行一些基本的操作，如：查看接口信息、版本信息（但不能查看配置文件）；运行一些简单的测试程序，如：Ping、Tracert 等。
在普通用户模式下，不能对路由器进行任何配置，也不能对路由器进行任何管理。

.3.3　特权用户模式



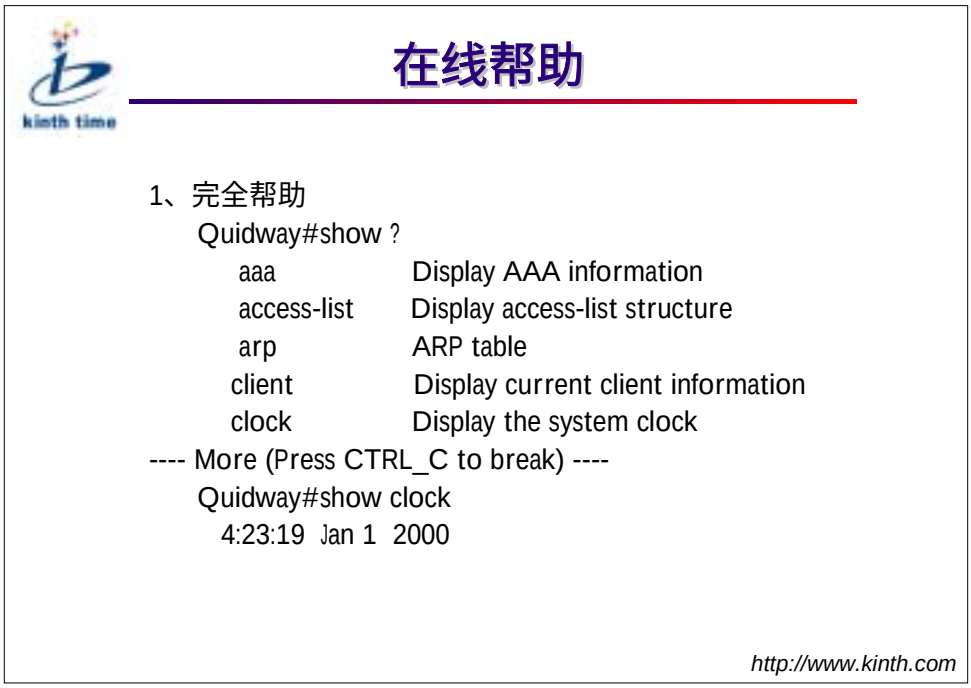
为了对路由器进行配置、管理，需要进入特权用户模式。进入特权用户模式时，需要输入特权用户口令。在特权用户模式下，能够完成对路由器的所有操作，包括对路由器的重新启动、删除所有的配置文件等操作。因此，在特权用户模式下时，所有的操作都要仔细考虑，以免带来不可预料的损失。同时，要保护好特权用户口令，不要让一些危险的人知道。

.3.4 在线帮助



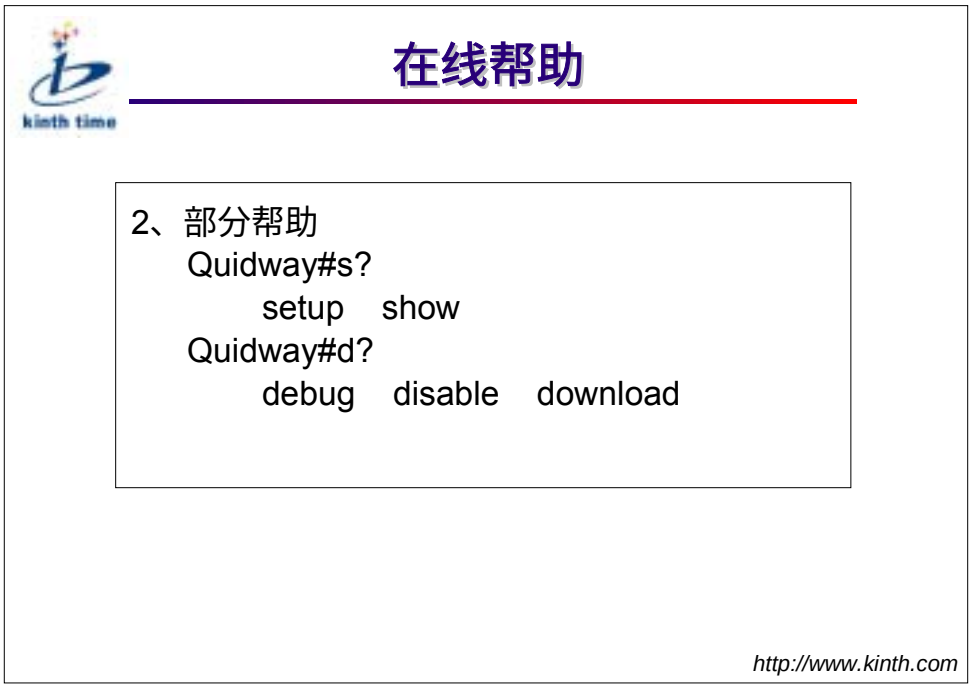
在任一的命令模式下，键入 **help** 获取有关帮助系统的简单描述。它向您介绍了如何在路由器中获取在线的帮助。Quidway 路由器提供两种帮助模式：完全帮助模式和部分帮助模式。

在线帮助：完全帮助



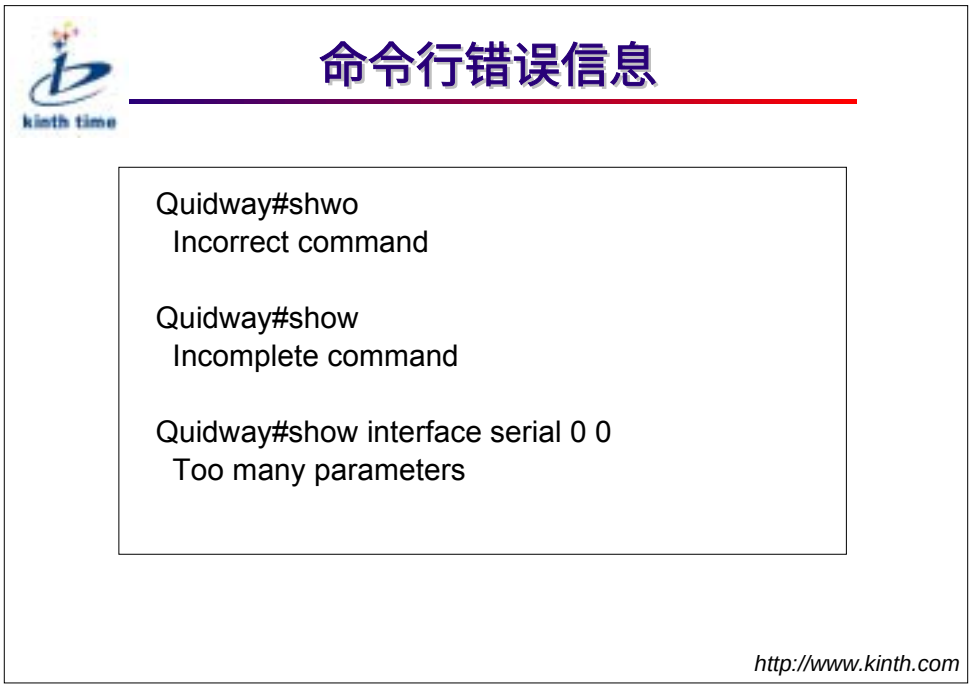
在任一命令模式下，键入“？”可以获取该命令模式下所有的命令及其简单描述。您还可以键入一命令，后接以空格分隔的“？”，如果该位置为关键字，则屏幕上会列出全部关键字及其简单描述。
如图所示，如果您想知道当前的系统时间，但您可能记不清楚用哪个命令，只知道该命令的第一个字为“**show**”。这时，您可以先键入“**show**”，再跟一空格，然后键入一“？”，屏幕上立即会列出能够在“**show**”后面使用的全部的关键字及其简单描述。根据提示，您可以发现使用“ **clock** ”关键字，可以得到当前的系统时间。

在线帮助：部分帮助



键入一字符串，其后紧接“？”，则会列出以该字符串开头的所有关键字。如图所示，在“s”后紧跟一“？”，则列出所有以“s”开头的关键字：“**setup**”、“**show**”。

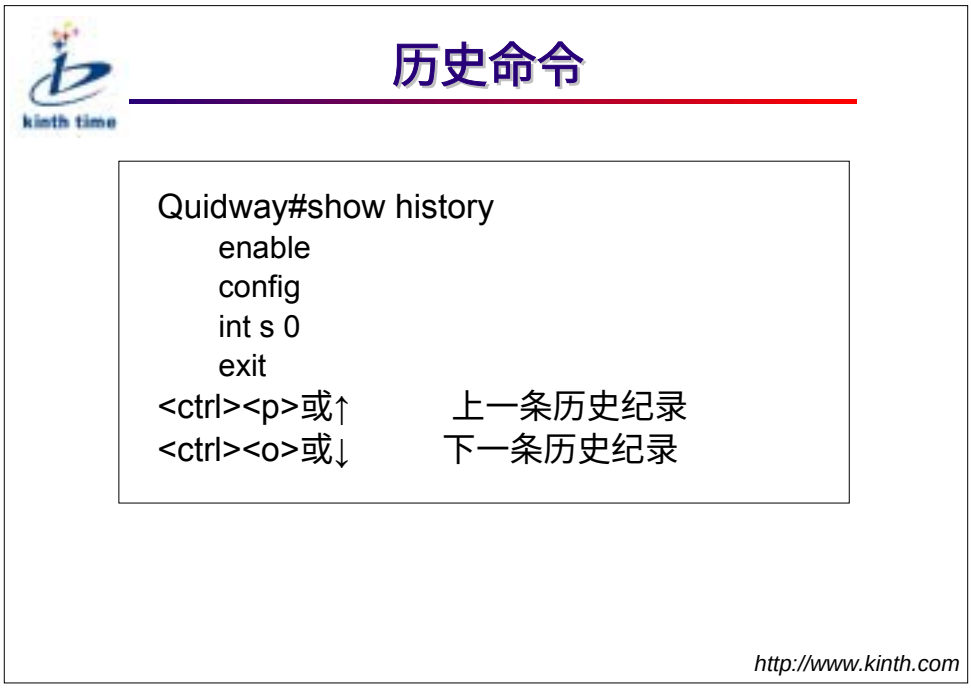
.3.5　命令行错误信息



所有用户键入的命令，如果通过了语法检查，则正确执行，否则向用户报告错误信息，常见的错误信息有三种：

- Incorrect command：未知的命令。错误原因包括：没有查到该命令、没有查到该关键字、参数类型错、参数值越界。
- Incomplete command：不完整的命令。错误的原因为输入的命令不完整。
- Too many parameters：参数输入太多。

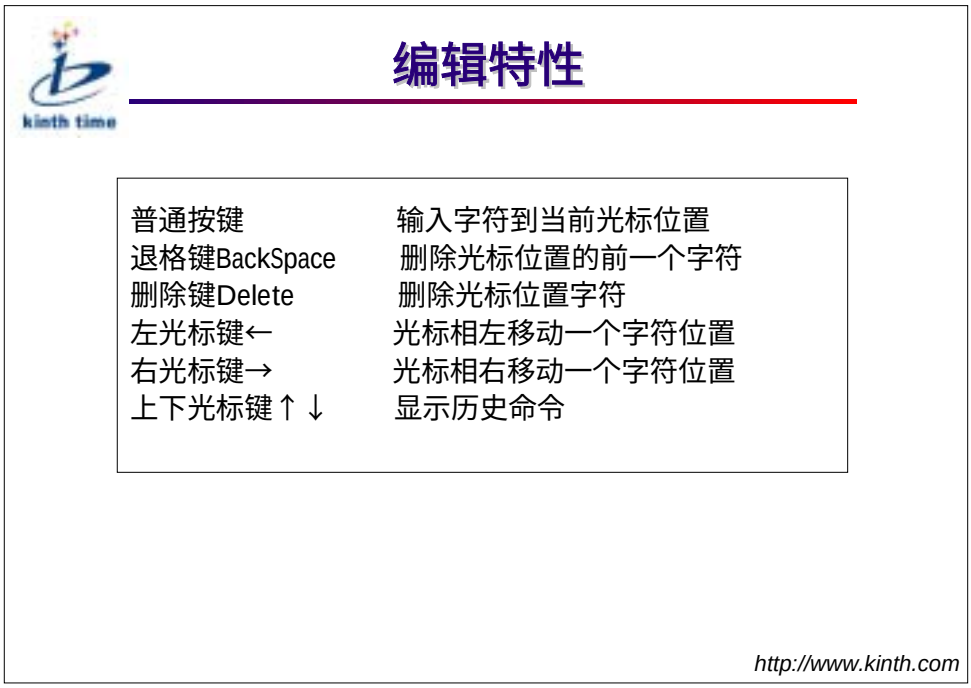
.3.6　历史命令



命令行接口提供类似 Doskey 功能，将用户键入的历史命令自动保存，用户可以随时调用命令行接口保存的历史命令，并重复执行。命令行接口为每个用户最多可以保存 10 条历史命令。

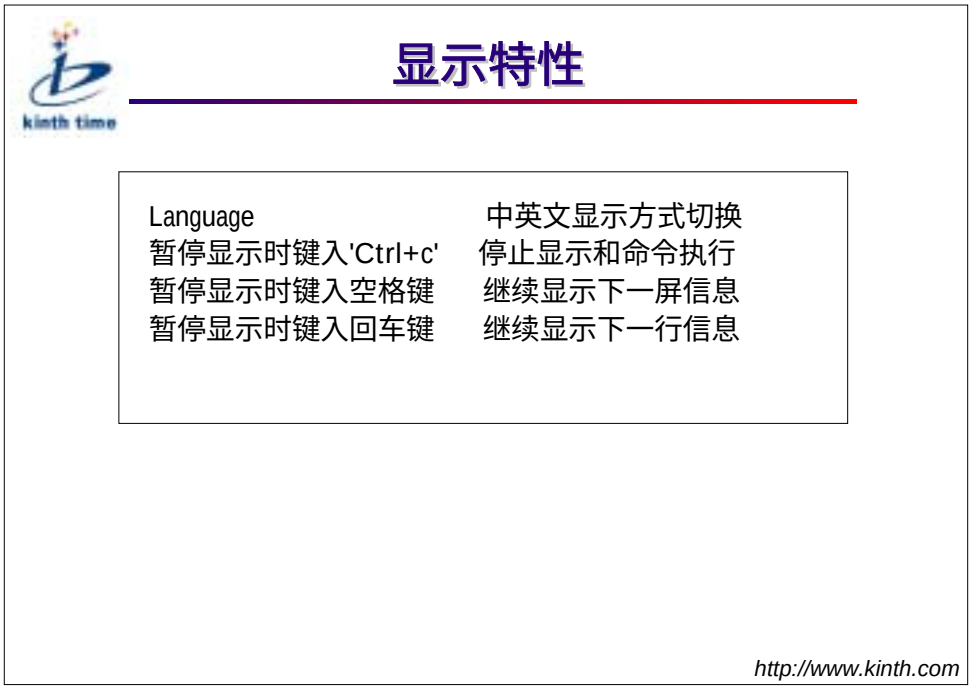
注：用光标键对历史命令进行访问，在 Window 3.x 的 Terminal 和 Telnet 下都是有效的，但对于 Win95 的超级终端，↑、↓光标键会无效，这是由于 Win95 的超级终端对这两个键作了不同解释所致，这时可以用组合键“Ctrl+o”和“Ctrl+p”来代替↑、↓光标键达到同样目的。

.3.7 编辑特性



命令行接口提供了基本的命令编辑功能，支持多行编辑，每条命令的最大长度为 256 个字符，若已经到达命令头或命令尾，则响铃告警。

.3.8 显示特性



命令行接口提供了如下的显示特性：

1、为方便用户，提示信息和帮助信息可以用中英文两种语言显示。

2、在一次显示信息超过一屏时，提供了暂停功能，这时用户可以有三种选择：

- 键入“Ctrl+c”，停止显示和命令执行。
- 键入“空格键”，继续显示下一屏信息。
- 键入“回车键”，继续显示下一行信息。

.4 忘记口令的处理

.4.1 忘记进入特权模式的口令的处理

为了防止别人知道特权用户口令，因此许多网络管理员将口令设得特别复杂。由于路由器配置完成后，很少去操作路由器。这样，过了一段时间后，因为网络的变化而需更改路由器的一些配置时，可能会因忘记特权用户口令而无法进行配置。

此时，只要您在路由器的旁边，您就可以按照以下步骤清除路由器的口令：

1、重新启动路由器（注意：由于您不能进入特权模式，因此只有通过对路由器先关机、再上电来重新启动路由器，一定要在网络空闲时操作，以免影响正常的工作）。

2、在启动时，屏幕上出现“Press Ctrl-B to enter Boot Menu ..”时键入“Ctrl+b”进入路由器的下载界面。

3、输入 Bootrom 口令（默认为空，直接回车即可）。

4、出现

“Boot Menu:

1: Download application program

2: Download Bootrom program

3: Modify Bootrom password

4: Exit the menu

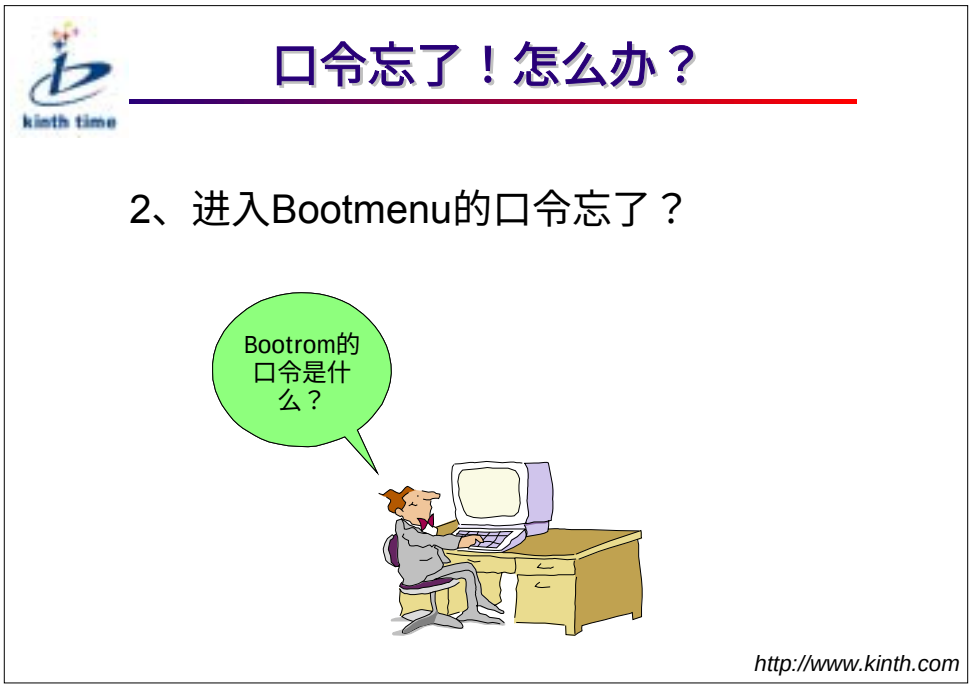
5: Reboot

Enter your choice(1-5):”

键入“Ctrl+p”，系统出现几个“#”后，将再次回到本界面。这次，选择“5：Reboot”。

5、路由器重新启动后，您将能直接进入特权用户模式。但路由器的特权用户口令并没有清除，您需要在配置模式下输入：“enable password XXX”来更改口令。注意：password 一定要写全，否则，将提示为错误的命令。

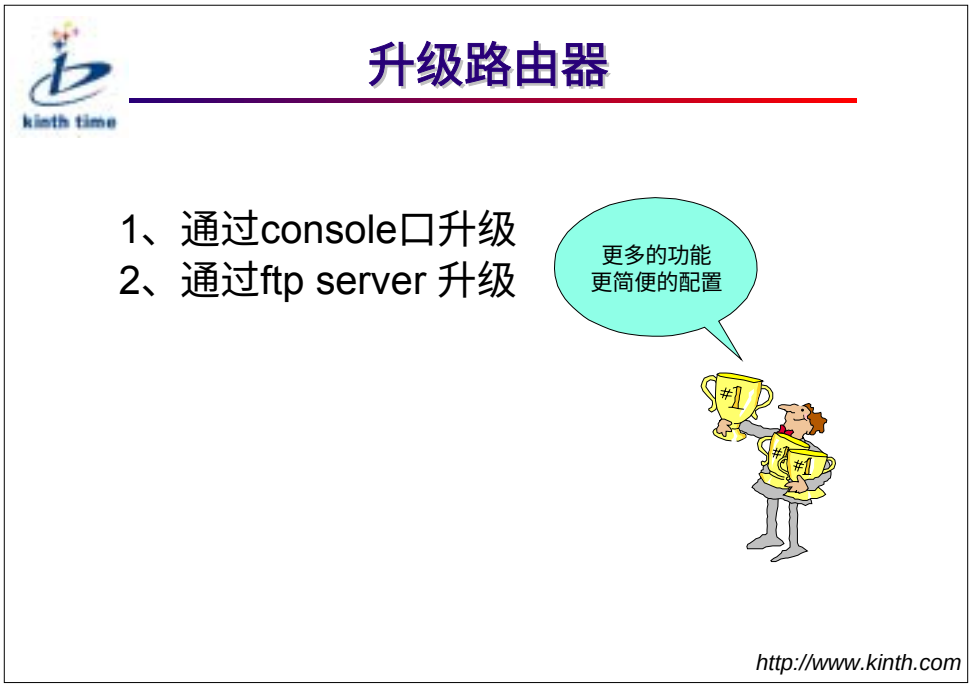
.4.2 忘记 Bootmenu 口令的处理



刚才提到，进入下载界面时要输入 Bootrom 口令。可是，如果以前设置了 Bootrom 口令，现在也不记得了，就只有通过输入 Bootrom 的通用口令进入下载界面。

Bootrom 的通用口令是：“ WhiteLily2970013 ”。

.5 升级路由器



随着 Quidway 路由器的新增功能的不断推出，路由器的升级时每一个网络管理员所必须掌握的技术。通过软件的升级，能提高网络的性能，增加网络的灵活性。

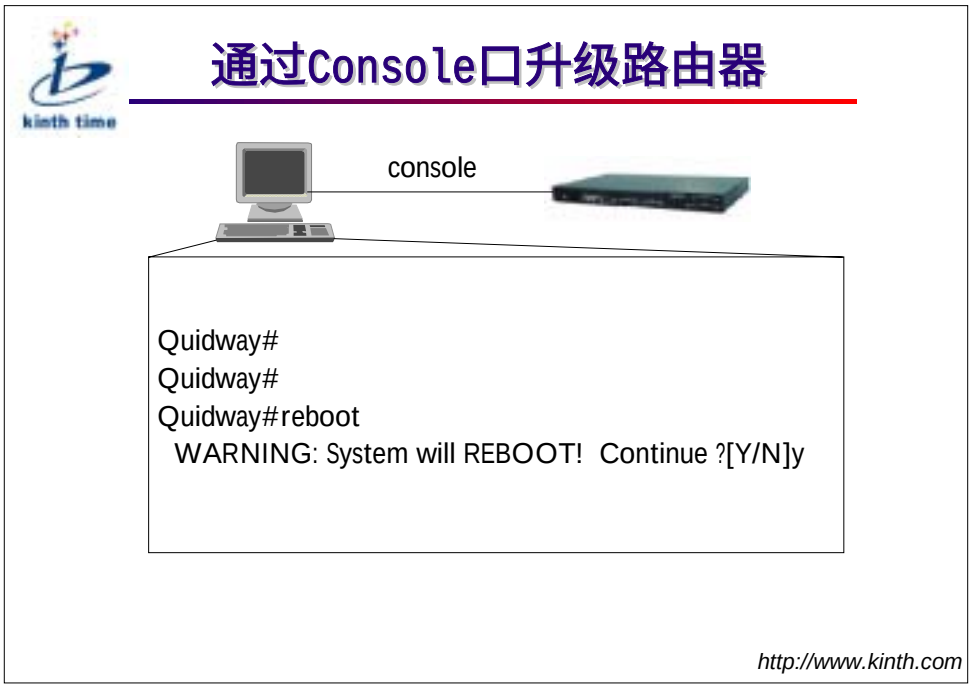
目前，Quidway 路由器支持两种升级的方式：通过 Console 口升级和通过 FTP Server 升级。

注：

请勿轻易进行路由器的软件升级，如有必要最好在技术支持人员的指导下进行。另外在进行路由器升级时，请注意 Bootrom 软件和主体软件的版本匹配。

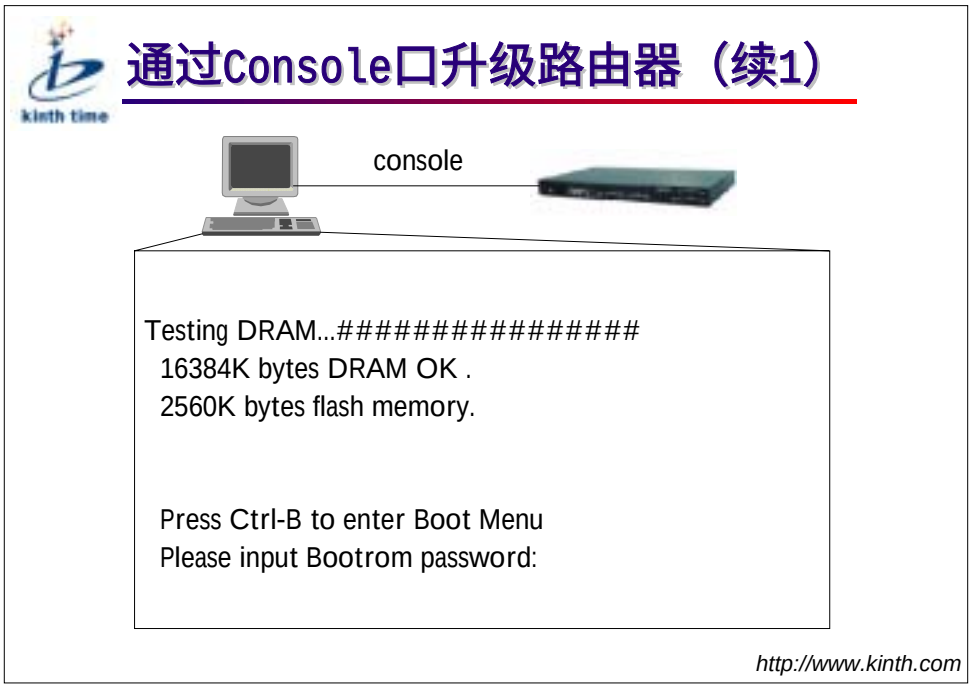
Quidway R2630/2631/3640/3680 路由器不支持对 Bootrom 软件的升级。

.5.1 通过 Console 口升级路由器



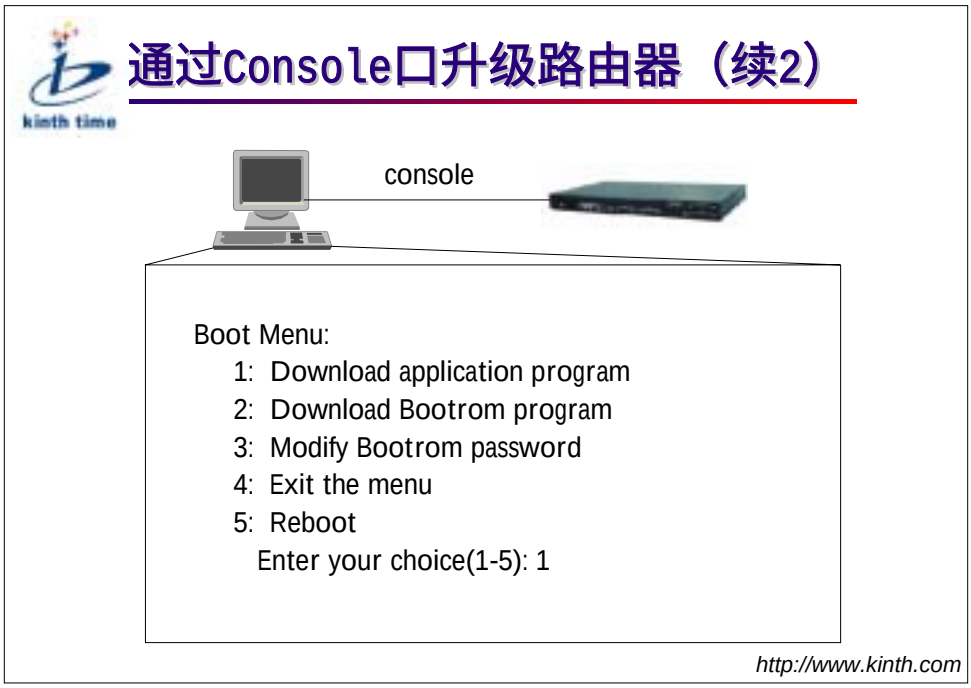
第一步：对路由器上电，如果您的路由器已经在配置模式下，请您保存配置信息后重新启动路由器。
不用担心，路由器升级后，您的配置将不会被改动。

通过 Console 口升级路由器（续1）



第二步：路由器自检结束，输出如下信息，提示用户输入 Ctrl-b 进入 Bootrom 菜单，如果在三秒之内没有输入 Ctrl-b，则转入路由器主体软件的运行。
输入 Ctrl-b，并输入正确的 Bootrom 口令，则可进入 Bootrom 菜单。

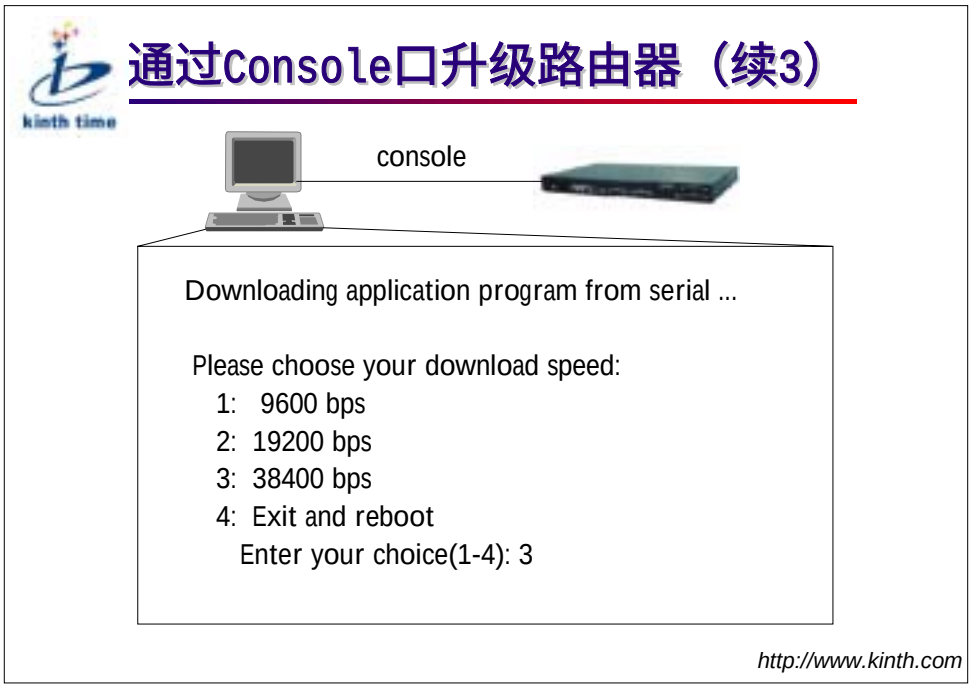
通过 Console 口升级路由器（续2）



第三步：如果选择 1 可以加载主体软件，选择 2 可以加载 Bootrom 软件，选择 3 可以修改 Bootrom 口令，选择 4 退出菜单转入路由器主体软件的运行。以选择 1 为例，系统提示用户选择加载软件所用的波特率。

注意：在通常情况下，对路由器的升级都是升级主体软件，即在本步选择“1”。如果将主体软件升级到 Bootrom 中，则将损坏路由器的 Bootrom ，造成路由器无法启动。

通过 Console 口升级路由器（续3）

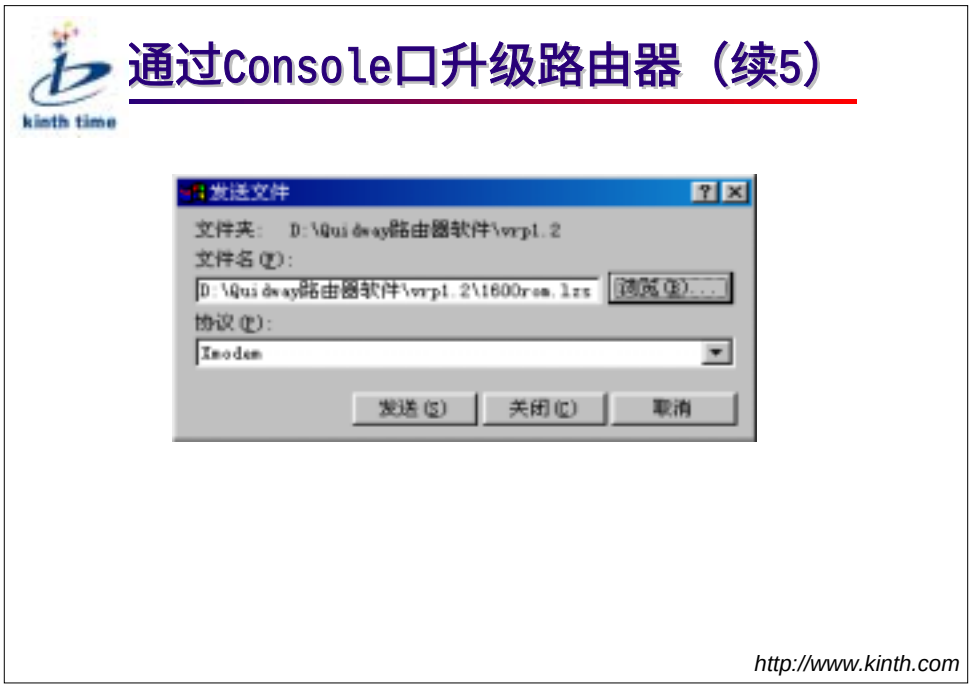


第四步：选择升级时所使用的波特率，为了提高升级的速度，我们通常选择 38400bps。

通过 Console 口升级路由器（续4）

第五步：以选择波特率 38400bps 为例，系统会提示用户修改波特率和选择 Xmodem 传输协议，在 Win95/Win98 环境“超级终端”下，可以进行如下操作：
菜单：“文件”(P)“属性”(P)“配置”，波特率选“38400”、数据位选“8”、奇偶校检选“无”、停止位选“1”、流量控制选“无”，按“确定”按钮；
在工具条处按“挂断”钮，再按“连接”钮（分别为第三、第四个钮）。

通过 Console 口升级路由器（续5）



第六步：路由器输出以下信息表示等待加载，用户需在终端仿真程序中选择要加载的文件，并将传输协议选择为“Xmodem”。

在 Win95/Win98“超级终端”环境下，“传送”(P)“发送文件”(P)“浏览”(P) 选定正确的“路由器主体软件”文件 (P)“发送”，发送过程中屏幕将出现发送文件的状态框：

Downloading...C C

加载完毕，路由器显示如下信息，并提示恢复终端仿真程序的波特率设置：

Download completed.

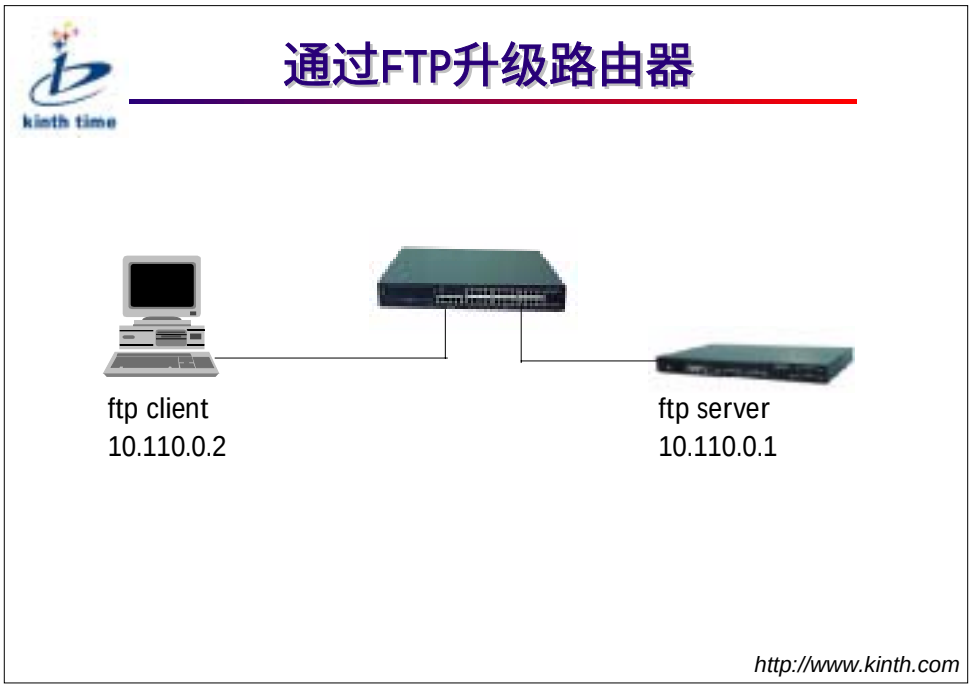
Write flash successfully !

Restore the terminal's speed to 9600 bps.

Press ENTER key when ready.

如果是对 Bootrom 软件进行升级，则由路由器自动重启；如果是对主体软件进行升级，则直接解压缩并装入内存执行。

.5.2 通过 FTP 升级路由器 *



配置路由器以太网口地址，使运行 FTP 客户端程序的主机与路由器的网络相通。

使用已经在路由器设置好的用户名、密码登录 FTP 服务器，以 Windows 98 所提供的 FTP 客户端程序为例：

☞ 在 DOS 提示符下，键入 FTP A.B.C.D（A.B.C.D 是路由器的以太网 IP 地址）。

☞ 在“username”提示下，键入用户名 ftp。

☞ 在“password”提示下，键入密码 123 ，验证通过后登录成功，显示 FTP 客户端提示符“ FTP > ”。

☞ 在“ FTP > ”提示符下键入 put。

☞ 在“local file”提示下，键入您所要上传的程序文件的名称。

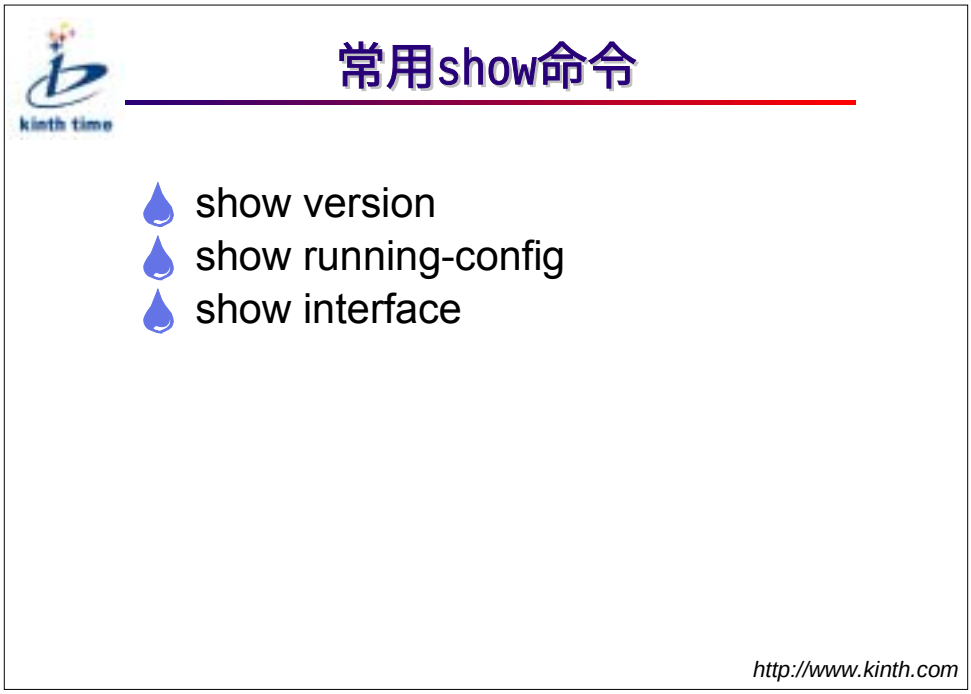
☞ 在“remote file”提示下，键入路由器端上传后所要保存的程序文件名称，该名称在上传操作之前必须在路由器端进行设置，缺省名称为 SYSTEM。

☞ 上传文件结束后，重新显示“FTP >”的提示符，键入 dir ，显示路由器上的文件名称和大小，上传成功则程序文件大小与主机上的文件大小一致。上传成功后，键入 quit 退出 FTP 客户端程序。

.6 基本操作命令

在路由器的日常的维护中，经常需要查看路由器的状态，相关的属性，以及网络的连接情况。更进一步，还需要了解路由器的工作状态。

.6.1 常用 Show 命令



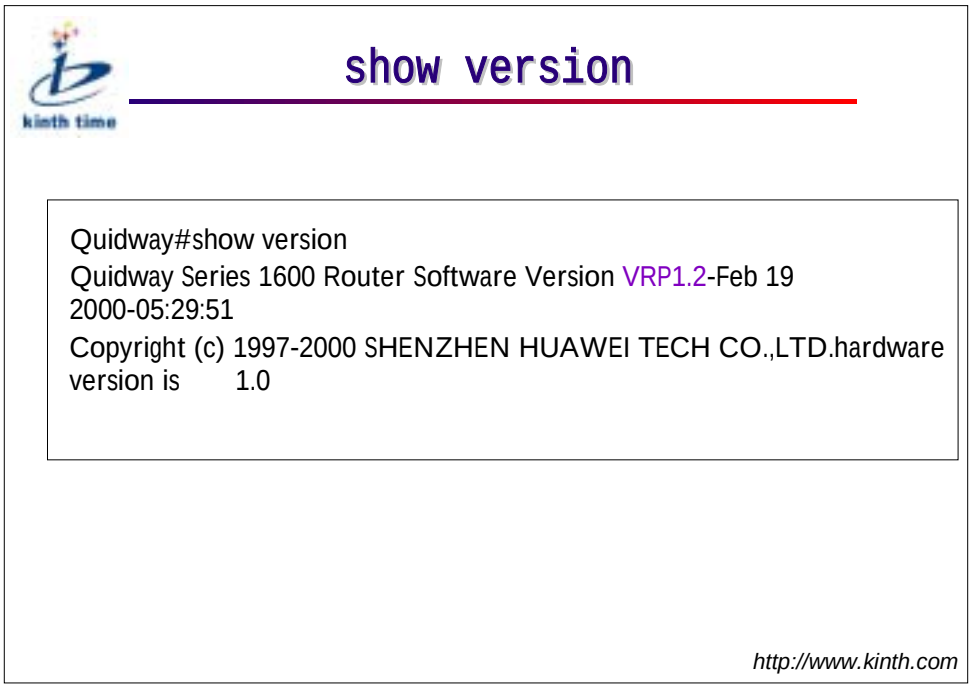
Show 命令是一种最常用的系统状态和系统信息查看命令。通过它，能使您了解到以下一些信息：

- 显示系统配置信息的命令；
- 显示系统运行状态的命令；
- 显示系统统计信息的命令。

当您向华为公司的技术人员寻求帮助时，他们往往要求您运行一些 show 命令，提供相关的信息，从而尽快的解决问题。

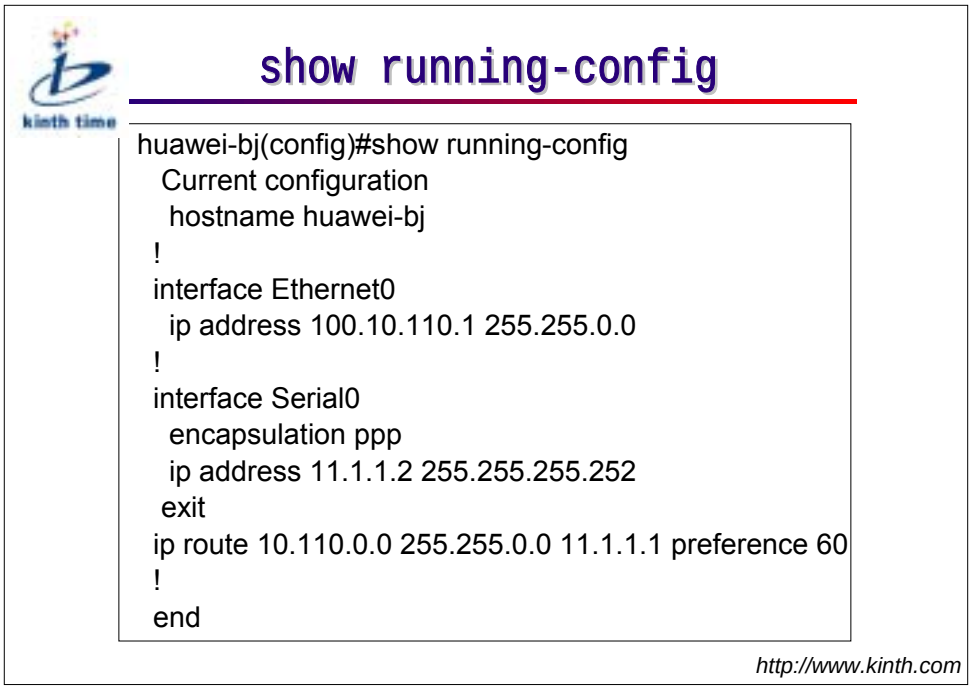
这里，我们介绍几种最常用的 show 命令，以供大家学习。

Show version



Show version 命令能够查看当前系统的软硬件信息。因为不同的版本有不同的特征，实现的功能也不完全相同。所以，查看版本信息解决问题的重要一步。

Show running-config

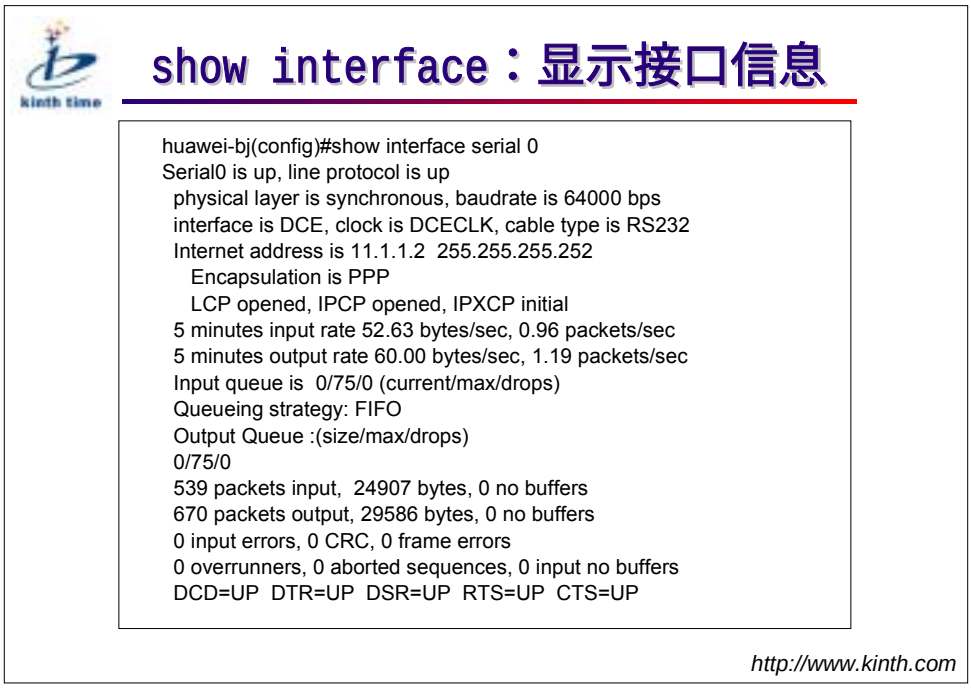


Show running-config 能查看当前的配置信息。注意：它是路由器目前正在运行的配置文件，当配置发生变动时，running-config 会立即改变。但是，只有使用了 write 命令后，该变动才会保存到 startup-config 中，在下次启动时自动执行。

配置文件为一文本文件，其格式如下：

- 以命令格式保存。
- 为了节省空间，只保存非缺省的常数命令的组织以命令模式为基本框架，同一命令模式的命令组织在一起，形成一节，节与节之间通常用空行或注释行隔开（以“！”开始的为注释行）。
- 节的顺序安排通常为：全局配置、物理接口配置、逻辑接口配置、路由协议配置等。
- 以 end 为结束。

Show interface



Show interface 能显示接口的状态。从中，能得到关于该接口的状态信息，帮助我们分析和解决问题。下面介绍常用的几行信息：

第一行：Serial0 is up， line protocol is up

表示物理层已经激活，链路层也已经激活。

第二行：Physical layer is synchronous， baudrate is 64000bps

表示物理层为同步方式，速率为 64000bps。

第三行：Internet address is 11.1.1.2 255.255.255.252

表示网络层的 IP 地址和子网掩码。

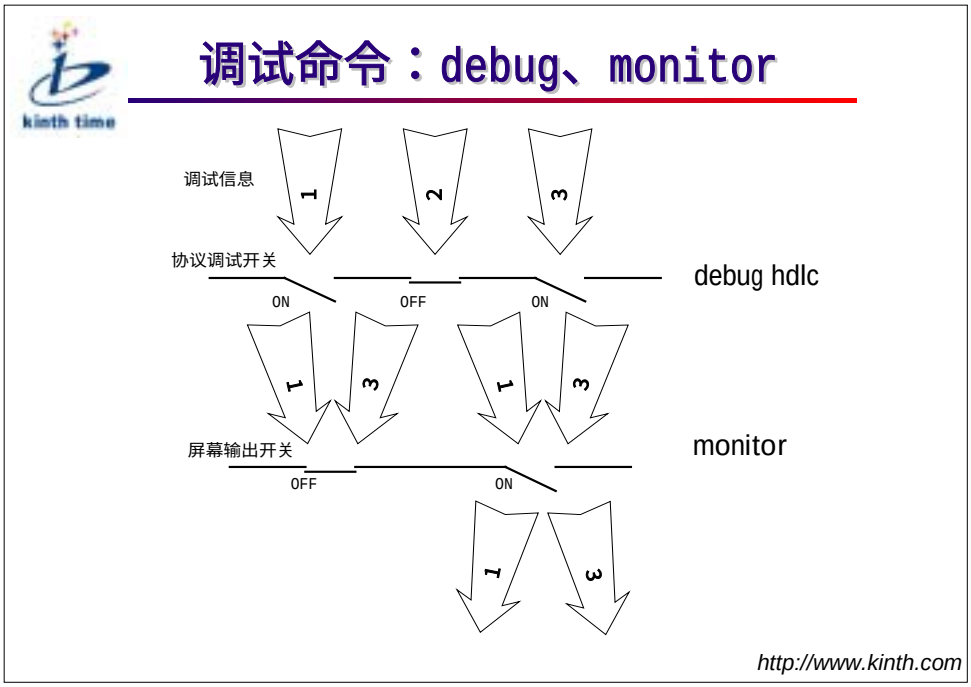
第四行：Encapsulation is PPP

表示链路层封装的协议为 PPP 协议。

最后一行：DCD=UP DTR=UP DSR=UP RTS=UP CTS=UP

表示该接口的物理连通性正常，所有应该有的 EIA 信好都出现了。

.6.2　调试命令



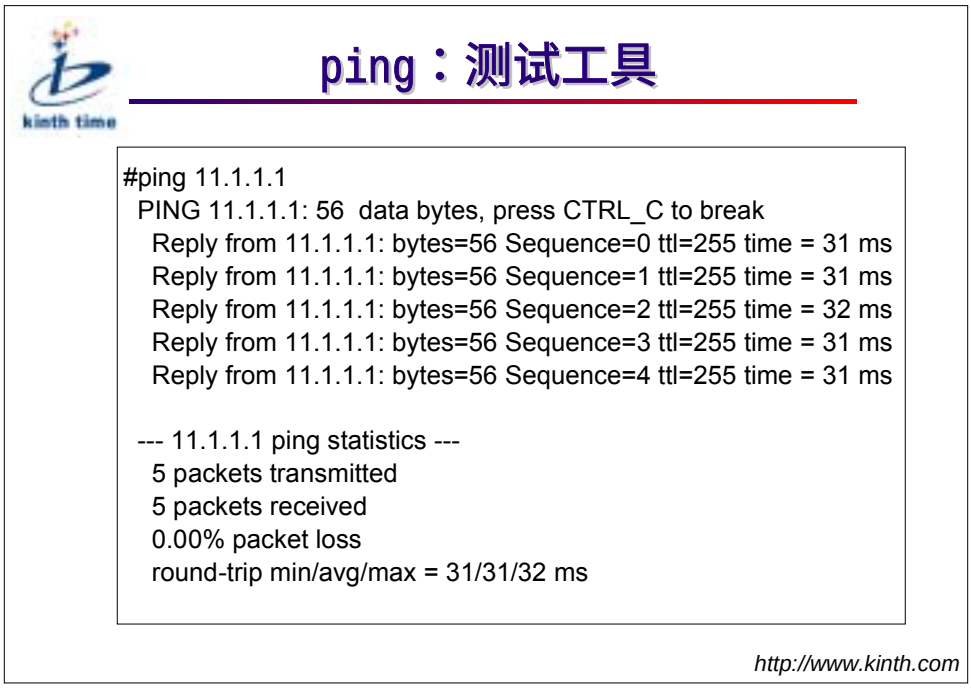
Quidway 系列路由器的命令行接口提供了种类丰富的调试功能，对于路由器所支持的各种协议和功能，基本上都提供了相应的调试功能，可以帮助用户进行错误的诊断和定位。

调试信息的输出可以由两个开关控制：

- ☞ 协议调试（Debug）开关，控制是否输出某协议的调试信息。
- ☞ 屏幕输出（Monitor）开关，控制是否在某个用户屏幕上输出调试信息。

注：由于调试信息的输出会影响路由器运行效率，请勿轻易打开调试开关，尤其慎用 debug all 命令，在调试结束后，应关闭全部调试开关。

.6.3 Ping 命令



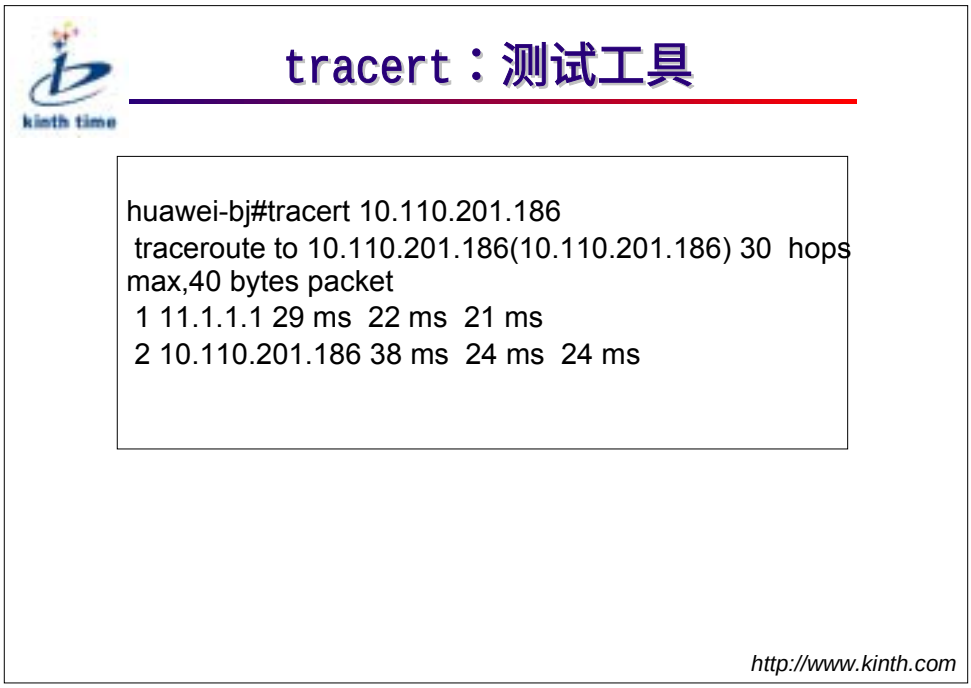
Ping 主要用于检查网络连接及主机是否可达。Ping 支持两种网络协议（IP 和 IPX），缺省为 IP。

命令执行结果输出包括：

对每一 Ping 报文的响应情况，如果超时到仍没有收到响应报文，则输出“Request time out.”，否则显示响应报文中数据字节数、报文序号、TTL 和响应时间等。

最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

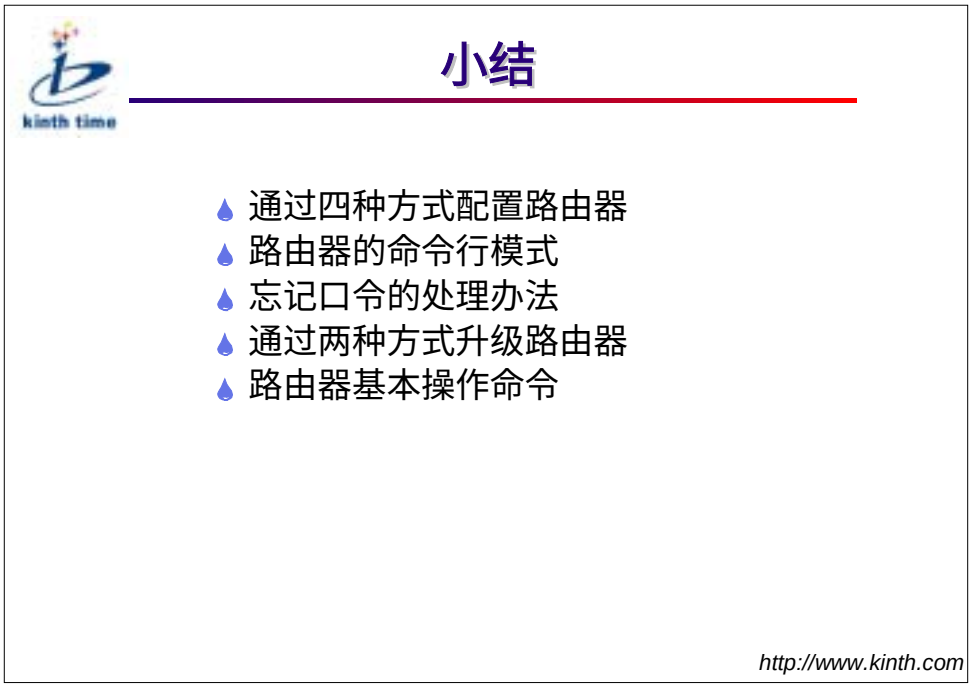
.6.4 Tracert 命令



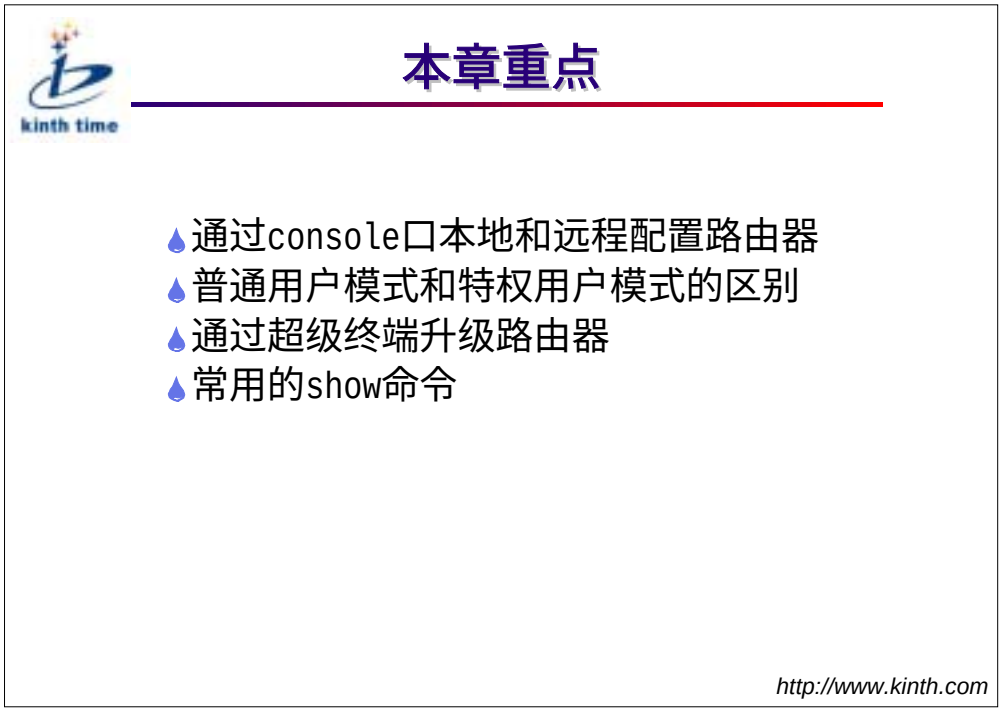
Tracert 用于测试数据包从发送主机到目的地所经过的网关，它主要用于检查网络连接是否可达，以及分析网络什么地方发生了故障。

Tracert 的执行过程是：首先发送一个 TTL 为 1 的数据包，因此第一跳发送回一个 ICMP 错误消息以指明此数据包不能被发送（因为 TTL 超时），之后此数据包被重新发送，TTL 为 2，同样第二跳返回 TTL 超时，这个过程不断进行，直到到达目的地。执行这些过程的目的是记录每一个 ICMP TTL 超时消息的源地址，以提供一个 IP 数据包到达目的地所经历的路径。

.7 小结

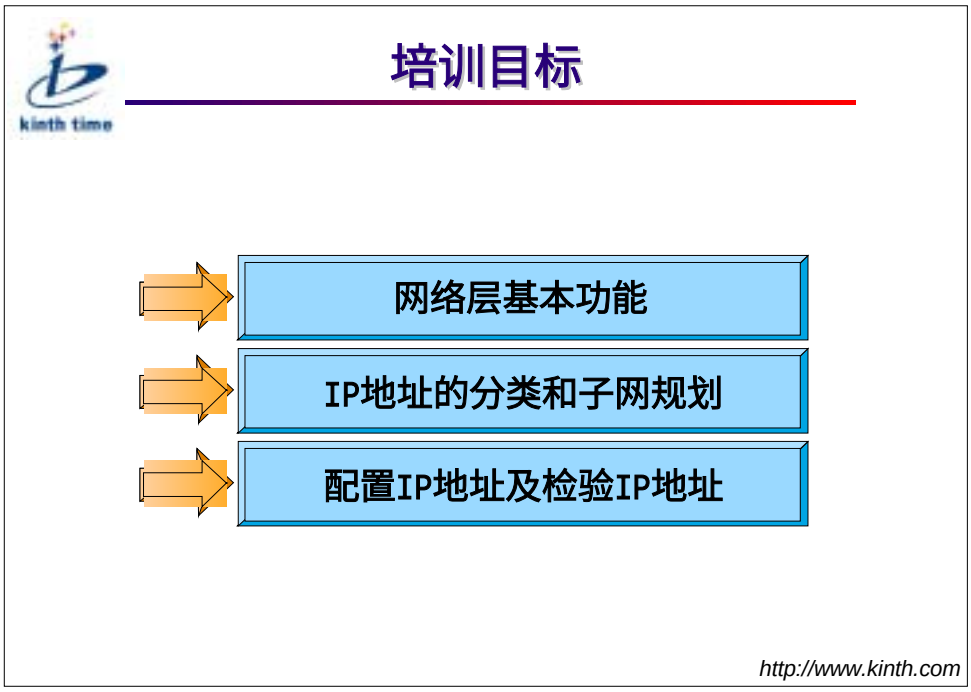

小结
通过四种方式配置路由器
路由器的命令行模式
忘记口令的处理办法
通过两种方式升级路由器
路由器基本操作命令
http://www.kinth.com

.8 本章重点


kinth time
本章重点
通过console口本地和远程配置路由器
普通用户模式和特权用户模式的区别
通过超级终端升级路由器
常用的show命令
http://www.kinth.com

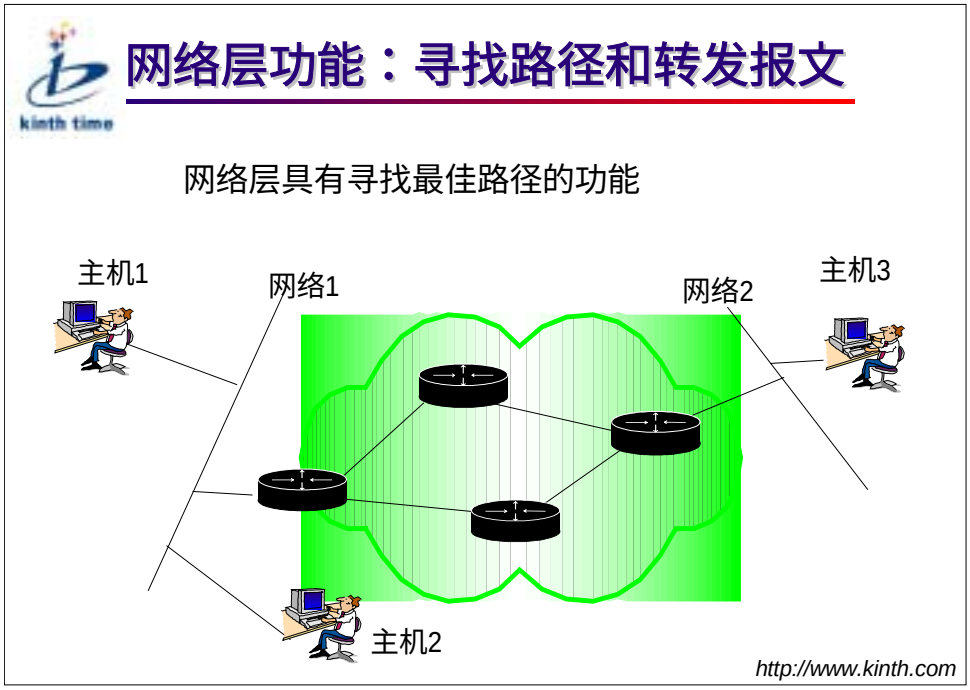
第七章　　网络层基础及子网规划

.1　培训目标



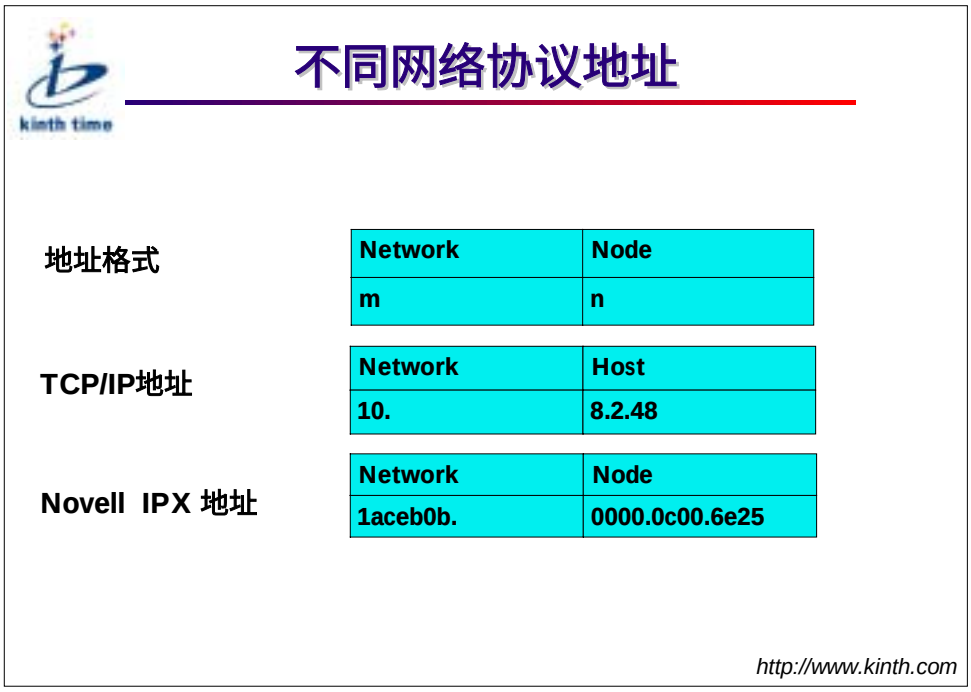
.2　网络层基础

.2.1　网络层功能



当报文在网络云中传送时，从源主机到达目的主机，需要各个中间点决定路径，即寻找路径，这种功能由路由器中的网络层完成。路由器的网络层评估到达目标的各个路径，对要转发报文进行适当的处理。路由器使用网络拓扑信息评估到达目标的各个路径，这些网络拓扑信息是由网络管理员手工配置或通过路由协议动态获得的。
网络层为它的上一层（传输层）提供报文转发的服务。网络层把报文从报文源发送到报文的目的地。网络层提供端到端的尽力传送的服务。

.2.2　网络协议地址



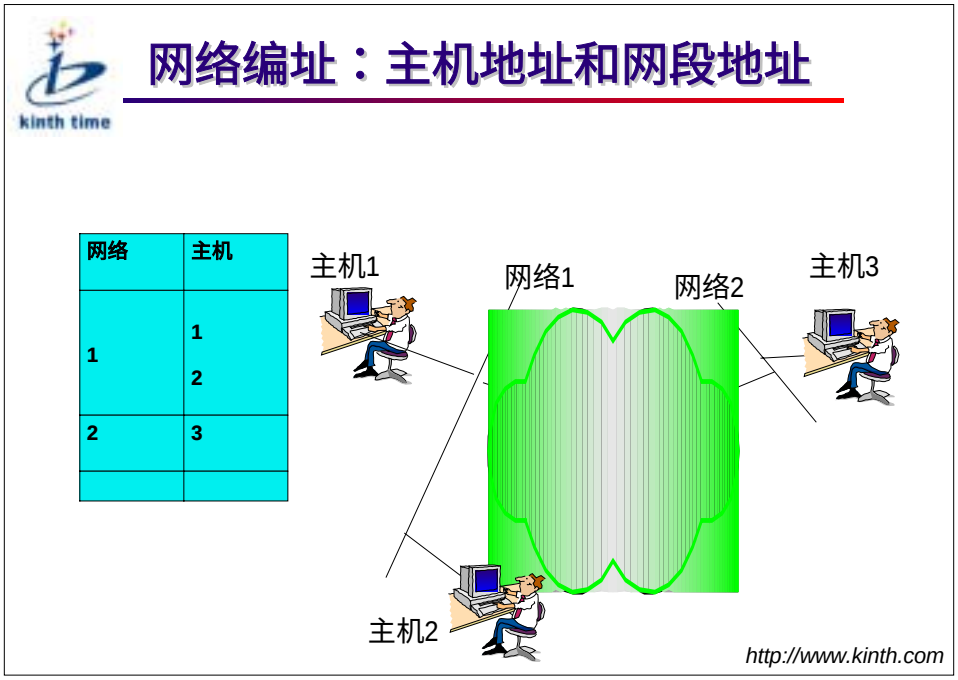
网络地址由两部分地址组成：网段地址和主机地址。如何解释两部分地址？地址分配应有何特权？不同协议这些问题的答案各不相同。

例如，TCP/IP 中 IP 地址采用点分十进制数字显示地址的网段部分和主机部分，利用掩码区分 IP 地址的网络部分、主机部分。如现有一个 IP 地址是 10.8.2.48，掩码是 255.0.0.0。将 IP 地址 10.8.2.48 与掩码 255.0.0.0 相与，得出 10.0.0.0。则 10 为网络部分，该 IP 地址的网络号为 10。IP 地址中剩余部分 8.2.48 是主机部分，该 IP 地址的主机号是 8.2.48。

又如，Novell IPX 使用与 IP 协议不同的网络地址，但也是由两部分组成：网段部分（32 比特）、主机部分（48 比特）。如 bc.0.0cb.47。网络号是 bc；主机号是 0.0cb.47。

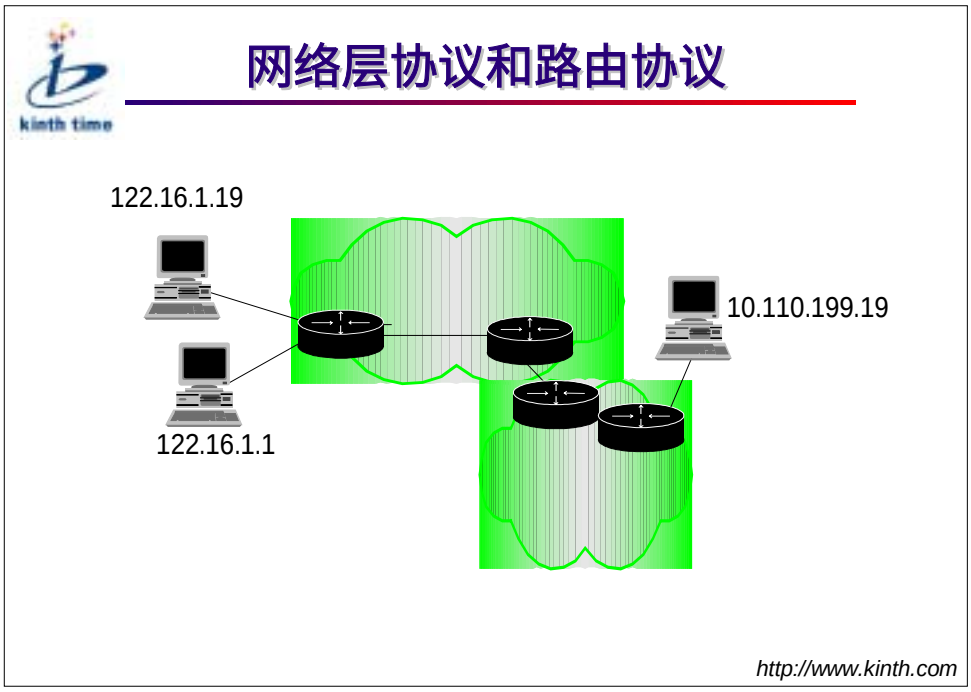
以上是两种最通用的网络层地址类型，在下面几页中，您将能学到更多的这些协议的地址规则 。

.2.3　网络协议编址



路由器的基本功能就是“将报文从一个地方送到另一个地方”。即：将报文从一个接口转发到另外一个接口。为了转发报文,路由器使用两种最基本功能:寻径和转发。
上图显示路由器如何使用寻径和转发功能。
路由器根据报文的网段地址在报文流经的中间路径实现报文的转发，根据报文的主机地址，在目的主机所在的网络中将报文发送给目的主机。寻径功能能够计算出从路由器到目的地的完整路径，路由器的责任就是转发报文到最佳路径的下一个网络，最佳路径代表一个到达目的地的方向。寻径功能使路由器选择最合适的接口发送报文。
转发功能使路由器把从一个接口收到的报文经由寻径功能选择的接口发送出去。

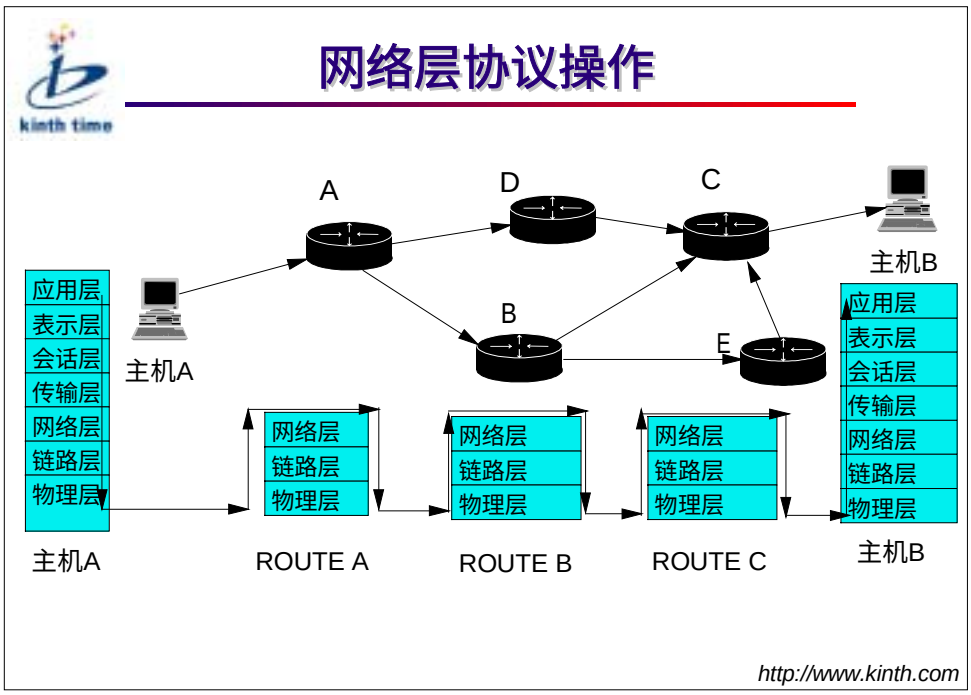
.2.4　网络协议与路由协议



任何网络层协议在它的网络层地址中提供足够的信息，以实现报文的发送。网络层协议中定义了报文的各个域的含意和用途。网络层协议目前实现了报文的端到端转发，IP　和 IPX　就是两种网络层协议。

路由协议通过提供“共享路由信息”的机制来支持网络层协议对报文进行寻径。路由协议通过网络层在路由器之间传递路由信息。路由协议使路由器能够修改和维护自己的路由表。路由协议不携带任何终端用户数据在网络间移动，用户数据要通过网络层协议在路由器之间传送。TCP/IP 路由协议包括 RIP、IGRP、OSPF 等等。

.2.5　网络层工作原理



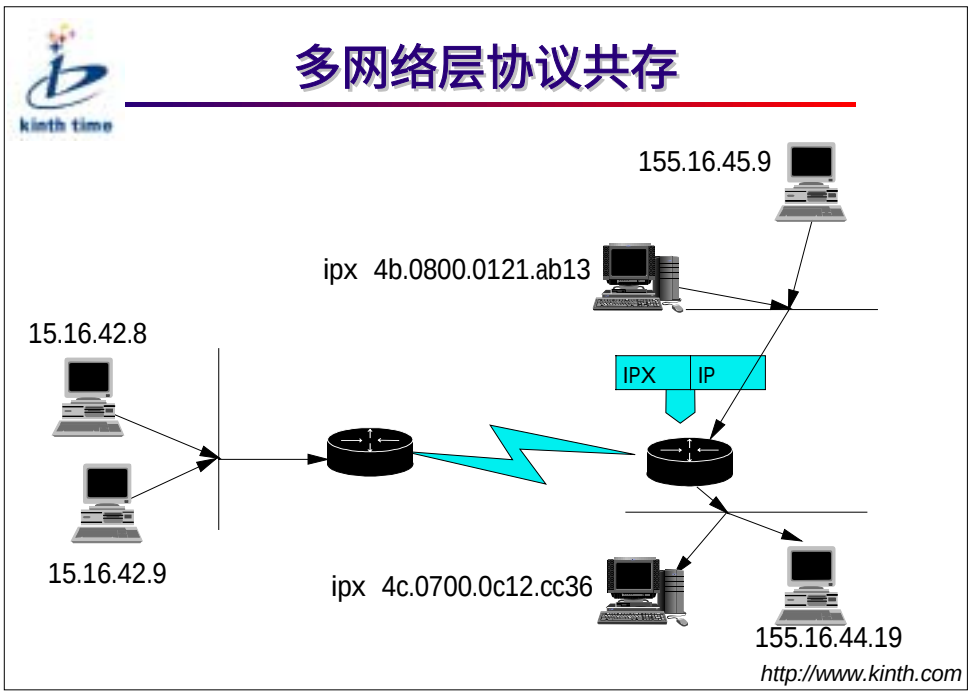
当主机应用程序需要发送报文到处于另一个物理网络的目的地时，与该主机在同一物理网络上的路由器的一个接口会收到数据帧，路由器中的链路层检查该帧，确定被携带的网络层数据类型，去掉链路层帧头，并将网络层数据送往相应的网络层进行处理。

