

# 国家信息化计算机教育认证项目

课程 CEAC-2203  
构建分布式网络  
(教 案)



**国家信息化培训认证管理办公室**

COMPUTER EDUCATION, AUTHORIZATION AND CERTIFICATION

## 目 录





## 课程介绍

- 为什么设计这门课
- 您将从中学到什么
- 学习后您可以达到

学习《分布式企业办公网络构建》课程后您希望达到

给自己拟定一个可行的计划

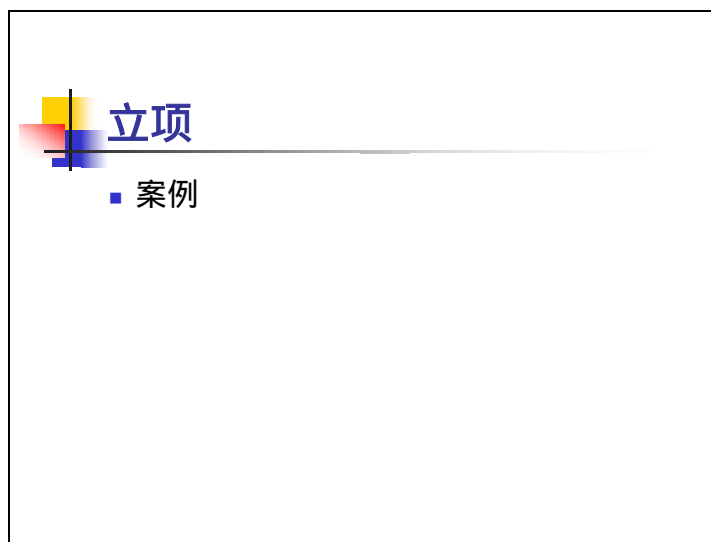


## 如何解决一个实际问题

- 立项
- 分析需求
- 项目拆分、计划
- 项目实施、测试

### 教学目标

明确解决实际问题的手段



## 教学目标

认知目标：熟悉案例。

能力目标：能够将工作中复杂的具体情况进行分析，抽象为一个项目。

## 教学准备

教师熟悉案例（详见学员手册），准备组织学员讨论。

## 教学过程

教师导入新内容：说明立项是我们解决一个实际问题的第一步。

学员阅读案例：空足够的时间让学员仔细阅读案例。

教师描述案例：这是一个实际的案例，教师在描述过程中应尽可能绘声绘色，使整件事情显得真实可靠，从而激发学员解决问题的主动性。

教师组织讨论：如果您是案例中公司的 IT 主管，您将如何处理这些问题？

学员讨论：教师要引导和控制讨论。

教师提问并且总结：实际工作中遇到的问题往往不够直观，而且很零散，我们先将这些问题抽象成为一个项目，然后按照分析需求、设计、实现的步骤合理解决。

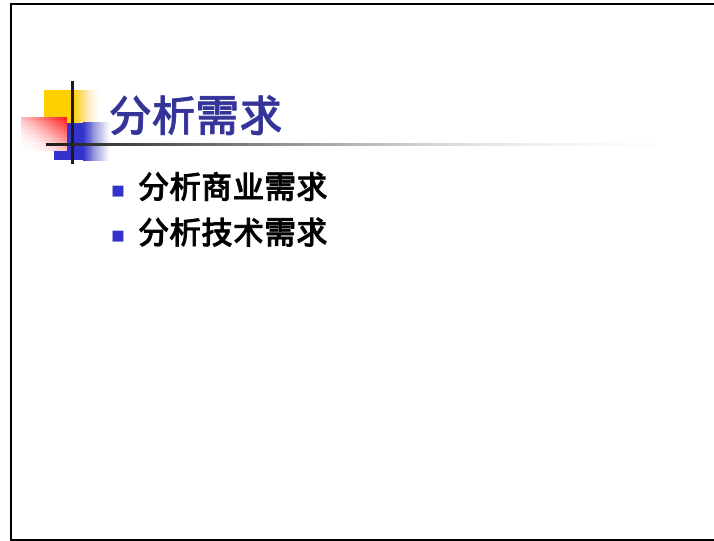
## 难点、重点分析

**难点：**学员初听到这样的问题会不知所措。（如果以前上过 CEAC-22 的课程会要一些）

**分析：**

学员中有的学习过前面的有关课程，有的没有，是直接来学习 CEAC-2203 的课程。所以，可能在遇到问题的时候还没有考虑过这一整套的解决方法。这里教师可以看学员的具体情况安排这段内容的详略。如果多数学员学习过前面的课程，那么可以简单总结；如果大部分学员都是直接来学习的这门课程，那么教师就需要明确提出解决问题的思路，并强调它的重要性。

解决问题的思路：分析商业需求、分析技术需求、设计、实现。



## 教学目标

明确需求分析要分为商业需求分析和技术需求分析两个阶段进行。

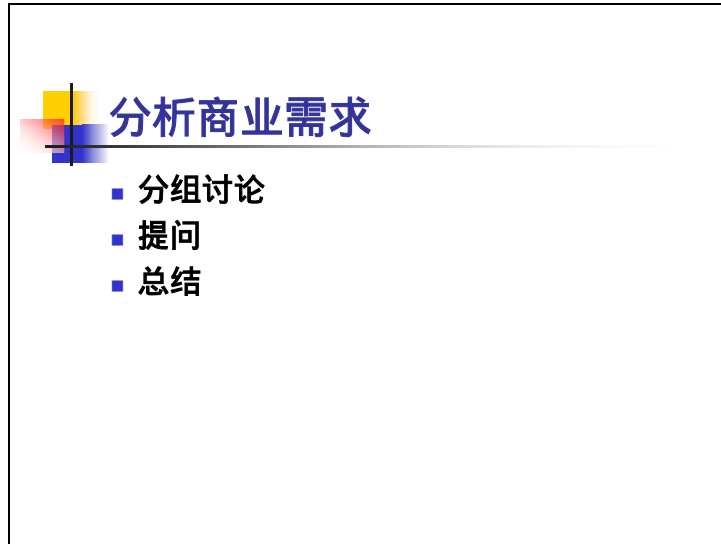
## 教学准备

## 教学过程

教师介绍需求分析分为商业需求分析和技术需求分析。

## 难点、重点分析





## 教学目标

认知目标：对案例进行商业需求分析

能力目标：让学员学会如何进行需求分析

## 教学准备

教师熟悉讨论内容（详见学员手册）

## 教学过程

教师导入新内容：强调商业需求的重要性，引导学员开始讨论

学员分组讨论：教师要对讨论过程进行控制

教师提问：一个小组作主要回答，其他小组补充

教师总结：明确案例中的商业需求（如果多数学员学习过前面的课程，教师总结的时候可以加上对比本案例和其他课程案例需求的不同。）

## 难点、重点分析

**难点：**学员讨论出需求后，接下来对其分类的讨论可能无法进行

**分析：**

学员基本上可以找出所有的需求，但接下来的归类工作可能会有困难，这里教师需要指导学员。

指导角度：提示学员可以从“一个用户对网络的请求”和“一个网络对另一个网络的请求”的角度来对这些需求分类。二者的区别主要是请求量的大小，如果请求量大就是网络对网络的请求，请求量小的就是一个用户对网络的请求。

**难点：学员讨论的控制：学员有可能不讨论，也可能讨论的时间太长**

**分析：**


教师一定要严格按照学员手册中的进度控制讨论。如果有的小组不讨论，教师可以尝试加入这个小组，了解问题产生的原因（刚认识，不熟，不愿意说话等），鼓励学员大胆发言。

**难点：讨论偏离方向，或者没有讨论得到所有的需求**

**分析：**教师可以给出需求分析表

需求	分类	技术手段
用户出差需要访问公司的网络	远程访问	
经理在家办公，访问公司的网络，要公司花话费	远程访问	
两个办公地点之间的访问	路由	
不同时间访问的许可不同	远程访问	
总体上的费用越少越好	远程访问和路由	
使用固定的电话访问公司的网络	远程访问	
大文件不允许传输	远程访问	
需要上传大文件	远程访问	
不同部门的用户的远程访问的需求是不一样的	远程访问	
控制用户进行远程访问连接后不使用的现象	远程访问	





## 分析技术需求

- 分析技术需求
- 介绍技术手段
  - 远程访问服务
  - 路由
  - 虚拟私有网络
  - 远程访问策略

## 教学目标

认知目标：了解各项商业需求的解决所对应的技术手段

## 教学准备

明确各项技术手段

## 教学过程

教师导入新内容：有了实际需求才会有相应的技术手段。

教师讲解：逐个分析需求，得到各项技术手段，然后重点讲解主要技术手段。

## 难点、重点分析

**难点：需求与技术手段的对应**

**分析：**

给出分析需求表：

需求	分类	技术手段
用户出差需要访问公司的网络	远程访问	RAS
经理在家办公，访问公司的网络，要公司花话费	远程访问	回拨

需求	分类	技术手段
两个办公地点之间的访问	路由	Routing
不同时间访问的许可不同	远程访问	远程访问策略
总体上的费用越少越好	远程访问和路由	VPN
使用固定的电话访问公司的网络	远程访问	远程访问策略；回拨
大文件不允许传输	远程访问	TTL
需要上传大文件		
	远程访问	MultiLink
不同部门的用户的远程访问的需求是不一样的	远程访问	group
控制用户进行远程访问连接后不使用的现象	远程访问	Idle

### 难点：各项技术手段的讲解深度难以掌握

#### 分析：

这里只需要介绍这些技术手段，给学员留一个整体印象，并不需要讲解具体内容，教师可能不好把握这个度。

建议先讲功能定义，再举例说明，然后稍加总结。

### 重点：远程访问服务

#### 分析：

功能定义：网络用来接受外部访问请求的技术。一个局域网络内部的访问我们已经清楚了，但是在实际的工作中需要用户在网络外部对局域网进行访问，这种访问需要专门的服务来接受，这种服务就是远程访问服务。

举例：信访办的例子：普通老百姓如果与政府打交道的过程中，如果出现了问题的话，那么老百姓可以写信上访。在每一级的政府部门都有信访办，专门就是用来接受群众的信访的。这个例子中信访办相当于是远程访问服务。

一座楼的门禁系统的例子：现代的小区中的每一座独立的楼都有自己的门禁系统。凡是本楼的用户都知道进门的密码，可以直接输入密码进楼，继而进入自己的家。不是本楼的人想要进入时，需要使用单元对讲系统，与想要访问的住户联系，获得许可后可以进入，否则不能进去。本例中的门禁系统相当于远程访问服务；大楼相当于局域网；每户人家相当于局域网中的计算机；外来的访客相当于是对网络进行远程访问的用户。

总结：远程访问服务就是网络用来接受外部访问请求的技术。

### 重点：路由

#### 分析：

功能定义：路由是选路的过程。两台计算机之间进行通讯，有多条路可以走，究竟走哪条路最近，哪条路最快，进行选择的过程就被称为路由。

举例：比如您要去火车站，可是不认识路，怎么办？您会去问在十字路口遇到的第一个交警：“火车站怎么走？”交警接到您的询问以后，会先想一下他知道不知道去火车站的路，如

果他知道的话，就会告诉您：“延着十字路口的这个口走，在下一个路口，您再去问那个路口的交通警。”（可能下课后会有学员问如果交通警察说不知道，会发生什么状况？教师可以反问学员如果是你，有人问你路，可以不知道，你会怎么办？如果是你问路，得到这样的结果，你会怎么办？去问下一个人）您会延着他告诉您的方向往前走，直到在下一个路口，遇到另一个警察，重复上面的过程，再去问他，直到走到火车站为止。上面这个问路的过程就是路由的过程。

总结：在网络之间进行路径选择的过程就是路由

### **重点：虚拟私有网络**

#### **分析：**

功能定义：VPN 就是对资源访问的方法。他就是把不同的局域网络通过公共网络安全的连接在一起，自由的交换数据，就好像是使用一根局域网的网线连接起来的一样，给人的感觉这种技术就像是在一个公共的网络之上建立了一个虚拟的专用网络，我们形象地称他为虚拟私有网络。

举例：比如现在的有线电视网络。如果你按时交纳有线电视费，那么你可以享受所有的服务，也就是看到所有的转播的节目，各种卫星电视都有；如果你不交纳费用，那么你能只能看到一些普通的节目，卫星电视节目不能够看到。在有线电视的网络中所有的信号都是同时传递的，但是有些信号是加密的，有些信号是不加密的，那些加密的信号构成了建立在有线电视信号的网络之上的一个虚拟的网络，可以使用这个网络中的资源的用户就是那些缴费的用户。

比如我们现在使用的电视网络，早期我们的电视网络都是公共网络，任何的电视台都可租用亚洲二号卫星发送自己的节目，任何用户都可以自由的接收这个网络中的所有电视信号。后来出现了有线电视，即希望只有付费的用户才可以看到一些更好的电视节目，这样有线电视台就租用亚洲二号卫星上的某个频道，在原有公共电视网络的基础之上建立自己的加密电视网络，在这个网络中只发送经过自己加密的电视节目。这样一来，只有就只是会费的用户才能看到加密的电视节目了。

