# 《计算机网络》课程教学设计



**一、课程定位**

本课程是面向全校本科各专业学生的一门重要的公共工程技术基础课程，是理论和实践紧密结合的一门课程，是提高学生信息素质和工程素养的一门重要的基础课程。通过本课程的教学，使学生能够系统地掌握计算机网络的基本概念、核心原理和常用的组网技术，为今后从事基于信息系统的作战、指挥、训练工作奠定必要的工程技术基础。

**二、教学对象**

《计算机网络》课程的授课对象是全校本科各专业学生，他们具有基础较好，理解能力强，有强烈的求知欲的特点，并且对计算机网络已有一些初步的认识，接触和使用过不少网络应用。他们希望通过课程学习了解计算机网络内部的工作原理，利用所学知识能解决一些在网络应用方面的实际问题。本课程要求学生具备计算机系统硬件、软件以及通信方面一些必要的基础知识。

**三、课程教学目标**

通过本课程的教学，使学生能够系统地掌握计算机网络的基本概念和核心原理，掌握因特网一些重要协议和常用网络设备的基本工作原理。培养学生学习复杂系统工作原理的能力；培养学生科学思维能力和自主学习能力，培养学生分析问题、归纳和综合知识的能力；培养学生理论指导实际，灵活利用所学原理与知识分析和解决实际网络应用中的问题的能力。通过本课程的教学提高学生的信息素质，以适应未来..….的需要。同时通过本课程的教学，可以为学习计算机、通信、信息类专业课程打下坚实的理论基础，为今后从事……工作奠定必要的工程技术基础。

**四、课程教学内容设计**

本课程教学分为理论教学（44学时）和实践教学（12学时）两部分。理论教学借助计算机网络五层原理性体系结构来组织教学内容，以因特网为实例，围绕基本概念和基本原理，按照：概述、物理层、数据链路层、网络层、运输层、应用层的顺序讲授各层内容，最后教授与以上各层都相关的网络安全。

一是概述。使学生对整个计算机网络和因特网的功能、构成有一个整体粗略的了解。了解分组交换的基本原理和特点。理解什么是网络协议，网络协议的分层体系结构及各层的基本功能。

二是物理层。主要让学生理解一些数据通信方面的基础知识和物理层能为上层提供什么样的服务，为理解上层协议的工作原理提供一定的基础知识。

三是数据链路层。掌握计算机网络的底层技术：数据链路层要解决的几个基本问题，重点是媒体访问控制和局域网技术。

四是网络层。网络层是计算机网络的核心，掌握网络层是理解整个计算机网络的工作原理的关键，要掌握IP地址、分组转发、路由选择、网络互联等计算机网络的核心技术和重要概念。还要掌握网络层和数据链路层的关系，以及将网络虚拟化链路的概念。

五是运输层。理解运输层在网络分层体系结构中承上启下的重要地位，掌握可靠数据传输和TCP的工作原理，掌握流量控制和拥塞控制的基本原理和方法。

六是应用层。由于学生对网络应用的使用较为熟悉，应用层主要是使学生理解应用层是如何利用下层提供的服务来实现各种网络应用的，理解应用层协议所要解决的问题。理解典型网络应用的基本原理。

七是网络安全。先介绍网络安全的内容，然后介绍网络安全服务的各种机制，最后简要介绍典型的网络安全协议和系统。

实践教学以强化学生的动手实践能力为目的，以提高操作技能和面向实用技术为设计原则，以组网技术和构建网络应用服务为核心设计实验内容。具体包括简单局域网组网、网络协议分析、路由器配置、典型应用服务器的配置和简单网络应用程序开发等实用性较强的实践内容。部分实验内容可根据学生学习能力和实际情况，让学生自主选做。

**五、课程教学模式设计**

采用以讲授原理性知识为主的教学模式，按照计算机网络五层原理性体系结构来组织教学内容，以因特网为实例，围绕基本概念和基本原理，按照“自底向上”的方法，逐层讲授各层内容，使学生逐步建立起计算机网络的知识体系结构。着眼原理知识，使学生获得长“保质期”的知识，同时关注目前流行的技术，将这些技术作为网络原理的应用实例来学习。

在学习计算机网络每层协议的原理时，主要按照“问题→方法和原理→具体技术实例”的思路讲解：先分析该层的主要任务是什么与上下层之间的关系是什么，要解决的主要问题有哪些。针对这些主要问题先讲解解决这些问题的基本方法和基本原理，然后介绍在因特网中实现这些功能的具体协议或网络设备。例如，网络层的一个重要问题就是如何找到一条到目的地的“最佳”路径，即路由选择问题。先讲授基本的原理性选路算法，如距离向量选路算法、链路状态选路算法，然后再介绍因特网中分别采用这两种算法的选路协议：RIP和OSPF。

由于计算机网络是一个极其复杂的系统，学习计算机网络的过程实际就是一个在学生的知识空间中“构建”一个计算机网络体系结构的过程。因此，对于每个知识点在授课中应强调知识点在整个体系结构中的位置，所起到的重要作用，以及与其他知识点之间的关系。在授课过程中，注重阶段性总结，每章结束时通过总结帮助学生将该章内容关联起来建立起计算机网络某一层的知识结构，然后再放入到整个网络体系结构去，这样学完整个课程后在每个学生掌握的是一个复杂的计算机网络系统，而不仅仅是一些零散的知识点和技术原理。

在教学方法上，由“单一的教员讲解”转变为采用引导、启发、研究、讲解、讨论等多种形式，引导学生主动思考、积极研究，激发学生的求知欲、想象力、创新欲和探索精神。

在教学过程中强调“课前”、“课中”、“课后”的有机结合。强调课前预习，先以预习作业的形式将问题布置给学生，学生在课前利用已学知识，分析问题并进行创新思维，大胆提出自己的解决方案。在学生充分课前思考的基础上，教员引导学生利用科学思维方法最终将要传授的知识转化为学生自己的创新成果。通过课后开放性问题进一步拓展学生的思维空间。

针对学生不会看书，不会学习，课堂互动深度不够，研究讨论参与度不高的问题，部分教学内容采用翻转课堂模式，学生根据教员给出的学习要求、学习资料和启发性问题在课前自学，课堂通过有深度的问题展开讨论，进行深度互动，迫使学生积极思考，指导学生的自主学习，及时纠正学生的学习偏差。

在教学手段上，采用幻灯和板书相结合的形式，充分利用多媒体课件形象、直观、能提高学生的学习兴趣和求知欲的特点，多用图例来描述网络原理和系统结构，用动画来描述协议交互过程和设备工作的流程。同时用板书记录关键性概念，并利用板书灵活动态的特点，在授课过程中对幻灯内容进行灵活扩展和发挥。

# 教学进度总体安排

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 教 学 内 容 | 课堂教学  学 时 | 实践教学  学　　时 | 网络教  学学时 |
| 1 | 概述 | 4 | 0 | 学生自  主学习 |
| 2 | 物理层 | 2 | 0 |
| 3 | 数据链路层 | 8 | 2 |
| 4 | 网络层 | 12 | 4 |
| 5 | 运输层 | 6 | 2 |
| 6 | 应用层 | 8 | 4 |
| 7 | 网络安全 | 4 | 0 |
| 总计 |  | 44 | 12 |

# 《计算机网络》课程教案

**第1讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：课程介绍、因特网概述、因特网的组成  目的要求：明确课程地位和意义，介绍学习方法。了解计算机网络（特别是因特网）的构成和术语。理解网络核心的分组交换技术的基本工作原理，理解电路交换、分组交换的区别。  重点难点：电路交换和分组交换的基本工作原理  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容:  §1 概述  预习思考题：  1.你主要用计算机网络或因特网干什么？你认为计算机网络由哪些关键元素组成？你所知道的网络设备有哪些？你知道的连接因特网的方式（上网方式）有哪些？  2.你认为计算机网络或因特网的核心功能是什么？与电话网、有线电视网有什么本质区别？  一、课程简介  (一)课程目标  (二) 内容、重难点  (三) 学习方法和要求  二、计算机网络在信息时代中的作用  通过提问的方式，让学生自己把计算机网络在信息时代中的作用讲出来，然后进行总结。突出并强调“计算机网络与传统通信基础设施最大的不同在于：其端系统是功能强大、具有智能的计算机！”，因此“应用层出不穷！需求推动网络技术飞速发展！”。  三、因特网概述  (一) 网络的网络  结合图示，介绍一些名词和术语：主机、端系统、链路、路由器。  (二) 因特网发展的三个阶段（简单介绍）  通过图示介绍一下因特网服务提供商和ISP多层结构的形成，和WWW对世界的影响，其他内容学生自学。  (三) 因特网的标准化工作（自学）  布置学生自学，要求学生知道IETF和RFC。  四、因特网的组成  (一) 因特网的边缘部分  简单讲一下其组成。  (二) 因特网的核心部分（重点）  重点讲解分组交换。  1、为何需要交换技术？(分析)  2、网络核心示意图  3、电路交换的基本原理（图例）  4、用电路交换进行计算机数据传输的问题（提问）  通过该问题，启发学生提出分组交换的思想。  5、分组交换的基本原理（图例）  分组、存储转发的概念  6、分组交换与电路交换的比较。  1）分组交换存在的问题：时延、丢包等  通过提问和启发的方式让学生自己将这些问题找出来  2）在资源分配和资源共享方面的比较；  3）在时延方面的比较；  回顾与小结：   1. 计算机网络（特别是因特网）的作用； 2. 因特网的组成； 3. 电路交换、分组交换的基本工作原理； 4. 列出本次课要掌握的知识点。   作业与思考题：  1. 习题1-01  2. 习题1-03  参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 此处板书  通过预习思考题，学生提前思考课堂内容，增强参与度。  此处板书  此处板书  使学生明确学习目标、方法。  此处板书  可将一部分放到课程简介之前作为开场白  此处板书  幻灯并讲解：使学生因特网有一个初步的认识。  幻灯并讲解：使学生知道什么是端系统，端系统中都有些什么。  此处板书  幻灯并讲解：使学生理解电路交换和分组交换的基本原理及其比较。  比较可能没有时间讲完，可让学生课后思考，下次课再讲 |