网络层检查报文头以决定目的地址所在网段，然后查找路由表获取相应输出接口。

输出接口的链路层为该报文加上链路层帧头，封装成数据帧并发送到下一跳。

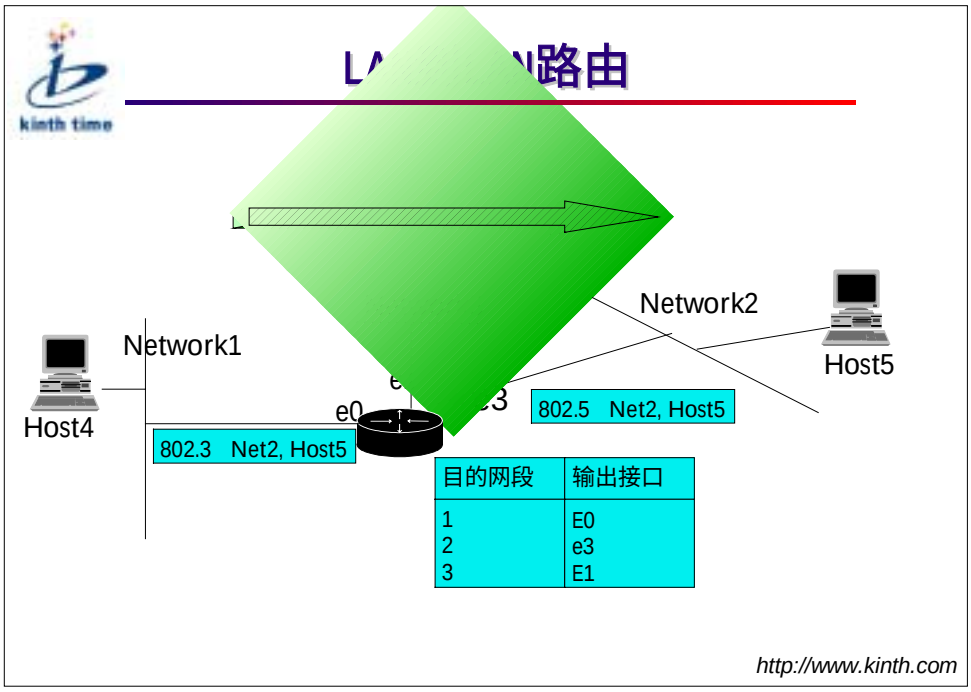
每一个报文的转发都要进行这一过程。在到达目的主机所在网络时，报文被封装成目地网络的链路层数据帧，发送给相应的目的主机。目的主机接收到该报文后，经过链路层、网络层的处理，去掉链路层帧头、网络层报文头后，送给相应的协议。

.2.6　多协议共存特性



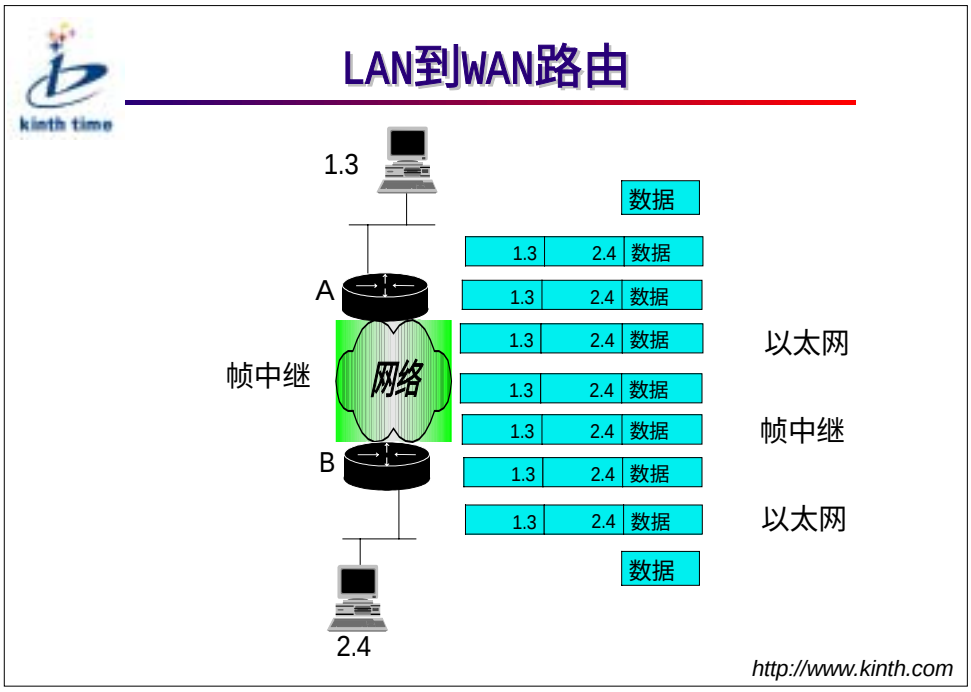
路由器能支持多个相互独立的路由协议，能为不同的网络层协议（如IP、IPX）维护各自的路由表。路由器的这种能力允许路由器能同时支持多种网络层协议，进行报文的转发。
网络层协议和路由协议相互间独立。

.2.7　LAN 到 LAN 路由



网络层必然要通过各种各样的链路层发送报文。
路由器一定要具备在不改变网络层地址的前提下无缝地将报文封装成各种链路层数据帧的能力。
如图，报文从处于 Net1 的 Host4 发送到 Net2 的 Host5。路由器根据报文的网络层目的地址寻找路径。
路由器查找路由表，发现最佳路径是从 E3 发出。路由器将报文封装成 E3 的链路层数据帧发送出去。
路由器转发报文时，链路层的帧格式会发生改变。但网络层的源地址和目的地址都不会发生变化。

.2.8　LAN 到 WAN 路由



随着网络的增长，报文传送过程中可能会遇到各种各样的数据链路。如图，报文从位于图顶端的工作站必须经过三个数据链路层到达文件服务器。

工作站将封装成以太网帧格式的报文发送到路由器 A。

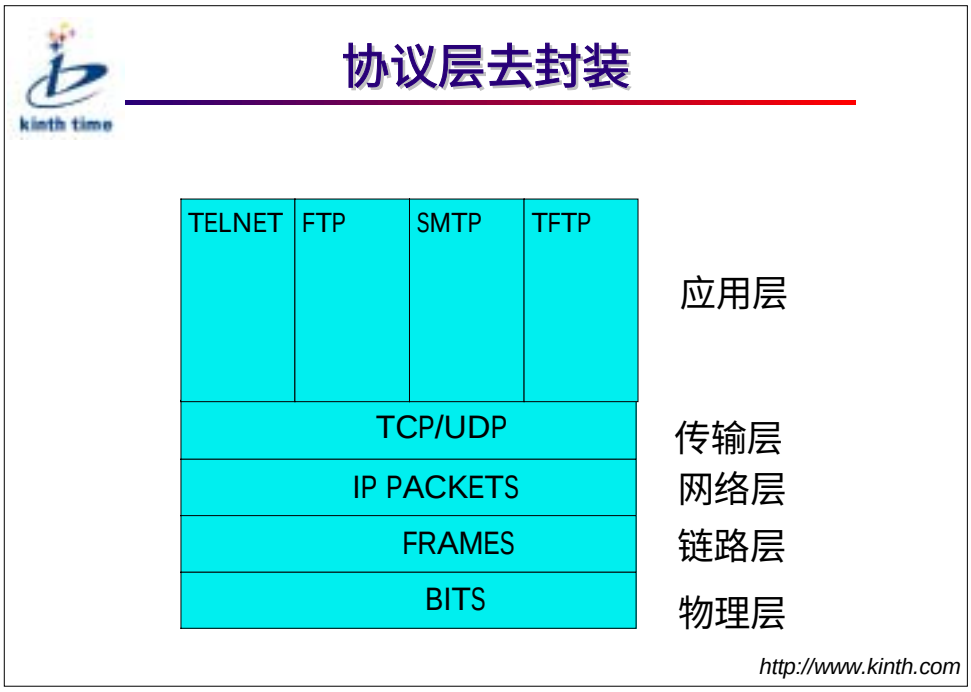
路由器 A 收到以太网帧格式的报文后根据输出端口的帧格式，将链路层的数据帧格式改成帧中继的帧格式，发送到路由器 B。

路由器 B 收到帧中继帧格式的报文后再改为以太网帧格式发送到文件服务器。

文件服务器收到报文后，交给相应的上层进程处理。

路由器在 LAN 到 WAN 报文转发中，始终保持端到端网络层的源 IP 地址和目标 IP 地址不变。

.2.9　协议层去封装



如同 ISO/OSI 协议层一样，TCP/IP 协议在报文转发过程中，封装和去封装发生在各层之间。

在发送方，加封装的操作是逐层进行的。应用程序将要发送的数据送给传输层；传输层（TCP/UDP）加上本层的报文头后，发送给网络层（IP 层）；网络层加上本层的报文头后，再发送给链路层（以太网、帧中继、PPP、HDLC 等）；链路层加上本层的帧头，就送给物理层将报文发送出去。

在接收方，这种去封装的操作也是逐层进行的。

从接口上发送的报文被组成链路层数据帧。在报文的链路层帧头域中，如果是以太网帧，则有 MAC 地址；如果是广域网，则有相应的广域网的链路层地址。

☞ 链路层帧头包含类型（Ethernet_II）和其它控制信息和数据。

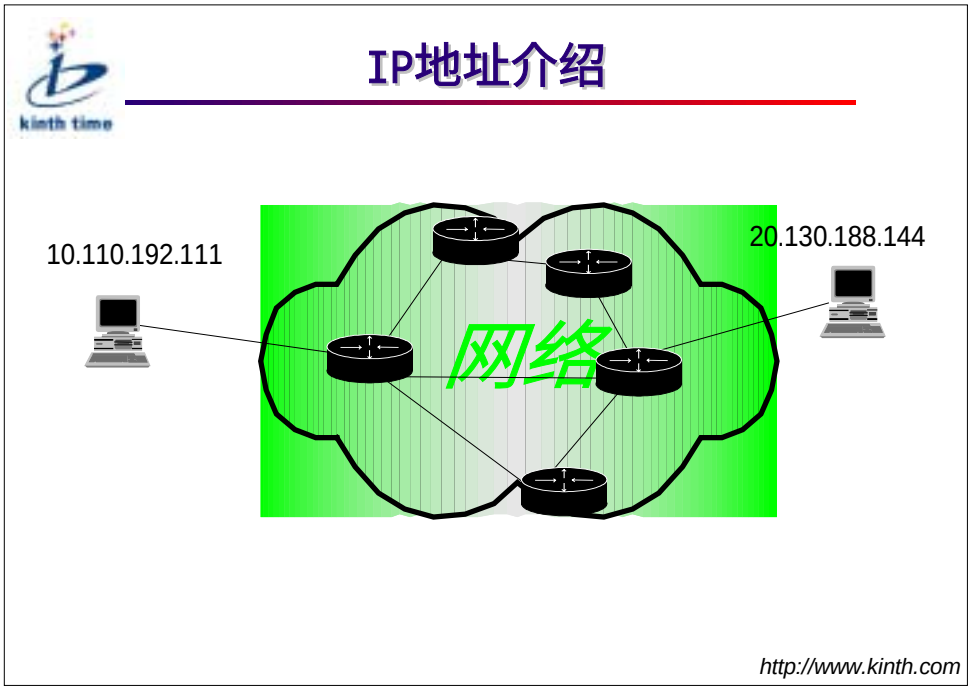
☞ 网络层的报文头，如 IP 报文头中包含它所携带的报文协议类型，这个数字指定第四层即传输层的协议是 UDP（17）还是 TCP（6），还是其他的协议。

☞ 在传输层报文头中，包含接收它所携带的数据的上层协议或应用程序的端口号，例如，Telnet 的端口号是 23。

☞ 应用层协议或应用程序利用传输层，向用户提供端到端的网络功能。

.3　IP 地址基础和子网规划

.3.1　IP 地址介绍

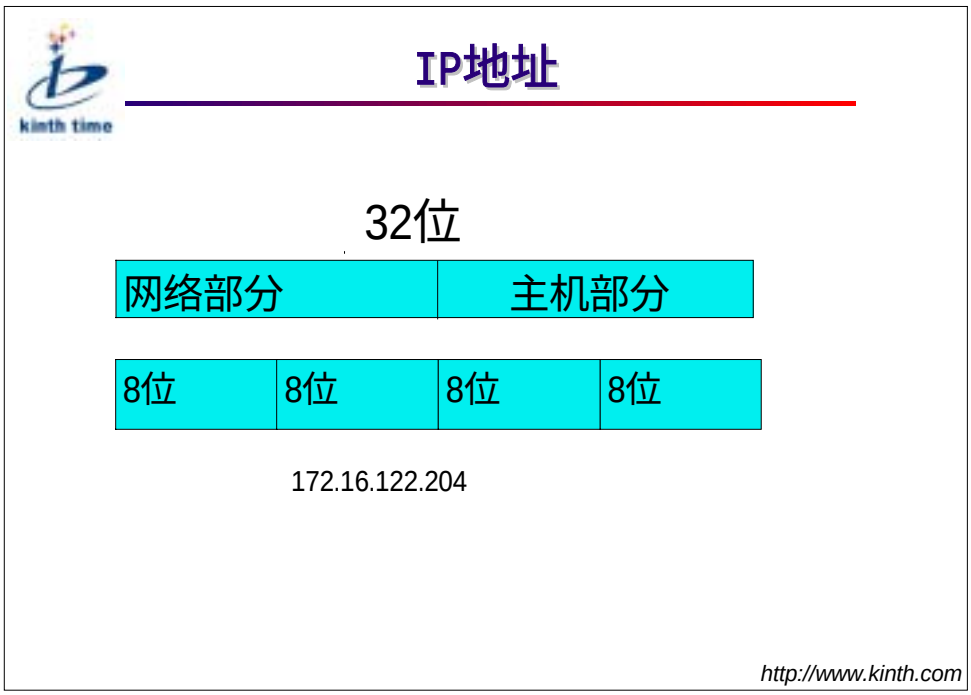


在 TCP/IP 环境中，各种各样的终端、工作站能同服务器、其它工作站无缝连接，是因为每一网络节点都使用了在全网范围内能够唯一标识本节点的 IP 地址。

在互联网上，报文的发送经常基于名称，而不是枯燥的 IP 地址。如果在通讯过程中使用名字而不是 IP 地址，则需先将名字转化成 IP 地址，然后再发送。

在互联网上每个公司被看作单个网络，在能访问到公司的主机之前必须先能访问到它所在的网络。每个网络有一个全网唯一的网络号，在该网络中的各主机共享这个网段号（网段地址）。同时，各主机有可唯一标识自己的主机号。

.3.2　IP 地址



IP 地址有 32 位比特位，分为两部分：

- ☞ 网段地址部分；
- ☞ 主机地址部份。

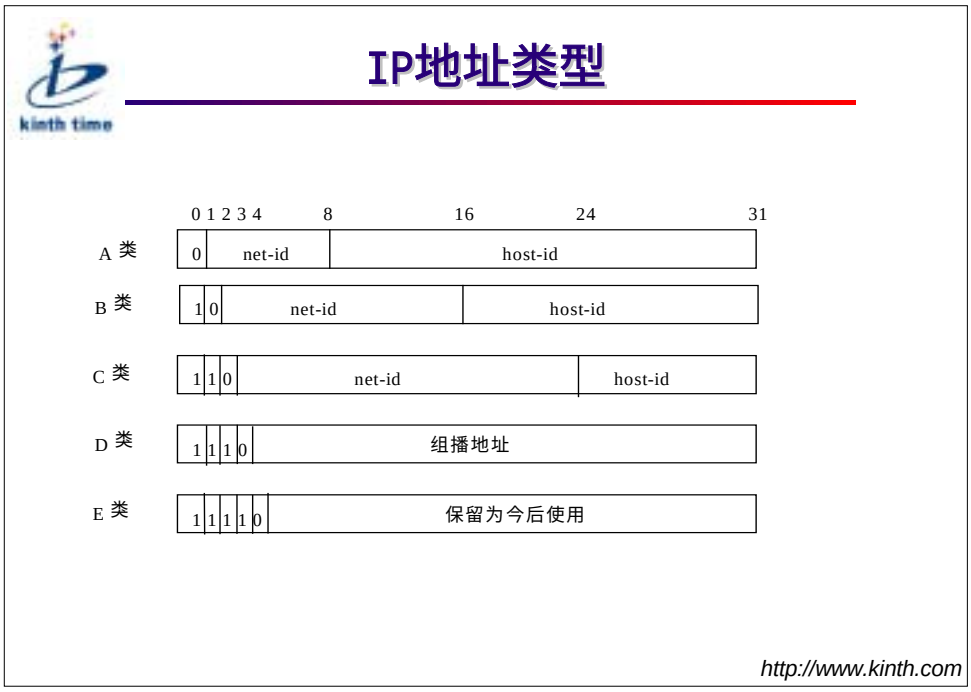
地址采用点分十进制格式：

如 172.16.112.204

- ☞ 八位组每位有二进制权（128，……，4，2，1）
- ☞ 八位组最大值为 255
- ☞ 八位组最小值为 0

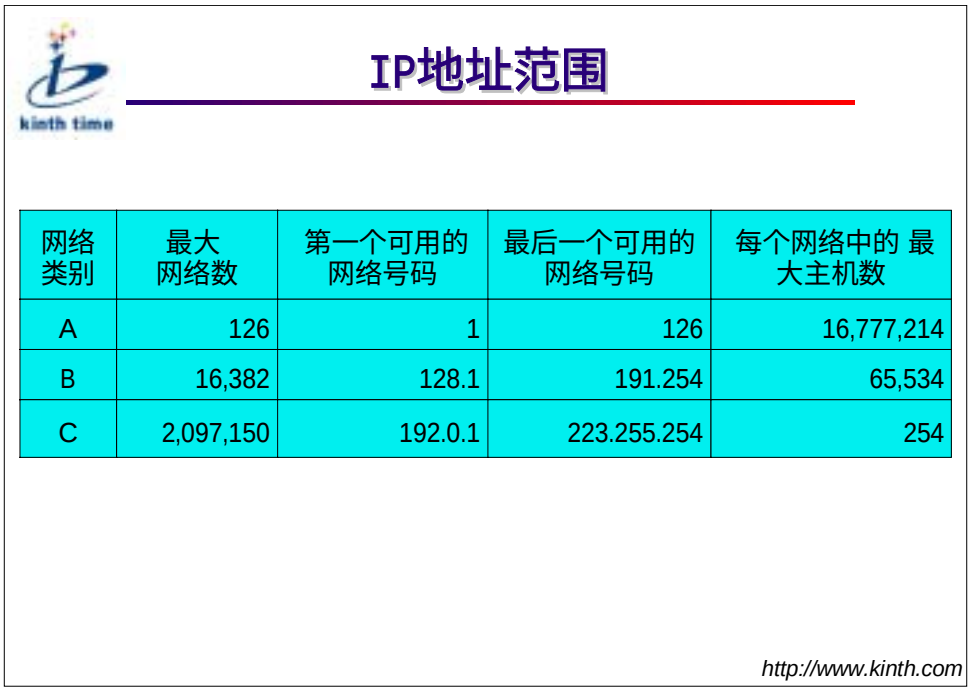
IP 地址的分配由地址分配中心管理。

.3.3　IP 地址类型



当初开发 IP 协议时，IP 地址并没有分类。后来为了管理上的需要，对 IP 地址进行了分类：
有 126 个 A 类网络，每个 A 类网络包括大约 1600 万个 IP 地址；有 16000 余个 B 类网络，每个 B 类网络包括 65534 个 IP 地址；有 200 多万个 C 类网络，每个 C 类网络包括 254 个 IP 地址。
这种地址分配原则允许地址管理机构基于网络大小来分配地址。
D 类地址从 224.0.0.0 开始，为多播使用。E 类地址从 240.0.0.0 开始，用于实验目的。

.3.4　IP 地址范围



IP 地址最高五位决定了 IP 地址的种类。

☞ A 类地址：

地址从 1.0.0.0 到 126.0.0.0 ，共 16777214 个主机地址；

☞ B 类地址：

地址从 128.1.0.0 到 191.254.0.0 ，共 65534 个主机地址；

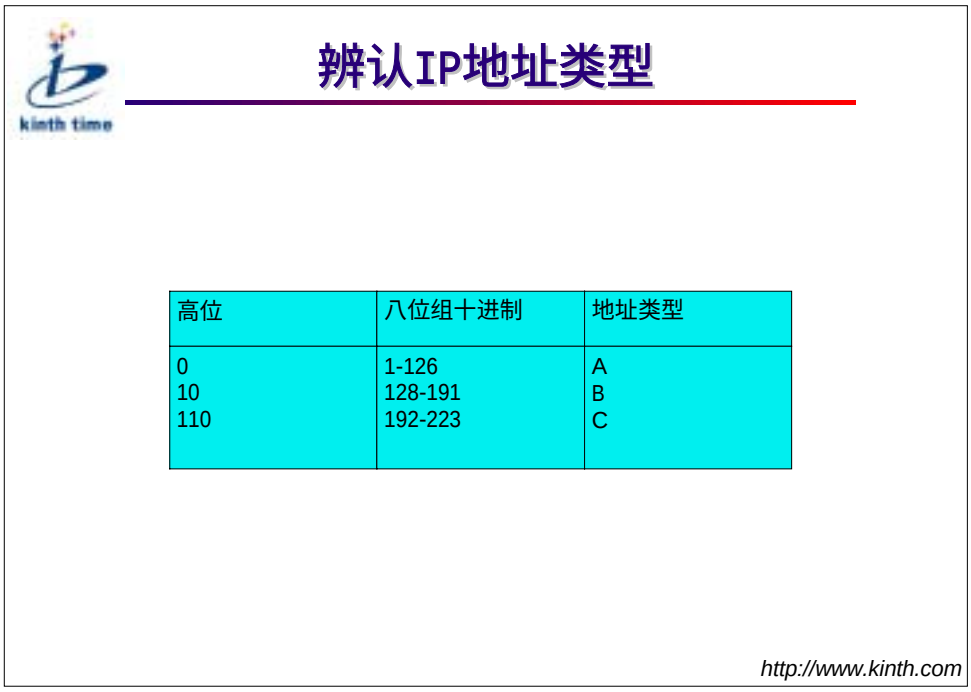
☞ C 类地址：

地址从 192.0.1.0 到 223.255.254.0 ，共 254 个主机地址；

☞ D 类地址：

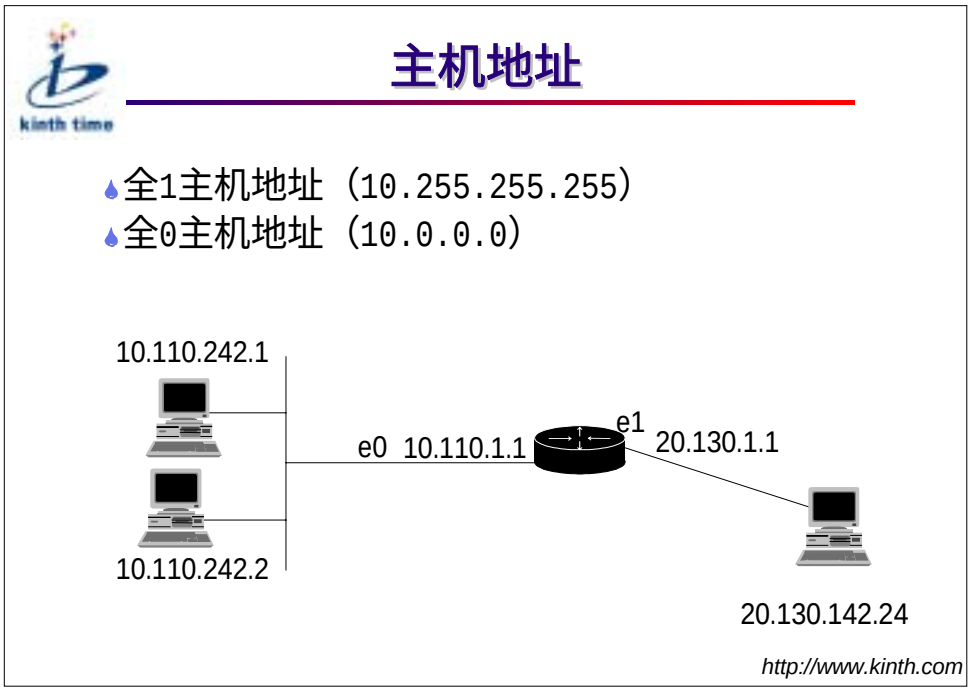
从 224.0.0.0　到 239.255.255.254。

.3.5　IP 地址辨别



图中第一个八位组决定了 IP 地址的类型。
IP 地址以这种方法定义，使用时可以很快从中抽出主机地址和网段地址部分。当决定将一个分组发往何处时，路由器使用地址的网段部分。路由器因为能高效地提取网段地址从而达到很高的报文转发速度。

.3.6　主机地址



每一设备和接口必须有一个主机地址（即 IP 地址的主机部分不能为全 0 或全为 1）。

☞ 全 1 主机地址保留给 IP 广播使用。

☞ 全 0 主机地址意味着这个网络本身，有些早期的网络把用它作为广播地址使用。

路由表中包含网段地址，它通常不包含主机地址。

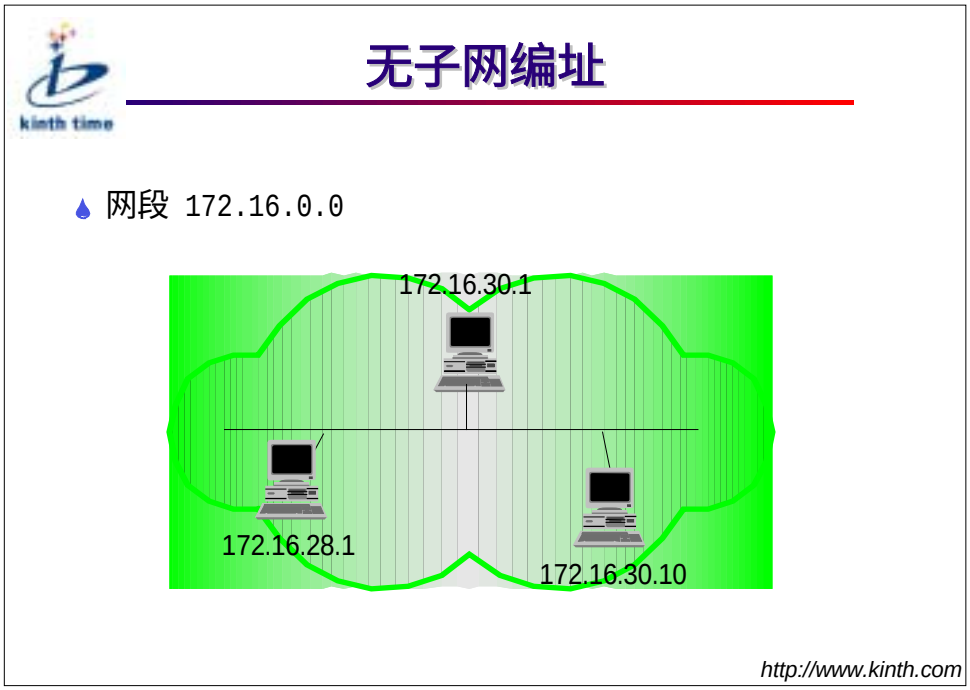
在接口上的 IP 地址和子网地址实现三个功能：

☞ 使系统收发报文；

☞ 指定设备地址；

☞ 指定共享同一线路的设备地址范围。

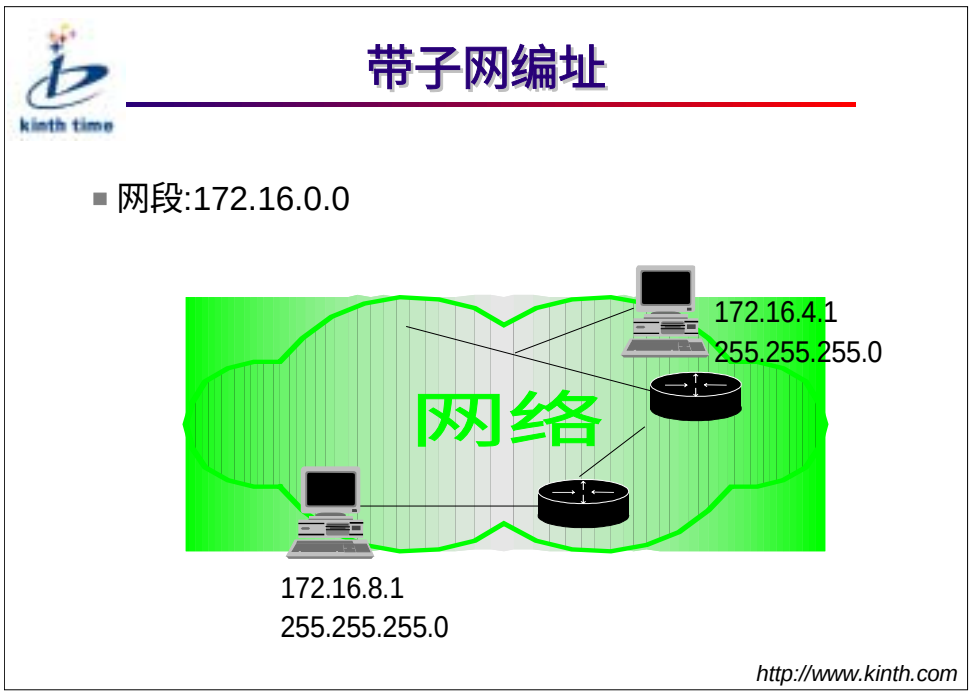
.3.7　无子网编址



对于没有子网的 IP 地址组织，外部将该组织看作单一网络，不需要知道内部结构。例如，所有到地址 172.16 .X.X 被认为同一方向，不考虑地址的第三和第四个 8 位分组，这种方案的好处是减少路由表的项目。但这种方案没法区分一个大的网络内不同的子网网段，这使网络内所有主机都能收到在该大的网络内的广播，会降低网络的性能。另外也不利于管理。

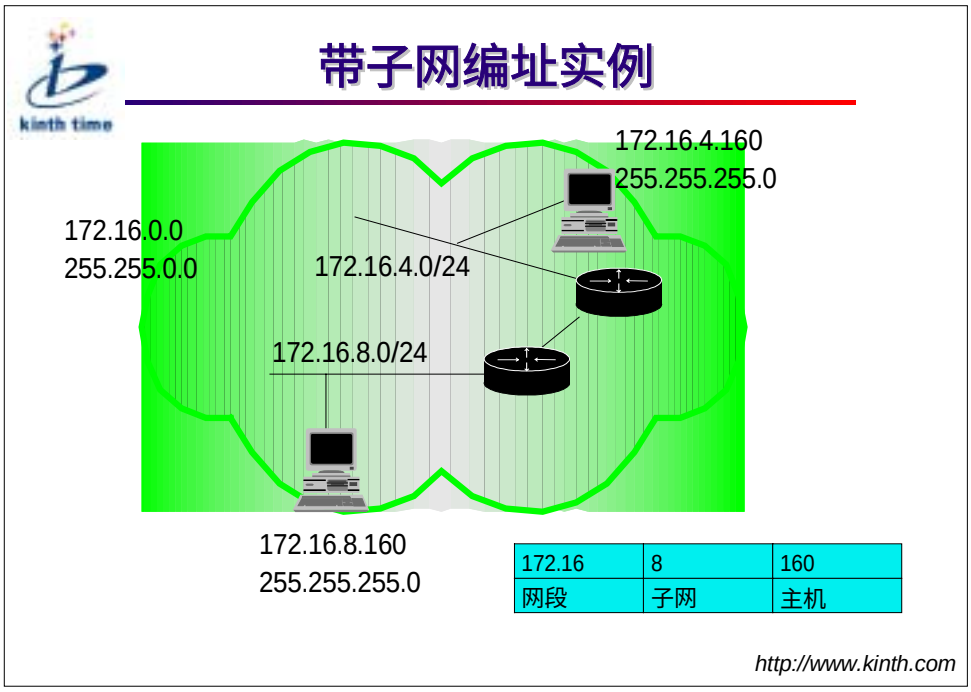
比如，一个 B 类网可容纳 65000 个主机在网络内。但是没有任何一个单位能够同时管理这么多主机。这就需要一种方法将这种网络分为不同的网段。按照各个子网段进行管理。

.3.8　带子网编址



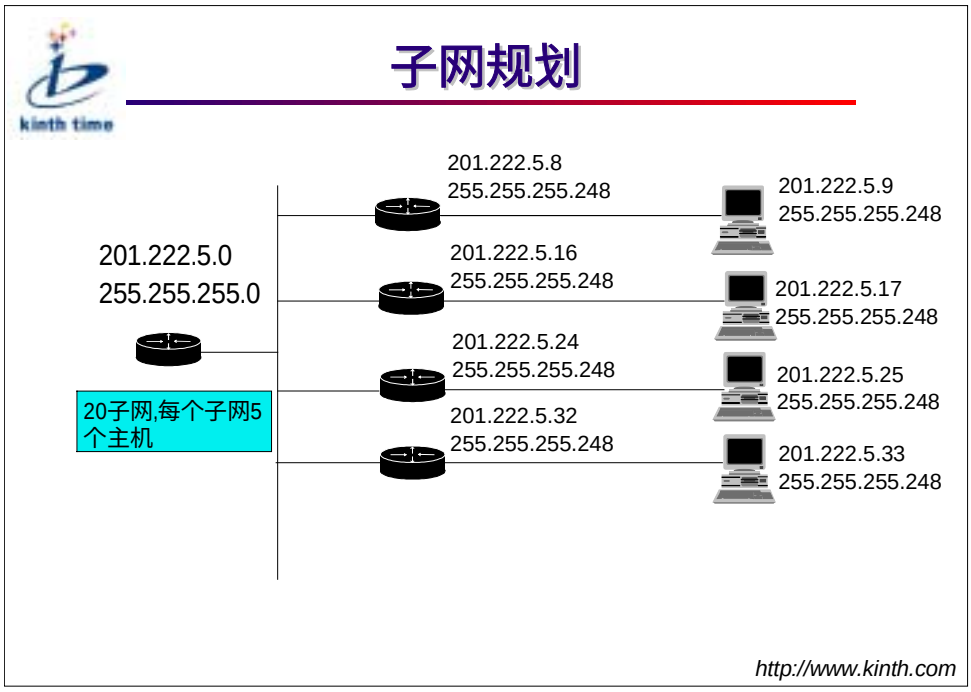
利用子网，网络地址的使用会更有效。对外 仍为一个网络，对内部而言，则分为不同的子网。
如图：网络 172.16.0.0 分为两个网段：172.16.4.0、172.16.8.0。
如果公司的财务部使用 172.16.4.0 子网段 ;公司的工程部使用 172.16.8.0 子网段。这样可使路由器根据目的子网地址进行路由，从而限制一个子网的广播报文发送到其它网段，不对网络的效率产生影响。

.3.9　带子网编址举例



从地址分配的角度来看，子网是网段地址的扩充。网络管理员根据组织增长的需要决定子网的大小。
网络设备使用子网掩码决定 IP 地址中哪部分为网络部分，哪部分为主机部分。

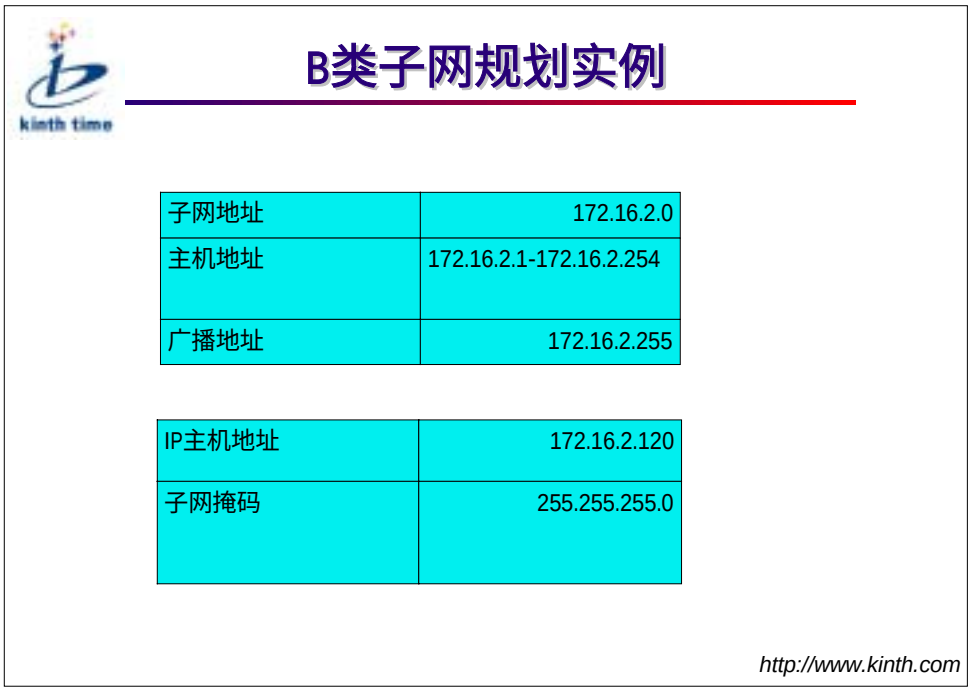
.3.10　子网规划



在这个例子中，网段地址是一个 C 类地址：201.222.5.0 。 假设需要 20 个子网，其中每个子网 5 个主机，就要把主机地址的最后一个八位组分成子网部分和主机部分。

子网部分的位数决定了子网的数目。在这个例子中子网部分占有 5 位，最大可提供 30 (2^5 -2) 个子网。剩余 3 位为主机部分。一共有 8 个 (2^3) 值。主机部分全是 0 的 IP 地址，是保留地址；主机部分全是 1 的 IP 地址是本子网的广播地址。这样就剩余 6 个主机地址。可以满足需要。

7.3.10.1　B 类子网规划实例

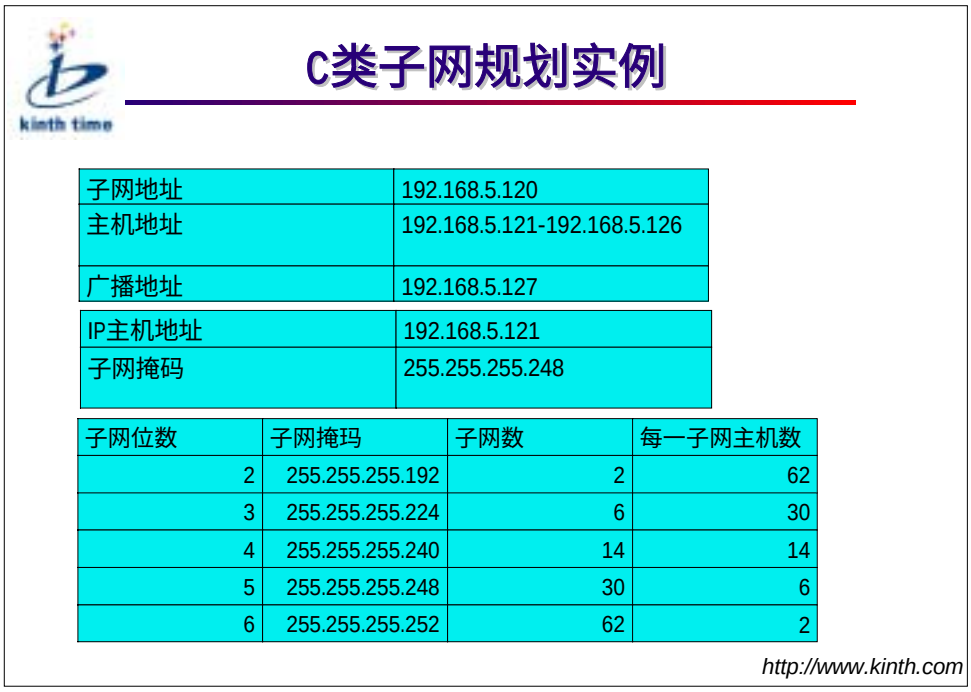


对于 B 类网络来说，如果子网有八位，则能提供 254 个子网，每个子网可容纳 254 台主机。

NO.Bits	Subnet Mask	No.Subnets	No.Hosts
2	255.255.192.0	2	16382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	

30		
12	255.255.255.240	4096
14		
13	255.255.255.248	8190
6		
14	255.255.255.252	16382
2		

7.3.10.2　C 类子网规划实例



对于图中 C 类网络来说，如果子网有五位，则能提供 30 个子网，每个子网可容纳 6 台主机。

NO.Bits　　Subnet　Mask　　No.Subnets　　No.Hosts

2　　255.255.255.192　　2　　62

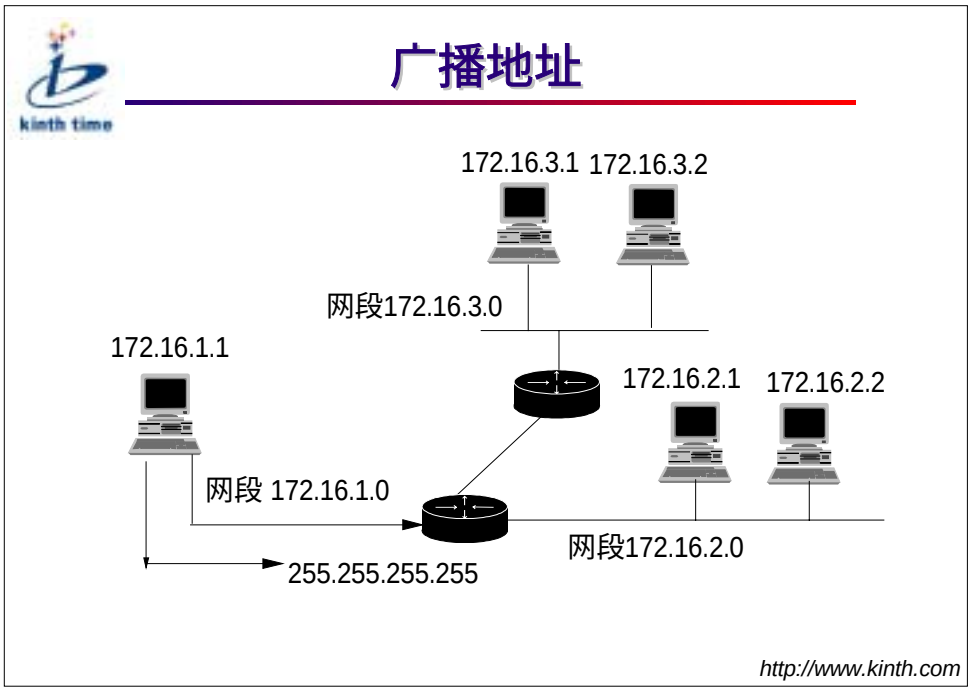
3　　255.255.255.224　　6　　30

4　　255.255.255.240　　14　　14

5　　255.255.255.248　　30　　6

6　　255.255.255.252　　62　　2

.3.11　广播地址



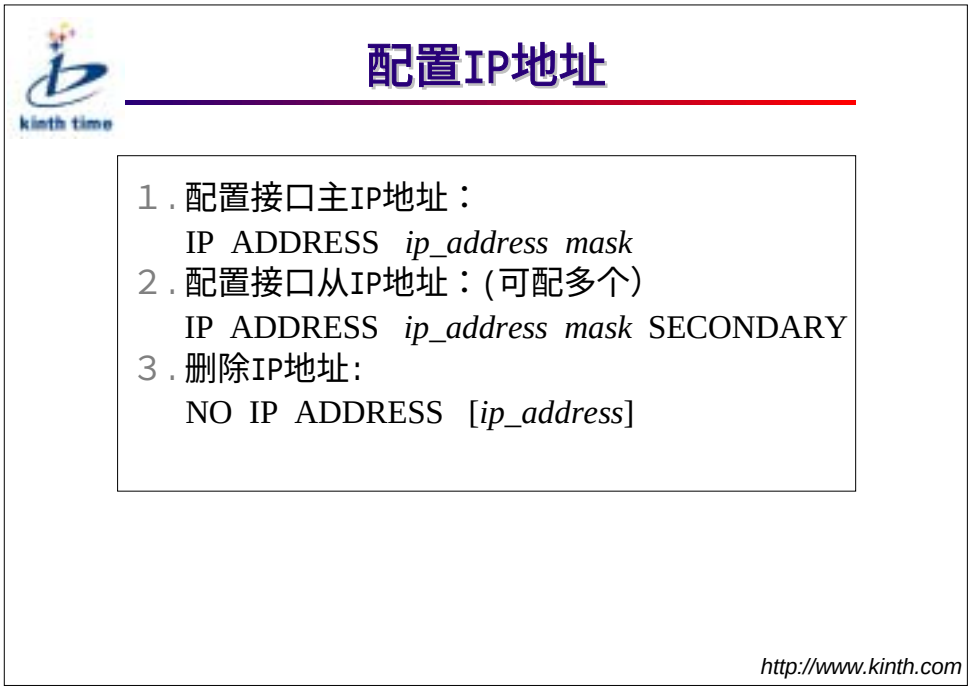
Internet 网支持广播地址。广播信息是那些要求每台主机都要收到的信息。广播地址有两种：

☞ 直接广播地址：有网络号但主机部分是全 1，可由路由器转发。

☞ 有限广播地址：全 1 的 IP 地址，即 255.255.255.255。不能被路由器传递，只能在本网段内广播。

.4　IP 地址配置及检验

.4.1　配置 IP 地址



路由器是通过掩码来识别 IP 地址的网络部分、主机部分。例如：路由器以太网口的 IP 地址是 129.9.30.42，掩码是 255.255.0.0，将 IP 地址与掩码相与，可知路由器以太网接口的 IP 地址的网络部分是 129.9.0.0，主机部分是 30.42。

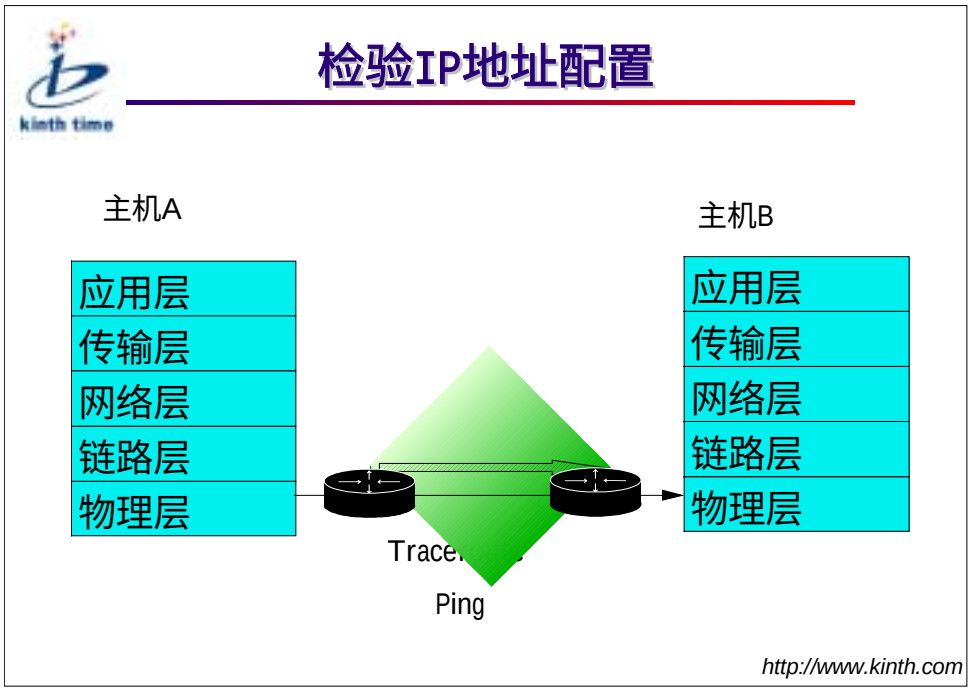
.4.2　静态域名解析

配置静态域名解析：

Quidway(config) #　host quidway1 129.102.10.1

当用户在 Quidway 路由器上配置了该命令，用户就可以使用 quidway1 来代替 129.102.10.1 这个 IP 地址了。

.4.3　网络检测工具

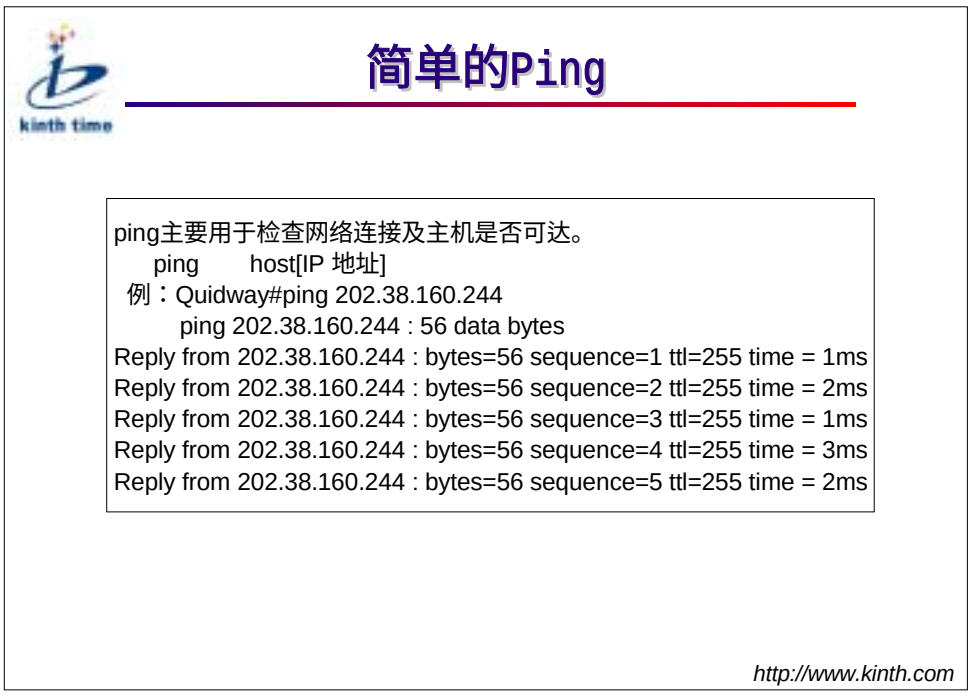


下面这些工具使您能检验 IP 地址配置的正确性：

Ping：是一种检验物理层、链路层、网络层连通性的测试工具。

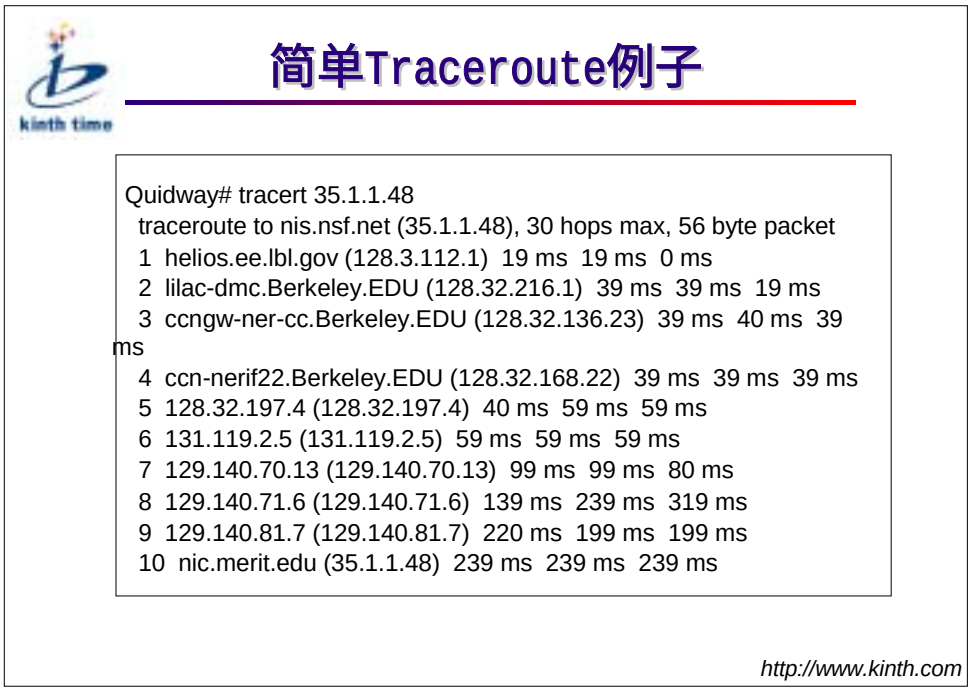
Tracert：是一种用来对远端网络或子网上设备和主机间的路由进行跟踪、探测的工具。

Ping 命令



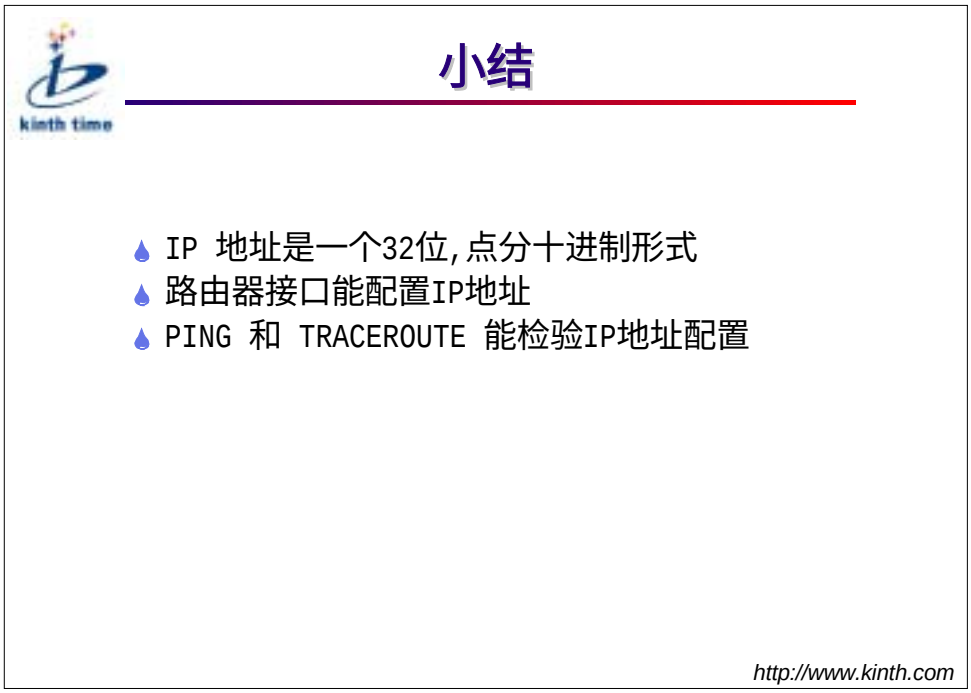
Ping 主要用于检查网络连接是否正常以及主机是否可达。

Traceroute 举例

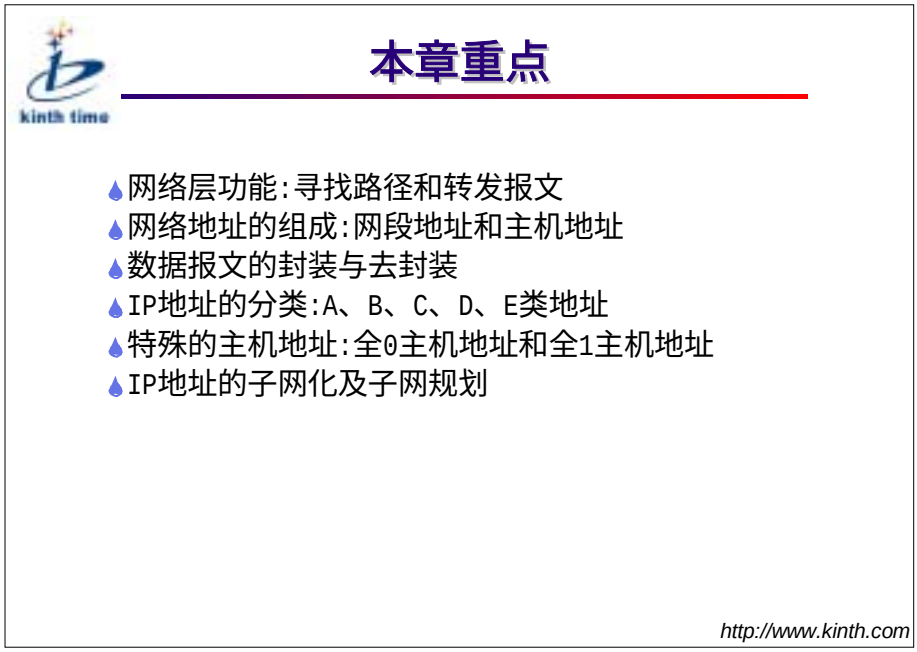


从上面结果可以看出从源主机到目的地都经过了哪些网关，这对于网络分析是非常有用的。

.5　小结


小结
IP 地址是一个32位,点分十进制形式
路由器接口能配置IP地址
PING 和 TRACEROUTE 能检验IP地址配置
http://www.kinth.com

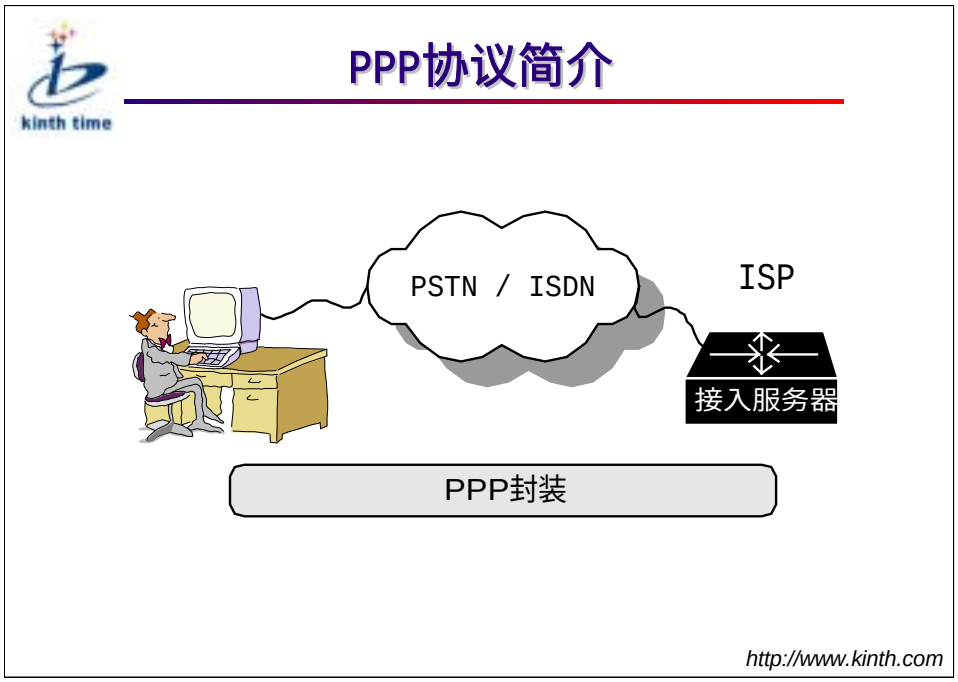
.6　本章重点


kinth time
本章重点
网络层功能:寻找路径和转发报文
网络地址的组成:网段地址和主机地址
数据报文的封装与去封装
IP地址的分类:A、B、C、D、E类地址
特殊的主机地址:全0主机地址和全1主机地址
IP地址的子网化及子网规划
http://www.kinth.com

第八章　　常见广域网协议及配置

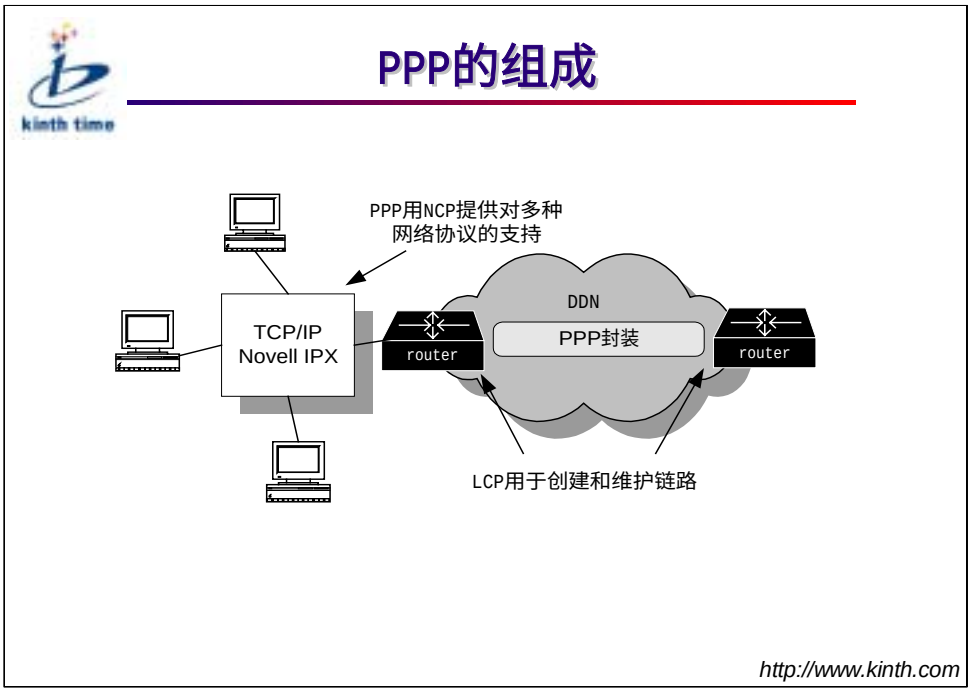
.1 PPP 协议及配置

.1.1　PPP 协议简介



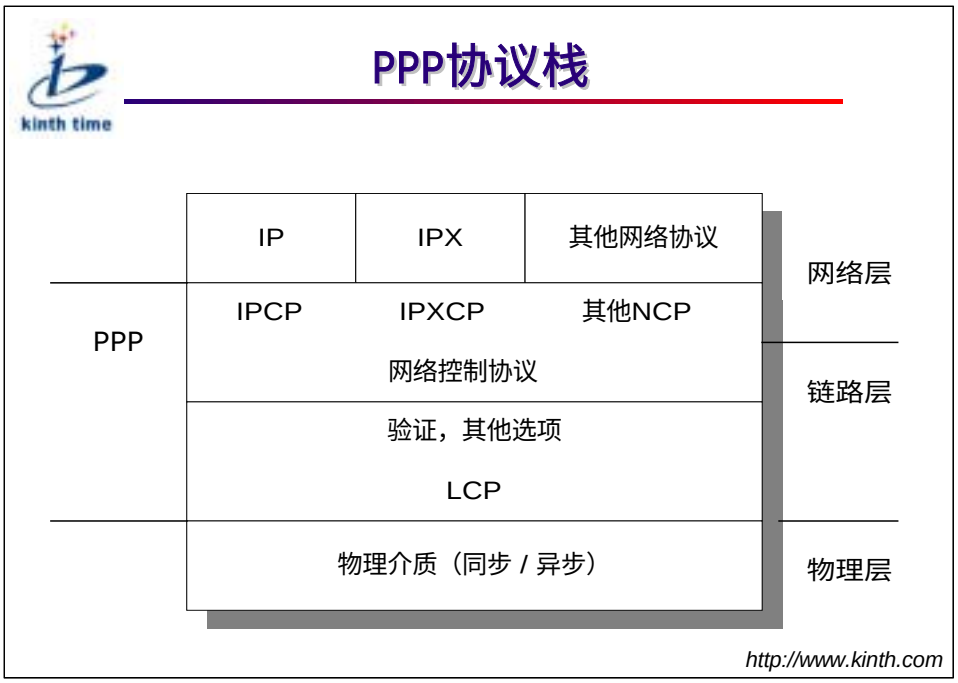
PPP 是一种得到广泛应用的广域网协议，它同时支持同/异步传输介质，也支持拨号方式。在我们的日常生活、工作中，拨号上网、DDN 专线等网络连接方式都是封装的 PPP 协议。

.1.2　PPP 的组成部分



PPP 包含一组协议，这些协议组合起来，就可以实现非常丰富的功能。PPP 协议族的一个重要组成部分是链路控制协议 LCP（Link Control Protocol），它用于协商链路的一些参数，负责创建并维护链路。
PPP 支持对多种网络层协议的封装。对于每一种网络层协议，它都提供一个对应的网络控制协议 NCP（Network Control Protocol），用来协商网络层协议的参数。

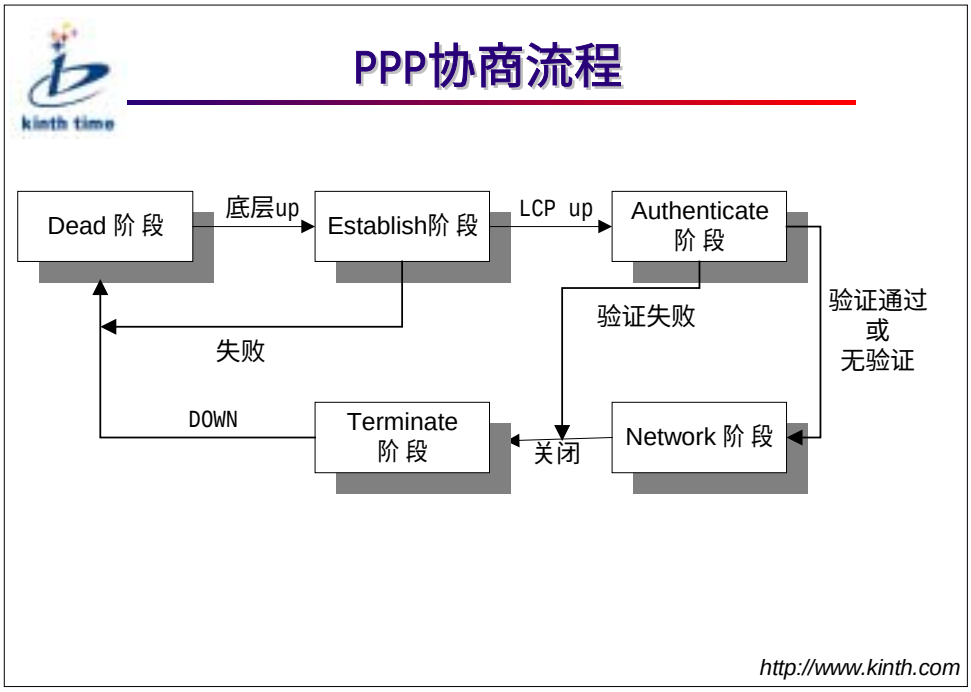
.1.3　PPP 协议栈



PPP 是一个分层结构。在底层，它能使用同步媒介（如 ISDN 或同步 DDN 专线），也能适用异步媒介（如基于 Modem 拨号的 PSTN 网络）。在数据链路层，PPP 在链路建立方面提供了丰富的服务，这些服务以 LCP 协商选项的形式提供。

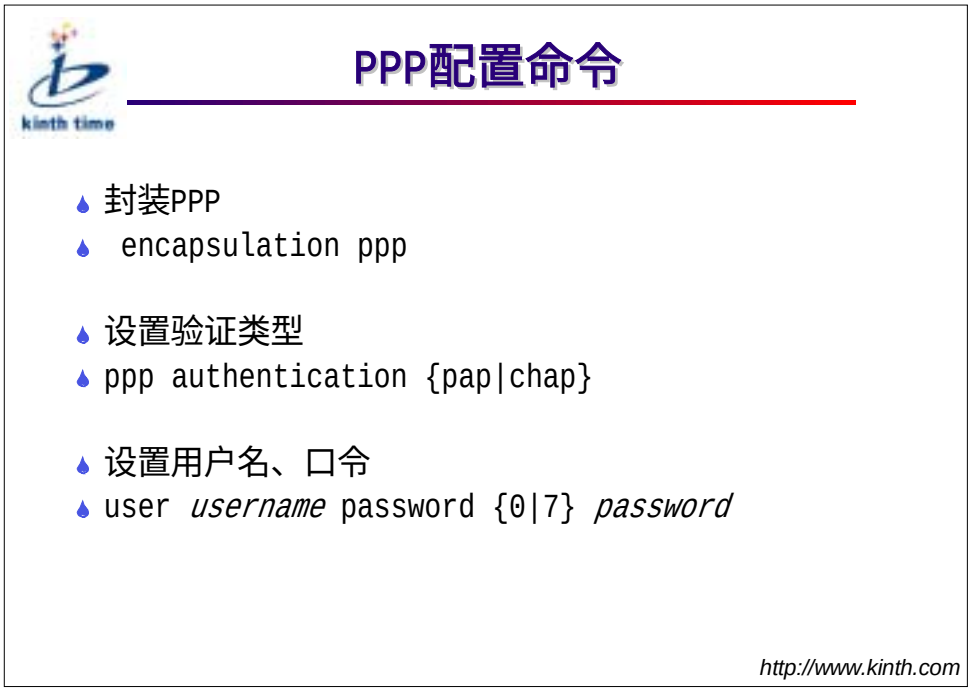
在上层，PPP 通过 NCPs 提供对多种网络层协议的支持。PPP 对于每一种网络层协议都有一种封装格式来区别它们的报文。

.1.4　PPP 协商流程



PPP 协商分为几个阶段：Dead 阶段、Establish 阶段、Authenticate 阶段、Network 阶段和 Terminate 阶段，在不同的阶段进行不同协议的协商。只有前面的协议协商出结果后，才能转入下一个阶段，进行下一个协议的协商。

.1.5　PPP 基本配置命令



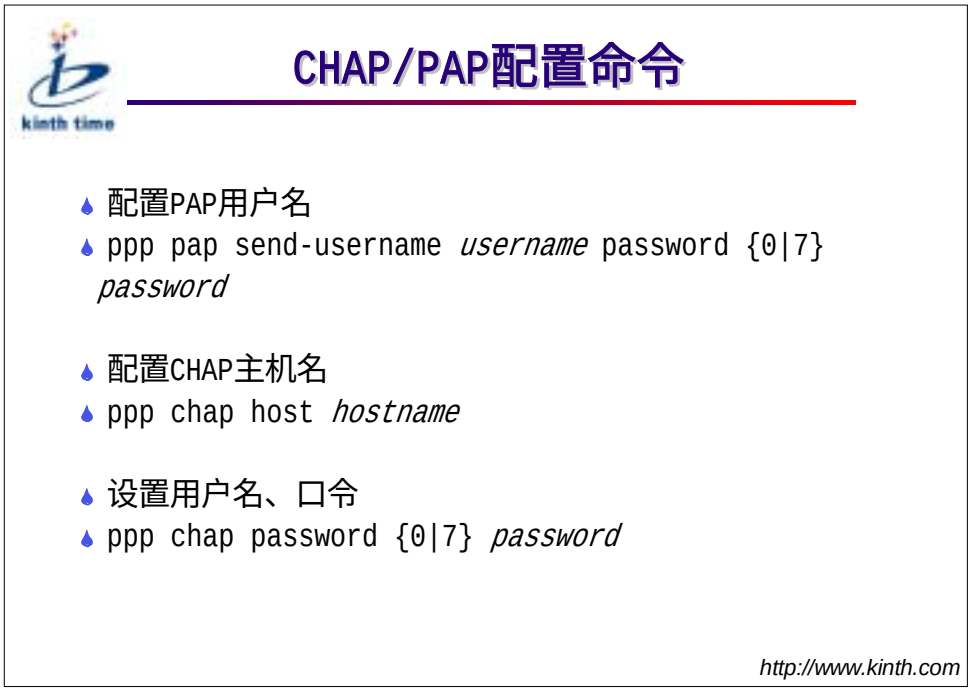
上面是 PPP 的基本配置命令。

encapsulation ppp 命令是接口配置命令，它指定一个广域网口的封装类型为 PPP。

ppp authentication 命令是接口配置命令，它指定验证方式，可选的验证方式为 PAP 和 CHAP。需要注意的是：验证是单向的，配置这条命令的一方作为验证方来验证对方。如果通讯的双方都要验证对方，则双方都应配置 ppp authentication 命令。

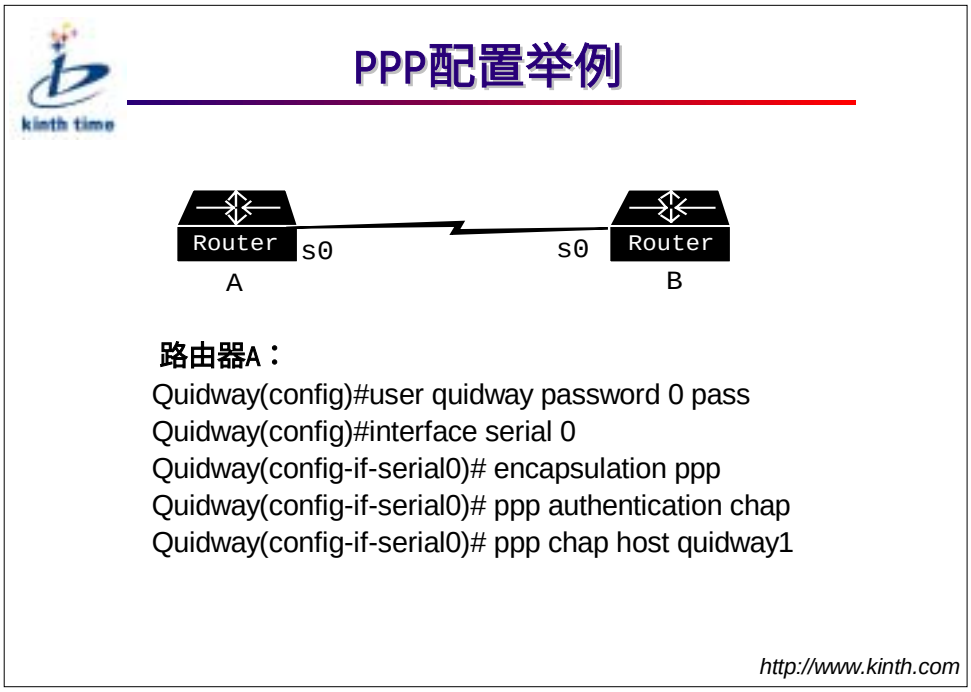
user 命令是全局配置命令，它配置验证所需的用户名和口令。命令字 password 后的可选参数中，0 表示以明文的方式显示后面的口令，7 表示以加密的方式显示后面的口令。

.1.6　CHAP/PAP 配置命令



PAP 是一种两次握手验证协议：
1、被验证方直接将用户名和口令传递给验证方；
2、验证方将这个用户名和口令与自己 user 命令配置的用户列表进行比较，如果相同则通过验证。
CHAP 是三次握手协议：
1、验证方生成一段随机报文传递到对方，并同时将本端的主机名附带上一起发送给被验证方；
2、被验证方接到对端对本端的验证请求时，便根据此报文中验证方的主机名和本端的用户表查找用户口令字，用此用户的口令对这段随机报文进行加密，然后与自己的用户名一起传递给对方；
3、验证方根据对方的用户名查找 user 列表，找到对应的口令，用这个口令对随机报文加密，与对方加密的随机报文比较，若相同则验证通过，否则失败。CHAP 不用在网络上传递口令，保密性较好。
PAP 有一条配置命令：ppp pap sentusername，是被验证方用来配置自己的用户名和口令。
CHAP 有两条配置命令：
☞ ppp chap hostname：配置 CHAP 的用户名；
☞ ppp chap password：配置 CHAP 的口令。

.1.7　PPP 配置举例



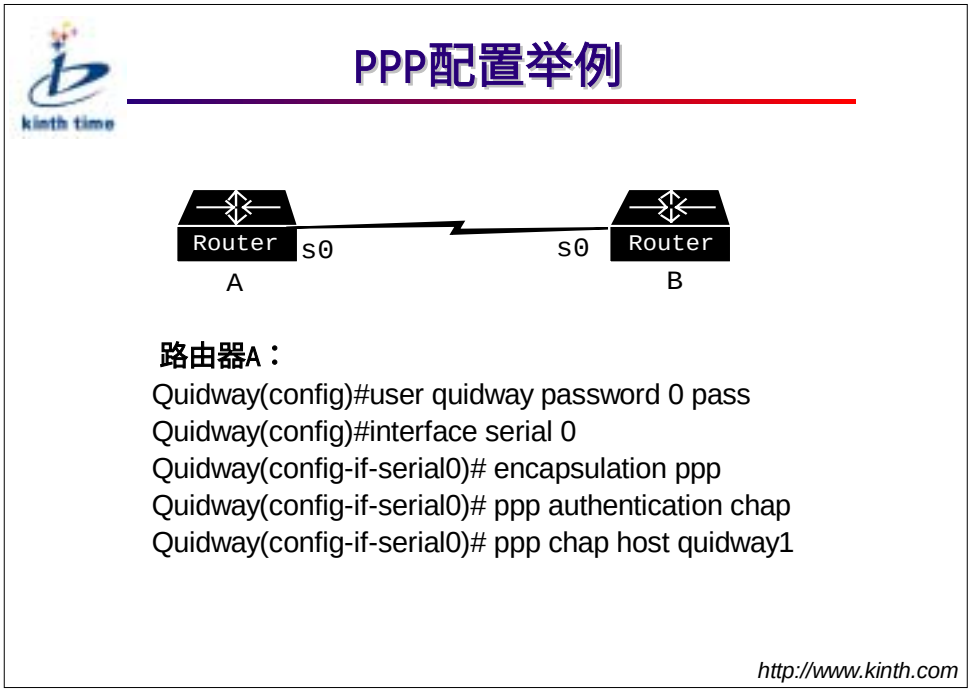
上面是 PPP 配置的一个简单例子。路由器 A 和 B 通过串口 0 直连，A 用 CHAP 对 B 进行验证。B 的用户名是 quidway，口令是 pass。在路由器 A，需要配置 user 命令，设置对方的用户名和口令。然后在串口 0 的接口配置状态下：