总结：VPN 就是一种对网络资源进行访问的技术。

### **重点：远程访问策略**

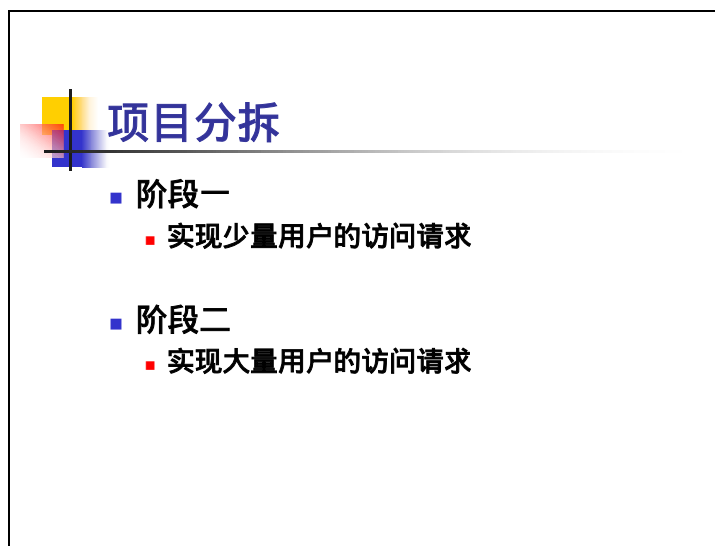
#### **分析：**

功能定义：远程访问策略是控制访问的手段。它可以控制什么样的用户在什么样的时间段内，以什么样的连接方式进行远程连接，这种连接的时间可以有多长等等。

策略包含了技术手段中提到的 TTL，GROUP，IDLE，MultiLink。

举例：比如大学里的实验楼内有很多不同的实验室：材料实验室、电机实验室、仪器仪表实验室等，对进入不同的实验室的学生的时间、着装、所属的系有不同的要求，这些要求以“实验室须知”的方式贴在相应的实验室门上，学生要想进入某一个实验室就必须符合这个须知上的要求，否则实验室的老师不会放他进去的。那么这个“实验室须知”就相当于是我们的远程访问策略。

总结：远程访问策略就是强制用户必须遵守的规则。



## 教学目标


让学员知道项目拆分的大阶段。

## 教学准备

## 教学过程

从用户访问量的角度可以把项目的实现分成两个大的阶段。

## 难点、重点分析



## 项目实施

- 实现少量用户的访问请求
  - 步骤一 实现普通用户的访问
  - 步骤二 完善用户的访问
  - 步骤三 控制用户的访问
- 实现大量用户的访问请求
  - 步骤一 连接两个办公地点
  - 步骤二 连接四个办公地点

## 教学目标

认知目标：明确每一阶段的实现过程

## 教学准备

教师先编写手册中要求的项目规划书。

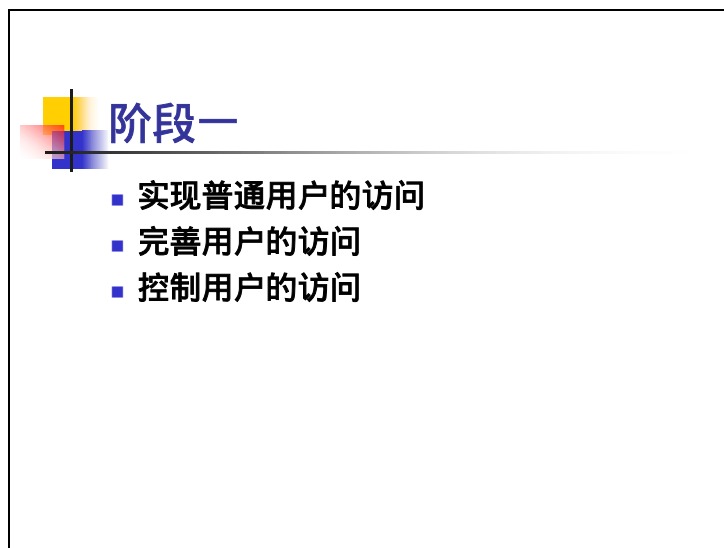
## 教学过程

教师导入新内容：

教师讲解各阶段实现的步骤，以及后面的课程安排。

## 难点、重点分析





## 教学目标

认知目标：明确阶段一的实现步骤。


能力目标：

## 教学准备

## 教学过程

教师讲解：                阶段一的实施步骤按这样三个阶段划分。

## 难点、重点分析



## 步骤一：实现普通用户的访问

- 分析需求
- 设计
- 实现

## 教学目标

认知目标：实现普通用户访问的技术手段是拨号远程访问。

## 教学准备

熟悉案例及其中的需求

## 教学过程

教师导入新内容：由案例引入我们这一阶段要实现的需求

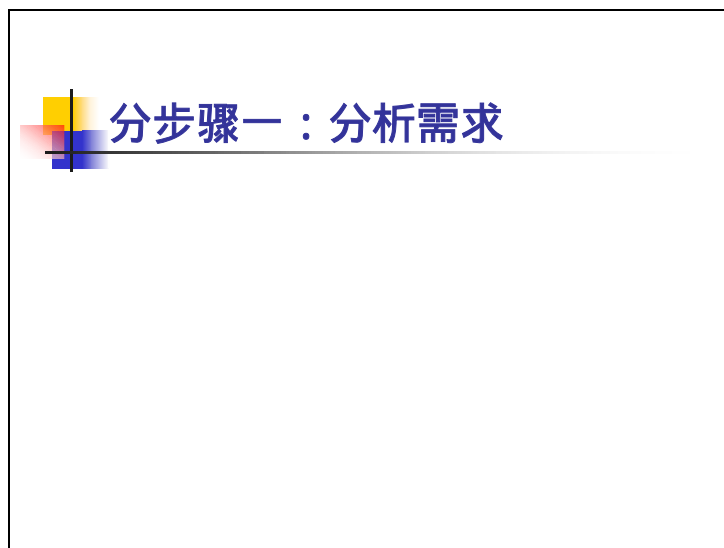
教师讲解：介绍远程访问服务。明确任何服务都需要计算机来提供，当前流行的方式是 C/S。

## 难点、重点分析

**难点：结合案例**

**分析：**

这里教师容易直接开始讲解相关知识，一定要结合案例。



## 教学目标

认知目标：结合案例进行步骤一的需求分析。

能力目标：


## 教学准备

教师准备实验、讨论：案例中需求分析的实验。

## 教学过程

教师组织讨论：完成手册上内容后，找一个小组发言，说说需求。

## 难点、重点分析



## 分步骤二：设计

- 知识准备：远程访问服务
- 专门设备的选择
- 客户端
- 服务器

### 教学目标


认知目标：明确普通用户的访问的设计步骤。

### 教学准备

### 教学过程

教师导入新内容：分析完需求后需要设计

### 难点、重点分析



## 知识准备：远程访问服务

- 什么是远程访问服务
- 如何启用服务
- 学习远程访问服务管理器的使用

## 教学目标

认知目标：建立 RRAS 的概念

## 教学准备

教师明确 RRAS 的概念

## 教学过程

教师导入新内容：前面已经简单介绍过了远程访问，主要的角度是从容易接受的地方出发，用生活中的例子帮助学员初步认识远程访问。现在我们要从做事情的角度出发，真正的来实现远程访问。因此这里的远程访问的介绍主要是从做事情的角度，加上相应的知识。

教师讲解实现过程：这里的讲课过程首先从做事情出发，要实现远程访问服务，我们首先需要从技术上认识远程访问，认识了远程访问如何使用呢？开始了远程访问服务的启用，启用之后如何进行管理呢？接下来是管理工具的学习，最后是来检查学习的效果。

## 难点、重点分析

这里我们还是要强调自我学习的重要性。尤其是我们这里的学习，一个单独的的服务的学习，可以在将来影响到我们对 Windows 2000 的其他服务的学习，所以这里我们一定要强调这一点。



## 教学目标

认知目标：建立 RRAS 服务器的概念

## 教学准备

教师明确 RRAS 服务器的概念

## 教学过程

教师导入新内容：

教师讲解：

首先从技术介绍中引出远程访问服务和路由服务，windows 2000 把它们组合在一起构成了 RRAS 服务；接下来有了服务的概念，那么服务器的概念随之可以得到建立；最后有了服务器就需要管理，如何进行呢？使用 RRAS 管理器

## 难点、重点分析

RRAS 服务：W2K 将 RAS 服务和 Routing 服务组合在一起，形成了 RRAS 服务。

RRAS 服务器：提供 RRAS 服务的计算机就是 RRAS 服务器。一个 RRAS 服务器既提供远程访问服务，同时又提供路由服务。

RRAS 管理器：在 RRAS 服务器上对 RRAS 服务进行管理的工具是 RRAS 管理器。RRAS 管理器即能管理远程访问服务，又能管理路由服务。



## 教学目标

能力目标：掌握启用 RRAS 服务

## 教学准备

教师准备实验（详见学员手册）

## 教学过程

教师导入新内容：

教师指导实验：

学员自学（详见学员手册）

教师总结：

## 难点、重点分析

**难点：**更多的学员喜欢使用向导中的提示直接启动

**分析：**

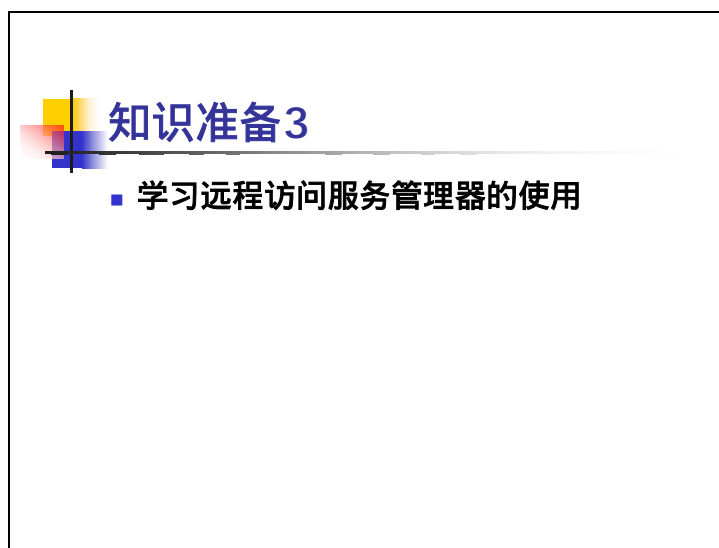
首先向导中的提示的内容，可以是教师讲解，也可以是让学员自己学习；其次引导学员考虑如果需要同时作向导中的两个不同的内容，那么怎么办？一定是使用向导中的提示没有办法做到的，这时候提出必须要选择“手动配置服务器”。他可以满足我们的各种需要，没有任何限制，并且对于像我们这样的职业管理员来说，一般是从来都不用向导的那种人。最后，提出

有个别的时候使用向导启动服务会发生一些莫名奇妙的事情，如果我们不想遇到的话，也使用手动配置。

#### **教师判断学员如何启用服务的方法**

这里对于教师还有一个要求：必须能够判断出学员当前的服务状态是用那种方式启动的，发现后立即禁用服务，重新用正确的方法启动。比如使用向导中的 VPN 启用的服务，那么在看学员的 RRAS 管理器时，可以发现端口中 PPTP 和 L2TP 的端口各有 128 个，其他的情况需要继续挖掘。





## 教学目标

能力目标：掌握使用 RRAS 管理器

## 教学准备

教师准备实验（详见学员手册）

学员手册中 Check List：IP 地址池；接口；端口；路由；策略；日志；远程访问客户端；RAS/ROUTER；Enable Routing

## 教学过程

教师导入新内容

教师指导实验：

学员自学：按照手册学习管理器的使用

教师总结：提问。

## 难点、重点分析

## 提问

### 根据手册中问题提问

教师设计问题：

日志

远程访问的客户端

接口

路由

策略

为什么用 IP 地址池？

为什么要使用端口？

此处 Routing 的作用？

### 总结的过程

教师提问日志、远程访问的客户端

教师总结并补充内容（因后面的课程中不在讲解与此相关的内容）

教师提问接口；路由；策略，学员了解到了哪些

教师提问 IP 地址池和端口和 Enable Routing，并深入讲解。

教师总结：

### 重点：IP 地址池

分析：

网络中主机都是用 TCP/IP 协议在通讯，TCP/IP 协议要通讯必须要具备 IP 地址，IP 池就是一段预留给远程访问客户的地址空间。

### 重点：端口

分析：

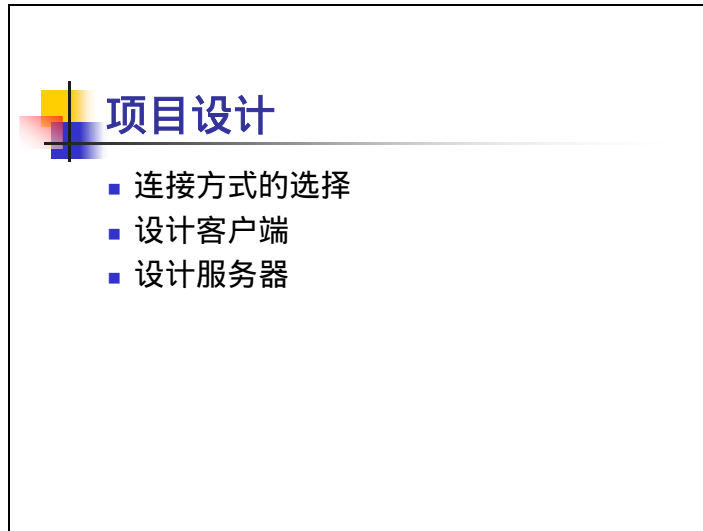
先提问学员为什么要使用端口，学员可能会回答不出来，（老师可以启发的再提另外一个问题，在 CEAC 的课程里是不是曾经用过端口，如果有人说的有的话，那么告诉他这两个端口是不同的。）老师先给端口下一个定义：是远程访问请求进出远程访问服务器的大门。比如：你站在一堵墙的外面，想知道墙里面的人在干什么，你会怎么办？你可以用大锤在墙上砸一个洞，你通过这个洞就可以看到墙里面的人在做什么，反过来，墙里面的人也可以通过这个洞看到墙外的人在做什么，但是在同一个时刻里，只能有一个人使用这个洞来看对方，如果同时看的话，则看到的是对方的眼睛，这是没有意义的，因此我们说，在同一个时刻里，只能有一个人使用这个洞。我们在这里所说的洞就相当于端口，端口是有方向的。即可以用来接收远程请求，也可以用来发送远程请求。但是在某一个时刻，端口只能有一个方向。