**第2讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：计算机网络的类别、性能、体系结构  目的要求：掌握计算机网络的基本性能指标、通过研讨理解计算机网络协议分层的意义和作用，理解5层原理体系结构中各层的基本功能。  重点难点： 分层体系结构  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  预习思考题：  1. 你关心的网络性能有哪些（你如何评价网络运行情况的好坏）？  2.如果上网很慢你认为可能的原因是什么？  3.两个人如何通过手电筒传递消息？要考虑哪些问题？请设计一种可行的方案。  内容回顾与本次课内容介绍  一、计算机网络的类别  (一)计算机网络的定义  (二)几种不同类别的网络  布置学生自学。  三、计算机网络的性能  (一)计算机网络的性能指标  速率、带宽、吞吐量、时延、利用率、丢包率的概念和单位。  (二)时延的类型（重点）  1、在路由器的节点时延示意图；  2、处理时延；  3、排队时延；  4、传输时延；  5、传播时延；  6、传输时延和传播时延的比较。  (三)丢包率（增加）  导致丢包的原因、拥塞的基本概念。  四、网络协议和计算机网络的体系结构  (一)网络协议  网络协议的重要性，网络协议的3要素。通过“手电通信”的工作原理的研讨，让学生意识到网络协议的重要性和网络协议所要规定的内容。  (二)灯塔通信问题（研讨题）  通过该实例的研究和讨论使学生理解计算机网络中最核心的问题和原理并不难，但同时意识到设计一个完善的网络系统的复杂性。启发学生用分层的思路去设计一个灯塔通信问题，从该问题的解决中理解分层结构在设计通信系统中的优点和作用。从而引出计算机网络的分层体系结构。  (三)计算机网络的5层原理体系结构  1、以图示的方法从底向上讲解各层的主要功能。然后从上而下总结各层的功能，并强调层间服务与被服务的关系。  2、以邮政系统为例说明分层体系结构在现实生活中的作用，并与网络系统进行比较，引出协议数据单元在各层间传递的流程和封装的概念  3、通过图示和动画讲解协议数据单元在各层间传递的过程，上层协议数据单元是如何封装到下层协议数据单元中的。  4、结合邮政系统说明首部在各层协议中的作用。  回顾与小结：   1. 分组交换网络中的几种主要时延产生的原因和区别； 2. 网络的分层体系结构； 3. 列出本次课要掌握的知识点。   作业与思考题：  1. 习题1-10  2. 习题 1-11  参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 采用学生主动发言与提问相结合的方式，就这些问题开展简要讨论  此处板书  此处板书  此处板书  使学生掌握分组交换网中时延的由哪几部分组成，在什么地方产生。  使学生认识到丢包问题是分组交换网中的一个重要问题  此处板书  将讨论题目布置给学生  重点让学生建立网络体系结构的概念  在讲解邮政系统时要突出分层的作用，不同层有不同的传递单元，有不同的控制信息和地址，引出封装的概念 |

**第3讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：物理层  目的要求：掌握物理层的基本功能，理解一些基本的数据通信方面的基础知识和概念。理解常用宽带接入技术的基本原理。  重点难点：带宽、调制解调、复用  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  §2 物理层  内容回顾与本次课内容介绍  一、物理层的基本概念  物理层的主要任务和物理层规程描述的内容。  二、数据通信的基础知识  (一)数字信号  1. 数字信号与模拟信号  2. 数字信号在传输中会失真  3. 带宽和传输速率极限  (二)调制解调技术  1. 在电信号中表示数字的不同方式  2. 几种基本的调制方式  AM、FM、PM  3. 调制技术的主要用途  三、物理层下面的传输媒体  1. 双绞线  2. 同轴电缆  3. 光纤  4. 无线媒体  四、信道复用技术  1. 复用的基本概念（图示）  2. 频分复用  3. 时分复用  4. 统计时分复用  五、数字传输系统  数字传输系统的作用  六、宽带接入技术  1. ADSL  简单介绍拨号上网的基本原理；  ADSL的基本原理；  ADSL与拨号上网的区别。  2. HFC  主要特点  补充：无线接入   1. 3G 2. Wi-Fi   回顾与小结：  1、物理层在整个计算机网络的作用；  2、对物理层要掌握到什么程度；  3、要掌握的本次课知识点。  作业与思考题：  习题2-05  参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 此处板书  此处板书  关键是使学生能理解数据是如何在媒体中传播的，媒体传输信号的速率是有限的。  此处板书  理解调制解调的基本概念和工作原理，以及其用途  此处板书  掌握各种传输媒体的特点，知道如何选用。  此处板书  信道复用的概念很重要，理解除统计时分复用外，信道复用技术就是将一个原来的传输媒体划分为多个小的子信道。  此处板书  此处板书  重点是让学生理解ADSL与拨号上网的本质区别  简单介绍一下无线接入技术，鼓励学生去查资料 |

**第4讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：数据链路层  目的要求：掌握数据链路层的三个基本问题。  重点难点：数据链路层的三个基本问题  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  预习思考题：  1. 你知道的接入因特网的方式有哪些，各有什么特点？  内容回顾与本次课内容介绍  §3 数据链路层  一、数据链路层的基本概念  介绍两个主机通过互联网进行通信时数据链路层所处的位置  强调：不同段的数据链路层可能采用不同的数据链路层协议  过渡：影响数据链路层协议的一个重要因素是信道类型的差异。  两种信道类型：点对点信道、广播信道。  二、使用点对点信道的数据链路层  （1）数据链路和帧  基本概念：链路、数据链路、规程、帧  点对点信道的数据链路层通信的主要步骤  （2）三个基本问题：  1、封装成帧  结合数据突发性解释封装成帧的原因和方法。  介绍MTU的概念。（MTU使得软硬件实现更简单）  2、透明传输  讨论帧定界符可能导致的错误，引出透明传输问题。  讲解：字节填充方法、零比特填充法  3、差错检测  由误码率引出差错检测问题，并介绍差错检测功能的实现方法。  讲解：循环冗余检验  （3）可靠传输：  1、可靠传输的工作原理  在不可靠的信道上实现可靠的数据传输  为上层提供一条可靠的逻辑通道    课堂讨论  两台计算机通过一条双向不可靠（可能出现比特差错、分组丢失）信道连接，请设计一个方法实现发送方到接收方的单向可靠数据通信（无差错、无丢失、不失序、不重复）。  先解决以上基本问题，再考虑若发送方和接收方之间的往返传播时延很大，你的方法效率如何？如何改进？    （一） 停止等待协议  （1）超时重传    （2）确认丢失    （3）确认迟到（过早超时）    （4）可靠通信的实现  使用上述的确认和重传机制，我们就可以在不可靠的传输网络上实现可靠的通信。  这种可靠传输协议常称为自动重传请求ARQ (Automatic Repeat reQuest)。  ARQ 表明重传的请求是自动进行的。接收方不需要请求发送方重传某个出错的分组 。  （5）信道利用率  停止等待协议的优点是简单，但缺点是信道利用率太低。    回顾与小结：  1、链路与数据链路  2、三个基本问题：封装成帧、透明传输、差错检测  3、要掌握的本次课知识点。  作业与思考题：   1. 习题3-04   预习讨论题：  能否找到一种方法使得多台计算机连接在同一条电缆上可以互相通信？你能想出几种方法？各有什么优缺点？主要论述一种。  参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 此处板书  此处板书  此处板书  重点是让学生理解为什么这三个问题是基本问题，不解决会有什么问题  可通过程序设计中转义字符的概念进行类比讲解  引导学生思考会出现什么问题，如何解决。  通过图例建立可靠数据传输的模型  让学生理解可靠数据传输不仅是运输层的功能  通过课堂讨论题让学生自己设计一个简单的可靠传输协议  注意引导学生考虑一些特殊情况  引导学生自己提出差错检测、确认、超时重传、序号等可靠数据传输机制  板书  前面经讨论已对停止等待协议的基本机制有了一定的认识，现在通过图例系统讲解停止等待协议对各种不同的情况的处理算法  关键是让学生理解ARQ名称的由来  通过图例说明停止等待协议的信道利用率太低引出连续ARQ协议  布置预习讨论题，并让学生开展分组合作设计解决方案，准备在后面的课堂中进行研讨交流 |

**第5讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：PPP协议与使用广播信道的数据链路层  目的要求：了解PPP协议的基本功能。理解媒体访问控制的概念，了解信道共享的一般技术，包括信道划分、受控接入和随机接入。掌握CSMA/CD协议基本原理。  重点难点：CSMA/CD协议  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  三、点对点协议PPP  (一)特点  （二）PPP协议不需要的功能  （三）PPP协议的组成  1、封装方法  2、链路控制协议LCP  为什么需要LCP，LCP的作用是什么  3、网络控制协议NCP  为什么需要NCP，NCP的作用是什么  （四）PPP协议的帧格式  1、帧格式  2、透明传输  （五）PPP协议的工作状态（课后自习）  简单介绍  四、局域网的数据链路层  1、局域网特点  2、局域网拓扑  3、媒体共享技术  [课堂讨论] 引出静态划分信道和动态划分信道，以及随机接入和受控接入的概念。  **讨论**广播信道带来的问题，引出静态划分信道和动态划分信道，以及随机接入和受控接入的概念。  静态划分信道  频分多址、时分多址、码分多址 …  动态媒体接入控制（多点接入）  随机接入，如以太网  如何减少冲突，冲突后如何办  受控接入 ，如多点线路探询(polling)，或轮询。    五、CSMA/CD协议  先介绍以太网环境：总线、广播方式，提供不可靠服务和曼彻斯特编码  介绍CSMA/CD概念，强调多点接入、载波监听和冲突检测。  分析CSMA的碰撞现象，讨论如何尽可能的有效利用信道资源。  分析：  （1）二进制指数类型退避方法  讨论一下这种退避方法的效果。  （2）争用期  用基本退避时间如何确定来引出争用期的讨论。强调争用期又称为“碰撞窗口”，并用作基本退避时间。  （3）最短有效帧长  解释引入最短有效帧长的目的。  （4）强化碰撞。  分析在强化碰撞的情况下，总线占用时间TB+TJ+τ  以太网的重要特性：   1. 碰撞与范围的关系 2. 碰撞与主机数量的关系   回顾与小结：   1. 链路与数据链路 2. 三个基本问题：封装成帧、透明传输、差错检测 3. PPP协议：字节填充、零比特填充 4. CSMA/CD：碰撞、退避方法、争用期、最短有效帧长、强化冲突   作业与思考题：  3-07，3-08，3-20、3-25、3-26  参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 此处板书  此处板书  让学生了解各协议之间的关系，建立PPP链路的过程  此处板书  此处板书  此处板书  通过讨论让学生主动思考，激发学生的创造热情和创新思维  讨论  通过讨论让学生自己提出较为可行的方法来实现媒体访问控制  注意引导学生发现其他同学提出方案的问题  此处板书  通过幻灯分析碰撞过程，讲解载波监听和冲突检测的目的。  讲解退避方法、分析退避效果。 |