1、封装 PPP 协议；

2、配置以 CHAP 验证对方；

3、配置本端 CHAP 主机名。

PPP 配置举例（续）



在路由器 B，要在串口 0 的接口配置状态下：

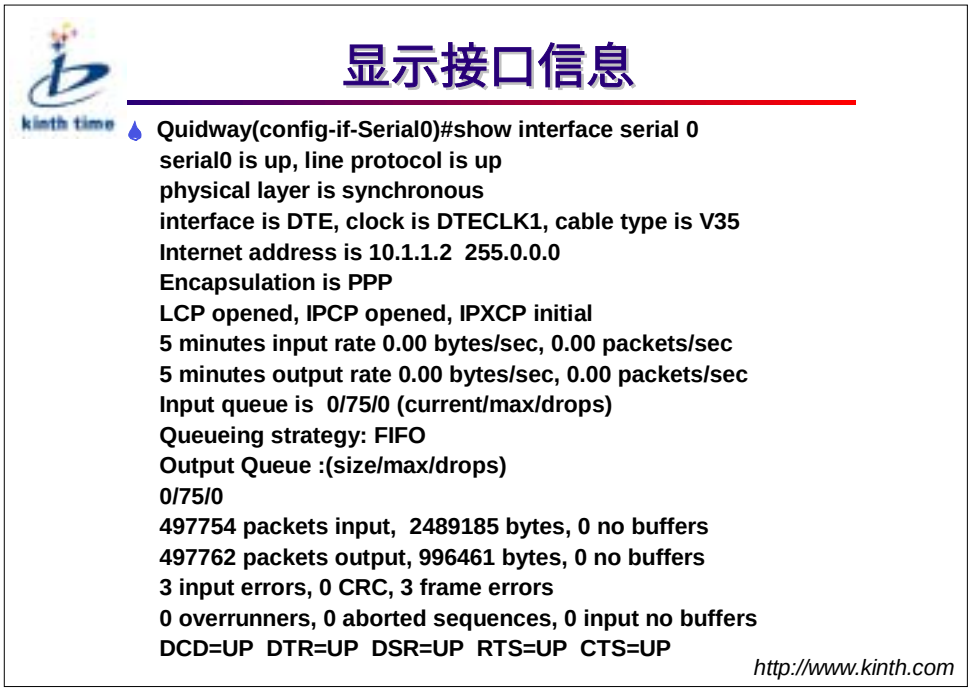
1、封装 PPP；

2、配置 CHAP 的用户名。

在全局配置模式下：

1、配置 用户列表。

.1.8　显示接口信息

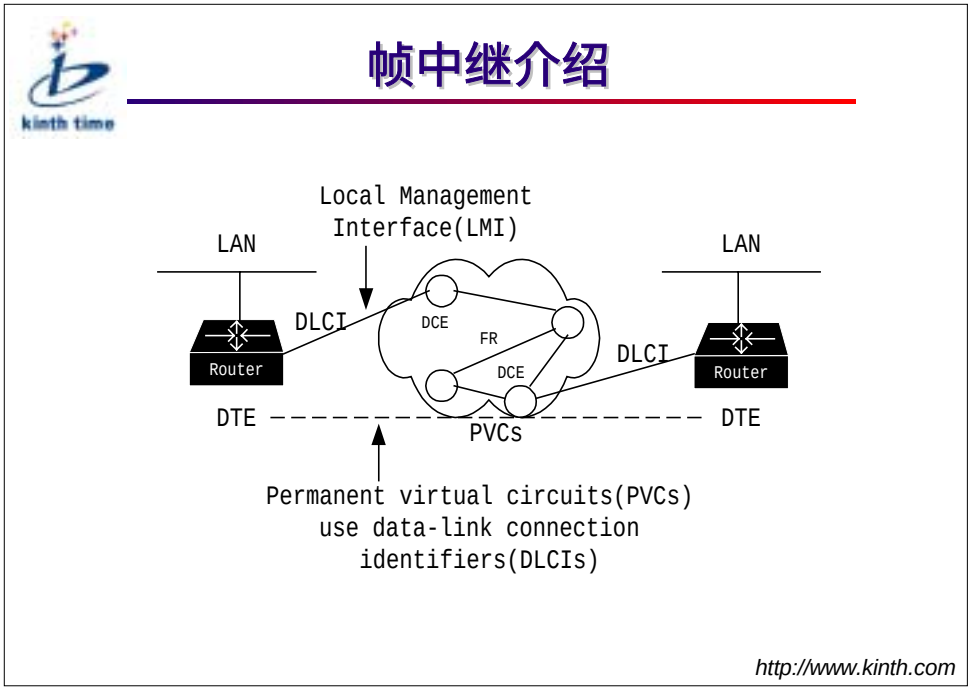


配置好 PPP 协议后，可以通过 show interface 命令检查 LCP 和 NCP 状态。

上面的例子显示的是同步串口的接口信息。

.2　帧中继协议及配置

.2.1　帧中继介绍



帧中继协议是在 X.25 分组交换技术的基础上发展起来的一种快速分组交换技术。概括地讲，帧中继技术是在数据链路层用简化的方法转发和交换数据单元的快速分组交换技术。帧中继技术是在通信线路质量不断提高，用户终端智能化不断提高的基础上发展起来的。

帧中继协议是改进了的 X.25 协议。相对于 X.25 协议，帧中继协议只完成链路层核心的功能，简单而高效。目前在许多国家，帧中继正在替代传统的复杂低速的报文交换服务。

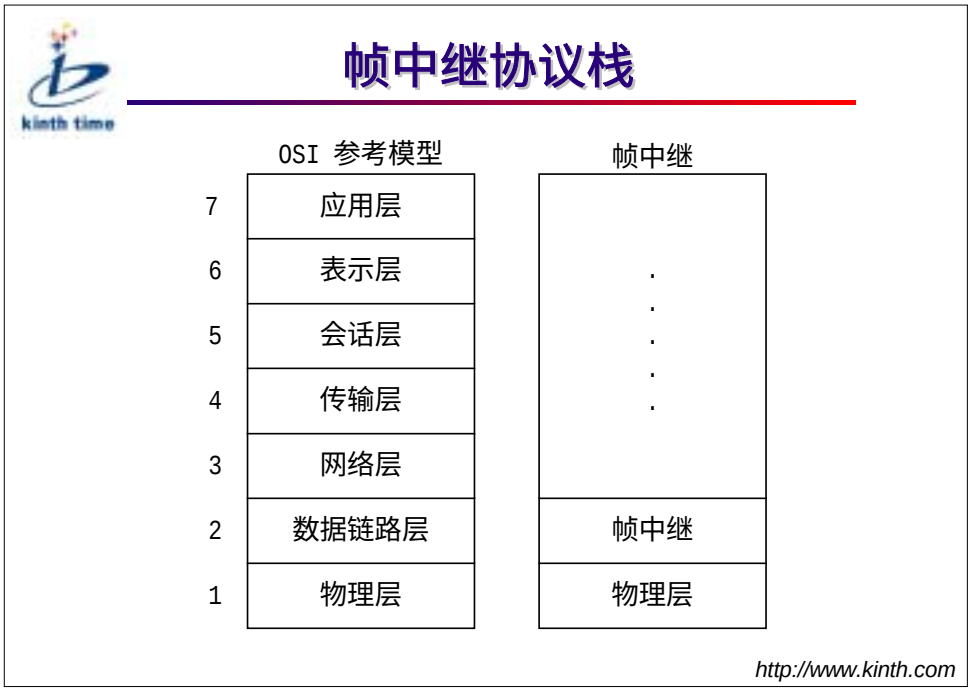
帧中继是基于虚电路的（Virtual Circuits, VCs）。由于帧中继较快的转发速度，而且帧中继数据单元至少可以 1600 字节，所以帧中继协议十分适合在广域网中连接局域网。用户的路由器封装帧中继协议，作为 DTE 设备连接到帧中继网中的 DCE 设备，即帧中继交换机。

目前比较常用的是帧中继的 PVC 业务。网络服务商为用户提供固定的虚电路连接，用户可以申请许多虚电路，通过帧中继网络交换到不同的远端用户。

DLCI（数据链路连接标识）用于标识每一个 PVC。通过帧中继帧中的地址字段的 DLCI，可以区分出该帧属于哪一条虚电路。

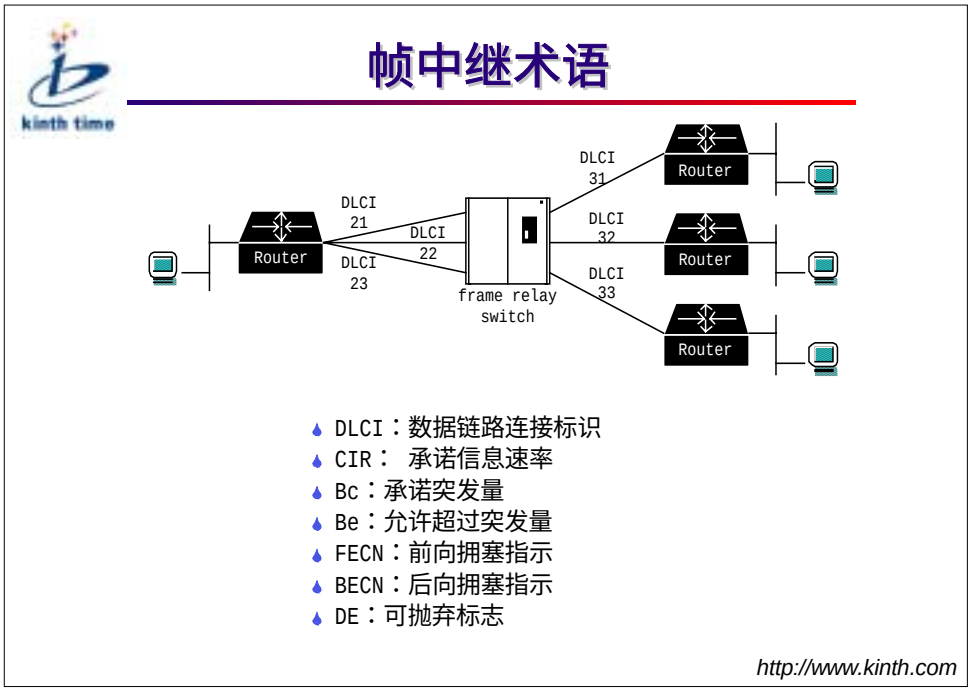
LMI（本地管理接口）协议用于建立和维护路由器和交换机之间的连接。LMI 协议还用于维护虚电路，包括虚电路的建立、删除和状态改变。

.2.2　帧中继协议栈



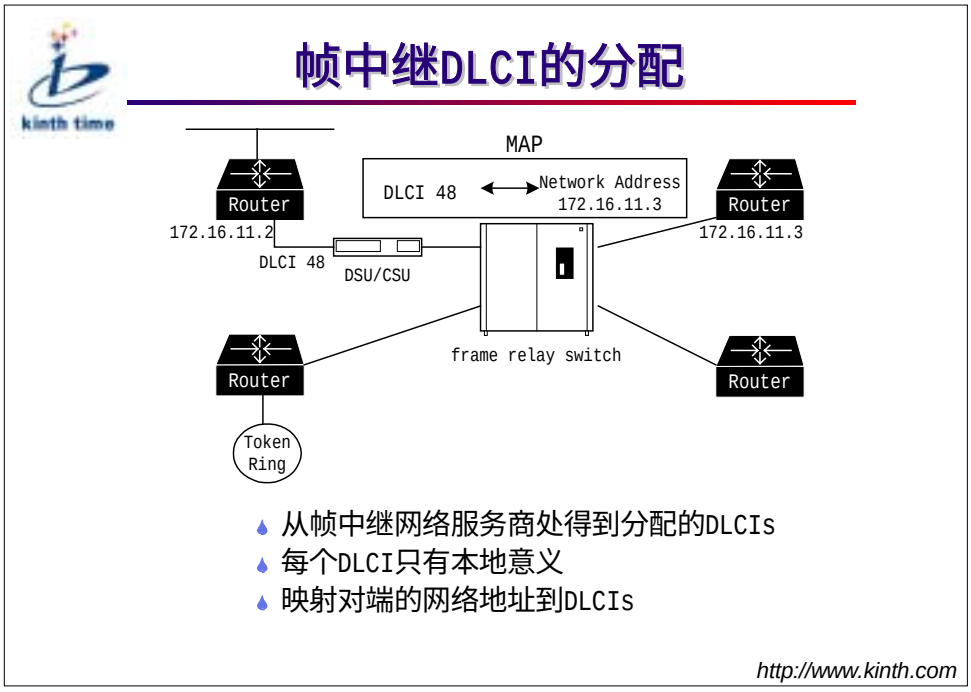
帧中继功能的核心部分对应 OSI 参考模型的下两层。
采用现代的物理层设施，例如光纤和数字传输线路，帧中继可以为终端站（典型的例子如局域网）提供高速的广域网连接。
因为工作在数据链路层，帧中继封装 OSI 栈中的上层信息。
帧中继与传统的广域网报文交换（例如 X.25）有一些共同之处。例如，在用户和网络设备之间的帧中继接口在统计复用的电路上使用 FIFO（先入先出）队列，一些逻辑连接（我们称之为虚电路）共用相同的物理连接。
与 X.25 不同的是，帧中继提供相对快速的服务：
☞ 帧中继转发速度范围较大，典型的帧中继连接转发速率为 56Kbps 或 64Kbps，一些设备可以提供 45Mbps 的转发速率；
☞ 帧中继是尽力传送的不可靠连接的服务，由于数字和光纤设施的进步，允许忽略错误检测、确认重传和流量控制等机制。

.2.3　帧中继术语



帧中继网络中的每一个连接都使用 DLCI 来标识。
每一个 PVC 可以配置自己的参数，典型的参数如下：
☞ CIR：承诺信息速率，单位 Kbps。这是交换机安全传播数据的最大保证带宽。超过这一速率限制的报文流量的 DE 位将被置 1。一旦遇到拥塞，DE 位被置位的报文将会被抛弃。许多网络服务提供零 CIR 的选择，该服务的费用比较少。如果选择零 CIR，应该有服务水平的协议来保证相当高百分比（95-99%）的数据流量会通过。
☞ Bc：承诺的突发量，帧中继网中控制报文流量的一个指标。在某一 CIR 下帧中继网络承诺可以接收和转发的最大数据量（以 bit 为单位）。
☞ Be：超过的突发量，帧中继网中控制报文流量的一个指标。当报文流量超过 Bc 后帧中继网络试图接收和转发的数据量。通常 Be 这部分流量传送出去的可能性比 Bc 这部分流量要低，因为 Be 这部分流量的 DE 位会被网络置位。
当转发队列中的报文长度超过一个阀值，可以认为发生了拥塞。当拥塞发生，在该队列中的报文的 FECN 位将被置位。如果拥塞持续下去，相反方向的报文的 BECN 位将被置位。
应该注意不同的服务商不总是提供这些可选参数。

.2.4　帧中继 DLCI 的分配



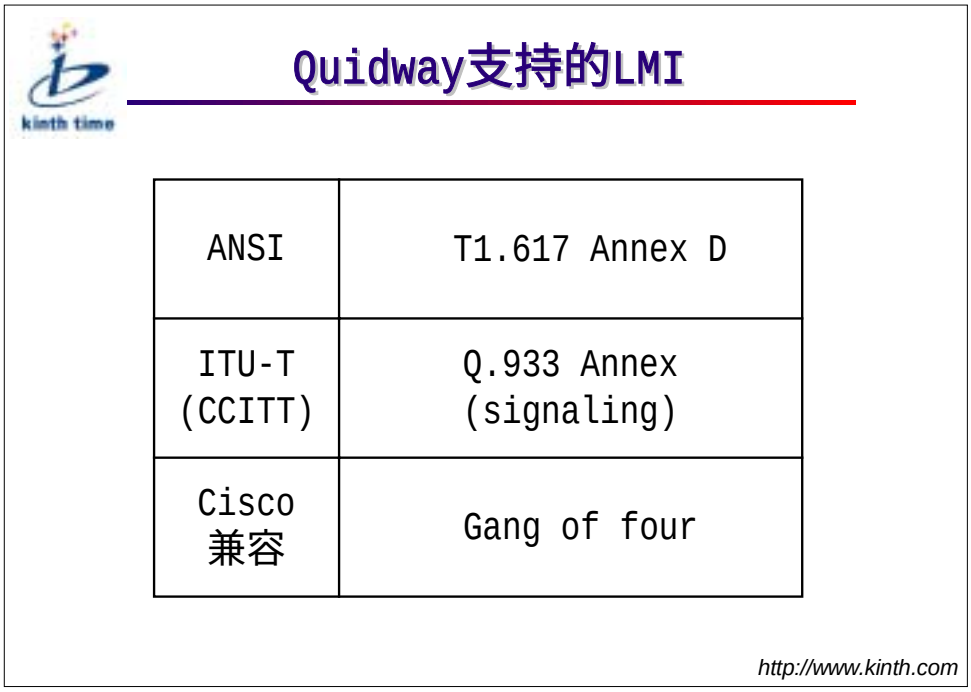
上图显示了帧中继网络中 DLCI 工作的情况。两个路由器被帧中继网络分别交换到远端。在图中帧中继网络中大交换机代表帧中继网络。帧中继网络作为一种公共设施，一般是由电话公司开发的，也可以通过自己私有的交换机组建帧中继网。对于任何一种方式，帧中继网络服务者为用户的路由器使用的 PVC 分配了 DLCI 号。

DLCIs 通常只具有本地意义，即任何一个本地应用的 DLCI 号可以被其它地点使用，但本地的 DLCI 号不可以重复。

一些 DLCI 代表特殊的功能，如 DLCI 0 和 1023 为 LMI 协议专用。

路由器管理者通过配置 MAP 把这些可用的 DLCI 号映射到远端的网络层地址。例如，可以映射到对端路由器一个接口的 IP 地址。在图中，路由器管理者配置了一个 MAP，建立了 IP 地址为 172.16.11.3 和 DLCI 值为 48 的 PVC 的映射。

.2.5　Quidway 支持的 LMI 格式



Quidway 路由器提供了三种帧中继 LMI 协议的支持：

ANSI —— ANSI（美国国家标准研究局）授权的 T1S1 委员会在 T1.617 附录 D 中描述了该帧中继信令标准。

Q933a —— ITU-T（国际电信联盟电信标准分部，前身为 CCITT）在 Q.933 附录 A 中描述了该帧中继信令标准。该组织在 20 世纪 80 年代中期把帧中继作为 ISDN 的一部分来开始研究，在路由器中把这种 LMI 成为 Q933a。

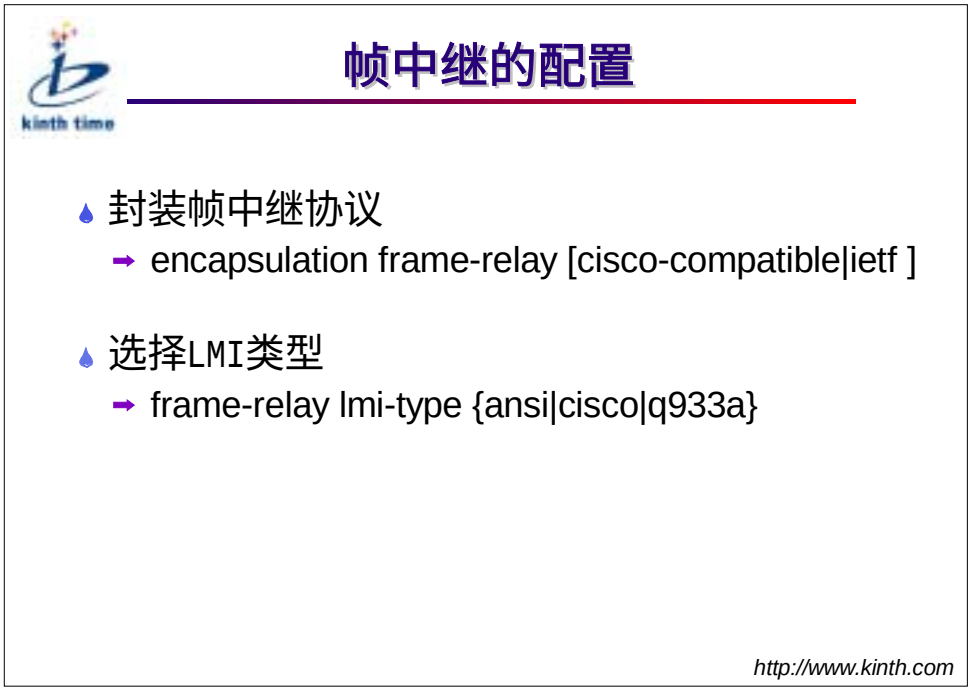
Cisco 兼容 —— 该标准是由 Cisco、DEC、NC 和 StrataCom 四家电信公司联合提出的，又名“gang of four”。在 20 世纪 90 年代初，这些公司联合起来致力于帧中继的研究工作，以加速产品的推广。

路由器管理者必须从这三种协议中选择一种合适的 LMI 协议类型连接到帧中继网络中，两边的 LMI 类型应该配置的一致。

Cisco 路由器也支持以上三种 LMI 类型，Quidway 路由器与之完全兼容。

.2.6　帧中继配置

1、协议封装及LMI类型选择



使用命令 encapsulation frame-relay 来指定链路层的封装类型为帧中继协议。通常是在连接到帧中继网络的路由器的同步串口上使用该命令来封装帧中继协议。

Quidway 支持两种链路封装格式：

☞ 缺省是 IETF 格式的封装。IETF 封装在 RFC1294/1490 中定义，该封装格式被很多厂家的路由器所支持。

☞ Cisco 兼容格式的封装。该封装格式由“gang of four”开发，一般 Cisco 的路由器支持该封装格式。Quidway 封装该格式可以与 Cisco 路由器互通。

封装格式可以在接口上指定，如本图所示。也可以在虚电路上指定，如下图所示。

使用命令 frame-relay lmi-type 来选择一种 LMI 类型。

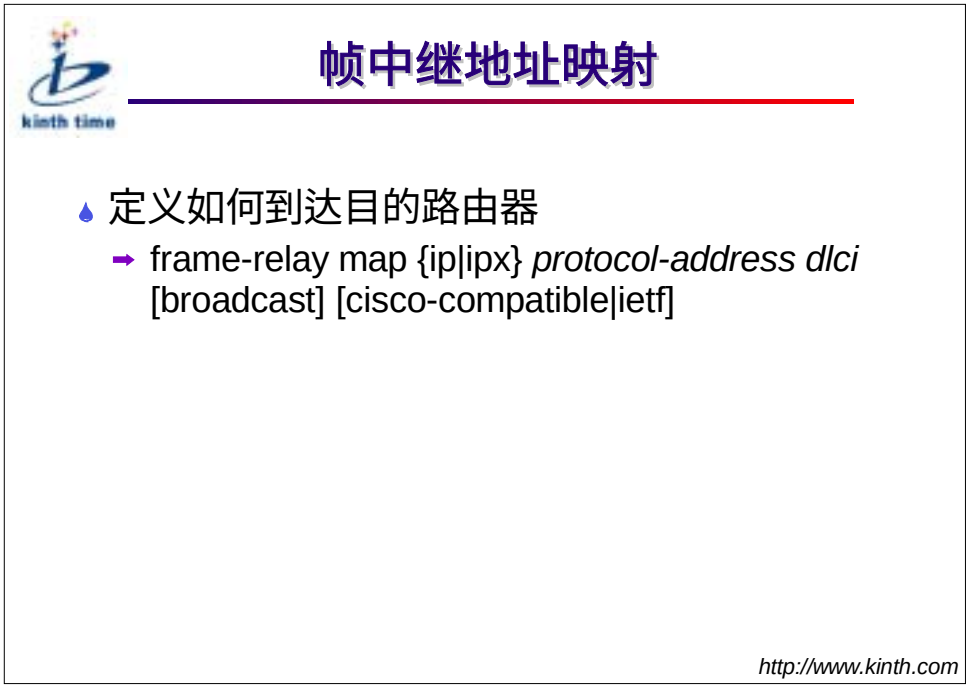
路由器必须配置一种合适的信令，以与帧中继交换机相匹配。Quidway 支持所有标准的 LMI 信令格式：

☞ ANSI —— ANSI T1.617 附录 D；

☞ ITU-T（或 Q933a）—— Q.933 附录 A；

☞ Cisco 兼容 ——“gang of four”定义的 LMI。

2、帧中继地址映射



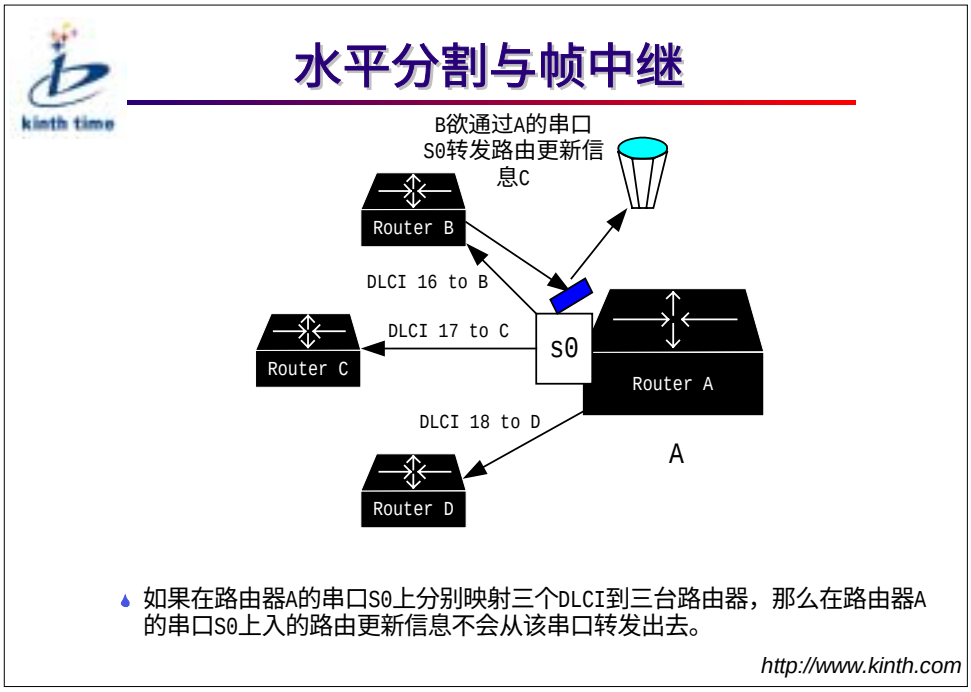
使用命令 frame-relay map 来配置一个静态 MAP，MAP 把目的网络协议地址映射到本地 DLCI。

frame-relay map

参数	描述
protocol	支持的协议：IP/IPX
Protocol-address	协议地址
DLCI	虚电路的 DLCI 号
broadcast	该 MAP 可转发广播报文（可选）
ietf	指定 IETF 封装格式（可选）
Cisco-compatible	指定 Cisco 兼容封装格式（可选）

如果没有通过 Inverse ARP 协议动态地建立本地虚电路到对端协议地址的映射，就需要使用该命令来显式的配置静态 MAP。

.2.7　水平分割与帧中继

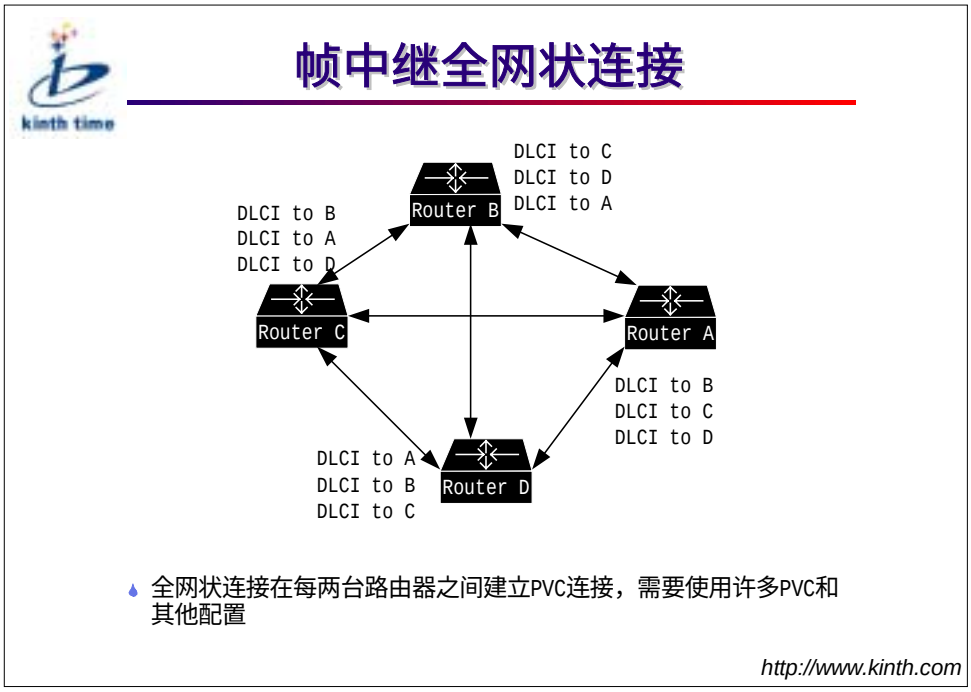


在 NBMA 环境当中，路由器如果要转发路由更新信息给传来的方向，就会产生问题。这种情况是由于连接到广域网中的路由器的串口上水平分割产生的作用。

采用水平分割，如果路由器从一个串口上收到路由信息，那么它不能从同一个串口将该路由信息传播回去。对于帧中继，这种情况适用于除了直接基于 IP 的所有路由协议，如 RIP、IGRP、Enhanced IGRP。

如果您从一个串口（例如路由器 A 的串口 0）映射一组 DLCI，只有从路由器 A 来或到路由器 A 去的更新信息可以穿过串口 0。如果路由器 B 试图发送更新信息通过路由器 A 到路由器 C 或 D，那么路由器 A 的水平分割过程将起作用。因为更新信息来自串口 0，由于水平分割，路由器 A 将不允许更新信息从串口 0 发送出去。

.2.8　帧中继全网状连接



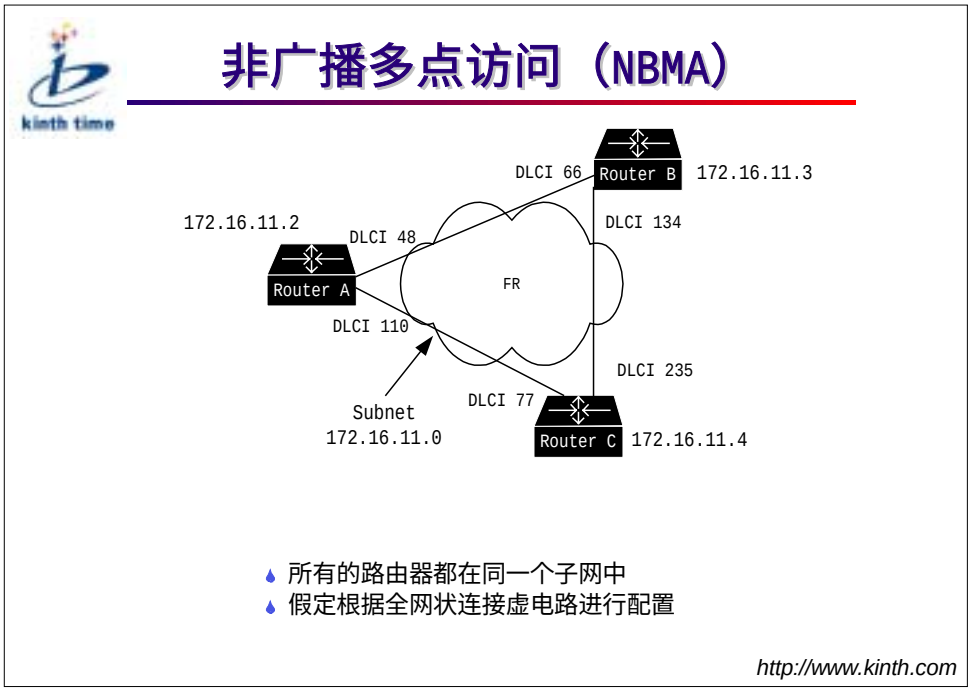
水平分割机制不允许路由器把从一个接口进来的更新信息再从该接口发送出去。我们可以建立一个全网状连接的帧中继连接，这需要为从每一个路由器到不同的目的路由器之间都建立一个帧中继数据连接，即在每一对路由器之间配置一个 DLCI。

但是，在帧中继广域网中这样连接路由器有几个关键的缺点：

☞ 路由器管理者必须从服务提供商那里申请许多帧中继的 PVC。服务提供商需要安装每一个分配的 PVC，该企业也因此将为每一个 PVC 付费，增大了企业的开支。

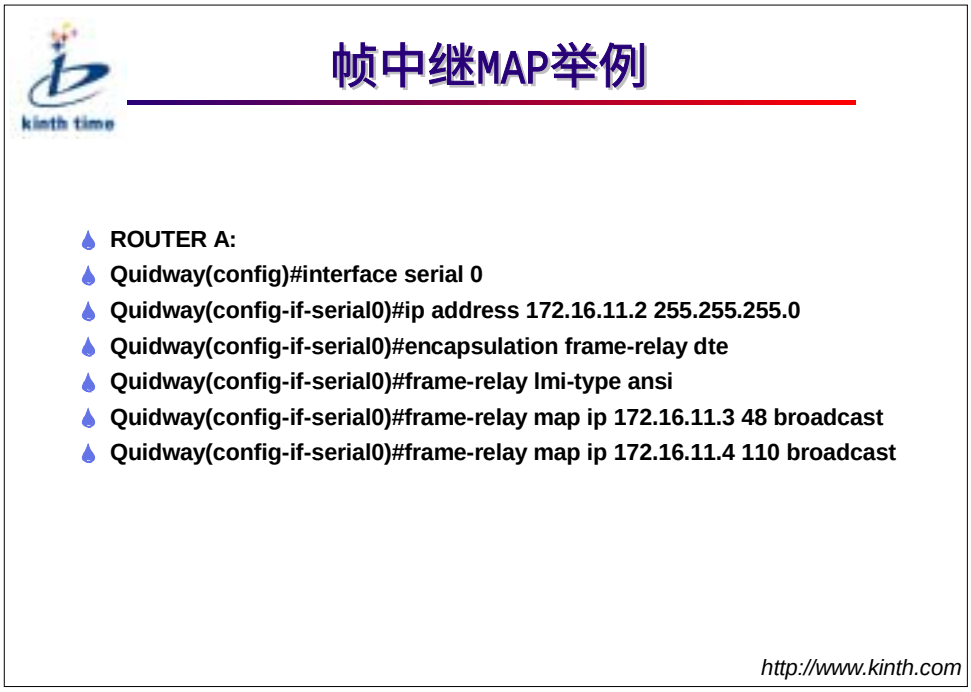
☞ 每一个路由器上的配置必须包含映射到每一个远端的 DLCI。为了到达每一个目的路由器，所有的路由器都必须使用全网状连接，这会需要大量的 MAP 配置。这种配置的建立和支持可能会相当困难。

.2.9　非广播多点访问（NBMA）



帧中继在广域网中一种模型称为 NBMA。NBMA 模型使所有 IP 地址在同一子网的路由器可以通过虚电路连接起来。因为帧中继不支持广播，所以必须把广播报文拷贝到各个虚电路，然后从各个虚电路转发出去。对于允许关闭水平分割的路由协议，可以把全网状连接改为部分网状连接。对于一些不允许关闭水平分割的路由协议，每一对路由器之间必须通过虚电路直接连接（全网状连接）。

.2.10　帧中继 MAP 举例



如下例：

encapsulation frame-relay —— 封装帧中继协议，选择封装类型为 IETF（缺省）

frame-relay lmi-type ansi —— 选择 LMI 类型为 ANSI

frame-relay map ip 172.16.11.3 48 broadcast

参数：

ip　　上层协议

172.16.11.3　　被映射的对端地址

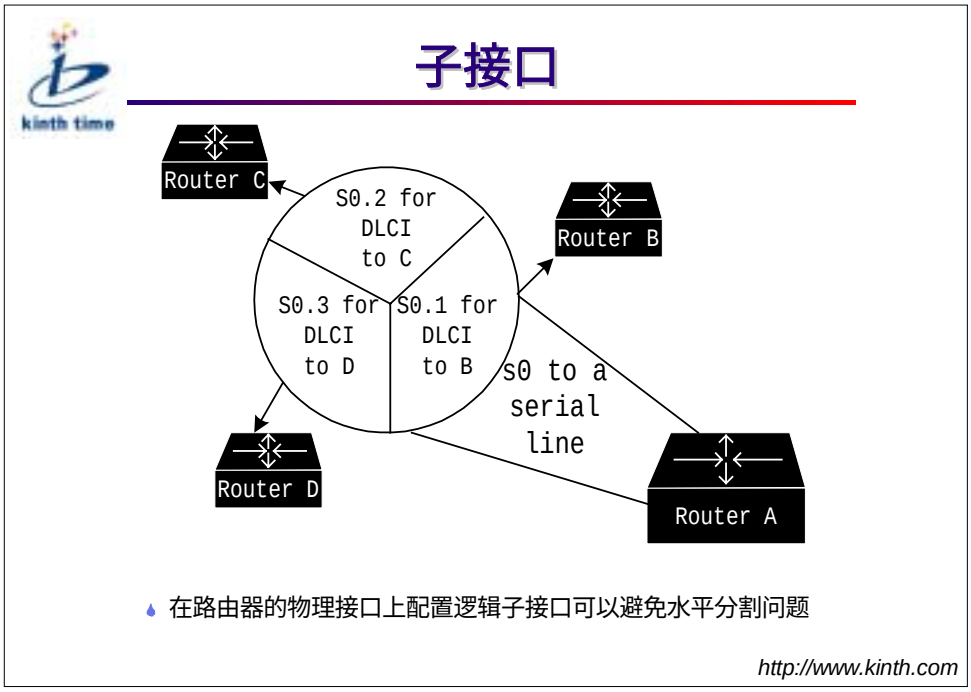
48　　到达对端的 DLCI 号

broadcast　　允许广播，如路由更新报文可以由此转发

去往 IP 地址为 172.16.11.3 的报文流量将使用 DLCI 48 发送到帧中继网中。广播的 IP 报文也将从串口 0 发送出去。

Quidway A 使用命令 frame-relay map 与每一个远端路由器之间配置了一个静态 MAP。在该例中，我们在三台路由器之间配置了全网状连接。因为路由协议要把更新信息广播到每一个对端，所以有必要限制在 NBMA 组中的路由器的数量。

.2.11　子接口*



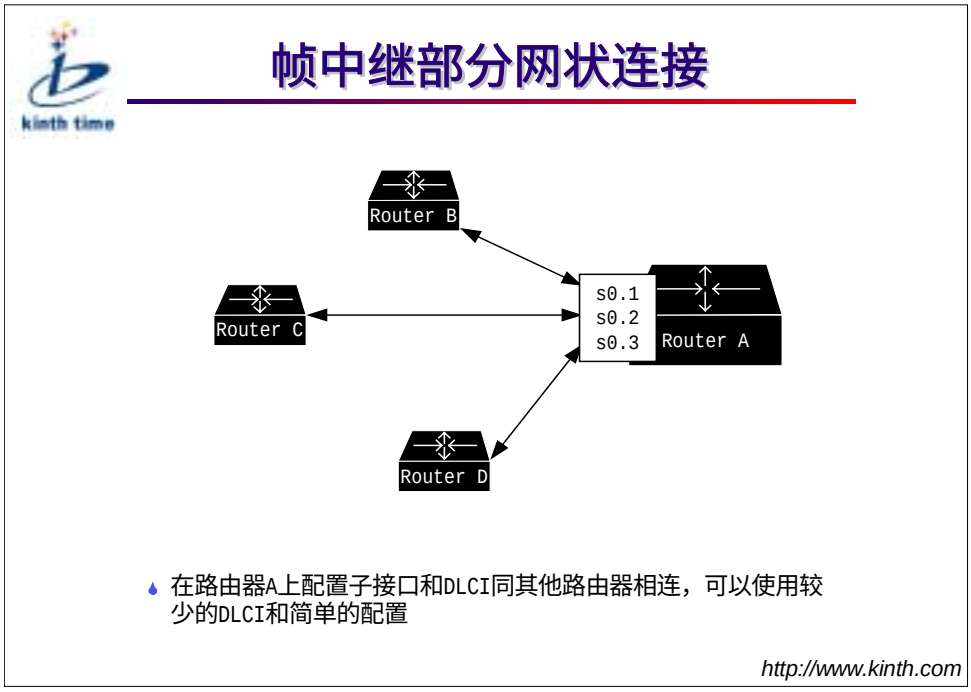
NBMA 广域网环境需要象局域网一样的多点访问操作。然而水平分割机制不允许多点访问的更新信息从一个接口进入，再从该接口出去。尽管路由器需要在水平分割的广域网中传播更新信息，但是通过提供全网状连接的方案是不切合实际的。

另外一个选择是在一个物理串口上建立一些虚拟接口，这些虚拟接口的逻辑结构称为**子接口**。

您可以在串口线路上定义这些逻辑子接口。每一个子接口使用一个或多个 DLCI 连接到对端的路由器。当您在子接口上配置了 DLCI 后，还需要建立目的端协议地址和该 DLCI 的映射。

这样，您虽然在路由器 A 上仅拥有一个物理串口 S0，但是在物理串口 S0 上您现在定义了 S0.1 子接口上的 DLCI 到路由器 B，S0.2 子接口上的 DLCI 到路由器 C，和 S0.3 子接口上的 DLCI 到路由器 D。

.2.12　帧中继部分网状连接*



当您在物理接口上定义了逻辑子接口，帧中继的连接就可以设计成部分网状连接。

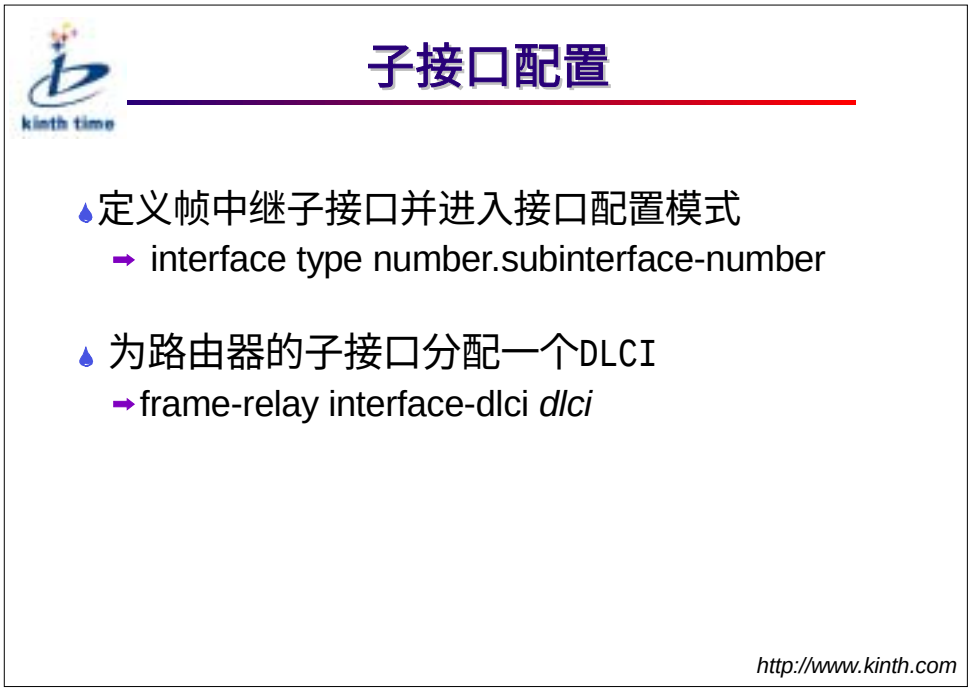
为了实现部分网状连接，您可以在一个子接口上配置一个 DLCI 映射到目的端协议地址，为每一个目的路由器配置一个子接口和一个 DLCI。

通过配置子接口，路由器可以实现相互连接，并能够转发更新信息。这样在路由器的一个物理接口上就可以避免水平分割带来的影响。

使用子接口，该路由器可以和每一个路由器实现连接，并且可以转发更新信息。在路由器 A 的物理接口 S0 上水平分割将不再起作用。

这样您就可以实现与每一台路由器的连接，而不必在每两台路由器之间配置一条帧中继的 PVC 了。所有路由器的配置都变得十分简单，不再需要为每一对路由器之间都配置一个 DLCI 了。

.2.13　子接口配置*



在您使用和配置帧中继子接口之前，您必须在某个物理接口上已经封装了帧中继协议。帧中继子接口的命令和描述见下，第一个命令定义了子接口。

命令 1：

interface type　number.subinterface-number　{point-to-point | multipoint}

参数	说明
type	帧中继支持的接口类型，通常是一个同步串口。
number.subinterface-number	Number 指明了物理接口号； Subinterface-number 是子接口号。
point-to-point | multipoint	子接口类型。

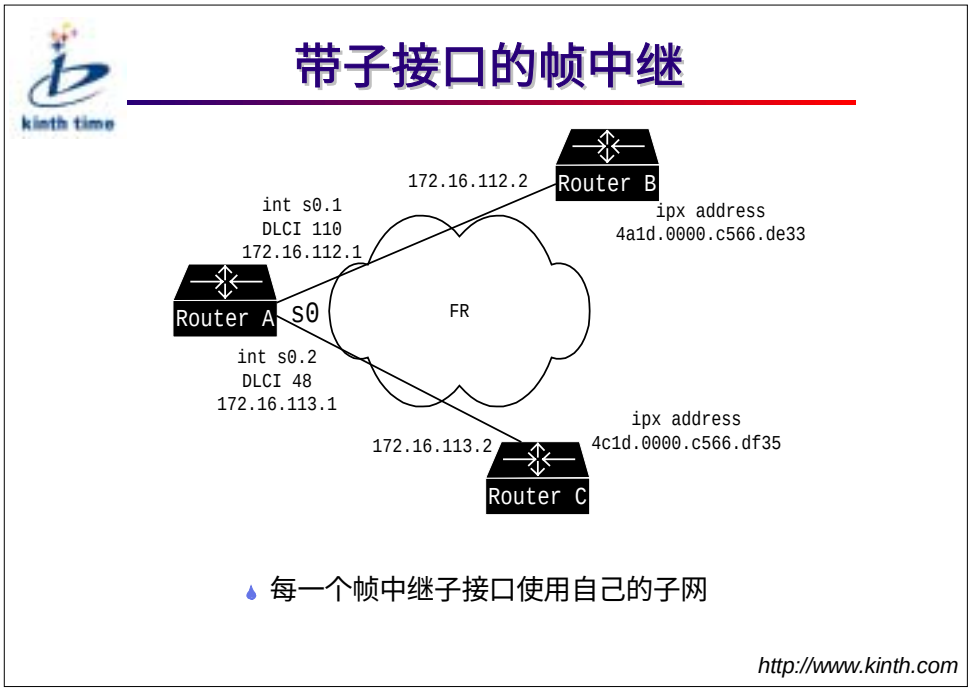
命令 2：

frame-relay　interface-dlci　*dlci* [broadcast]

参数	说明
dlci	定义的虚电路号
broadcast	可选，表示可以在该虚电路上转发广播信息

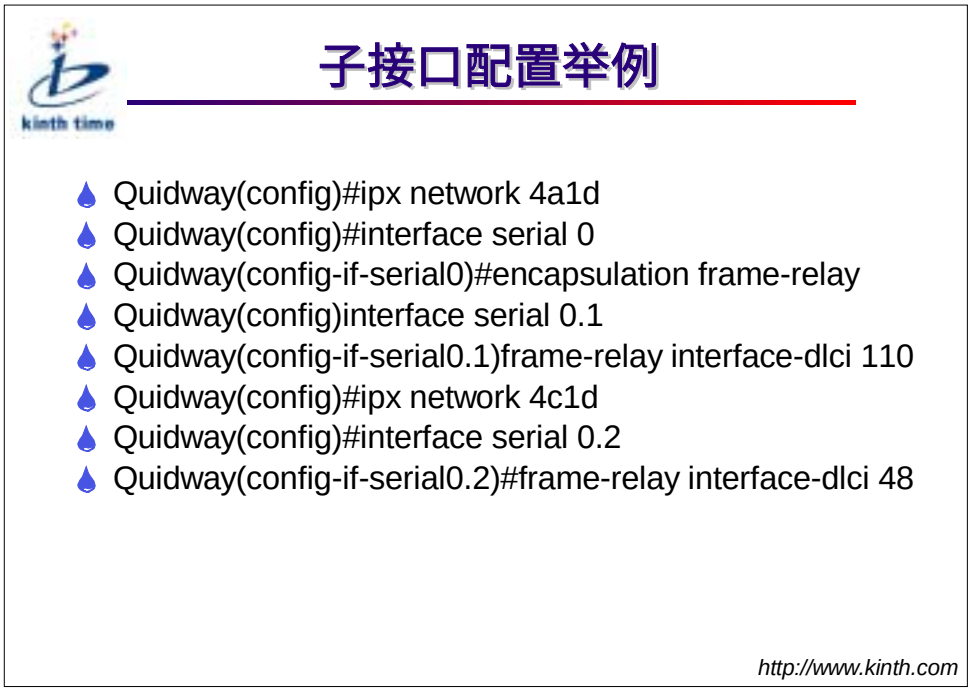
除了以上命令，您还需要在子接口上配置网络地址。

.2.14　带子接口的帧中继*



如图所示，当您配置了子接口和帧中继 DLCI，该网络结构将对不同子接口上的虚电路连接使用不同的子网网段。
在路由器 A 上，子接口 S0.1 对于 IP 子网段 172.16.112.0（假设 8 位掩码）使用 DLCI 110。对于子接口 S0.2，DLCI 48 连接到 172.16.113.1。
这种设计与前面 NBMA 环境下的点对点的两两连接不同。在那种配置中，所有的路由器都在同一个子网段中，使用全网状连接的 PVC。
但是当您使用帧中继的子接口时，只有相连接的两个路由器的子接口在同一子网段。这个帧中继配置中包含有许多子网。
子接口上的 DLCI 承载一个或几个目的协议地址。
在路由器 A 上，DLCI 110 连接到目的 IPX 地址网段为 4a1d 的网络。DLCI 48 连接到目的 IPX 地址网段为 4c1d 的网络。
下一小节显示了实现该网络结构的具体配置命令。
在该配置下，全网状连接已经不再是必要的了。在右侧的两台路由器之间不再需要直接的帧中继连接设施。这种结构和配置与全网状连接相比节省了大量开支。

.2.15　子接口配置举例*



配置帧中继子接口，先从前面介绍的命令开始。这个例子假定帧中继 LMI 类型为缺省 Q933a。在这个例子中：

命令 interface s 0.n point-to-point 在物理接口 S0 上建立了一个子接口。

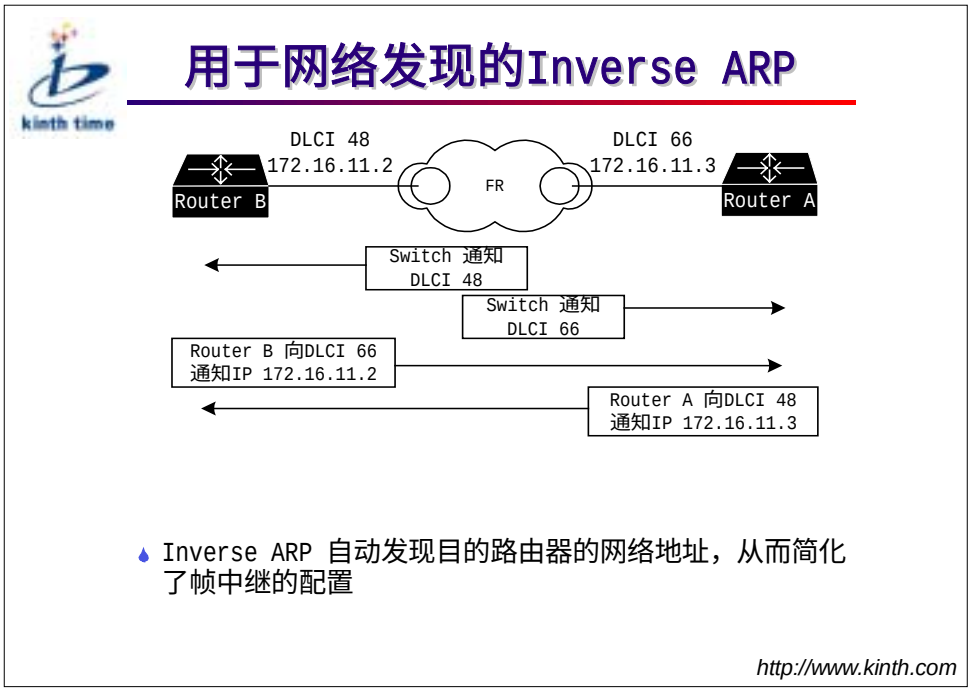
参数	**说明**
n	子接口号，从 1 到 4294967293。
point-to-point	建立的子接口的类型

命令 frame-relay interface-dlci nn broadcast 在该子接口上配置一个 DLCI。

参数	**说明**
nn	由帧中继网络服务商分配的本地唯一的 DLCI
broadcast	指明广播报文可以使用该 DLCI 到目的地址

命令 ipx network nnnn 配置 IPX 网络号。

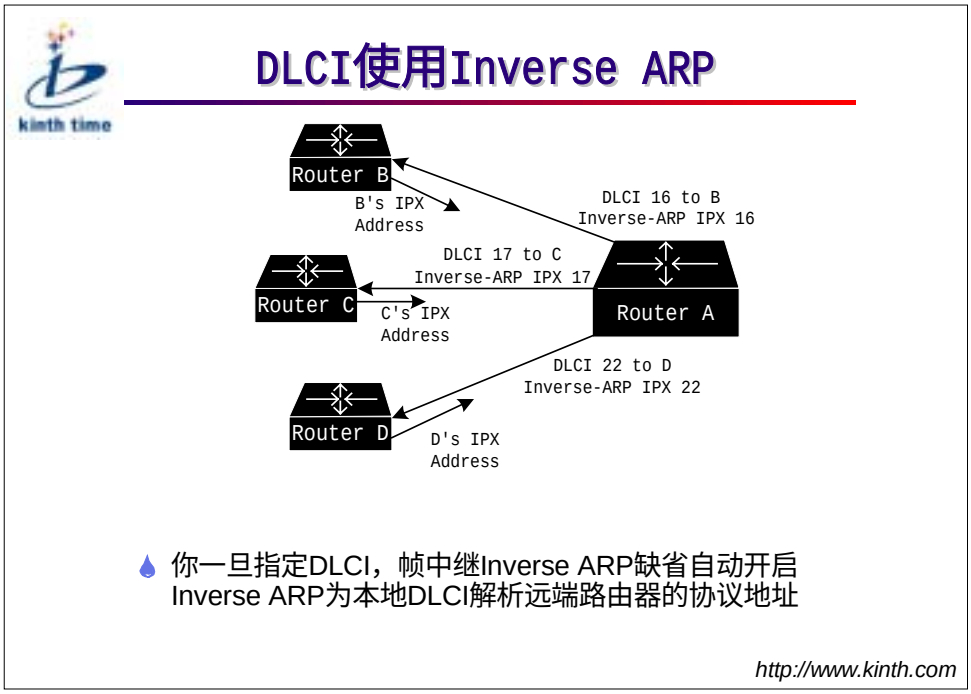
.2.16　用于网络发现的 Inverse ARP



无论是 NBMA 环境还是子接口 DLCI 下，通过使用 Inverse ARP 协议可以简化配置。通过 Inverse ARP 协议，在 NBMA 或子接口环境中路由器只需要知道自己的网络协议地址。

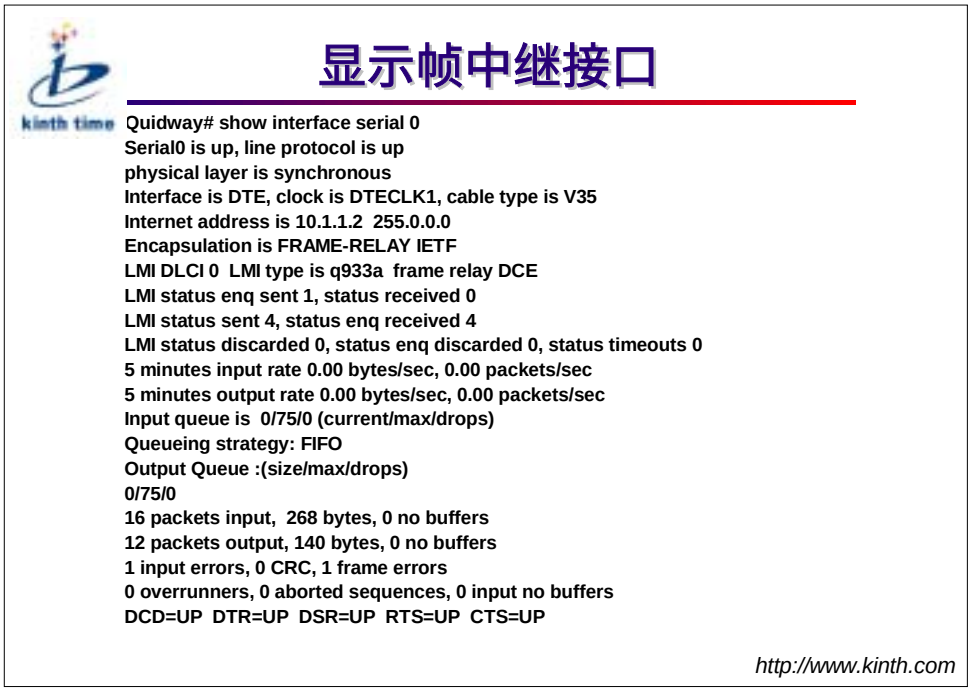
路由器通过 LMI 信令从帧中继交换机得到虚电路信息，然后通过在每个虚电路上发送 Inverse ARP 消息得到对端路由器的网络协议地址。

.2.17　DLCI 使用 Inverse ARP



您一旦为帧中继指定了 DLCI，Inverse ARP 协议将自动启动。
通过 Inverse ARP 协议，路由器将自动解析对端的网络协议地址。路由器首先发出 Inverse ARP 请求，把自己的网络地址和虚电路号传给对端。对端回应 Inverse ARP 响应，携带对端的网络地址和虚电路号。
因为帧中继 Inverse ARP 协议缺省是自动启动的，如果您需要在某个 DLCI 上禁止 Inverse ARP 协议，需要执行命令 no frame-relay inverse-arp。使用 Inverse ARP 协议，就可以不用手工的配置静态的地址映射，Inverse ARP 协议可以动态地生成地址映射，简化了路由器的配置。

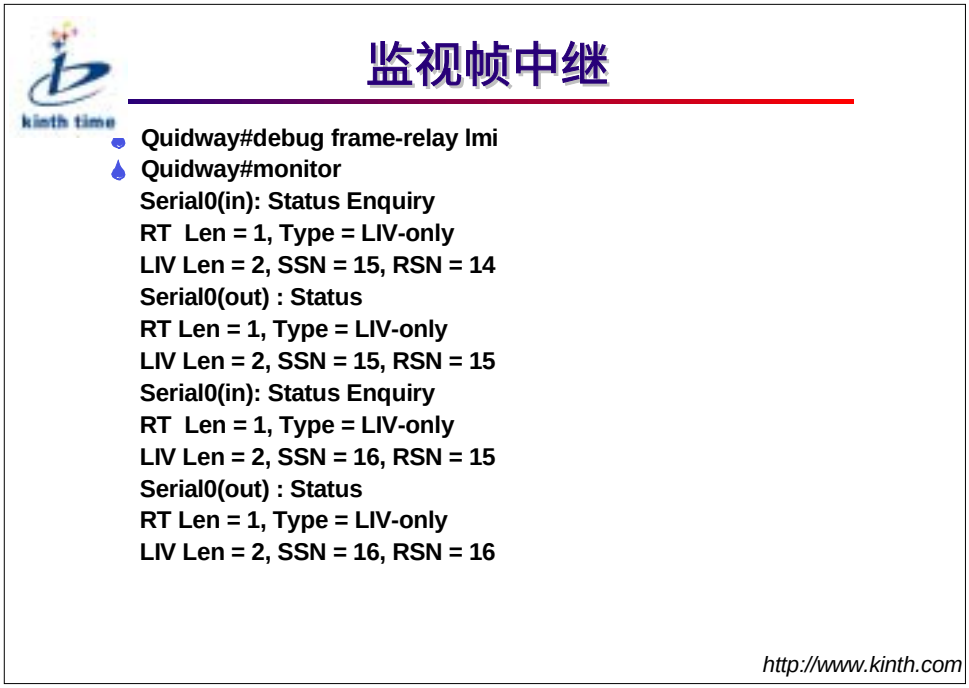
.2.18　显示帧中继接口



使用命令 show interface serial n 显示接口信息和帧中继的一些配置。上图是该命令一个显示结果的例子。

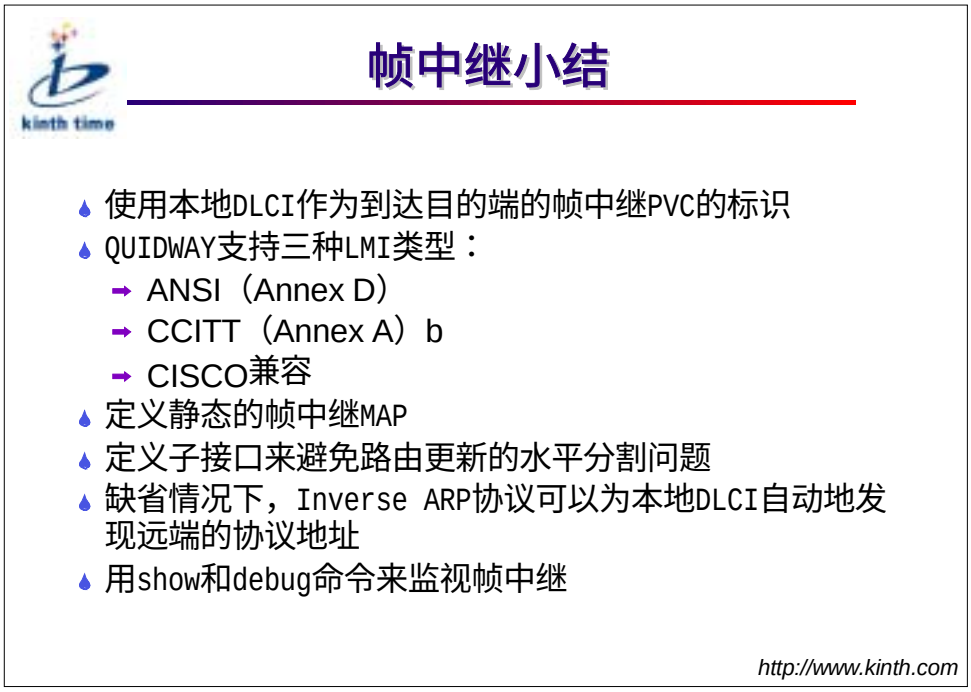
其他的 show 和 debug 命令用来调试路由器帧中继协议的运行情况，具体可以参见《用户手册》。

.2.19　监视帧中继

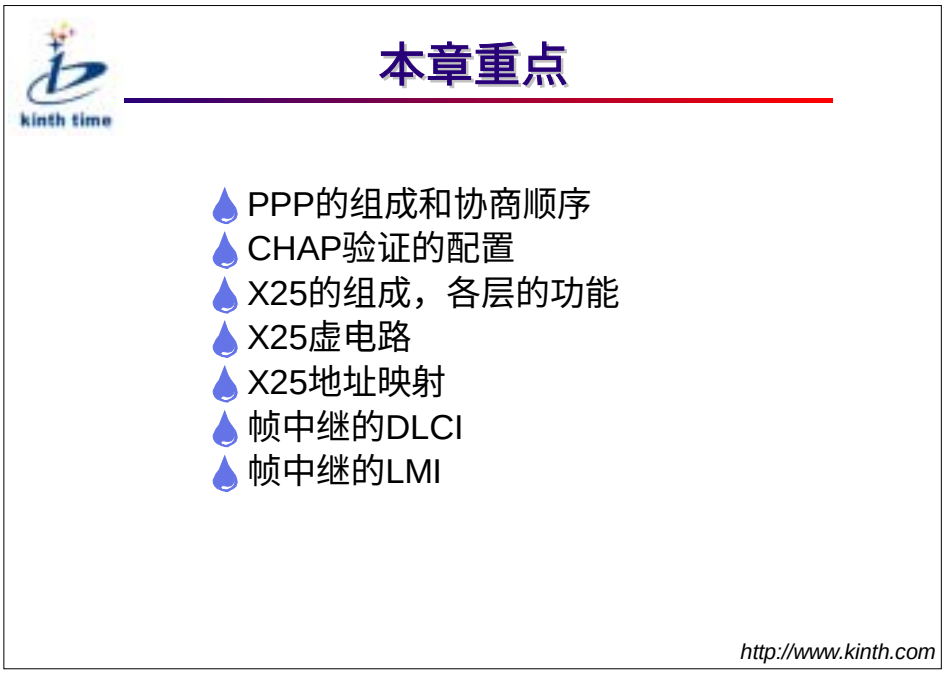


如果在路由器的某接口上封装了帧中继协议，路由器需要和帧中继交换机交换 LMI 报文。可以使用命令 show frame-relay lmi 来显示路由器和交换机之间的 LMI 交换报文的信息。
上图显示了执行该命令后，屏幕打印出来的 LMI 消息的调试信息。

.2.20　帧中继小结

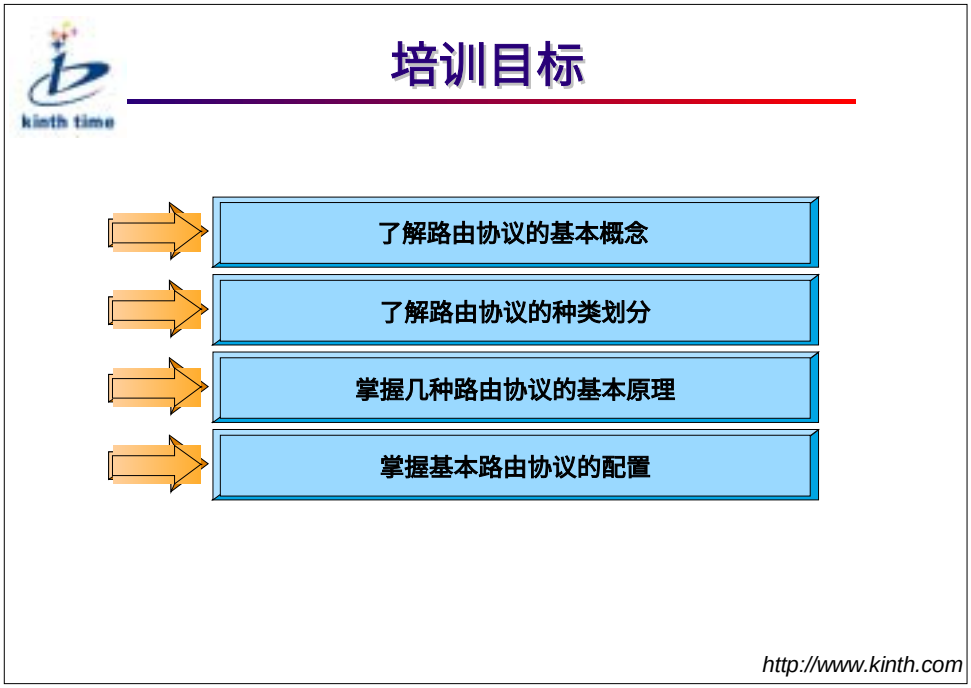

帧中继小结
使用本地DLCI作为到达目的端的帧中继PVC的标识
QUIDWAY支持三种LMI类型：
ANSI（Annex D）
CCITT（Annex A）b
CISCO兼容
定义静态的帧中继MAP
定义子接口来避免路由更新的水平分割问题
缺省情况下，Inverse ARP协议可以为本地DLCI自动地发现远端的协议地址
用show和debug命令来监视帧中继
http://www.kinth.com

.3　本章重点


kinth time
本章重点
PPP的组成和协商顺序
CHAP验证的配置
X25的组成，各层的功能
X25虚电路
X25地址映射
帧中继的DLCI
帧中继的LMI
http://www.kinth.com

第九章 路由协议

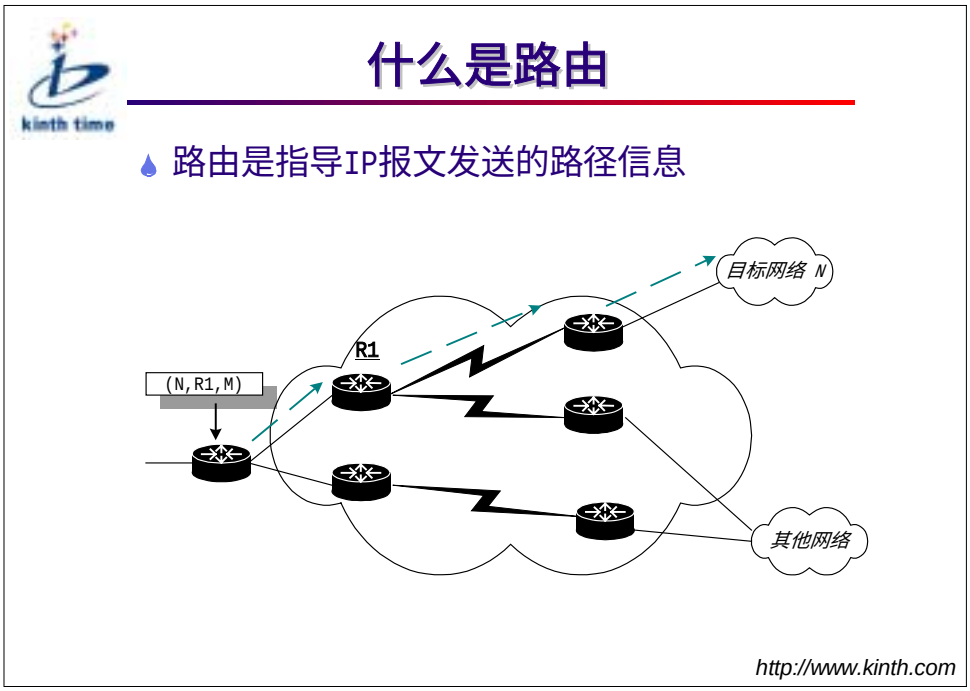
.1 培训目标



本章讲述路由协议及其配置，内容主要包括路由协议共通的基本概念和原理，并依据不同的原则对现有路由协议进行种类划分，以使读者对路由协议具有整体概念和基本了解。同时介绍了静态路由和几种基本的动态路由协议的原理和配置方法，以及一些典型配置的实例说明。

.2 路由的基本概念及算法

.2.1 什么是路由



在基于 TCP/IP 的网络中，所有数据的流向都是由 IP 地址来指定的，网络协议根据报文的目的地址将报文从适当的接口发送出去。而**路由**就是指导报文发送的路径信息。

就像实际上生活中交叉路口的路标一样，路由信息在网络路径的交叉点（路由器）上标明去往目标网络的正确途径，网络层协议可以根据报文的目的地查找到对应的路由信息，把报文按正确的途径发送出去。一般一条路由信息至少包含以下几方面内容：目标网络，用以配置报文的目的地址，进行路由选择；下一跳，指明路由的发送路径；Metric、路由权，标示路径的好环，是进行路由选择的标准。

例如，在上图中路由器上有一条去往目标网络 N 的路由，下一跳是 R1。所有经过此路由器的去往目标网络 N 的报文都被转发到路由器 R1 上去，再重复这种路由过程，直到到达正确的目的地。

.2.2 路由的分类

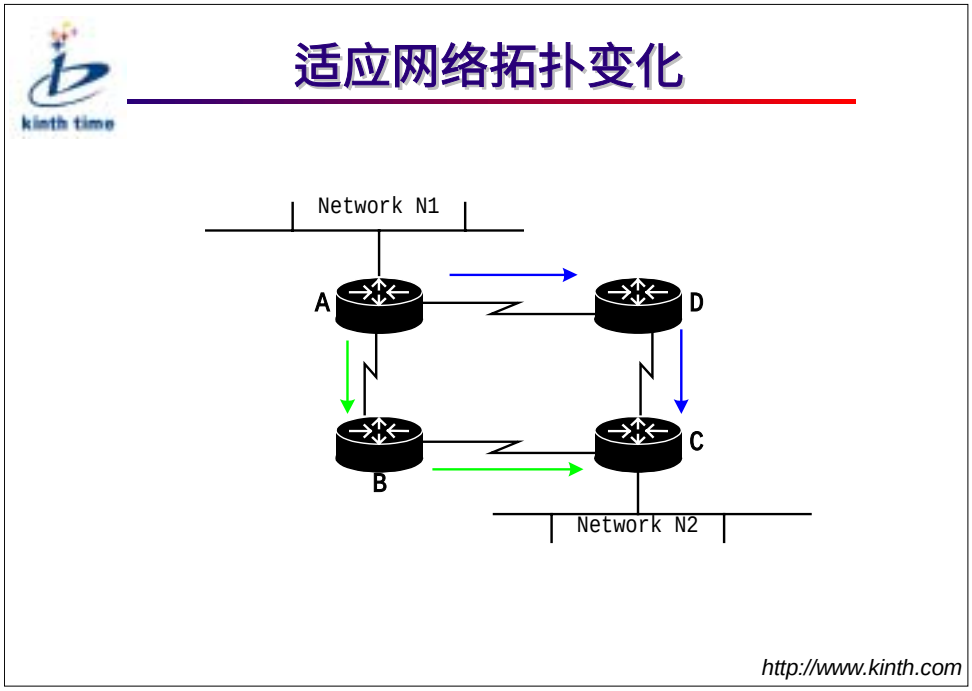
通常情况下，指导 IP 转发的路由信息可以通过如下三种不同的途径来获得：

静态路由 —— 由系统管理员手动配置的到目标网络的唯一路径，当网络结构发生变化时也必须由系统管理员手动的修改配置。但合理的使用静态路由可以改进网络的性能，为重要的应用保存带宽。

缺省路由 —— 由系统管理员手动配置的一种特殊路由，可以将所有找不到匹配路由的报文转发到指定的缺省网关。

动态路由 —— 由动态路由协议从其他路由器学到的到达目标网络的发送路径，可以根据网络结构的变化动态地更新路由信息。

.2.3 对网络拓扑变化的适应性



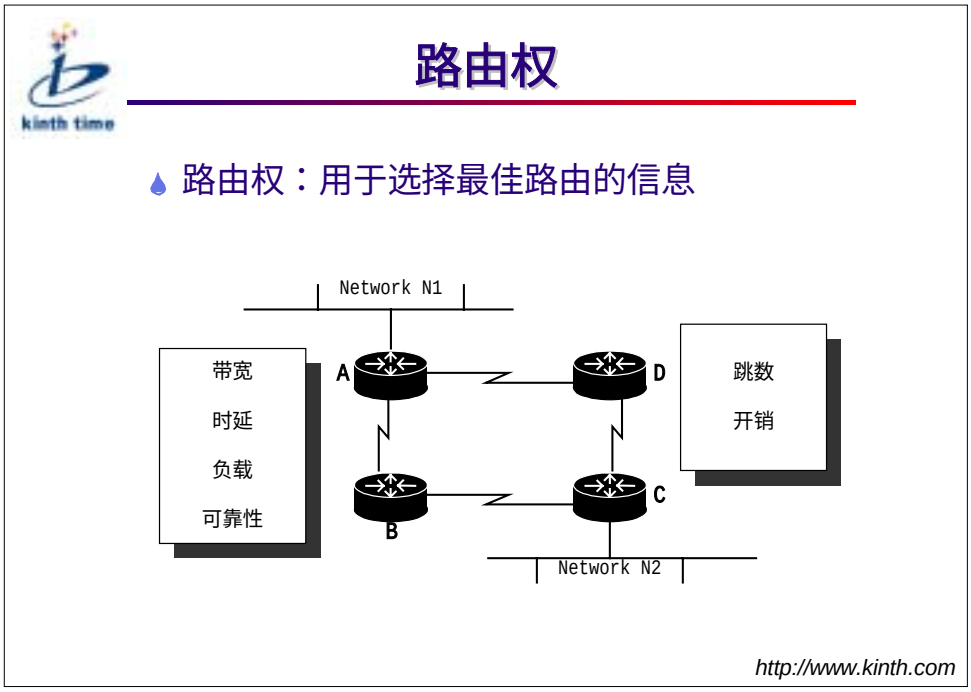
网络的配置不同决定了其对网络拓扑结构变化的适应能力，这取决于网络中是否使用动态路由协议。

静态路由信息可以指导报文的正常转发。再如图所示的网络中，为到达目标网络 N2 ，在路由器 A 上配置静态路由指向路由器 D ，在路由器 D 上配置静态路由指向路由器 C ，这样，从网络 N1 发往 N2 的报文就可以经过路由器 A、D、C 最后到达目标网络 N2。

但假如从路由器 A 到 D 的通路出现了问题，那么路由器 A 就不能根据静态路由的指示将报文发送到路由器 D 上去。如果想要保证网络的畅通，就必须由网管员手动配置一条经由路由器 B 的静态路由，这样，报文就可以经由路由器 A、B、C ，最后到达目标网络。

如果网络中运行了某种动态路由协议（如 RIP 协议）情况就会有所不同。当经由路由器 D 的路由失效之后，路由器之间会通过动态路由协议的路由信息传递，自动的发现另外一条到达目标网络经由路由器 B 的路由，并修改路由表，指导报文进行正确的转发。

.2.4 路由权



路由算法修改路由表的基本目的是将最好路由信息添加到路由表中，路由的好坏是由路由算法根据自己获得的路由信息计算出来的。对于每一条路由，路由算法产生一种权值来表示路由的好坏。通常情况下，这种权值越小，该路径越好。

路由权的计算可能基于路径某单一特性计算，也可能基于路径多种属性进行计算。有几种路径特性经常被用于权值计算，如下：

☞ 带宽 —— 链路的数据容量。例如，通常情况下 10M 以太网链路比 64K 出租线路要更好。

☞ 时延 —— 报文从到达目标网络所需要的时间。

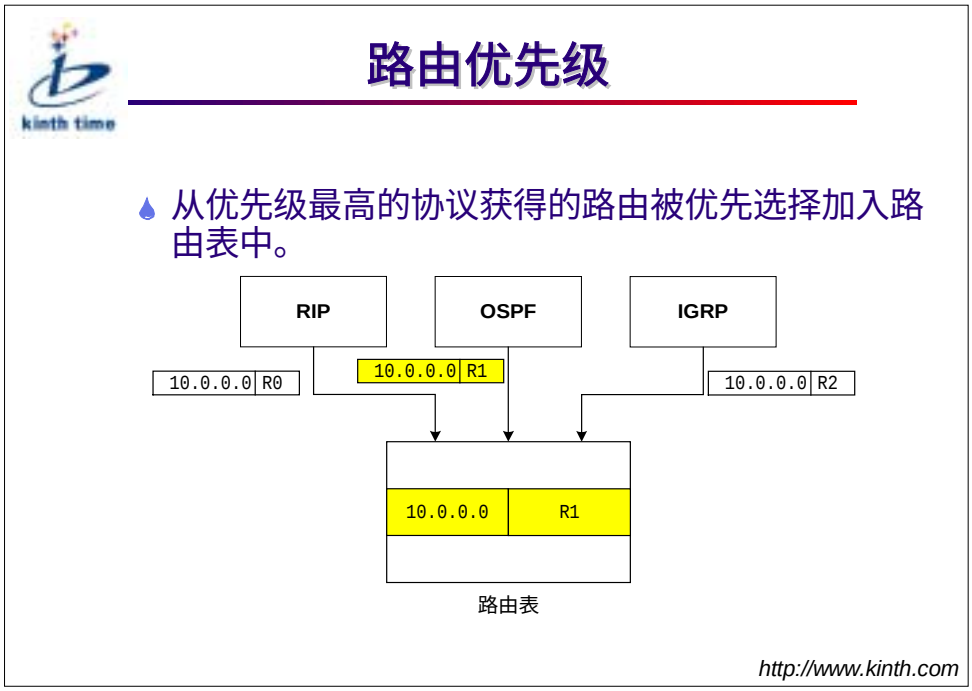
☞ 负载 —— 处于活跃状态的网络资源数量。

☞ 可靠性 —— 每条数据链路的出错率。

☞ 跳数 —— 报文到目的地需要经过的网络数。

☞ 开销 —— 一种人为设定的值，通常由网络管理员根据带宽、线路价格或其他一些因素综合得出。

.2.5 路由优先级

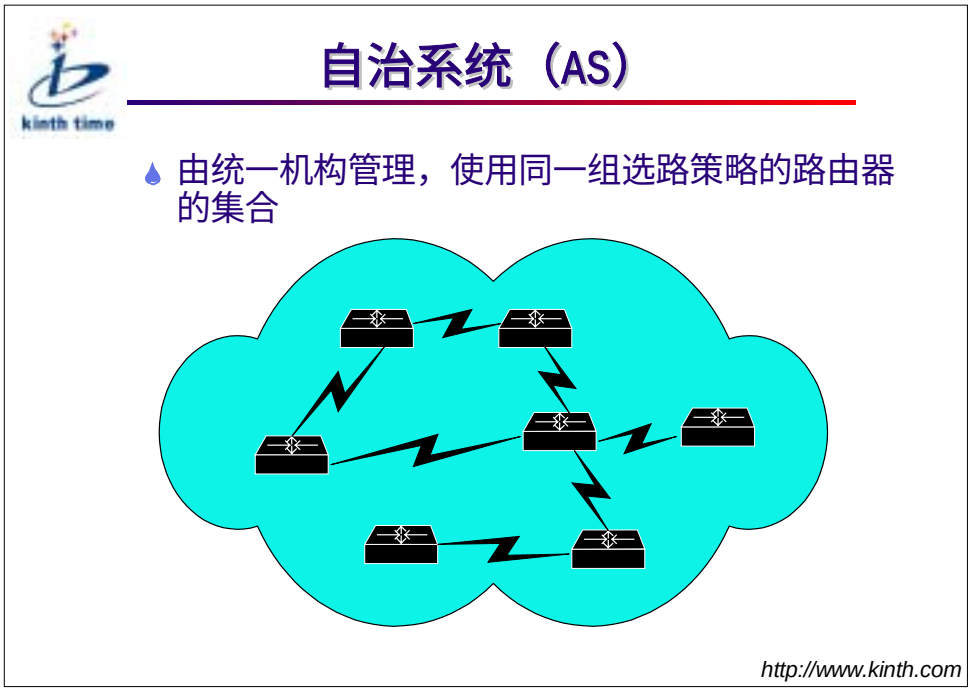


前面讲过，各个路由协议都有自己的标准来衡量路由的好坏（有的采用下一跳次数、有的采用带宽、有的采用时延，一般在路由数据中用度量 Metric 来量化），并且每个路由协议都试图将自己认为是最好的路由送到路由表中，这样我们就有可能从不同的协议得到到达同一目标网络的不同路由。尽管每个路由协议都给出了度量值，但是由于各个协议所采用度量值的含意不同，它们之间没有可比性。这就需要有种策略来决定使用哪一条路由。按照策略，判断最优的路由，我们才将它加入路由表，利用它来进行包的转发。