### 重点：Enable Routing

分析：

提问学员此处的 Routing 的作用。这不是一个很难回答的问题，只要学员按照试验手册中

的要求进行了学习就可以回答。此处的 Routing 的作用主要是设置远程访问的客户端对于远程服务器所在的局域网络的访问。如果选中了复选框，那么表示远程访问的用户可以在访问远程访问服务器的同时，也可以访问远程访问服务器所在的局域网络。反之，只能访问远程访问服务器，而不能访问其他的任何计算机。缺省情况下是选中的，如果公司的网络对于安全性要求比较高，只允许访问远程访问服务器，不允许访问局域网络，所有需要访问的内容统统复制到远程访问服务器上一份，这样即使有黑客攻击了远程访问服务器，也不会影响到后面的局域网络，这种情况下需要清空这个选项。



## 教学目标

认知目标：进行项目的设计。

能力目标：

## 教学准备

准备手册上的设计。

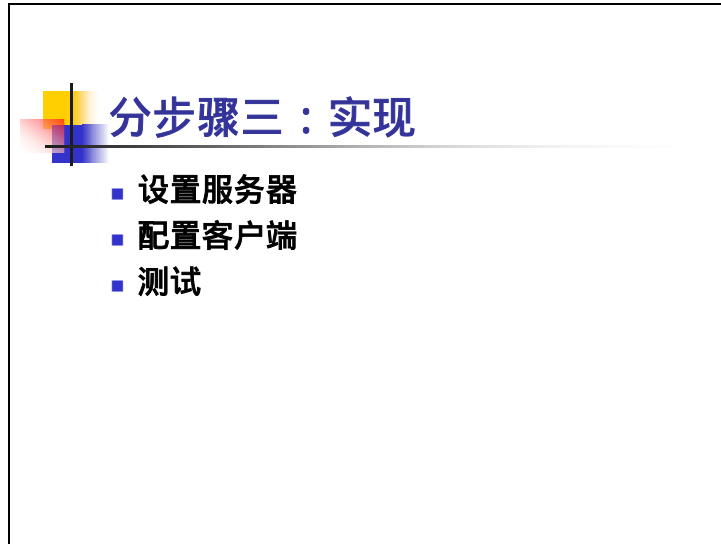
## 教学过程

教师导入新内容：知识准备完成了，下面该思考如何根据掌握的知识对系统进行设计了？

学员完成：手册上设计的内容。

教师讲评：各组讲评设计，教师总结设计。

## 难点、重点分析



## 教学目标

认知目标：实现案例中要求。

能力目标：

## 教学准备

教师准备实验、讨论：准备学员手册中实验。

## 教学过程

教师导入新内容：设计完了要实现，按前面设计内容实现

教师指导实验：完成手册中项目实现的内容

教师总结：总结实现过程中的问题。

## 难点、重点分析

**难点：**实现内容较长教师要对整个过程进行控制。

这个实现内容涉及较多，教师要对整个的过程进行控制，要要注意学员的进度，留意各个小组进行到了什么阶段。注意控制不要让他们研究与课程无关的内容。后面的实现中的一些问题进行了阐述。

**难点：**安装 Modem

导入新内容：首先物理连接是一切远程访问的基础，任何时候准备远程访问都要先准备物理连接；其次物理连接有很多种选择，性能价格比也不同，适应的企业也不同，要具体情况具体分析；

教师讲解：选择 MODEM 设备

教师讲解、指导实验：最简单的物理设备的安装：MODEM。其他设备的安装一般都有专门的人负责，并且也不复杂。

学员实验：

教师总结：解决安装中可能出现的问题

### **配置拨号客户端**

教师导入新内容：这一段内容主要就是远程访问客户端的配置。前面的服务器已经配置完成，可以配置与客户有关的内容了。

教师讲解配置过程：首先配置用户的远程访问许可，只有有了许可才能够进行远程访问；其次是配置客户端，远程访问需要专门的客户端启用他。这些都做完了之后，就可以进行远程访问了，进行远程访问的测试。

### **配置用户允许接入的老 PPT**

学员在这一部分的学习可能会发现一些比较多的深入的内容，集中出现在用户的拨入属性中，静态的 IP 地址，静态的路由，（学员可能会问为什么这里我还要再设置地址，路由）等等。对于这些问题，教师可以回答，也可以不回答，让学员再去读取帮助。最简单的回答就是这里的优先级最高。

### 配置拨号客户端的老 PPT

一个拨号连接的属性页中的内容比较丰富，可能会有学员自学，也可能不学，那么教师应该倡导学员多看多想，可能会给将来问题的解决带来线索。

还是这个拨号连接的属性页中的域名的复选框，什么时候使用该选项，教师可以作为试验做得比较快的学员的提问的问题。有学员比较快地完成实验之后，教师看到他无所事事，那么过去问他这个问题，看看是不是可以回答得出来。当然对于这一点，这种方式并不是最好的提问方式。最好的方法是教师一步一步的引出整个问题：从拨号连接需要用户帐户说起，用户帐户的信息总要存在什么地方吧，在 Windows2000 中有两个地方可以存储：SAM 和 AD，接下来究竟用户帐户的信息存储在什么地方了呢？取决于远程访问服务器究竟是一台成员服务器，还是一台域控制器。如果是成员服务器，两种存储帐户信息的地方都可能有，如果是域控制器，那么只有一种。如果有两种了，怎么办？如何清楚地告诉远程访问服务器现在的帐户信息存储在什么地方呢？就需要使用这里的域名的复选框。

### 测试

如果测试成功，说明 RAS 服务器和客户机的设置都是正确的。我们实现了案例中所描述公司一个办公地点的用户对另一个办公地点的局域网中的资源的远程访问。

如果测试失败，分析原因，并及时排错。

虽然远程访问需求已经实现，但在费用、控制方面是否存在缺陷？

### 难点：学员可能不明白自己的第二个地址

#### 分析：

通过检查自己的 IP 地址，学员看到自己的 IP 地址已经增加了一个新的，很多人在这时候可能不了解是什么原因。教师在这里一定要结合前面我们讲过的知识，帮助学员理解这里的现象，否则前面的学习就将半途而废。

在没有进行远程访问连接以前，学员已经认识到不进行远程访问连接是不可能访问到另外一个小组中的计算机的。很明显两台计算机不在同一个 IP 地址段，并且没有路由器做连接。在进行了远程访问连接之后，两台计算机可以进行访问了。

我们在讲解远程访问服务器的配置的时候，提出远程访问服务器必须配置 IP 地址的分配方案，我们在那里提出任何一个远程访问用户都需要一个局域网通讯协议（这里我们是 TCP/IP）与远程访问服务器，及其后面的局域网络进行访问。这种情况下我们可以把远程访问的用户看成是局域网络的外延，我们新获得的 IP 地址就是由远程访问服务器分配的，给局域网通讯协议使用的。局域网通讯协议是进行远程访问时不可缺少的。两台计算机之间的广域网通讯协议的连接建立之后，就开始局域网通讯协议的连接过程。在这个过程的最开始，就是局域网协议的通讯前的准备工作，也就是我们这里看到的 IP 地址的由来（当然其他的局域网通讯协议也有类似的内容：比如 IPX/SPX，NetBEUI）。

### **查看远程访问用户的老 PPT**

教师提问导入实验：管理员是不是应该提供更多的服务给用户使用；没有管理的网络是否可以存在

学员实验

教师总结：现有的控制手段有哪些。

### **难点：教师可能不理解提问的意义**

**分析：**

一个网络管理员按照我们前面的设置，配置完了一个远程访问服务器之后，就已经可以成功的接受用户的访问了。能够让我们的用户享受能够提供的服务，是网络管理员应该做的，在大部分情况下，可能也是主要的。充分的挖掘网络的功能，让网络发挥最大的作用是网络管理员日常的工作。

但是与此同时，网络管理员还有一个很重要的工作，就是管理网络，也就是说网络中的一切行为都应该在网络管理员的控制之下。现在我们设置了远程访问服务器，用户已经可以进行远程访问了，那么是不是谁都可以进行远程访问呢？是不是知道了我们的远程访问服务器的电话号码的人都可以访问呢？当然不可以。我们一定要控制。那么现在我们可以做的控制有哪些呢？

用户帐户的远程访问许可的设置

电话号码只有有限的人知道

服务器上可以检查什么人已经在进行远程访问





## 教学目标

认知目标：深入理解拨号远程访问

## 教学准备

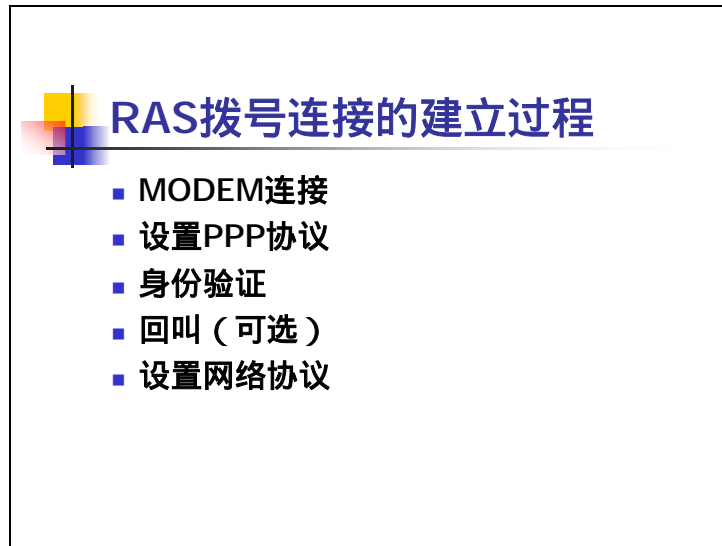
教师掌握 RAS 拨号连接的建立过程和远程访问的原理。

## 教学过程

教师总结远程访问的实现过程，包括设置服务器，设置客户端，建立连接，最后测试；

教师从理论的角度来讲解拨号远程访问的过程，这个过程与局域网内计算机之间建立访问的不同之处在什么地方；

教师讲解：再深入一步，包括网络底层的连接是如何建立的，网络上的应用始终是不变的。



## 教学目标

认知目标：从理论角度理解拨号的过程

## 教学准备

教师掌握 RAS 拨号连接的建立过程

## 教学过程

教师讲解 RAS 拨号的连接建立的过程，然后把整个过程与实际情况对应起来。

## 难点、重点分析

**难点：拨号连接的过程不能清楚地描述**

**分析：**

1. 远程访问客户机通过 MODEM 对远程访问服务器进行拨号。MODEM 收到用户的拨号请求以后,开始初始化并向远程访问服务器拨号,如果拨通了的话,则两个 MODEM 建立握手,两个硬件设备之间开始进行会话协商,如连接时的速率等。
2. 然后进行 PPP 协议的设置。设置包括:PPP 参数的协商、使用哪种身份验证协议对远程访问的客户进行身份验证、MultiLink 的设置等。
3. 接下来使用上一步 PPP 协议设置中指定的身份验证协议对远程访问的客户进行身份验证。

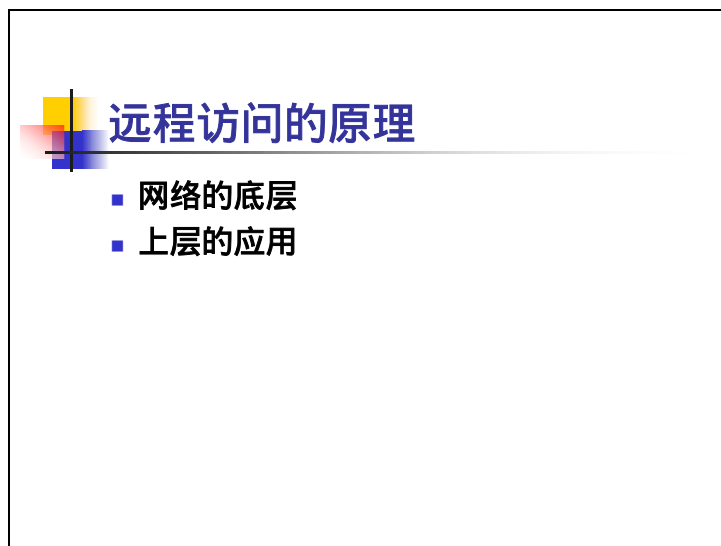
4. PPP 协议中包括了一个可选的回叫步骤。在验证成功后,使用回叫控制对 PPP 协议的回叫选项进行设置。
5. 在 PPP 设置和回叫(可选)设置以后,进行网络协议设置。如 TCP/IP 需要设置 IP 地址,IPX 或 NetBEUI 需要设置各自相应的参数。

**难点：不能把拨号的过程与局域网连接的过程很好的比较**

**分析：**

不能很好的比较的根本原因在于不能够把拨号连接与局域网连接进行很好的对应。主要是 PPP 协议工作的位置。拨号连接中的电话线和局域网中的网线相同,工作在同一层;拨号连接中的调制解调器和局域网中的网卡一样,工作在同一层;拨号连接的 PPP 和局域网中的 Ethernet 一样,工作在同一层。局域网中的计算机之间进行通讯,发送方会在数据的前面加上 Ethernet 的包头,通过局域网的网卡发送出去,接受方从局域网的网卡收下来后会去掉 Ethernet 的包头,察看其中的数据。通过拨号连接的计算机之间进行通讯,发送方会在数据的前面加上 PPP 的包头,通过调制解调器发送出去,接受方从调制解调器收下来后会去掉 PPP 的包头,察看其中的数据。

举一个例子来说明这两件事情：比如我现在要给洛杉矶快递一箱西红柿。我打电话通知快递公司,快递公司上门取货,在箱子上贴上标签：北京市海淀区学院路 229 号到洛杉矶克林顿大街 51 号。不可能快递公司开着上门取货的车直接把西红柿送到洛杉矶,一看上面的标签就知道应该首先送到首都机场。首都机场看到这箱西红柿后,贴上一个新的标签：北京到洛杉矶。盖住原来的那张标签。然后送上飞机。飞机到洛杉矶后,机场的人撕去外面的标签,露出里面的标签,一看是送到什么地方的,直接送过去。这个过程中北京和洛杉矶的城市交通比作我们的局域网络,北京到洛杉矶之间的飞机航运比作我们的拨号连接。快递公司的标签就相当于我们的 Ethernet 的包头,机场的标签就相当于 PPP 的包头。唯一的与现实不符的地方就是机场在快递公司的标签外面附上了一层标签,而实际中是丢掉了 Ethernet 的包头,而换上了 PPP 的包头。