**第6讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：使用广播信道的以太网及其扩展  目的要求：掌握集线器的工作原理、MAC地址等概念；掌握以太网扩展的方法，理解网桥工作原理和碰撞域等概念。  重点难点：MAC地址、网桥工作原理、碰撞域概念  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  教学内容与时间安排:  预习思考题：  网桥和集线器有什么区别？  一、使用广播信道的以太网  (一)使用集线器的星形拓扑  （1）介绍从粗同轴电缆到细同轴电缆到集线器  （2）使用集线器的双绞线以太网  集线器的构造、特点  （二）、MAC地址  （1）MAC的作用  多点接入的标识问题。  （2）MAC地址的类型  单播地址、广播地址和多播地址  （三）、以太网的帧格式  课后思考：如何判断帧结束？有没有透明传输问题？  二、扩展的以太网  (一)在物理层扩展以太网  转发器扩展和光纤扩展  结合例子，解释在物理层上扩展以太网时，碰撞域的变化情况。  总结用集线器扩展局域网的优点和缺点  并引出数据链路层上扩展局域网的方法。  (二)在数据链路层上扩展局域网  网桥的内部结构、并图示工作过程。  网桥能够隔离碰撞域  分析网桥的好处和缺点  介绍广播风暴的概念。  (三)透明网桥  1、透明的含义  2、网桥的自学习转发表的过程  比较网桥和集线器的区别。  回顾与小结：  1、以太网的拓扑、MAC地址和帧结构  2、以太网的扩展方法：物理层扩展和数据链路层扩展。  3、冲突域、广播风暴。  作业与思考题：  3-32  作业与思考题：  参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 此处板书  此处板书  此处板书  关键是理解为何需要MAC地址  此处板书  结合幻灯片简单介绍一下以太网帧格式  此处板书  此处板书  分析碰撞域的变化情况  此处板书  用图示的方法介绍网桥的工作过程。  此处板书  根据网桥的基本结构和工作原理引导学生思考如何实现“透明”  用动画图示的方法介绍透明网桥学习转发表的过程。  强调：集线器工作在物理层，逻辑上仍然是一个总线网 |

**第7讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：以太网扩展（续）、高速以太网、无线局域网  目的要求：理解交换机的环路问题、理解VLAN的作用，了解高速以太网的发展，了解无线局域网的基本组成、隐蔽站问题、CSMA/CA的基本工作过程。  重点难点：虚拟局域网、无线局域网  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  预习思考题：  1.交换机，用交换机能互连全球所有的主机吗？有什么问题？  教学内容与时间安排:  内容回顾与本次课内容介绍  一、数据链路层上扩展以太网（续）  (二)透明网桥  4、讨论透明网桥的环路问题和解决方法  (三)多接口网桥  1、以太网交换机的实质就是多接口的网桥  2、以太网交换机的特点  全双工、独占带宽  3、虚拟局域网  虚拟局域网是局域网给用户提供的一种服务。  VLAN抑制了广播风暴  VLAN的实现方法：VLAN的以太网帧  基于端口的VLAN划分:  VLAN的以太网帧格式:  二、高速以太网  （1）100Base-T以太网  （2）使用以太网进行宽带接入    三、无线局域网  (一)无线局域网的组成  1、有固定基础设施的无线局域网  2、移动自组织网络  (二)802.11的MAC层  提问思考：考虑到无线信道的特点，CSMA/CD协议能否直接用于无线局域网？  1、隐蔽站问题  2、CSMA/CA协议  分析IEEE 802.11多路访问特殊性，引出CSMA/CA协议概念和避免碰撞的关键思想。  3、确认与帧间间隔  介绍站点在进行数据收发之前需要分别等待一个时间间隔，以图示说明帧间间隔的作用。  4、利用退避避免碰撞  为避免碰撞，如果要发送数据的站发现信道忙在信道恢复空闲时并不是立即发送数据，而是要退避一段随机的时间（大于DIFS）若信道仍然空闲才能发送数据  5、利用预约避免碰撞  讲解802.11协议中预约机制的工作原理及解决的问题。  回顾与小结：  1、VLAN的概念、网桥和交换机中的生成树算法的目的  2、802.11 LAN 体系结构  3、CSMA/CA工作原理  作业与思考题：  1. 3-27  2. 3-28  3. 试描述IEEE 802.11CSMA/CA协议。假设IEEE 802.11 RTS和CTS帧与标准的DATA数据和ACK帧一样长，使用CTS和RTS帧还会有好处吗？为什么？  预习作业：  1.用网桥和交换机能否方便地互连大量异构网络（不同类型的物理网络，这些网络的帧结构、物理地址长度可能都不同）？为什么？  2.为什么路由器有多个IP地址？  参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 此处板书  根据网桥的基本结构和工作原理引导学生思考如何实现“透明”  此处板书  幻灯并讲解：以太网交换机和虚拟局域网  此处板书  此处板书  图示讲解  重点是接入点的作用。  此处板书  图示讲解  介绍移动自组织网络的军事应用  此处板书  以图示说明为什么无线局域网不能使用碰撞检测  此处板书  此处板书  说明为什么要确认  以图示说明  帧间间隔的作用  与CSMA/CD算法进行比较。  以图示说明预约是如何解决隐蔽站碰撞的问题 |

**第8讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：IP协议  目的要求：理解虚拟互连网络的概念，理解异构网络互联的方法及“网络的网络”概念、理解分类IP地址的概念。  重点难点：异构网络互联的方法及“网络的网络”概念  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  内容回顾与本次课内容介绍  §4 网络层  4.1 网络层提供的两种服务  通过图示介绍两种不同的分组交换技术：数据报服务和虚电路服务：  **H1**  **H5**  **H2**  **H4**  **H3**  A  C  B  D  **H6**  E  **H1**  **H5**  **H2**  **H4**  **H3**  A  C  B  D  **H6**  E  **VC1**  **VC2**  仍然是分组交换  数据报网络提供网络层无连接服务：  因特网的网络层采用的是数据报方式。  虚电路网络提供网络层连接服务：  在传输数据前要先在源主机和目的主机间建立一个连接----虚电路  很多广域网采用虚电路方式，如ATM、帧中继、MPLS  虚电路服务（补充）  1、虚电路号  什么是虚电路号，虚电路号的分配过程。  提问：为什么虚电路号要在每段链路独立分配，而不分配一个全局唯一的号码？  2、虚电路的基本工作原理  虚电路交换机的转发表  虚电路号的改变  3、虚电路的组成  从源到目的地的路径(一系列链路和路由器)  路径上每条链路一个独立的VC号标识经过该链路的各条VC  沿路径每台路由器的转发表中的表项   1. 虚电路的信令协议 2. 虚电路和数据报的比较   4.2 互连网协议IP  4.2.1 概述  1. 虚拟互连网络    2、网络连接设备  物理层：集线器(hub) 、转发器(repeater)  数据链路层：交换机(switch)、网桥 (bridge)  网络层：路由器(router)  由于历史的原因，许多有关 TCP/IP 的文献将网络层使用的路由器称为网关。  网络层以上的中继系统：网关(gateway)  3、因特网体系结构  比较OSI、TCP/IP和五层原理体系结构    4.2.2 地址  IP 地址及其表示方法  〔提问〕：如何设计IP地址更利于路由器转发和寻址？类似于MAC地址这样的唯一标识行吗？  1 分类IP地址  不能分配给主机的特殊IP 地址  常用的三种类别的 IP 地址  2 划分子网  从两级 IP 地址到三级 IP 地址  两级的 IP 地址不够灵活。  划分子网的基本思路  从主机号借用若干个位作为子网号subnet-id，而主机号 host-id 也就相应减少了若干个位。  划分子网后 IP 地址就变成了三级结构。  IP地址 ::= {<网络号>, <子网号>, <主机号>} (4-2)  3. 无分类编址  划分子网在一定程度上缓解了因特网在发展中遇到的困难。但还是不够灵活，仍然有大量地址空间不能被充分利用，大量C类地址块由于容纳主机数太小而无法充分被利用。  提出构成超网方法：将多个C类地址块合起来形成一个更大的地址块分配给某个组织的网络。  解决办法(1993年)：32位IP地址中的网络号的长度可以占任意比例－－网络前缀。  无分类编址方式：无分类域间路由选择 CIDR (Classless Inter-Domain Routing)  无分类的两级编址的记法是：  IP地址 ::= {<网络前缀>, <主机号>} (4-3)  CIDR 把网络前缀都相同的连续的 IP 地址组成“CIDR 地址块”，每块中的地址个数是2的乘方。  将“CIDR 地址块”分配给一个组织，该组织还可以将该地址块划分为多个更小的地址块（前缀更长）分配给组织内的小单位。  用不定长的网络前缀来替代原来分类IP地址中的网络号，路由器按目的地址块进行选路和转发。  子网掩码  在划分子网和无分类编址方式中，从一个 IP 数据报的首部并无法判断目的IP地址的网络前缀/网络号。  使用子网掩码(subnet mask)可以找出 IP 地址中的网络部分(网络前缀)。  CIDR 虽然不使用子网了，但仍然使用“掩码” 或“子网掩码”这一名词。  用32位的子网掩码来表示网络前缀的长度  CIDR 还使用“斜线记法” ，它又称为CIDR记法，即在 IP 地址面加上一个斜线“/”，然后写上网络前缀所占的位数。  CIDR 地址块  128.14.32.0/20 表示的地址块共有 212 个地址（因为斜线后面的 20 是网络前缀的位数，所以这个地址的主机号是 12 位）。  128.14.32.0/20 表示的地址（212 个地址）  CIDR 地址块划分举例  IP 地址的编址方法  分类IP地址。这是最基本的编址方法，在 1981 年就通过了相应的标准协议。  子网划分。这是对最基本的编址方法的改进，其标准[RFC 950]在 1985 年通过。  无分类编址。即构成超网，这是比较新的无分类编址方法。1993 年提出后很快就得到推广应用。  作业与思考题：  1. 比较虚电路和数据报网络的特点。  2. 4-10  预习4.2.5节，回答：  1. 什么情况下IP报文会被分片？  2.为什么路由器有多个IP地址？  参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 此处板书  图示讲解  强调这两种服务都是分组交换  此处板书  以图示说明虚电路的分配过程  以图示说明  转发表的作用和虚电路号的改变  强调该转发表与数据报分组交换机的转发表有何不同。  以图示说明虚电路的建立过程  此处板书  此处板书  此处板书  通过图例说明虚拟互连网络的概念  此处板书  讲解各网络连接设备的区别和工作层次  此处板书  通过图例说明三种体系结构的联系和区别  此处板书  此处板书  通过提问启发学生思考如何设计IP地址的结构  从而理解分类IP地址  此处板书  仅简单介绍  重点是分析特点和缺点  此处板书  仅简单介绍  重点是分析特点和缺点  此处板书  为什么要提出无分类编址  通过黑板练习来说明CIDR地址块的计算 |