通常，我们使用路由优先级来判断不同路由协议所获得路由的好坏。每一种路由协议都由自己的优先级，当不同路由协议之间的路由发生冲突时，选择其中优先级最高的路由协议获得的路由。路由优先级是根据路由算法的优劣等因素得出的经验数值，也可以由网管员手动修改。

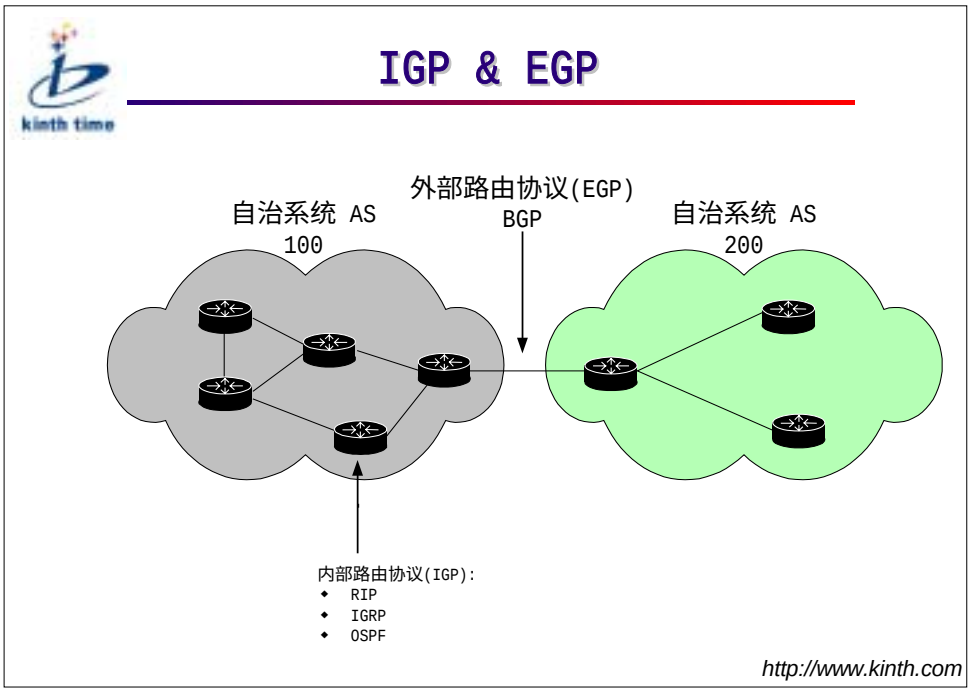
在上图中，三种路由协议 RIP 、OSPF 、IGRP 各自得到了一条到达目标网络 10.0.0.0 的路由。我们假定三种协议之间的路由优先级的次序是 OSPF > IGRP > RIP ，则最终选定 OSPF 路由作为最优路由。

.2.6 自治系统



为了便于网络的管理，人为地将互联网划分成若干自治系统。每一个自治系统由一组在统一的机构管理下的路由器组成，整个系统对外呈现统一的路由机制，并被看成独立的网络组成单元。
自治系统由一个 16bit 的整数标示，这个整数被称作自治系统号。自治系统号是由 NIC（Network Information Center）统一分配和管理的。

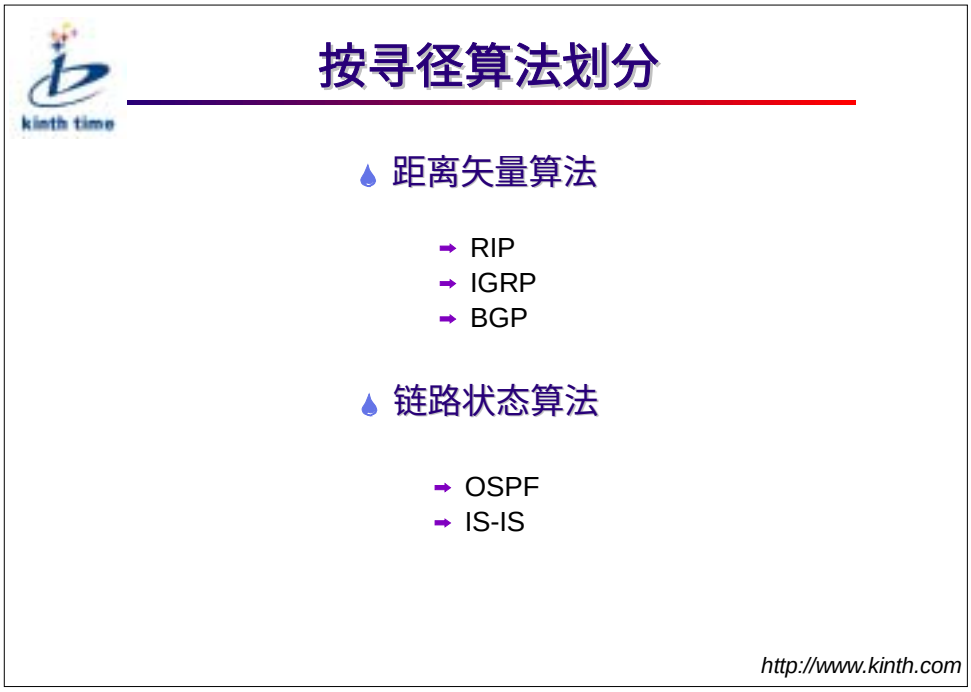
.2.7 IGP 和 EGP



从上一节所定义的自治系统我们可以把网络化分成若干区域，从而可以标示路由协议的作用范围。根据路由协议的不同作用范围，我们可以将路由协议划分成域内路由协议（IGP）和域间路由协议（EGP）。顾名思义，域内路由协议的作用范围被限制在自治系统内部，而域间路由协议适用于不同自治系统间的路由交换。

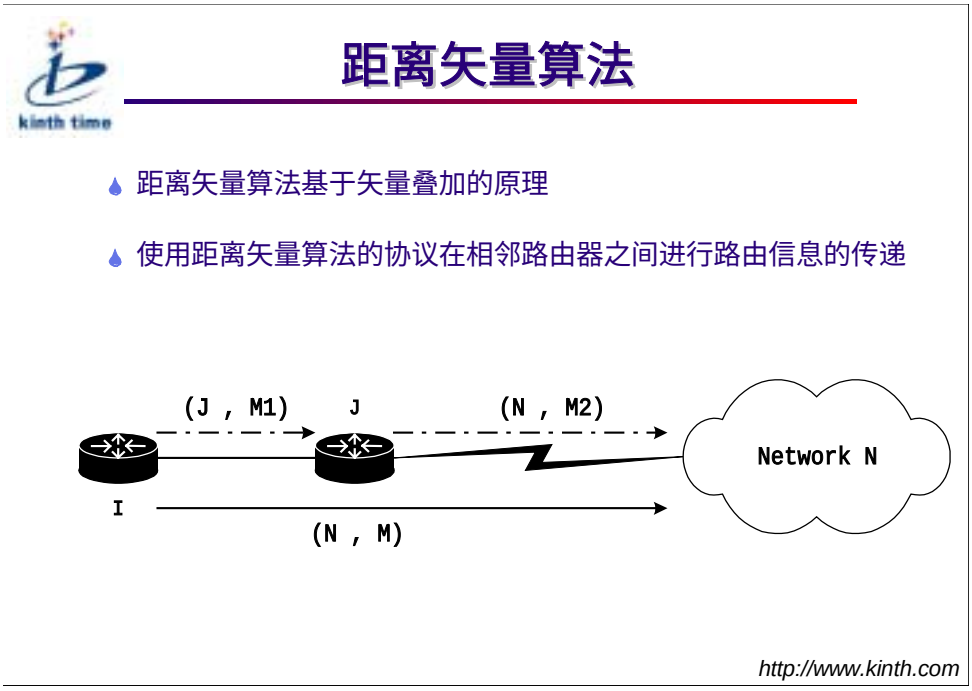
IGP 包括 RIP、IGRP、OSPF、IS-IS 等，而 EGP 目前只有 BGP 协议。

.2.8 按寻径算法划分路由协议



根据寻径算法，单播路由协议可分成距离矢量协议（Distance-Vector）和链接状态协议（Link-State）。距离矢量协议包括 RIP、IGRP、EIGRP、BGP，链接状态协议包括 OSPF、IS-IS。

.2.9 距离矢量算法



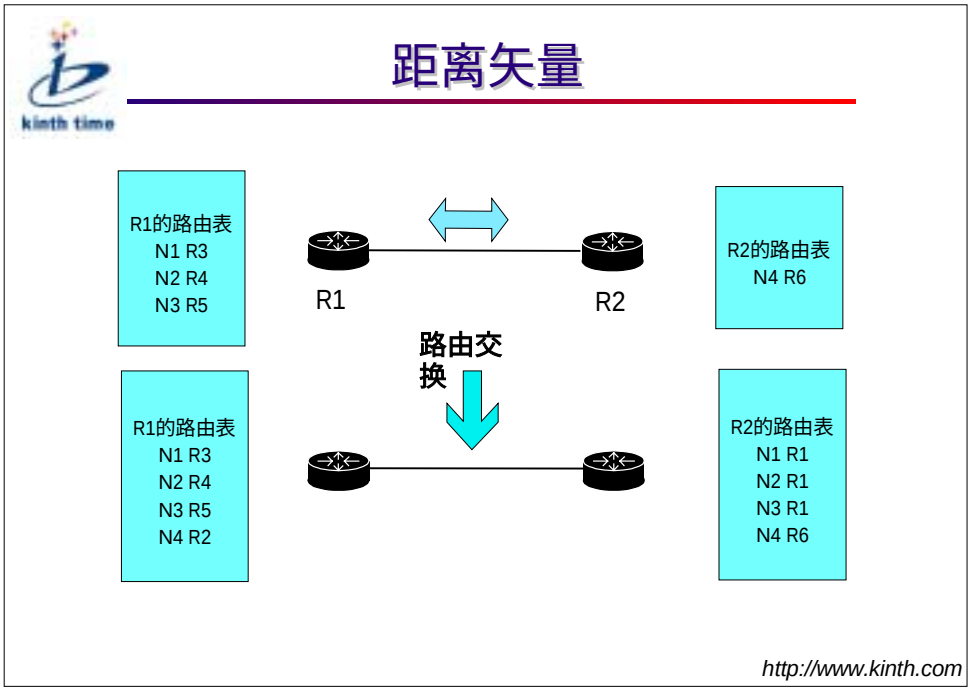
距离矢量算法是动态路由协议常用的一种路由算法，其基本原理就是运用矢量叠加的方式获取和计算路由信息。

所谓距离矢量即是将一条路由信息考虑成一个由目标和距离（用 Metric 来度量）组称的矢量，每一台路由器从其邻居处获得路由信息，并在每一条路由信息上叠加从自己到这个邻居的距离矢量，从而形成自己的路由信息。

在上图所示的例子中，路由器 I 从路由器 J 获得到达目标网络 N 的路由信息（N，M2），其中 N 标示目标网络，M2 标示距离长短的 Metric 值。并且在这条矢量数据上叠加从 I 到 J 的距离矢量（J，M1），形成 从 I 到目标网络 N 的路由信息（N，M），其中 M = M1+M2 。

这种过程发生在路由器的各个邻接方向上，通过 这种方法路由器可以获得到达网络中目标网络的途径和距离，并从中选择最佳路径形成和维护自己的路由表。

.2.10 距离矢量协议

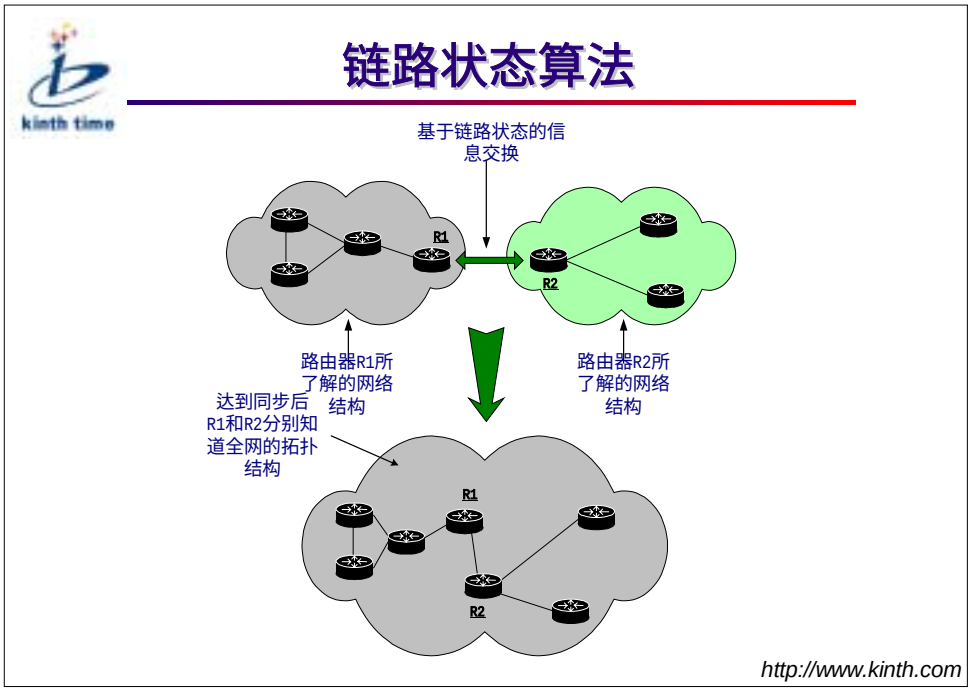


距离矢量协议直接传送各自的路由表信息。网络中的路由器从自己的邻居路由器得到路由信息，并将这些路由信息连同自己的本地路由信息发送给其他邻居，这样一级级的传递下去以达到全网同步。每个路由器都不了解整个网络拓扑，它们只知道与自己直接相连的网络情况，并根据从邻居得到的路由信息更新自己的路由表。

距离矢量协议无论是实现还是管理都比较简单，但是它的收敛速度慢，报文量大，占用较多网络开销，并且为避免路由环路得做各种特殊处理。

目前基于距离矢量算法的协议包括 RIP、IGRP、EIGRP、BGP。其中 BGP 是距离矢量协议变种，它是一种路径矢量协议。

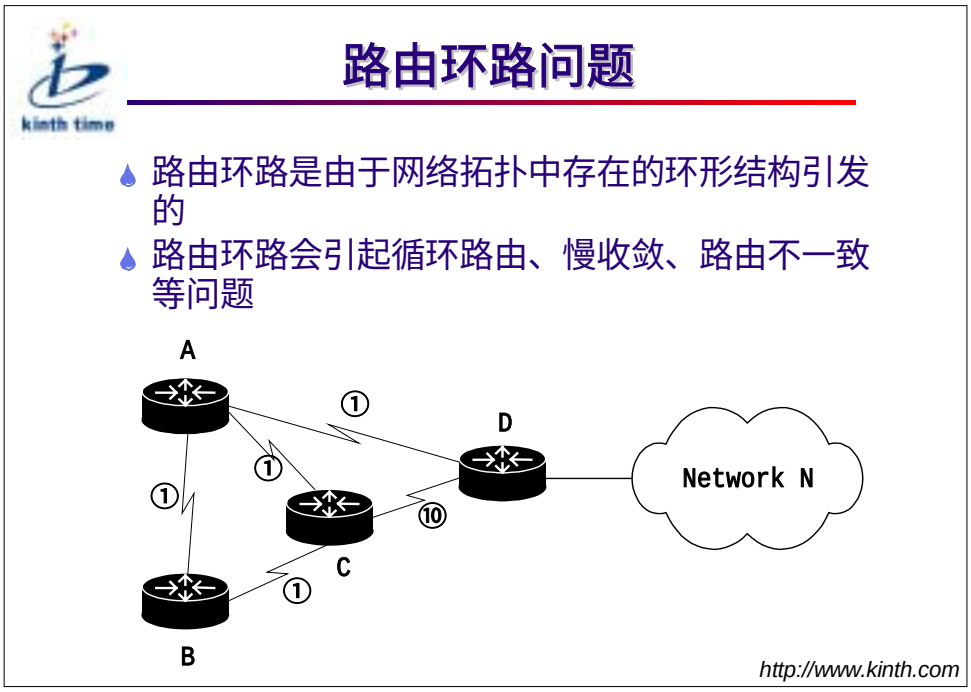
.2.11 链路状态协议



链接状态协议传送路由器之间的连接状态，每个路由器将自己所知道的链路状态通知其他路由器。这样网络中的路由器都知道整个网络拓扑结构，路由根据 SPF（Shortest Path First）算法得出。基于链路状态算法的协议结构复杂，难于管理。但由于每一台路由器都了解全网的拓扑结构，所以不用担心路由环路的影响，同时它的收敛速度快，需要传递的信息量少，可以节省网络带宽。

典型的基于链路状态算法的协议有 OSPF 和 IS-IS。

.2.12 路由环路问题



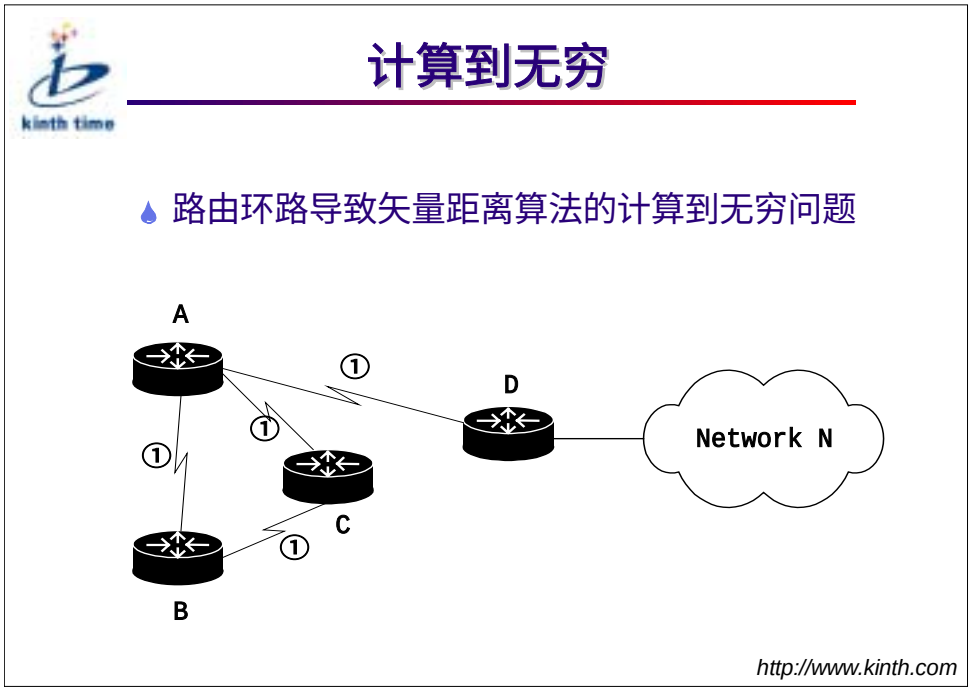
路由环路问题是当网络拓扑结构发生变化，由于网络中存在的环状结构所引发的。上图是一个简单的例子。

如图所示，路由器 D 与目标网络 N 直接相连，而路由器 A、B、C 之间组成了一个环形网络，连接路由器的路径旁边的数字显示了路径对应的权值。这样在路由器 A 上就有一条经过路由器 D 的去往目标网络的路由，权值为 1，而路由器 B、C 上分别有一条经过路由器 A 的去往目标网络的路由，权值为 2。假设，路由器 A 与 D 之间的通信出现了问题，这时候就有可能产生路由环路问题，并导致慢收敛。为了简单起见，我们假设所有的路由器都同时发送路由更新报文，下表显示了路由器 A、B、C 上到达目标网络的路由随时间的变化。

时间 T ——〉						
路由器A	不可达	(C，3)	(C，4)	。。。	(C，10)	(C，11)
路由器B	(A，2)	(C，3)	(C，4)	。。。	(C，10)	(C，11)
路由器C	(A，2)	(B，3)	(B，4)	。。。	(A，10)	(D，10)

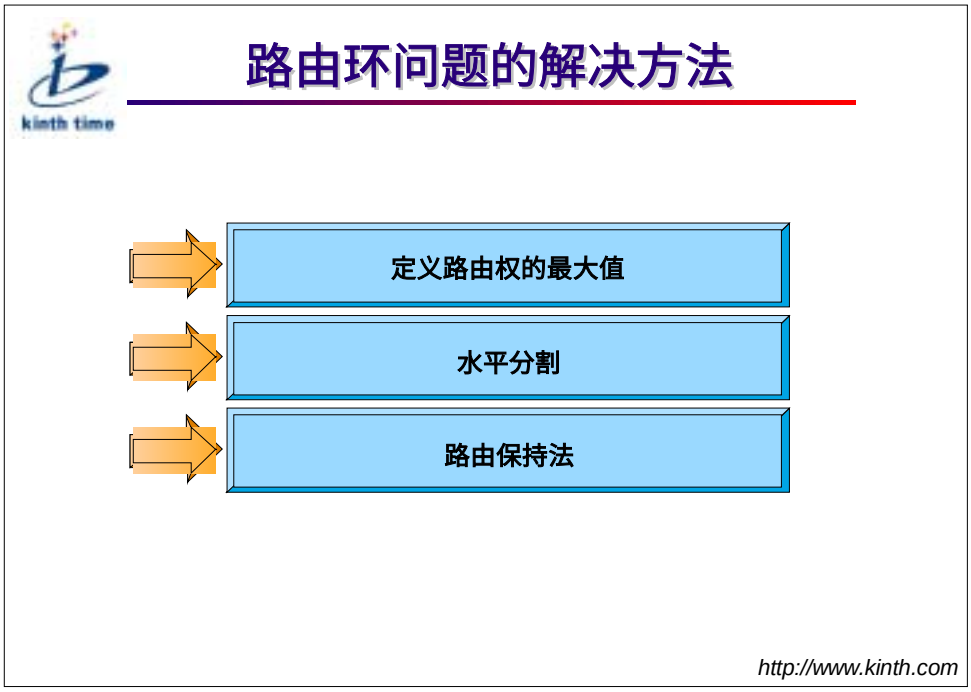
虽然算法最终收敛，但在漫长的收敛过程中在各个路由器上的路由并不能反映网络的真实结构，A、B、C 三台路由器之间相互欺骗，把错误的路由信息在网络中相互传递。

.1.1 计算到无穷



仍然考虑如前面的网络结构，这里我们假设路由器 C 与 D 之间没有直接的通路相连，这时再断掉路由器 A 与 D 之间的连接，循环路由就会持续进行下去，错误的路由在路由环中一直传播下去。在前面所述的例子中，这种循环最终会停下来是因为路由器 C 得到了一条更好的路由（D，10），从而中止了路由循环的继续传播。现在这个中止条件没有了，路由信息的循环累加就会不停的继续下去，直到路由权值累加到无穷大。这就被称为计算到无穷问题。

.1.2 解决路由环问题的几种方法

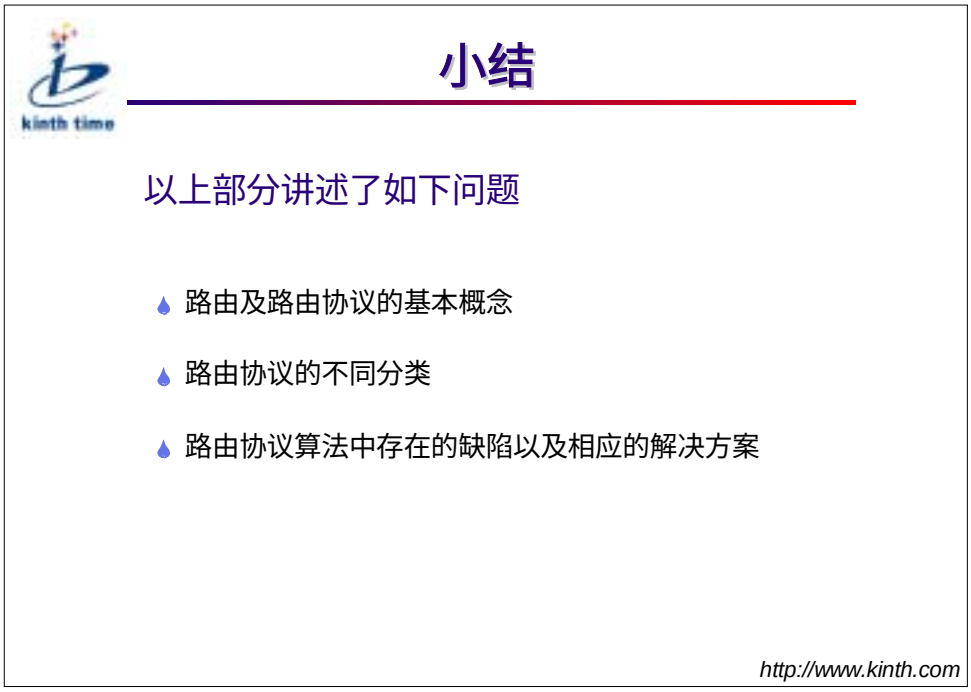


为解决路由环问题首先要设定一个最大值作为路由权的无穷大值，这个数值通常要根据协议的路由权值的计算方法而定。比如在 RIP 中以跳数来作为路由权的度量，它的最大值就是 16，也就是说如果某条路由的 Metric 值为 16 就表示这条路由不可达。

最大值的设定只能解决无限循环的问题，而并不能解决慢收敛问题。路由环路产生的一个重要原因就是不正确的路由信息通过获得这条信息的接口再发送回去，替代了新的正确的路由，这也就导致了错误路由信息的循环往复。如在我们前面提到的例子中，正是因为路由器 C 将从路由器 A 上得到的路由信息有发送回路由器 A，才会导致路由的循环依赖。由此我们得到一个解决路由环路的方法：水平分割。水平分割就是从某个接口接收到的路由信息不再从这个接口发送回去，从而避免错误的路由信息被使用。

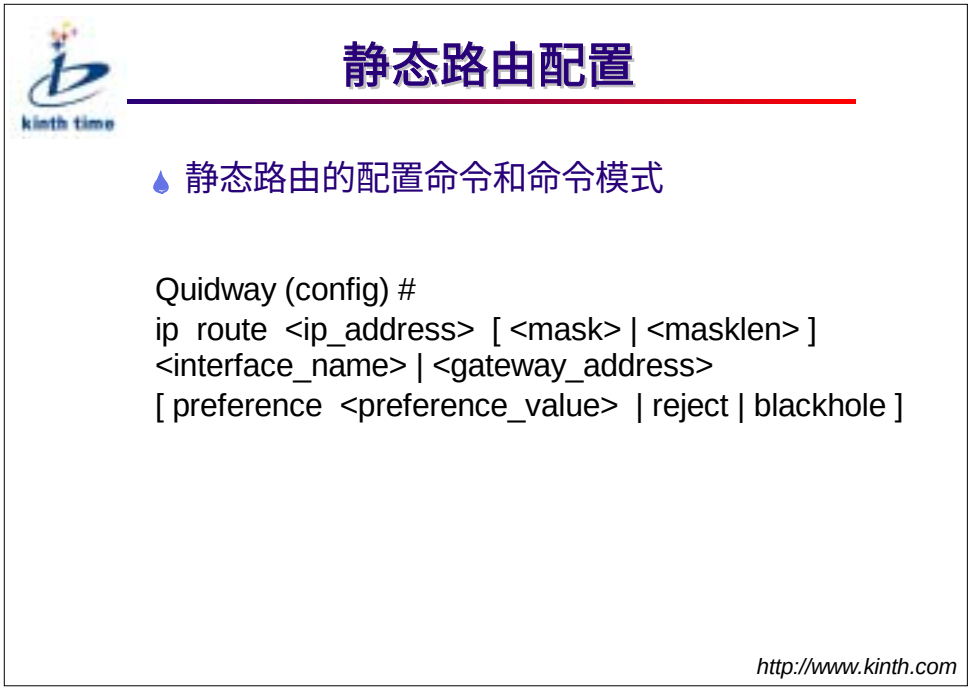
另一个方法就是路由保持法，也就是将路由的不可达状态保持一段时间，在这段时间内不对这条路由作任何修改，直到这条路由的不可达状态被尽可能的扩散出去。这样也可以防止错误路由的传播。

.1.3 小结


小结
以上部分讲述了如下问题
路由及路由协议的基本概念
路由协议的不同分类
路由协议算法中存在的缺陷以及相应的解决方案
http://www.kinth.com

.2 路由的基本配置方法

.2.1 配置静态路由

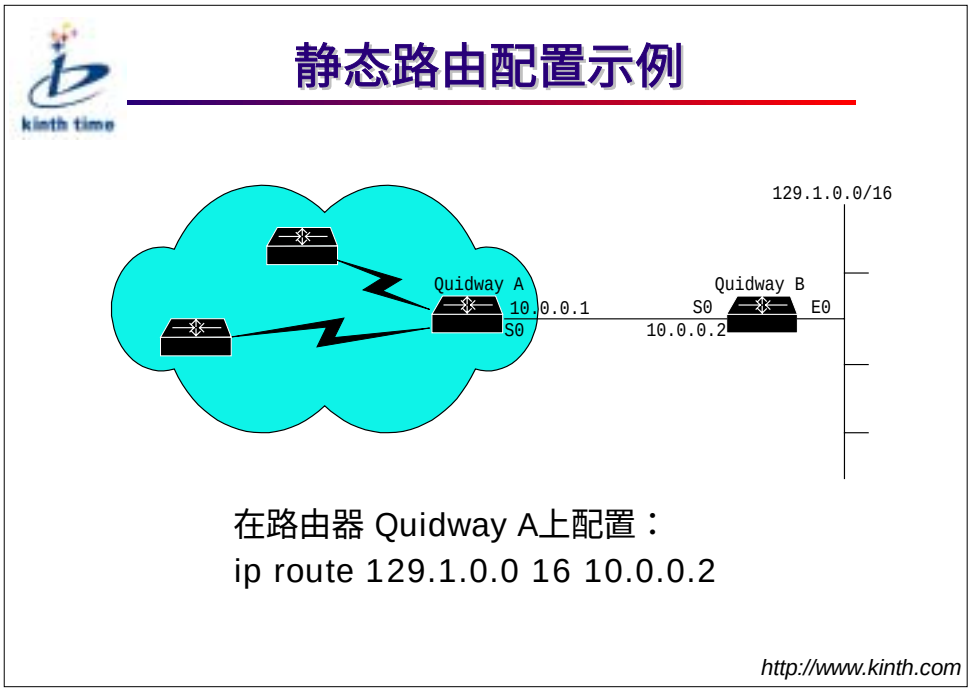


用户可以在全局配置模式下通过命令 ip route 来配置一条静态路由。命令的参数说明如下：

ip_address	目标网络的网络地址
mask	目标网络的子网掩码
masklen	目标网络的掩码长度
interface_name	指定去往目标网络的报文的发送接口
Gateway_addr	指定去往目标网络的报文经由的下一条地址
preference_value	静态路由加到核心路由表中的优先级

静态路由允许网管员手工配置路由表，但不能够动态的反映网络的变化，因此，此方法对保证网络不间断运行存在一定的局限性。
而在网络结构相对稳定的网络中使用静态路由就可以减少路由选择问题，并节省网络开销。同时，使用静态路由还可以实现负载平衡和路由备份功能等特殊应用。

.2.2 静态路由配置举例



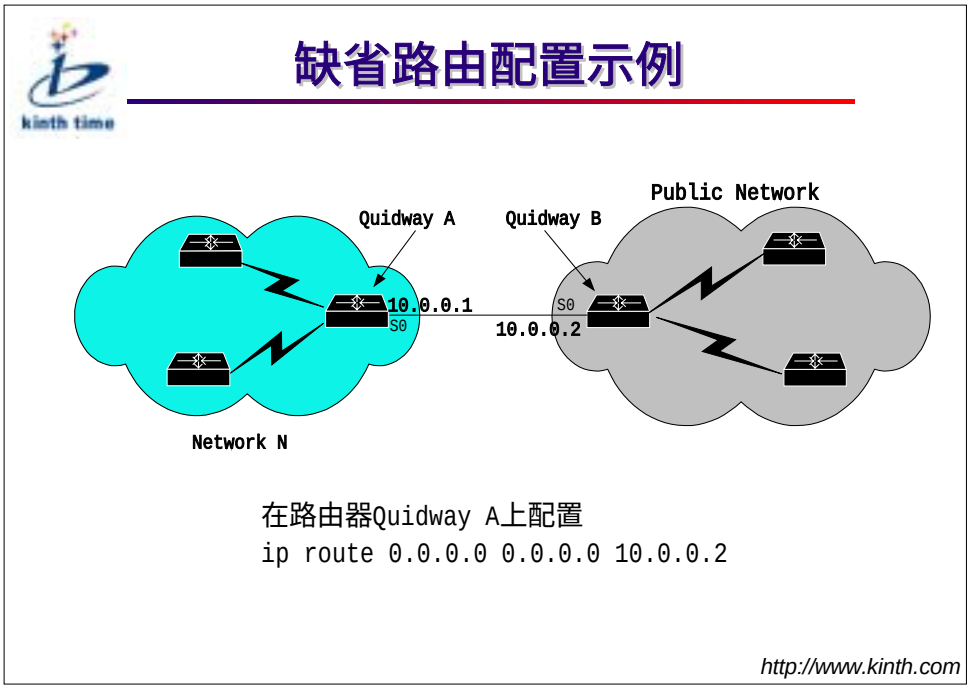
在这个例子中使用 IP ROUTE 命令来配置静态路由：

ip route 129.1.0.0 16 10.0.0.2

命令	说明
ip route	配置一条到达目标网络（129.1.0.0）的静态路由。
16	目标网络的掩码长度，也可以用点分法表示，如 255.255.0.0 。
10.0.0.2	去往目标网络的报文所经由的下一个路由器（下一跳）的 IP 地址。

通过这个配置在路由器 Quidway A 上配置到目标网络网络 129.1.0.0/16 的静态路由，此路径经过路由器 Quidway B，目标网络与路由器 Quidway B 的以太网口相连。

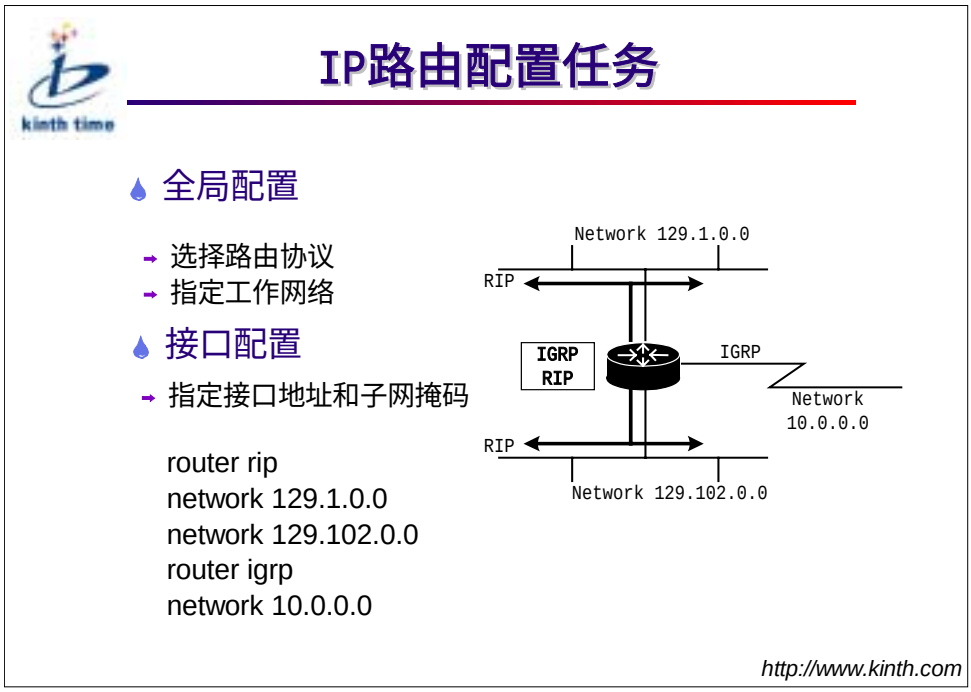
.2.3 缺省路由的配置及举例



在本例中，网络 N 只有一个到公网的出口，就是通过路由器 Quidway B。于是可以通过配置缺省路由使得从网络 N 内可以访问公网内的所有网络，而不必逐个网络的配置静态路由。

缺省路由的配置也使用命令 ip route ，并且命令的格式和参数都相同，但与普通静态路由的配置不同的是，缺省路由的目标网络的地址和掩码必须全部为零。

.2.4 IP 路由配置任务



路由器上配置动态路由协议包括全局配置和接口配置两个方面。

在全局配置下：

选择一种路由协议，如 RIP、IGRP、OSPF 等。启动对应路由协议的处理进程。

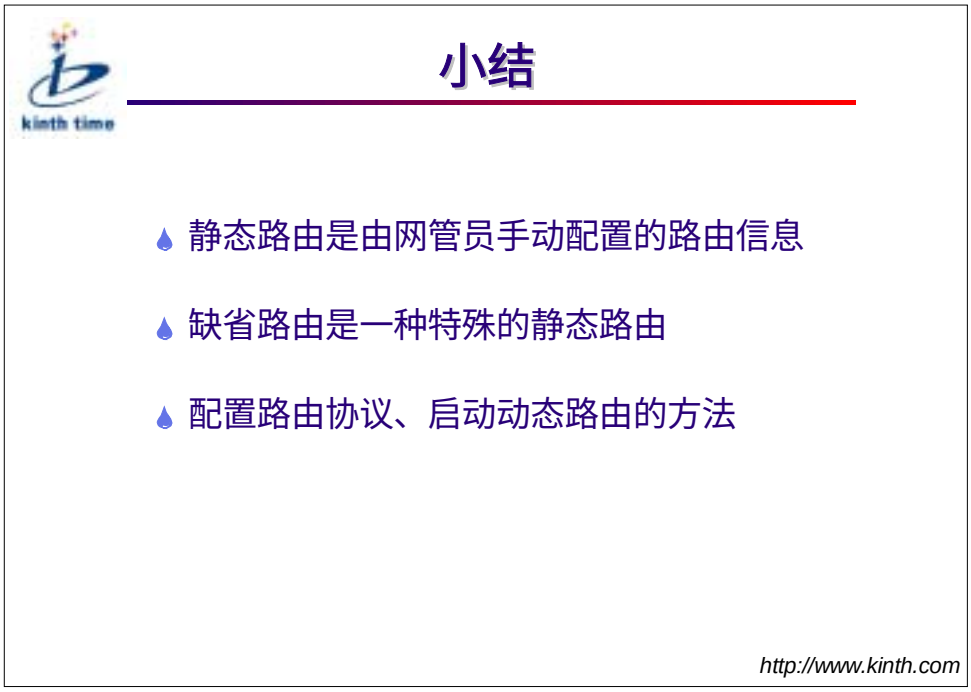
☞ 使用全局配置命令 router protocol [keyword] 进行配置。

命令及参数	说明
router protocol	指定所选择的协议，如 RIP、IGRP、EIGRP、OSPF、BGP 等
keyword	进程 ID 或自治系统号，某些需要指定自治系统号协议如 BGP 要使用此参数

☞ 指定工作网络，需要注意的是，此时不能同时指定子网掩码。

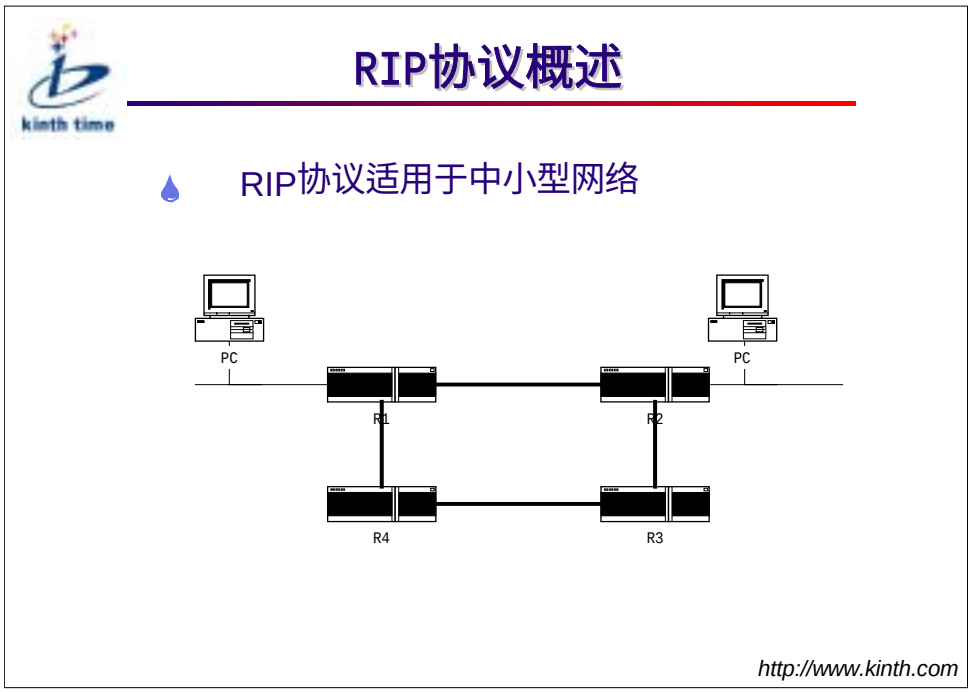
命令及参数	说明
network network-number	指定一个直接相连的网络在接口上需要配置 IP 地址和对应网络的子网掩码。

.2.5 小结


小结
静态路由是由网管员手动配置的路由信息
缺省路由是一种特殊的静态路由
配置路由协议、启动动态路由的方法
http://www.kinth.com

.3 RIP 协议及配置

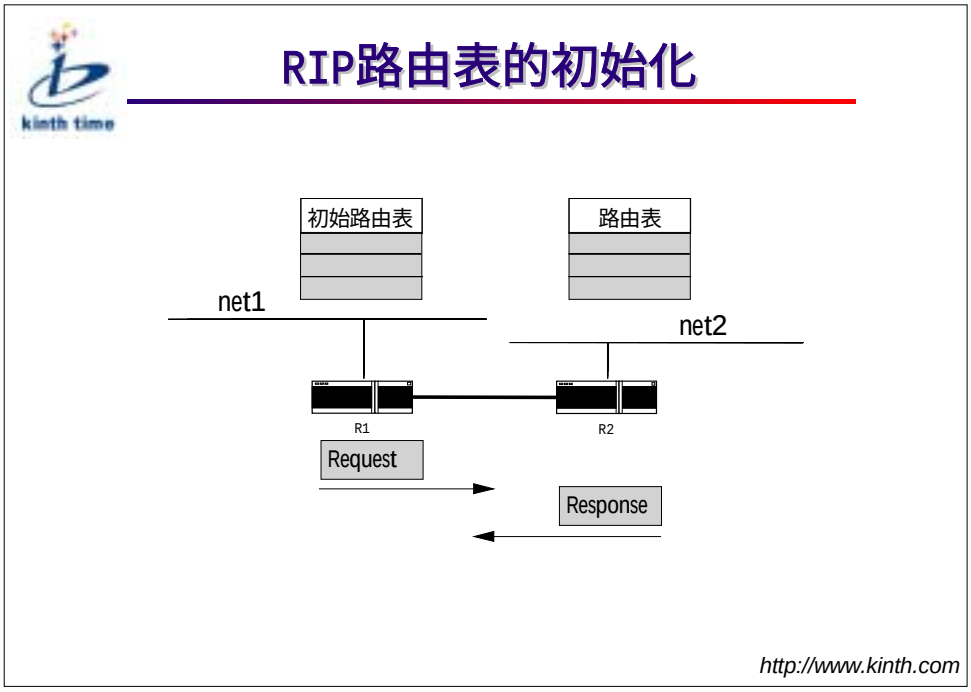
.3.1 RIP 协议概述



RIP 协议要点：

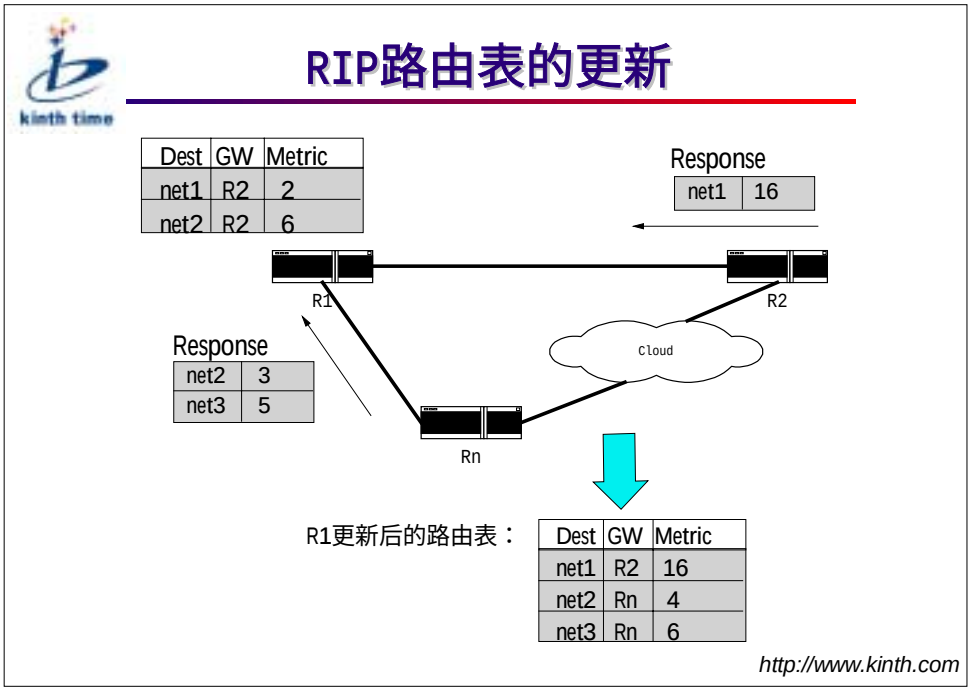
- RIP 协议基于距离向量算法，属于内部网关协议；
- RIP 协议以到达目的地址所经过的路由器个数（跳数）为衡量路由好坏的度量值，最大跳数为 15；
- RIP version 1 不支持子网掩码，version 2 支持变长掩码；
- RIP 协议适用于基于 IP 的中小型网络。

.3.2 RIP 路由表的初始化



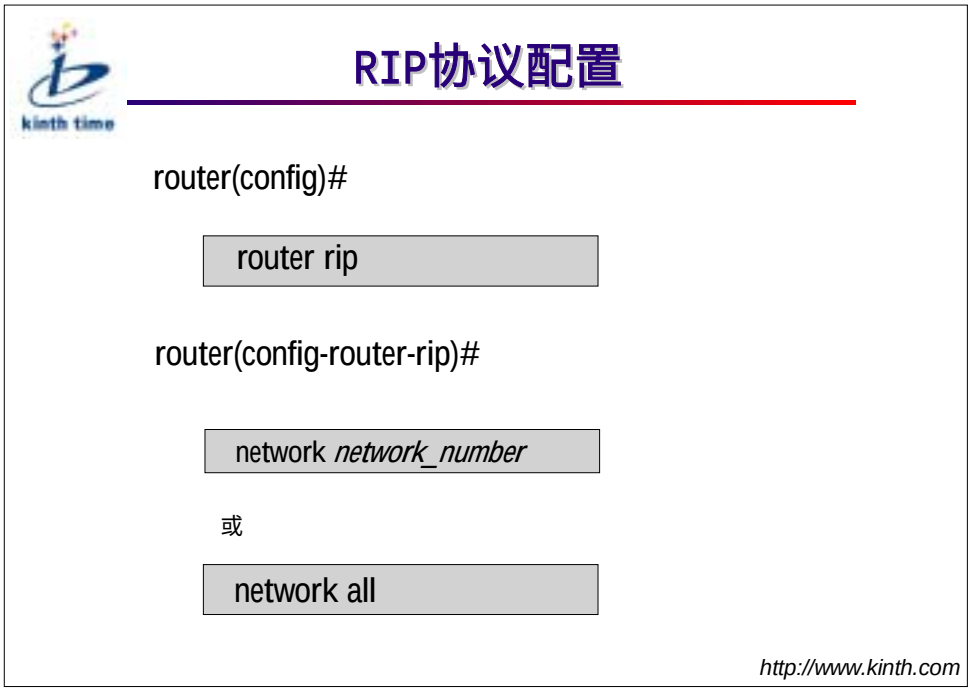
☞ RIP 启动时的初始路由表仅包含本路由器的一些接口路由。
☞ RIP 协议启动后向各接口广播一个 Request 报 文。
☞ 邻居路由器的 RIP 协议从某接口收到 Request 报文后，根据自己的路由表，形成 Response 报文向该接口对应的网络广播。
☞ RIP 接收邻居路由器回复的包含邻居路由器路由表的 Response 报文，形成自己的路由表。

.3.3 RIP 路由的更新



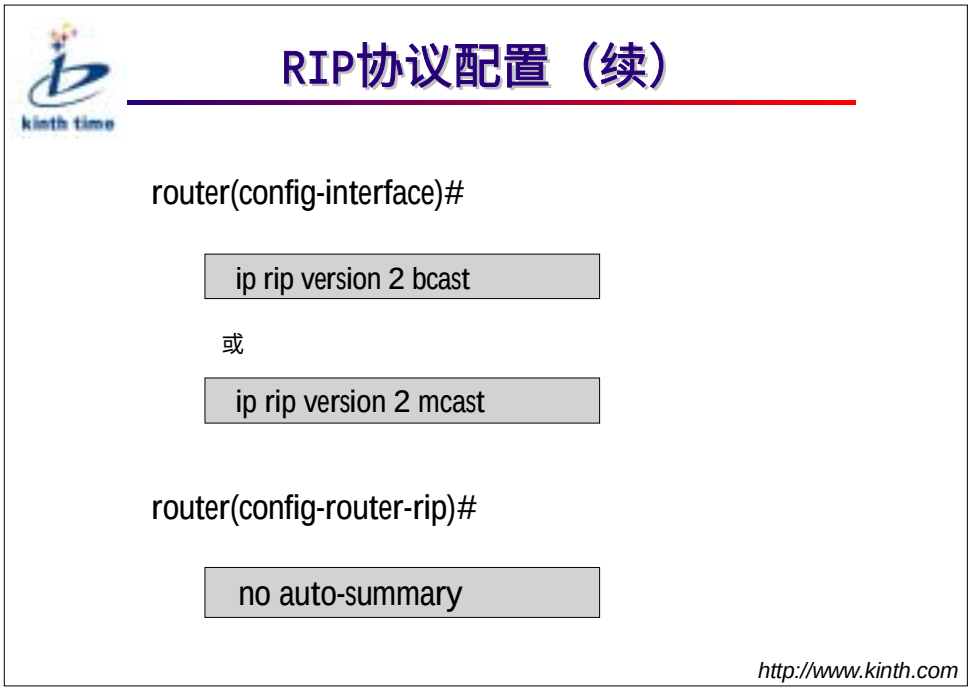
☞ RIP 协议以 30 秒为周期用 Response 报文广播自己的路由表。
☞ 收到邻居发送而来的 Response 报文后，RIP 协议计算报文中的路由项的度量值，比较其与本地路由表路由项度量值的差别，更新自己的路由表。
☞ 报文中路由项度量值的计算：metric' = MIN（metric + cost, 16），metric 为报文中携带的度量值信息，cost 为接收报文的网络的度量值开销，缺省为 1（1 跳），16 代表不可达。
☞ RIP 路由表的更新原则：
对本路由表中已有的路由项，当发送报文的网关相同时，不论度量值增大或是减少，都更新该路由项（度量值相同时只将其老化定时器清零）；
对本路由表中已有的路由项，当发送报文的网关不同时，只在度量值减少时，更新该路由项；
对本路由表中不存在的路由项，在度量值小于不可达（16）时，在路由表中增加该路由项；
☞ 路由表中的每一路由项都对应一老化定时器，当路由项在 180 秒内没有任何更新时，定时器超时，该路由项的度量值变为不可达（16）。
☞ 某路由项的度量值变为不可达后，以该度量值在 Response 报文中发布四次（120 秒），之后从路由表中清除。

.3.4 RIP 协议配置



☞ 在全局配置模式下用 router rip 命令启动 RIP 协议并进入 RIP 协议配置模式。
☞ 在 RIP 协议配置模式下用 network network_number 命令在某一网段对应的接口上使能 RIP 协议。
☞ network all 命令在路由器的所有接口上使能 RIP 协议。
☞ 这种配置下 RIP 协议在接口上广播 version 1 类型的报文，RIP V1 不发布子网信息。

RIP 协议配置（续）



☞ 在接口上使能 RIP version 2

在接口配置模式下使能广播方式的 RIP V2（bcast）或多播方式的 RIP V2（mcast）；

RIP 协议缺省进行路由聚合，在 RIP 协议配置模式下取消 RIP 的自动聚合功能，使其发布子网信息。

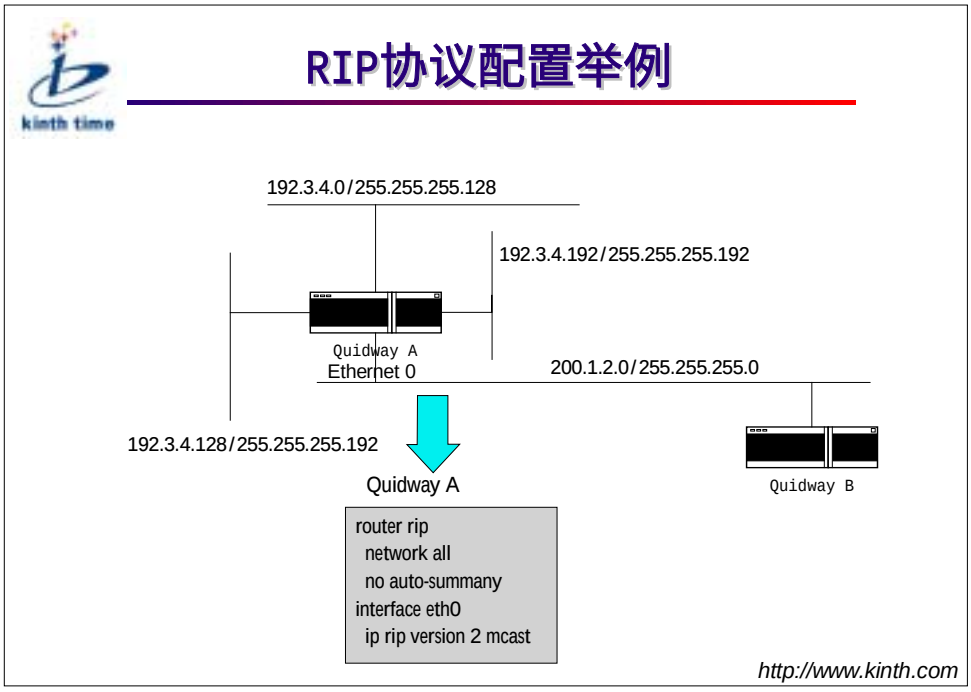
☞ RIP V2 广播方式与多播方式

RIP V2 的广播方式以广播地址（255.255.255.255）周期发布 RIP V2 报文，RIP V2 的多播方式以多播地址（224.0.0.9）周期发布 RIP V2 报文；

RIP V2 缺省使用多播方式，以减少周期发布的 RIP 报文对不监听 RIP 信息的主机的影响；

RIP V2 的广播方式是 RIP V1 与 RIP V2 之间的兼容方式，以广播方式发布的 RIP V2 报文可以被 RIP V1 路由器和 RIP V2 路由器（广播方式或多播方式）接收，同时运行在广播方式的 RIP V2 路由器可以接收 RIP V1 的广播报文和 RIP V2 的广播或多播报文。

.3.5 RIP 配置举例

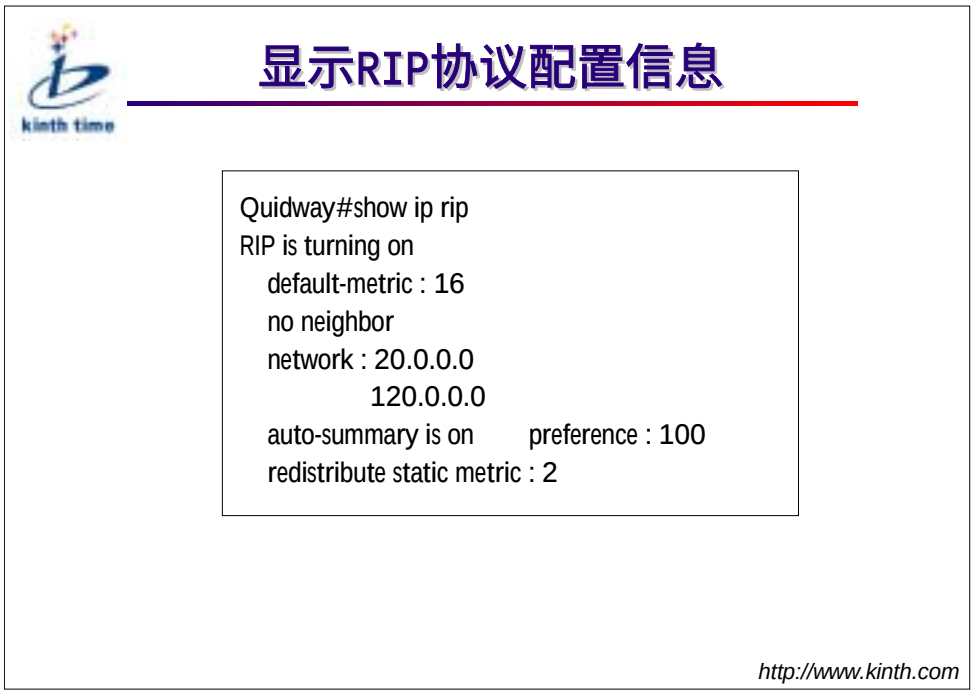


☞ 在全局配置模式下启动 RIP 协议。

☞ 在 RIP 协议配置模式下使能接口，并禁止 RIP 协议的路由聚合功能。

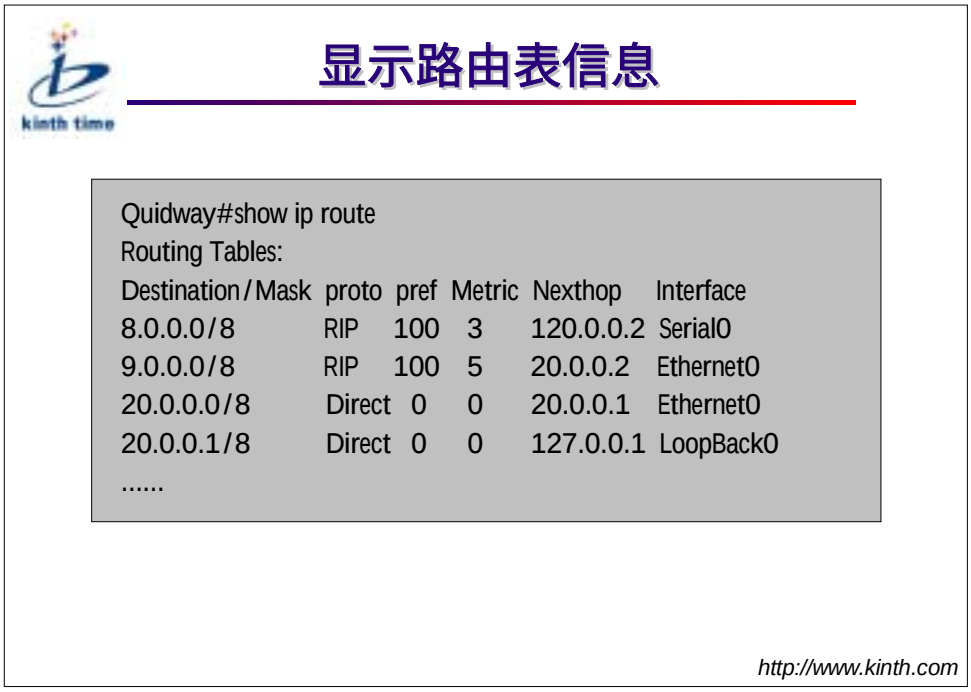
☞ 在接口配置模式下使能多播方式的 RIP V2 以发布子网信息。

.3.6 显示 RIP 协议配置信息



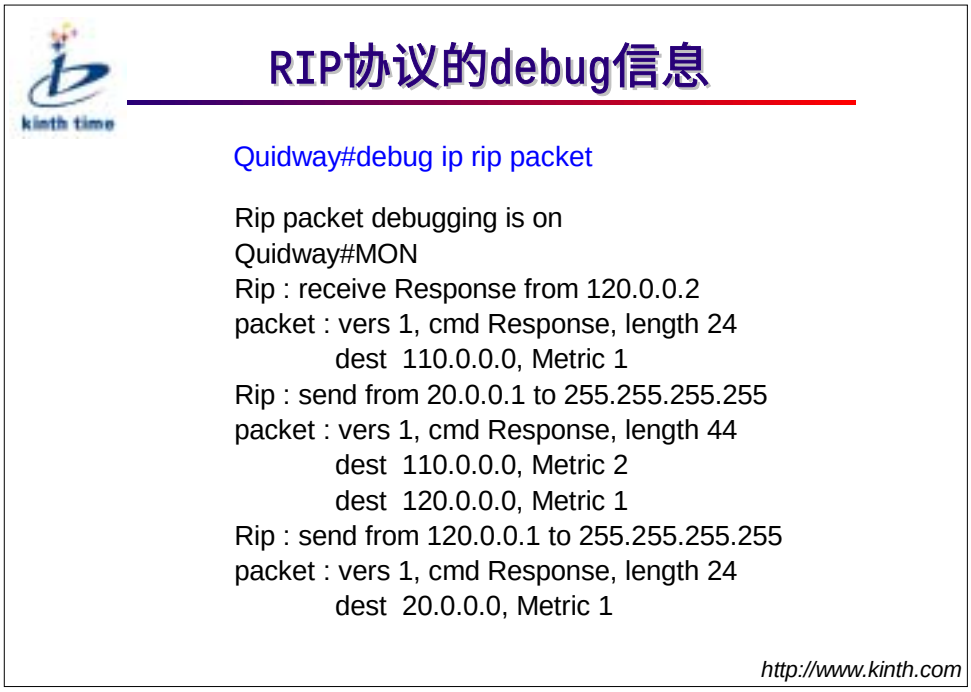
☞ 显示当前 RIP 协议的运行状态：
缺省路由权为 16；
没有指定定点传送地址；
在 20.0.0.0 与 120.0.0.0 网段上使能 RIP 协议；
自动聚合路由；
RIP 路由的 reference 为 100；
引入静态路由，并设置其度量值为 2。

.3.7 显示路由表信息



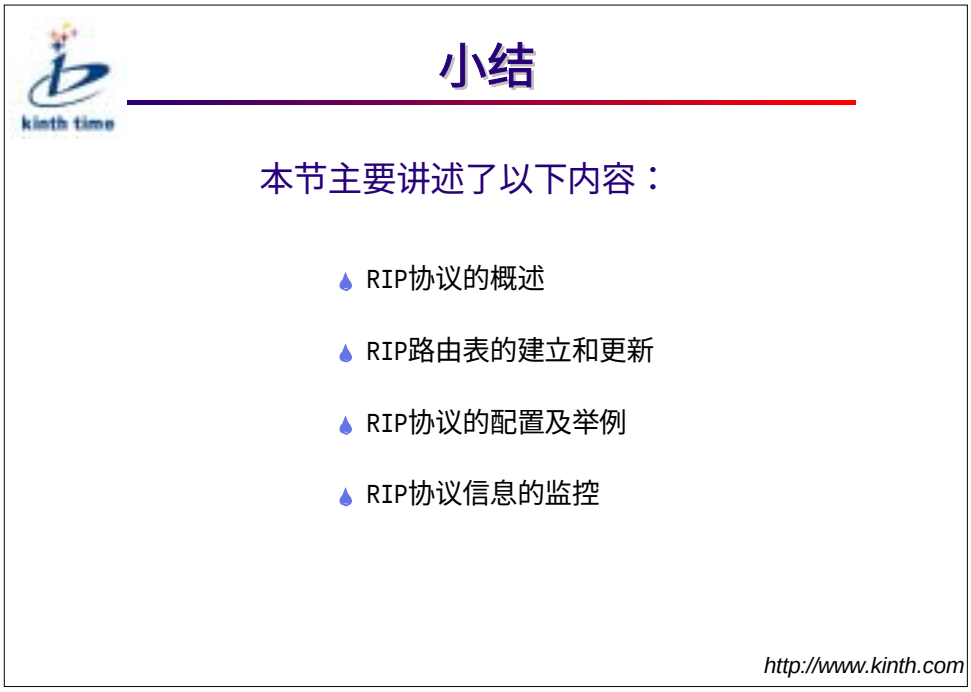
☞ 显示当前的路由表信息，其中有两条 RIP 路由：
RIP 路由 1：目的地址 8.0.0.0/8，下一跳为 120.0.0.2，度量值为 3；
RIP 路由 2：目的地址 9.0.0.0/8，下一跳为 20.0.0.2，度量值为 5。

.3.8 RIP 协议的 debug 信息



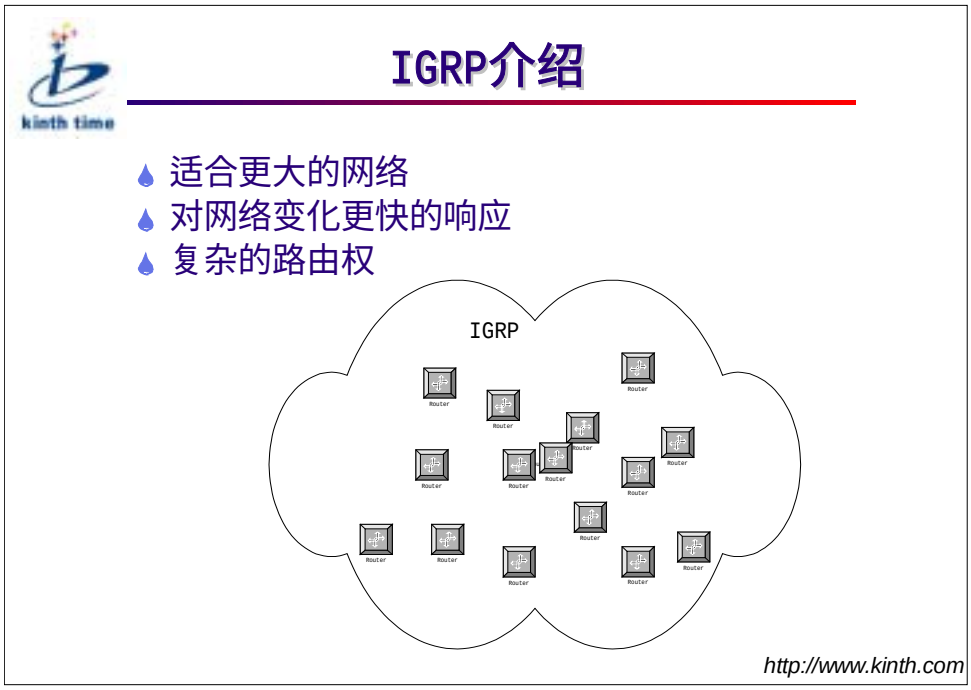
☞ debug ip rip packet 打开 RIP 协议的调试开关：
RIP 协议从 120.0.0.2 接收到一条目的地址为 110.0.0.0 的路由信息，度量值为 1；
RIP 协议向 20.0.0.1 与 120.0.0.1 分别发送路由更新信息，分别包含两条路由信息和一条路由信息。

.3.9 小结


小结
本节主要讲述了以下内容：
RIP协议的概述
RIP路由表的建立和更新
RIP协议的配置及举例
RIP协议信息的监控
http://www.kinth.com

.4 IGRP 协议及配置

.4.1 IGRP 简介



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。它比较 RIP 而言，主要有以下几点改进：

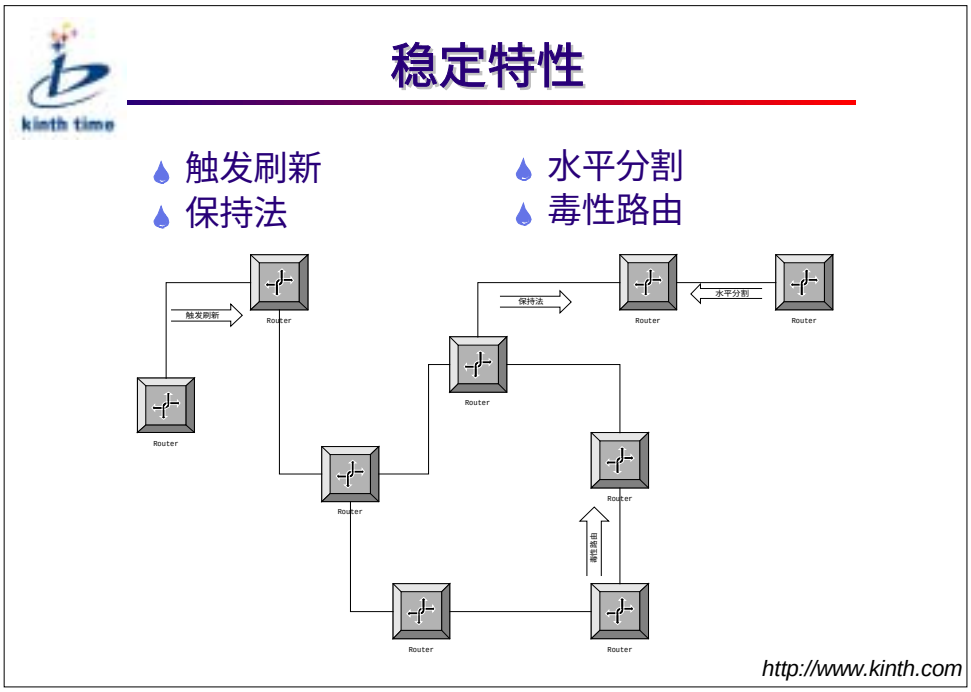
☞ IGRP 路由的跳数不再受 16 跳的限制，同时在路由更新上引入新的特性，使得 IGRP 协议适用于更大的网络；

☞ 引入了触发刷新、路由保持、水平分割和毒性路由等机制，使得 IGRP 对网络变化有着较快的响应的速度，并且在拓扑结构改变后仍然能够保持稳定。

☞ 在 Metric 值的范围和计算上有了很大的改进，使得路由的选择更加准确，同时使路由的选择可以适应不同的服务类型。

运行 IGRP 协议的路由器通过广播地址向相邻的路由器周期性的发送自己的路由表，同时当它收到相邻路由器发送的路由表后，根据收到的路由表增加、删除、修改本地的路由表，以达到全局路由的一致性。

.4.2 稳定特性



动态路由协议的基本功能是当网络中的路由发生改变时，将此改变迅速有效的传递到网络中的每一台路由器。同时，由于网络传递的不可靠、时延等各种偶然因素的存在，可能造成路由信息的反复变化，从而导致网络的不稳定。IGRP 协议引入了引入了触发刷新、路由保持、水平分割和毒性路由等机制，较为有效的解决了这些问题：

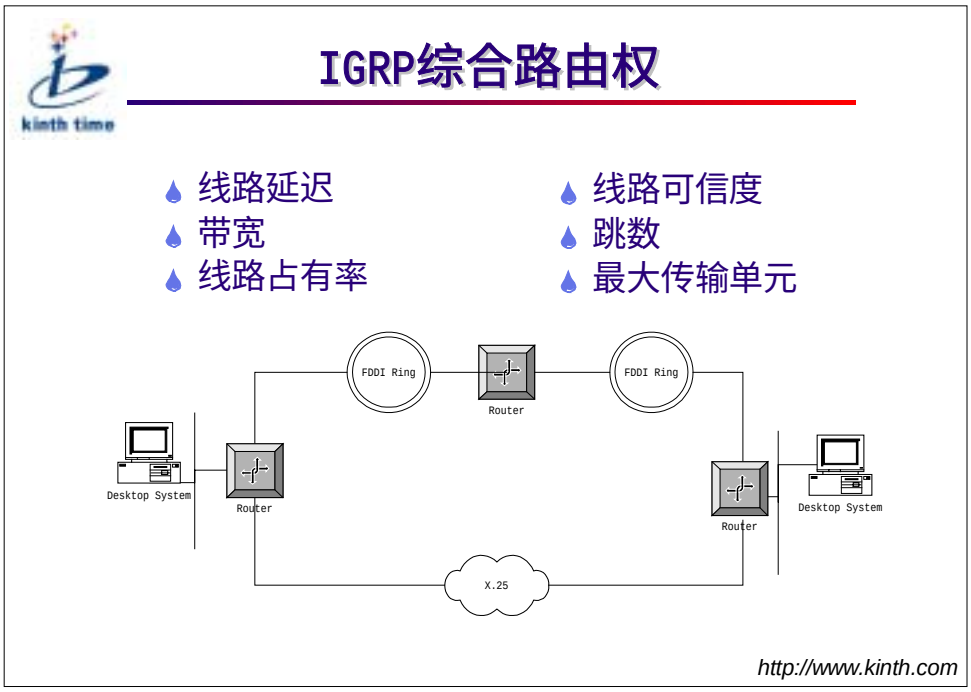
☞ 触发刷新：当路由发生改变，立即将新发生改变的路由送出，而不必等到下一次的周期性刷新，从而使得最新的路由信息很快地传送到网络中的各个路由器；

☞ 路由保持：路由保持是指当一条路径被删除后，此路由在一定的时间内要以不可达发送，在此段时间内即使有可达路径的报文,也丢弃不理。这样做可以使不可达路由信息在不可靠传送的情况可以最大限度的发送出去，而不会丢失和引起网络波动；

☞ 水平分割：水平分割规定不能将从某一网关送来的路由信息再送回此网关。即它如果要发送刷新报文给相邻网关 A，那么必须把路由中 A 送来的信息全部去掉，这样可以有效地避免相邻网关中环路的形成；

☞ 毒性路由：毒性路由是指如果一条路由的刷新使它的路由权的增长率大于某一比率，则此路由必须删除，并使其处于 Holddown 状态。这样做可以免在网络中形成更大的环路。

.4.3 综合路由权



路由权是路由协议在计算路由时的主要依据，所以路由权的定义对路由的选择有着重要的影响。网络结构千变万化，单纯的跳数根本无法反映实际的网络结构，所以 IGRP 协议使用综合路由权，使得 IGRP 协议对网络路径的计算更加准确。IGRP 协议的综合路由权包括如下内容：

☞ 带宽：网络的带宽，单位 kbytes/s，范围 0~16777215；

☞ 时延：网络的时延，每单位代表 10 微秒，范围 1~4294967295；

☞ 信道可信度：网络传输的可靠性，范围 1 ~255，这里 255 代表 100% 可信；

☞ 信道占用率：网络的当前占用率，范围 1~255，这里 255 代表 100% 被占用；

☞ 最大传输单元：接口的最大传输单元，单位字节，范围 1~65535；

☞ 跳数：路径每经过一台路由器为一跳。

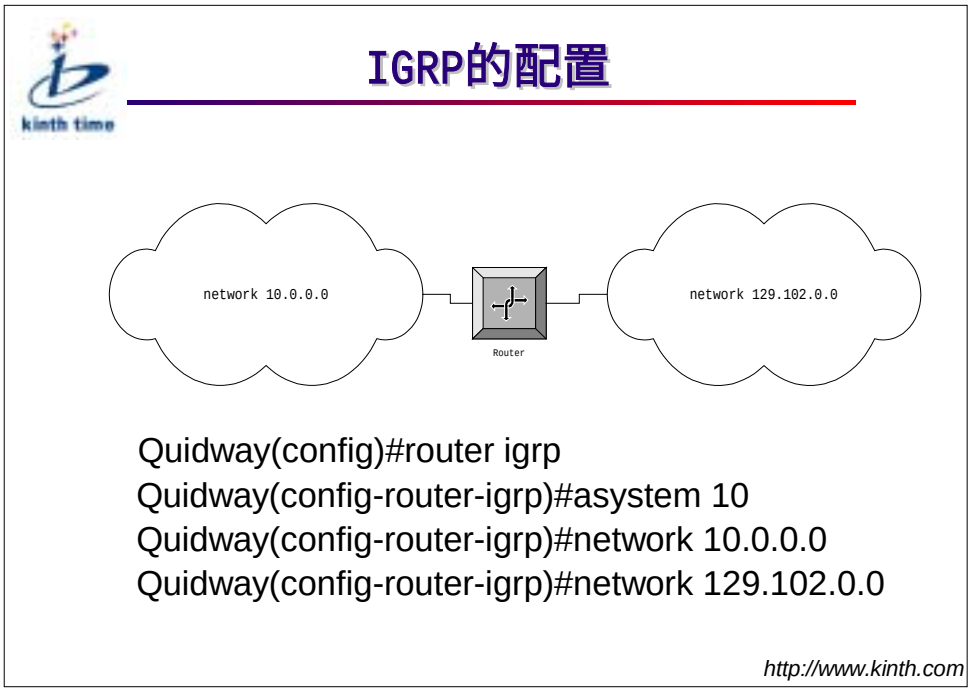
在实际计算路由权时，通常情况下不考虑信道可信度和占用率，最大传输单元根据实际接口特性获得，以下列举几个典型网络的带宽和时延：