## 教学目标

认知目标：掌握远程访问的原理

## 教学准备

教师掌握远程访问的原理

## 教学过程

教师总结网络底层的两种方式：一种是局域网中的工作方式；一种是拨号连接的工作方式，然后再提出无论底层是什么，上层的应用始终不变。

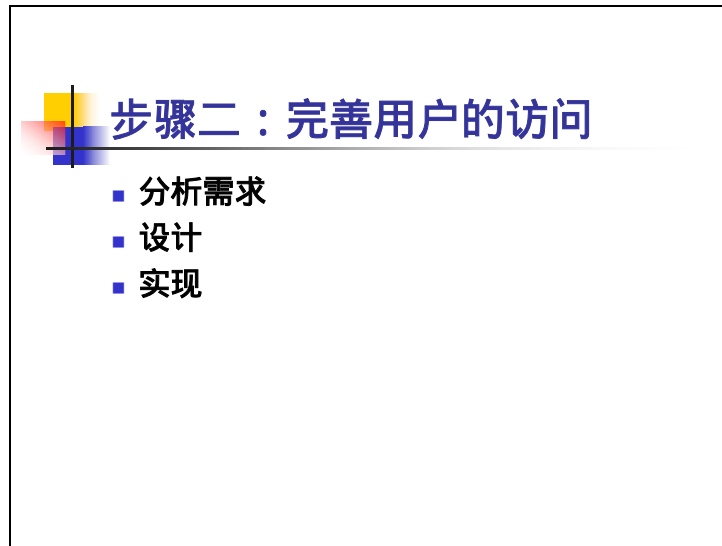
教师总结：从上面的过程，我们可以看出局域网中的两台计算机之间进行通讯使用的是局域网通讯协议（TCP/IP），建立在局域网连接的基础之上（网线连接）；广域网中的两台计算机之间进行通讯，使用的是广域网通讯协议（PPP 协议），建立在广域网连接的基础之上（MODEM 连接）。这些都是网络底层的事情。

无论底层是广域网还是局域网，上层的应用都没有变化，例如：访问共享文件夹，使用网络打印机。

## 难点、重点分析

**难点：**更多的学员会在前面的实验中寻找远程访问的界面  
**分析：**

远程访问是一种对远程资源进行访问的一种方式。主要的内容我们已经讲过。与局域网的计算机之间的区别只体现在网络的底层，网络的上层并没有任何变化。因此在局域网中我们如何使用对资源的访问，那么在远程访问时也同样应用。所有的我们在局域网中使用的方法在进行远程访问时都同样适用，比如资源的访问控制，文件夹的共享，等等。唯一的不同只是体现在局域网的连接是时时存在的，而远程访问的连接在每次我们需要的时候进行连接，连接之后的所有事情都和局域网一模一样，因此不需要任何单独的界面来进行远程访问。



## 教学目标

认知目标：开始了远程访问的另一种形式的实现

## 教学准备

教师掌握虚拟私有网络访问

## 教学过程

教师导入新内容：提示新的实现方式的开始


教师介绍什么是虚拟私有网络

教师组织讨论如何设置虚拟私有网络的服务器和客户端，并且进行连接，

教师总结：

## 难点、重点分析

按照我们的阶梯式学习方法，先讲，领着做；自己做，可以问；独立作。前面的拨号远程访问我们基本上是讲完后让学员按照指导来做的，这里的内容从动手上来说只有一点与前面不同就是端口的配置，因此这一段内容我们的主旨是只讲概念性的一些知识，实验完全独立完成。



## 分步骤一：分析需求

- 用户访问时出现占线
- 费用高
- 不能同时有更多人使用

## 教学目标

认知目标：进一步明确需求

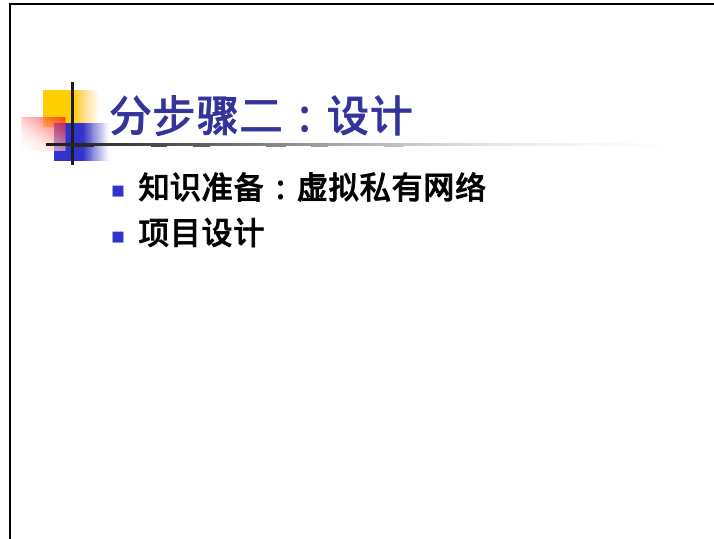
能力目标：

## 教学准备

## 教学过程

教师导入新内容：分析拨号线路的缺点。

教师组织讨论：分析需求



## 教学目标

认知目标：明确分步骤二的课程安排。

能力目标：

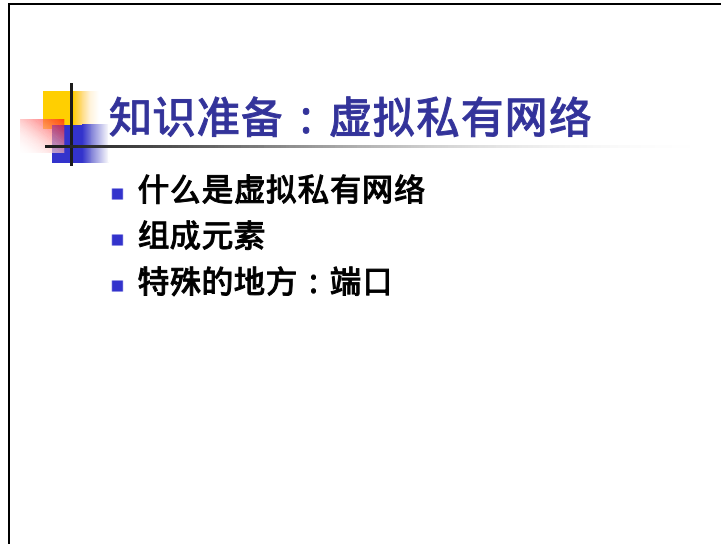
## 教学准备

## 教学过程

教师导入新内容：

教师讲解：分步骤二的课程安排





## 教学目标

认知目标：认识虚拟私有网络，掌握 VPN；管道；管道协议

## 教学准备

教师掌握虚拟私有网络

## 教学过程

教师导入新内容：从前面拨号的远程访问的局限性引出新的需求，从而开始讨论虚拟私有网络。

组织讨论 MODEM 的局限性

教师总结

教师介绍虚拟私有网络及其组成元素

教师总结：虚拟私有网络的配置与拨号的唯一的不同就是端口的配置。

## 难点、重点分析

**难点：**学员不太能够体会出 MODEM 的局限性。

**分析：**

1. 同时接受的连接数目有限。主要是服务器端的硬件受限制。一台不管是什么样的计算机可以连接的设备总是有限的。那我们这里来说，一台计算机的插槽是有限的，比如

ISA 和 PCI 最多不过 5 个 ,也就是说你最多连接 5 个调制解调器( 必须留一个空给网卡 ,那么只有 4 个 )。一个调制解调器同时只能接受一个连接 ,如果你有 6 个人同时进行远程访问 ,那么一台远程访问服务器将不能够满足你的要求 ,你只能在增加新的远程访问服务器。或者你还有另外一种办法 ,就是使用调制解调器池 ,一种专门的硬件设备 ,就是给这种情况下来使用的 ,这样的确可以满足我们的需求 ,但是会带来新的投入 ,而且可以想象这种调制解调器池也是有限制的 ,不可能无限制的连接调制解调器 ,如果在满了呢 ,怎么办 ? 因此只能采用其他的连接技术才能彻底解决这样的问题。

- 2 . 电话费高。这一点基本上不用怎么说。电话费总是比较高 ,相对而言 ,对什么呢 ,对网费 ,并且现在国家在尽量的降低网费 ,更何况很多公司现在都有专门的线路连接互联网络 ,比如 5A 智能型写字间 ,不需要使用电话线路进行上网。这样看来 ,无论如何你的网络的费用都是要花费的 ,为什么还需要使用电话呢 ,为什么不充分利用已有的网络来降低成本呢。
- 3 . 扩展性差。直接拨号使用的是电话号码 ,对于电话号码来说基本上我们不能做任何的控制 ,除了电信局可以。比如将来我们又增加了新的远程访问服务器 ,这是我们不得不对外公布一个新的电话号码 ,告诉所有的员工这个号码也可以进行远程访问。这是一件很麻烦的事情 ,也就是扩展起来很不容易。当然想这个问题 ,拨号本身是无论如何也不能解决的 ,只能依赖于其他的技术手段。 ,也就是扩展起来很不容易。当然想这个问题 ,拨号本身是无论如何也不能解决的 ,只能依赖于其他的技术手段。

传统 RAS 解决方案	带有 VPN/Internet 的 RAS
用户只能通过 56KBPS 或 ISDN 接入	<ul style="list-style-type: none"><li>• ISP 提供 56KBPS , ISDN , DSL , CABLE MODEM 接入</li></ul>
总部提供 800 拨号支持 , 并支付长话费用	<ul style="list-style-type: none"><li>• 用户能选择 ISP 提供的 800 号、漫游号码服务</li></ul>
总部提供独立完成 RSA 设备的部署	<ul style="list-style-type: none"><li>• 无需独立部署 RAS 设备( 与 VPN Application 集成 )</li></ul>
IS 购置专用软件提供集中的管理和远程用户支持	<ul style="list-style-type: none"><li>• 仅使用 WINDOWS 平台上的 VPN 客户机软件</li></ul>
IS 管理拨号接入线路费用和容量规划 , 会增加接入成本	<ul style="list-style-type: none"><li>• 无 , 由 ISP 提供管理 , 利用 ISP 的各种方案来控制接入成本</li></ul>
是否符合 2000 年标准	<ul style="list-style-type: none"><li>• 符合 , 100%符合 2000 年标准</li></ul>
可能存在后门安全性隐患	<ul style="list-style-type: none"><li>• 不存在</li></ul>

**难点：VPN 的组成元素及其之间的关系****分析：**

为了克服拨号远程访问的缺陷，我们可以采用另外一种技术来实现远程访问，即 VPN。VPN 即可用来实现一个用户对一个局域网络的访问，也可以实现两个或多个局域网间的相互访问。

（需要强调）

VPN 连接包含了以下组成元素：VPN 服务器、VPN 客户机、管道、VPN 连接、管道协议、传送网络。

管道，管道协议，VPN 连接之间的关系是不容易理解的内容。

管道是传输 VPN 数据的通道，不是真实的通道，是采用技术虚拟出来的在传输网络之上的通道。

这里的技术就是管道协议。管道协议是用来管理管道和对数据进行封装的数据标准。对数据进行封装是管道协议的根本，也就是在这里我们可以更清楚地来认识管道，管道具体到实现上就是数据包头。使用管道协议就是给数据包加一个特殊的包头，在这个特殊的包头中记录着管道的标识。

管道协议有很多种，在 Windows 2000 种支持的主要是两种管道协议：PPTP 和 L2TP。无论是那种管道协议，都可以管理管道，生成他们自己的数据包的包头。

所有的想知道这个数据包内容的人或者应用程序都能够看到这个包头，看到管道的标识，知道这里存在着一个管道。那么是不是可以直接看到管道内的内容呢？我们来看 VPN 连接，一个完整的 VPN 连接包括传递数据的管道，以及在传递前对数据进行加密和封装的过程。这里的对数据进行加密，就决定了是否可以看到管道内的内容。如果进行加密，那么就不能够看到管道中的数据；反之，就可以看到。现实中，由于 VPN 的传输网络一般是使用互联网，而互联网上有很多黑客，试图捕获别人的数据，非常不安全，所以现实中没有不加密的 VPN。

总之，管道，管道协议，VPN 连接是 VPN 的主要组成元素，管道协议负责管理管道和数据的封装的标准，VPN 连接包含了管道，并且对数据进行加密和封装，理解他们对于了解 VPN 的工作方式有非常大的帮助，但是对于我们的用户来说，这些都是网络底层的工作，或者说对于用户的透明的，用户不需要了解任何这里的知识，建立好的 VPN 同一个局域网络的连接没有什么两样，用户使用起来都是完全一样的，当然对于网络管理员来说，也是完全透明的。