**第9讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：IP协议（续）  目的要求：理解ARP协议的工作原理和作用范围，理解IP报文的转发过程和IP报文的格式。  重点难点：IP报文的转发过程和IP报文分片  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  内容回顾与本次课内容介绍  4.2 互连网协议IP（续）  4.2.2 IP地址及编址方式(续)  课堂练习：IP地址的分配  4.2.3 IP 地址与硬件地址  IP地址与硬件地址关系    IP数据报通过不同类型的网络    4.2.4 地址解析协议ARP（续）  1. ARP的工作过程  每一个主机都设有一个 ARP 高速缓存(ARP cache)，缓存已知的IP 地址到硬件地址的映射。  当主机 A 欲向本局域网上的某个主机 B 发送 IP 数据报时，就先在其 ARP 高速缓存中查看有无主机 B 的 IP 地址。  如有，就可查出其对应的硬件地址，再将此硬件地址写入 MAC 帧，然后通过局域网将该 MAC 帧发往此硬件地址。否则，执行ARP。  2. 应当注意的问题  ARP 是解决同一个局域网上的主机或路由器的 IP 地址和硬件地址的映射问题。  如果所要找的主机和源主机不在同一个局域网上，那么就要通过 ARP 找到一个位于本局域网上的某个路由器的硬件地址，然后把分组发送给这个路由器，让这个路由器把分组转发给下一个网络。剩下的工作就由下一个网络来做。  课堂讨论题    作业与思考题：  1. 考虑图中的网络。假设开始时所有计算机的ARP表为空，交换机的转发表也为空，不考虑其他通信的进程。现在计算机D上一个程序发送一个IP报文给C，问计算机A, F和H的网卡分别能检测到哪些分组（什么报文，IP地址和MAC地址和内容）？而计算机A, F和H的协议软件能接收到哪些分组？接着，计算机C上的一个程序发送一个IP报文给D，问计算机A, F和H的网卡分别能检测到哪些分组？而计算机A, F和H的协议软件能接收到哪些分组？    2. 4-22  预习作业：  1.预习4.3节，回答：划分子网和构造超网解决什么问题？子网掩码是干什么的？  参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 此处板书  此处板书  通过课堂练习让学生掌握计算方法，并及时纠正错误  板书  通过图示说明IP报文和数据链路层帧的关系  板书  通过提问引出ARP协议，使学生理解为何需要ARP协议  通过图例讲解  关键是强调ARP的作用范围  通过图例说明路由器转发IP报文的过程  启发学生自己去设计一个简单的路由选择协议 |

**第10讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：划分子网和构造超网  目的要求：划分子网、构造超网和无分类IP编址的概念，掌握IP地址的分配。  重点难点：IP地址的分配  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  内容回顾与本次课内容介绍  4.2.5 IP 数据报的格式    1. 首部长度  2. 总长度  3. 区分服务  4. 生存时间  提问：以太网交换机是如何解决环路问题的？  5. 协议  提问：与以太网帧中的哪个字段有相似的功能？  6. 首部校验和  7. 源地址和目的地址  8. IP报文的分片  (1)为什么要分片  (2)如何分片和重新组装    4.2.6 IP数据报的转发  1. 路由表和IP报文转发    2. 默认路由    3. 分组转发算法  (1) 从数据报的首部提取目的主机的 IP 地址 D, 得出目的网络地址为 N。  (2) 若网络 N 与此路由器直接相连，则把数据报直接交付目的主机 D；否则是间接交付，执行(3)。  (3) 若路由表中有目的地址为 D 的特定主机路由，则把数据报传送给路由表中所指明的下一跳路由器；否则，执行(4)。  (4) 若路由表中有到达网络 N 的路由，则把数据报传送给路由表指明的下一跳路由器；否则，执行(5)。  (5) 若路由表中有一个默认路由，则把数据报传送给路由表中所指明的默认路由器；否则，执行(6)。  (6) 报告转发分组出错。  4. 路由聚合  路由聚合举例  5. 最长前缀匹配  使用 CIDR 时，路由表中的每个项目由“网络前缀”和“下一跳地址”组成。在查找路由表时可能会得到不止一个匹配结果。  应当从匹配结果中选择具有最长网络前缀的路由：最长前缀匹配(longest-prefix matching)。  网络前缀越长，其地址块就越小，因而路由就越具体(more specific) 。  最长前缀匹配又称为最长匹配或最佳匹配。  6. CIDR 最主要的特点  CIDR 消除了传统的 A 类、B 类和 C 类地址以及划分子网的概念，因而可以更加有效地分配 IPv4 的地址空间。  CIDR使用各种长度的“网络前缀”(network-prefix)来代替分类地址中的网络号和子网号。  CIDR虽然形式上是二级编址，但实际上可实现多级编址，大的地址块还可以划分为更小的地址块进行分配。  等级结构的CIDR地址块分配便于实现路由聚合。  作业与思考题：  1. 4-20  2. 4-29    参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 板书  板书  主要让学生理解为何要提出划分子网  通过板书画图说明  让学生上黑板进行计算  板书  板书  板书  让学生归纳出IP分组转发的过程  板书  通过实例讲解  让学生来填写路由表  板书  启发学生思考为什么会存在多个匹配结果，为何要最长前缀匹配  总结 |

**第11讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：ICMP和路由选择  目的要求：理解ICMP的作用、掌握常用ICMP功能、理解路由选择协议的基本工作原理。  重点难点：路由选择协议  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  内容回顾与本次课内容介绍  4.4 网际控制报文协议ICMP  由于IP不提供可靠数据传输服务，在网际层使用网际控制报文协议 ICMP (Internet Control Message Protocol) 允许主机或路由器报告差错情况和提供有关异常情况的报告。  4.3.1 ICMP报文的种类  ICMP 报文的种类有两种，即 ICMP 差错报告报文和 ICMP 询问报文。  1. ICMP差错报告报文  (1)终点不可达  包括协议不可达、主机不可达、端口不可达、不能分片等  (2)源点抑制(Source quench)  网络层拥塞控制，实际中很少使用  (3)时间超时  包括TTL为0和分片超时  (4)参数问题  (5)改变路由（重定向）(Redirect)  举例说明重定向的作用。  2. ICMP询问报文  (1)回送请求和回答报文  (2)时间戳请求和回答报文  4.4.2 ICMP的应用举例  1. PING程序  PING 用来测试两个主机之间的连通性。  PING 使用了 ICMP 回送请求与回送回答报文。  PING 是应用层直接使用网络层 ICMP 的例子，它没有通过运输层的 TCP 或UDP。  PING程序执行实例。  2. Tracerout(Tracert)  Tracerout程序基本原理和工作流程。  (1)源向目的地发送一系列UDP段  第一个 TTL =1  第二个 TTL=2, 等  不可达的端口号  (2)当第n个数据报到达第n个路由器:  路由器丢弃数据报  并向源发送一个ICMP差错报文 (超时报文)  报文包含该路由器的IP地址  源根据收到的ICMP报文计算RTT  Traceroute执行上述过程3次  (3)停止规则  UDP段最终到达目的主机  目的地返回ICMP “终点不可达”分组(由于无进程接收该分组)  当源得到该ICMP, 停止  4.5 因特网的路由选择协议  1. 引入问题    2. 静态路由选择和动态路由选择  静态路由选择——即非自适应路由选择，其特点是简单和路由器开销较小，但不能及时适应网络状态的变化，只能用于简单的小型网络。  动态路由选择——对于复杂多变的大型网络必须采用动态路由选择。动态路由选路能适应网络状态的不断变化，但实现起来较为复杂，路由器的开销也比较大。  4.5.1 有关路由选择协议的几个基本概念  1. 理想的路由算法  算法必须是正确的和完整的。  算法在计算上应简单。  算法应能适应通信量和网络拓扑的变化，这就是说，要有自适应性。  算法应具有稳定性。  算法应是公平的。  算法应是最佳的。  2. 动态路由选择的基本方法  路由器之间要互相不断交换网络拓扑和状态信息，然后根据这些信息求出到所有目的地的最佳路由  路由选择协议要解决的5个问题  Best，什么是最佳路由？  Who，和谁进行交换信息？  What，交换什么信息？  When，何时进行交换信息？  How，如何计算和更新路由表？  课堂讨论    4.5.2 路由选择协议实例：RIP  1. RIP协议中的最佳路由  一条好的路由是经过路由器少的路由。  RIP中“距离”的定义：  从一个路由器到直接连接的网络的距离定义为 1。  从一个路由器到非直接连接的网络的距离定义为所经过的路由器数加 1。  RIP 协议中的“距离”也称为“跳数”，因为每经过一个路由器，跳数就加 1。  2. RIP协议的基本工作原理  RIP协议的基本思想：    RIP协议的基本工作原理：  (1)仅和相邻路由器交换信息。  (2)交换的信息是本路由器当前知道的到所有目的地的距离（最短距离），即自己的路由表（含距离）。  (3)按固定的时间间隔交换路由信息，例如，每隔 30 秒。当路由表变化时也及时向相邻路由器通告路由信息。  (4)每个路由器根据收到的路由信息更新自己的路由表。  路由器更新路由表实例：    3.“坏消息传播得慢”问题  “坏消息传播得慢”问题实例：    [提问]：这种情况会导致什么后果？出现该问题的原因是什么？如何解决该问题？  水平分割：如果R2到某网络的下一站为R1，则R2不向R1通告它到该网络的距离。  [提问]：水平分割能彻底解决该问题吗？  水平分割不能彻底解决该问题的实例：    4. RIP2 协议的报文格式    5.RIP 协议的优缺点  (1)RIP 协议最大的优点就是实现简单，开销较小。  (2)RIP 存在的一个问题是当网络出现故障时，要经过比较长的时间才能将此信息传送到所有的路由器。  (3)RIP 限制了网络的规模，它能使用的最大距离为 15（16 表示不可达）。  (4)路由器之间交换的路由信息是路由器中的完整路由表，因而随着网络规模的扩大，开销也就增加，收敛慢。  作业与思考题：  1. 4-26  2. 4-30(广域网WAN是点到点链路)    参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 板书  介绍ICMP的基本概念和作用  板书  图例说明ICMP报文的基本格式。强调ICMP报文是封装在IP报文中传输的  举例说明  板书画图，通过图例来说明ICMP重定向报文的用途。  板书  板书  板书  通过例子和演示来说明PING程序的用途。  板书  通过板书画图和实例来说明Tracerout程序是如何利用ICMP报文和IP报文的TTL字段实现Tracert程序的。  板书  图例讲解  通过静态路由引出动态路由以及动态路由要解决的问题。  板书  板书  关键是强调任何一种算法都不可能是理想的，但都需要考虑这些问题，可能各有侧重  板书  启发学生理解为什么需要解决这些问题。  课前根据学生提交的讨论课件，选择3个典型  案例，各10分钟，并引导学生发现问题、提出问题并解决问题  板书  板书  针对路由选择协议要解决的5个问题讲解RIP协议是如何考虑的。  板书  通过图例启发学生思考并自己提出RIP协议的基本思路并引出RIP协议的基本工作原理  本次课的重点  通过实例讲解RIP协议中路由器更新路由表的算法  板书  通过实例引出“坏消息传播得慢”问题  通过提问引出“水平分割”  该问题留给有余力的学生课后继续思考 |