卫星传输： 时延 2,000,000 ms ，带宽 500Mbit；

10M 以太网： 时延 1,000 ms ，带宽 10,000Kbps；

64K 专线： 时延 20,000 ms ，带宽 64Kbps。

.4.4 IGRP 的配置



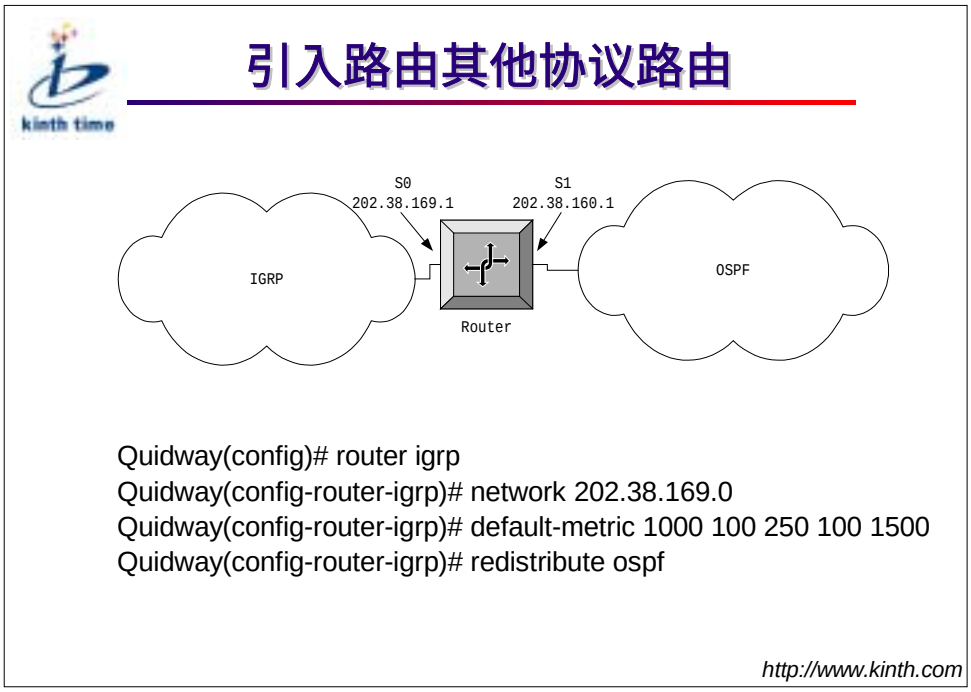
IGRP 协议的配置很简单，主要有以下几个步骤：

☞ router igrp 命令启动 IGRP 协议进程；

☞ asystem 10 命令配置 IGRP 的自治系统号，此自治系统号要求和对端路由器的自治系统号保持一致；

☞ network 10.0.0.0 和 network 129.102.0.0 命令分别在相应的网络范围内的接口上使能 IGRP 协议。

.4.5 引入其他协议路由



路由器一般可以支持多种路由协议，各种路由协议之间可以通过互相引用来共享彼此的路由信息。

IGRP 协议在引入其他协议路由时可以设定引入路由的路由权，如果没有设定，则必需使用 default-metric 命令设定缺省路由权，没有设定引入路由权的引入路由协议会使用缺省路由权作为它的路由权。注意：缺省路由权的缺省值为不可达，所以引入路由时一定要设定引入路由权或设定缺省路由权。

Default-metric 命令的配置表示：路径的带宽 1000kb/s，拓扑延迟 1000 微秒，路径的可信度 98%，路径的通道占用率 39%，最大传输单元 1500 字节。

注意路由器上需配置了 OSPF 协议。

.4.6 IGRP 协议的监控和调试

对 IGRP 协议的监控和调试主要使用以下命令：

show ip igrp 命令可以显示当前 IGRP 协议中各个配置项的值，包括缺省配置的参数值。

debug ip igrp packet 命令打开 IGRP 协议的调试开关，可以看到 IGRP 协议的收发报文情况。下面是一个 IGRP 的典型收发报文的示例：

Quidway 路由器收发对端路由器收到的报文：

IGRP:receive update from 12.0.0.4 (Ethernet0)

packet:vers 1, edition 1, as 1, interior 0, system 1, exterior 0, length 26

dest 98.0.0.0 , metric 180571,hop 0

Quidway 路由器发送更新报文：

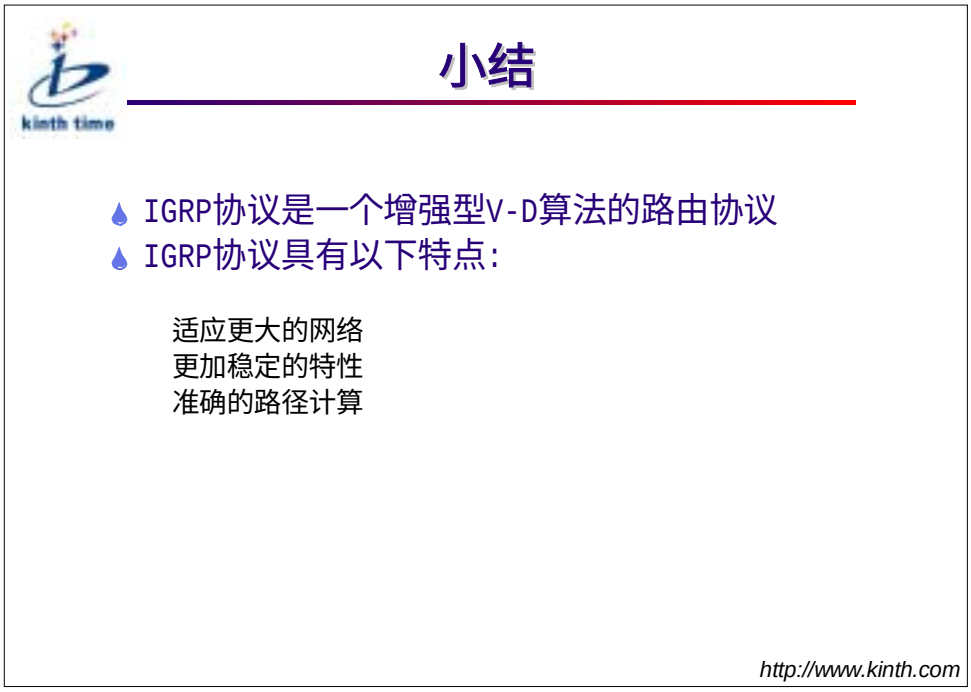
IGRP: send update 12.0.0.1 to 255.255.255.255 (ethernet0)

packet: vers 1, edition 8, as 1, interior 0, system 2,exterior 0,length 40

dest 30.0.0.0 , metric 1041700,hop 0

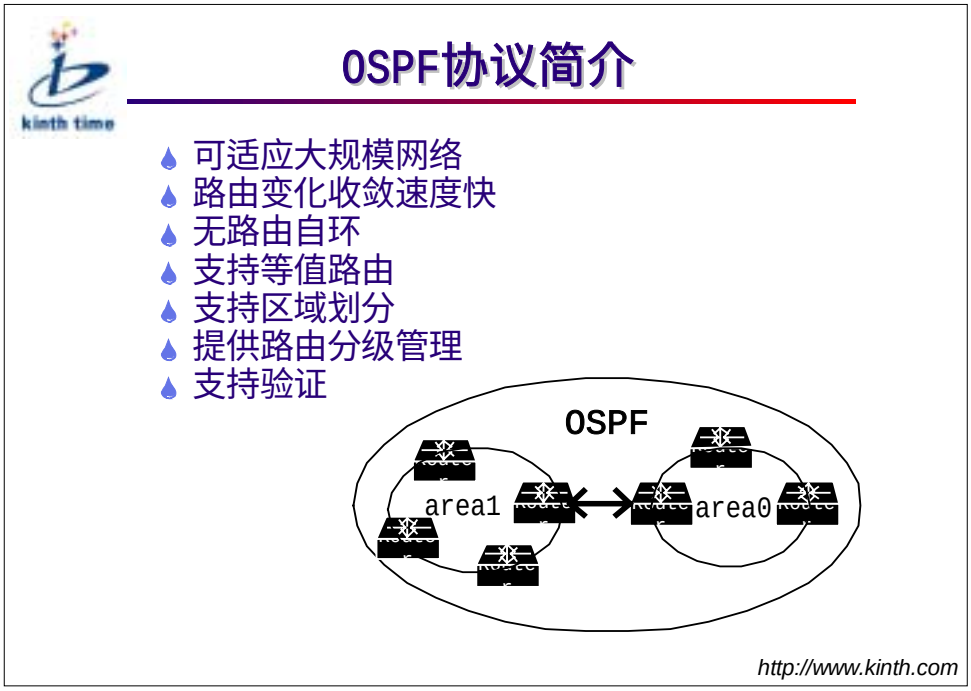
dest 20.0.0.0 , metric 1041700,hop 0

.4.7 小结


小结
IGRP协议是一个增强型V-D算法的路由协议
IGRP协议具有以下特点:
适应更大的网络
更加稳定的特性
准确的路径计算
http://www.kinth.com

.5 OSPF 协议及配置

.5.1 OSPF 协议概述



OSPF 是 Open Shortest Path First（即“开放最短路由优先协议”）的缩写。它是 IETF 组织开发的一个基于链路状态的自治系统内部路由协议。在 IP 网络上，它通过收集和传递自治系统的链路状态来动态地发现并传播路由。

☞ 适应范围 —— OSPF 支持各种规模的网络，最多可支持几百台路由器。

☞ 快速收敛 —— 如果网络的拓扑结构发生变化，OSPF 立即发送更新报文，使这一变化在自治系统中同步。

☞ 无自环 —— 由于 OSPF 通过收集到的链路状态用最小生成树算法计算路由，故从算法本身保证了不会生成自环路由。

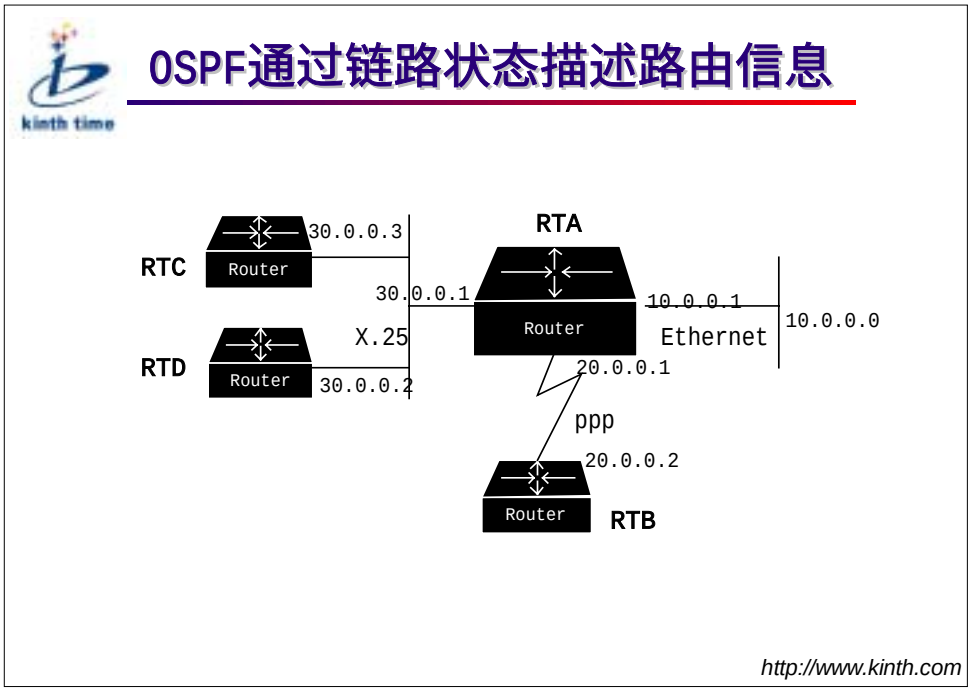
☞ 区域划分 —— OSPF 协议允许自治系统的网络被划分成区域来管理，区域间传送的路由信息被进一步抽象，从而减少了占用网络的带宽。

☞ 等值路由 —— OSPF 支持到同一目的地址的最多三条等值路由。

☞ 路由分级 —— 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。

☞ 支持验证 —— 它支持基于接口的报文验证以保证路由计算的安全性。

.5.2 链路状态



上图中 RTA 通过 PPP 协议与另一台路由器 RTB 直接相连，通过一个 X.25 网络与 RTC 和 RTD 相连，并且 RTA 连接着一个局域网。RTA 通过如下的一条 LSA（链路状态广播）来描述周边网络的拓扑结构。

连接数目 = 3 ；本路由器一共有三个连接

/* 对 X.25 网络的描述*/

连接标识 = 30.0.0.3 ；本网段中某台路由器的 IP 地址.

连接数据 = 30.0.0.1 ；RTA 连接到本网段的接口的 IP 地址

连接类型 = 2 ；连接的类型是一个转换网段（网段中还有其它 路由器）

连接花费 = 1 ；从 30.0.0.1 接口发送报文的花费值

/* 对 Ethernet 的描述*/

连接标识 = 10.0.0.0 ；本网段的地址

连接数据 = 0xff000000 ；本网段的掩码

连接类型 = 3 ；连接的类型是一个末端网段（网段中没有其它 路由器）

连接花费 = 2 ；从 10.0.0.1 接口发送报文的花费值

/* 对 ppp 的描述*/

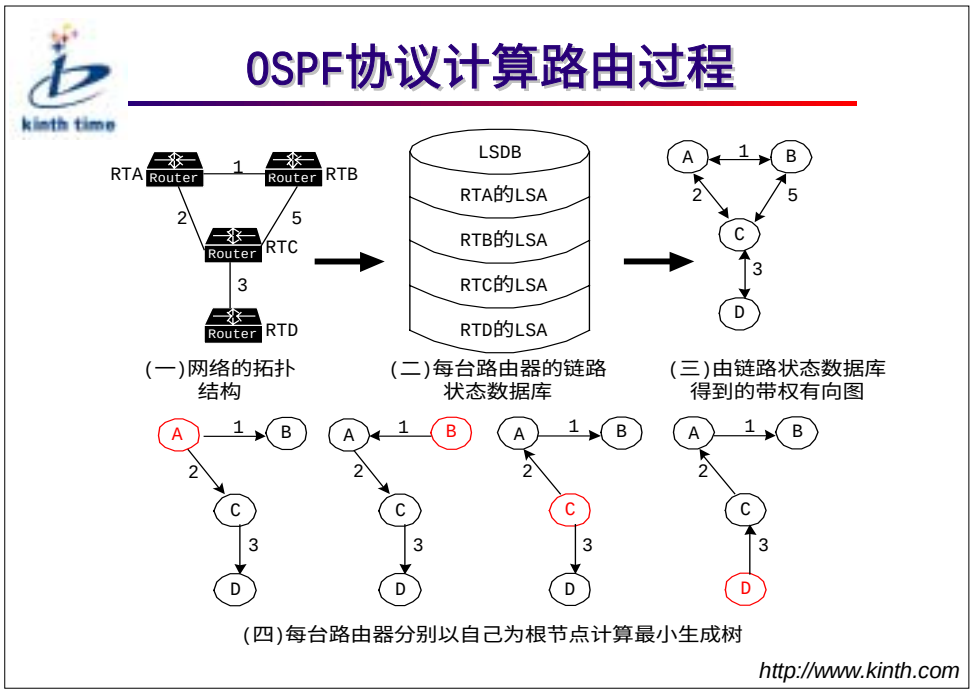
连接标识= 20.0.0.2 ；邻接点 RTB 的路由器标识(router id)

连接数据= 20.0.0.2 ；邻接点 RTB 的 IP 地址

连接类型= 1 ；连接的类型是另一台路由器

连接花费= 8 ；从 20.0.0.1 接口发送报文的花费值

.5.3 计算路由



上图中描述了通过 OSPF 协议计算路由的过程。

（一）由四台路由器组成的网络，连线旁边的数字表示从一台路由器到另一台路由器所需要的花费。为简化问题，我们假定两台路由器相互之间发送报文所需花费是相同的。

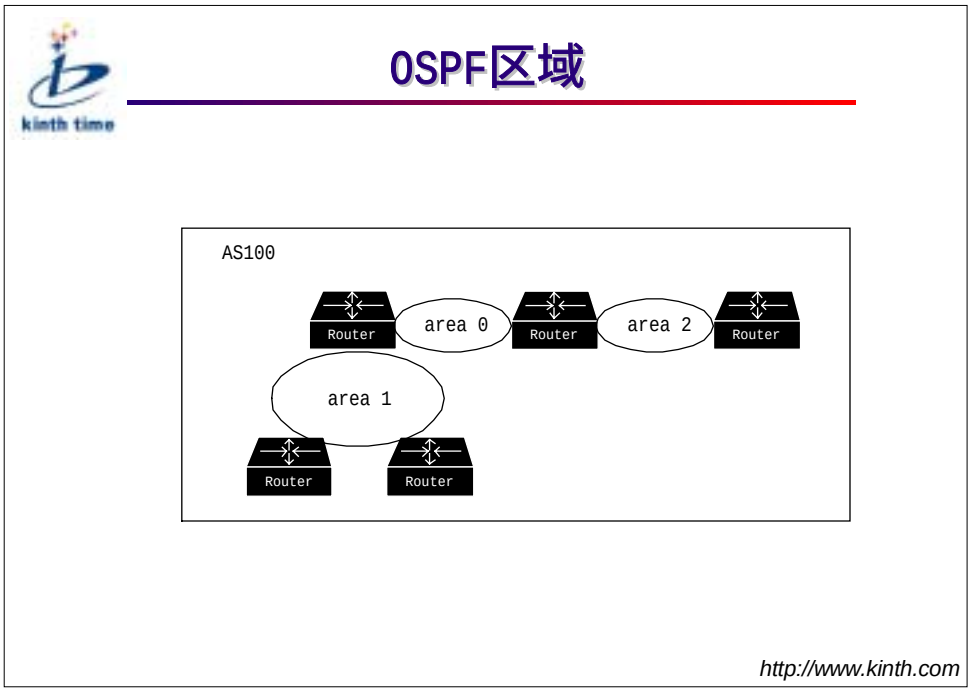
（二）每台路由器都根据自己周围的网络拓扑结构生成一条 LSA（链路状态广播），并通过相互之间发送协议报文将这条 LSA 发送给网络中其它的所有路由器。这样每台路由器都收到了其它路由器的 LSA，所有的 LSA 放在一起称作 LSDB（链路状态数据库）。显然，4 台路由器的 LSDB 都是相同的。

（三）由于一条 LSA 是对一台路由器周围网络拓扑结构的描述，那么 LSDB 则是对整个网络的拓扑结构的描述。路由器很容易将 LSDB 转换成一张带权的有向图，这张图便是对整个网络拓扑结构的真实反映。显然，4 台路由器得到的是一张完全相同的图。

（四）接下来每台路由器在图中以自己为根节点，使用相应的算法计算出一棵最小生成树，由这棵树得到了到网络中各个节点的路由表。显然，4 台路由器各自得到的路由表是不同的。

这样每台路由器都计算出了到其它路由器的路由。

.5.4 区域划分



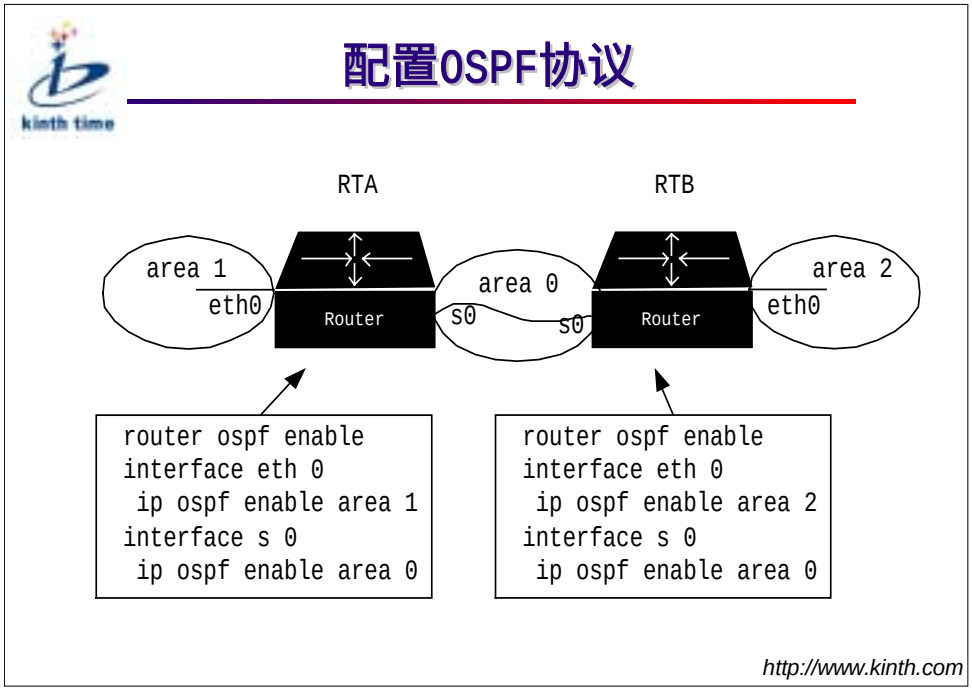
OSPF 协议允许自治系统的网络被划分成区域来管理，区域间传送的路由信息被进一步抽象，从而减少了占用网络的带宽。

本图中在 AS100 内运行 OSPF 协议，自治系统被划分为三个不同的区域，分别用不同的区域号（AREA ID）来标识。其中区域号为 0 的区域被称作“骨干区域”。

注意：

如果自治系统被划分成一个以上的区域，则必须有一个区域是骨干区域，并且保证其它区域与骨干区域直接相连或逻辑上相连，且骨干区域自身也必须是连通的。

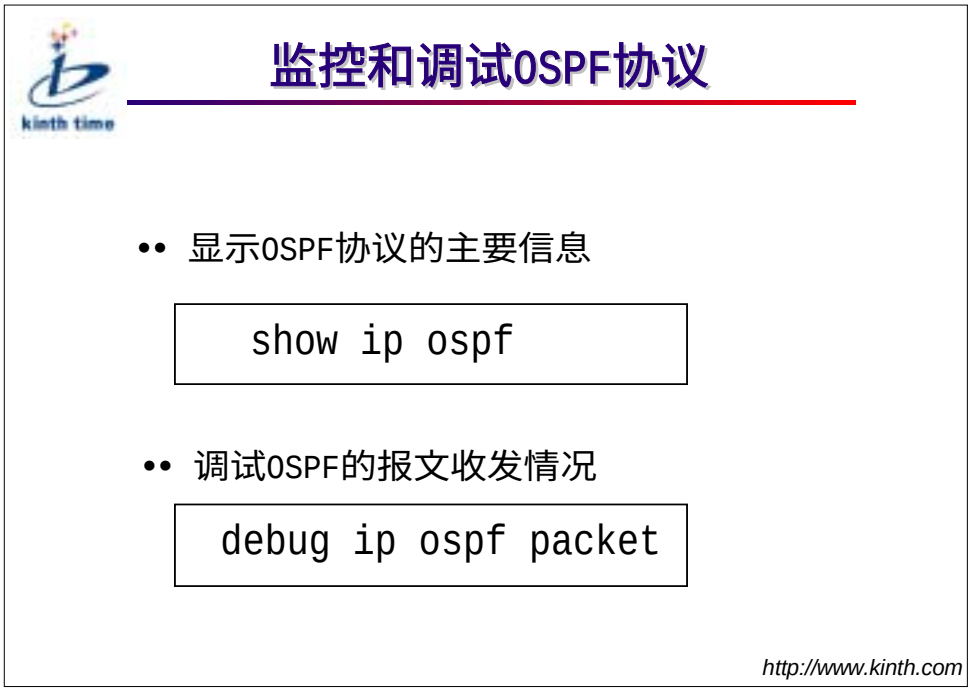
.5.5 OSPF 协议配置



本例中 RTA 在两个接口上配置 OSPF 协议，以太网配置为区域 1，串口 S0 配置成区域 0。

命令	含义
router ospf enable	启动 OSPF 协议
ip ospf enable area 0	指定本接口运行的区域号

.5.6 调试和监控



用以上两条命令监控和调试 OSPF 协议。

show ip ospf 命令可以查看当前路由器配置 OSPF 的情况：路由器的标识（router id），区域状态，接口状态，引入的外部路由情况等。

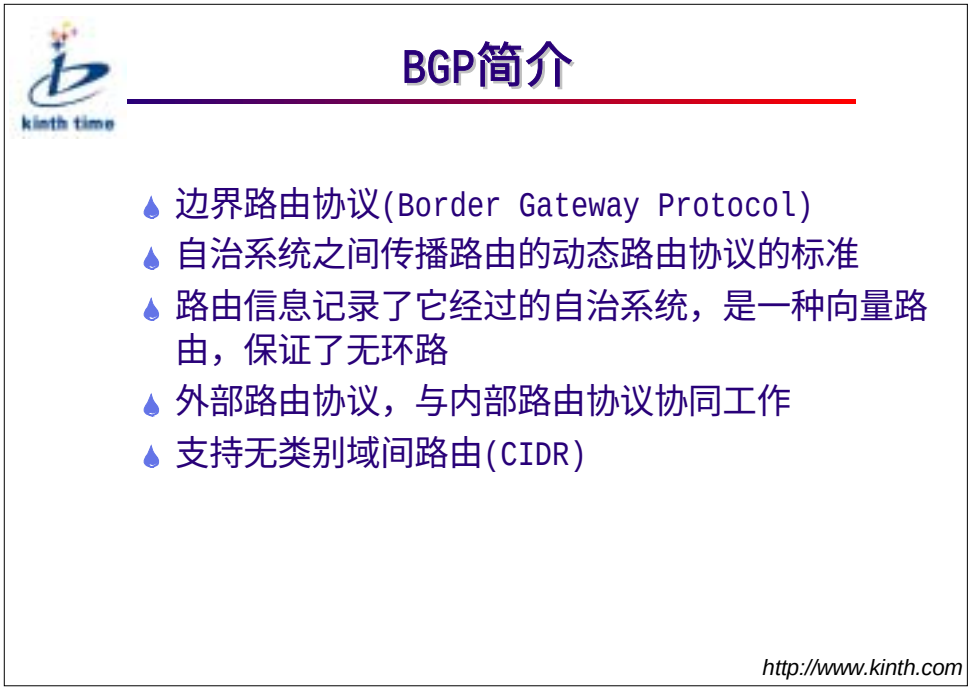
debug ip ospf packet 可以监控 OSPF 协议收发报文的情况，并打印出报文内容。

.5.7 小结


OSPF小结
OSPF是基于链路状态的协议
OSPF通过最小生成树来产生路由
OSPF将整个网络化分成不同的区域
http://www.kinth.com

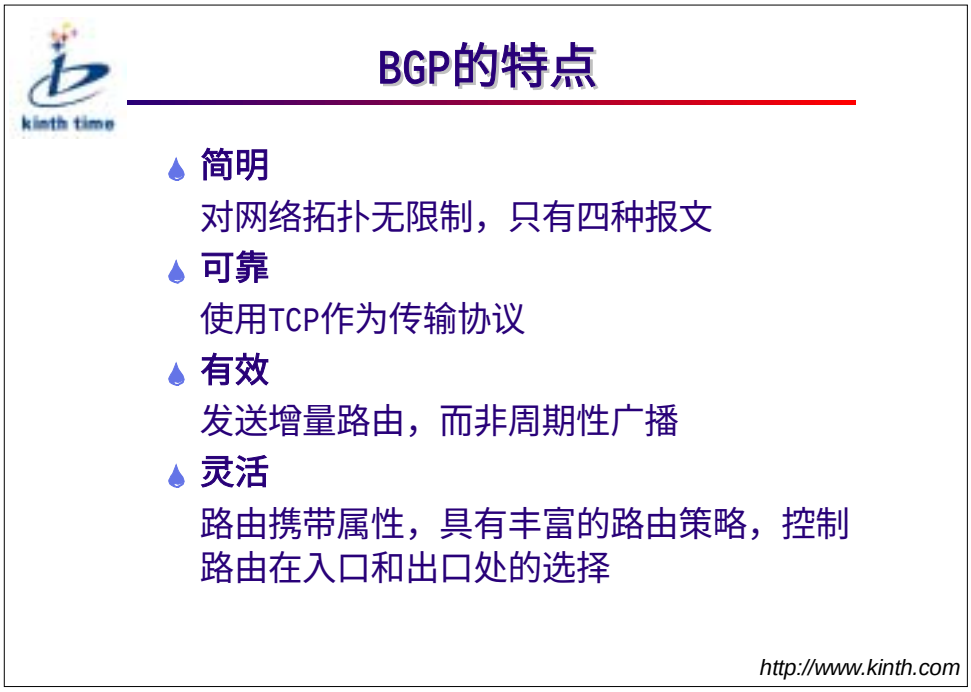
.6 BGP 协议及配置

.6.1 BGP 简介



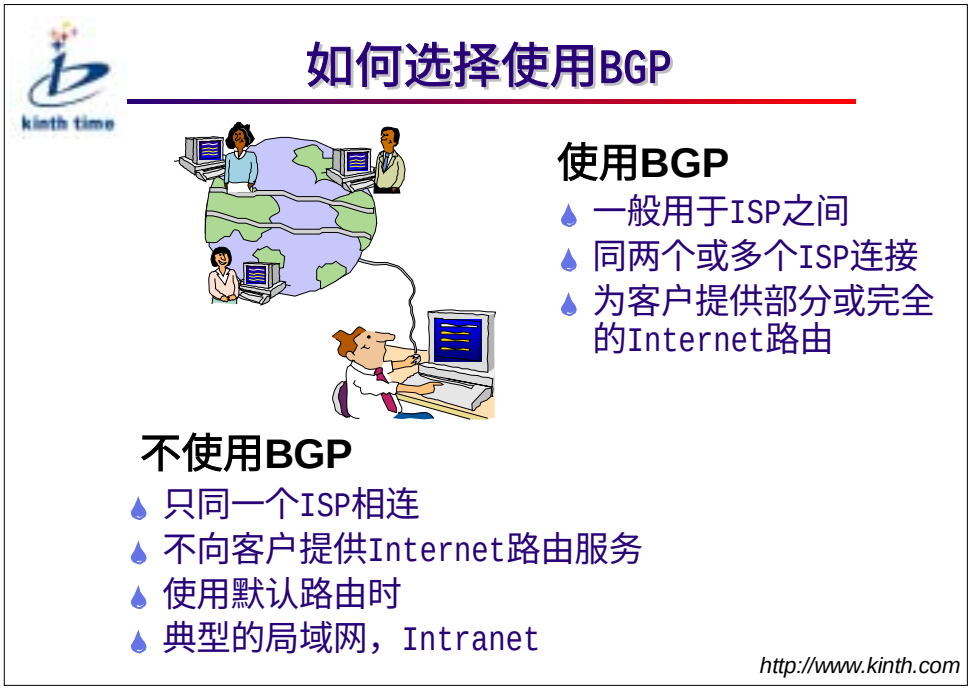
BGP 的最初版本在 1989 年提出，发展到 1993 年开始开发的 BGP4 ，它是自治系统之间的事实上的路由协议的标准。边界是指自治系统的边界。它是一种外部路由协议，与 OSPF、RIP 等内部路由协议不同，其着眼点不在于发现和计算路由，而在于控制路由的传播和选择最好的路由。因此，BGP 不是单独工作的，它同内部路由协议协同，内部路由协议（如 OSPF）在自治系统内工作，而 BGP 在自治系统之间工作。它是第一个支持 CIDR 的路由协议，通过路由聚合可以有效的抑制因特网上路由的爆炸性增长。通过携带 AS 路径信息，它可以彻底解决路由循环问题。

.6.2 BGP 的特点



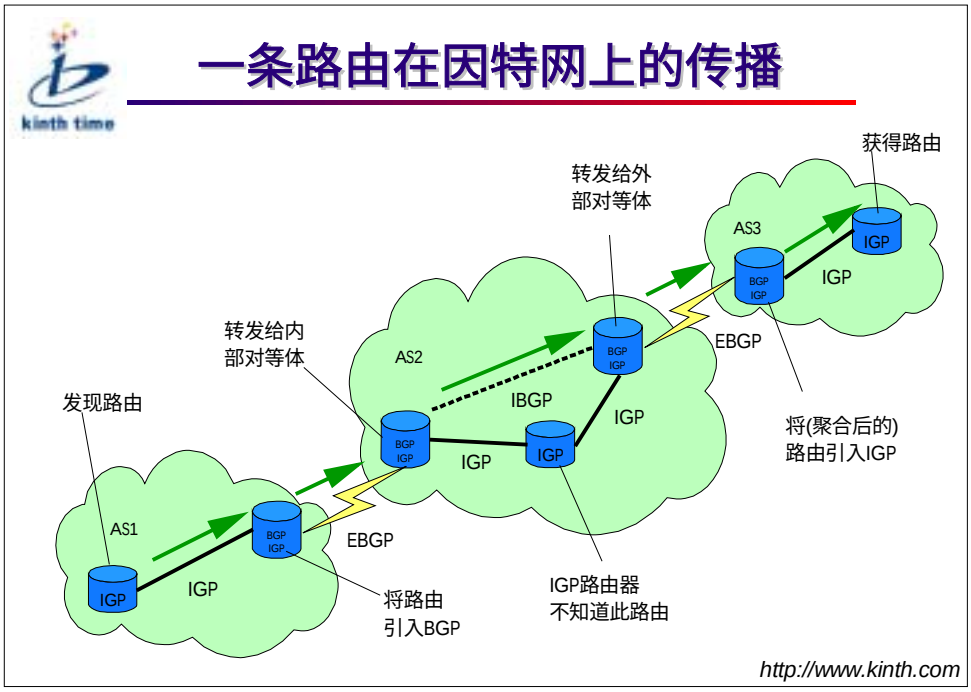
BGP 协议看起来很简单，它并不需要规划网络的拓扑，事实上，Internet 并不是从上而下由某个组织建立起来的，而是一些网络自下而上互相连接而成的，每个这样的网络称为一个自治系统。
而由于政治的、经济的原因，每个自治系统希望对路由进行过滤、选择和控制，因此，BGP 路由携带了丰富的属性，由 BGP 的路由策略来使用，正是这一特性使得 BGP 是如此简明而又如此灵活和强大，它还使得 BGP 便于扩展，以支持因特网新的发展。BGP 协议使用 TCP 作为其传输层协议，不仅提高了协议的可靠性，而且使得发送增量路由成为可能，这就大大减少了 BGP 传播路由所占用的带宽，适用于在 Internet 上传播大量的路由信息。

.6.3 BGP 的适用范围



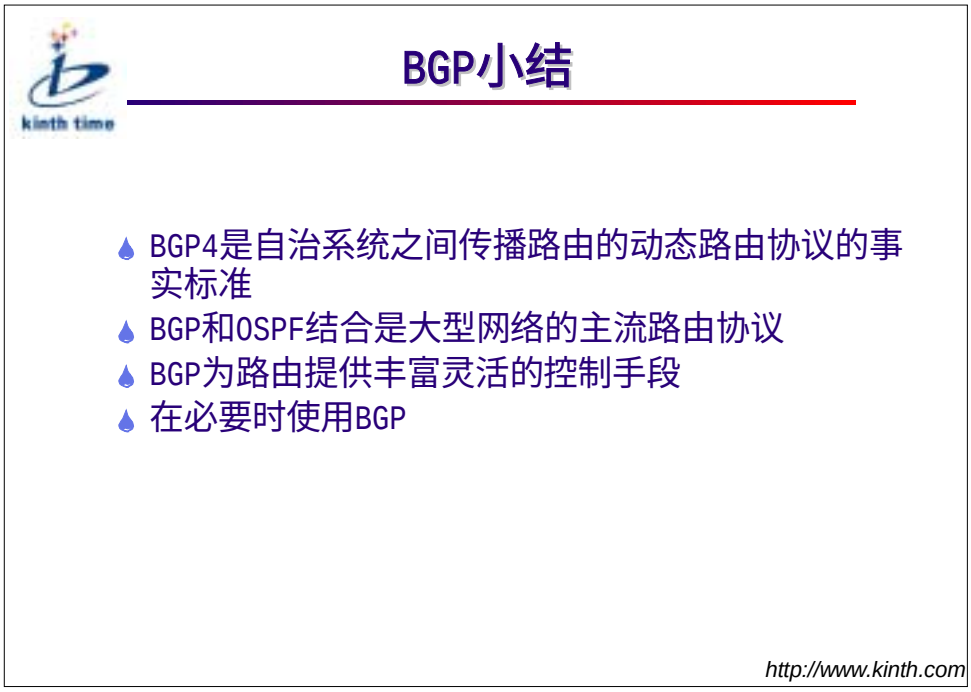
正如前面所述的，BGP 用在自治系统之间。一般来说，在 ISP 之间才需要使用 BGP，在这时，你要同多个 ISP 连接，需要在多个相同目的地的路由之间进行选择，并且为客户提供 Internet 路由。如果你只是 ISP 的客户，同一个 ISP 连接，最简单地，可以使用一个默认路由来指向 ISP，并不需要使用 BGP。对于大多数的局域网和 Intranet 来说，BGP 是一种奢侈品，只有你准备同多个 ISP 连接或成为一个 ISP 时，才使用 BGP。

.6.4 BGP 路由的传播



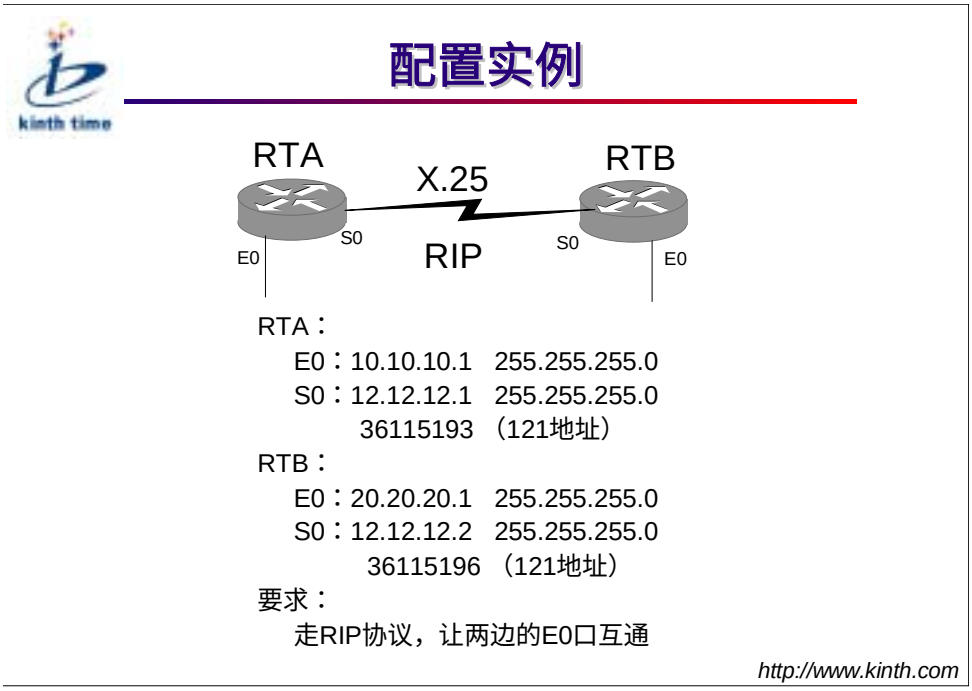
一条路由在一般情况下是从自治系统内部产生的，它由某种内部路由协议发现和计算，传递到自治系统的边界，由自治系统边界路由器（ASBR）通过 BGP 传播到其它自治系统中，这种连接称为 EBGP，两个 ASBR 互称对等体。路由在传播过程中可能会经过若干个自治系统，这些自治系统称为过渡自治系统。若这个自治系统有多个边界路由器，这些路由器之间也运行 BGP 来交换路由信息，称为 IBGP。这时内部的路由器并不需要知道这些外部路由，它们只需要在边界路由器之间维护 IP 连通性。路由到达自治系统边界后，若内部路由器需要知道这些外部路由，ASBR 可以将路由引入内部路由协议。外部路由的数量是很大的，通常会超出内部路由器的处理能力，因此引入外部路由时一般需要过滤或聚合，以减少路由的数量，极端的情况是使用默认路由。

.6.5 小结


kinth time
BGP小结
BGP4是自治系统之间传播路由的动态路由协议的事实标准
BGP和OSPF结合是大型网络的主流路由协议
BGP为路由提供丰富灵活的控制手段
在必要时使用BGP
http://www.kinth.com

.7 配置实例

.7.1 组网介绍



.7.2 数据配置

配置实例（续）

RTA路由器的配置：

```
RTA#config
RTA(config)#router  rip
RTA(config)#int e 0
RTA(config-if-Ethernet0)#ip address 10.10.10.1 255.255.255.0
RTA(config-if-Ethernet0)#int  s 0
RTA(config-if-Serial0)#ip address 12.12.12.1 255.255.255.0
RTA(config-if-Serial0)#encap  x25
RTA(config-if-Serial0)#x25  address  36115193
RTA(config-if-Serial0)#x25  map ip 12.12.12.2  36115196  broadcast
RTA(config-if-Serial0)#exit
RTA(config)#exit
RTA#write
```

http://www.kinth.com

在 X25 的地址映射配置中，最后加了一个 broadcast 参数，目的是让 X25 能承载 IP 广播包。因为 RIP 协议是通过广播包发送路由信息的，所以如果不加这个参数的话，两台路由器之间交换不了路由信息。

数据配置（续）

配置实例（续）

RTB路由器的配置：

```
RTB#config
RTB(config)#router  rip
RTB(config)#int e 0
RTB(config-if-Ethernet0)#ip address 20.20.20.1 255.255.255.0
RTB(config-if-Ethernet0)#int  s 0
RTB(config-if-Serial0)#ip address 12.12.12.2 255.255.255.0
RTB(config-if-Serial0)#encap  x25
RTB(config-if-Serial0)#x25  address  36115196
RTB(config-if-Serial0)#x25  map ip 12.12.12.1  36115193  broadcast
RTB(config-if-Serial0)#exit
RTB(config)#exit
RTB#write
```

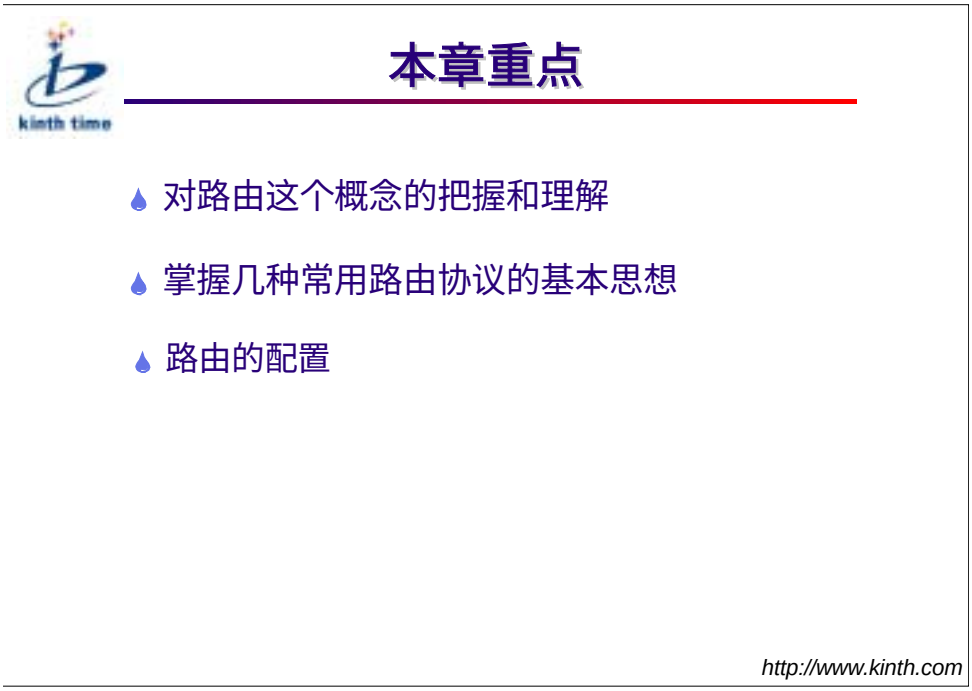
http://www.kinth.com

RTB 路由器的配置与 RTA 路由器的配置类似。需要注意的是在 X25 的地址映射配置中，不要忘记加上 broadcast 参数。

.8 总结


路由协议总结
路由及路由协议的基本概念
路由器上可以配置一种或多种路由协议
介绍了四种动态路由协议及其配置
RIP
IGRP
OSPF
BGP
http://www.kinth.com

.9 本章重点



路由是数据网络基本而又重要的一个概念，必须理解和掌握。
距离矢量和链路状态是动态路由协议两种基本的寻径算法。

第十章 防火墙及配置

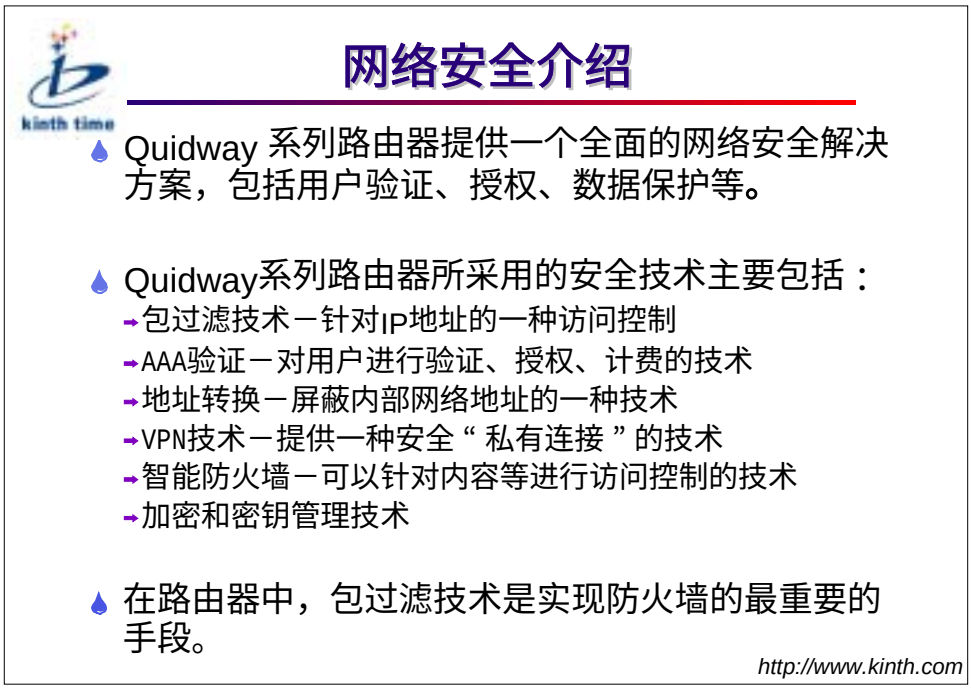
.1 防火墙介绍

现代的防火墙体系不应该只是一个“入口的屏障”，防火墙应该是几个网络的接入控制点，所有经过被防火墙保护的网络的数据流都应该首先经过防火墙，形成一个信息进入的关口。

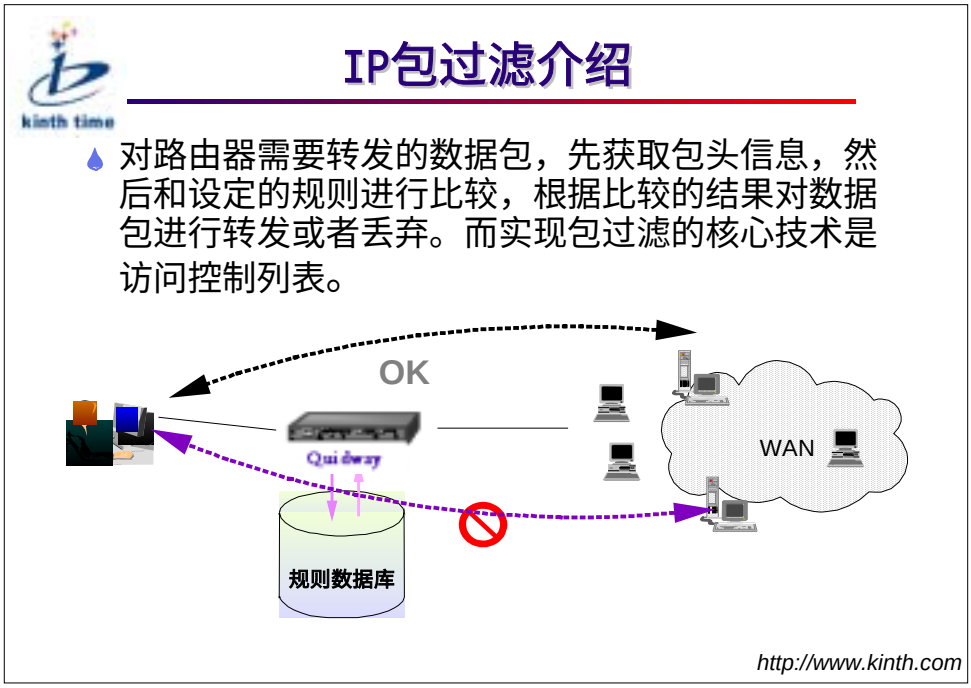
因此防火墙不但可以保护内部网络在 Internet 中的安全，同时还可以保护若干主机在一个内部网络中的安全。在每一个被防火墙分割的网络中，所有的计算机之间是被认为“可信任的”，它们之间的通信不受防火墙的干涉。而在各个被防火墙分割的网络之间，必须按照防火墙规定的“策略”进行互相的访问。

.2 网络安全技术

.2.1 网络安全技术介绍

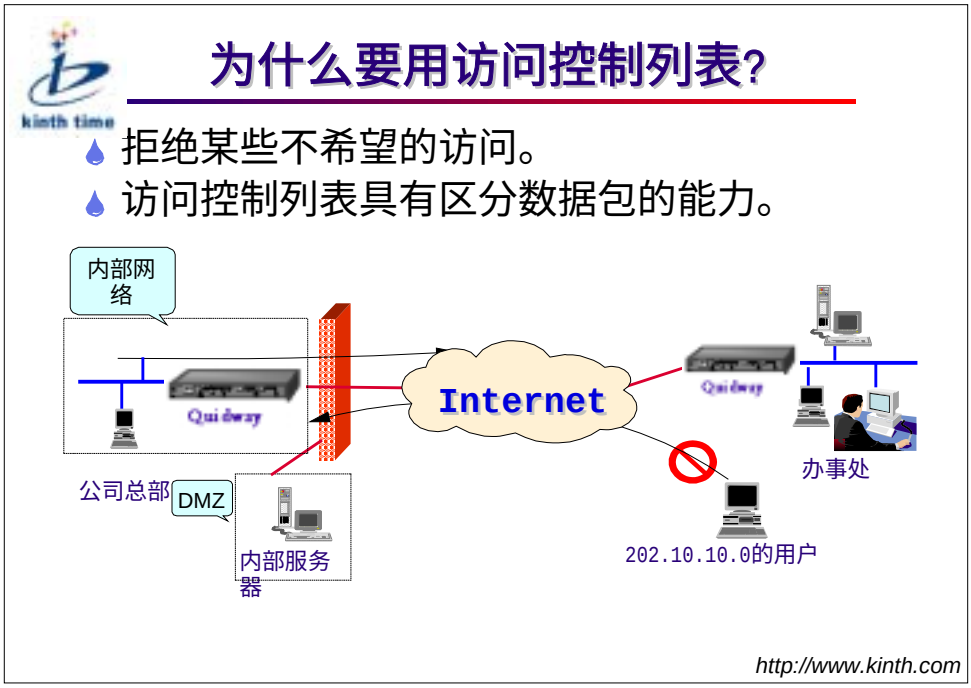


.2.2 IP 包过滤技术介绍



包过滤技术主要是设定一定的规则，控制数据包。路由器会根据设定的规则和数据包的包头信息比较，来决定是否允许这个数据包通过。实现包过滤技术最核心内容就是访问控制列表。

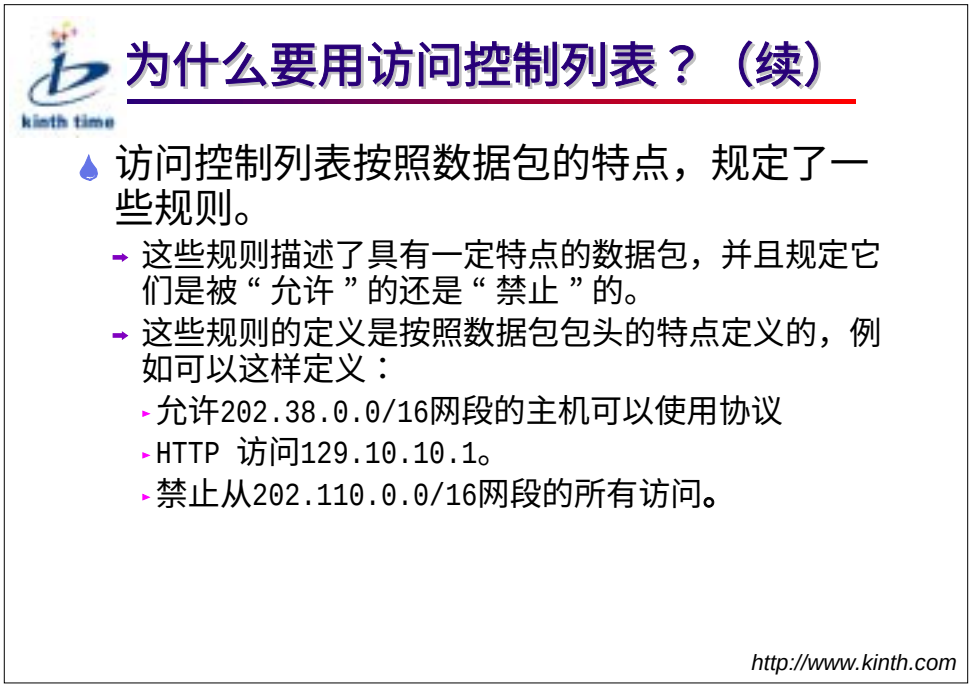
.2.3 访问控制列表



用户可以通过 Internet 和外部网络进行联系，网络管理员都面临着一个问题，就是如何拒绝一些不希望的连接，同时又要保证合法用户进行的访问。

为了达到这样的效果，我们需要有一定的规则来定义哪些数据包是“合法”的（或者是可以允许访问），哪些是“非法”的（或者是禁止访问）。这些规则就是访问控制列表。

访问控制列表（续）

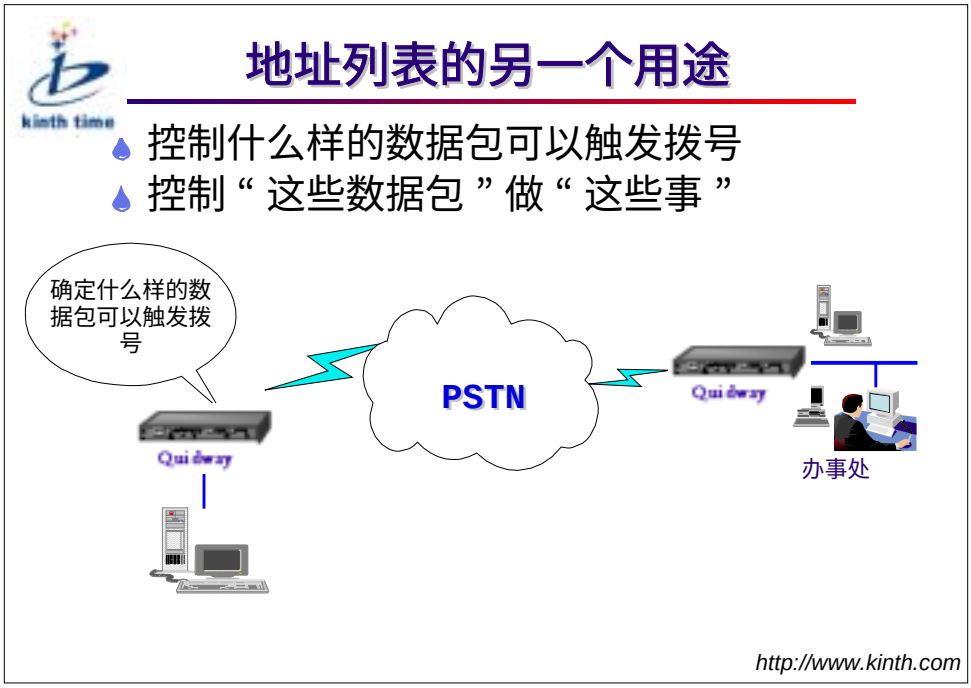


访问控制列表就可以提供这样的功能，它按照数据包的特点，规定了一些规则。

这些规则描述了具有一定特点的数据包，（例如所有源地址是202.10.10.0 地址段的数据包、所有使用 Telnet 访问的数据包等等）并且规定它们是被“允许”的还是“禁止”的。

这样可以将访问控制列表规则应用到路由器的接口，阻止一些非法的访问，同时并不影响合法用户的访问。访问控制列表提供了一种区分数据包种类的手段，它把各种数据包按照各自的特点区分成各种不同的种类，达到控制用户访问的目的。

.2.4 地址列表的其他用途

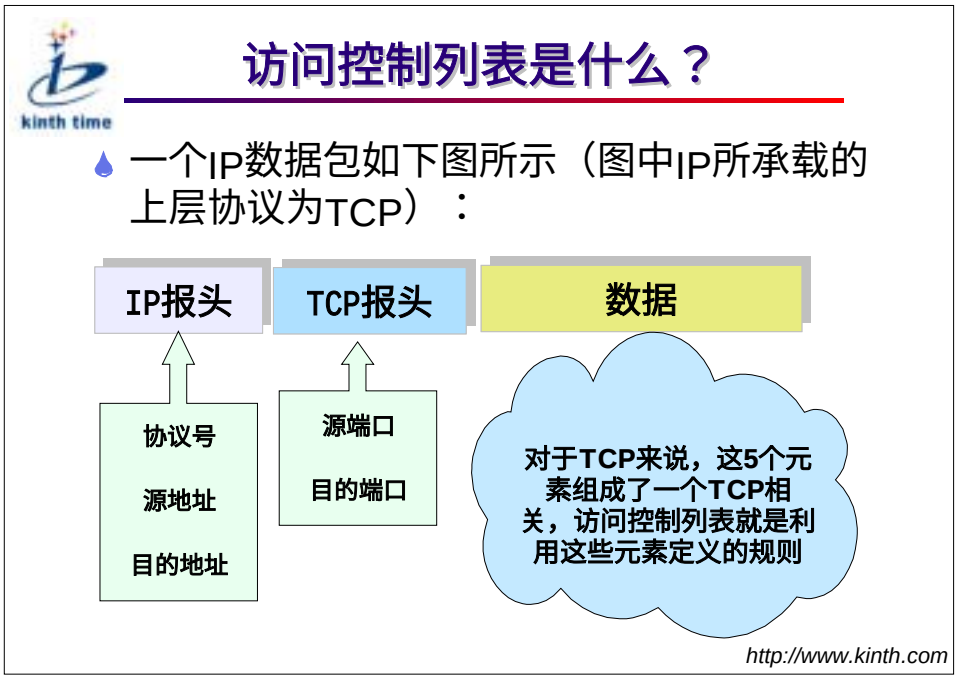


由于访问控制列表具有区分数据包的功能，因此，访问控制列表可以控制“什么样的数据包”，可以做什么样的事情。

例如，当企业内部网通过拨号方式访问 Internet ，如果不希望所有的用户都可以拨号上网，就可以利用控制列表决定哪些主机可以触发拨号，以达到访问 Internet 的目的。

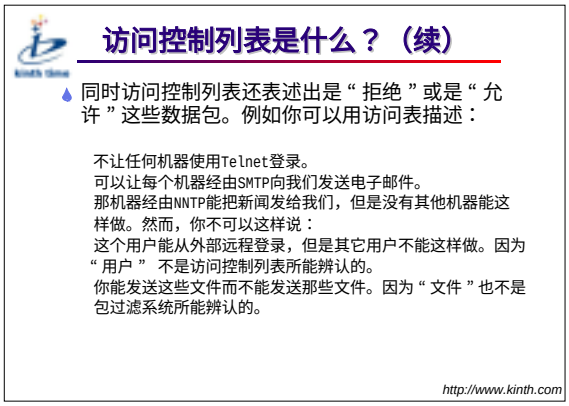
利用访问控制列表可以控制数据包的触发拨号，同样在 IPSec、地址转换等应用中，可以利用控制列表描述什么样的数据包可以加密，什么样的数据包可以地址转换等。

.2.5 访问控制列表原理

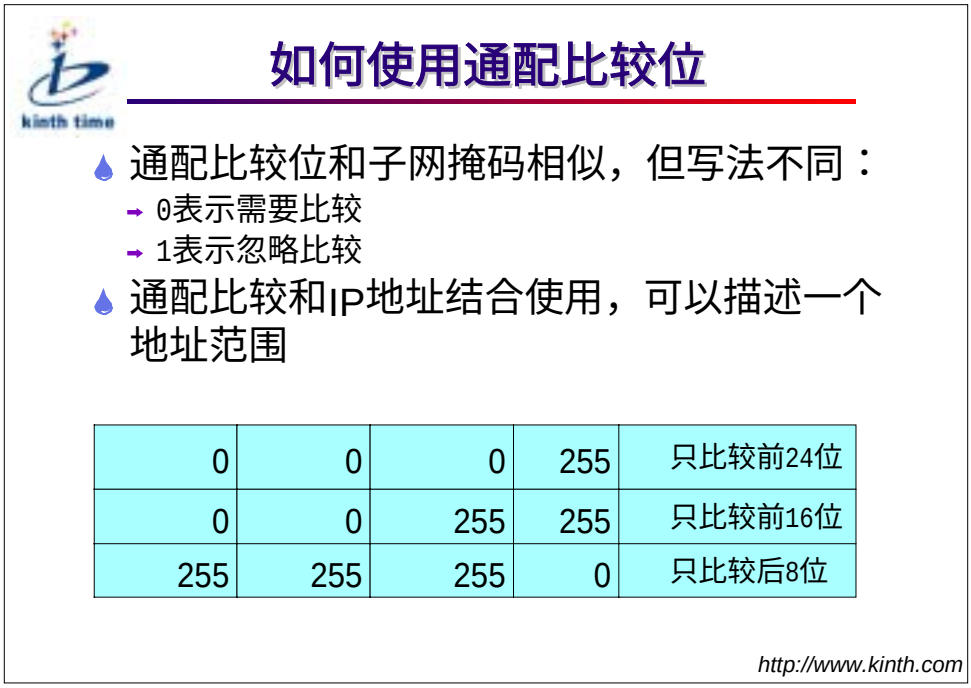


IP 数据包具有一定的特征，例如，对于每个 TCP 数据包，都包含有上图所示的 5 个元素，利用这 5 个元素就可以描述出一个数据包的特征。访问控制列表利用的就是这些包头的信息来定义规则的。

访问控制列表原理（续）

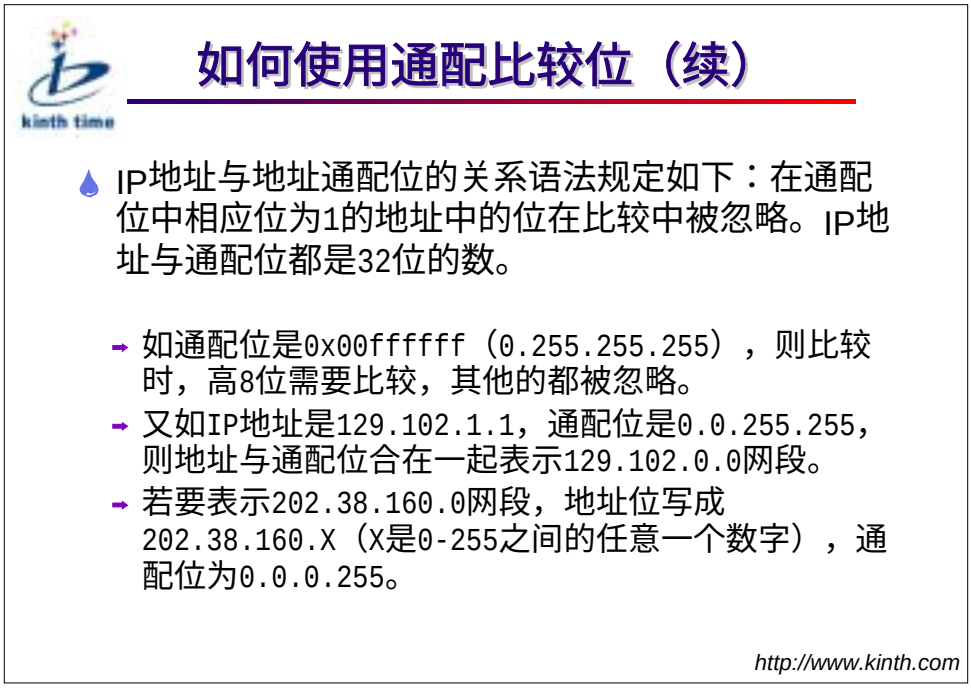

访问控制列表是什么？（续）
同时访问控制列表还表述出是“ 拒绝 ”或是“ 允许 ”这些数据包。例如你可以用访问表描述：
不让任何机器使用Telnet登录。
可以让每个机器经由SMTP向我们发送电子邮件。
那机器经由NNTP能把新闻发给我们，但是没有其他机器能这样做。然而，你不可以这样说：
这个用户能从外部远程登录，但是其它用户不能这样做。因为“ 用户 ” 不是访问控制列表所能辨认的。
你能发送这些文件而不能发送那些文件。因为“ 文件 ”也不是包过滤系统所能辨认的。
http://www.kinth.com

访问控制列表原理（续）

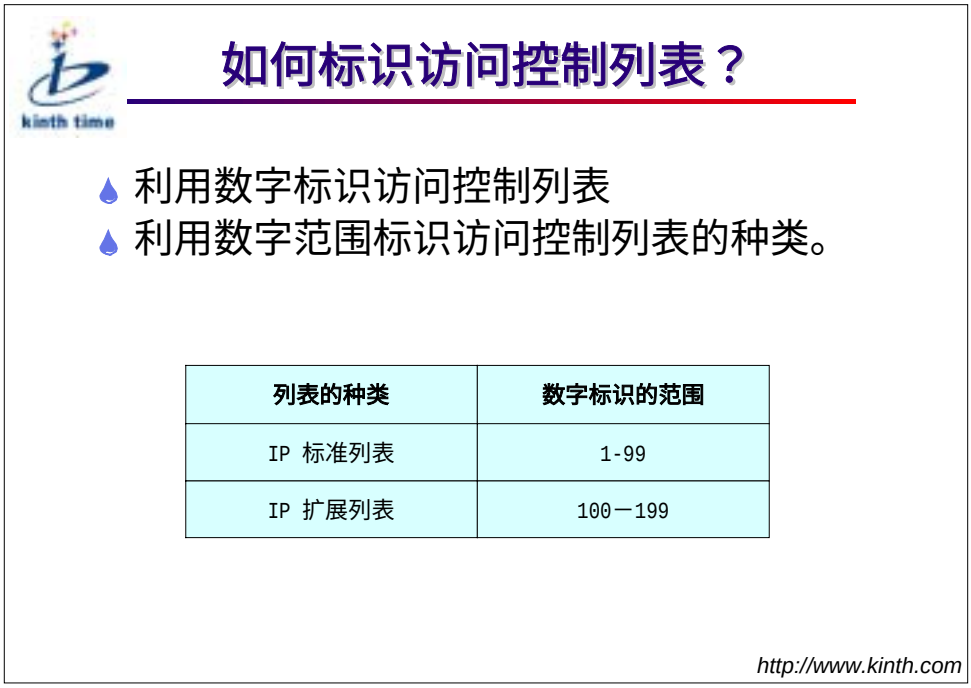


通配比较位的意义和子网掩码很相似，但是用法上是不一样的。利用通配比较位可以定义一个范围内的地址。例如定义一个 10.110.0.0/16 网段的所有主机。

访问控制列表原理（续）


如何使用通配比较位（续）
IP地址与地址通配位的关系语法规定如下：在通配位中相应位为1的地址中的位在比较中被忽略。IP地址与通配位都是32位的数。
如通配位是0x00ffffff（0.255.255.255），则比较时，高8位需要比较，其他的都被忽略。
又如IP地址是129.102.1.1，通配位是0.0.255.255，则地址与通配位合在一起表示129.102.0.0网段。
若要表示202.38.160.0网段，地址位写成202.38.160.X（X是0-255之间的任意一个数字），通配位为0.0.0.255。
http://www.kinth.com

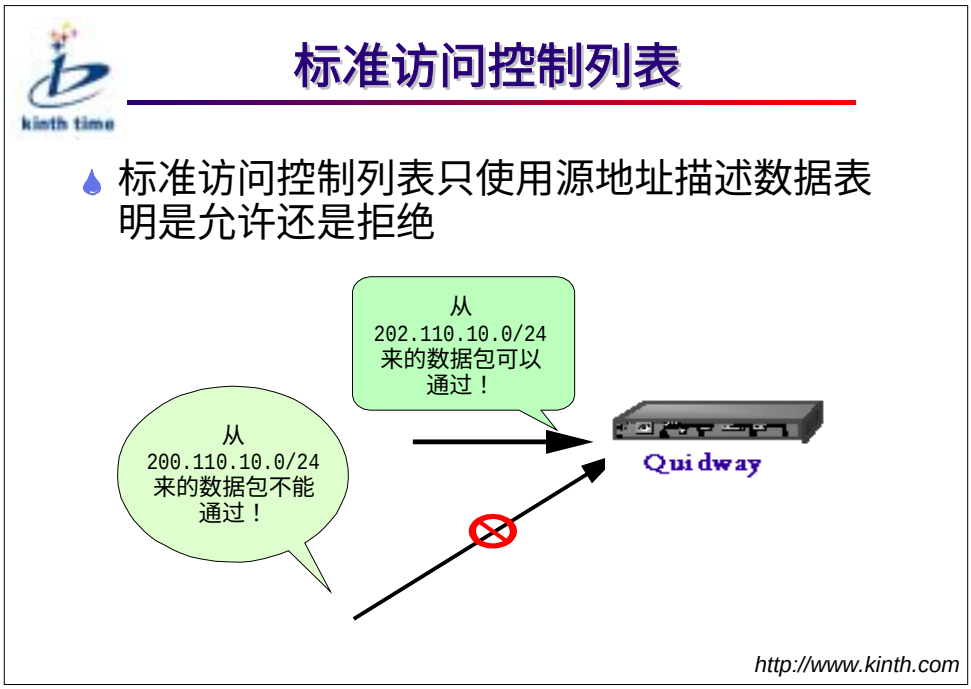
访问控制列表原理（续）



在配置访问控制列表时，有一个规则序列号，利用这个规则序列号来标识访问控制列表，同时提供了引用访问控制列表的方法。
规则序列号的范围表示了它属于什么样的访问控制列表。例如：
access-list 1 permit 202.110.10.0 0.0.0.255
表示序号为 1 的访问控制列表，它是标准访问列表。
access-list 100 deny udp any any eq rip
表示序号为 100 的访问控制列表，它是扩展访问列表。

.3 标准访问控制列表

.3.1 标准访问控制列表概况



标准列表的规则序列号的范围为：1~99。
标准列表只使用 1 个条件判别数据包：数据包的源地址。
标准访问列表可以指定一个源地址段，这是由 IP 地址和地址通配符组合定义的一个地址段。

.3.2 标准访问控制列表的命令配置

此格式表示：允许或拒绝来自指定网络的数据包，该网络由 IP 地址（ip-address）和地址通配掩码位（wildcard-mask）指定。其中：

normal 和 special 表示该规则是在普通时间段中有效还是在特殊时间段中有效。

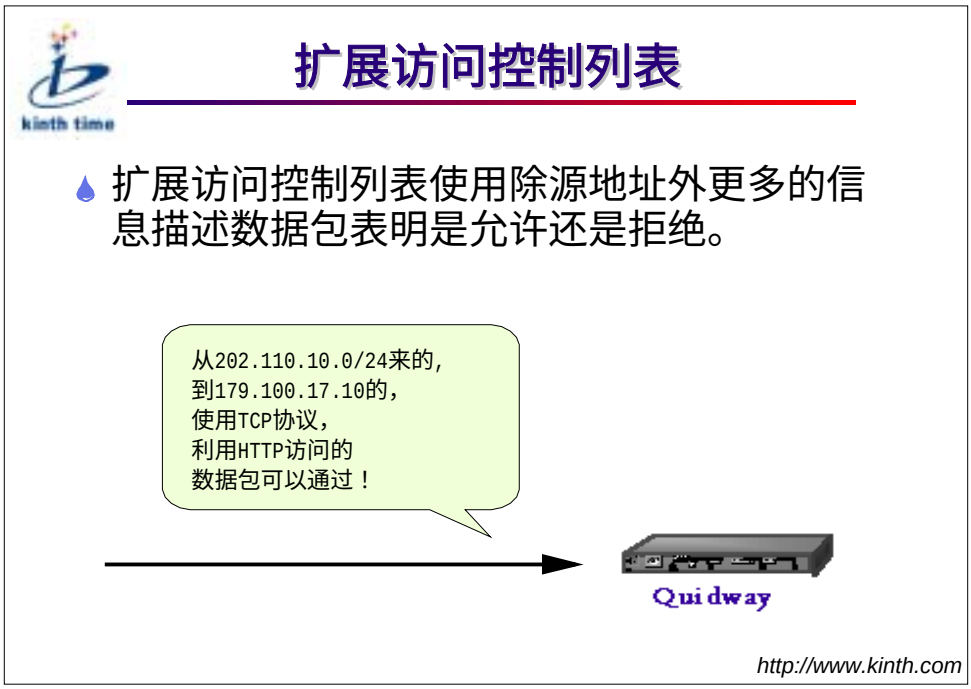
listnumber 为规则序号，标准访问列表的规则序号范围为 1-99。

permit 和 deny 表示允许或禁止满足该规则的数据包通过 。

ip-address 和 wildcard-mask 分别为 IP 地址和通配比较位，用来指定某个网络。如果 IP 地址指定为 any ，则表示所有 IP 地址，而且不需配置指定相应的通配位（通配位缺省为 0.0.0.0 ）。

.4 扩展访问控制列表

.4.1 扩展访问控制列表概况

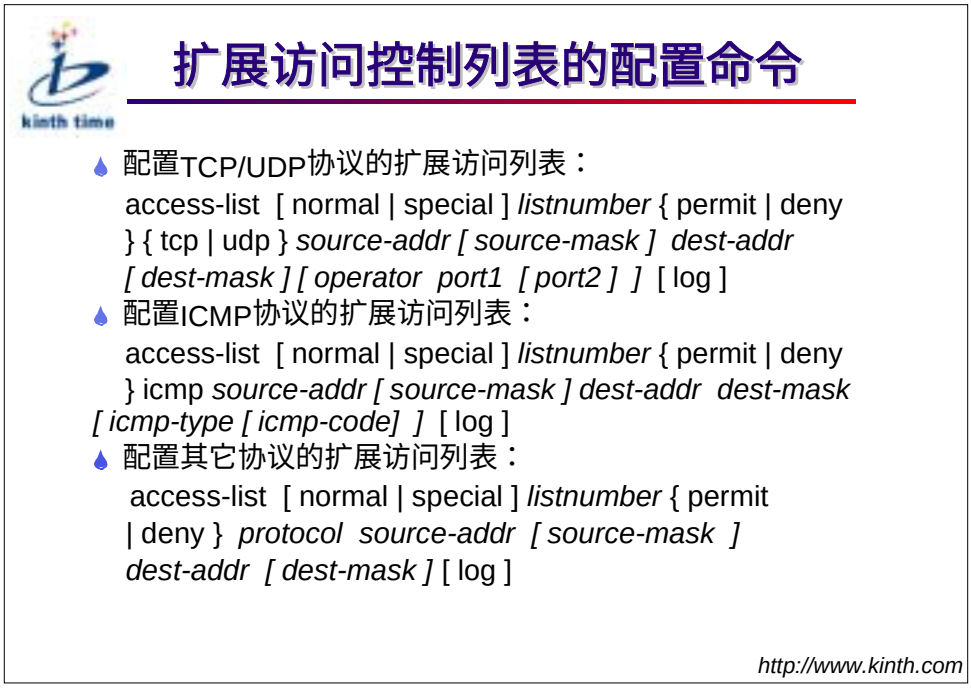


扩展列表使用数据包的源地址的同时，还使用目的地址，和协议号（TCP、UDP 等）。

对于 TCP、UDP 协议可以同时使用目的端口号。

例如，利用扩展列表可以描述“从 202.110.10.0/24 的网段到 110.10.10.0/24 的网段的所有 IP 数据包是被拒绝的”，或者“从 202.110.10.0/24 网段到 110.10.10.0/24 网段的所有 Telnet（使用 TCP 协议的 23 端口）访问是被拒绝的”。它们到底如何表示？我们将从具体配置命令来入手来介绍。

.4.2 扩展访问控制列表的配置命令



Normal 和 special 表示该规则是在普通时间段生效还是在特殊时间段有效，缺省的情况是在普通时间段。

Listnumber 为规则序号，扩展访问列表的规则序号范围为 100-199。

Permit 和 deny 表示允许或禁止满足该规则的数据包通过 。

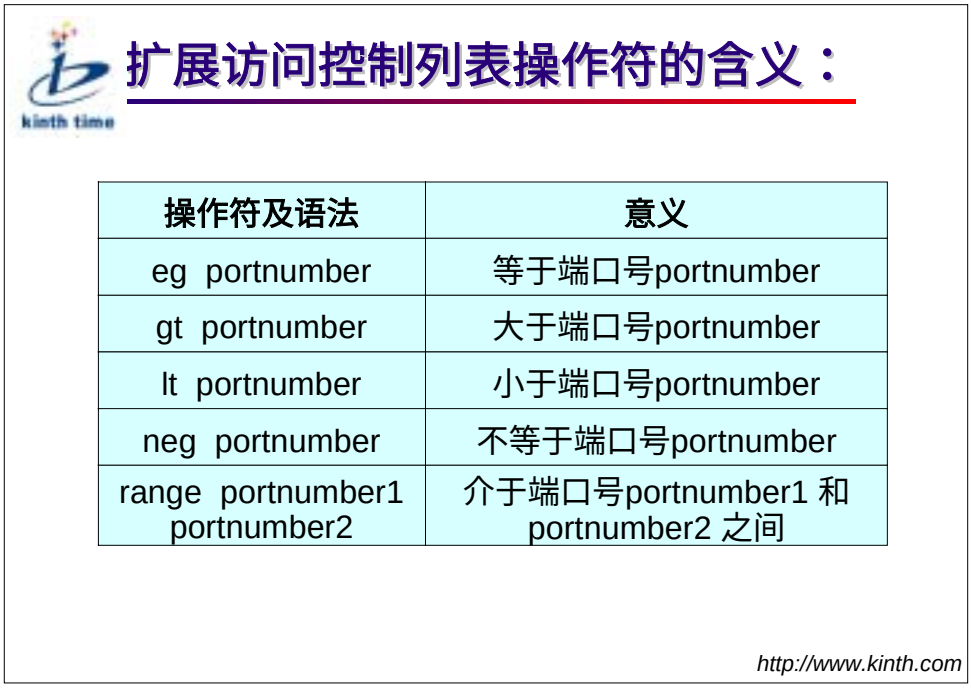
Protocol 可以指定为 0-255 之间的任一协议号（如 1 表示 ICMP 协议），对于常见协议（如 TCP 和 UDP、ICMP），可以直观地指定协议名，若指定为 IP ，则该规则对所有 IP 包均起作用。

source -addr 和 source-mask 分别为源地址和源地址的通配符。

Dest-addr 和 dest-mask 分别为目的地址和目的地址的通配符。如果 IP 地址指定为 any ，则表示所有 IP 地址，而且不需配置指定相应的通配位（通配位缺省为 0.0.0.0） 。

operator port1 - port2 用于指定端口范围，缺省为全部端口号 0-65535，只有 TCP 和 UDP 协议需要指定端口范围。operate 的意义如下页表所示。