**难点：端口****分析：**

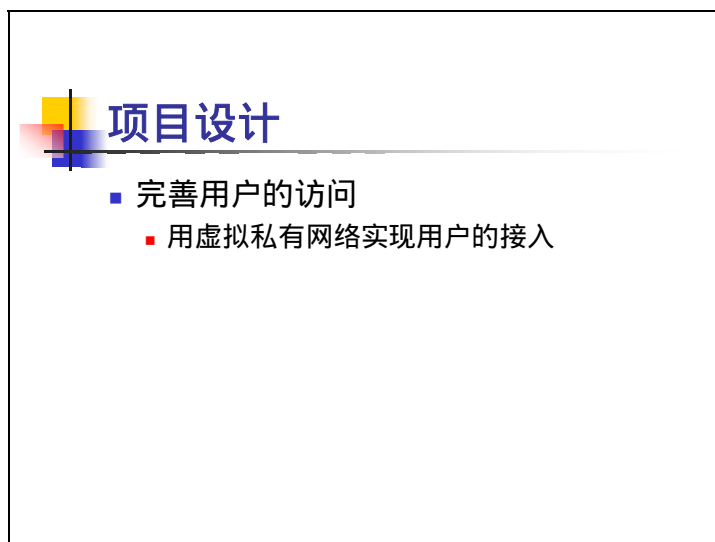
这里的端口和我们前面讨论得端口是一个概念，都是服务器接受用户连接或者发出连接的大门。由上面的两种管道协议，我们这里的端口也有两种：PPTP 和 L2TP。缺省情况下，Windows 2000 默认有 5 个 PPTP 的端口和 5 个 L2TP 的端口，可以根据我们的需要通过设置最大端口数目来增加或者减少端口。对于 VPN 的配置，唯一的与直接拨号不同的就是端口的设置。直接拨号使用的是调制解调器得端口，而 VPN 的设置使用的是专门的 VPN 的端口。

**难点：教师不能做一个好的总结****分析：**

通过上面对于 VPN 的认识，学员已经初步了解了 VPN 及其组成元素。在这一段内容结束之前，一定要有一个清楚地总结，从更高的层次上让学员准确的认识 VPN。只有这样，才能理解 VPN 以及后面我们的内容的安排。

VPN 叫做虚拟私有网络。是在一个共享或者公共的网络纸上建立一个虚拟的网络来进行通讯和资源访问的技术。这种技术被广泛应用在各个领域，同时也存在许多种不同的实现方式，

比如硬件的，软件的等等。无论在什么地方应用，也无论是如何实现的，主要的思想都是架构在一个已有的网络上的安全的通讯传输。在 Windows 2000 中实现虚拟私有网络是建立在 IP 网络基础之上的，也就是说只要 IP 网络的通讯可以进行，那么就可以再 IP 网络之上创建 VPN，实现安全的通讯传输。所以最后对于我们来说，如果两台计算机之间或者两个网络之间的 IP 相同的，也就是可以互相 PING 的到，那么我们就可以创建虚拟私有网络来进行安全的通讯。



## 教学目标

认知目标：进行步骤二设计

## 教学准备

实验准备：手册中设计的内容。


## 教学过程

教师导入新内容：知识准备完了，该设计了。

教师布置：布置设计，在手册中完成设计。

学员实验：完成手册中设计。

教师讲评：各组发言，教师讲评设计。



## 分步骤三：实现

- 设置服务器
- 配置客户端
- 测试

## 教学目标

能力目标：掌握配置 VPN 服务器

能力目标：掌握设置用户的拨入许可

## 教学准备

教师准备实验（详见学员手册）

教师设计提问：VPN 服务器和远程访问服务器有何异同？

能力目标：掌握配置 VPN 的客户端

## 教学过程

教师提问：VPN 服务器和远程访问服务器有何异同？

教师讲解：回忆远程访问服务器的设置，比较得出 VPN 服务器和远程访问服务器是一回事，接下来比较设置的不同点就是端口。

教师指导实验：

学员实验：完善用户的访问。

教师总结：完成了 VPN 服务器的配置，可以接受远程访问客户机的访问请求了

教师提问：比较配置 VPN 服务器和配置 RAS 服务器，在方法和步骤上有什么区别？

教师总结：

## 难点、重点分析

接下来的这一段内容与前面的远程访问的内容基本一样,唯一的区别就是 VPN 客户端的配置有一个是否拨叫初始化连接,只要注意这一点就好了。

### 用户拨入权限

学员在这一部分的学习可能会发现一些比较多的深入的内容,集中出现在用户的拨入属性中,静态的 IP 地址,静态的路由,(学员可能会问为什么这里我还要再设置地址,路由)等等。对于这些问题,教师可以回答,也可以不回答,让学员再去读取帮助。最简单的回答就是这里的优先级最高。

### 配置客户端

这一次的配置 VPN 客户端的向导可以使这学员自己动手来做,唯一的会出现问题的地方也就是 VPN 和 RAS 的客户端配置不同的地方,即是否拨叫初始化连接。这个内容的学员是否理解,或者是否可以独立的完成设置,取决于 VPN 的概念介绍完后的总结是否听到,是否听明白了,所以这里首先是要我们教师一定要注意前面的总结对这里有着直接的影响,不能一带而过,或者含混的提一句,都是不可以的。

现有的教室环境中,我们模拟了一个共享的网络,采用的方法是教室中所有的偶数好的计算机都在同一个 IP 网段内,它们之间已经可以互相 PING 通,所以这里不需要拨叫初始化连接。

## 测试

教师总结：

1. 如果这个实验做成功了，即测试时都得到了正确的结果，说明 VPN 服务器和客户机的配置都是正确的。通过这样的配置，可以实现案例中所描述公司一个办公地点的用户对另一个办公地点的局域网中的资源的远程访问。
2. 如果在实验中，VPN 客户机连接 VPN 服务器失败，或者连接成功，但在测试时，有些步骤没得到正确的结果，则使用 VPN 客户机和服务器的同学彼此之间进行排错，找到发生错误的原因。
3. 现在我们即可用 MODEM 拨号的方式，也可用虚拟私有网络的方式实现案例中所描述的公司对资源远程访问的需求，比较一下，这两种方法在使用上各有什么优、缺点？
4. 拨号和 VPN 在配置服务器和客户机上有什么区别？

## 测试的难点

测试的重点是体现远程访问的真正意义。VPN 客户机和 VPN 服务器之间本身就是可以互相 PING 的通的，所以无论是否建立的远程访问连接，都可以互相访问，从这里体现不出远程访问的，这一点和 MODEM 拨号连接是不同的，MODEM 没有拨号之间就是不能访问，拨号之后就可以了。因此这里的测试主要是要体现远程访问，所以我们的测试重点是 VPN 客户机是否可以通过远程访问服务器访问后面的局域网中的计算机，如果可以，那么证明了远程访问的意义。没有联接的时候是无论如何不能访问的。应该让学员在测试的时候主要体会这一点。



### 查看 VPN 连接状况

注意让学员认识管理的重要性。提问管理员是不是应该提供更多的服务给用户使用；然后提问没有管理的网络是否可以存在？

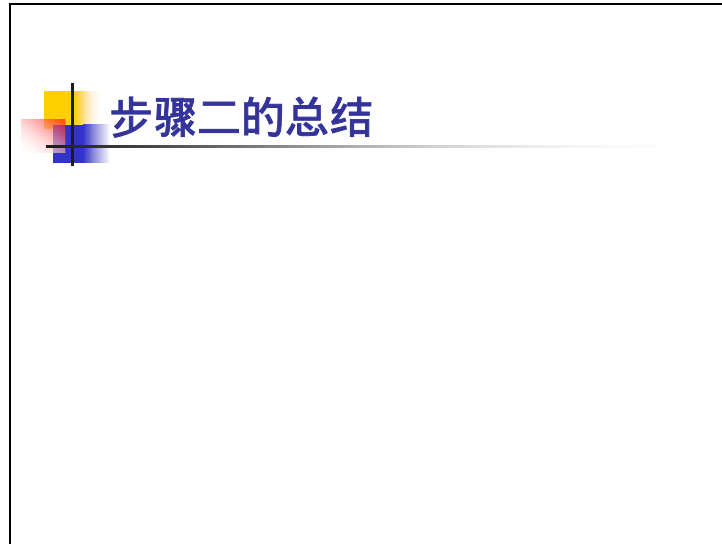
一个网络管理员按照我们前面的设置，配置完了一个远程访问服务器之后，就已经可以成功的接受用户的访问了。能够让我们的用户享受能够提供的服务，是网络管理员应该做的，在大部分情况下，可能也是主要的。充分的挖掘网络的功能，让网络发挥最大的作用是网络管理员日常的工作。

但是与此同时，网络管理员还有一个很重要的工作，就是管理网络，也就是说网络中的一切行为都应该在网络管理员的控制之下。现在我们设置了远程访问服务器，用户已经可以进行远程访问了，那么是不是谁都可以进行远程访问呢？是不是知道了我们的远程访问服务器的电话号码的人都可以访问呢？当然不可以。我们一定要控制。那么现在我们可以做的控制有哪些呢？

- 用户帐户的远程访问许可的设置

- 电话号码只有有限的人知道

- 服务器上可以检查什么人已经在进行远程访问



## 教学目标

总结 VPN

## 教学准备

教师深入掌握 VPN

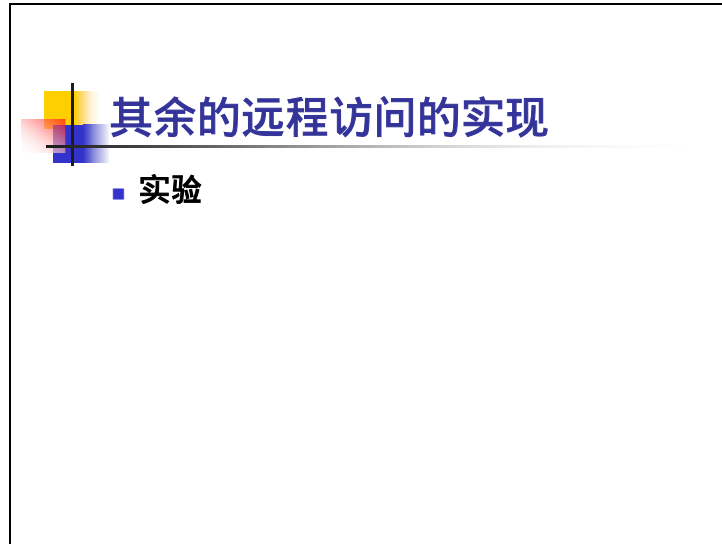
## 教学过程

教师总结

## 难点、重点分析

实际上，拨号网络连接和 VPN 连接在本质上是一样的，所以在配置和管理上也基本上没有区别。两者不同的只是连接的介质不同，一个是 PSTN，另一个是 TCP/IP 网络；一个拨的是电话号码，另一个拨的是 IP 地址。

VPN 最大的优点，在于当有了固定、快速的 Internet 连接时，当我们连接公司的内部网络或者连接公司的两个地点时，就不再需要通过 PSTN 或 ISDN 拨号了，可以直接用 VPN。



## 教学目标

完整实现一个项目，让所有的学员亲历所有的过程，保证没有动手的死角

## 教学准备

教师准备实验（详见学员手册）

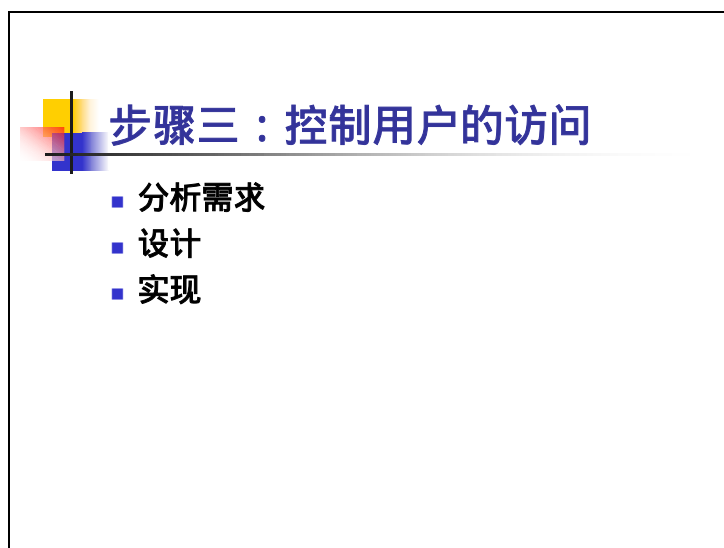
## 教学过程

学员实验

## 难点、重点分析

这里不需要教师讲解，只要安排学员自己动手实现就可以了。与任何一个学员动手或者讨论的地方同样，教师在整个过程中一定要控制。这里的更多的控制是不要让一个学员包办所有的实验，协调学员之间的关系，让每个人都参与其中。还有就是某些组的成员可能水平整体比较高，试验完成得比较快，那么可以安排是否单独的开一些小灶，多学一些我们不讲的，但是有可能会在实际工作中遇到的问题，但是一定要注意内容的选择和范围不要太大（小范围，最好不要形成全班的讨论，否则可能会出现局面失控。那些比较慢的学员会认为他们少学东西了）