**第12讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：OSPF和路由器  目的要求：理解ICMP的作用、掌握常用ICMP功能、理解路由选择协议的基本工作原理。  重点难点：路由选择协议  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  内容回顾与本次课内容介绍  4.5.3 内部网关协议 OSPF  1. OSPF 协议的基本特点  是分布式的链路状态协议。  (1)向本自治系统中所有路由器发送信息，这里使用的方法是洪泛法（广播）。  (2)发送的信息就是与相邻路由器间的所有链路的状态，但这只是路由器所知道的部分信息。“链路状态”就是说明本路由器都和哪些路由器相邻，以及该链路的“度量”(metric)。  (3)只有当链路状态发生变化时，路由器才用洪泛法向所有路由器发送此信息。  2. 链路状态数据库  由于各路由器之间频繁地交换链路状态信息，因此所有的路由器最终都能建立一个链路状态数据库。  这个数据库实际上就是全网的拓扑结构图，它在全网范围内是一致的（这称为链路状态数据库的同步）。  3. 层次OSPF    4. OSPF 的五种分组类型  类型1，问候(Hello)分组。  类型2，数据库描述(Database Description)分组。  类型3，链路状态请求(Link State Request)分组。  类型4，链路状态更新(Link State Update)分组，  用洪泛法对全网更新链路状态。  类型5，链路状态确认(Link State Acknowledgment)  分组。  5. OSPF 的特点  OSPF 对不同的链路可根据 IP 分组的不同服务类型 TOS 而设置成不同的代价。因此，OSPF 对于不同类型的业务可计算出不同的路由。  如果到同一个目的网络有多条相同代价的路径，那么可以将通信量分配给这几条路径。这叫作多路径间的负载平衡。  支持可变长度的子网划分和无分类编址 CIDR。  OSPF支持域内层次路由，因此当互联网规模很大时，OSPF 协议要比距离向量协议 RIP 好得多。  OSPF 没有“坏消息传播得慢”的问题，据统计，其响应网络变化的时间小于 100 ms。  由于OSPF每个路由器获得的是全局信息并独立计算路由，不易因故障或攻击导致整个路由错误，因此比RIP更加具有健壮性。  4.5.4 外部网关协议 BGP  1. 分层次的路由选择协议  因特网采用分层次的路由选择协议。  因特网的规模非常大。如果让所有的路由器知道所有的网络应怎样到达，则这种路由表将非常大，处理起来也太花时间。而所有这些路由器之间交换路由信息所需的带宽就会使因特网的通信链路饱和。  许多单位不愿意外界了解自己单位网络的布局细节和本部门所采用的路由选择协议（这属于本部门内部的事情），但同时还希望连接到因特网上。  分层路由和自治系统（图例）  内部网关协议 IGP (Interior Gateway Protocol) ：具体的协议有多种，如RIP、OSPF  外部网关协议 EGP (External Gateway Protocol) ：目前使用的协议就是BGP-4  2．BGP 使用的环境不同  因特网的规模太大，使得自治系统之间路由选择非常困难。对于自治系统之间的路由选择，要寻找最佳路由是很不现实的。  当一条路径通过几个不同 AS 时，要想对这样的路径计算出有意义的代价是不太可能的。  比较合理的做法是在 AS 之间交换“可达性”信息。  自治系统之间的路由选择必须考虑有关策略。  因此，边界网关协议 BGP 只能是力求寻找一条能够到达目的网络且比较好的路由（不能兜圈子），而并非要寻找一条最佳路由。  3．BGP 发言人和自治系统 AS  （1）BGP 交换路由信息  一个 BGP 发言人与其他自治系统中的 BGP 发言人要交换路由信息，就要先建立 TCP 连接，然后在此连接上交换 BGP 报文以建立 BGP 会话(session)，利用 BGP 会话交换路由信息。  使用 TCP 连接能提供可靠的服务，也简化了路由选择协议。  使用 TCP 连接交换路由信息的两个 BGP 发言人，彼此成为对方的邻站或对等站。  BGP发言人向邻站通告到所有已知网络的最短路径（包含经过的所有AS号）  （2）BGP 发言人交换路径向量 （图例）  [提问]BGP有“坏消息传播得慢”的问题吗？  （3）AS 的连通图举例 （图例）  BGP 所交换的网络可达性的信息就是要到达某个网络所要经过的一系列 AS。  各 BGP 发言人根据收到的路由信息中找出到达各网络的较好路由（经过AS最少且无环路的路径），这些路由构成了一个树状拓扑。  BGP 协议的特点  BGP 协议交换路由信息的结点数量级是自治系统数的量级，这要比这些自治系统中的网络数少很多。  每一个自治系统中 BGP 发言人（或边界路由器）的数目是很少的。这样就使得自治系统之间的路由选择不致过分复杂。  4．BGP 协议的特点  BGP 支持 CIDR，因此 BGP 的路由表也就应当包括目的网络前缀、下一跳路由器，以及到达该目的网络所要经过的各个自治系统序列。  在BGP 刚刚运行时，BGP 的邻站是交换整个的 BGP 路由表。但以后只需要在发生变化时更新有变化的部分。这样做对节省网络带宽和减少路由器的处理开销方面都有好处。  是一个路径向量算法（类似距离向量算法），但没有“坏消息传播得慢的问题”  4.5.5 路由器的结构  路由器的结构图    1. 输入端口  数据链路层剥去帧首部和尾部后，将分组送到网络层的队列中排队等待处理。这会产生一定的时延。   1. 交换结构 2. 通过存储器 3. 通过总线 4. 通过互连网络   3. 输出端口  当交换结构传送过来的分组先进行缓存。数据链路层处理模块将分组加上链路层的首部和尾部，交给物理层后发送到外部线路。  作业：  1. 4-41  2. 4-42  预习作业  1. 预习4.5.4回答：BGP为什么不存在“坏消息传播得慢”的问题（路由环路问题）？    参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 板书  板书  针对路由选择协议要解决的5个问题讲解OSPF协议是如何考虑的。  板书  板书  通过图例讲解边界路由器、主干路由器、内部路由器和区域边界路由器的作用  板书  理解各报文的作用即可  板书  通过与RIP比较讲解  板书  首先是要强调为什么要进行分层路由  图例讲解  通过图例讲解IGP和EGP的关系  为什么BGP不精确求解“最佳”路由  关键是要理解BGP发言人的作用，BGP路由通告中的内容  通过提问启发学生思考BGP与RIP的本质区别  理解路径向量算法  板书  结合图例讲解路由器的组成及其各部分的关系  关键强调是查找路由表是在输入队列中完成的  三种交换结构的比较  关键是理解排队时延的产生原因 |

**第13讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：多播、VPN和IPv6  目的要求：理解多播的概念、理解VPN和IP隧道技术、了解IPv6的特点。  重点难点：IP隧道技术  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  4.6 IP 多播  1. IP 多播的一些特点  (1) 多播使用组地址—— IP 使用 D 类地址支持多播。多播地址只能用于目的地址，而不能用于源地址。  (2) 任何主机可以发送多播分组给一个多播组。  (3) 动态的组成员，能够支持任意多的组成员，主机能随时加入或离开组。  (4) 在局域网上利用硬件多播功能。  2. 在局域网上进行硬件多播  D类IP地址与以太网多播地址的映射关系  3. IGMP和多播路由选择协议  为了使路由器知道多播组成员的信息，需要利用网际组管理协议 IGMP (Internet Group Management Protocol)。  IGMP的作用范围  连接在局域网上的多播路由器还必须和因特网上的其他多播路由器协同工作，以便把多播数据报用最小代价传送给所有的组成员。这就需要使用多播路由选择协议。  4.7 VPN 和NAT 4.7.1 虚拟专用网 VPN  全球地址——全球唯一的IP地址，必须向因特网的管理机构申请。  本地地址——仅在机构内部使用的 IP 地址，可以由本机构自行分配，而不需要向因特网的管理机构申请。在因特网中的所有路由器对目的地址是专用地址的数据报一律不进行转发。  10.0.0.0 到 10.255.255.255  172.16.0.0 到 172.31.255.255  192.168.0.0 到 192.168.255.255  用专线实现专用网（图例）  用隧道技术实现虚拟专用网（图例）  远程接入VPN（图例）  4.8 下一代的网际协议 IPv6  IPv6 仍支持无连接的传送所引进的主要变化如下：  更大的地址空间。IPv6 将地址从 IPv4 的 32 位 增大到了 128 位。  扩展的地址层次结构。  灵活的首部格式。  改进的选项。  允许协议继续扩充。  支持即插即用（即自动配置）  支持资源的预分配。  1．IPv6首部  2.IPv6编址  128位  IPv6 数据报的目的地址可以是以下三种基本类型地址之一：  (1) 单播(unicast) 单播就是传统的点对点通信。  (2) 多播(multicast) 多播是一点对多点的通信。  (3) 任播(anycast) 这是 IPv6 增加的一种类型。任播的目的站是一组计算机，但数据报在交付时只交付其中的一个，通常是距离最近的一个。  4.8.4 从 IPv4 向 IPv6 过渡  用双协议栈  使用隧道技术从 IPv4 到 IPv6 过渡  作业  1. 5-08  2. 5-11  课堂讨论题  两台计算机通过一条双向不可靠（可能出现比特差错、分组丢失）信道连接，请设计一个方法实现发送方到接收方的单向可靠数据通信（无差错、无丢失、不失序、不重复）。  先解决以上基本问题，再考虑若发送方和接收方之间的往返传播时延很大，你的方法效率如何？如何改进？    参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 板书  通过图例说明IP多播的用途和重要性  简单介绍IP多播的特点和优点  理解IGMP和多播选路的各自的作用  通过图例讲解IGMP的作用和作用范围  通过图例说明多播路由选择协议的作用  板书  板书  通过例子说明为何需要虚拟专用网，虚拟专用网实现中的隧道技术和协议封装  通过图例讲解，关键是让学生理解IP隧道技术的原理  板书  让学生了解IPv6的引入的变化  强调IPv6首部的简洁性  强调地址空间的大小  让学生了解双栈和隧道的区别 |