扩展访问列表的操作符 operate 定义



在指定 portnumber 时，对于常用的端口号可以使用“助记符”代替。如 FTP、Telnet 等。

下列表格所列为可能用到的各类端口号与助记符的对照表，供参照*。

协议	助记符	意义及实际值
TCP	Bgp	Border Gateway Protocol (179)
	Chargen	Character generator (19)
	Cmd	Remote commands (rcmd, 514)
	Daytime	Daytime (13)
	Discard	Discard (9)
	Domain	Domain Name Service (53)
	Echo	Echo (7)
	Exec	Exec (rsh, 512)
	Finger	Finger (79)
	Ftp	File Transfer Protocol (21)
	Ftp-data	FTP data connections (20)
	Gopher	Gopher (70)
	Hostname	NIC hostname server (101)
	Irc	Internet Relay Chat (194)
	Klogin	Kerberos login (543)
	Kshell	Kerberos shell (544)
	Login	Login (rlogin, 513)
	Lpd	Printer service (515)

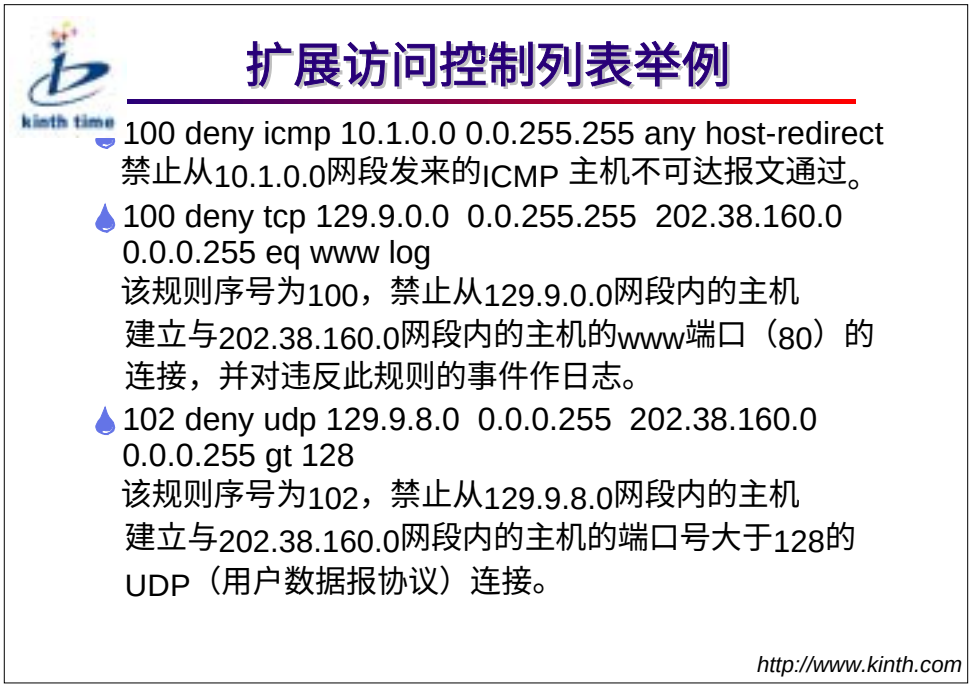
	Nntp	Network News Transport Protocol (119)
	Pop2	Post Office Protocol v2 (109)
	Pop3	Post Office Protocol v3 (110)
	Smtp	Simple Mail Transport Protocol (25)
	Sunrpc	Sun Remote Procedure Call (111)
	Syslog	Syslog (514)
	Tacacs	TAC Access Control System (49)
	Talk	Talk (517)
	Telnet	Telnet (23)
	Time	Time (37)
	Uucp	Unix-to-Unix Copy Program (540)
	Whois	Nicname (43)
	Www	World Wide Web (HTTP, 80)
UDP	biff	Mail notify (512)
	bootpc	Bootstrap Protocol Client (68)
	bootps	Bootstrap Protocol Server (67)
	discard	Discard (9)
	dns	Mail notify (512)
	dnsix	DNSIX Securit Attribute Token Map (90)
	echo	Echo (7)
	mobilip-ag	MobileIP-Agent (434)
	mobilip-mn	MobilIP-MN (435)
	nameserver	Host Name Server (42)
	netbios-dgm	NETBIOS Datagram Service (138)
	netbios-ns	NETBIOS Name Service (137)
	netbios-ssn	NETBIOS Session Service (139)
	ntp	Network Time Protocol (123)
	rip	Routing Information Protocol (520)
	snmp	SNMP (161)
	snmptrap	SNMPTRAP (162)
	sunrpc	SUN Remote Procedure Call (111)
	syslog	Syslog (514)
	tacacs-ds	TACACS-Database Service (65)
	talk	Talk (517)
	tftp	Trivial File Transfer (69)
	time	Time (37)
	who	Who(513)
	xdmcp	X Display Manager Control Protocol (177)

对于 ICMP 协议可以指定 ICMP 报文类型，缺省为全部 ICMP 报文。指定 ICMP 报文类型时，可以用数字（0-255），也可以用助记符。助记符如下：

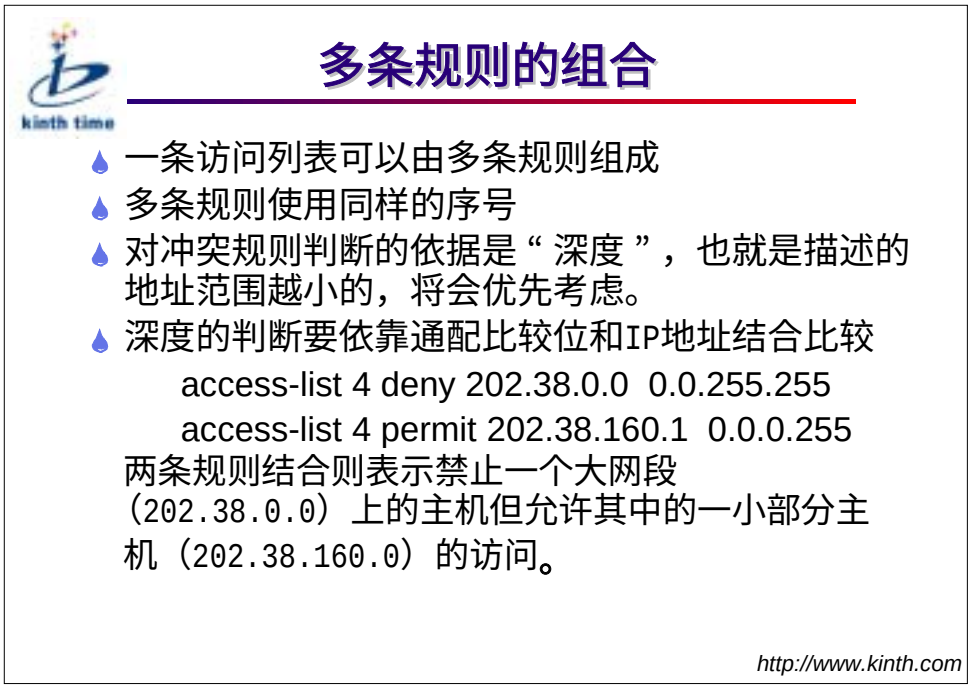
助记符	意义
echo	Type=8, Code=0
echo-reply	Type=0, Code=0
fragmentneed-DFset	Type=3, Code=4

host-redirect	Type=5, Code=1
host-tos-redirect	Type=5, Code=3
host-unreachable	Type=3, Code=1
information-reply	Type=16,Code=0
information-request	Type=15,Code=0
net-redirect	Type=5, Code=0
net-tos-redirect	Type=5, Code=2
net-unreachable	Type=3, Code=0
parameter-problem	Type=12,Code=0
port-unreachable	Type=3, Code=3
protocol-unreachable	Type=3, Code=2
reassembly-timeout	Type=11,Code=1
source-quench	Type=4, Code=0
source-route-failed	Type=3, Code=5
timestamp-reply	Type=14,Code=0
timestamp-request	Type=13,Code=0
ttl-exceeded	Type=11,Code=0

.4.3 扩展访问控制列表的举例



.5 多条规则的组合



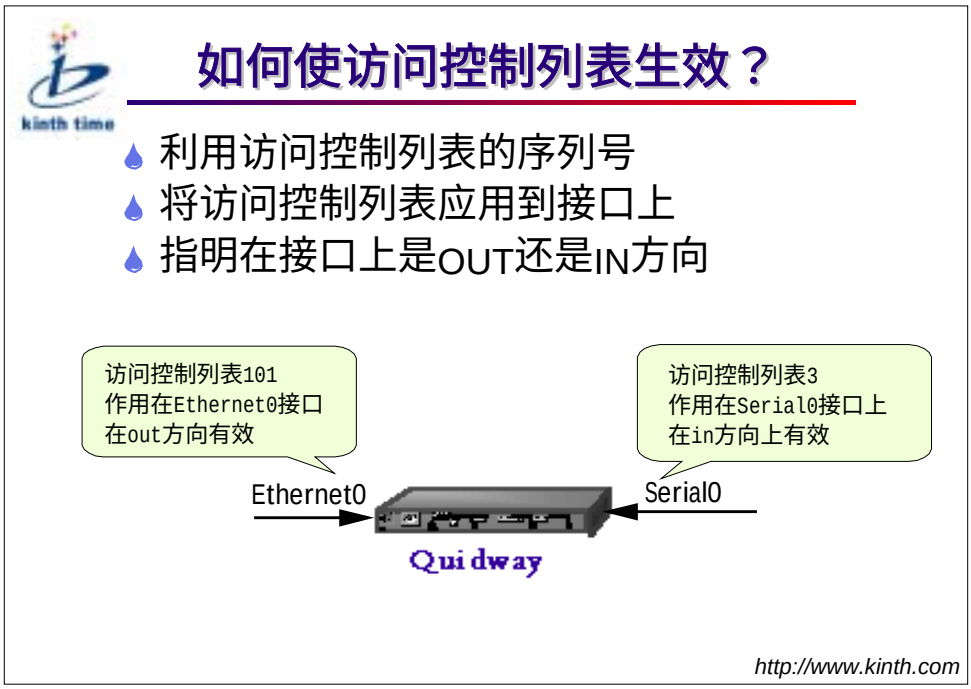
可以使用相同的序号，建立多条规则，构成一个访问控制列表。
对于两条有冲突的规则或是有地址重叠的情况，判断的依据是“深度”，也就是描述的地址范围越小的，将会优先考虑。例如：

access-list 1 permit 202.38.160.0 0.0.255.255
access-list 1 deny 202.38.160.0 0.0.0.255

对于 202.38.160.23 这样的地址，访问列表是认为是拒绝的。因为第二条指定的地址范围小。

.6 访问列表的生效

.6.1 访问列表的生效



为了使访问控制列表生效，将访问控制列表定义在接口上。
具体命令配置如下页所示。

.6.2 访问列表在接口生效的命令配置

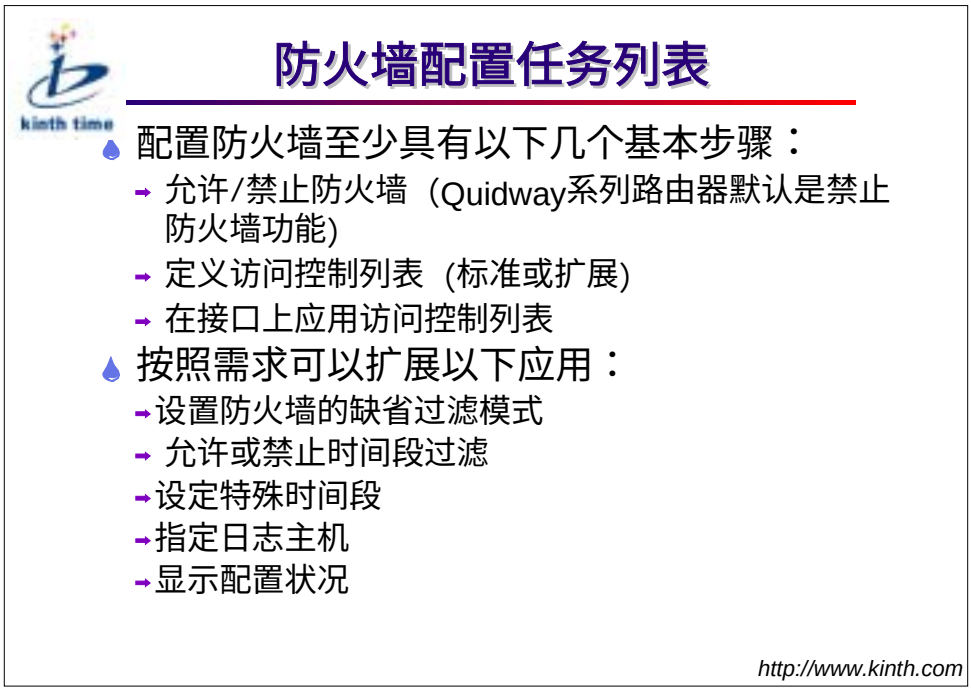
访问列表在接口生效命令配置

- 基于接口配置访问列表，使访问列表生效
  [no] ip access-group命令
  - ip access-group *listnumber* { in|out }
  - no ip access-group *listnumber* { in|out }
- 实例
  - 在Serial0口配置模式下执行
  - ip access-group 1 in
    将在Serial0口上，对进入的数据包，使用访问控制列表1进行过滤。

http://www.kinth.com

.7 防火墙基本配置任务列表

.7.1 防火墙基本配置任务



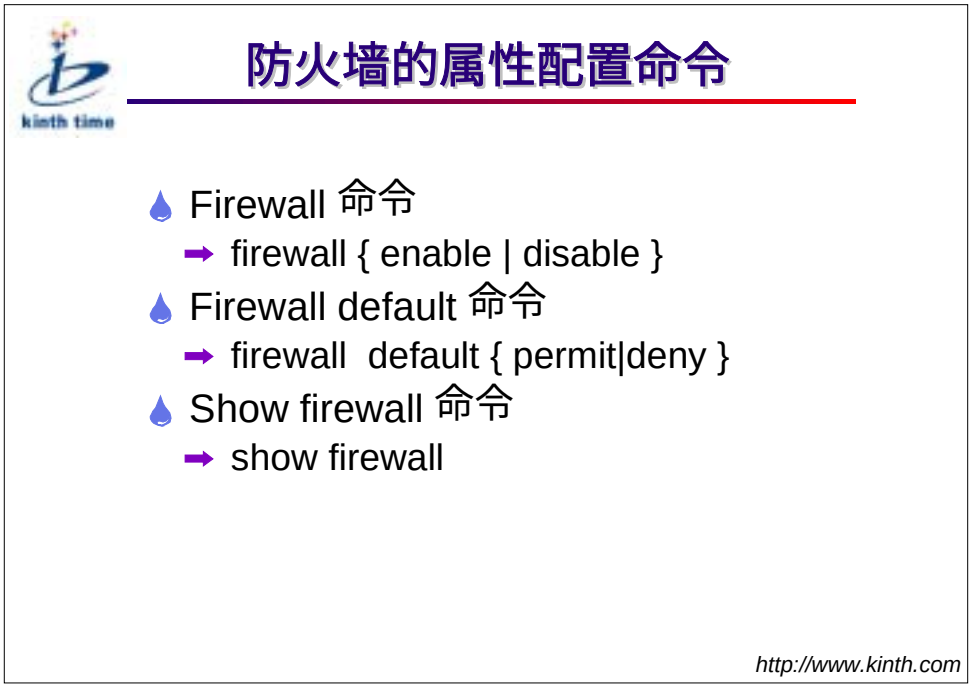
前面我们零星的介绍了 Quidway 系列路由器配置防火墙的相关内容，本页所示为完成防火墙配置的步骤。

在实际的使用中，还可能用到以下的扩展应用：

1. 设置防火墙的缺省过滤模式；
2. 允许或禁止时间段；
3. 设定时间段；
4. 允许日志主机；
5. 指定日志主机；
6. 显示配置状况。

其中，2 和 4 均在配置访问列表中设置，1、3、5 和 6 由专门的命令完成。

.7.2 防火墙的属性配置命令



属性命令中，首先是打开防火墙的操作：

firewall {enable | disable} 允许/ 禁止防火墙过滤；

其次，是设置防火墙的缺省过滤模式的操作：

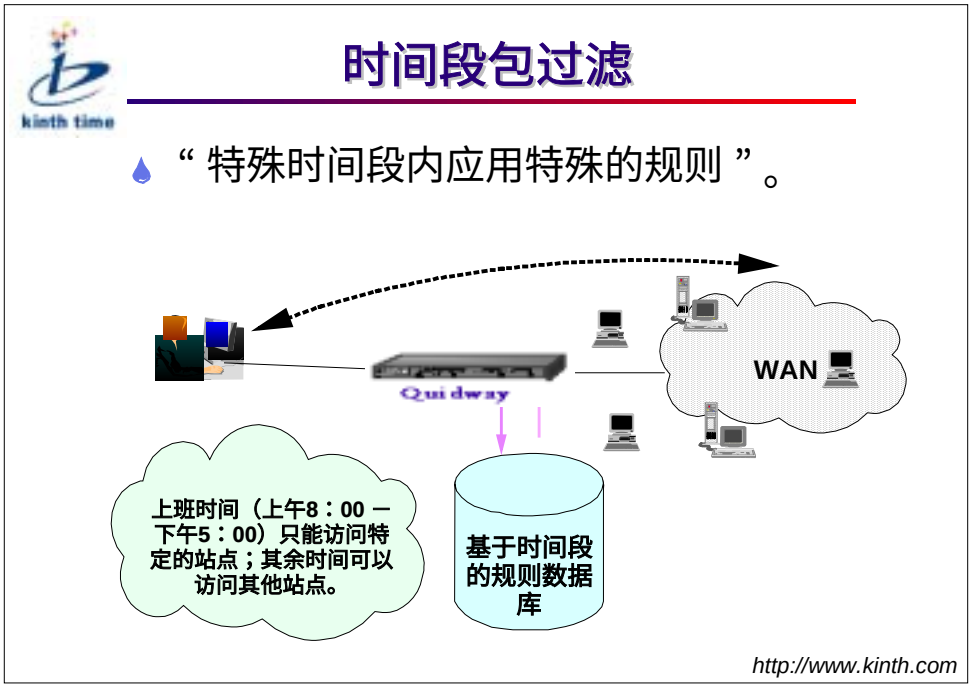
firewall default {permit | disable } 缺省方式是禁止还是允许；

缺省过滤模式用以定义对访问列表控制以外的 IP 或者 TCP 等数据包的处理，

Quidway 系列路由器防火墙的默认过滤模式是允许。

用 show firewall 命令可以 显示防火墙状态信息。

.7.3 时间段包过滤



基于时间段，用户可以指定一天 24 小时中的任意时间段为特殊时间段（可以是多个），不在任何特殊时间段的其他时间称为普通时间段。用户在定义访问列表时，可以指定该规则是在特殊时间段还是在普通时间段生效。

时间段包过滤（续）

timerange { enable|disable } 允许 | 禁止时间段

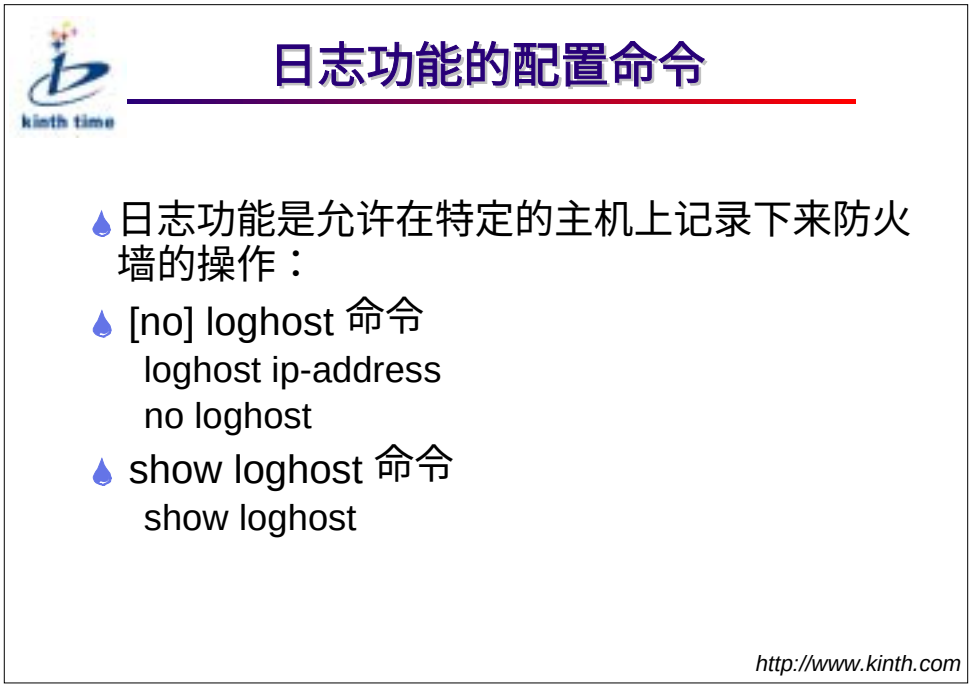
Quidway 防火墙默认为禁止时间段。

settr begin-time end-time [begin-time end-time .....] 设置特殊时间段

show isintr 显示当前时间是否在特殊时间段内

show timerange 显示配置的时间段

.7.4 日志功能



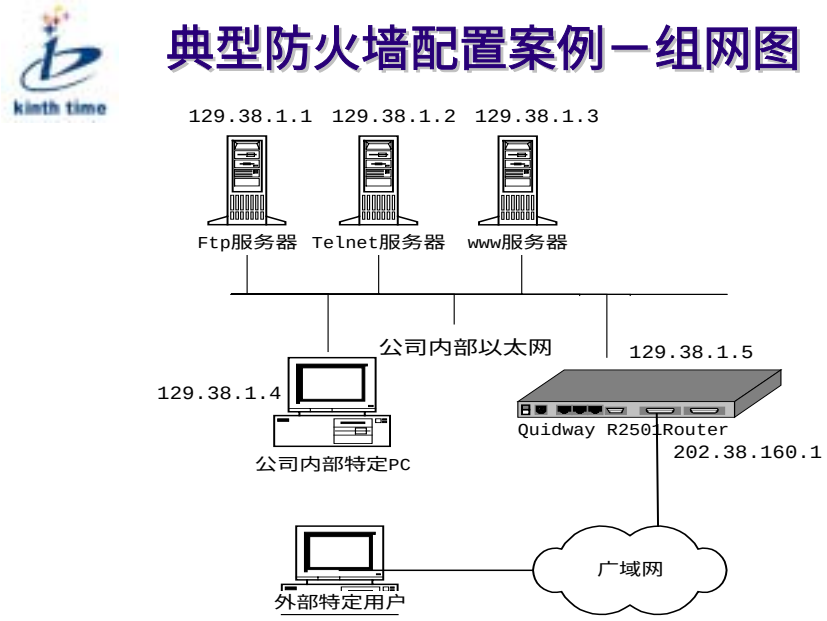
日志功能用以记录下所有来犯防火墙的操作信息，在访问列表允许日志功能后，需再配置如下一条命令，以指定日志主机的位置，日志主机可以是一台普通的网络工作站，也可以是专用的服务器，它们之上需运行标准的日志程序，以接收路由器发回的日志记录。

loghost ip-address 指定日志主机的 IP 地址。

用 show loghost 命令可以显示当前日志主机状况。

.8 防火墙配置举例

.8.1 组网图



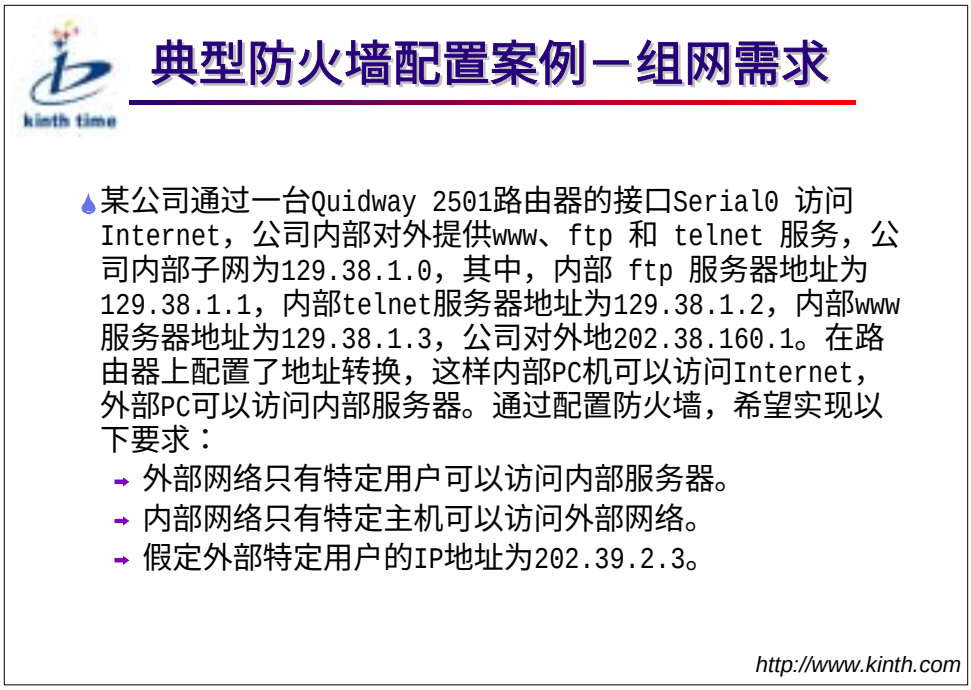
某公司通过一台 Quidway 2501 路由器的接口 Serial0 访问 Internet ，公司内部对外提供 www、ftp 和 telnet 服务，公司内部子网为 129.38.1.0，其中，内部 ftp 服务器地址为 129.38.1.1，内部 telnet 服务器地址为 129.38.1.2，内部 www 服务器地址为 129.38.1.3，公司对外地 202.38.160.1。在路由器上配置了地址转换，这样内部特定 PC 机（129.38.1.4）可以访问 Internet ，外部 PC 可以访问内部服务器。通过配置防火墙，希望实现以下要求：

外部网络只有特定用户可以访问内部服务器。

内部网络只有特定主机可以访问外部网络。

假定外部特定用户的 IP 地址为 202.39.2.3 。

.8.2 组网需求与配置



参考配置如下：

允许防火墙：

Quidway(config)# firewall enable

设置防火墙缺省过滤方式为允许包通过：

Quidway(config)# firewall default permit

配置访问规则禁止所有包通过：

Quidway(config)# access-list 100 deny ip any any

配置规则允许特定主机（129.38.1.4）访问外部网，允许内部服务器访问外部网：

Quidway(config)# access-list 101 permit ip 129.38.1.4 0 any

Quidway(config)# access-list 101 permit ip 129.38.1.1 0 any

Quidway(config)# access-list 101 permit ip 129.38.1.2 0 any

Quidway(config)# access-list 101 permit ip 129.38.1.3 0 any

配置规则允许特定用户从外部网访问内部服务器：

Quidway(config)# access-list 102 permit tcp 202.39.2.3 0 202.38.160.1 0

配置规则允许特定用户从外部网取得数据（只允许端口号大于 1024 的包）：

Quidway(config) # access-list 102 permit tcp any 202.38.160.1 0 gt 1024

Quidway(config) # access-list normal 102 deny ip any any

将规则 100 作用于从接口 Ethernet0 进入的包：

Quidway(config)# interface ethernet 0

Quidway(config-if-Ethernet0)# ip access-group 100 in

将规则 101 作用于从接口 Ethernet0 进入的包：

Quidway(config-if-Ethernet0)#ip access-group 101 in

将规则 102 作用于从接口 Serial0 进入的包：

Quidway(config-if-Serial0)# ip access-group 102 in

在接口 Serial0 上作地址转换：

Quidway(config-if-Serial0)# nat enable

在全局模式下配置 Nat server ：

natserver ftphost 129.38.1.1

natserver telnethost 129.38.1.2

natserver wwwhost 129.38.1.3

其他内容如各端口 IP 地址，封装协议等这里不再赘述。

.9 本章重点

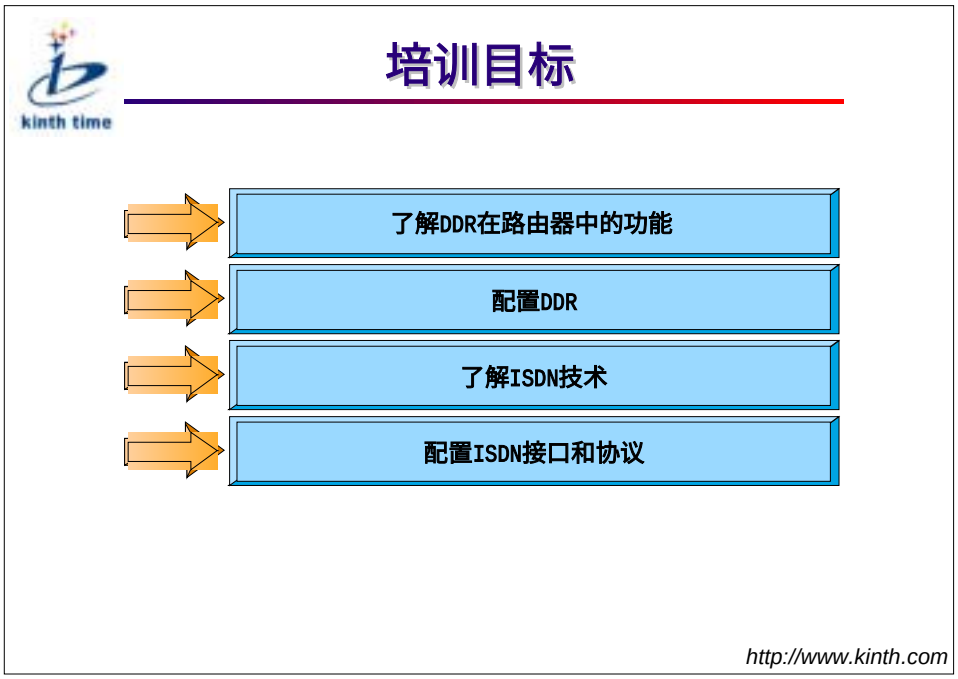
本章重点

- 包过滤原理；
- 标准访问列表的配置原则；
- 扩展访问列表的配置原则；
- 在端口上引用访问控制列表实现防火墙功能

http://www.kinth.com

第十一章　DDR、ISDN 配置

.1　培训目标



本章讨论 Quidway 路由器 DDR 和 ISDN 的配置方法，包括基本概念、配置方法以及配置实例等。

.2 DDR 简介

DDR 是英文 Dial-On-Demand Routing 的缩写，意思是按需拨号路由。指路由器之间通过公用交换网进行互连时，所采用的路由技术。当前主要有两种公用交换网，即 PSTN 和 ISDN 网。它们在使用前都需要首先拨号。

路由器之间以异步串口通过 PSTN 互连，或以 ISDN 口（BRI 或 PRI）通过 ISDN 网互连时，采用 DDR。在通常情况下，路由器之间是不建立连接的，只有当它们之间有包需要传送时，启动 DDR，拨号建立连接，传送数据包。当链路空闲时，DDR 会自动断开连接。

在两点之间信息量较少，且多为突发传送时，DDR 是非常经济的。

DDR 不是协议，没有国际标准。是各路由器厂商根据需要自己实现的。

.3　DDR 的基本配置

DDR 的配置过程可以分为下列几个步骤：

☞ 根据具体的组网方式决定要配置的端口是要向单点还是多点发出呼叫、是要接收单点还是多点的呼叫或者既要接收呼叫又要发出呼叫。

☞ 配置 DDR 的目的是为了实现按需拨号，即只在有数据要发送的时候才开始拨号建立连接，所以要配置一个开始拨号的触发条件：Dialer-list。

☞ DDR 还有一个特点就是在已经建立了连接以后，如果过了一段时间没有数据传送，DDR 就会自动断开连接。这段时间到底是多少呢？当然可以使用系统的默认值，但是你也可以根据实际情况自己配置。类似这些参数都是 DDR 的相关参数。

☞ Dialer 口是一个逻辑拨号口，一个 Dialer 口可以包含多个物理口，它们继承了 Dialer 口的特性。运用 Dialer 口可以简化 DDR 的配置。

.3.1　对单点的呼叫

当通过异步串口进行呼叫时，需要使用 dialer in-band 命令；对于 ISDN 接口，系统会自动加载，不需用此命令配置。
只有当通过该接口只呼叫一个目的地址时，才可使用 dialer string 命令。

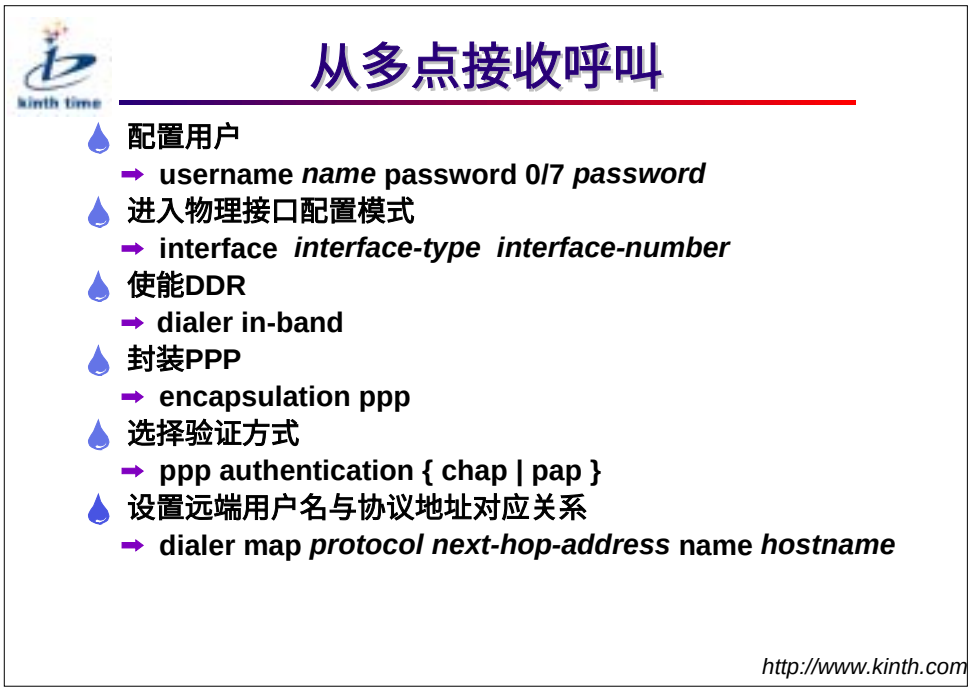
.3.2　对多点的呼叫

因为是对多点的呼叫，所以不能使用 Dialer string 命令，而要使用 Dialer map 命令，以建立不同目的 IP 地址和拨号号码的关系。

.3.3 从一个单点接收呼叫

配置一个端口从一个单点接收呼叫，只需使能 DDR 即可。 对于 ISDN 接口不需执行此命令。

.3.4　从多点接收呼叫

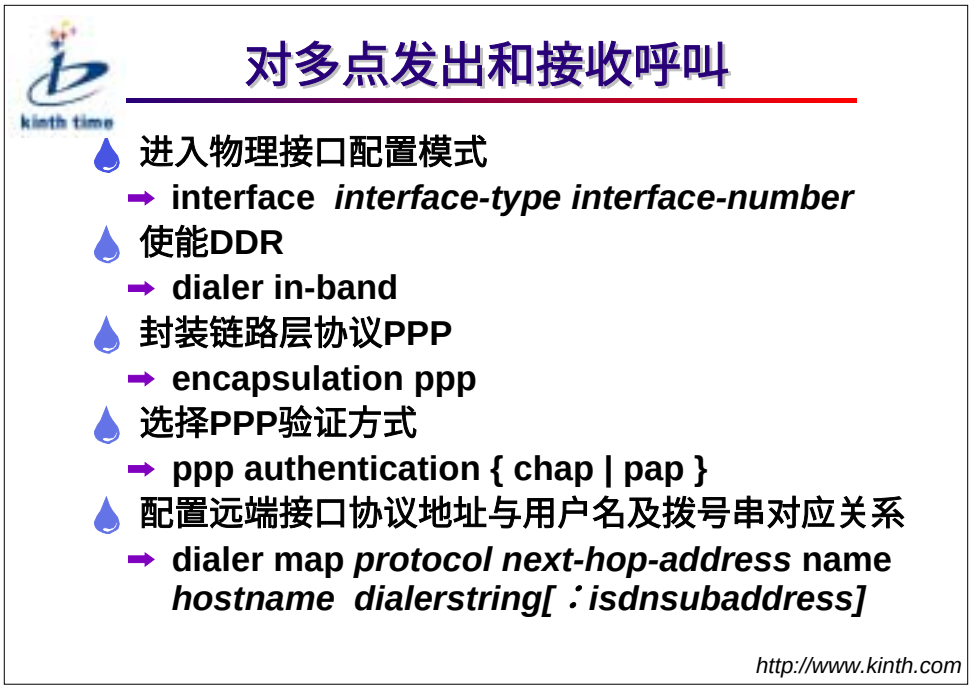


由于需要从多点接收呼叫，所以需要使用 CHAP 或 PAP 验证，否则无法区分各点。一般推荐使用 CHAP，因为它在传送用户名和随机报文时，做了加密；而 PAP 是明文传送用户名和口令。当然如果不需要区分对端路由器也可以不配置 PAP 或 CHAP 验证。

.3.5　对一个点发出和接收呼叫

对一个点发出和接收呼叫，只需进行如上配置，封装 PPP ，可以不选择验证方法。

.3.6　对多点发出和接收呼叫



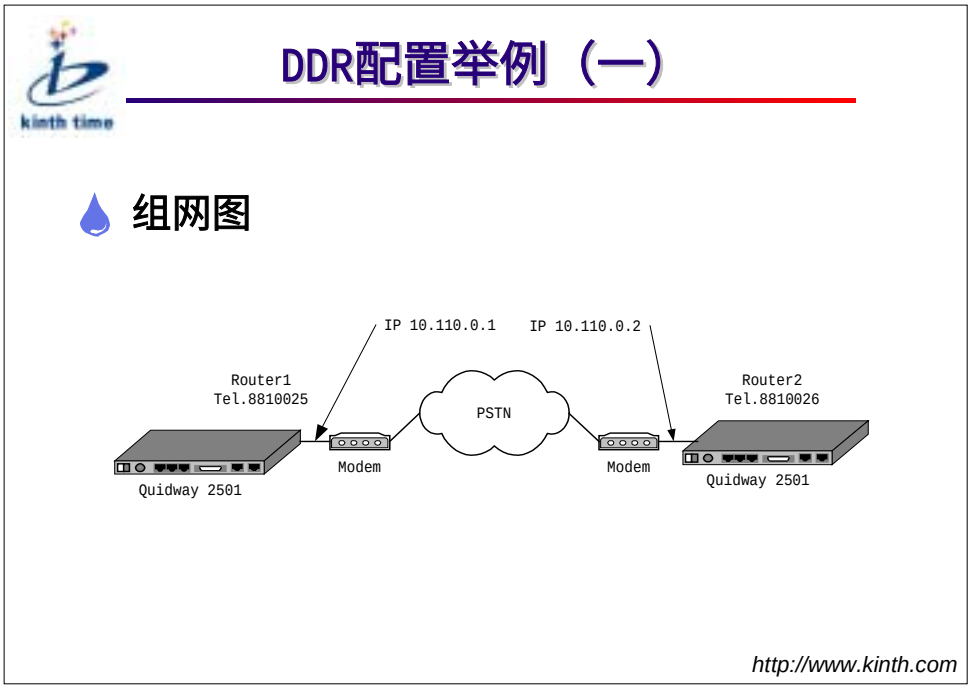
与前面所提到的“从多点接收呼叫”类似，由于“对多点发出和接收呼叫”也需要从多点接收呼叫，所以需要使用 CHAP 或 PAP 验证。否则无法区分各点。一般推荐使用 CHAP，因为它在传送因为它在传送用户名和随机报文时，做了加密；而 PAP 是明文传送用户名和口令。当然如果不需要区分对端路由器也可以不配置 PAP 或 CHAP 验证。

.4　配置 Dialer-list

Dialer-list 的作用是区分数据包是否是需要通过 DDR 传送的包，只有经过 Dialer-list 确认后的包才能触发 DDR 开始拨号建立连接。配置 Dialer-list 要求在全局配置模式下进行，一个配置好的 Dialer-list 中可以加入多个拨号端口。

.5　DDR 配置举例（一）

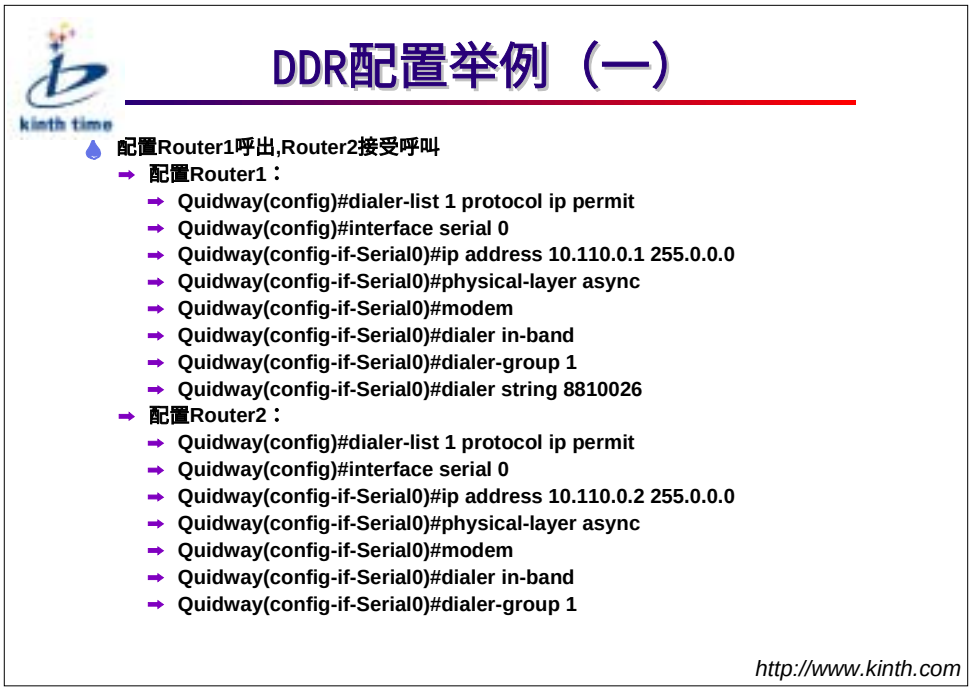
.5.1　组网图



这是一个通过 DDR 拨号连接两台 Quidway2501 路由器的例子。从图中可以看出，Router1 的同/异步口 Serial0 通过 Modem 接入电话网，Serial0 的 IP 地址是 10.110.0.1，电话号码是 8810025。 Router2 的同/异步口 Serial0 通过 Modem 接入电话网，Serial0 的 IP 地址是 10.110.0.2，电话号码是 8810026。

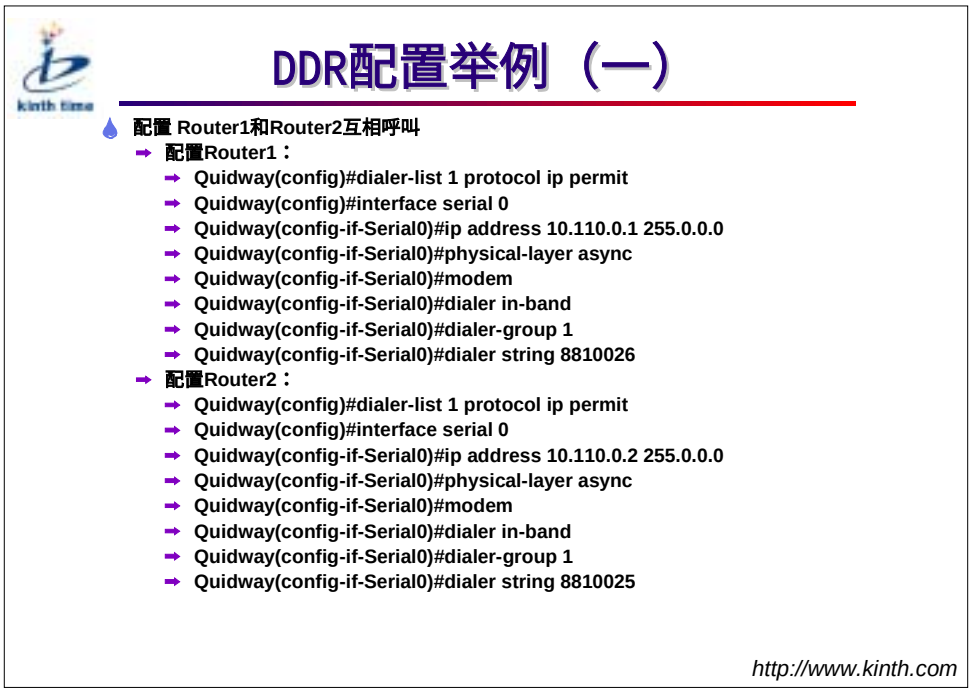
.5.2　配置

1、配置 Router1 呼叫 Router2



在这个配置实例中 Router1 作为主叫方向 Router2 发起呼叫建立连接，所以 Router1 应该配置为“对一个单点的呼叫”；Router2 应该配置为“从一个单点接收呼叫”。以上配置完成后，从 Router1 上 ping 10.110.0.2 以产生触发拨号的数据包开始拨号。

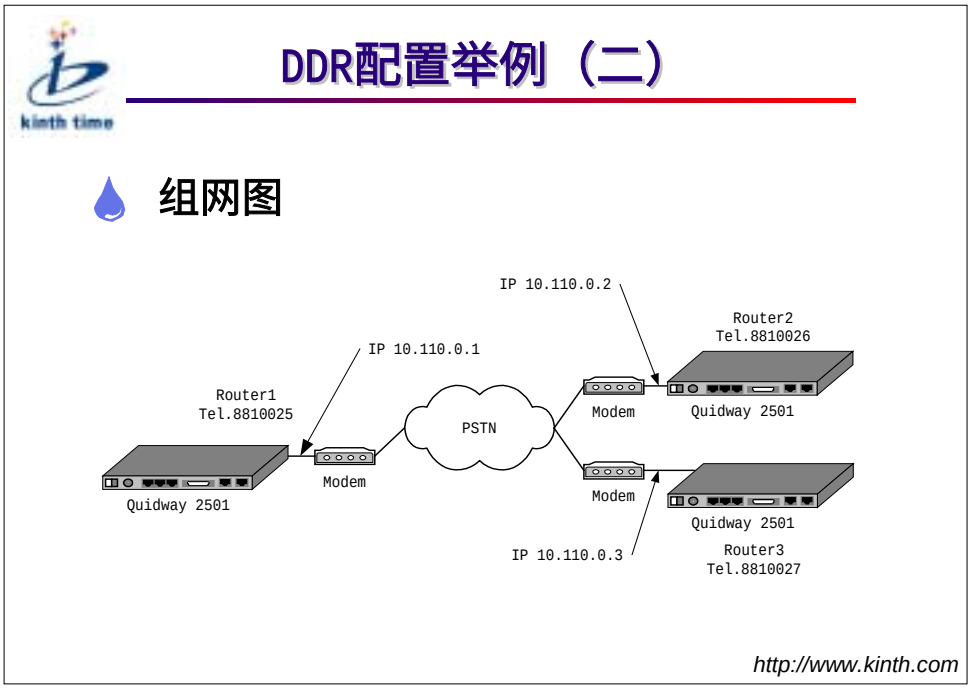
2、配置 Router1 和 Router2 互相呼叫



在这个配置实例中 Router1 和 Router2 都可以作为主叫方发起呼叫建立连接，所以 Router1 应该配置为“对一个点发出和接收呼叫”；Router2 也应该配置为“对一个点发出和接收呼叫”。以上配置完成后，从 Router1 或 Router2 上 ping 对端都可以产生触发拨号的数据包开始拨号。

.6　DDR 配置举例（二）

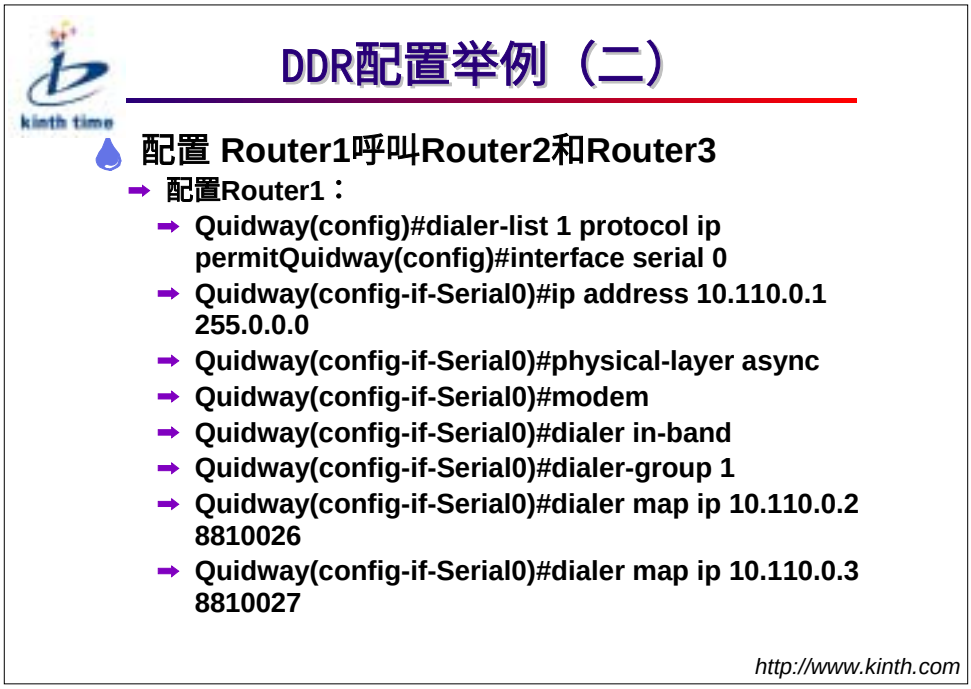
.6.1　组网图



这是一个通过 DDR 拨号一台 Quidway2501 路由器连接两台 Quidway2501 路由器的例子，从图中可以看出，Router1 的同/异步口 Serial0 通过 Modem 接入电话网，Serial0 的 IP 地址是 10.110.0.1，电话号码是 8810025。Router2 的同/异步口 Serial0 通过 Modem 接入电话网，Serial0 的 IP 地址是 10.110.0.2，电话号码是 8810026。Router3 的同/异步口 Serial0 通过 Modem 接入电话网，Serial0 的 IP 地址是 10.110.0.3，电话号码是 8810027。

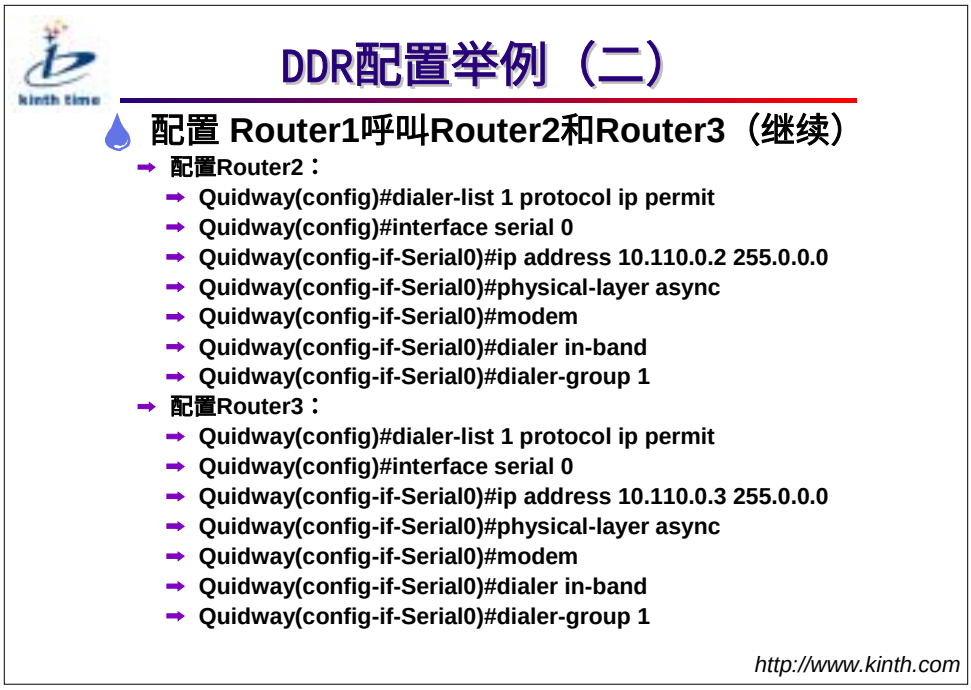
.6.2　配置

1、配置 Router1 接收 Router2 和 Router3 的呼叫



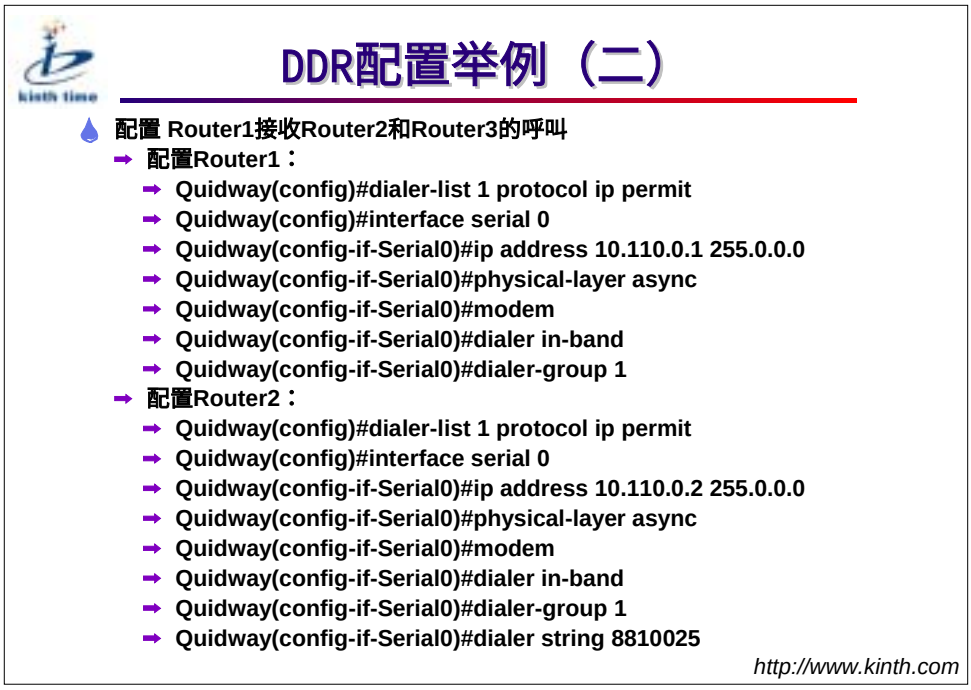
在这个配置实例中 Router1 作为主叫方向 Router2 和 Router3 发起呼叫建立连接，所以 Router1 应该配置为“对一个多点的呼叫”；Router2 和 Router3 应该配置为“从一个单点接收呼叫”。以上配置完成后，从 Router1 上 ping Router2 或 Router3 路由器的 IP 地址，路由器根据 Dialer map 确定呼叫号码开始拨号。

配置 Router1 接收 Router2 和 Router3 的呼叫（续）



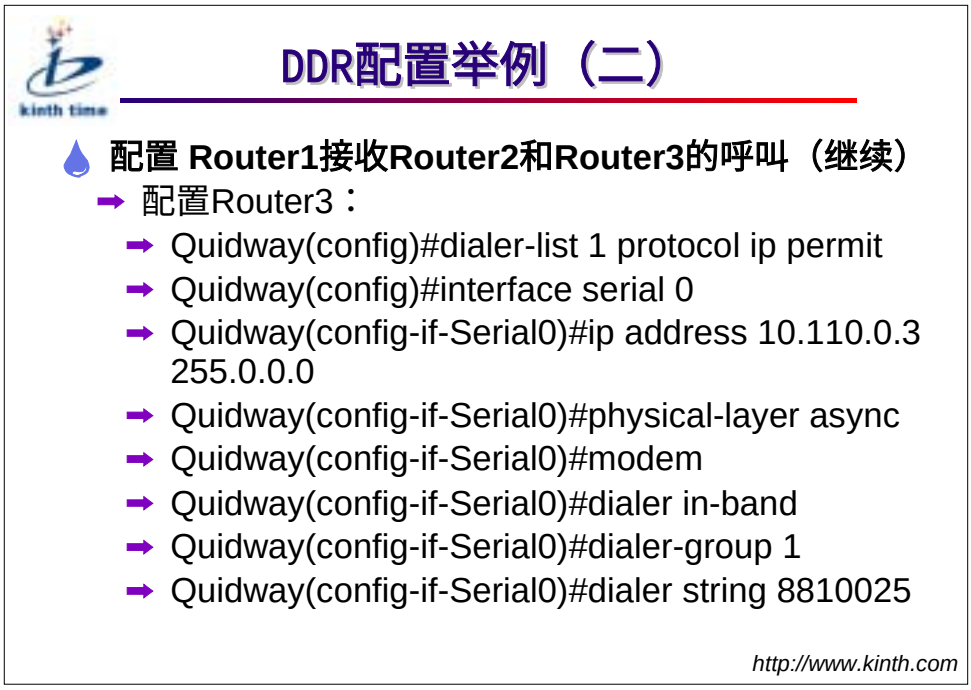
这是上一页的继续，是关于 Router3 的配置，Router3 被配置为“从一个单点接收呼叫”。

2、配置 Router1 接收 Router2 和 Router3 的呼叫



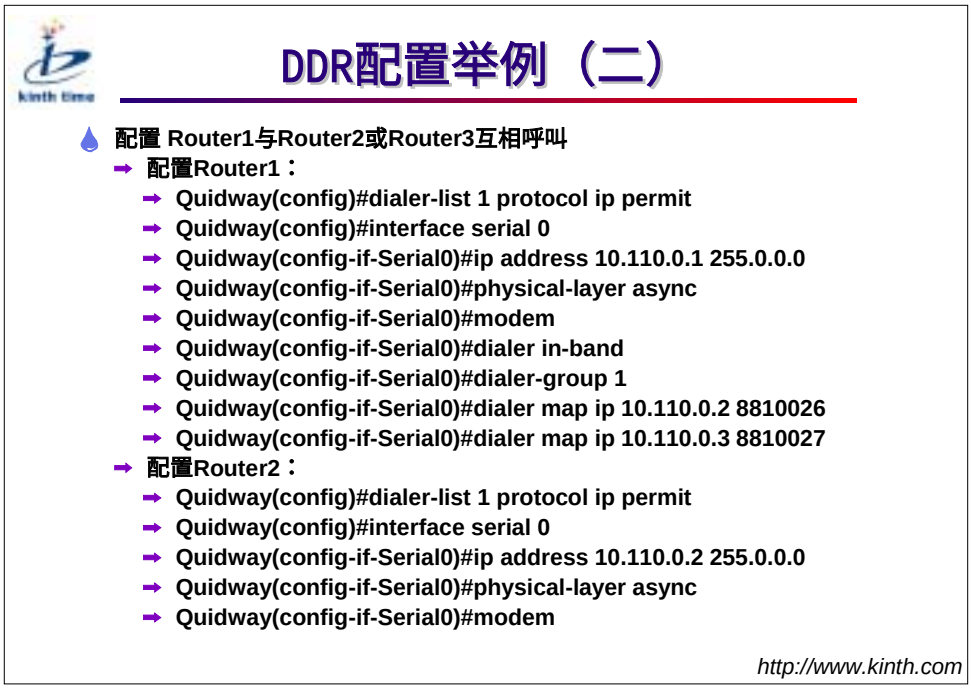
在这个配置实例中 Router1 接收 Router2 和 Router3 发起的呼叫建立连接，所以 Router1 应该配置为“从多点接收呼叫”；Router2 和 Router3 应该配置为“对单点的呼叫”。以上配置完成后，从 Router2 或 Router3 上 ping Router1 路由器的 IP 地址开始拨号。

配置 Router1 接收 Router2 和 Router3 的呼叫（续）



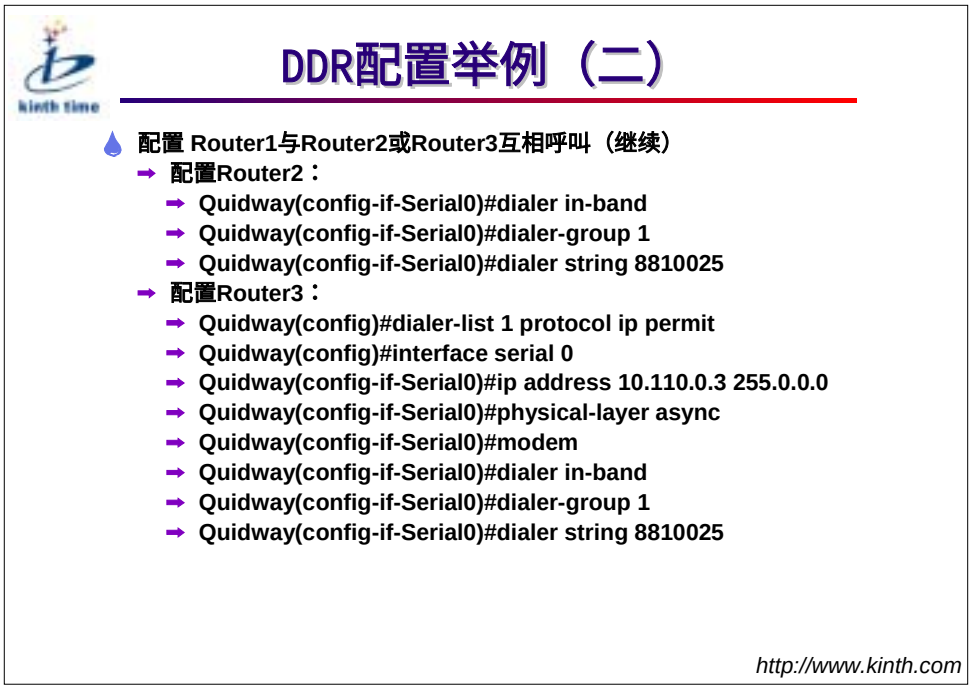
这是上一页的继续，是关于 Router3 的配置，Router3 被配置为“对单点的呼叫”。

3、配置 Router1 与 Router2 或 Router3 互相呼叫



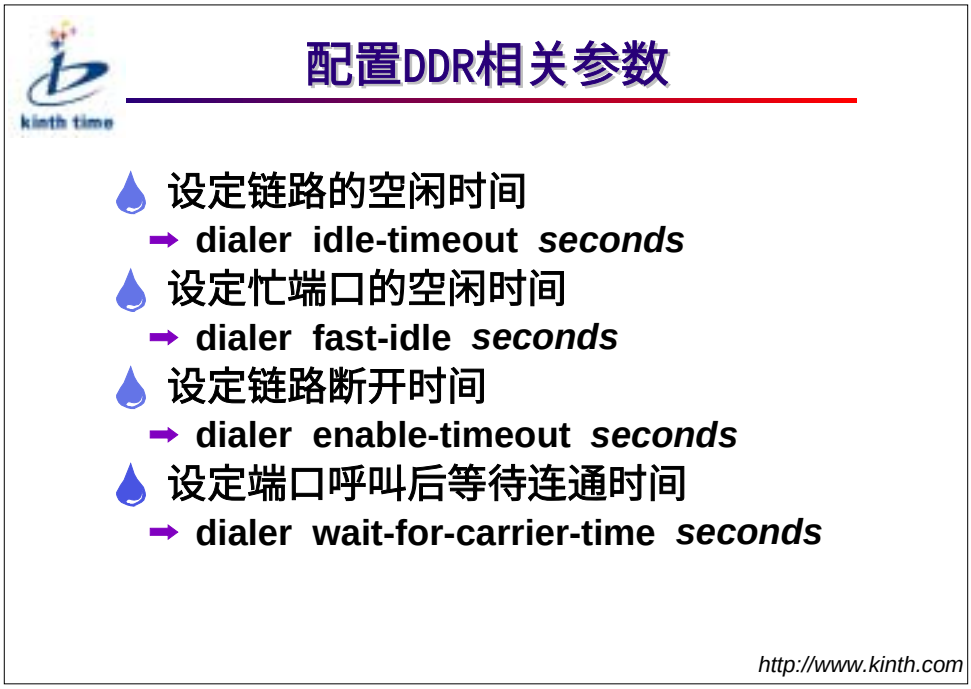
在这个配置实例中 Router1 与 Router2、Router1 与 Router3 可以互相呼叫建立连接；Router2 与 Router3 之间不可以互相呼叫建立连接。所以 Router1 应该配置为“对多点发出和接收呼叫”；Router2 和 Router3 应该配置为“对一个点发出和接收呼叫”。以上配置完成后，从 Router2 或 Router3 上 ping Router1 路由器的 IP 地址可以开始拨号；从 Router1 上 Ping Router2 或 Router3 路由器的 IP 地址也可以开始拨号。

配置 Router1 与 Router2 或 Router3 互相呼叫（续）



这是上一页的继续，是关于 Router3 的配置，Router3 被配置为“对一个点发出和接收呼叫”。

.7　配置 DDR 相关参数



DDR 最大的特点是平时不建立连接，只有当它们之间有数据需要传输时才建立连接，数据传输完毕后，自动断开连接。可是怎样来判断数据传输完成呢？这就是由 DDR 的相关参数决定的。

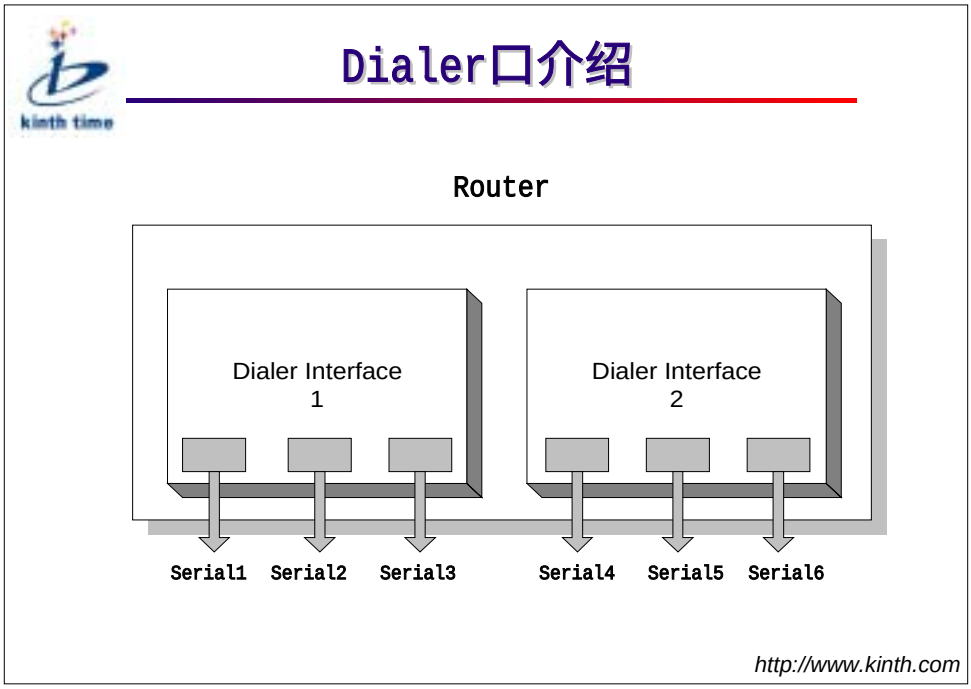
链路空闲时间就是当链路空闲超过了设定的链路空闲时间后，DDR 将断开链路。

忙端口的空闲时间是指当端口已经建立了一条链路时，这时另一端口需要与它建立新链路，称为竞争。如果第一条链路空闲超过了设定的忙端口的空闲时间后，DDR 将断开链路。

链路断开时间是指当链路因失败或挂断而处于断开状态后，经过设定的链路断开时间才能建立新的连接。

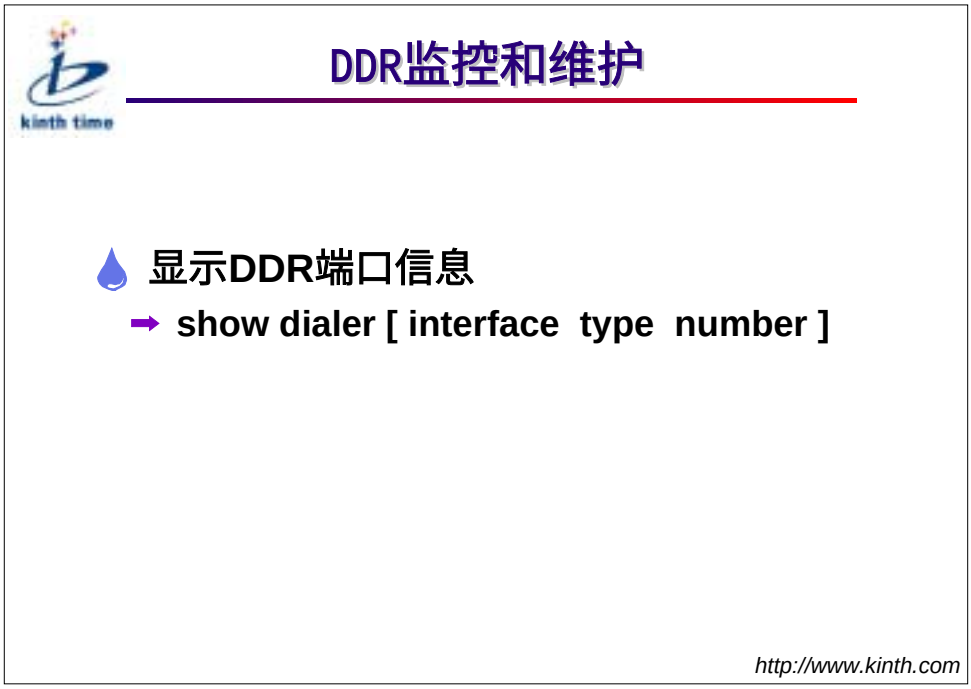
端口数据可以发送等待时间是指发送数据前等待链路建立的时间必须小于设定的端口数据可以发送等待时间。

.8　Dialer 口介绍 *



Dialer 口是一个逻辑接口，其中包含一组物理接口。对一个 Dialer interface 的配置将会继承给这个接口中的所有物理接口。在完成了 Dialer interface 的配置后，将某个物理接口置入其中，这个物理接口将会继承对 dialer interface 的所有配置。如上图所示，Dialer Interface 1 包含三个物理接口 Serial1、Serial 2 和 Serial3；Dialer Interface 2 同样包含三个物理接口 Serial4、Serial5 和 Serial6。对 Dialer Interface 1 的配置将会继承给 Serial1、Serial2 和 Serial3； 对 Dialer Interface 2 的配置将会继承给 Serial4、Serial5 和 Serial6。

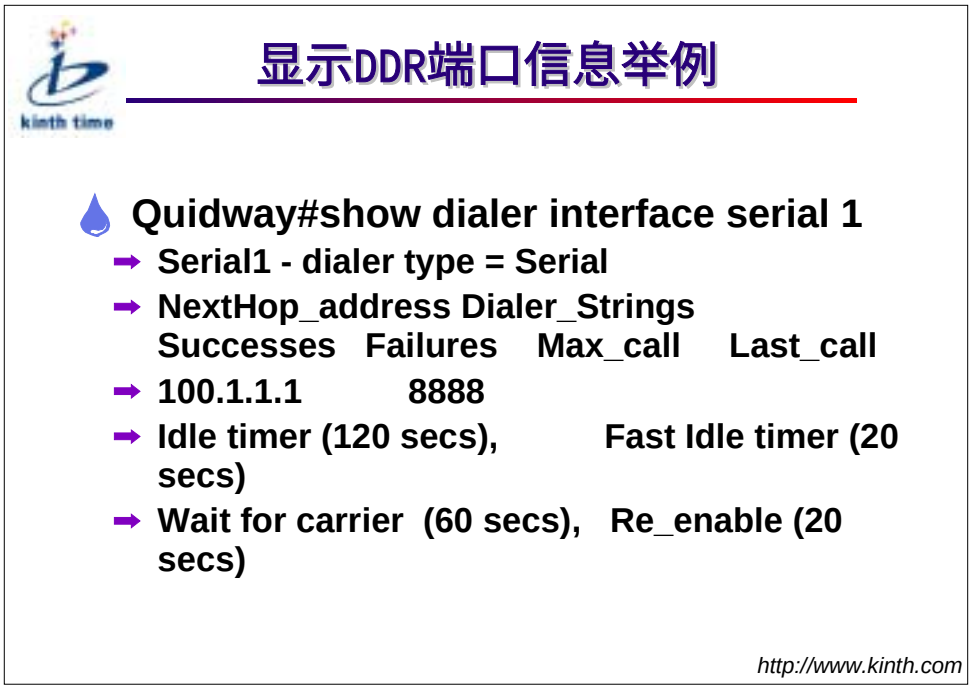
.9　DDR 监控和维护



显示的端口信息所代表的意义见下表：

域名	意义
NextHop_address	端口上一条Dialer map对应的对端地址
Dialer_Strings	此Dialer map对应拨号串
Successes	此Dialer map呼叫成功次数
Failures	此Dialer map呼叫失败次数
Max_call	此Dialer map最长使用时间
Last_call	此Dialer map上次呼叫使用时间
Idle timer	由Dialer idle-timeout命令设定的时间
Fast Idle timer	由Dialer fast-idle命令设定的时间
Wait for carrier	由Dialer wait-for-carrier命令设定的时间
Re_enable	由Dialer enable-timeout命令设定的时间

显示 DDR 端口信息举例



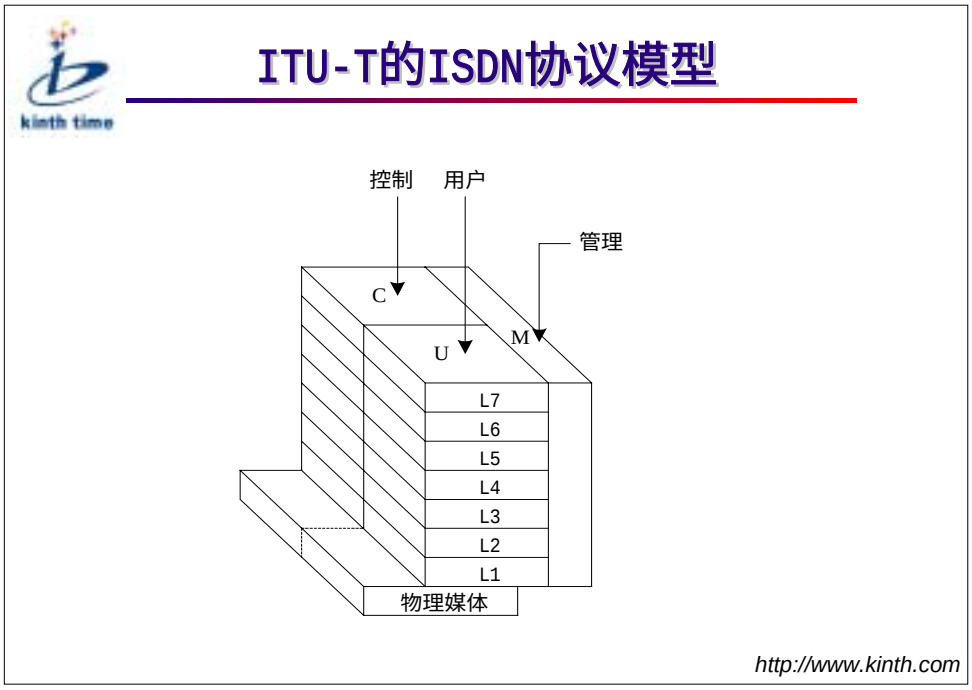
以上显示的信息代表的意义如下：
接口类型为异步串口；对端 IP 地址为 100.1.1.1；对端的号码为 8888；链路空闲时间为 120 秒；忙端口的空闲时间为 20 秒；数据可发送等待时间为 60 秒；链路断开时间为 20 秒。

.10　ISDN 技术概述

综合业务数字网（Integrated Services Digital Network，简称 ISDN）是自 70 年代发展起来的一种新兴技术。提供从终端用户到终端用户的全数字服务，实现了语音、数据、视频等综合信息的全数字化传递。

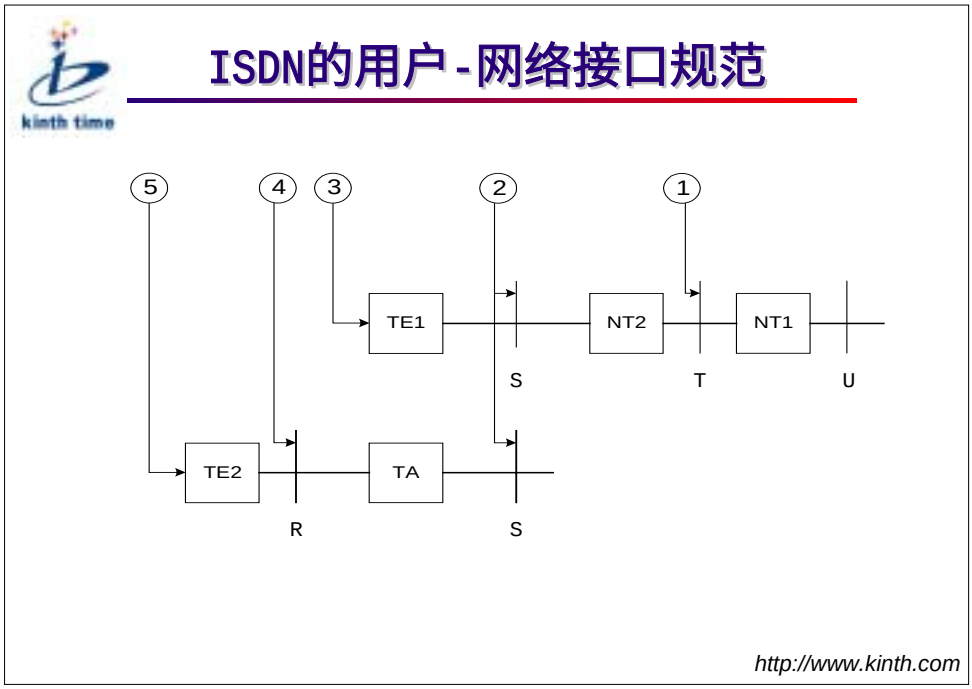
ISDN 不同于传统的 PSTN 网络，传统 PSTN 网络中用户的信息通过模拟的用户环路送至交换机后经 A/D 转换成为数字信号，经过数字交换和传输网络后，到达目的用户又将还原成模拟信号。ISDN 解决了用户环路的数字传输问题，实现了端到端的数字化，并通过这个标准化的数字接口，解决各种数字和模拟信息的传递。此外通过标准化工作，ITU-T 制定了 ISDN 业务规范，使综合业务成为可能，制定了 I.430、Q.921 和 Q.931 等协议，使所有符合 ITU-T 物理接口和软件协议的设备均可无障碍地进入 ISDN 网络。