## 教学目标

认知目标：引入远程访问的控制的思想


## 教学准备

教师掌握远程访问策略

## 教学过程

教师导入新内容：首先从前面的实验出发，引入远程访问必须要控制，然后如何控制呢，使用远程访问策略，策略都有哪些内容呢，如何对远程访问进行的控制呢？最后是实现

## 难点、重点分析



## 分步骤一：分析需求

- 控制用户能否访问
- 控制用户如何访问

## 教学目标

认知目标：分析控制用户访问的需求。

能力目标：

## 教学准备

教师准备实验、讨论：完成手册上内容。

## 教学过程

教师导入新内容：结合案例分析控制的需求。

教师组织讨论：分析需求。

教师总结：小组发言，教师总结需求。

## 难点、重点分析



## 分步骤二：设计

- 知识准备：远程访问策略
- 服务器

### 教学目标

认知目标：明确设计的课程安排


### 教学准备

教师准备：设计的课程安排

### 教学过程

教师讲解：设计部分的课程安排。

### 难点、重点分析



## 知识准备：远程访问策略

- 什么是远程访问策略
- 组件
- 工作原理

## 教学目标

认知目标：

能力目标：

## 教学准备

教师准备实验、讨论：

教师准备教具：

教师准备哪些知识：

教师设计提问：

## 教学过程

教师导入新内容：

教师讲解：

教师组织讨论：

教师指导实验：

学员实验：

学员自学：

教师总结：

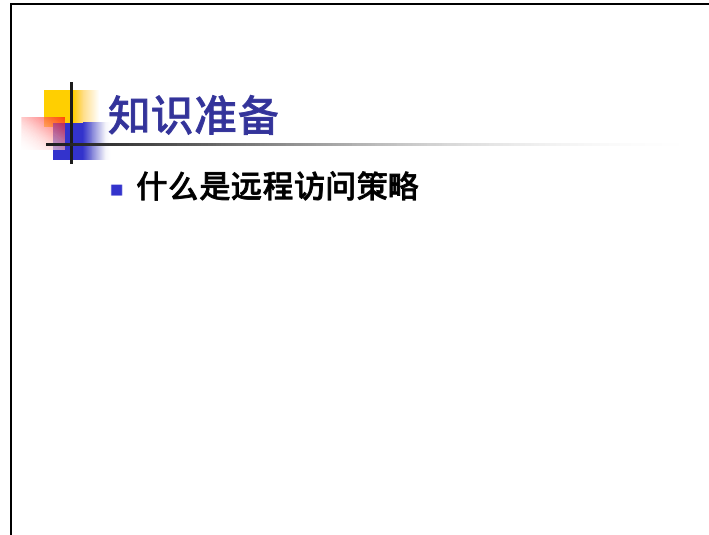


## 难点、重点分析

难点：

分析：

## 资料



## 教学目标

认知目标：掌握远程访问策略

## 教师准备

教师掌握远程访问策略

## 教学过程

教师导入新内容：首先从需要控制出发，引入远程访问策略；

讨论：什么是远程访问策略

教师总结：

远程访问策略：根据一系列的条件和连接设置来审核用户，赋予每个用户不同的远程访问权限的技术。

## 难点、重点分析

**难点：**这里讨论策略可能学员会觉得突然

**分析：**

还是从前面的实验出发，所有的学员已经感受到了远程访问，知道远程访问可以以两种形式进行。无论是那种远程访问，都可以让我们的用户随时随地的访问我们的网络。但是，我们同时也看到无论是如何访问，都不能是没有控制的。没有控制的访问如同没有了法律的社会一

样会天下大乱。这样学员会渐渐的认识对于远程访问一定需要控制的。用什么呢，远程访问策略。

**难点：不理解策略，没有接触过策略这种东西**

**分析：**

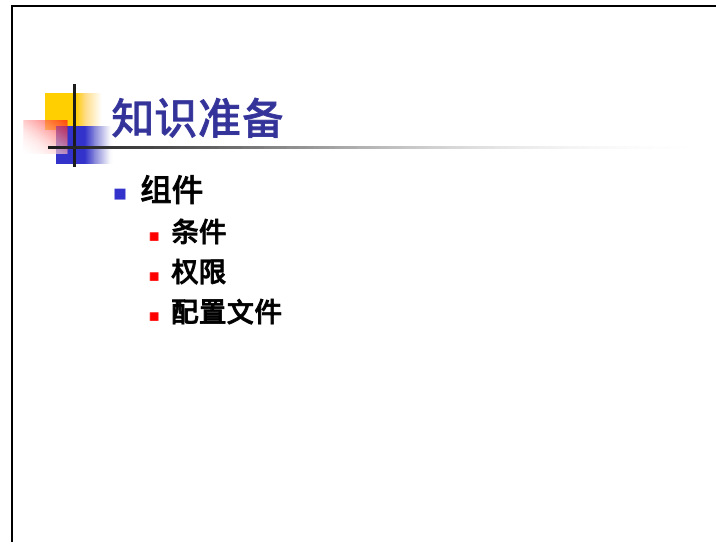
我们在上面的引入中讨论了策略就好像生活中的法律一样，那么我们继续这个例子。首先每一部法律都有很多的条文，对很多东西作了规定；其次每一部法律适用的人或者对象不同，比如经济法是对商业行为的，民法是对民事诉讼的等等；最后任何事情都要受到法律的约束，没有可以逃出法律的控制之外的东西。我们的策略也是一样，任何一个策略中都有许多的内容；每一个策略都有它的条件，符合条件的才适用，否则不生效；只要是远程访问就要受到远程访问策略的控制，如果意外没有任何策略的话，那么谁也不能进行远程访问。

**难点：教师不明白策略的由来（或者叫做特点）**

**分析：**

我们这里所谈的策略是所有的策略，非专指远程访问策略。策略的特点主要是两个：一个是批量的进行设置。也就是说在任何一个策略中都可以同时设置很多的内容。也许这些内容我们可以一个一个地进行设置，但是使用策略可以让我们批量地进行设置，一次设置很多内容，这样提高工作效率，节省工作时间。第二个特点是一个策略可以同时影响很多人或者计算机。任何的策略都会有一些条件，人或者计算机只要符合这些条件，那么都会受到策略的影响，无论是一个人还是几个人，也无论是一台计算机还是几台计算机。当然这样也可以提高工作效率，节省工作时间。从策略的两个特点来说，我们可以得出结论是用策略最大的好处就是提高工作效率，节省工作时间。因此在任何需要提高工作效率，节省工作时间的时候，我们都可以首先考虑是不是可以使用策略来帮助我们。

结合我们的远程访问策略来说，我们希望对远程访问进行控制。首先我们希望控制的内容是多方面的，有允许连接的时间，连接的时间长度，连接的方法，使用的方式等等；其次我们希望远程访问的用户都要受到策略的约束，无论是谁，是哪个部门的等等，也许我们还会有更高的要求，就是不同部门的人我们可能会有不同要求，希望可以实现。这里我们使用远程访问策略基本上就是为了满足我们的这些要求，而且远程访问策略的确也可以完成我们的要求，这也就是我们使用策略的原因。



## 教学目标

认知目标：掌握策略的内容

## 教学准备

教师掌握策略的内容

条件；权限；配置文件

条件：一组参数的列表，其中包括每天的时间、用户组、Caller ID 或 IP 地址等。这些参数用来和请求连接到服务器的远程客户的参数相比较。

权限：是否允许用户进行远程访问可有两种选择：允许或者拒绝。但是一个用户真正能否进行远程访问的许可由两部分内容构成：用户帐户的拨入权限和远程访问策略的权限。

配置文件：设置的主要内容包括验证协议和加密协议等，这些设置将应用于符合策略条件和拨入许可的远程连接。

## 教学过程

教师讲解策略的内容：逐个讲解（不能颠倒次序，这个次序也是策略执行的顺序）

## 难点、重点分析

### 难点：不懂什么是条件

#### 分析：

条件中的内容是一些参数的集合。在这里可以形象地告诉学员条件中的内容就是在远程访问连接尚未建立之前可以检查的参数。还没有建立连接，你可以知道什么东西呢？时间总是可以知道的吧，谁总是知道的吧，就是类似的这些东西。

### 难点：容易混淆权限和用户的拨入许可

#### 分析：

这里的权限专指远程访问策略中设置的权限。只有两种选择：yes or no.没有其他的选择。而我们在前面也提到过类似的事情，就是用户的拨入许可。一个用户是否可以进行远程访问，在用户帐户的属性中可以设置用户的拨入许可。这里的许可设置有三种：允许访问；拒绝访问；和由远程访问策略来控制。前面的两个许可，设什么就是什么。只有当设置第三种：由远程访问策略控制的时候，由我们现在设置的权限生效。我们在前面一直设置的都是用户的拨入许可，现在我们来查看策略中的权限的设置。

### 难点：配置文件与条件的区别

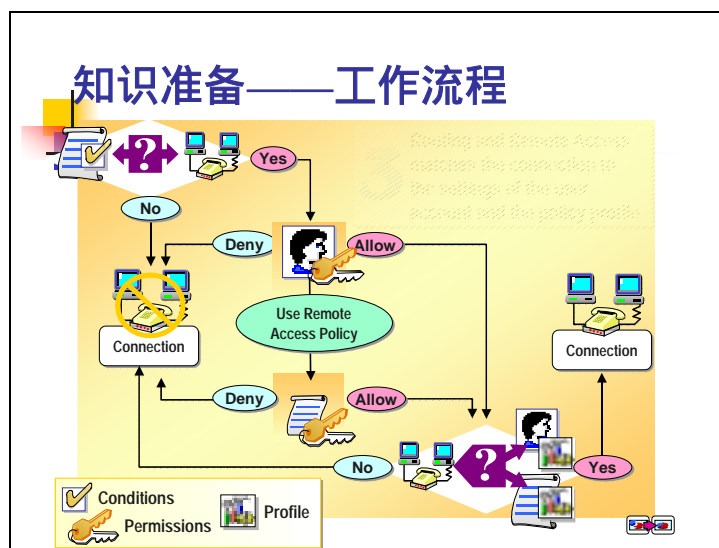
#### 分析：

配置文件是对远程访问连接更精细的控制，不仅影响当前的连接是否可以建立，而且在连接建立后仍然可以发挥作用，比如在连接建立后的一段时间内断开等等。

### 难点：不清楚什么时候应用配置文件

#### 分析：

在介绍配置文件的时候，一定要突出的指出配置文件适用于符合条件的和有远程访问许可的用户。这里的条件指的就是远程访问策略中设置的条件，也就是上面我们刚刚讲过的条件。只有条件符合，才有可能应用配置文件；如果不符合条件，那么根本就不会应用配置文件。这是其一；其二，必须要有远程访问许可。试图进行远程访问的用户必须有远程访问许可才有可能应用配置文件，否则也同样不会应用配置文件。当这两个条件都满足的情况下，才会应用配置文件中的内容，一定是同时满足才应用。如果这里的内容我们讲清楚了，那么学员就会明白什么时候应用配置文件，同时对于策略的执行顺序，也就是接下来我们要讲的内容，学员也基本上可以自己直接理解其中的内容，教师不再需要花费太多的时间来进行讲解策略的执行顺序。这种知识之间的关系和连续性是我们做教师的应该多多发现和挖掘的地方，需要多下功夫。



## 教学目标

认知目标：掌握工作流程

## 教学准备

教师掌握工作流程

## 教学过程

教师讲解工作流程

## 难点、重点分析

**重点：工作流程**

1. 检查条件：  
检查策略的条件和正在请求的远程连接的条件是否一致：  
是，那么进行下一步检查。  
否，那么远程连接自动断开。
2. 检查许可：  
检查远程访问连接许可的三种可能（活动目录的用户 D Dial-in 属性页）：

Allow Access：那么进行下一步检查。

Deny Access：那么远程连接自动断开。

Control access through Remote Access Policy：检查策略中的权限设置：

Allow Access：那么进行下一步检查。

Deny Access：那么远程连接自动断开。

3. 检查配置文件：

远程访问服务器将策略中策略的设置应用于正在请求的远程连接：

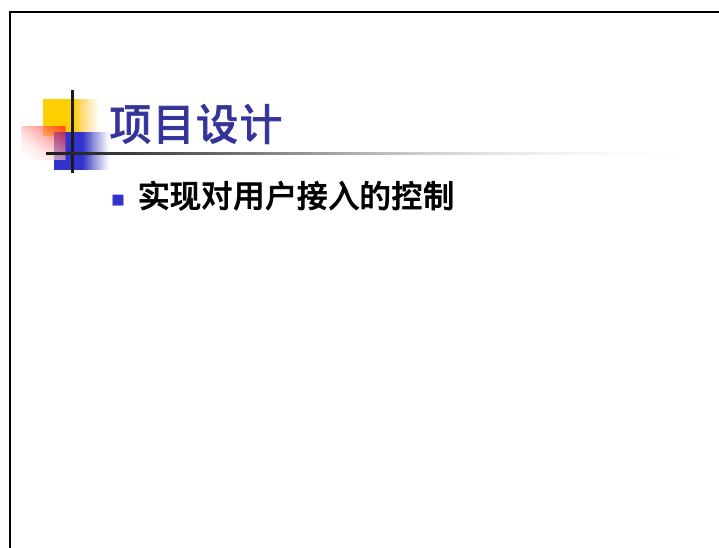
匹配，远程访问连接得到建立。（即使这样，将来也有可能由配置文件中的设置主动断开连接）

不匹配，远程访问请求会被拒绝。

**难点：不理解这个过程**

**分析：**

1. 一定要讲两遍
2. 充分理解整个工作过程是需要时间和思考的。可以使用缺省的远程访问策略来帮助学员进一步理解工作流程。在工作流程讲完两遍之后，给学员 5 分钟的时间分析缺省的远程访问策略，然后提问这个策略的控制的目的是什么。注意：开始之前一定要告诉学员配置文件中没有做任何设置，不需要更多的关注里面的内容。