**第14讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：运输层概述  目的要求：理解运输层的作用、理解运输层复用与分用、理解端口号。  重点难点：运输层复用与分用  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  §5 运输层  5.1 运输层协议概述  5.1.1 进程之间的通信  运输层为相互通信的应用进程提供了逻辑通信    两个主机进行通信实际上就是两个主机中的应用进程互相通信。  应用进程之间的通信又称为端到端的通信。  运输层的一个很重要的功能就是复用和分用。应用层不同进程的报文通过不同的端口向下交到运输层，再往下就共用网络层提供的服务。  “运输层提供应用进程间的逻辑通信”。“逻辑通信”的意思是：运输层之间的通信好像是沿水平方向传送数据。但事实上这两个运输层之间并没有一条水平方向的物理连接。  5.1.2 运输层的两个主要协议  1. TCP/IP 的运输层有两个不同的协议：  (1) 用户数据报协议 UDP (User Datagram Protocol)  TCP 传送的协议数据单元是 TCP 报文段  (2) 传输控制协议 TCP (Transmission Control Protocol)  UDP 传送的协议数据单元是 UDP 报文  2. TCP 与 UDP的区别  UDP 在传送数据之前不需要先建立连接。对方的运输层在收到 UDP 报文后，不需要给出任何确认。虽然 UDP 不提供可靠交付，但在某些情况下 UDP 是一种最有效的工作方式。  TCP 则提供面向连接的服务。TCP 不提供广播或多播服务。由于 TCP 要提供可靠的、面向连接的运输服务，因此不可避免地增加了许多的开销。这不仅使协议数据单元的首部增大很多，还要占用许多的处理机资源。  5.1.3 运输层的端口  端口号(protocol port number)  在运输层使用协议端口号(protocol port number)，或通常简称为端口(port)，来帮助标识目的或源应用进程。  端口号可以看作是应用进程的运输层地址。  在协议栈层间的抽象的协议端口是软件端口。  路由器或交换机上的端口是硬件端口。  硬件端口是不同硬件设备进行交互的接口，而软件端口是应用层的各种协议进程与运输实体进行层间交互的一种地址。  端口用一个 16 位端口号进行标志。  端口号只具有本地意义，即端口号只是为了标志本计算机应用层中的各进程。在因特网中不同计算机的相同端口号是没有联系的。  三类端口：  (1) 熟知端口，数值一般为 0~1023。  (2) 登记端口号，数值为1024~49151，为没有熟知端口号的应用程序使用的。使用这个范围的端口号必须在 因特网号码管理局 登记，以防止重复。  (3) 客户端口号或短暂端口号，数值为49152~65535，留给客户进程选择暂时使用。当服务器进程收到客户进程的报文时，就知道了客户进程所使用的动态端口号。通信结束后，这个端口号可供其他客户进程以后使用。  5.2 用户数据报协议 UDP  5.2.1 UDP 概述  UDP 只在 IP 的数据报服务之上增加了很少一点的功能，即端口的功能和差错检测的功能。  虽然 UDP 用户数据报只能提供不可靠的交付，但 UDP 在某些方面有其特殊的优点。  UDP 的主要特点  (1) UDP 是无连接的，即发送数据之前不需要建立连接。  (2) UDP 使用尽最大努力交付，即不保证可靠交付，同时也不使用拥塞控制。  (3) UDP 是面向报文的。UDP 没有拥塞控制，很适合多媒体通信的要求。  (4) UDP 支持一对一、一对多、多对一和多对多的交互通信。  (5) UDP 的首部开销小，只有 8 个字节。  5.2.2 UDP 的首部格式    5.3 传输控制协议 TCP 概述  5.3.1 TCP 最主要的特点  TCP 是面向连接的运输层协议。  每一条 TCP 连接只能有两个端点(endpoint)，每一条 TCP 连接只能是点对点的（一对一）。  TCP 提供可靠交付的服务。  TCP 提供全双工通信。  面向字节流。  TCP 面向流的概念    应当注意  TCP 连接是一条虚连接而不是一条真正的物理连接。  TCP 对应用进程一次把多长的报文发送到TCP 的缓存中是不关心的。  TCP 根据网络情况决定一次发送多少个字节（一个报文段）  UDP 发送的报文长度是应用进程给出的。  TCP 可把太长的数据块划分短一些再传送。TCP 也可等待积累有足够多的字节后再构成报文段发送出去。  5.3.2 TCP 的连接  TCP 把连接作为最基本的抽象。  每一条 TCP 连接有两个端点。  TCP 连接的端点不是主机，不是主机的IP 地址，不是应用进程，也不是运输层的协议端口。TCP 连接的端点叫做套接字(socket)或插口。  端口号拼接到(contatenated with) IP 地址即构成了套接字。  套接字 (socket)  套接字 socket = (IP地址: 端口号)  每一条 TCP 连接唯一地被通信两端的两个端点（即两个套接字）所确定。即：  TCP 连接 ::= {socket1, socket2}  = {(IP1: port1), (IP2: port2)}  补充： 网络地址转换 NAT  (Network Address Translation)  1. 概念  网络地址转换 NAT 方法于1994年提出。  需要在专用网连接到因特网的路由器上安装 NAT 软件。装有 NAT 软件的路由器叫做 NAT路由器，它至少有一个有效的外部全球地址 IPG。  所有使用本地地址的主机在和外界通信时都要在 NAT 路由器上将其本地地址转换成 IPG 才能和因特网连接。  2. NAT: 网络地址转换例子    3. 使用端口号的NAT    4. NAT的特点  对所有本地网络主机只用少数几个对外IP地址（节省IP地址）  能够改变本地网络中的设备地址，而不必通知外部  本地网络中的设备不显式地可寻址、由外部所见(增强安全性)  通信必须由内部发起，专网主机不能充当因特网服务器  作业  1. 5-08  2. 5-11  课堂讨论题  两台计算机通过一条双向不可靠（可能出现比特差错、分组丢失）信道连接，请设计一个方法实现发送方到接收方的单向可靠数据通信（无差错、无丢失、不失序、不重复）。  先解决以上基本问题，再考虑若发送方和接收方之间的往返传播时延很大，你的方法效率如何？如何改进？    参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 板书  板书  根据图例讲解运输层的作用和进程间的通信  强调“逻辑通信”的概念  板书  突出UDP和TCP的区别  板书  理解端口就是运输层地址的概念  让学生理解为什么需要端口号  板书  板书  UDP与IP的不同  强调为何需要UDP  板书  图例讲解  关键是端口号和校验和  板书  板书  关键是让学生理解连接的概念  通过图例讲解字节流的概念  板书  与UDP比较讲解面向连接和无连接复用的区别  板书  关键是讲清楚为什么需要NAT  NAT解决什么问题  图示讲解  通过例子讲解NAT的基本工作原理  图示讲解  通过例子讲解使用端口号的NAT  要使学生理解为何要使用端口号  要突出讲解NAT的跨层特性和某些对应用的影响  通过课堂讨论题让学生自己设计一个简单的可靠传输协议，有助于理解下次课内容，激发学生的创新意识 |

**第15讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：TCP的可靠数据传输  目的要求：掌握TCP可靠传输原理、流量控制和超时时间的计算。  重点难点：可靠传输原理和流量控制  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  回顾与引入  连续 ARQ\GBN协议与累积确认  5.6 TCP 可靠传输的实现  1. TCP可靠传输机制  TCP 连接的每一端都必须设有两个窗口  一个发送窗口和一个接收窗口。  TCP 的可靠传输机制用字节的序号进行控制。TCP 所有的确认都是基于序号而不是基于报文段。  TCP 两端的四个窗口经常处于动态变化之中。  TCP连接的往返时间 RTT 也不是固定不变的。需要使用特定的算法估算较为合理的重传时间。  TCP 面向流的概念  2. TCP报文首部字段中可靠传输相关字段    3. 举例    4. TCP与GBN的区别  接收窗口大小不为1，发送窗口和接收窗口大小动态变化。  TCP 标准没有规定对不按序到达的数据应如何处理。通常是先临时存放在接收窗口中，等到字节流中所缺少的字节收到后，再按序交付上层的应用进程。  TCP 要求接收方必须有累积确认的功能。  发生超时，TCP发送方仅对超时的分组重传。  5. TCP的发送窗口与接收窗口    6. 发送缓存    7. 接收缓存    5.7 TCP 的流量控制  5.7.1 利用滑动窗口实现流量控制  一般说来，我们总是希望数据传输得更快一些。但如果发送方把数据发送得过快，接收方就可能来不及接收，这就会造成数据的丢失。  流量控制(flow control)就是让发送方的发送速率不要太快，要让接收方来得及接收。  利用滑动窗口机制可以很方便地在 TCP 连接上实现流量控制。    5.6.3 选择确认 SACK（不要求）  (Selective ACK)  累积确认的缺点是无法对已正确到达接收方但失序的数据，可能会因超时导致这些数据的无效重传。  一些TCP实现采用选择确认  接收方收到序号在接收窗口内的失序字节时，在TCP首部SACK选项中准确告诉发送方收到了哪些失序的数据块，使发送方不要再重复发送这些已收到的数据。  5.6.2 超时重传时间的选择  重传机制是 TCP 中最重要和最复杂的问题之一。  1. 往返时延的方差很大  由于 TCP 的下层是一个互联网环境，IP 数据报所选择的路由变化很大。因而运输层的往返时间的方差也很大。    2. 加权平均往返时间  新的RTTS = (1−α)×(旧的RTTS)+α×(新的RTT样本) (5-4)  3. 超时重传时间 RTO (RetransmissionTime-Out)  RTO 应略大于上面得出的加权平均往返时间 RTTS。  RTO = RTTS + 4 × RTTD (5-5)  RTTD 是 RTT 的偏差的加权平均值：  新的 RTTD = (1 − β) × (旧的RTTD)  + β × ⏐RTTS − 新的 RTT 样本⏐ (5-6)  4. Karn 算法  重传时无法正确测量RTT    Karn 算法  在计算平均往返时间 RTT 时，只要报文段重传了，就不采用其往返时间样本。  报文段每重传一次，就把RTO增大一些：  新的 RTO = γ × (旧的 RTO)  作业  1. 5-23  2. 5-26  3. 5-30  预习作业  预习5.6.2、5.8（5.8.3不要求），回答以下问题：  1. 什么是拥塞控制？  2. TCP拥塞控制的基本思想是什么（用3句话总结）？  参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 板书  板书  先简单介绍一下TCP可靠传输的主要机制  板书  介绍TCP报文首部字段中可靠传输相关字段  通过举例说明TCP的可靠传输  与GBN比较学习  要让学生理解发送窗口和接收窗口的作用  关键是发送缓存与发送窗口的关系  关键是接收缓存与接收窗口的关系  板书  板书  通过实例，结合图示与板书讲解流量控制  简单提一下提一下SACK要解决的问题  板书  板书  板书  通过图示讲解说明为什么超时重传时间的选择在TCP中很重要  板书  突出加权平均的物理意义  板书  超时重传时间 RTO与RTTD的关系  图示讲解为什么不能对重传报文段进行估计往返时延 |