.10.1　ITU-T 的 ISDN 协议模型



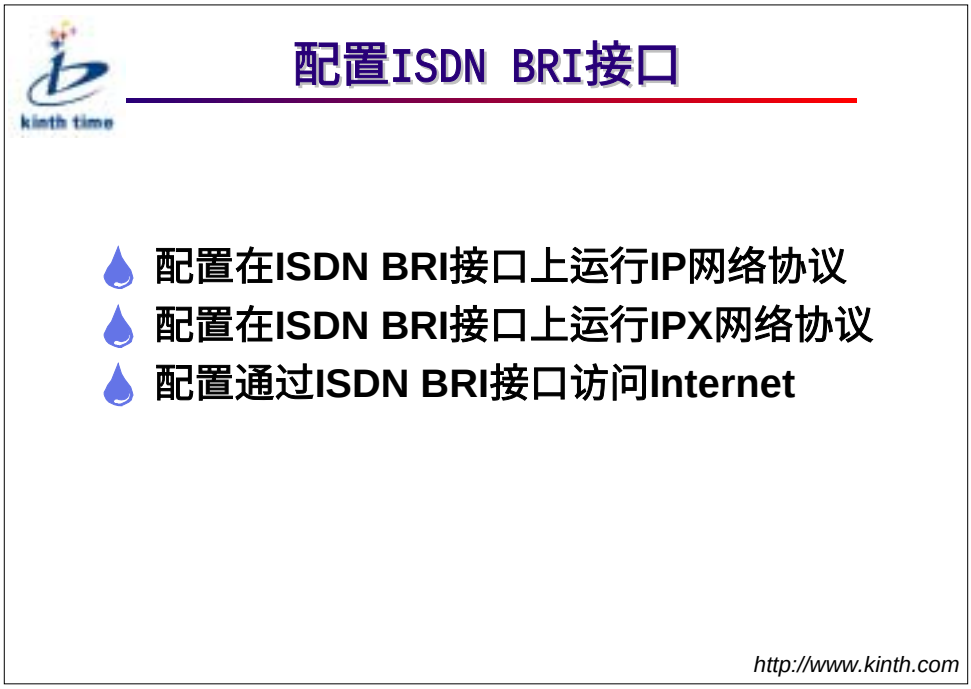
国际电信联盟电信标准化委员会（ITU-T）在 OSI 模型的基础上专门为 ISDN 协议设计了立体的结构模型：
模型由三个平面组成，分别对应着三种不同类型的信息：
☞ 控制平面 C：是关于控制信令的协议，共分七层，它覆盖了所有对呼叫和对网络性能的控制。
☞ 用户平面 U：是关于用户信息的协议，也分七层，它覆盖了在用户信息传送的信道上实行数据交换的全部规则。
☞ 管理平面 M：不分层，是关于终端或 ISDN 节点内部操作功能的规则。
一般说来，C 平面和 U 平面都可以通过原语和管理平面 M 进行通信，由 M 平面中的管理实体来协调 C 和 U 之间的动作。C 和 U 之间不直接通信。

.10.2　ISDN 的用户-网络接口规范



ISDN 的用户-网络接口规范：
在 ITU-T I.411 建议中，根据功能群（用户接入 ISDN 所需的一组功能）、参考点（用来分功能群的概念上的点）的概念，提出了 ISDN 用户-网络接口的参考配置。
功能群分为：
☞ 网络终端 1（NT1）：主要实现了 OSI 第一层的功能，包含用户线传输功能、环路测试和 D 信道竞争等。
☞ 网络终端 2（NT2）：又称为智能网络终端，包含了 OSI 的 1~3 层。
☞ 1 类终端设备（TE1）：又称为 ISDN 标准终端，是符合 ISDN 接口标准的用户设备（如数字话机等）。
☞ 2 类终端设备（TE2）：又称为非 ISDN 标准终端设备，是不符合 ISDN 接口标准的用户设备。
☞ 终端适配器（TA）：完成适配功能，使 TE2 接入 ISDN 标准接口。
参考点包括：
☞ R 参考点：位于非 ISDN 设备和 TA 之间。
☞ S 参考点：位于用户终端和 NT2 之间。
☞ T 参考点：位于 NT1 和 NT2 之间。
☞ U 参考点：位于 NT1 设备和线路终端设备之间。

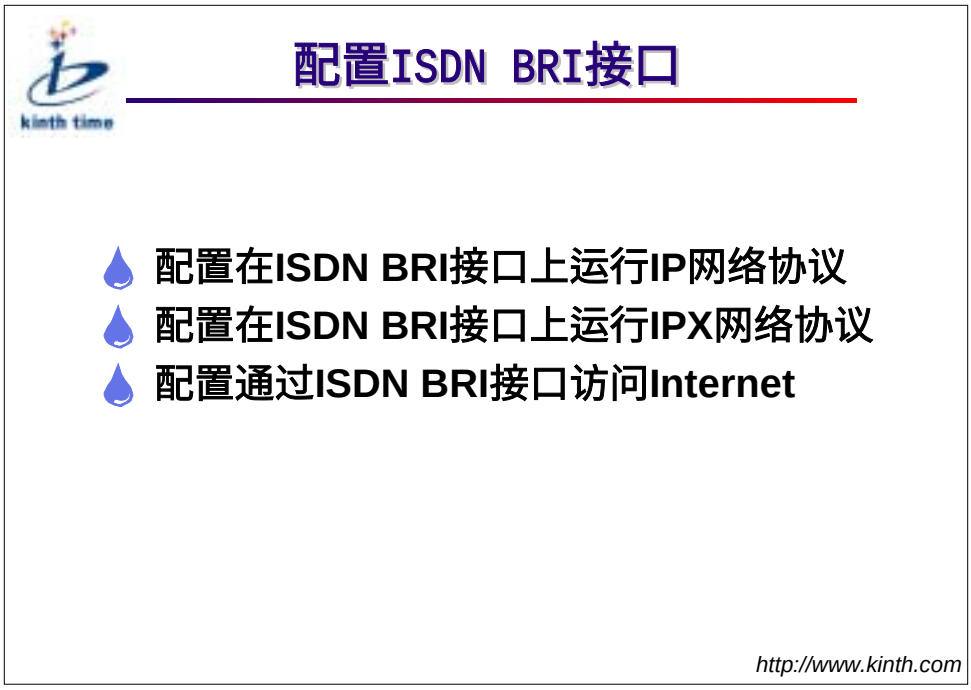
.11　配置 ISDN BRI 接口



ISDN BRI 接口包含 2B+D 三个通信信道。B 信道是用户信道，用来传送话音、数据等用户信息，传送数率是 64kbps；D 信道是控制信道，它传送公共信道信令，这些信令用来控制同一接口的 B 信道上的呼叫。D 信道的数率是 16kbps。

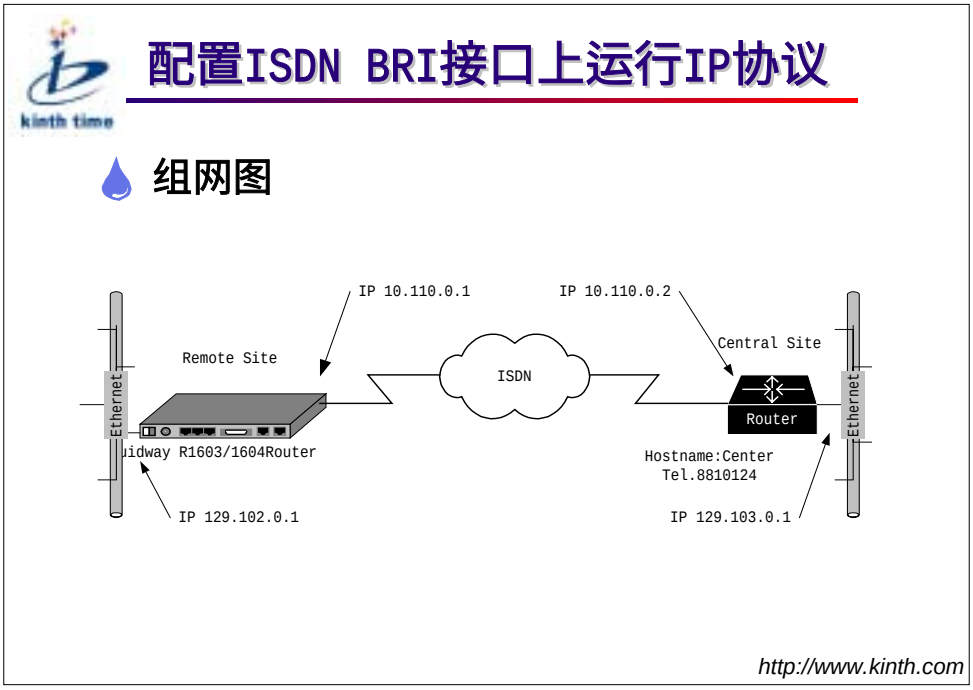
ISDN BRI 接口缺省封装链路层协议为 PPP，支持 IP 和 IPX 等网络层协议。

.11.1　配置在 ISDN BRI 接口上运行 IP 协议



配置 ISDN 协议工作参数主要是设置进行 Q.921 TEI 协商的时间、设置数字入呼叫时需要检查的被叫号码或子地址、设置模拟入呼叫时需要检查的被叫号码或子地址。
配置 Dialer Map 是为了设置对端 ISDN 的号码和 IP 地址的对应关系。
为了保证数据传输的安全性，需要配置 PAP 或 CHAP 验证。
由于 ISDN 也需要拨号呼叫建立连接，所以需要配置相关的 DDR 工作参数。具体方法请参见有关 DDR 的章节。

.11.2　配置在 ISDN BRI 接口上运行 IP 协议实例



这是一个通过 ISDN 一台 Quidway16 系列路由器连接中心路由器的例子，从图中可以
看出，Router1 的 BRI 口 Bri0 接入 ISDN 网，Bri0 的 IP 地址是 10.110.0.1。中心路由器的 BRI 口的 IP 地址是 10.110.0.2，号码是 8810124。

在 ISDN BRI 接口上运行 IP 协议举例 — 配置

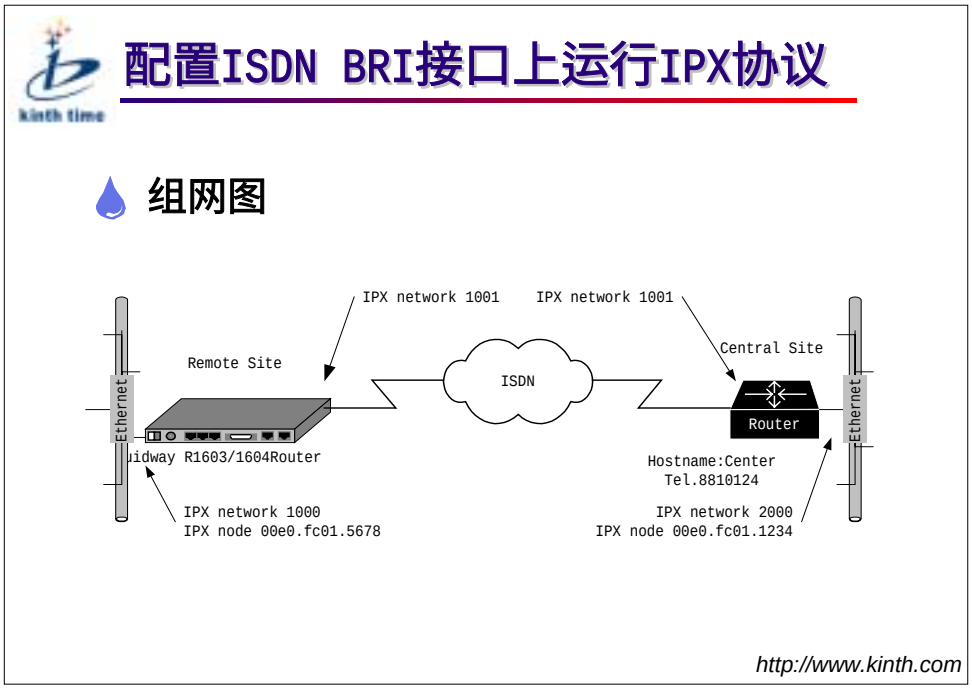
以上配置对应的说明如下：

- 配置 PPP 验证的用户名和口令
- 配置 ISDN BRI 接口 IP 地址
- 配置到中心路由器的呼出 Dialer Map
- 在 BRI 口上封装链路层协议 PPP
- 指定 Dialer Group
- 重新启动 ISDN BRI 接口，使上述配置生效
- 配置到中心路由器的静态路由
- 配置激活拨号的规则

.11.3　配置在 ISDN BRI 接口上运行 IPX 协议

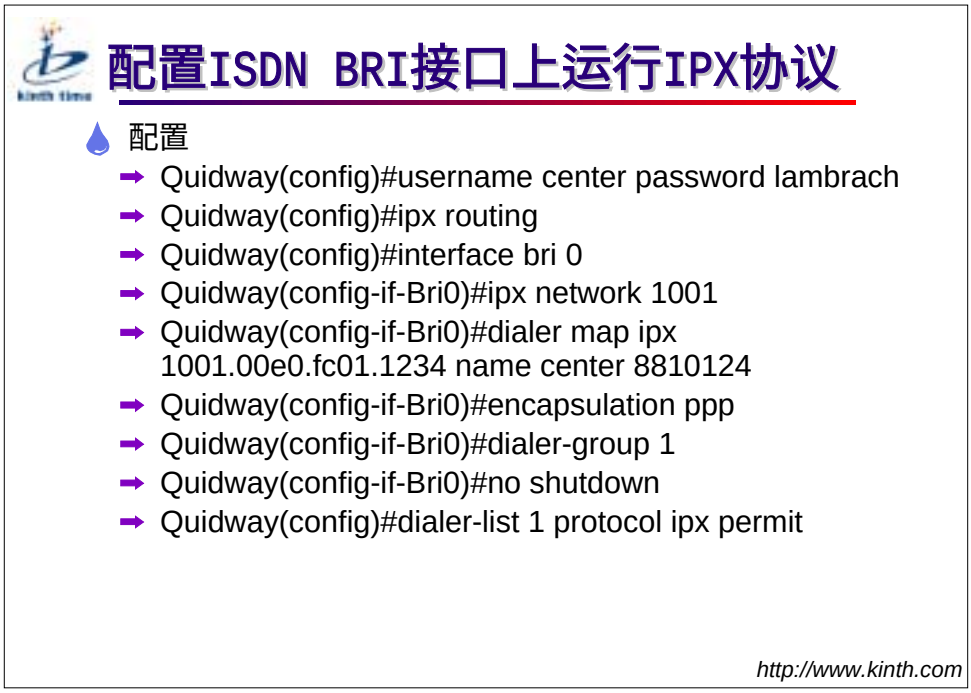
配置在 ISDN BRI 接口上运行 IPX 协议与配置在 ISDN BRI 接口上运行 IP 协议的过程基本相同，只是接口上封装的网络协议不同。

.11.4　配置在 ISDN BRI 接口上运行 IPX 协议实例



这是一个通过 ISDN 一台 Quidway1600 系列路由器连接中心路由器的例子，从图中可以看出，Router1 的 BRI 口 Bri0 接入 ISDN 网，Bri0 的 IPX 网络号是 1001。中心路由器的号码是 8810124。

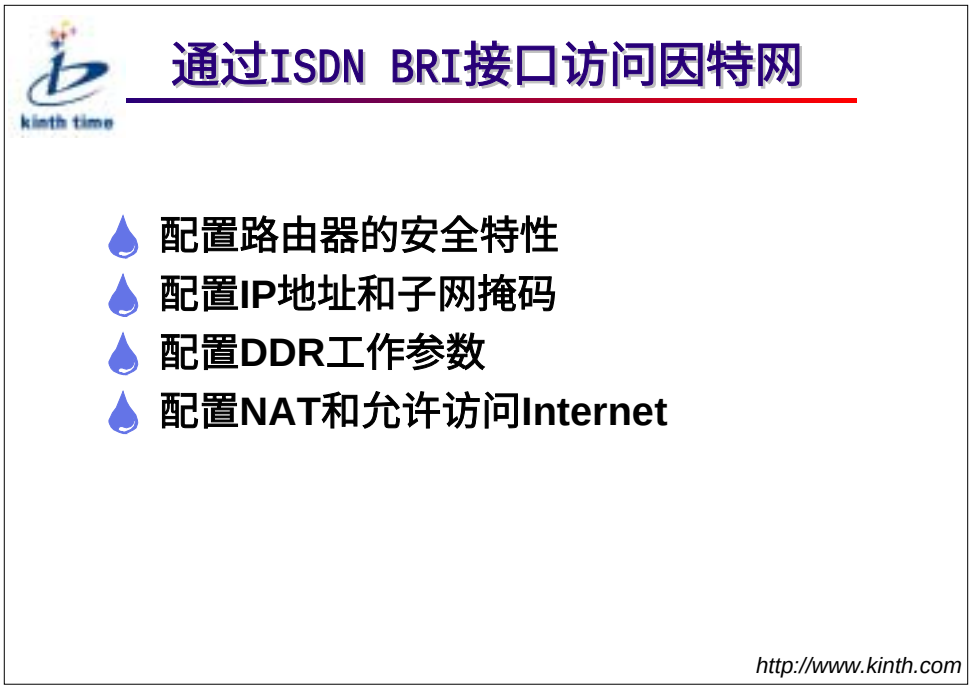
在 ISDN BRI 接口上运行 IPX 协议举例 — 配置



以上配置对应的说明如下：

- 配置 PPP 验证的用户名和口令
- 使能 IPX
- 配置 ISDN BRI 接口 IPX 网络号
- 配置到中心路由器的呼出 Dialer Map
- 封装链路层协议 PPP
- 指定 Dialer Group
- 重新启动 ISDN BRI 接口，使上述配置生效
- 配置激活拨号的规则

.11.5　配置通过 ISDN BRI 接口访问 Internet



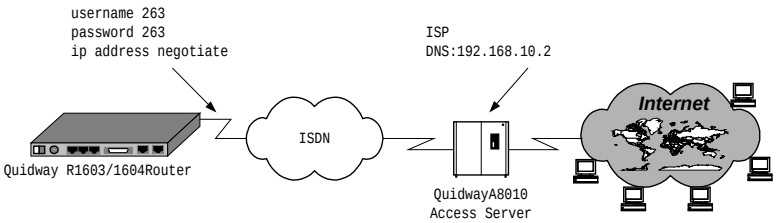
路由器连入 Internet 以后，与路由器相连的内部网就有可能受到恶意的攻击，同时 Internet 用户也可以访问内部网服务器。配置路由器的安全特性就是要防止类似问题的发生。

NAT 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。

.11.6　配置通过 ISDN BRI 接口访问 Internet 实例

通过ISDN BRI接口访问因特网

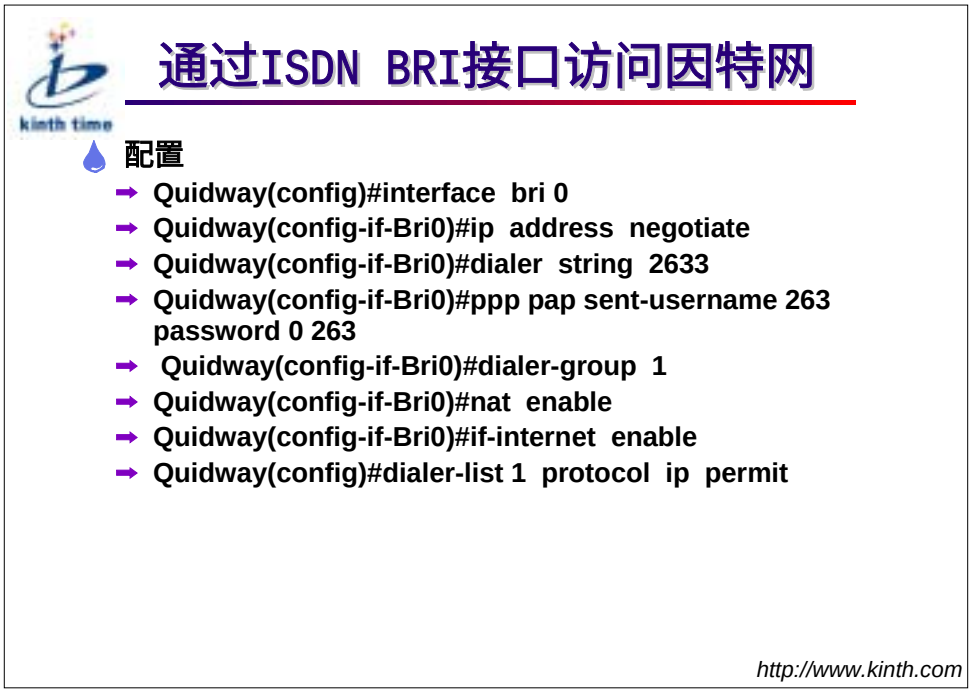
组网图



http://www.kinth.com

这是一个通过 ISDN 访问 Internet 的例子，这个例子中假设 ISP 为 263（首都在线），接入号码为 2633。

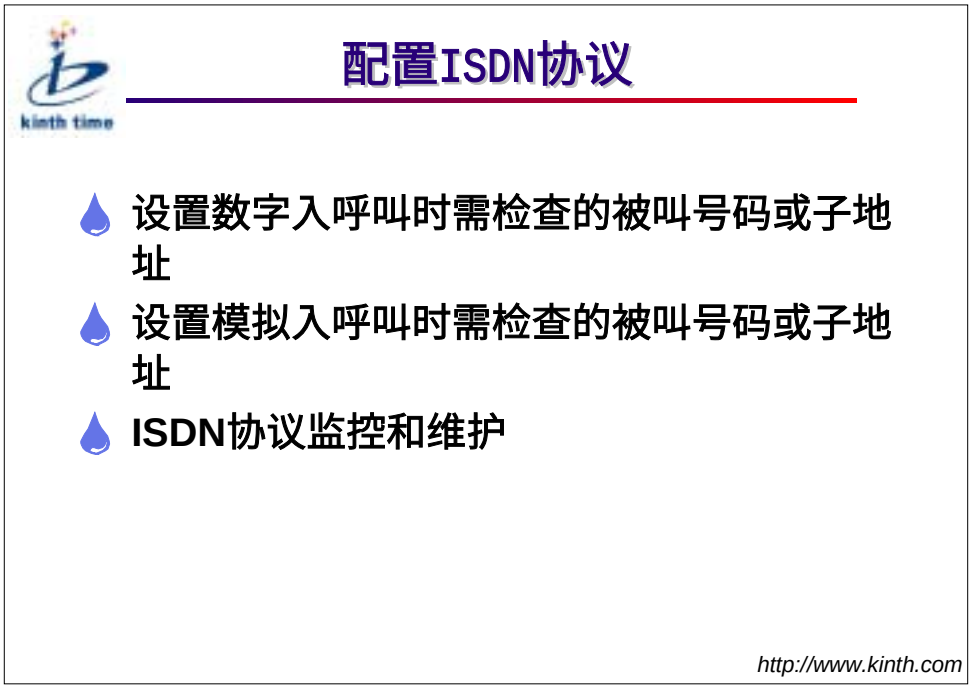
通过 ISDN BRI 接口访问 Internet 举例 — 配置



以上配置对应的说明如下：

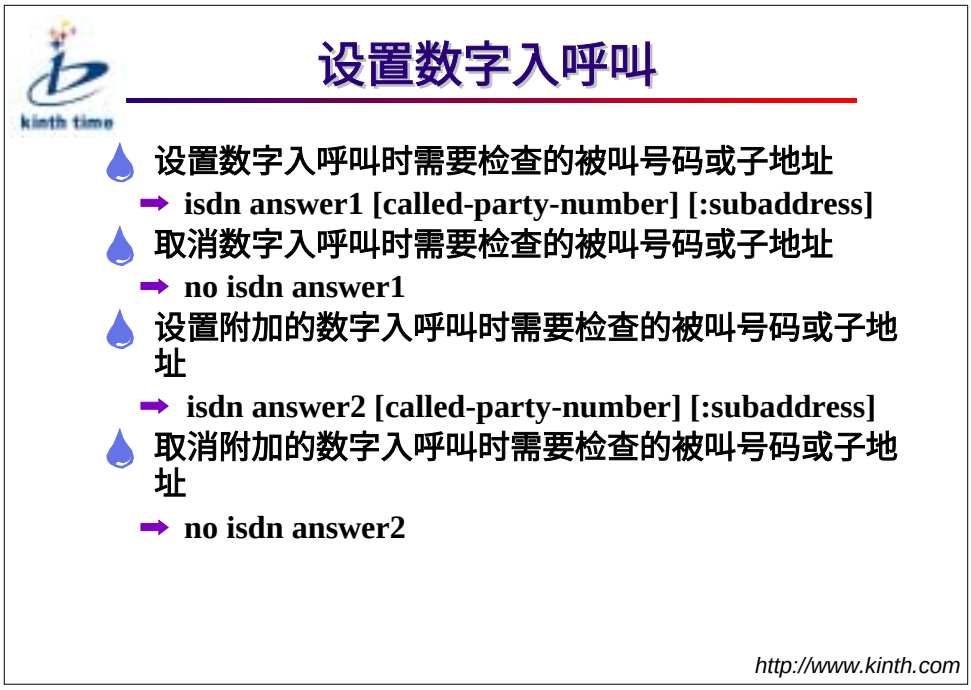
- 进入配置 BRI 接口配置模式
- 配置接口 Bri0 的 IP 地址由 ISP 分配
- 配置接口的拨号串并指定 Dialer group
- 允许通过接口 Bri0 地址转换和访问 Internet
- 配置激活接口 Bri0 拨号的条件

.12 配置 ISDN 协议



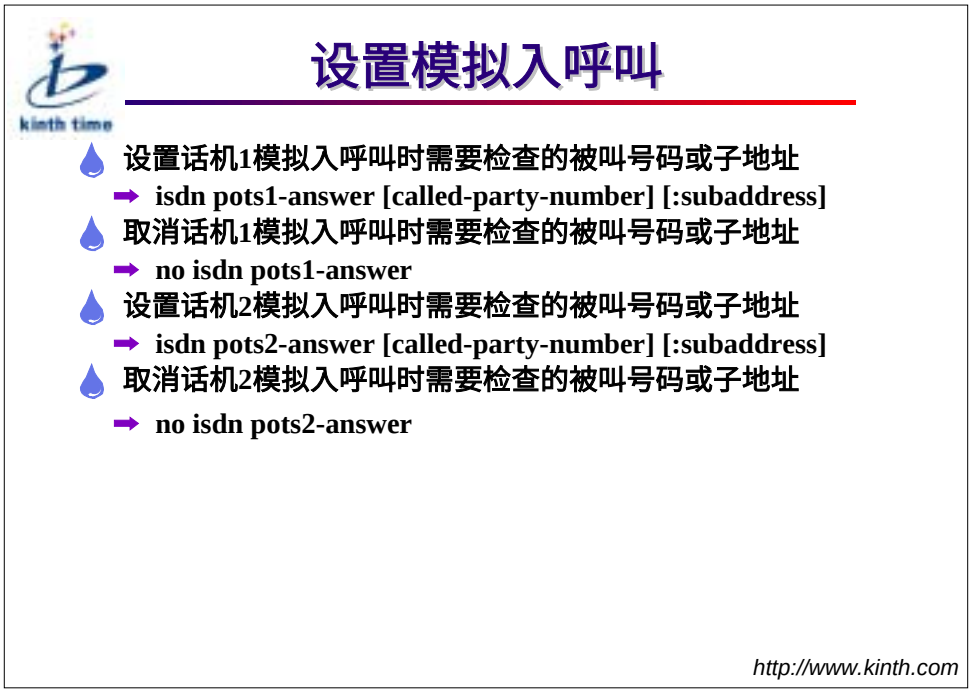
配置 ISDN 协议主要是配置 ISDN 的一些特性，是对 ISDN BRI 口配置的补充，包括：设置入呼叫时需检查的被叫号码或子地址、对 ISDN 协议的监控和维护。

.12.1　设置数字入呼叫



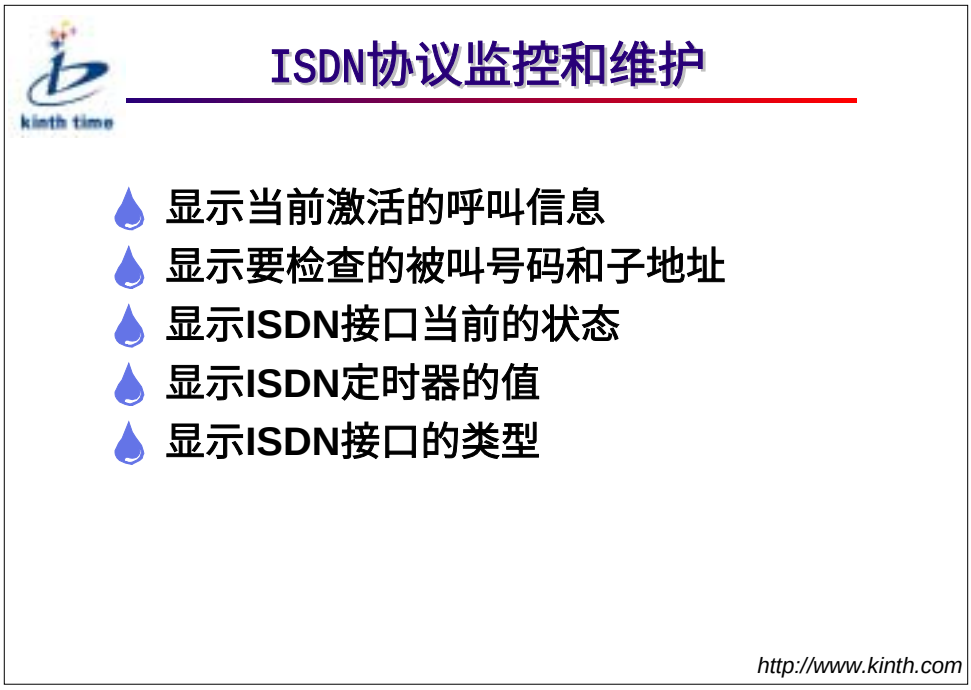
这两条命令用于数字呼入时的检查项设置。只要设定了子地址，对方无论是未发送或发送错子地址，都拒绝该呼叫。上述两条命令是独立的，分别起作用。入呼叫只要满足其中的一项设置，就接受该呼叫。

.12.2　设置模拟入呼叫



这两条命令用于模拟呼入时话机 1 和话机 2 的检查项设置。若某话机设定了子地址，对方发送子地址，但该子地址与此话机设置不同，则该话机不接受此呼叫。

.12.3　ISDN 协议监控和维护



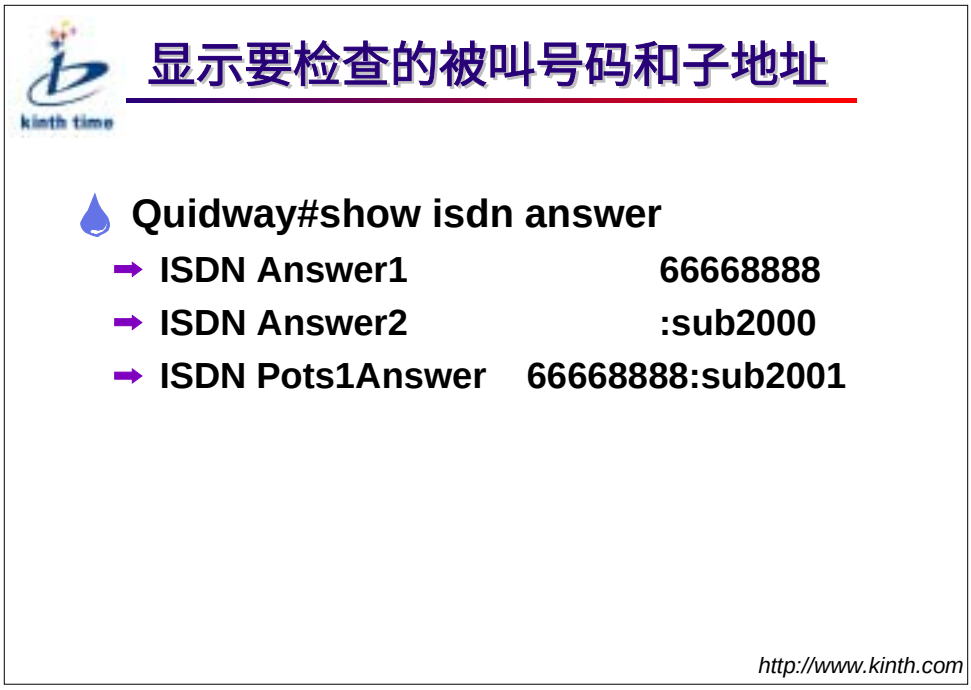
ISDN 协议监控和维护主要用于排除 ISDN 故障，以及监视目前使用情况。

.12.4　显示当前激活的呼叫信息

以上显示信息表示在 ISDN BRI 接口上，当前有两条激活的呼叫：

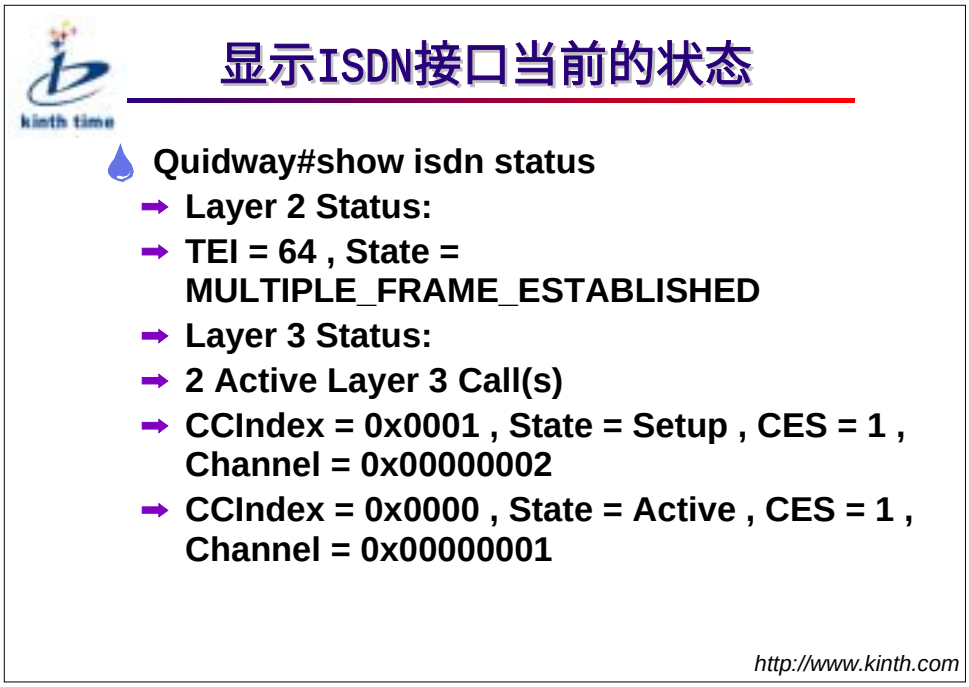
- B1 通道呼出到 8810124 的数字呼叫。
- B2 通道由号码为 8810118、子地址为 380 的终端呼入的模拟呼叫。

.12.5　显示要检查的被叫号码和子地址



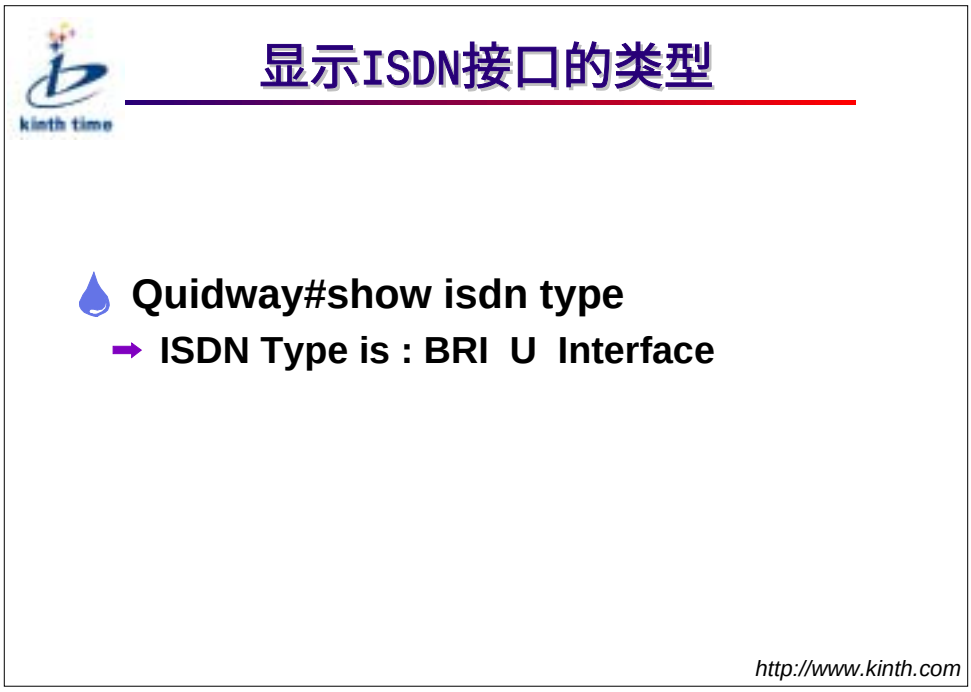
以上显示信息表示在数字入呼叫时要检查的被叫号码为 66668888，附加检查的子地址为 sub2000，在话机 1 模拟入呼叫时要检查的被叫号码为 66668888，子地址为 sub2001。

.12.6　显示 ISDN 接口当前的状态



以上显示信息表示 ISDN 接口的第二层的链路 TEI 为 64，状态为多帧建立；第三层活动呼叫数为 2，索引号为 0x0001 的呼叫，状态为正在建立中，CES 为 1，通道为 0x00000002，索引号为 0x0000 的呼叫，状态为激活，CES 为 1，通道为 0x00000001。

.12.7 显示 ISDN 接口的类型



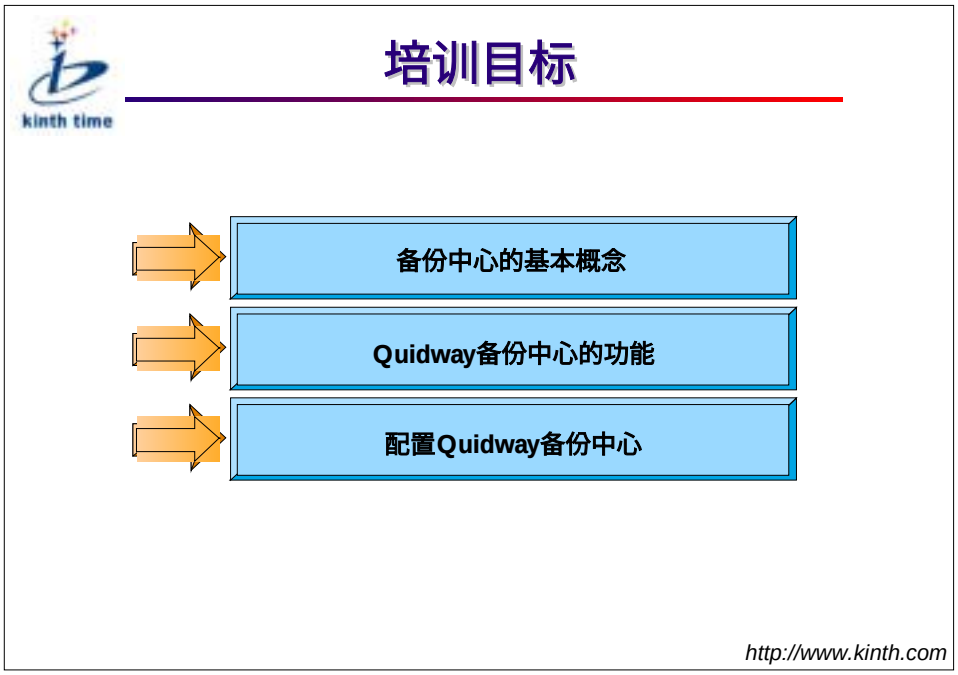
以上输出信息表示 ISDN 接口类型为 BRI U 接口。

.13 本章重点


kinth time
本章重点
了解DDR的用途及功能
掌握DDR的基本配置
了解ISDN技术
掌握ISDN的基本配置
http://www.kinth.com

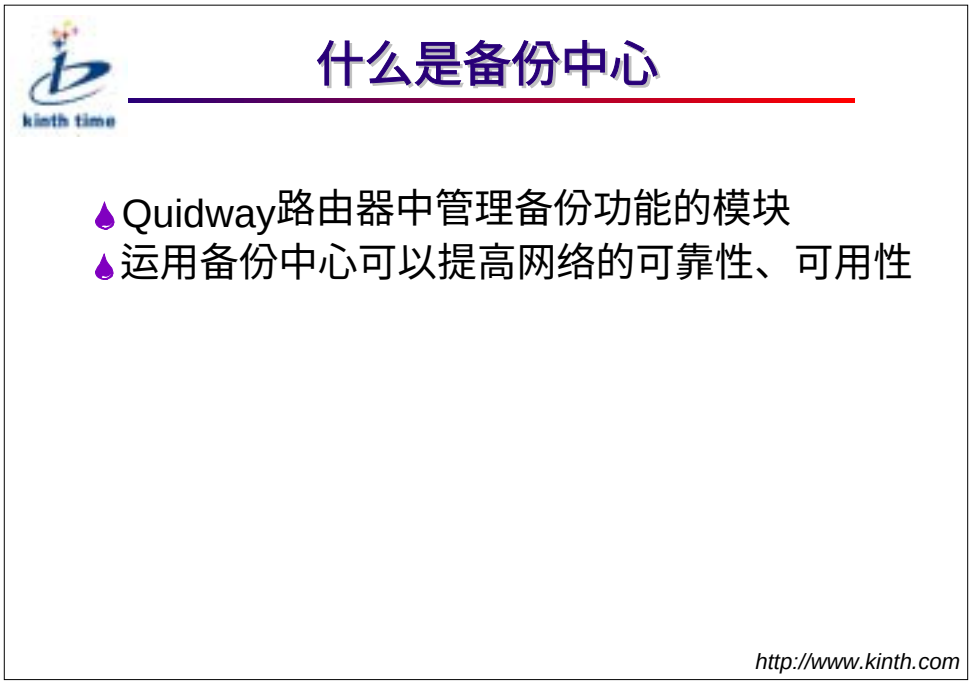
第十二章　　备份中心配置

.1　培训目标



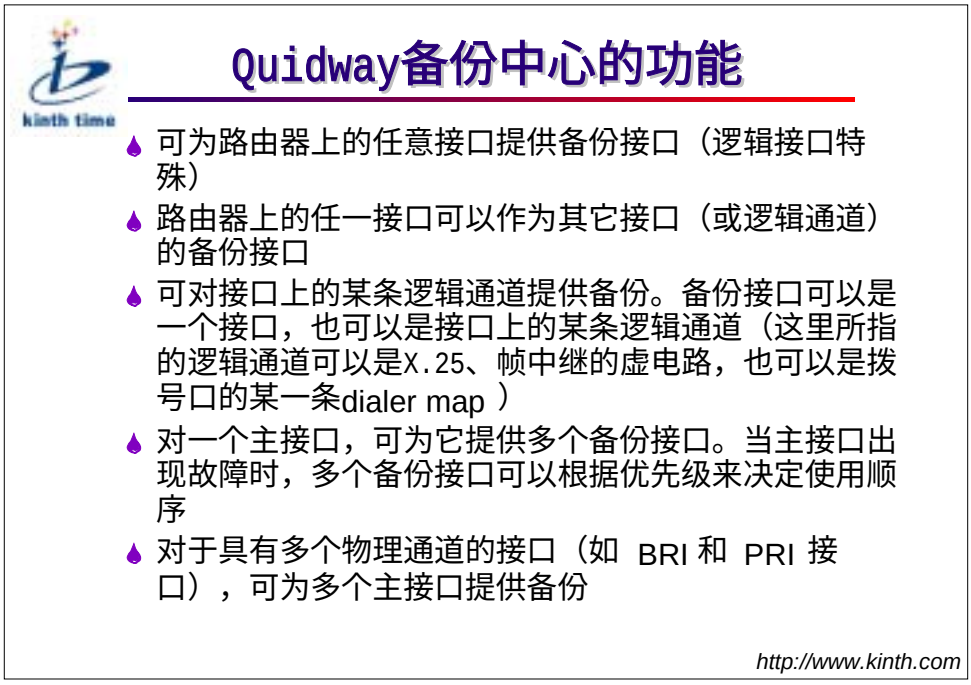
本章讨论 Quidway 路由器备份中心的基本概念、功能及配置方法。

.2　什么是备份中心



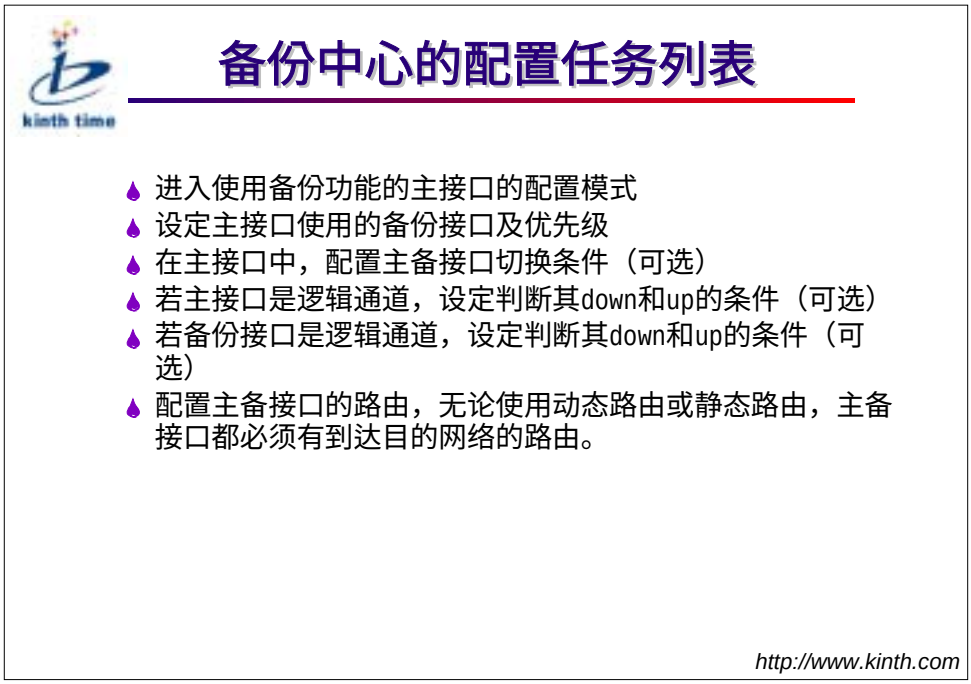
备份中心是 Quidway 路由器中管理备份功能的模块，没有运用备份中心时，一旦接口上的线路发生故障，数据传输就中断了。运用备份中心后，当主接口上的线路发生故障 Down 掉后，备份中心根据用户配置的延迟启动备份接口上的线路进行通讯，数据传输又可以继续进行了。因此运用备份中心可以提高网络的可靠性，增强网络的可用性。

.3　Quidway 备份中心的功能



Quidway 备份中心提供了完整的接口备份功能，不仅可以对任意的物理接口进行备份，还可以对逻辑通道进行备份；同样的，任意的物理接口或逻辑通道都可以作为其它接口或逻辑通道的备份接口。Quidway 备份中心还提供了设置多个备份口的功能，这样当主接口上的通讯线路发生故障时，多个备份接口就会根据预先设置好的优先级顺序启动，保证数据传输的万无一失。另外，对于有多个物理通道的接口，例如：BRI 和 PRI 口，每一个物理通道都可以为一个主接口提供备份的功能，降低备份的通讯成本。

.4　Quidway 备份中心的配置任务列表



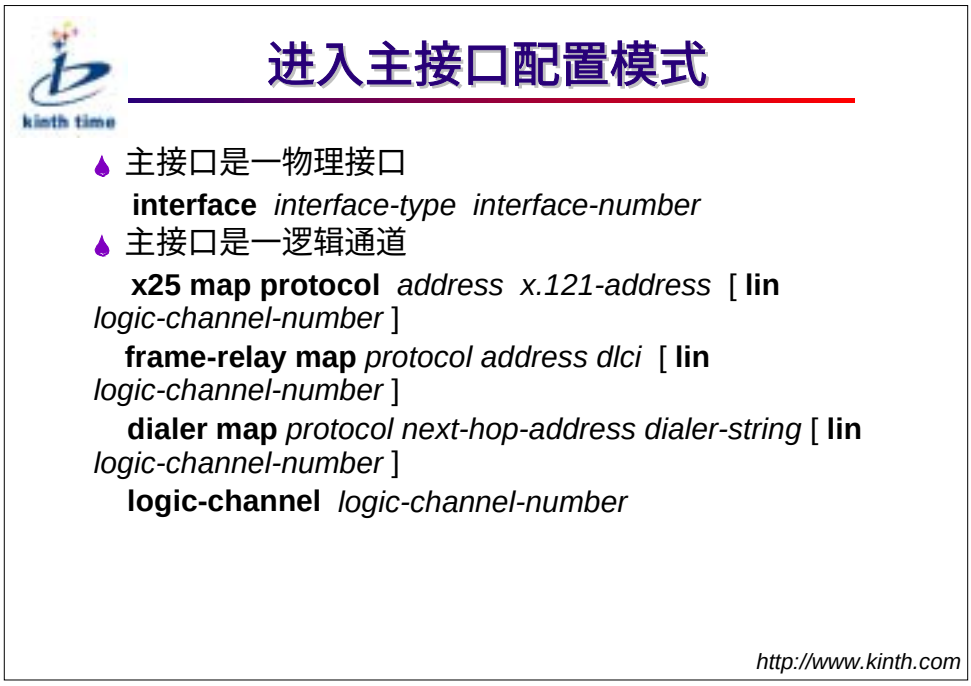
配置 Quidway 备份中心首先要确定主接口是物理接口还是逻辑通道，如果是物理接口，直接进入该接口的配置模式就可以开始配置了，如果是逻辑通道，就要先配置好逻辑通道，然后进入该逻辑通道开始配置。

如果要对主接口指定多个备份接口，那么就要对这些备份接口指定不同的优先级，以便当主接口上的通讯线路发生故障时，按照优先级选用不同的备份接口。

另外，Quidway 备份中心还可以配置主备接口的切换条件，以及逻辑通道判断其 down 和 up 的条件。

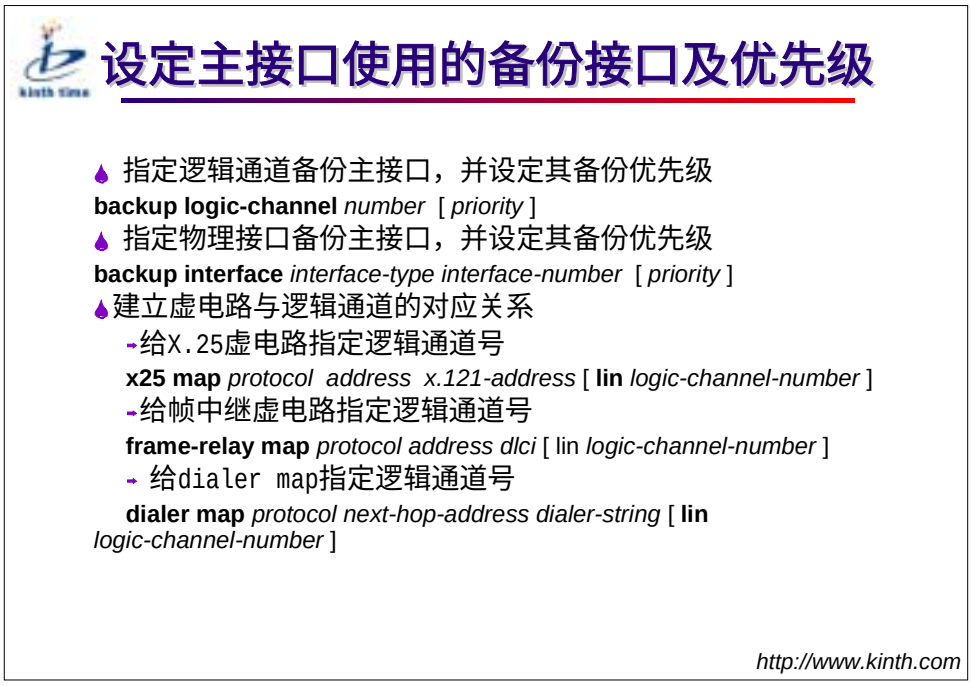
需要注意的是，配置备份中心时，不论是采用动态路由还是静态路由，主备接口都必须有到达目的网络的路由。

.4.1　进入主接口配置模式



如果主接口是一物理接口，直接用 Interface 命令就可以进入接口配置模式了；如果主接口是逻辑通道，那就需要根据使用的是 X.25、帧中继、拨号口，先配置逻辑通道，再用 logic-channel 命令进入接口配置模式。

.4.2　设定主接口使用的备份接口及优先级

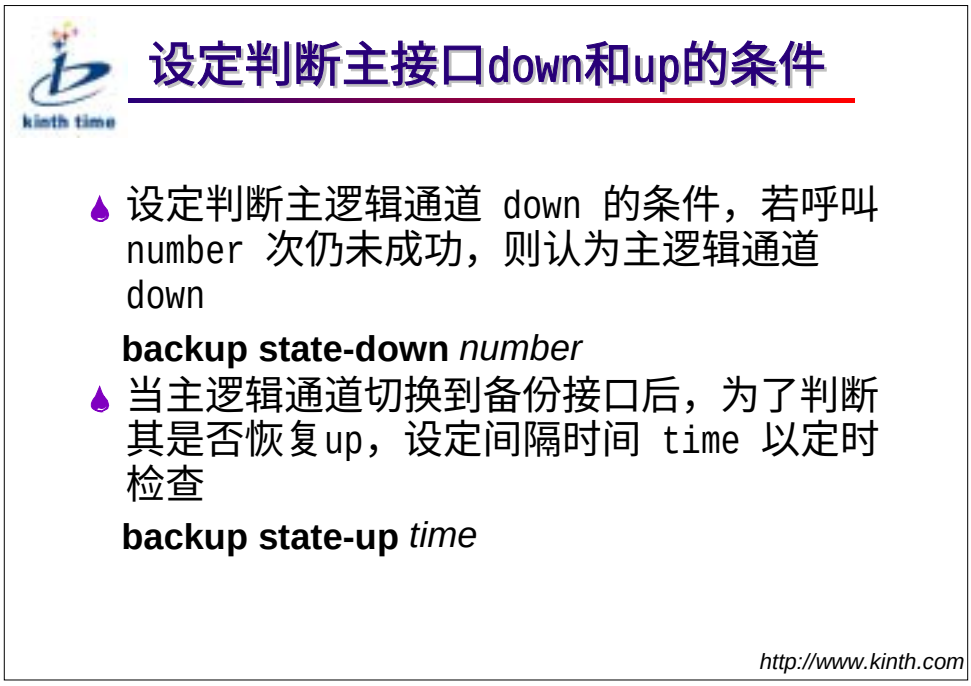


如果要指定物理接口备份主接口，只要用 backup interface 命令指定相应的备份接口和优先级就可以了。如果要指定逻辑通道备份主接口，就需要先建立虚电路与逻辑通道的对应关系，然后再用 backup logic-channel 命令指定相应的备份逻辑通道和优先级。

.4.3　配置主备接口切换条件

当主接口由 up 转为 down 后，并不立即切换到备份接口，而是等待 enable-delay 秒后，若主接口状态仍为 down，才切换到备份接口。
当主接口由 down 转为 up 后，并不立即切换回主接口，而是等待 disable-delay 秒后，若主接口状态仍为 up，才切换回主接口。
如果选择 **never** 则不会进行切换。

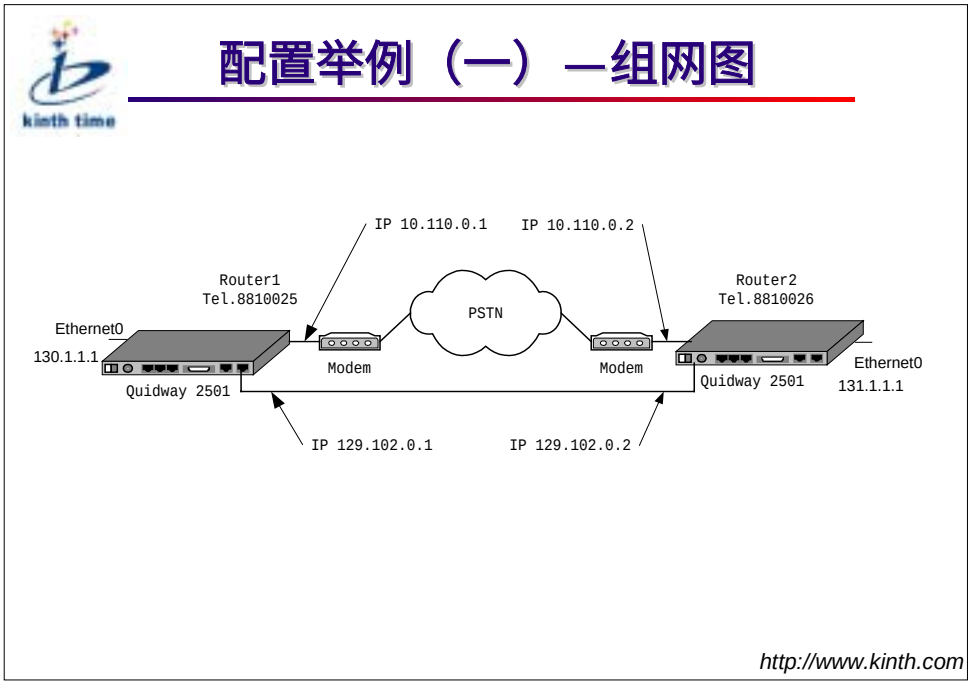
.4.4　设定判断主接口 down 和 up 的条件



当主接口是逻辑通道时，如果在呼叫指定次数仍未成功，则认为主逻辑通道处于 down 状态；当主逻辑通道切换到备份接口后，为了判断其是否恢复 up 状态，需要按指定时间间隔定时检查主逻辑通道状态。

.5　配置举例（一）

.5.1　组网图



这是一个简单的配置实例，拨号口 Serial 1 被配置为 Serial 0 的备份接口，主接口 down 掉后备份接口自动开始拨号建立连接，主接口恢复后从备份接口切换回主接口。

.5.2　配置

配置举例（一）—配置

配置Router1：

```
Quidway(config)#  interface  ethernet 0
Quidway(config-if-Ethernet)#ip address 130.1.1.1 255.255.255.0
Quidway(config-if-Ethernet)#interface serial 0
Quidway(config-if-Serial0)#ip address 129.102.0.1 255.255.0.0
Quidway(config-if-Serial0)#  backup interface  serial  1
Quidway(config-if-Serial0)#  interface serial 1
Quidway(config-if-Serial1)#physical asynchronous
Quidway(config-if-Serial1)#ip address 10.110.0.1 255.255.0.0
Quidway(config-if-Serial1)#dialer in-band
Quidway(config-if-Serial1)#dialer-group 1
Quidway(config-if-Serial1)#dialer map ip 10.110.0.2 8810026
Quidway(config-if-Serial1)#exit
Quidway(config)#dialer-list 1 protocol ip permit
Quidway(config)#ip route 131.1.1.1 255.255.255.0 129.102.0.2
Quidway(config)#ip route 131.1.1.1 255.255.255.0 10.110.0.2
```

http://www.kinth.com

配置举例（一）—配置

配置Router2：

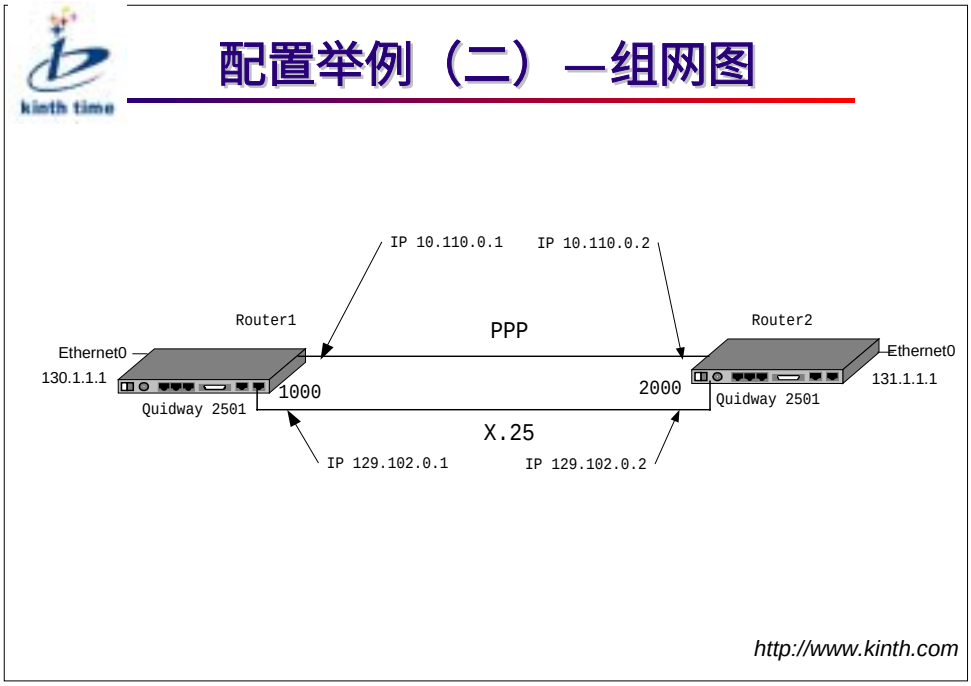
```
Quidway(config)#  interface  ethernet 0
Quidway(config-if-Ethernet)#ip address 131.1.1.1 255.255.255.0
Quidway(config-if-Ethernet)#interface serial 0
Quidway(config-if-Serial0)#ip address 129.102.0.2 255.255.0.0
Quidway(config-if-Serial0)#  backup interface  serial  1
Quidway(config-if-Serial0)#  interface serial 1
Quidway(config-if-Serial1)#physical asynchronous
Quidway(config-if-Serial1)#ip address 10.110.0.2 255.255.0.0
Quidway(config-if-Serial1)#dialer in-band
Quidway(config-if-Serial1)#dialer-group 1
Quidway(config-if-Serial1)#dialer map ip 10.110.0.1 8810025
Quidway(config-if-Serial1)#exit
Quidway(config)#dialer-list 1 protocol ip permit
Quidway(config)#ip route 130.1.1.1 255.255.255.0 129.102.0.1
Quidway(config)#ip route 130.1.1.1 255.255.255.0 10.110.0.1
```

http://www.kinth.com

在本配置中，Serial0 接口配置为 PPP 封装，作为主接口。Serial1 接口配置成拨号口，作为备份接口。

.6　配置举例（二）

.6.1　组网图



这是一个使用 PPP 连接备份 X.25 逻辑通道的配置实例，Serial 1 被配置为 Serial 0 上的逻辑通道 10 的备份接口。

.6.2　配置

配置举例（二）—配置

配置Router1：

```
Quidway(config)#  interface ethernet  0
Quidway(config-if-Ethernet)#ip address 130.1.1.1 255.255.255.0
Quidway(config-if-Ethernet)#interface serial 0
Quidway(config-if-Serial0)#  encapsulation x25 dce
Quidway(config-if-Serial0)#ip address 129.102.0.1 255.255.0.0
Quidway(config-if-Serial0)#x25 address 1000
Quidway(config-if-Serial0)#  x25 map ip 129.102.0.2   2000  lin  10
Quidway(config-if-Serial0)#exit
Quidway(config)#  logic-channel 10
Quidway(config-logic-channel10)#  backup interface serial 1
Quidway(config-logic-channel10)#  backup state-up  10
Quidway(config-logic-channel0)#exit
Quidway(config)#interface serial 1
Quidway(config-if-Serial1)#encapsulation ppp
Quidway(config-if-Serial1)#ip address 10.110.0.1 255.0.0.0
Quidway(config)#ip route 131.1.1.1 255.255.255.0 129.102.0.2
Quidway(config)#ip route 131.1.1.1 255.255.255.0 10.110.0.2
```

http://www.kinth.com

配置举例（二）—配置

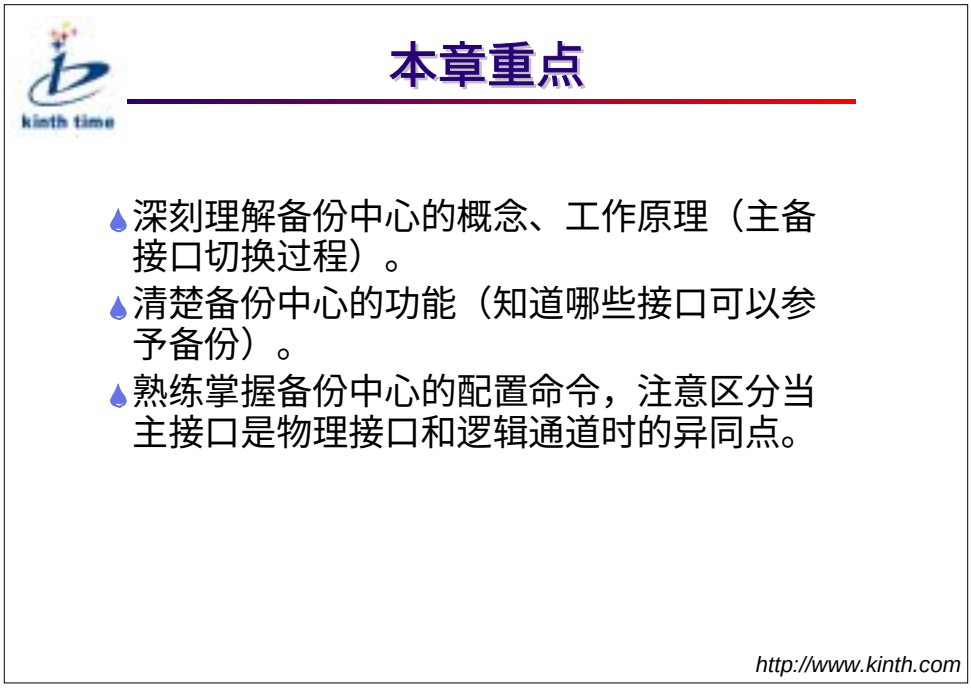
配置Router2：

```
Quidway(config)#  interface ethernet  0
Quidway(config-if-Ethernet)#ip address 131.1.1.1 255.255.255.0
Quidway(config-if-Ethernet)#interface serial 0
Quidway(config-if-Serial0)#encapsulation x25 dte
Quidway(config-if-Serial0)#ip address 129.102.0.2 255.255.0.0
Quidway(config-if-Serial0)#x25 address 2000
Quidway(config-if-Serial0)#x25 map ip 129.102.0.1   1000  lin  10
Quidway(config-if-Serial0)#interface serial 1
Quidway(config-if-Serial1)#encapsulation ppp
Quidway(config-if-Serial1)#ip address 10.110.0.2 255.0.0.0
Quidway(config-if-Serial1)#exit
Quidway(config)#ip route 130.1.1.1 255.255.255.0 129.102.0.1
Quidway(config)#ip route 130.1.1.1 255.255.255.0 10.110.0.1
```

http://www.kinth.com

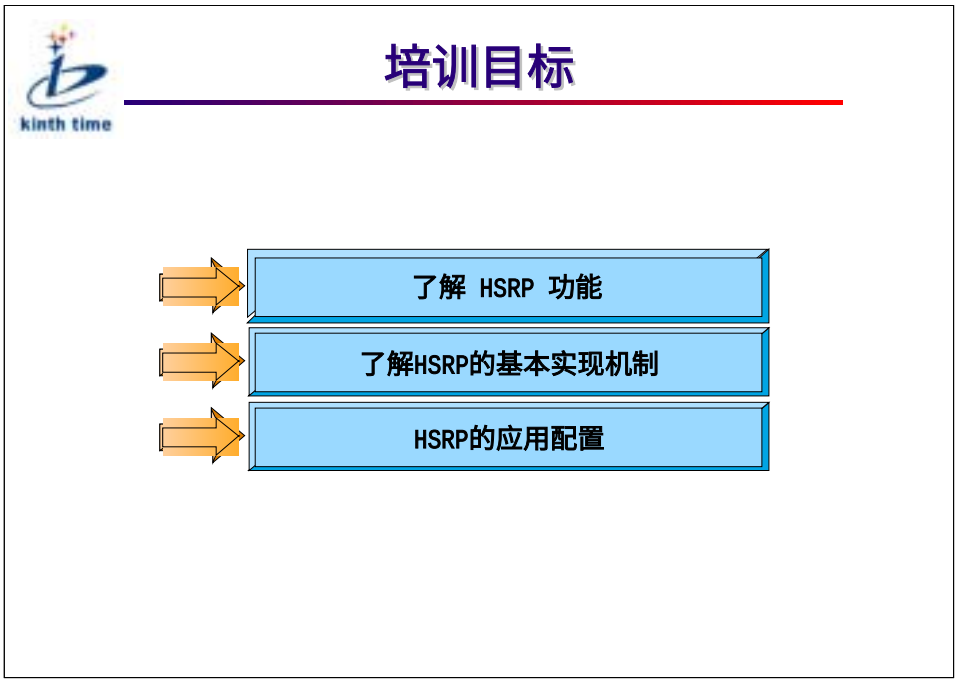
在本配置中，在 Serial0 上定义了逻辑通道 10，作为主接口。Serial1 接口配置成 PPP 封装，并设置当主逻辑通道 Down 掉后，每隔 10 秒检查其是否恢复 Up。

7 本章重点


本章重点
深刻理解备份中心的概念、工作原理（主备接口切换过程）。
清楚备份中心的功能（知道哪些接口可以参予备份）。
熟练掌握备份中心的配置命令，注意区分当主接口是物理接口和逻辑通道时的异同点。
http://www.kinth.com

第十三章 HSRP 协议及配置

.1 培训目标



本章讨论 HSRP 协议的功能和实现、Quidway 路由器 HSRP 用途、实现及应用。

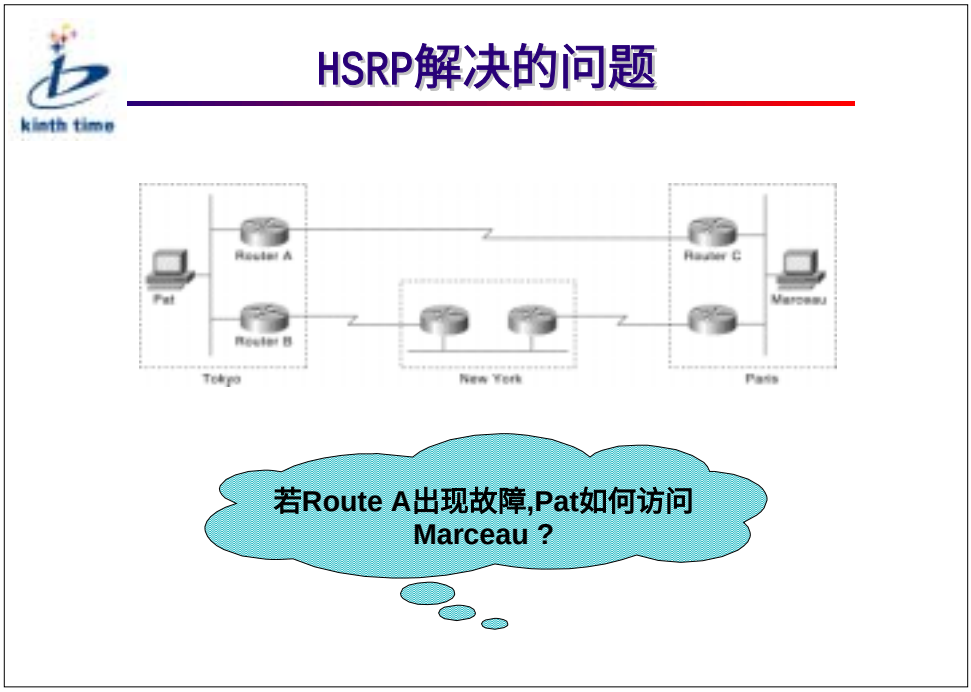
.2 HSRP 协议简介

.2.1 HSRP 的概念

HSRP 是 Hot Standby Routing Protocol（热备份路由协议）的缩写。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，尽量不被察觉。

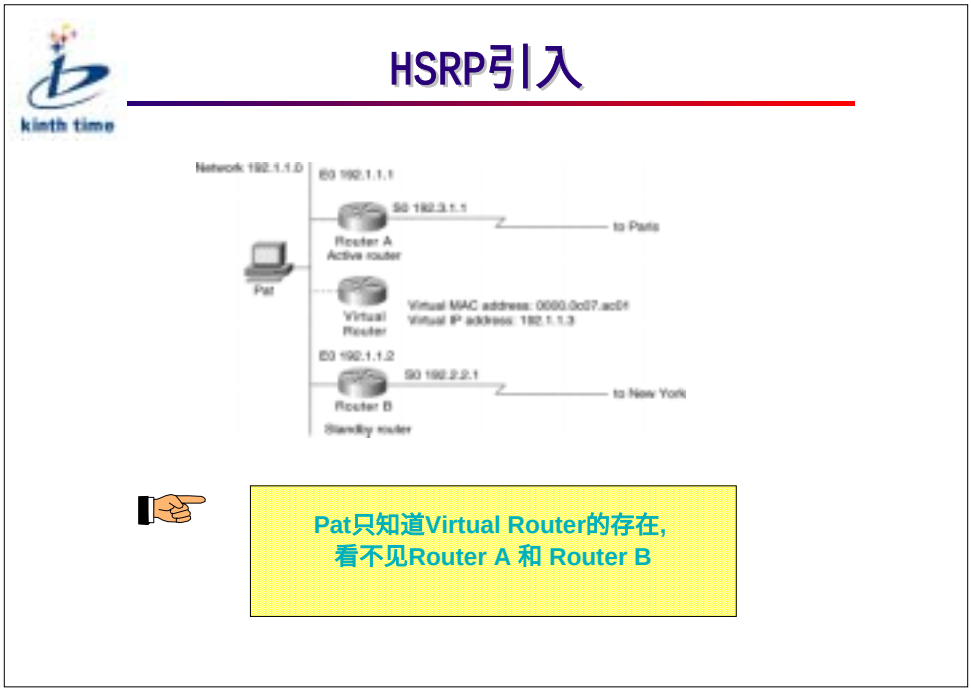
通常，我们的网络上主机设置一条缺省路由，指向主机所在网段内的一个路由器 R，这样，主机发出的目的地址不在本网段的报文将被通过缺省路由发往路由器 R，从而实现了主机与外部网络的通信。在这种情况下，当路由器 R 坏掉时，本网段内所有以路由器 R 为缺省路由下一跳的主机将断掉与外部的通信。HSRP 实现容错备份功能，可以有效解决上述可靠性问题。

.2.2　HSRP 解决的问题



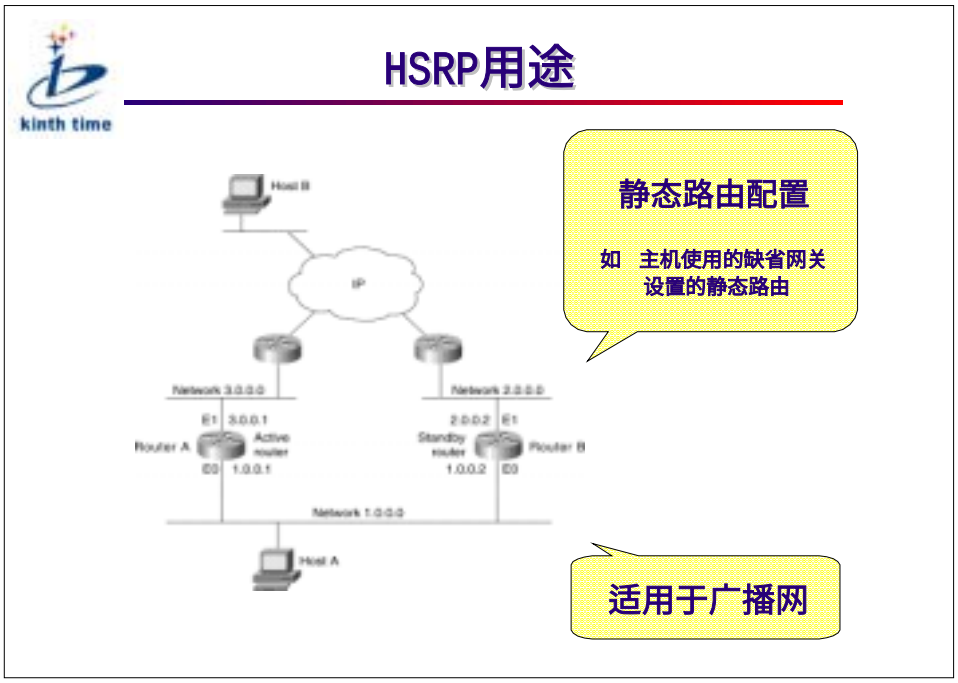
主机 Pat 设置缺省网关 Router A，这样访问主机 Marceau 需要通过 Router A 来进行。一旦 Router A 出现故障，主机 Pat 将失去与主机 Marceau 的联系，除非主机 Pat 重新指定其它的缺省网关，如 Router B。

.2.3　HSRP 的引入



让我们看一下引入 HSRP 是如何解决问题的。通过在 Router A 和 Router B 上配置 HSRP，使它们共同组成一个备份组，可以把这个组抽象成一个虚拟路由器，它有自己的 IP 地址和 MAC 地址，分别称作虚拟 IP 地址和虚拟 MAC 地址。这样主机 Pat 可以把自己的缺省网关设置成虚拟 IP 地址，访问主机 Marceau 就可以通过虚拟路由器来进行。当然，虚拟路由器是一个抽象的概念，实际的网关工作是由 Router A 和 Router B 中的一个来完成的，我们称完成实际网关工作的路由器为活动路由器，另外一个路由器为备份路由器。如果活动路由器出现故障，就像前面提到的 Router A 发生故障，备份路由器（如 Router B）会接替成为活动路由器，因此，主机 Pat 在不察觉情况下，仍然可以通过 Router B 来访问主机 Marceau。

.2.4　HSRP 的用途



HSRP 用于广播或多播局域网上的路由器热备份，并适于静态的路由配置，实际上 HSRP 正是解决设备不能动态适应路由改变的问题。

HSRP 主要用途：

1、主机设置缺省网关

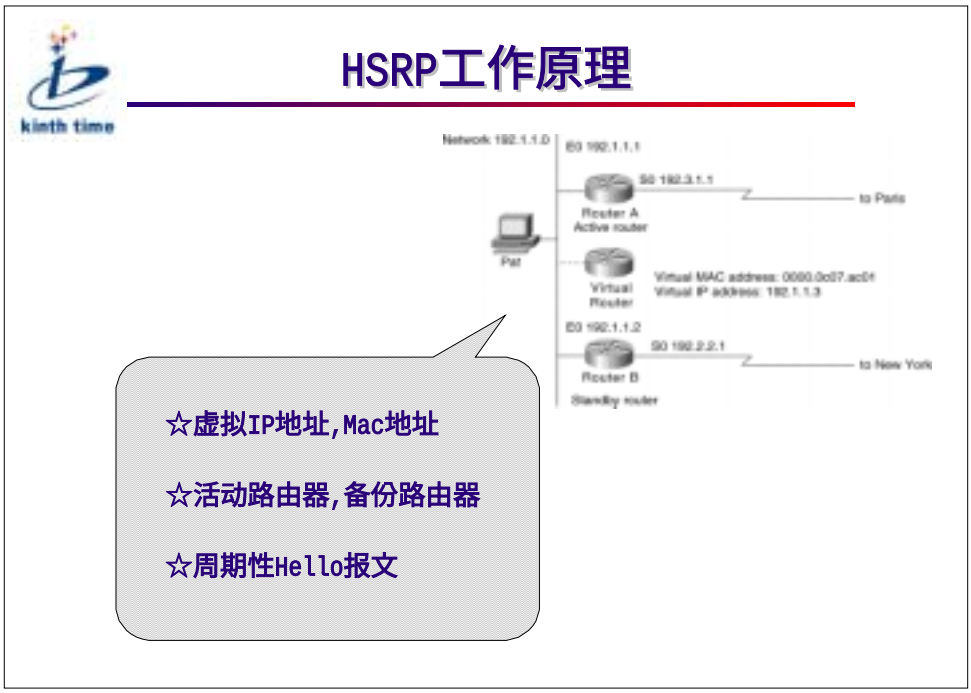
假设主机 A 是局域网中一台需要访问远程数据的服务器，要求远程访问能力可靠。由于主机 A 中静态设置缺省网关，一旦想更换网关，必须在主机中重新配置。 通过使用 HSRP，主机中设置虚拟路由器为缺省网关，具体由虚拟路由器中的哪台路由器完成网关的实际工作，主机并不关心，这就为应用提供了较好的可靠性和灵活性。