## 教学目标

认知目标：完成对用户接入的控制的设计

能力目标：

## 教学准备

教师准备实验、讨论：完成手册中的设计。

教师准备教具：

教师准备哪些知识：

教师设计提问：

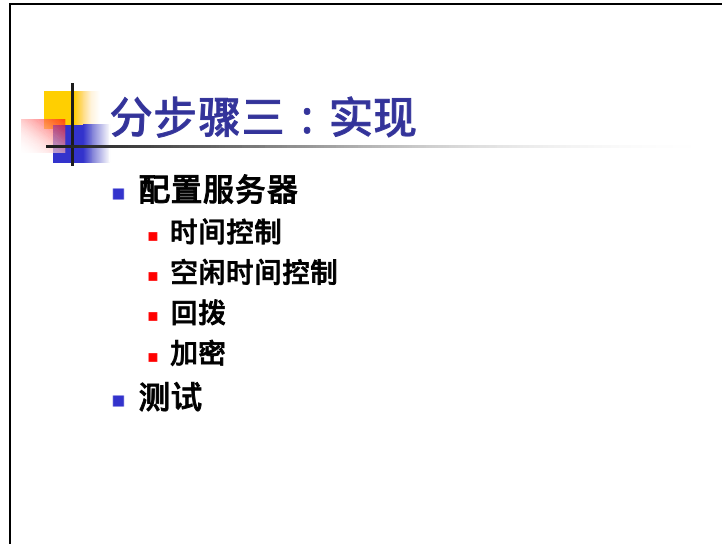
## 教学过程

教师导入新内容：具备了相关的知识后要完成对用户接入控制的设计。

学员实验：完成手册中设计。

## 难点、重点分析





## 教学目标

能力目标：掌握使用远程访问策略控制远程访问

## 教学准备

教师准备实验

## 教学过程

教师示范：

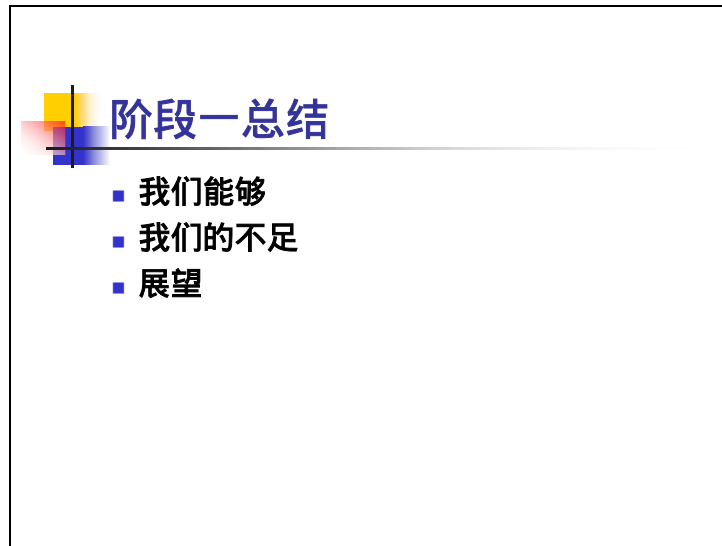
教师可以在这里选择是否示范策略的使用，决定的因素为前面的对于缺省远程访问策略的理解：如果那时候已经有很多的学员看到了策略的界面，这里可以安排直接做实验；反之，如果那时候更多的时间花在了对策略的工作流程的理解上，那么这里要演示使用时间控制远程访问。

学员实验：

学员自学：

教师总结：

## 难点、重点分析



## 教学目标

总结所有的远程访问的东西

## 教学准备

## 教学过程

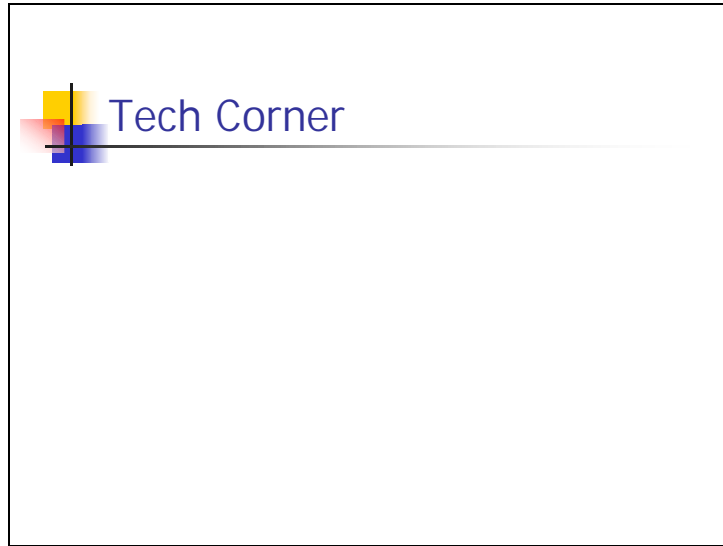
教师总结：

1. 总结我们现在能够实现的远程访问。我们现在可以用两种方法实现远程访问：一种是用 MODEM 进行拨号连接，另一种是用 VPN 的方式进行连接，并且可以通过策略对远程访问进行精确的控制。
2. 我们的不足。如果网络比较大，网络中的远程访问服务器比较多，没有统一的管理。
3. 展望 1. 希望能够对远程访问服务器进行统一的管理。2. 希望对不同的远程访问用户进行更加精确的控制。

## 难点、重点分析







## 目的

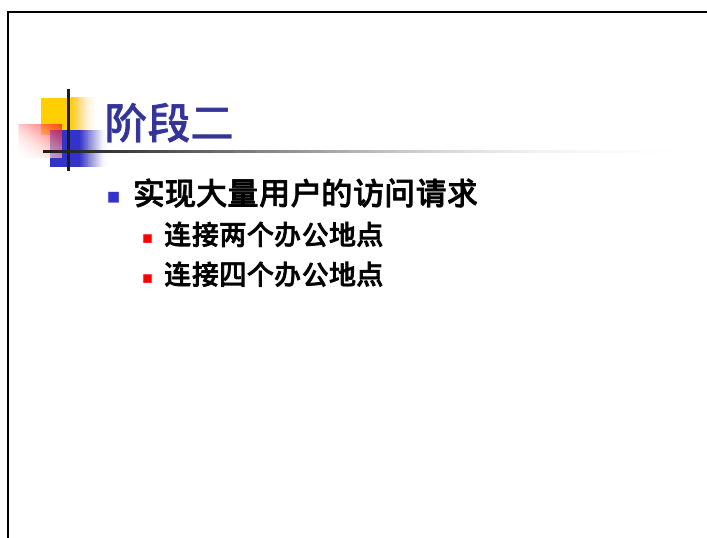
## 知识点

多个策略的工作流程及举例说明；远程访问的身份验证；管道协议；管道协议的数据包的形成过程；IAS；VPN 的默认路由；为什么集成远程访问服务和路由服务为一个

## 讲课过程

## 难点和方法





## 教学目标

告诉学员开始实现的第二个大阶段

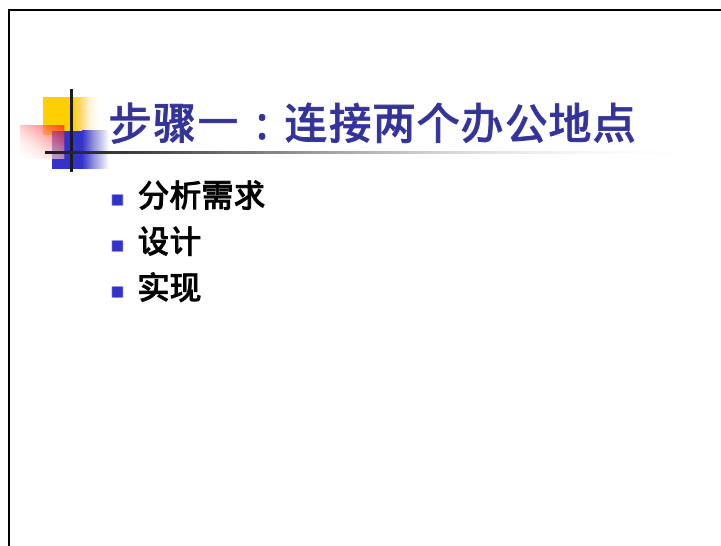
## 教学准备

教师掌握路由

## 教学过程

教师导入新内容：简单回顾前面我们已经可以实现的远程访问，提到他的缺点，引出实现的第二个阶段：路由。路由概念本身已经在 TCP/IP 的课程中讲过了，在这里只是简单的回顾路由，然后就可以把重点放在我们的请求是拨号路由地实现上了：分为两点和四点路由。（他们的区别主要是体现在路由的拓扑结构上。）

## 难点、重点分析



## 教学目标

认知目标：明确连接两个办公地点的课程安排。

## 教学准备


教师准备：连接两个办公地点的课程安排。

## 教学过程

教师讲解：连接两个办公地点的课程安排。

## 难点、重点分析





## 分步骤一：分析需求

- 大量的数据交换
- 很多的计算机之间的互相访问

### 教学目标

认知目标：分析连接两个办公地点的需求。

能力目标：

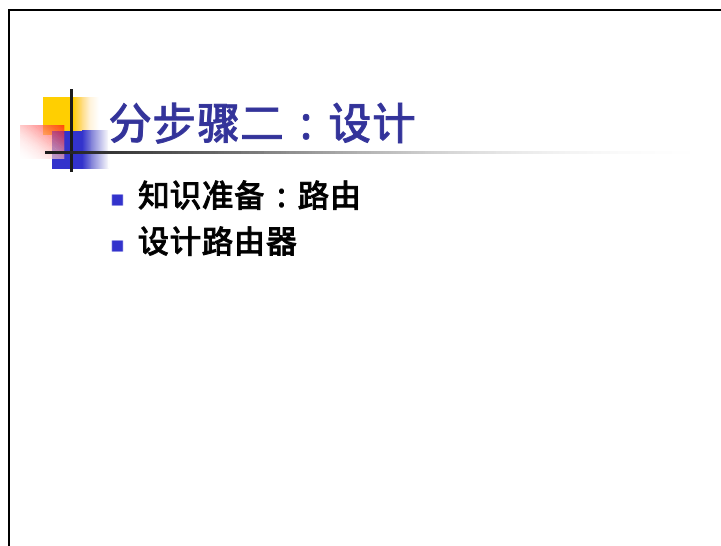
### 教学准备

教师准备实验、讨论：完成手册中要求的分析。

### 教学过程

教师组织讨论：连接两个办公地点的需求

### 难点、重点分析



## 教学目标

认知目标：设计连接两个办公地点的课程安排

能力目标：

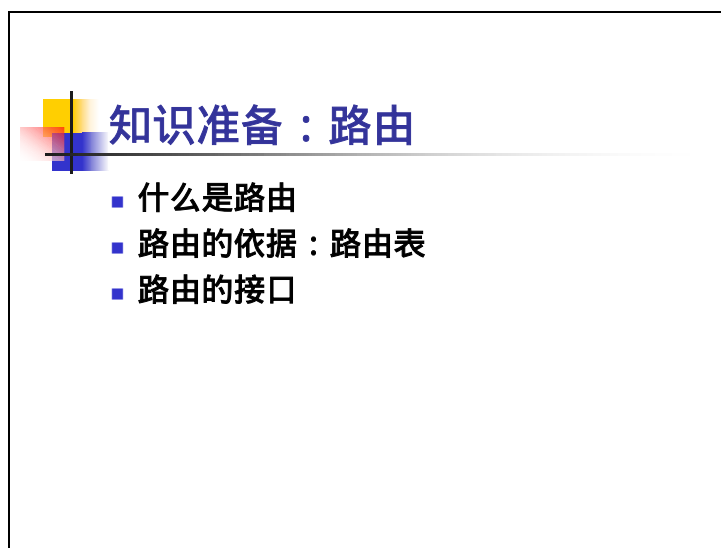
## 教学准备

教师准备实验、讨论：准备手册中设计。

## 教学过程

教师导入新内容：需求分析完了需要设计。

教师讲解：进入设计阶段。



## 教学目标

认知目标：复习路由、路由表、路由接口

## 教学准备

## 教学过程

教师导入新内容：从远程访问的缺点引入路由，然后回顾路由的内容。

## 难点、重点分析

**难点：不会路由的引入**

**方法：**

在上面的课程中，我们已经完成了用户对一个局域网的远程访问。但这样的访问当用户数目比较多时，如果仍然采用远程访问的方式进行资源访问，那么每个用户都要使用一条电话线，或者一个 VPN 的端口，占去一块网络带宽，远程访问服务器端会因为用户数目的增多而服务的质量会降低，同时费用较高，效率低下。这时比较好的方法是在两个频繁进行相互访问的局域网之间采用路由来进行连接，所有的用户的请求都通过同一条路线送到远程网络，是在共享同一个连接，从而完成对资源的访问。这样当然可以解决上面我们提到的那些问题。

**难点：忘记了路由，路由表，路由接口**

**方法：**

路由是在互相连接的网络之间转发报文的过程。路由的主要依据是路由表，路由接口是进

出数据的通道。负责路由功能的计算机叫路由器。

路由表：存放路由信息的地方。路由表中包括了和路由器相连的网络的记录，这些记录表示出当数据要发送到一个特定的网络时，路由器应该向何处进行转发。

任何一张路由表中都包含有缺省的路由记录，比如 127.0.0.0 等等，但也可以添加更多地记录。

根据路由表中路由记录的变化形式，可以把路由分成静态路由和动态路由。静态路由是由管理员负责维护，手动添加和删除静态路由记录来实现的对路由表的管理。动态路由是使用动态路由协议来实现的对路由表的自动管理。

路由接口：路由器上进出数据的端口。

**难点；不理解请求是拨号路由接口是做什么用的**

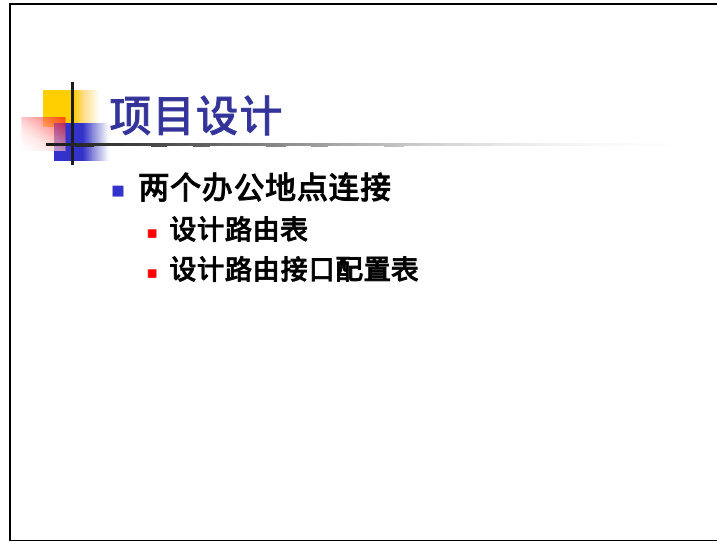
**方法：**

路由接口是路由器上进出数据的端口。普通的路由接口不判断端口上的网络的连接状况，只要有数据需要发送，就会直接进行发送；在 Windows2000 中有一种特殊的路由接口，当数据发送到这种接口上时，他首先会判断当前网络的连接状况，如果网络联通，那么直接发送数据；如果网络断开，那么它会首先建立网络连接，再进行数据的发送。这种接口就是请求式拨号接口。这种路由接口之所以不同于其他的路由接口就在于它可以检测网络的连接状况。如果没有他还可以自己建立连接。