**第16讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：TCP连接管理与拥塞控制机制  目的要求：理解TCP为何需要建立连接、掌握TCP建立连接和释放连接的过程；掌握拥塞控制的基本概念和TCP的拥塞控制机制的基本原理。  重点难点：三次握手、TCP的拥塞控制机制  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  拥塞控制  目的要求：  教学内容与时间安排:  5.9 TCP 的运输连接管理 1. 运输连接的三个阶段  运输连接就有三个阶段，即：连接建立、数据传送和连接释放。运输连接的管理就是使运输连接的建立和释放都能正常地进行。  连接建立过程中要解决以下三个问题：  要使每一方能够确知对方的存在。  要允许双方协商一些参数（如最大报文段长度，最大窗口大小，服务质量等）。  能够对运输实体资源（如缓存大小，连接表中的项目等）进行分配。  客户服务器方式  TCP 连接的建立都是采用客户服务器方式。  主动发起连接建立的应用进程叫做客户(client)。  被动等待连接建立的应用进程叫做服务器(server)。  2. TCP报文段首部中与TCP连接管理相关的字段    3. TCP建立连接的过程（三次握手）    三次握手的原因  4. TCP释放连接的过程  提问：为何要超时等待？  7.4.8 TCP 的有限状态机(不要求)  每台机器都要对每个TCP连接维护其状态。  TCP 连接表对每个连接都登记了其连接信息。除本地和远地的 IP 地址和端口号外，还要记录每一个连接所处的状态。  5.8 TCP的拥塞控制 5.8.1 拥塞控制的一般原理  1. 拥塞控制的概念  在某段时间，若对网络中某资源的需求超过了该资源所能提供的可用部分，网络的性能就要变坏——产生拥塞(congestion)。  出现资源拥塞的条件：  对资源需求的总和 > 可用资源 (5-7)  2. 网络拥塞的危害    理想吞吐量为100M  不加任何控制只能达到60M  当分组丢失时, 任何用于传输该分组的上游传输能力都被浪费!  3. 拥塞控制所起的作用    4. 拥塞控制与流量控制的关系  拥塞控制是一个全局性的过程，涉及到所有的主机、所有的路由器，以及与降低网络传输性能有关的所有因素。  流量控制往往指在给定的发送端和接收端之间的点对点通信量的控制。  流量控制所要做的就是抑制发送端发送数据的速率，以便使接收端来得及接收。  5. 拥塞控制方法  网络辅助的拥塞控制:  路由器为端系统提供反馈  端到端的拥塞控制:  不能从网络得到明确的反馈  从端系统根据观察到的时延和丢包现象推断出拥塞  这是TCP所采用的方法  5.8.2 几种拥塞控制方法(TCP的拥塞控制机制) 1. 拥塞窗口  发送方维持一个叫做拥塞窗口 cwnd (congestion window)的状态变量。拥塞窗口的大小取决于网络的拥塞程度，并且动态地在变化。发送窗口不能大于拥塞窗口。  发送方控制拥塞窗口的原则是：只要网络没有出现拥塞，拥塞窗口就再增大一些，以便把更多的分组发送出去。但只要网络出现拥塞，拥塞窗口就减小一些，以减少注入到网络中的分组数。  2. 慢开始  刚建立连接准备发送数据时不知道网络可用带宽情况，先慢慢发送，再逐步提高发送速率，试探网络可用带宽  在主机刚刚开始发送报文段时可先设置拥塞窗口 cwnd = 1（一个最大报文段 MSS 的数值）。  在每收到一个对新的报文段的确认后，将拥塞窗口加 1，即增加一个 MSS 的数值。  用这样的方法逐步增大发送端的拥塞窗口 cwnd，可以使分组注入到网络的速率更加合理。    注意：虽然初始拥塞窗口很小，但随时间以指数方式增长。  3. 拥塞避免  由于慢开始窗口增长很快，为避免很快又导致网络拥塞，在接近上次发生拥塞的地方就放慢窗口的增长速度，进入拥塞避免阶段  当发生拥塞时，将当时的拥塞窗口的一半（但不能小于2）设置为从慢开始到拥塞避免的门限： ssthresh  当 cwnd < ssthresh 时，使用慢开始算法。  当 cwnd > ssthresh 时，停止使用慢开始算法而改用拥塞避免算法，即使拥塞窗口 cwnd 按线性规律缓慢增长，即每经过一个往返时间 RTT 就把发送方的拥塞窗口 cwnd 加 1 ，而不是加倍 。  当 cwnd = ssthresh 时，既可使用慢开始算法，也可使用拥塞避免算法。  当网络出现拥塞时  无论在慢开始阶段还是在拥塞避免阶段，只要发送方判断网络出现拥塞（其根据就是没有按时收到确认），就要把慢开始门限 ssthresh 设置为出现拥塞时的发送方窗口值的一半（但不能小于2）。  然后把拥塞窗口 cwnd 重新设置为 1，执行慢开始算法。  这样做的目的就是要迅速减少主机发送到网络中的分组数，使得发生拥塞的路由器有足够时间把队列中积压的分组处理完毕。  慢开始和拥塞避免算法的实现举例    通过冗余ACK发现分组丢失    4. 快重传和快恢复  发送方只要一连收到三个重复确认就认为有报文段丢失，应当立即重传该报文段。  快重传并非取消重传计时器，而是在某些情况下可更早地重传丢失的报文段。  发现分组丢失，说明网络拥塞，应采取行动  快恢复算法  (1) 当发送端收到连续三个重复的确认时，就执行“乘法减小”算法，把慢开始门限 ssthresh 减半。(但不执行慢开始算法)。  (2)发送方认为网络拥塞不严重，因此不执行慢开始算法，即拥塞窗口 cwnd 现在不设置为 1，而是设置为慢开始门限 ssthresh 减半后的新数值，然后开始执行拥塞避免算法（“加法增大”），使拥塞窗口缓慢地线性增大。  连续收到三个重复的确认转入拥塞避免    作业  1. 5-39  预习作业  预习5.9（理解图5-31\5-32, 5.9.3不要求），回答以下问题：  TCP为什么要在传输数据前先要建立连接？  如何判断一个TCP报文段是一个连接请求报文？  如何判断一个TCP报文段是一个释放连接请求的报文？  参考资料：  1．《计算机网络—自顶向下方法与Internet特色》（第4版），（美）James F. Kurose Keith W. Ross著/陈鸣译，机械工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  本次课教学体会： | 板书  关键是让学生理解为何要建立连接，连接的建立过程中通信双方作了哪些准备工作  板书  图示讲解  介绍与连接管理相关的字段  板书  图示讲解  介绍TCP建立连接的基本过程  分析为什么要进行三次握手  板书  图示讲解  突出TCP连接的关闭是两个方向分别关闭的  提问  板书  板书  板书  板书  通过实例讲解网络拥塞所带来的危害，以及为什么会有这样的危害  板书  突出辩证思维  板书  本质区别和联系  板书  板书  板书  理解TCP控制流量的基本方法  板书  通过板书讲解  关键是让学生理解虽然初始拥塞窗口很小，但随时间以指数方式增长。  板书  突出为何需要拥塞避免  通过实例讲解拥塞控制的过程  通过实例引出快速重传  板书  通过提问  让学生理解对待拥塞现象为何要采取不同的控制行为 |

**第17讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：应用层协议原理、因特网目录服务DNS  目的要求：理解应用层协议原理，包括网络应用程序体系结构、进程通信、应用层协议的功能和作用、以及应用所需的服务和因特网运输层提供的服务。掌握DNS的功能和作用，理解其工作过程和原理。  重点难点：DNS的工作原理  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  §6 应用层  内容回顾与本次课内容介绍  一、应用层协议原理(§6.1)  (一)概述  1、网络应用程序例子；  2、在端系统之间的网络应用通信示意图。  (二)网络应用程序体系结构  1、应用程序体系结构；  2、客户机/服务器体系结构（图例）；  3、P2P体系结构（图例）；  4、混合体系结构。  (三)进程通信  1、客户机和服务器进程；  2、套接字；  3、应用进程、套接字和运输协议的关系图；  4、端进程寻址。  (四)应用层协议  1、应用层协议定义的内容；  2、应用层协议和网络应用的区别（实例说明）。  (五)应用需要什么服务  1、可靠数据传输；  2、实时性；  3、部分应用对服务的要求对照表。  (六)因特网运输协议提供的服务  1、TCP服务；  2、UDP服务；  3、部分应用使用的运输协议。  二、DNS：因特网目录服务(§6.5) 45 分钟  1. 主机名和IP地址；  2. 为何需要DNS。  (一)DNS提供的服务  1. DNS及其功能；  2. 举例说明访问网页时如何利用DNS获得IP地址；  3. DNS提供的一些重要服务。  (二)DNS工作机理概述  1. 分布式、层次数据库；  2. DNS服务器；  3. 递归查询和迭代查询（图例）；  4. DNS缓存。  (三)DNS记录和报文  1. DNS记录4元组；  2. DNS报文格式；  3. 在DNS数据库中插入记录。  回顾与小结： 5 分钟   1. 网络应用程序体系结构、进程通信； 2. 应用层协议的功能和作用； 3. 应用所需的服务和因特网运输层提供的服务； 4. 为何需要DNS； 5. DNS的工作原理。   作业与思考题：  1．简述应用层协议定义的内容。  2．DNS有哪两种查询方式，简述这两种方式。  参考资料：  1．《计算机网络》（第4版），谢希仁编著，电子工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  3．《计算机网络与互联网》，（美）Douglas E. Comer著/徐良贤等译，电子工业出版社。  本次课教学体会： | 此处板书  幻灯并讲解：强调应用层位于网络的端系统中。  此处板书  幻灯并讲解：  此处重点强调客户机/服务器体系结构，其他略讲。  此处板书  幻灯并讲解：使学生理解客户机/服务器的概念，理解套接字接口的作用。  此处板书  幻灯并讲解：重点是应用层协议要规定什么。  此处板书  幻灯并讲解：使学生理解不同应用对网络传输有不同的要求。  此处板书  幻灯并讲解：从服务的角度介绍TCP和UDP。  此处板书  幻灯并讲解：使学生理解DNS的目的。  此处板书  幻灯并讲解：使学生理解DNS能干什么。  此处板书  幻灯并讲解：使学生掌握DNS工作原理，各DNS服务器的作用。  此处板书  幻灯并讲解：使学生理解DNS是如何维护信息的。 |

**第18讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：Web应用和HTTP协议  目的要求：掌握Web应用的基本工作原理，掌握HTTP的三种连接方式，掌握Cookie的用途和基本工作原理，掌握Web缓存的工作原理和作用。  重点难点：HTTP的三种连接方式  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  内容回顾与本次课内容介绍  一、Web应用和HTTP协议(§6.2)  (一) Web应用和HTTP概述  1. Web应用的地位  2. 术语：对象、基本HTML文件、浏览器、Web服务器等；  2. HTTP请求与响应（图例）  (二)非持久连接和持久连接  1. 非持久连接的工作过程（图例）；  2. 并行连接；  3. 持久连接的工作过程（图例）；  4. 非流水线方式和流水线方式。  (三)HTTP报文格式  1. HTTP请求报文（图例）；  2. HTTP响应报文（图例）。  (四)Cookie技术  1. Cookie技术的基本工作原理（图例）；  2. Cookie技术的用途。  (五)Web缓存  1. Web缓存工作原理（图例）；  2. 条件GET方法。  回顾与小结：   1. Web应用的基本工作原理； 2. HTTP的三种连接方式； 3. Cookie的用途和基本工作原理； 4. Web缓存的工作原理和作用。   作业与思考题：  1．某网页包含3个对象（例如3幅图片），分别画出持久方式非流水线和持久方式流水线方式下，访问该网页时浏览器和Web服务器之间的交互图（不包括建立连接的过程）。  2．简述Web缓存器的作用和工作原理。  3．习题7  参考资料：  1．《计算机网络》（第4版），谢希仁编著，电子工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  3．《计算机网络与互联网》，（美）Douglas E. Comer著/徐良贤等译，电子工业出版社。  本次课教学体会： | 此处板书  幻灯并讲解：让学生对Web应用的基本工作原理有一个整体的认识。  此处板书  幻灯并讲解：比较不同连接方式的效率。  此处板书  幻灯并讲解：通过分析报文格式讲解协议功能。  此处板书  幻灯并讲解：要理解为何需要Cookie技术。  此处板书  幻灯并讲解：理解Web缓存带来的好处。 |