2、设置静态路由

可以通过配置静态缺省路由指向虚拟路由器来实现另外一种备份。

.3　HSRP的实现

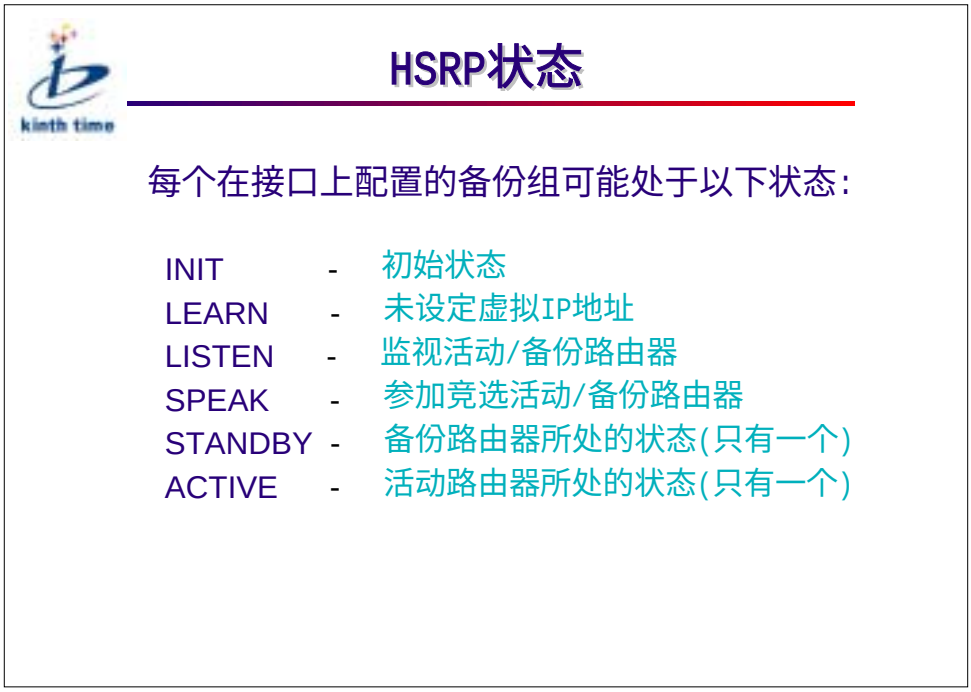
.3.1　HSRP 工作原理



当采用 HSRP， 用户看到的是一台虚拟路由器，该虚拟路由器有自己的虚拟 IP 地址和虚拟 MAC 地址，该虚拟路由器是由一组路由器组成的，这组路由器称为备份组。备份组内由一台活动路由器、一台备份路由器，以及群众路由器构成。一般情况下，一旦活动路由器坏掉，该备份路由器成为活动路由器，然后备份组内选举组内的另一台路由器为备份路由器。

组内路由器通过接受来自活动路由器的周期性 Hello 报文来判断活动路由器是否工作正常。如果组内备份路由器 R 在一定时间间隔未收到活动路由器 Hello 报文，就认为活动路由器坏掉了，优先级高的备份路由器最终成为活动路由器。备份路由器也是通过类似过程产生的。这样总能保证备份组中有一台活动路由器，一台备份路由器。

.3.2 HSRP 状态



备份组内的路由器处于各自的状态，根据相互间发送 HSRP 报文来调整新的状态。

HSRP 状态：

（1）INIT

所有备份组内组员的初始状态为 INIT，当组员配置属性或端口 UP 时，进入 INIT 状态。

（2）LEARN

该组员未设定虚拟 IP 地址，并等待从本组活动路由器发出的认证的 Hello 报文中学习得到自己的虚拟 IP 地址。

（3）LISTEN

该组员已得知或设置了虚拟 IP 地址，通过监听 Hello 报文监视活动/备份路由器，一旦发现活动/备份路由器长时间未发送 Hello 报文，则进入 SPEAK 状态，开始竞选。

（4）SPEAK

参加竞选活动/备份路由器的组员所处的状态，通过发送 Hello 报文使竞选者间相互比较、竞争。

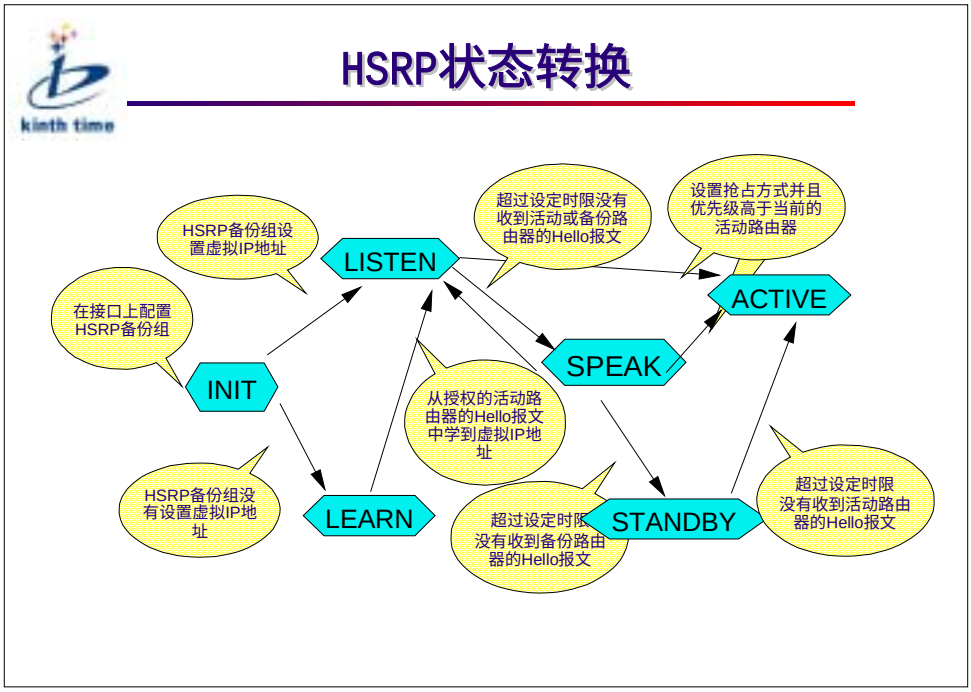
（5）STANDBY

组内备份路由器所处的状态，备份组员监视活动路由器，准备随时在活动路由器坏掉时接替活动路由器。备份路由器也周期性发送 Hello 报文告诉其他组员自己没有坏掉。

（6）ACTIVE

组内活动路由器即负责虚拟路由器实际路由工作的组员所处的状态。活动路由器周期性发送 Hello 报文告诉其他组员自己没有坏掉。

.3.3　HSRP 状态转换



HSRP 协议中定义了一个自动状态机，不同的触发事件会产生相应的状态变化和动作。

.3.4 HSRP 报文

- Version ：1 Byte

HSRP 报文的版本号。本文档的 HSRP 报文版本为 0 。

- Oper Code ：1 Byte

描述了 HSRP 报文的类型，共有 3 种报文类型：

（1）0 —— Hello

Hello 类型报文说明发送者处在运行状态，有能力成为活动/备份路由器。

（2）1 —— COUP

COUP 类型报文说明发送者希望成为活动路由器。

（3）2 —— RESIGN

COUP 类型报文说明发送者不再是活动路由器。

- State ：1 Byte

描述发送者发送报文时所处的状态。

- Hello Time ：1 Byte

该域只在 Hello 报文中有意义。它包含发送者发送 Hello 报文的时间间隔，以秒计；

如果路由器上未配置 Hello Time 值，它可以从组中活动路由器发送的 Hello 报文中学习到，但须本路由器认证该 Hello 报文；

如果路由器上既未配置 Hello Time，也未学习到，则赋予缺省值 3。

- Hold Time ：1 Byte

该域只在 Hello 报文中有意义。它包含发送者发送 Hello 报文的持有时间，以秒计；

Hold Time 必须大于 Hello Time ，而且最好大于三倍 Hello Time ；

如果路由器上未配置 Hold Time ，它可以从组中活动路由器发送的 Hello 报文中学习到，但须本路由器认证该 Hello 报文；
如果路由器上既未配置 Hello Time ，也未学习到，则赋予缺省值 10 。

- Priority ：1 Byte

该域用来选举活动/备份路由器。当选举过程中出现竞争（多个路由器都想成为活动/备份路由器）时，优先级最高的竞争者胜，对于优先级相等的竞争者，IP 地址最大的竞争者胜。

- Group ：1 Byte

此域中记录发送者所在的备份组号。对于以太网，Group 取值范围为 0-255 。

- Authentication Data ：8 Byte

8 字符长的的口令，用于组内成员相互鉴别。

- Vritual IP Address ：4 Byte

备份组的虚拟 IP 地址，备份组模拟的虚拟路由器的 IP 地址。虚拟路由器还有一 MAC 地址，它由组号直接映射而成：0X00 00 0C 07 AC ** ，其中“**”为备份组号。
组内各成员须至少有如下信息：
（1）备份组号（Group）；
（2）虚拟 MAC 地址（Virtual MAC Address）；
（3）优先级（Priority）；
（4）Authentication Data；
（5）Hello Time；
（6）Hold Time；
至少一位组员有如下信息：
（1）虚拟 IP 地址（Virtual IP Address）；
每位组员可选择配置如下信息：
（1）抢占标志（Preempt）；
如果某位组员的 Preempt 置位，又收到活动路由器的 Hello 报文，发现自己的优先级比活动路由器高，则该组员可强行取代成为活动路由器。

.3.5 HSRP 多备份组（MHSRP）

在一网段内，多个备份组可以共存。每个备份组模拟成一虚拟路由器，每个这样的虚拟路由器配置一虚拟 MAC 地址和一虚拟 IP 地址。该虚拟 IP 地址应属于本网段，而且不与网段内的任何路由器和主机的 IP 地址相同，也不与网段内的其他虚拟路由器的虚拟 IP 地址相同。
一台路由器也可以参加多个备份组，为多个组作备份。
路由器的 HSRP 配置是针对具体接口的，因此需要在接口模式下配置。
在一台路由器上，备份组由（接口，组号）唯一确定。每个备份组都有属于自己的数据和状态。
如果一台路由器有两个以太网口，可以分别在两个接口上配置两个 HSRP 备份组，为不同网段使用。

.4　HSRP 的配置方法

.4.1　HSRP 基本配置

- [no] standby　[group-number] ip [virtual ip address]

说明：

使路由器在指定局域网段加入或退出一个备份组。需要指定备份组号和虚拟 IP 地址。备份组号范围从 0 到 255，如 group-number 不指定，备份组号缺省为 0，virtual ip address 如果不指定，路由器不会参与备份，直到从备份组中的活动路由器获得虚拟 IP 地址。注意虚拟 IP 地址应该是接口所在网段的地址。一旦退出 HSRP 备份组，则路由器在该备份组上设置的所有 HSRP 特性不再有效（如优先级，授权字等）。

- standby　[group-number] priority [priority-value]

说明：

HSRP 中根据优先级来确定参与备份组的每台路由器的地位，备份组中优先级最大并且已获得虚拟 IP 地址的路由器将成为活动路由器，优先级其次的路由器将成为备份路由器。优先级缺省值是 100，可设置范围从 0 到 255。

- standby　[group-number] preempt

说明：

一旦备份组中的某台路由器成为活动路由器，只要它没有出现故障，其它路由器即使随后被配置更高的优先级，也不会成为活动路由器，除非被设置抢占方式。路由器如果设置抢占方式，它一旦发现自己的优先级比当前的活动路由器的优先级高，就会成为活动路由器。相应

地，原活动路由器会退出活动态，成为备份路由器或其它。缺省方式是不抢占。

- standby [group-number] authentication string

说明：

HSRP 授权字确认同备份组间其它路由器的有效性。授权字 string 的长度不超过 8 个字节。注意：同一备份组要设置相同的授权字。

- standby [group-number] timers [hello_time] [hold_time]

说明：

HSRP 备份组路由器之间通过定时发送 Hello 报文确认相互的状态，超过一定时间（hold time）没有收到某台路由器的 Hello 报文，则认为它已关机或出现故障。用户可以调整发送 Hello 报文的间隔时间（hello time）和超时时间（hold time）。缺省值分别是 3 秒和 10 秒。时间单位是秒。注意：同一备份组要设置相同的 hello time 和 hold time。

- standby [group-number] track interface_name [priority-reduced]

说明：

HSRP 监视接口功能，更好地扩充了备份功能，即不仅在路由器出现故障时提供备份功能，而且在某网络接口不可用时，也可以使用备份功能。命令作用是监视接口 interface_name，如果接口变为不可用，则将优先级减少 priority-reduced （priority-reduced 缺省值为 10） 。

.4.2 HSRP 其它配置

- standby use-bia

当主机使用 HSRP 备份组，除了使用虚拟 IP 地址，还要使用备份组的虚拟 MAC 地址，缺省方式下，每个 HSRP 备份组使用特殊保留的 MAC 地址作为虚拟 MAC 地址，以保证备份组对主机的透明性。然而，用户也可以设置 HSRP 备份组使用活动路由器的真实 MAC 地址。

- standby use-ovmac xx-xx-xx-xx-xx-xx

对于 HSRP 备份组的虚拟 MAC 地址， 随生产厂家而不同。为了实现与其它厂家路由器的互通，Quidway 提供用户更改虚拟 MAC 地址的设置。

- show standby

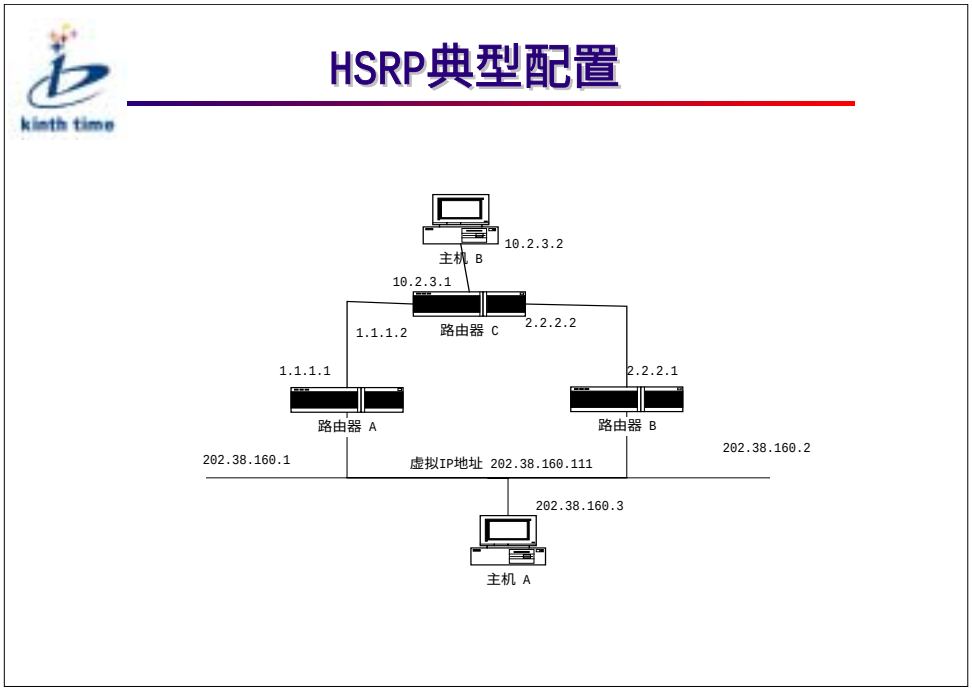
显示 HSRP 信息。

- debug standby

显示调试信息。

.4.3　HSRP 配置实例

14.4.3.1　组网



以上图说明 HSRP 的典型配置，以路由器 A、B 作为备份路由器实现热备份。

14.4.3.2　HSRP 典型配置（一）

配置需求一：
主机 A 把路由器 A 和路由器 B 组成的 HSRP 备份组作为自己的缺省网关，访问 Internet，如主机 B。
HSRP 备份组构成：备份组号为 0，虚拟 IP 地址为 202.38.160.111，路由器 A 做活动路由器，路由器 B 做备份路由器，允许抢占。

14.4.3.3　HSRP 典型配置（一）（续）

HSRP典型配置（一）Cont.

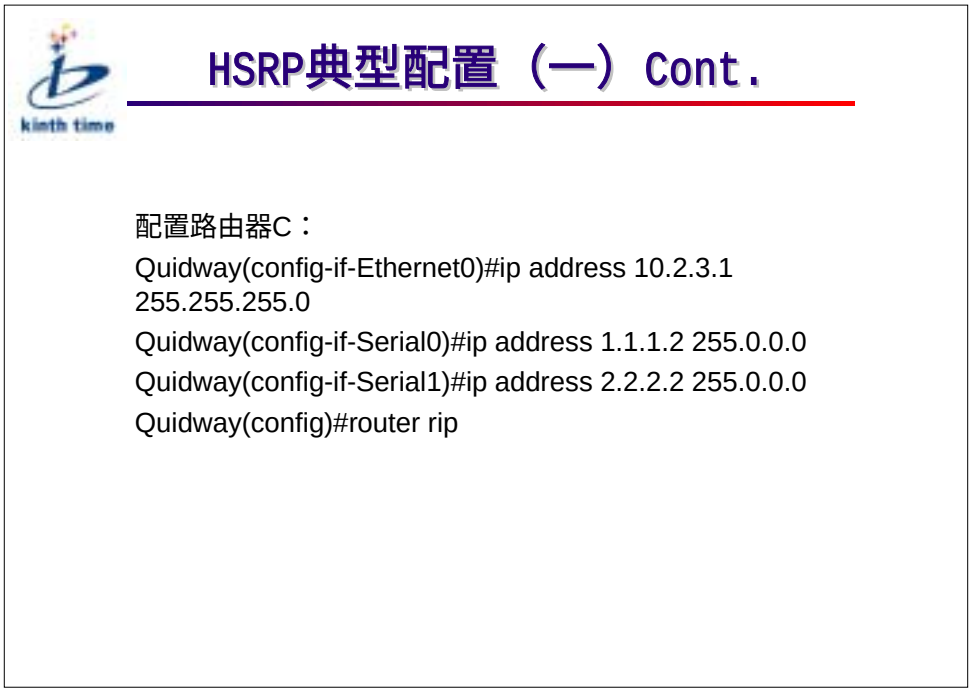
配置路由器A：

```
Quidway(config-if-Ethernet0)# standby  ip 202.38.160.111
Quidway(config-if-Ethernet0)# standby  preempt
Quidway(config-if-Ethernet0)# standby  priority 120
Quidway(config-if-Ethernet0)#ip address 202.38.160.1
255.255.255.0
Quidway(config-if-Serial0)#ip address 1.1.1.1 255.0.0.0
Quidway(config)#router rip
```

HSRP典型配置（一）Cont.

配置路由器B：

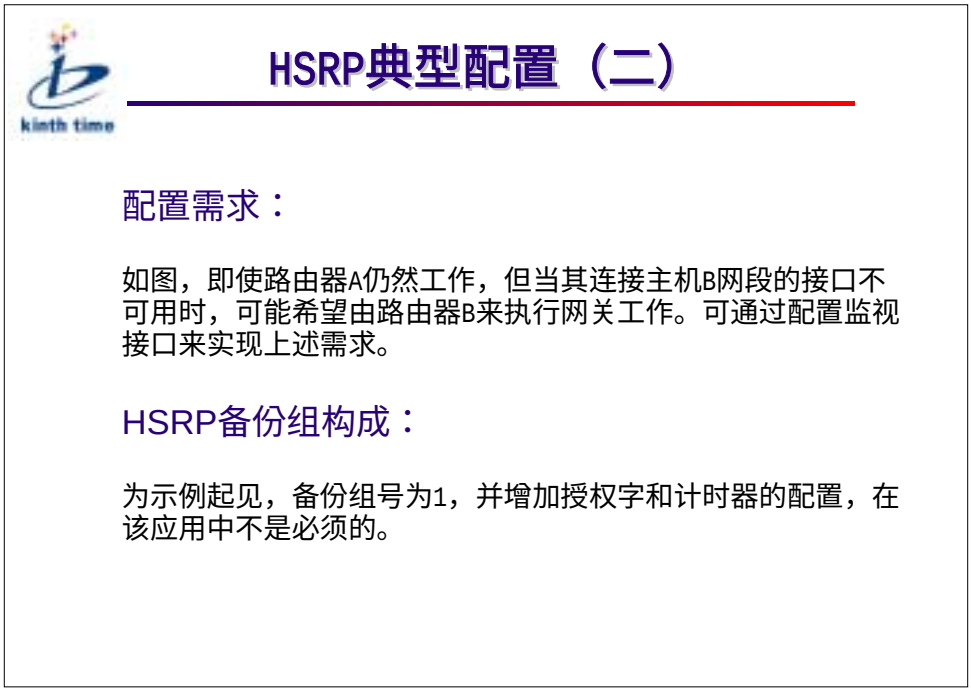
```
Quidway(config-if-Ethernet0)# standby  ip 202.38.160.111
Quidway(config-if-Ethernet0)# standby  preempt
Quidway(config-if-Ethernet0)#ip address 202.38.160.2
255.255.255.0
Quidway(config-if-Serial0)#ip address 2.2.2.1 255.0.0.0
Quidway(config)#router rip
```



配置说明：

备份组配置后不久，就可以使用。主机 A 可将缺省网关设为 202.38.160.111 。正常情况下，路由器 A 执行网关工作，当路由器 A 关机或出现故障，路由器 B 将接替执行网关工作。设置抢占方式，目的是当路由器 A 恢复工作后，能够继续成为活动路由器执行网关工作。

14.4.3.4 HSRP 典型配置（二）



配置需求二：
如上图， 即使路由器 A 仍然工作，但当其连接 Internet 的接口不可用时，可能希望由路由器 B 来执行网关工作。可通过配置监视接口来实现上述需求。
为示例起见，备份组号为 1，并增加授权字和计时器的配置，在该应用中不是必须的。

14.4.3.5　HSRP 典型配置（二）（续）

HSRP典型配置（二）Cont.

监视接口

配置路由器A：

```
Quidway(config-if-Ethernet0)# standby  1 ip 202.38.160.111
Quidway(config-if-Ethernet0)# standby  1 preempt
Quidway(config-if-Ethernet0)# standby  1 priority 120
Quidway(config-if-Ethernet0)# standby  1 authentication QUIDWAY
Quidway(config-if-Ethernet0)# standby  1 timers  5  15
Quidway(config-if-Ethernet0)# standby  1track  serial0  30
Quidway(config-if-Ethernet0)#ip address 202.38.160.1 255.255.255.0
Quidway(config-if-Serial0)#ip address 1.1.1.1 255.0.0.0
Quidway(config)#router rip
```

HSRP典型配置（二）Cont.

监视接口

配置路由器B：

```
Quidway(config-if-Ethernet0)# standby  1 ip 202.38.160.111
Quidway(config-if-Ethernet0)# standby  1 preempt
Quidway(config-if-Ethernet0)# standby  1 authentication QUIDWAY
Quidway(config-if-Ethernet0)# standby  1 timers  5  15
Quidway(config-if-Ethernet0)#ip address 202.38.160.2 255.255.255.0
Quidway(config-if-Serial0)#ip address 2.2.2.1 255.0.0.0
Quidway(config)#router rip
```

配置说明：

正常情况下，路由器 A 执行网关工作，当路由器 A 的接口 serial0 不可用时，路由器 A 的优先级降低 30，低于路由器 B 优先级，路由器 B 将抢占成为活动路由器执行网关工作。当路由器 A 的接口 serial0 恢复工作后，路由器 A 能够继续成为活动路由器执行网关工作。

14.4.3.6　HSRP 典型配置（三）

配置需求三：

Quidway 允许一台路由器为多个备份组作备份。

通过多备份组设置可以实现 Load Sharing。如路由器 A 作为备份组 1 的活动路由器，同时又兼职备份组 2 的备份路由器，而路由器 B 正相反，作为备份组 2 的活动路由器，并兼职备份组 1 的备份路由器。一部分主机使用备份组 1 作网关，另一部分主机使用备份组 2 作为网关。这样，可以达到分担数据流，而又相互备份的目的。

14.4.3.7 HSRP 典型配置（三）（续）

HSRP典型配置（三）Cont.

多备份组配置 (Load Sharing)

配置路由器A：

```
Quidway(config-if-Ethernet0)# standby  1 ip 202.38.160.111
Quidway(config-if-Ethernet0)# standby  1 preempt
Quidway(config-if-Ethernet0)# standby  1 priority 120
Quidway(config-if-Ethernet0)# standby  2 ip 202.38.160.112
Quidway(config-if-Ethernet0)# standby  2 preempt
Quidway(config-if-Ethernet0)#ip address 202.38.160.1 255.255.255.0
Quidway(config-if-Serial0)#ip address 1.1.1.1 255.0.0.0
Quidway(config)#router rip
```

HSRP典型配置（三）Cont.

多备份组配置 (Load Sharing)

配置路由器B：

```
Quidway(config-if-Ethernet0)# standby  1 ip 202.38.160.111
Quidway(config-if-Ethernet0)# standby  1 preempt
Quidway(config-if-Ethernet0)# standby  2 ip 202.38.160.112
Quidway(config-if-Ethernet0)# standby  2 preempt
Quidway(config-if-Ethernet0)# standby  2 priority 120
Quidway(config-if-Ethernet0)#ip address 202.38.160.2 255.255.255.0
Quidway(config-if-Serial0)#ip address 2.2.2.1 255.0.0.0
Quidway(config)#router rip
```

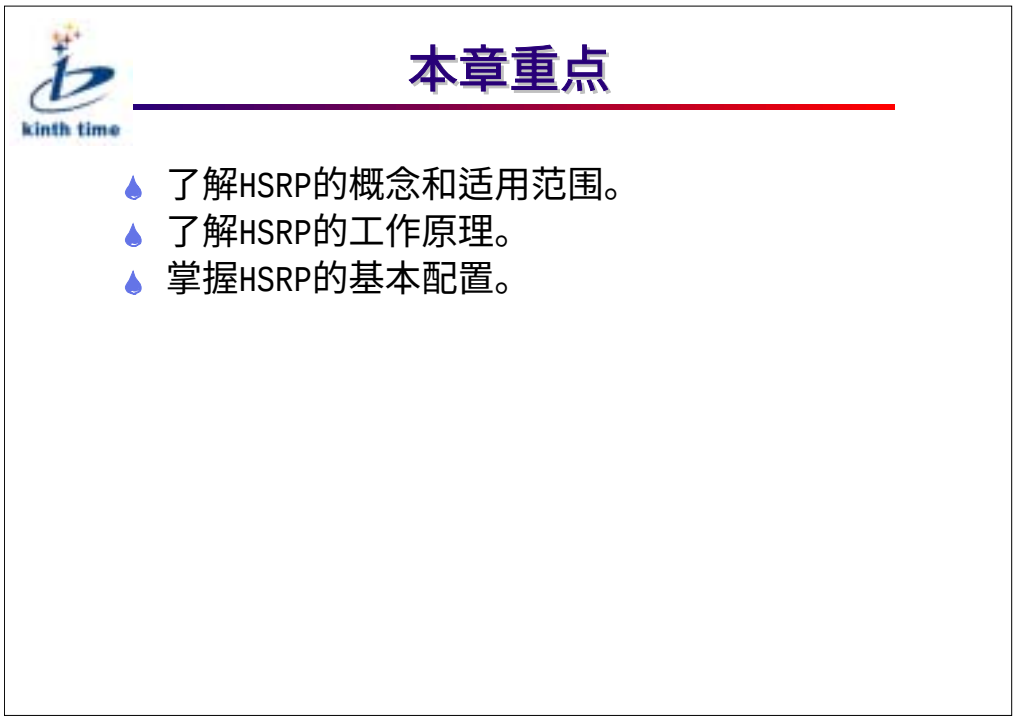
HSRP典型配置（三）Cont.

多备份组配置 (Load Sharing)

配置路由器C：

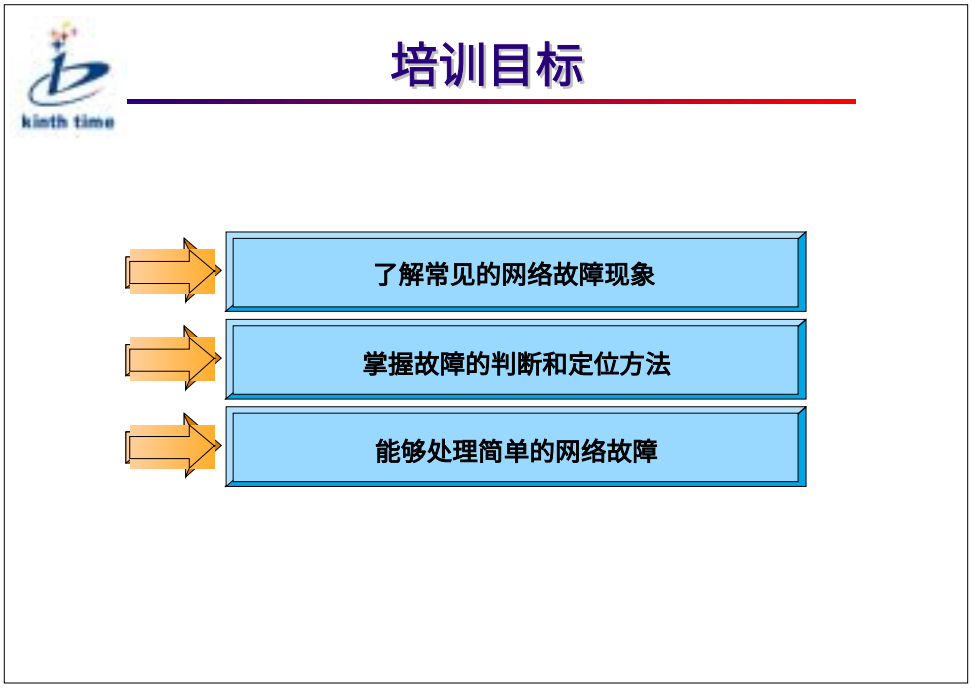
```
Quidway(config-if-Ethernet0)#ip address 10.2.3.1 255.255.255.0
Quidway(config-if-Serial0)#ip address 1.1.1.2 255.0.0.0
Quidway(config-if-Serial1)#ip address 2.2.2.2 255.0.0.0
Quidway(config)#router rip
```

.5 本章重点



第十四章　　常见网络问题分析及处理

.1　培训目标



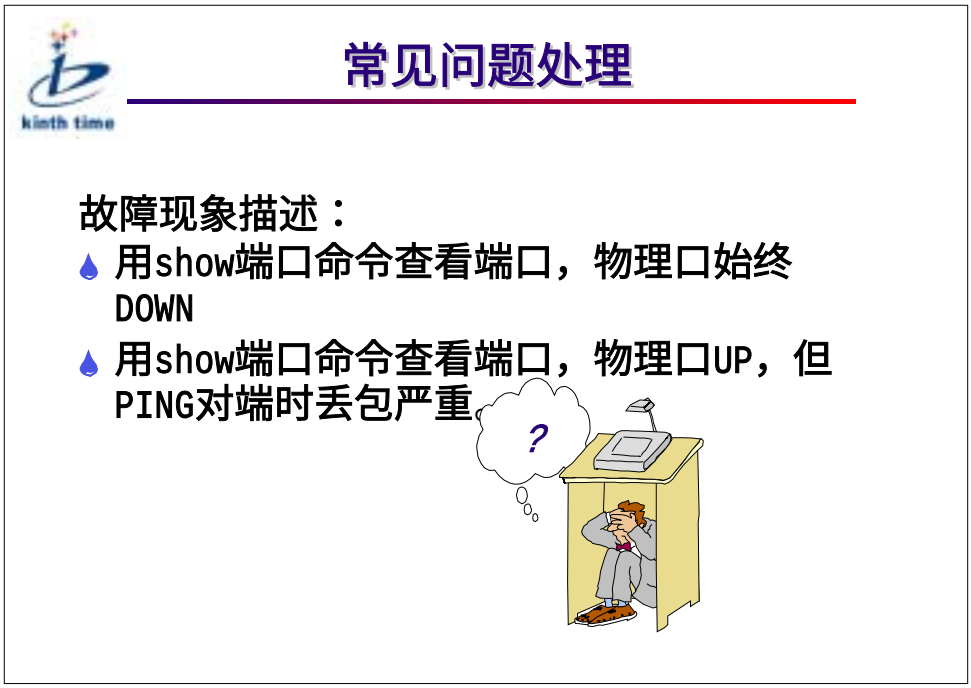
路由器是一种用于网络互连的专用计算机设备，工作在 OSI 参考模型的第三层（网络层），它的主要作用是为收到的报文寻找正确的路径，并把它们转发出去。

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）

在分析路由器运行中的故障时，我们应该遵循网络的层次，即物理层嗍荼绰凡汔网络层，将问题逐级定位。

.2　物理层问题



.2.1　故障分析定位

1. 端口 down　时有 2 种状态：

（1）端口（如 serial number） is administratively down，line protocol is down ：表示该接口被 shutdown 。

（2）端口（如 serial number ） is down, line protocol is down ：表示 端口没有被激活或物理层没有转为 up 状态。

2. 丢包严重是线路时钟问题，一般出在广域口专线上。

.2.2　故障解决过程

1.　端口 down：

（1）第一种情况是由于在端口上配置了 shutdown 命令，用 no　shutdown 命令取消即可；

（2）如是第二种情况，用 show 端口命令查看底层 DTR、DSR、 RTS、CTS、DCD 信号是否都 UP， 如不是，说明 DTE 与 DCE　间物理线路没连好，查一下连接电缆问题。 以上 5 个信号的含义分别是：

DTR：数据终端设备（DTE）准备好信号，输入信号。

DSR：数据终接设备（DCE）准备好信号，输出信号。

RTS：请求发送信号，输入信号。

CTS：清除发送信号，输出信号。

DCD：数据载波检测信号，输出信号。

Quidway 路由器默认设置要检测以上 5 个信号，其中 CTS、RTS 信号是关于异步串口流控检测的信号，即异步串口在发送数据时，自动检测 CTS 信号，有 CTS 信号正常发送，无 CTS 信号停止发送；我们可以通过在串口相关参数对此功能进行屏蔽，即：

Quidway(config-if-serial0)# flowcontrol normal

将异步串口的流控方式设置为 normal ，则串口在发送数据时，不检测 CTS 信号而直接发送，如果因此产生发送错误，系统将自动重发。

而 DTR、DSR、DCD 信号使能了串口的电平检测功能，即系统不仅检测串口是否外接电缆，同时要检测 DCD 信号，只有当该信号有效时，系统才认为串口处于 UP 状态。当该信号无效时，串口为 DOWN 状态，可通过以下命令可以屏蔽此功能，命令：

Quidway(config-if-serial0)# no detect dsr-dtr

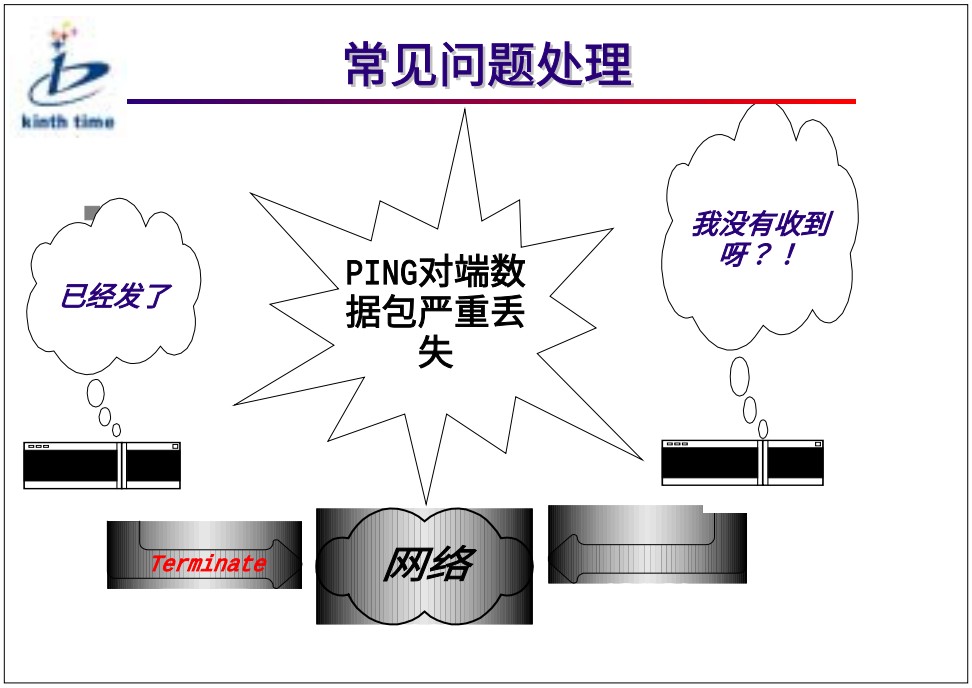
对于广域网口，路由器配有 V.24　和 V.35 等多种接口电缆，以及 DTE 和 DCE 的配置，确认路由器广域网口是在同步还是在 异步方式下工作，如果为异步方式，则检查波特率是否设置正确 ;如果为同步 DCE 方式，时钟由路由器产生，检查时钟速率和时钟方式是否正确；

对于以太网口，确认以太网连接是否正确，若使用 HUB 或 LAN Switch 连接以太网，确认 HUB 或 LAN Switch 上的指示灯显示测试机和路由器的以太网接口是否正常。10Base-T 标准规定有全双工和半双工两种工作方式。在使用共享式的 HUB 时，应该以半双工方式工作，使用交换式的 Switch 时，在 Switch 设置了全双工方式时，可以使用全双工方式工作。

2. 丢包严重：

可在两端相应连接专线的串口上翻转时钟，配置命令为 invert transmit-clock 。

.2.3　问题举例



☞ 问题 1：　两台 2501 专线连通后，互相 Ping 对端时丢报严重

☞ 分析：　丢报严重可能是线路上的时钟错位导致线路两端路由器收和发不能同步引起，在接口上将时钟翻转 invert transmit-clock 后相当于使时钟改变半个周期而使时钟对准。时钟不准并不是丢报严重的唯一原因，如果改变时钟后仍不能解决问题，且确认配置无误，则需要检查线路是否正常。

☞ 解决：可在两端相应连接专线的串口上翻转时钟，配置命令为 invert transmit-clock 。

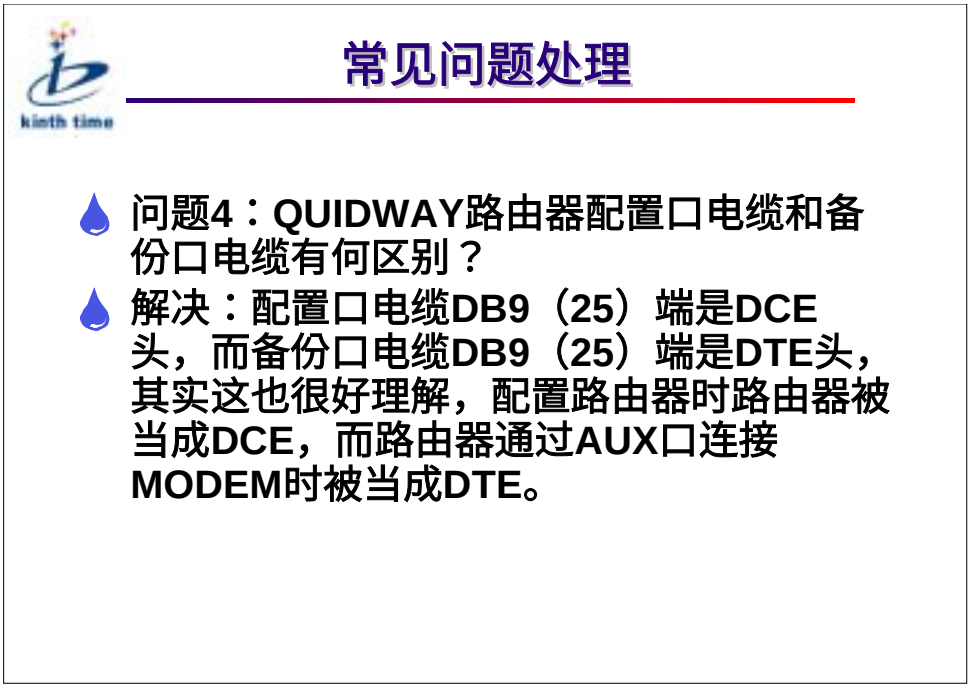
问题举例（续）


常见问题处理
问题2：在查看某路由器串口状态时发现物理口DOWN，且注意到以下几个信号状态是：
DCD=UP DTR=DOWN DSR=UP
RTS=DOWN CTS=UP 这是什么原因？
答：我们知道DTR、RTS信号都是从DTE（数据终端）一端发出的信号，所以可能是由于DTE设备没有接好，检查DTE设备是否连接正确，电缆、线路是否有问题。

问题举例（续）

问题 3：路由器指示灯的含义
解释：
POWER：电源指示。
SERIAL0（WAN1）：
同异步串口数据收发指示灯，有数据收发时闪，无收发时亮。
SERIAL1（WAN2）：
同异步串口数据收发指示灯，有数据收发时闪，无收发时亮。
DATA：
E1 口数据收发指示灯，有数据收发时闪，无收发时灭。
RLOS：
E1 口同步告警灯，不同步或无同步时亮或闪，同步正常时灭。
10Base-T（AUI)：
以太网口数据收发指示灯，有数据收发时闪，无收发时灭。
ACT：
ISDN BRI 口激活指示，快闪表示正在激活，慢闪表示未激活，亮表示已激活。
B0：
ISDNBRI 口 B0 道占用指示，闪表示试图占用 B0 道，亮表示 B0 道已占用，灭表示未占用。
B1：
ISDNBRI 口 B1 道占用指示，闪表示试图占用 B1 道，亮表示 B1 道已占用，灭表示未占用。

问题举例（续）


常见问题处理
问题4：QUIDWAY路由器配置口电缆和备份口电缆有何区别？
解决：配置口电缆DB9（25）端是DCE头，而备份口电缆DB9（25）端是DTE头，其实这也很好理解，配置路由器时路由器被当成DCE，而路由器通过AUX口连接MODEM时被当成DTE。

.3　链路层问题

常见问题处理

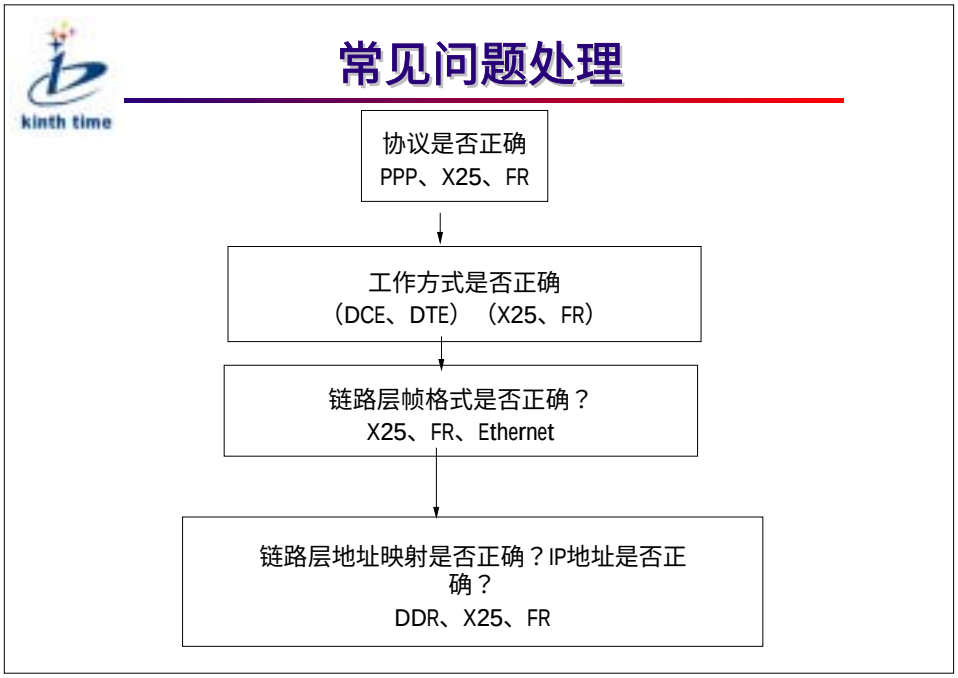
故障现象描述

- 1.用show 端口命令查看端口，物理口up，协议down。
- 2. 用show 端口命令查看端口，物理口up，协议up，但ping 不通对端。
- 3. 用show 端口命令查看端口，物理口up，协议up，但数据量大时丢包严重，此问题一般在以太口。

.3.1　故障分析定位

1. 端口（如 serial number ）　is up, line protocol is down　：表示该接口已激活，　但链路协商仍没有通过。
2. 链路层地址映射有误或工作方式有误。
3. 链路层帧格式有误。

故障判断流程：



.3.2　故障解决过程及实例分析

故障的定位需分别对照不同的链路协议解决。

1.　PPP 协议

（1）检查链路层协议是否正确设置，只有广域网两侧的路由器设置了相同的协议，才可以相互通信。

（2）如果使用 PPP 协议，并采用 PAP 或 CHAP 做口令认证时，需确认双方口令设置是否正确 ，当验证不正确时，打开 PPP 的调试开关：

```
# debug　　ppp　　packet
# mon
```

会看到 LCP 协商成功并转为 UP 状态后进行 PAP 或 CHAP 协商，然后 LCP 转为 Down 状态。

问题举例

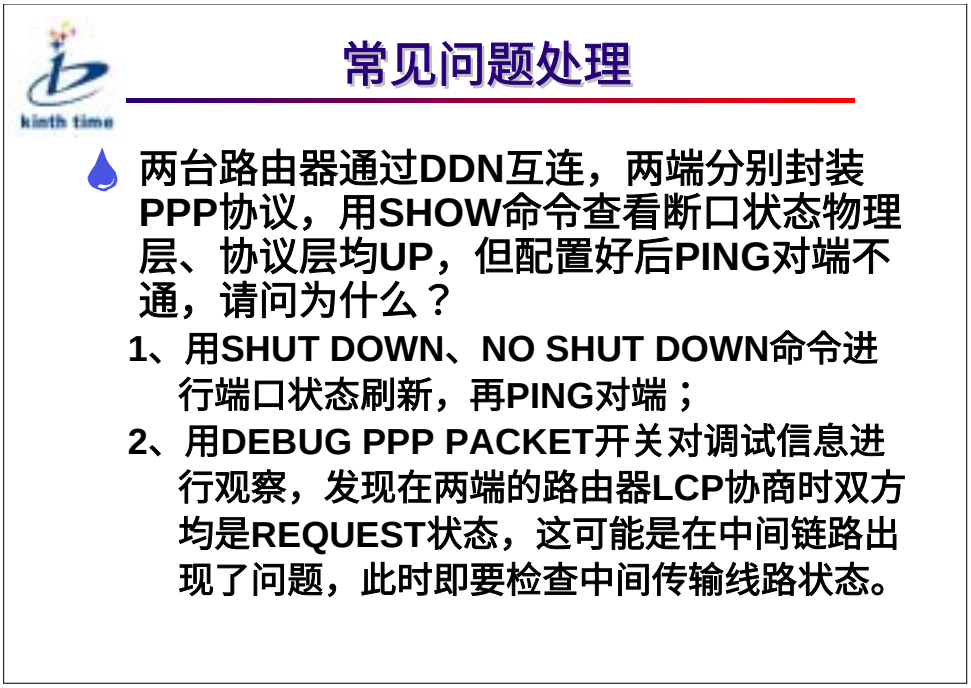
☞ 分析： Cisco 路由器的默认协议是 HDLC ，而华为的路由器默认协议为 PPP ， 用户使用华为路由器的时候，因为和 Cisco 的路由器相似，容易误认为 Cisco 也是 PPP 协议而没有改动 Cisco 的配置，当在 2501 上用 show in s N (N为串口号，0或1）命令时，会发现串口 up ，链路协议 down 。将 Quiaway 端协议改为 hdlc 即可。

☞ 解决：在相应端口下将 Quidway 端的协议封装改为 HDLC。

☞ 命令：enc hdlc

且将华为 2501 的广域网口地址设为和 Cisco 的广域网口地址 同一网段。

问题举例（续）



☞ 分析：PPP 协议属 ISO 二层协议，所以判断问题所在要从第一层起判断，用 show in s N（N 为所用串口）查看底层 DTR 、DSR、RTS、CTS、DCD 信号是否都 UP ， 如不是，说明 DTE 与 DCE 间物理线路没连好，查一下连接电缆问题，当串口提示 UP 且无错帧时，说明物理层正常。如物理层没问题，则用 show in s N 命令查一下 LCP，IPCP 是否 OPEN 如 LCP OPEN 而 IPCP INITIAL ，说明 PPP 验证没通过，查一下 PPP 验证的问题。

☞ 解决：以 PAP 为例。

验证方配置：

```
Quidway(config)#    user 169 password 0 169
Quidway(config-if-serial0)#    ppp authentication pap
```

被验证方配置：

```
Quidway(config-if-serial0)#    ppp pap send-username 169 password    0 169
```

验证中注意用户名和口令一致。

2. X.25 协议

（1）检查链路层协议是否正确设置，只有广域网两侧的路由器设置了相同的协议，才可以相互通信。当协议未配置对时端口提示 line protocol is down ；

（2）本地的工作方式配错了，例如，一个背靠背连接的两侧都是 DTE 或 DCE 。需改变封装的工作方式；在端口上：

Quidway(config-if-serial0)#encapsulation x25 dte 或

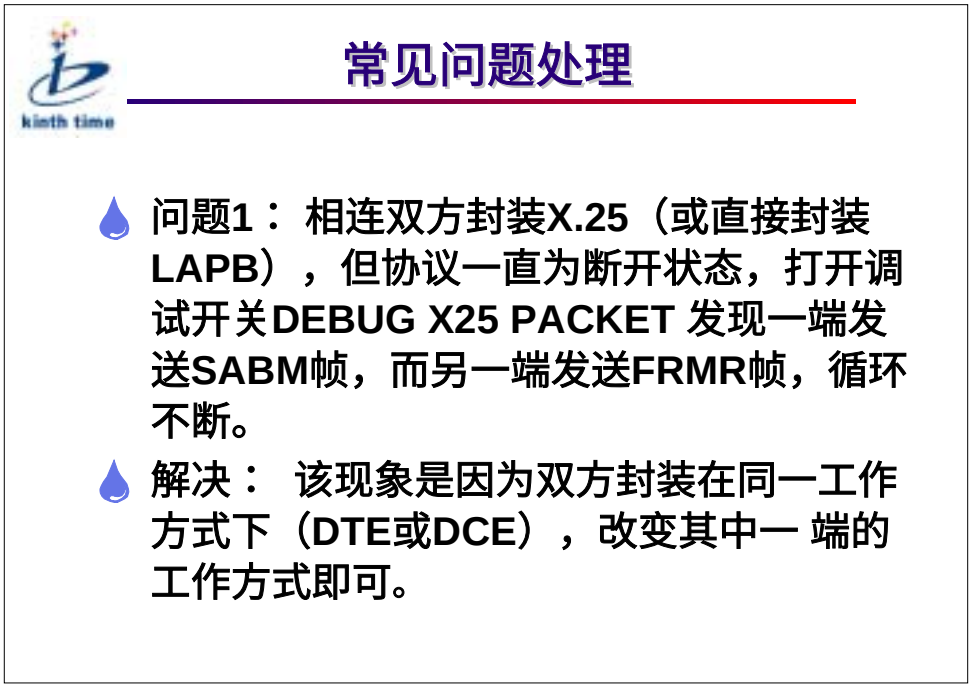
Quidway(config-if-serial0)#encapsulation x25 dce

（3）X.25 协议已经“UP”，但是却无法建立虚电路，即无法 Ping 通。这种情况有可能是下列原因之一造成的：

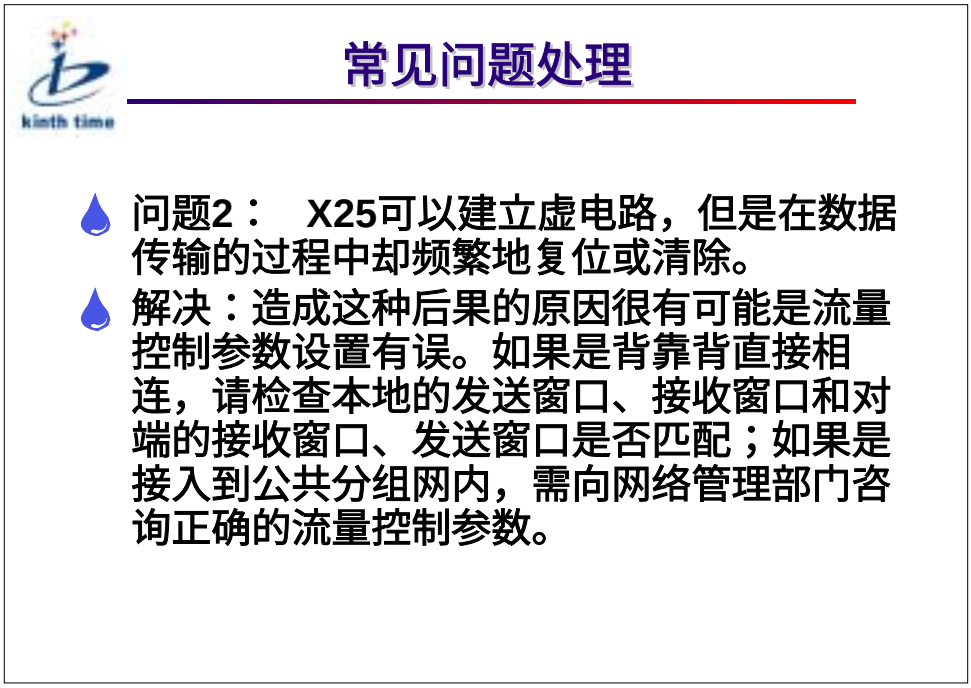
- 未配置本地 X.121 地址
- 未配置到对端的地址映射
- 未配置对端 X.121 地址
- 未配置对端到本地的地址映射
- 信道范围不正确
- 携带了网络不允许的设施选项。

注意：如果地址配置或映射不正确，只要修改为正确的配置即可；对于后两个原因，应该向网络管理部门咨询正确的信道范围和允许的设施选项。

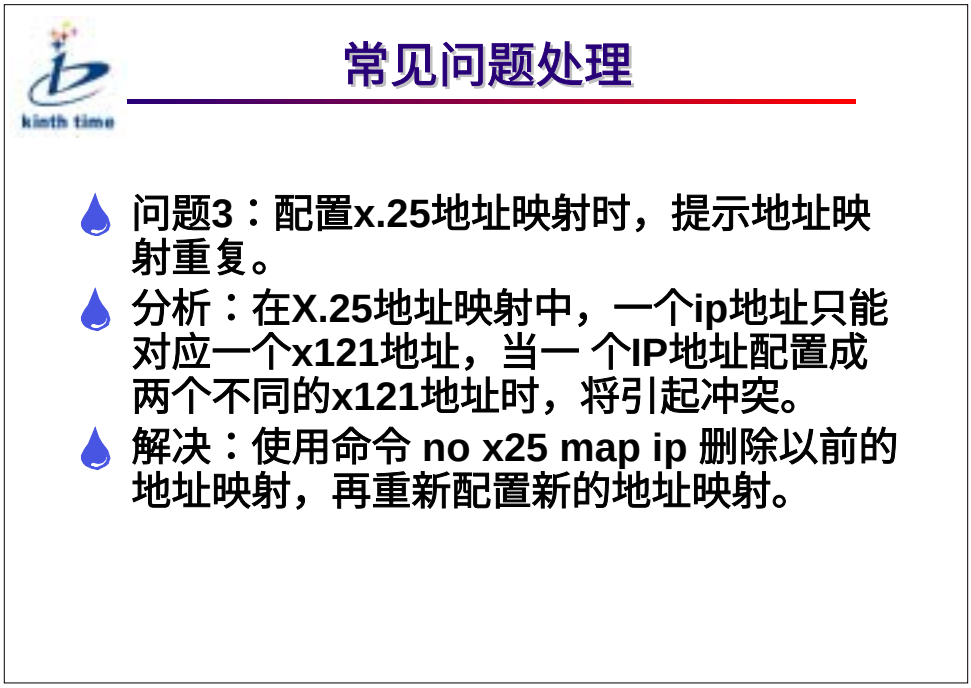
问题举例


常见问题处理
问题1： 相连双方封装X.25（或直接封装LAPB），但协议一直为断开状态，打开调试开关DEBUG X25 PACKET 发现一端发送SABM帧，而另一端发送FRMR帧，循环不断。
解决： 该现象是因为双方封装在同一工作方式下（DTE或DCE），改变其中一 端的工作方式即可。

问题举例（续）


常见问题处理
问题2：　X25可以建立虚电路，但是在数据传输的过程中却频繁地复位或清除。
解决：造成这种后果的原因很有可能是流量控制参数设置有误。如果是背靠背直接相连，请检查本地的发送窗口、接收窗口和对端的接收窗口、发送窗口是否匹配；如果是接入到公共分组网内，需向网络管理部门咨询正确的流量控制参数。

问题举例（续）



3. 帧中继协议

(1) 查看端口信息，当提示端口 up ，而 line protocol is down ，需检查：

A .检查两侧的路由器是否都设置相同的帧中继协议

B. 如果两台路由器直连，检查本地设备和对端设备是否配置成一端是帧

中继 DTE 接口，一端是帧中继 DCE 接口

C. 检查两端设备是否封装为相同的帧格式

D. 检查两端设备的本地管理信息类型（LMI）是否一致

E. 如果以上检查都已经通过，可以打开帧中继 LMI 消息的监视开关，是否是 Status Enquiry 消息与 Status 消息有一一对应关系。如果没有的话， 说明物理层数据收发不正确，需检查物理层的问题。打开帧中继 LMI 消　息的监视开关的命令请参见 debug frame-relay lmi 命令。

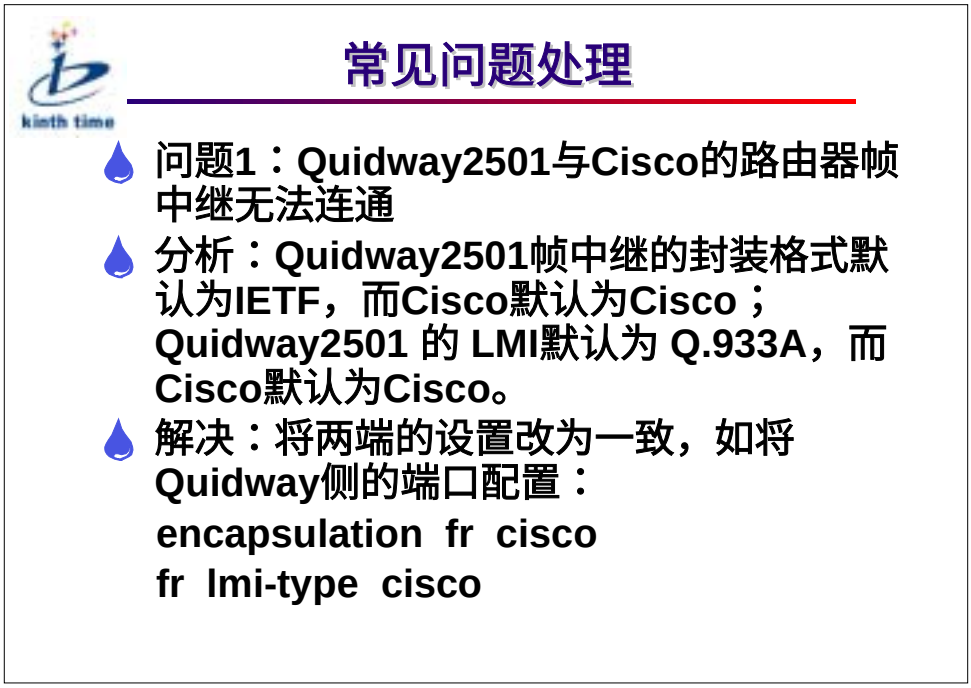
(2) 帧中继链路层协议处于 UP 状态，但不能 Ping 通对方。

A.检查两端设备的链路层协议是否都处于 UP 状态。

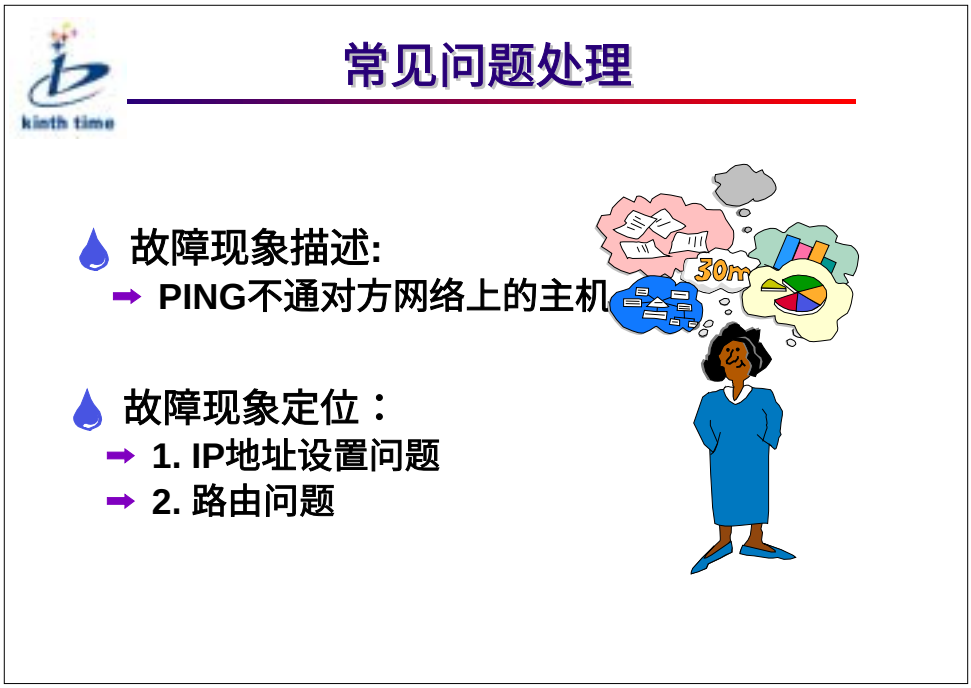
B.检查两端设备是否都为对端配置（或产生）了正确的地址映射。

C.检查路由表，是否有到达对端的路由。

问题举例


常见问题处理
问题1：Quidway2501与Cisco的路由器帧中继无法连通
分析：Quidway2501帧中继的封装格式默认为IETF，而Cisco默认为Cisco；Quidway2501 的 LMI默认为 Q.933A，而Cisco默认为Cisco。
解决：将两端的设置改为一致，如将Quidway侧的端口配置：
encapsulation fr cisco
fr lmi-type cisco

.4　网络层问题



.4.1　故障分析定位

路由器是网络互连设备，因而在给接口配置 IP 地址时，必须清楚组网需求和子网的划分。一般应遵循如下原则：
路由器以太网口 IP 地址必须与该以太网口所连的局域网在同一网段。
需分别对照不同的路由协议解决。
(1) 静态路由
☞ 用 show ip route static 命令查看是否正确配置相应静态路由。
☞ 用 show ip route 命令查看该静态路由是否已经生效。
(2) OSPF
如果物理连接和下层协议正常，检查在接口上配置的 OSPF 参数，必须保证与和该接口相邻的路由器的参数一致。这些参数包括 hellointerval、deadinterval 和 authentication 等。

☞ 检查在同一接口上 deadinterval 值应至少为 hellointerval 值的 4 倍。若网络的类型为 NBMA 或点到多点，则必须手工指定 neighbor 。配置命令为：

Quidway(config)# ip　ospf　neighbor　(对端 IP 地址)

☞ 若网络的类型为广播网或 NBMA ，至少有一个接口的 priority 应大于零。配置命令为：

Quidway(config)# ip　ospf　priority

☞ 同一网段的区域（area）号必须相同。

☞ 若配置了两个以上的区域，则至少有一个区域应配成骨干区域（即　area 号为 0 ）。

☞ 应保证骨干区域与所有的区域相连接。

☞ 虚连接不能穿越 stub 区域。

(3)　RIP

相应的接口上 RIP 没有运行（如执行了 no ip rip work　命令）或该接口被禁用（如执行 了相应 discard 命令）。

☞ 若网络的类型为 NBMA 或点到多点，则必须手工指定 neighbor 。在端口下的配置命令为：

Quidway (config-if-serial0)#　neighbor　(对端 IP 地址)

☞ 对端路由器上配置的是多播模式（如执行了 ip rip version 2 mcast 命令），但在本地路由器上没有配多播。

.4.2　问题举例

常见问题处理

- 问题：在配置防火墙时,配置如下命令：Access-list normal 102 permit udp any 202.38.160.1 0.0.0.0 neq rip时,发现在ip地址为202.38.160.1(掩码为3个255)的接口上仍然能够收到rip包。

☞ 分析：rip 报文是一种广播包,向外发送时，rip 包的目的地址是 ip 网段，而不是某一个具体的 ip 地址。

☞ 解决：将配置命令改为

Access-list normal 102 permit udp any 202.38.160.1　　0.0.0.255 neq rip

或改为

Access-list normal 102 permit udp any 202.38.160.255　0.0.0.0 neq rip

☞ 问题 2：在两个网络中分别使用了 RIP 和 OSPF 路由协议，在 OSPF 引入了 RIP 路由，却仍然无法引入 OSPF 和 RIP 之间的那台路由器靠近 RIP 这一端的接口上的地址，导致在使用 OSPF 路由协议的网络中的一些路由器无法 Ping 通该地址。

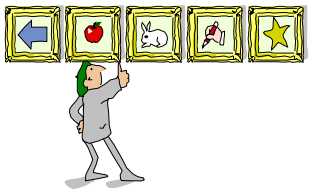
☞ 分析：由于在两个网络间的那台路由器里生成的路由表中关于该接口的 Protocol 是 direct ，而不是 RIP ,所以 OSPF 网络就不会广播该地址。

☞ 解决：在 OSPF 协议配置模式下,执行命令 Redistribute ospfase connected。使 OSPF 能引入直连路由。

问题举例（续）

常见问题处理

- **问题3：QUIDWAY 路由器与CISCO互通跑OSPF须注意哪些事项?**



☞ 分析：Cisco 路由器跑 OSPF 时,其 HELLO-INTERVAL 和 DEAD-INTERVAL 默认为 30 和 120，而华为路由器以太网口的默认值与之不同，分别为 10 和 40，另外，对应不同的协议，端口也许指定 OSPF 网络类型.。

☞ 解决：我司 Quidway 路由器与 Cisco 互通跑 OSPF 时，除了以前与我司自己路由器互通使的配置以外，有些设置需要注意：

（1）须将以太网口 DEAD INTERVAL 和 HELLO INTERVAL 做以下修改，改为与 Cisco 一致：

```
Quidway(config-if-Ethernet0)# ip ospf hello-interval 30
Quidway(config-if-Ethernet0)# ip ospf dead-interval 120
```

（2）.还须将 OSPF 网络类型改为：

A ：跑 X25 或帧中继时：

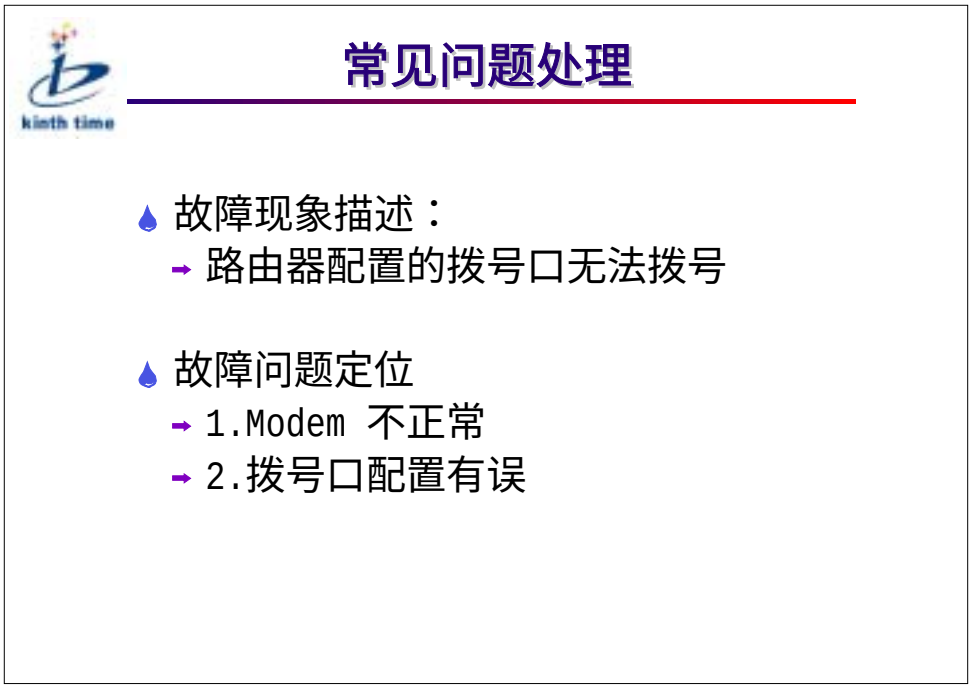
```
Quidway(config-if-Serial0)#ip ospf network-type nonbroadcast
```

B：跑 PPP 时：

Quidway(config-if-Serial0)#ip ospf network-type point-to-point

（3）用 show ip ospf 命令察看所有的端口的 OSPF 的 hello-interval 和 dead-inerval，看是否为 30 和 120 ；如不是则修改，方法与上同。

.5　DDR 问题



.5.1　故障分析定位

1. 检查与 Modem 连线是否正确和 Modem 的初始化是否正确。若 Modem 状态不正常，如长鸣不止或一直发出忙音。一般可通过在 Modem 连接的物理接口上执行 shutdown 和 no shutdown 命令而使其状态转为正常。若其状态仍不正常，可通过在 Modem 连接的物理端口上运行 AT 命令串使其状态转为正常， 如：

```
Quidway(config)#chat-script yaho "" AT&F OK ATE0S0=0&C1&D2
                                    OK AT&W
Quidway(config)#interface serial 0
Quidway(config-if-Serial0)#start-chat yaho
```

2. 拨号口配置有误时：

(1) 查看接口上是否配置了网络层地址

若在 Dialer 接口或直接使能 DDR 的物理接口上未配置网络层地址，则网络层在寻找路由时不会找到本拨号接口，从而 DDR 不能进行拨号。

(2) 查看 dialer-group 是否配置

在 Dialer 接口上或直接使能 DDR 的物理接口上必须配置 dialer-group ， 否则 DDR 将不处理从该拨号端口上发送和接收的数据包。

(3) 查看 dialer-list 是否正确配置

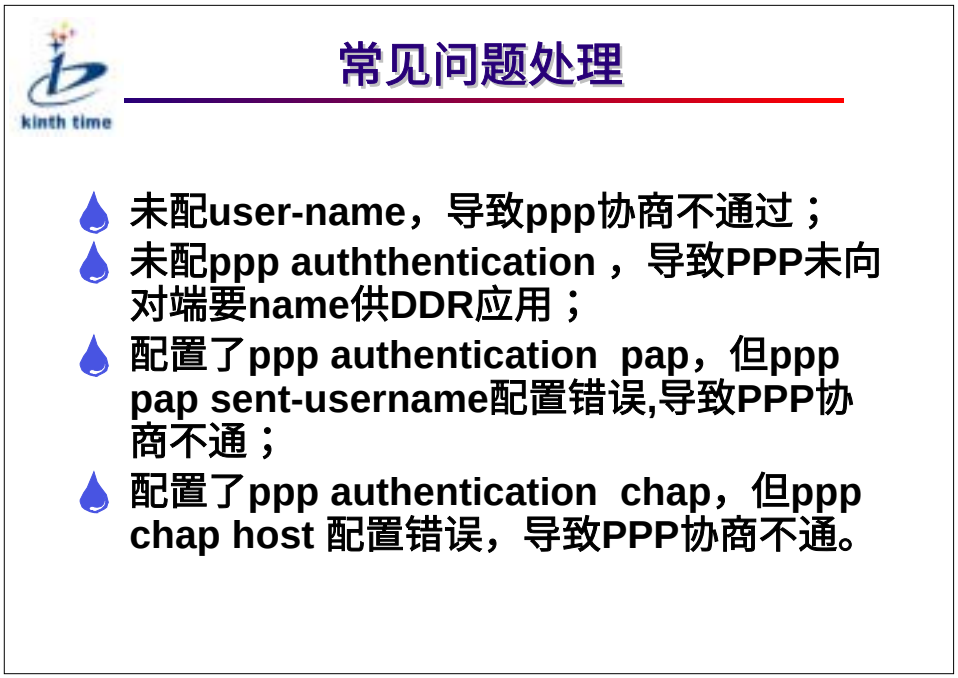
DDR 根据用户配置的 dialer-group 所对应的 dialer-list ， 确定一个发送至拨号接口的数据包是否进行拨号发送。数据包被分为两种，一种为 interesting 包即 通过访问控制，另一种为 uninteresting 包即没有通过访问控制。

当 DDR 端口收到一个 interesting 包后，如果相应的链路已经建立，DDR 通过此链路发出包，并清 idle-time 定时器。如果相应链路没有建立，则发起建立链路的呼叫。

当 DDR 端口收到一个 uninteresting 包后，如果相应的链路已经建立，DDR 通过此链路发出包，不清 idle-time 定时器。如果相应链路没有建立，不发出呼叫，丢弃此包。

(4) 查看 PPP 验证的有关配置是否正确

在灵活 DDR 配置方式下，若本端要求能够接收入呼叫，则在本端和对端必须配置 PPP 验证。若 PPP 验证配置错误或 PPP 协商而得的对端名字与 DDR 配置的 remote-name 不一致，则两端不能互通。PPP 验证配置错误可能为下面所列原因之一：



（5）查看同/异步串口是否正确地配置为异步模式，是否配置 Modem 。同/ 异步串口必须首先配置为异步口，并配置 Modem 配置命令，之后才可进行 DDR 配置。若在同/异步串口上 dialer 配置命令不可见，一般是因为该同/异步串口未配置为异步口。此时在该同/异步串口运行如下两条配置命令，可使 dialer 配置命令可见：

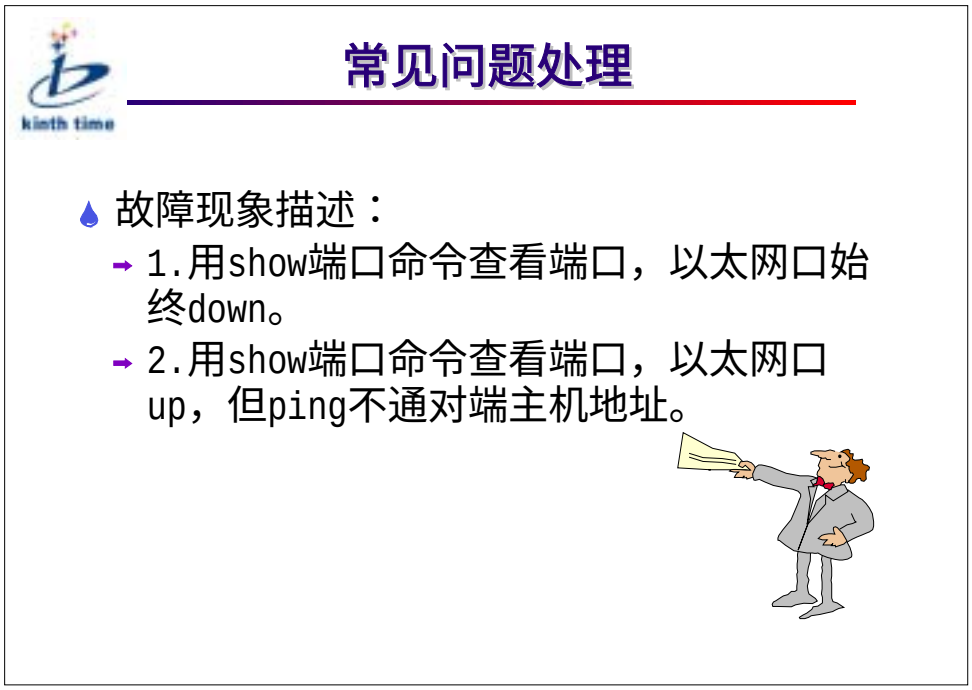
```
Quidway(config-if-Serial0)# physical-layer asynchronous
Quidway(config-if-Serial0)# modem
```

（6）查看同/异步串口是否挂至 Dialer 接口或直接使能 DDR 同/异步串口必须挂至 Dialer 接口或直接使能 DDR，才能应用于拨号连接。直接使能 DDR 的配置命令为 dialer in-band 。

.5.2　问题举例


常见问题处理
问题：Modem不拨号？
硬件原因
与Modem连线是否正确。
Modem的初始化是否正确。
软件原因
若端口是同/异步端口，没有设置为异步方式。
没有配置Modem inout命令。
没有使能DDR。
没有配置与数据包对应的dialer map或dialer string。
没有配置dialer-group命令。
数据包是uninteresting包。它不触发呼叫。可通过dialer-list命令将数据包设置为interesting包。

.6　以太网问题



.6.1　故障分析定位

- 没有配置以太网口的 IP 地址。
- IP 地址或以太网协议配置有误。

.6.2　故障解决过程

(1) 查看端口信息，当提示端口 down 时看是否配置了 IP 地址。
(2) Ping 不通以太网上的主机时，首先查看微机和路由器的以太网口 IP 地址是否位于同一子网内，即二者的网络地址必须是相同的，仅有主机地址不相同。如果不在同一子网，需重新设置 IP 地址。但地址已在同一网段时需查看协议是否匹配。目前以太网（ IP 网络）可以采用的协议标准有两种： Ethernet_II 或 Ethernet_SNAP。这两种协议具有不同的封装格式和最大传输单元（MTU），前者为 1500 字节，后者为 1492 字节。只有两台设备采用相同的协议时，这两台设备才能可靠地通信。Quidway 系列路由器可以同时接收这两种不同格式的数据，但发送的数据格式可以由用户指定 Ethernet_II 或 Ethernet_SNAP 中的任何一种，需确认路由　器的数据发送格式与以太网上其它微机是否相同。
在以太口上的配置如下：
send-frame-type Ethernet_II　或：send-frame-type　　Ethernet_SNAP

.6.3　问题举例

☞ 分析：以太网上的服务器未设网关，当报文从路由器转发给服务器后，服务器从报文中判断源地址不是本网地址，按协议规定应答报文应发给网关，但由于未设网关地址导致服务器无法响应做出回答，所以远程终端处因收不到报文而引起超时错误。加设网关后服务器可顺利回发应答报文完成 Ping 的协议过程。

☞ 解决：在服务器上的网络设置中，将网卡的 TCP/IP 属性中的网关指向 2509 路由器的以太网口。

.7　小结

综上所述，路由器的问题可以从以下几方面进行分析：
1、物理层问题的分析与解决
2、链路层问题的分析与解决
3、网络层问题的分析与解决
4、DDR 问题的分析与解决
5、以太网问题的分析与解决
重点学习分析问题的方法，能够解决简单的常见问题。