**难点：不理解请求是拨号路由的验证是如何进行的。**

**方法：**

上面我们提到这种特殊的接口可依自己判断网络的连接状况，如果网络连接，那么直接传送数据；如果没有，开始初始化连接，在连接建立后传送数据。这时候很多学员可能会问出这样的问题：我们在进行远程访问的时候，连接建立的时候会输入用户名和口令，那么这种请求是拨号连接的双方是如何找到对方的呢？（如果学员没有问出这个问题，教师也可以提问）。我们在讲远程访问策略的时候提到策略的组件的第一个条件中的内容是连接建立之前就可以知道的事情，比如时间，用户名称等等。我们使用用户名称作为搜索条件，查找当前计算机上的请求是拨号接口的名称，是否有相同的，如果有的话，那么这个请求式拨号接口启用，回拨，之后就是建立连接。从这里可以看出用户的名字不再是随便起的了，必须使对方的接口的名字才能够使用，这一点估计一会的实验中还是会有人搞错，一定要牢牢的记住用户的名字必须与接口的名字相同。



## 教学目标

认知目标：完成连接两个办公地点的设计。

## 教学准备

教师准备实验、讨论：完成手册中的设计。

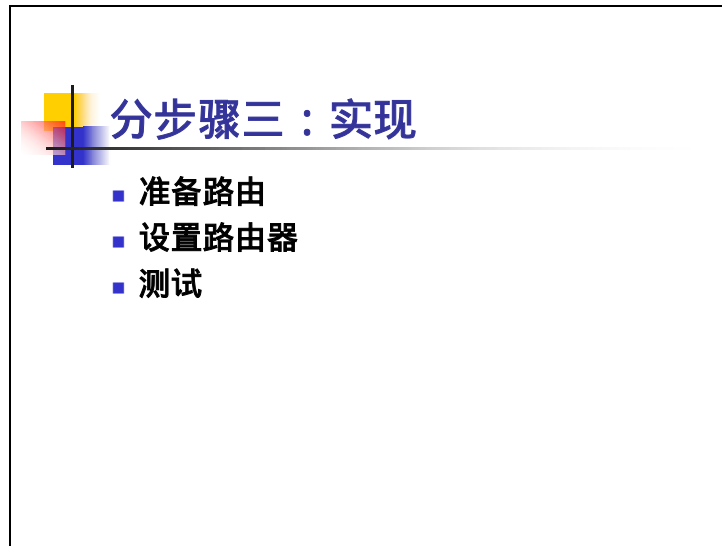
## 教学过程

学员实验：学员完成手册中的设计

教师总结：设计的内容。

## 难点、重点分析

在这里要强调用户名和拨号连接名的对应关系。



## 教学目标

能力目标：实现两个办公地点的连接。

## 教学准备

教师准备实验（详见学员手册）

## 教学过程

学员自学请求式拨号路由接口的向导；

学员写出路由接口配置表。

学员自学得出结论：MODEM 也可以实现。

教师总结：通过这个实验，我们在案例中描述公司的两个办公地点的局域网中分别建立了软件路由器，通过它可以实现公司一个办公地点的用户对另一个办公地点的局域网中资源的远程访问，并且费用较少。

## 难点、重点分析

**难点：**不明白路由接口配置表的重要性（教师和学员）。

**方法：**

请求式拨号路由唯一的会让学员除状况的地方就是需要准备的内容太多，并且容易混淆，

为了能够很清楚地实现请求式拨号路由我们设计了这个路由接口配置表，就是为了清楚所有的内容以及什么地方需要他们。

学员可能会不理解路由接口配置表，因此这里我们教师首先要讲一遍路由接口配置表中的内容，每个内容都要解释，尤其是用户帐户。

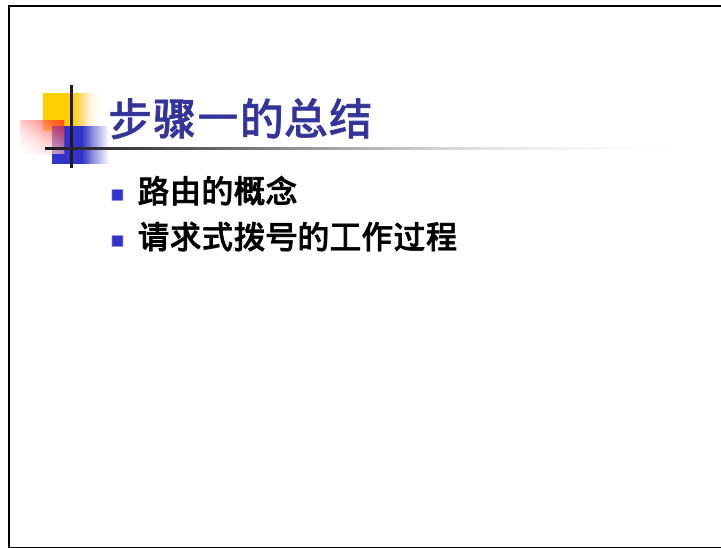
路由接口配置表		
路由器	( 呼叫路由器的名字，如 pc552 )	( 应答路由器的名字，如 pc553 )
接口名称	Topc552	Topc553
拨入用户的帐户名	Topc552	Topc553
拨入用户的密码	123	456
拨入用户所属的域	Nwtraders.msft	Contoso.com
拨出用户的帐户名	Topc553	Topc552
拨出用户的密码	456	123
拨出用户所属的域	Contoso.com	Nwtraders.msft
公共网络 IP 地址	10.0.0.1	10.0.0.3
子网掩码	255.0.0.0	255.0.0.0
私有网络 IP 地址	192.168.1.1	192.168.2.3
子网掩码	255.255.255.0	255.255.255.0
RRAS 服务器分配 IP 地址的范围	192.168.1.5-10	192.168.2.5-10
路由记录中接口的名称	Topc552	Topc553
路由记录中目标网段的 IP 地址	192.168.2.0	192.168.1.0
路由记录中目标网段的子网掩码	255.255.255.0	255.255.255.0

### 测试

测试的方法：一定是双向都通才行。一方先 PING 对方，一次 TIME OUT，二次 Unreachable，三次 connected. 然后切换到 MMC 中，右键刷新，可以看到 connected. 对方也可以看到。接下来，断开重新反过来一次。







## 教学目标

总结

## 教学准备

教师深入掌握两点路由

## 教学过程

教师首先还是简单回顾路由，然后重点总结请求式拨号的工作过程，一个完整的过程。


## 难点、重点分析

**难点：请求式拨号的完整的工作过程。**

**分析：**

1. 一个用户发出了一个连接远程网络计算机的请求（IP）
2. 请求被发送到缺省网关，也就是我们的路由和远程访问服务器。
3. 路由和远程访问服务器检查自己的路由表，发现一条对应的路由纪录
4. 根据路由记录中指定的接口把数据包发送过去
5. 请求式拨号接口受到数据包后检查接口的状态，发现没有连接，开始触发连接

6. 请求式拨号连接的请求发送到对方的路由和远程访问服务器
7. 验证用户的身份，检查是否由远程访问的拨入许可
8. 根据用户的名称检查当前的请求式拨号接口是否有同名的
9. 同名的接口启用，触发回去的拨号
10. 在进行同样的验证用户，检查拨入许可
11. 连接建立
12. 把数据包发送过去



## 步骤二：连接四个办公地点

- 分析需求
- 设计
- 实现

## 教学目标

认知目标：实现四点路由

## 教学准备

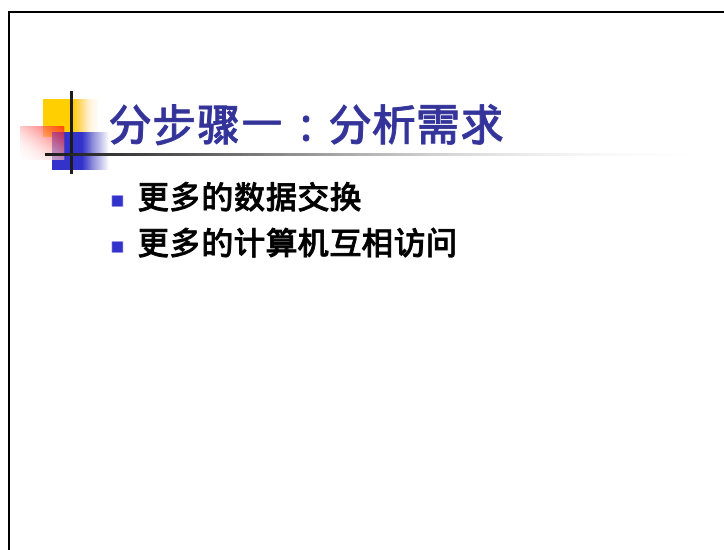
教师掌握四点路由

## 教学过程

教师讲解：

## 难点、重点分析

不同于两点路由，这里需要进行规划。否则很有可能数据包不能被正确的传输，或者根本就不能到达目的地。强调完规划的重要性之后，其他照旧。引导学员开始讨论路由的规划问题。讨论后，找出最具有特色的方案（就是最复杂的方案），实现。



## 教学目标


认知目标：分析四个地点连接的需求。

## 教学准备

## 教学过程

教师指导实验：分析四个地点连接的需求

## 难点、重点分析



## 分步骤二：设计

- 设计路由拓扑
- 设计路由表
- 设计路由接口配置表

## 教学目标

认知目标：初步认识规划

## 教学准备

教师掌握规划路由

教师准备讨论规划路由方案（详见学员手册）

## 教学过程

教师组织讨论：

首先规划路由的拓扑结构，也就是数据包从任何一个地方出发，到任何一个地方走的路线。然后写出所有的路由表，最后为实现写出路由接口配置表。

教师总结：在方案设计时，你遇到了最大困难是什么？怎么解决的？

## 难点、重点分析

规划的例子：

背景；共四个地点：1，2，3，4。每个地点有2台计算机，其中一台有 modem 一只，另外一台连接在教师的公网上。

规划1：modem 分成两对，对拨；VPN 互补连接成另外的两对

规划 2：VPN 连接成网。

规划 3：有待补充

**难点：学员设计的方案中的数据包运输路线可能过于简单**

**方法：**

在这里，我们的实验手册中需要学员设计数据包的传输路线，主要是为了下一步写路由表做准备的。大部分学员在这里都会想得比较简单，需要发送数据到什么地方，直接发送好了。实际的情况下一般不会这么简单，因此在这个时候，如果教师发现班里有比较多的这种情况，可以在白板上作一下示范，示范数据包可以有多种方式到达目的地，以此来启发学员的思路，丰富学员的路由表。

比如数据包从小组 1 到小组 2，可能的路线有：

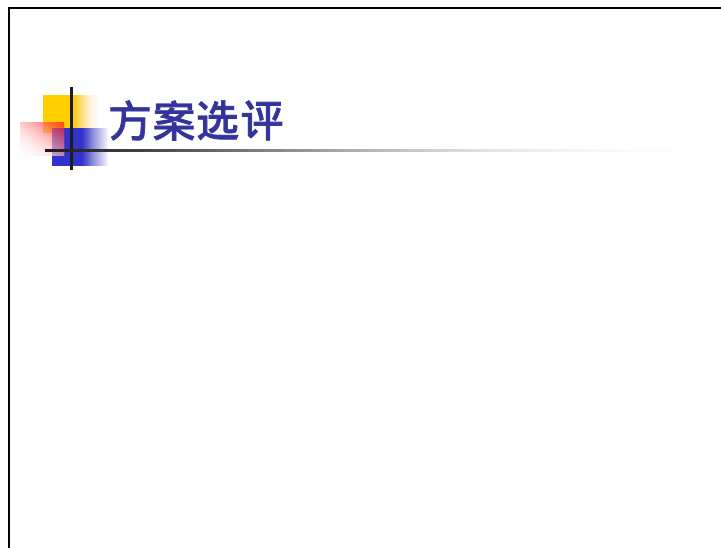
1- 2；

1- 3- 2；

1- 4- 2；

1- 3- 4- 2；

1- 4- 3- 2



## 教学目标

选择方案

## 教学准备


## 教学过程

## 难点和方法

评价无所谓好坏，只是更合理







### 分步骤三：实现

- 准备路由
- 设置RRAS路由器
- 测试

## 教学目标

能力目标：如何实现一个复杂的方案

## 教学准备

教师准备讨论

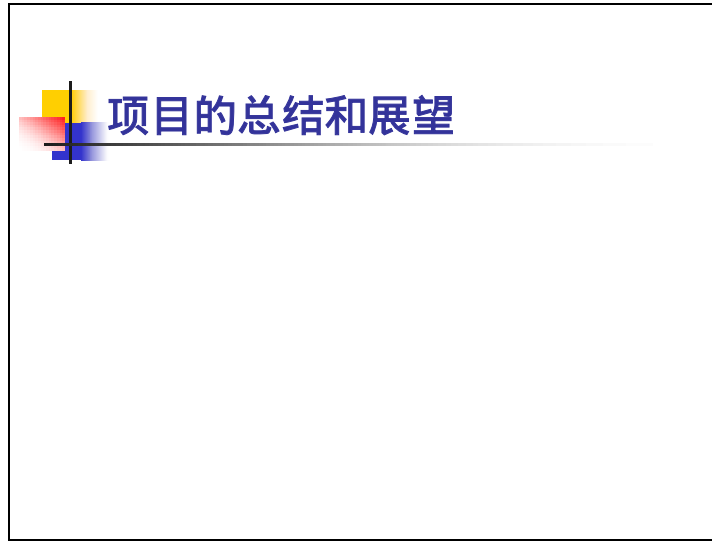
## 教学过程

教师组织讨论

教师总结

## 难点、重点分析





## 教学目标

回顾所有的内容，展望工作的远景

## 教学准备

## 教学过程

首先回顾所有做过的事情，然后设想工作的环境与我们的实现之间的异同；最后展望我们这门课程的扩展，除了可以完成这些事情，还可以做什么。

## 难点、重点分析