**第19讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：文件传送协议、因特网电子邮件  目的要求：掌握文件传送、电子邮件等网络应用的工作原理。通过应用层协议实例加深对应用层协议功能和作用的理解。掌握SMTP、POP3和IMAP的区别。  重点难点：SMTP、POP3和IMAP的区别  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  时间地点：  教学内容与时间安排:  内容回顾与本次课内容介绍  一、文件传送协议(§6.3)  1. FTP的功能（图例）；  2. 控制连接和数据连接（图例）；  3. FTP命令和应答。  二、电子邮件(§6.4)  1. 因特网电子邮件总体描述（图例）；  2. 术语：用户代理、邮件服务器、简单邮件传送协议、邮箱；  (一)SMTP  1. SMTP的基本操作过程（图例）；  2. 实例说明SMTP工作过程。  (二)与HTTP的对比  1. 拉协议；  2. 推协议；  3. 编码；  4. 对象封装。  (三)邮件报文格式和MIME  1. 非ASCII编码数据的MIME扩展；  2. 发送的报文格式；  3. 接收的报文格式。  (四)邮件访问协议  提问：服务器能用SMTP将邮件发送给用户代理吗？  提问：用户能用SMTP从服务器下载邮件吗？  1. POP3；  2. IMAP；  3. 基于Web的电子邮件。  回顾与小结：   1. 文件传送、电子邮件等网络应用的工作原理； 2. 应用层协议功能和作用。   作业与思考题：  1．电子邮件系统为何不只使用一种协议来实现，而要使用SMTP和POP3两种协议？  参考资料：  1．《计算机网络》（第4版），谢希仁编著，电子工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  3．《计算机网络与互联网》，（美）Douglas E. Comer著/徐良贤等译，电子工业出版社。  本次课教学体会： | 此处板书  幻灯并讲解：理解FTP的基本工作过程和原理。  此处板书  幻灯并讲解：使学生了解电子邮件系统的构成。  建议学生利用telnet与SMTP服务器进行直接对话。  此处板书  幻灯并讲解：通过比较加深对两个协议的理解。  此处板书  幻灯并讲解：使学生理解MIME的作用。  此处板书  通过问题引出邮件访问协议。  幻灯并讲解：使学生理解为何要有邮件访问协议。 |

**第20讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：P2P文件共享、TCP套接字编程、UDP套接字编程  目的要求：掌握P2P文件共享的基本原理。掌握集中目录、洪泛查询和分层覆盖网络三种方式的区别和特点。了解套接字的工作原理和套接字编程的基本方法。  重点难点：P2P文件共享的基本原理  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  教学内容与时间安排:  6.7 P2P文件共享  P2P文件共享应用介绍  6.7.1 集中式目录  1. 集中式目录对等模式（图例）；  2. 集中式目录方式的问题。  6.7.2 查询洪泛  1. 覆盖网络的概念；  2. 洪泛查询；  3. 限范围的洪泛查询；  4. 加入和离开。  6.7.3 利用异质性  1. KaZaA中的组长；  2. 层次覆盖网络（图例）；  3. KaZaA的技术改进。  6.8 多媒体网络应用  多媒体网络应用往往数据量巨大，要求更高的网络带宽，并且与传统的弹性应用（如电子邮件、文件传输、网页浏览等）不同的是，对端到端时延和时延抖动高度敏感，但却可容忍少量的数据丢失。  6.8.1 实时多媒体数据传输中的问题  1. 音频和视频压缩技术  2. 时延抖动消除技术  3. 丢失分组恢复技术  6.8.2 实时传输协议RTP  实时传输协议RTP (Real-time Transport Protocol) 在UDP之上为实时多媒体网络应用提供端到端的传输服务。  6.8.3 流式存储音频/视频  从万维网服务器下载后播放  6.8.4 流式实况音频/视频  一个实况直播节目可能有大量用户在同时收听或收看，因此特别适合使用多播技术来实现流式实况音频/视频。  6.8.5 实时交互音频/视频  典型的实时交互应用包括因特网电话和视频会议。在这方面IETF和ITU制定了很多标准[RFC 3261-3266]。  6.9 TCP套接字编程  6.9.1 TCP套接字编程  1. 进程通过TCP套接字通信示意图；  2. 客户机套接字、欢迎套接字和连接套接字（图例）；  3. 可靠字节流的概念。  6.9.2一个Java客户机/服务器应用程序例子  1. 例子应用要实现的功能；  2. 客户机/服务器交换过程（图例）；  3. 客户机代码；  4. 服务器代码。  6.10 UCP套接字编程  6.10.1 UDP套接字编程  1. UDP与TCP的不同；  1. 例子应用要实现的功能；  2. 客户机/服务器交换过程（图例）；  3. 客户机代码；  4. 服务器代码。  6.11 应用层小结  1. 典型的请求/响应交互方式:  (1)客户机请求信息或服务  (2)服务器用数据进行响应  2. 报文格式:  (1)首部: 关于数据的信息字段  (2)数据: 被传输的信息  3. 控制报文和数据报文  (1)带内传输  (2)带外传输  4. 集中方式和非集中方式  5. 网络为应用提供的服务：可靠和不可靠数据传输  6. 复杂性放在网络的边缘  回顾与小结：  应用层小结(即第三部分)  作业与思考题：  1．简述P2P文件共享的集中式目录方式的工作原理。  2．简述P2P文件共享的洪泛查询方式的工作原理。  参考资料：  1．《计算机网络》（第4版），谢希仁编著，电子工业出版社。  2．《计算机网络》（第4版），（美）特南鲍姆著/潘爱民译，清华大学出版社；  3．《计算机网络与互联网》，（美）Douglas E. Comer著/徐良贤等译，电子工业出版社。  本次课教学体会： | 板书  使学生理解P2P应用能干什么。  板书  幻灯并讲解：使学生理解集中式目录方式工作原理和问题。  板书  幻灯并讲解：使学生理解集在覆盖网络上的洪泛查询的工作过程。  板书  幻灯并讲解：理解KaZaA的基本工作原理。  板书  板书  结合生活中实际在线视频播放的应用进行讲解  板书  在实际的RTP中是如何解决上面提到的问题  板书  板书  板书  此处板书  幻灯并讲解：使学生理解客户机套接字、欢迎套接字和连接套接字的作用，理解可靠字节流概念。  此处板书  幻灯并讲解：通过分析实例使学生了解如何编写一个TCP应用程序，理解TCP应用程序是如何访问运输层服务器的。  此处板书  幻灯并讲解：  通过分析实例使学生了解如何编写一个UDP应用程序，理解UDP应用程序是如何访问运输层服务器的。  最重要的是: 通过应用层协议实例学习了协议是什么 |

**第21讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：网络安全  目的要求：了解网络安全的概念，理解机密性与密码学、报文完整性的原理  重点难点：机密性与密码学的理解  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  教学内容与时间安排:  §7 网络安全  7.1 网络安全概述  7.1.1 安全威胁  计算机网络上的通信面临以下的四种威胁：  (1) 截获——从网络上窃听他人的通信内容。  (2) 中断——有意中断他人在网络上的通信。  (3) 篡改——故意篡改网络上传送的报文。  (4) 伪造——伪造信息在网络上传送。  截获信息的攻击称为被动攻击，而更改信息和拒绝用户使用资源的攻击称为主动攻击。  7.1.2 安全服务  1. 机密性(confidentiality) 确保计算机系统中的信息或网络中传输的信息不会泄漏给非授权用户。这是计算机网络中最基本的安全服务。  2. 报文完整性(message intergrity) 确保计算机系统中的信息或网络中传输的信息不被非授权用户篡改或伪造。后者要求对报文源进行鉴别。  3. 不可否认性(nonrepudiation) 防止发送方或接收方否认传输或接收过某信息。在电子商务中这是一种非常重要安全服务。  4. 实体鉴别(entity authentication) 通信实体能够验证正在通信的对端实体的真实身份，确保不会与冒充者进行通信。  5. 访问控制(access control) 系统具有限制和控制不同实体对信息源或其他系统资源进行访问的能力。系统必须在鉴别实体身份的基础上对实体的访问权限进行控制。  6. 可用性(availability) 确保授权用户能够正常访问系统信息或资源。拒绝服务攻击是可用性的最直接的威胁。  7.2 机密性与密码学  机密性应该是密码学最早的应用领域，但我们在后面几节将会看到密码学技术和鉴别、报文完整性以及不可否认性等是紧密相关的，可以说密码学是计算机网络安全的基础。  如果不论截取者获得了多少密文，但在密文中都没有足够的信息来唯一地确定出对应的明文，则这一密码体制称为无条件安全的，或称为理论上是不可破的。  如果密码体制中的密码不能被可使用的计算资源破译，则这一密码体制称为在计算上是安全的。  7.2.1对称密钥密码体制  所谓对称密钥密码体制是一种加密密钥与解密密钥相同的密码体制。  在这种加密系统中两个参与者共享同一个秘密密钥，如果用一个特定的密钥加密一条消息，也必须要使用相同的密钥来解密该消息。该系统又称为对称密钥系统。  数据加密标准DES原理：  在加密前，先对整个明文进行分组。每一个组长为 64 bit。  然后对每一个 64 bit 二进制数据进行加密处理，产生一组 64 bit 密文数据。  最后将各组密文串接起来，即得出整个的密文  使用的密钥为 64 bit（实际密钥长度为 56 bit，有 8 bit 用于奇偶校验)。  7.2.2 公钥密码体制  使用不同的加密密钥与解密密钥，加密密钥(即公开密钥) PK 是公开信息，而解密密钥(即秘密密钥) SK 是需要保密的  加密算法 E 和解密算法 D 也都是公开的  虽然秘密密钥 SK 是由公开密钥 PK 决定的，但却不能根据 PK 计算出 SK  发送者用加密密钥 PK 对明文 X 加密后，在接收者用解密密钥 SK 解密，即可恢复出明文，即  DSK(EPK(X)) ＝ X  加密和解密的运算可以对调，即  EPK(DSK(X)) ＝ X  DES基本流程  7.3 报文完整性  有时，通信双方并不关心通信的内容是否会被人窃听，而只关心通信的内容是否被人篡改或伪造，这就是报文完整性问题。  7.3.1报文摘要和报文鉴别码  使用加密就可达到报文鉴别的目的。但对于不需要保密，而只需要报文鉴别的网络应用，对整个报文的加密和解密，会使计算机增加很多不必要的负担。  更有效的方法是使用报文摘要MD (Message Digest)来进行报文鉴别。  7.3.2 数字签名  1.目的  接收者能够核实发送者对报文的签名  发送者事后不能抵赖对报文的签名  接收者不能伪造对报文的签名  2.采用公开密钥算法要比采用常规密钥算法更容易实现  3.采用公开密钥体制进行签名的前提是加密和解密互逆    作业与思考题  （1）怎样利用公开密钥密码系统进行数字签名？  本次课教学体会 | 板书  板书  通过生活中的实例来说明  板书  让学生理解安全服务的特点  板书  通过图示讲解加密系统的基本模型  板书  板书  与对称密钥密码体制进行对比教学  举例说明  板书  板书  突出使用摘要的好处  讲清楚报文鉴别并不需要具有可逆性  板书  与报文鉴别码进行比较  为何具有不可抵赖性  在讲解过程中注意各种安全机制的关系和区别。 |

**第22讲**

|  |  |
| --- | --- |
| **内 容** | **备 注** |
| 讲课题目：网络安全  目的要求：理解实体鉴别的作用，了解对称密钥的分发与认证、因特网网络安全协议、防火墙和入侵检测系统的原理和作用。  重点难点：理解实体鉴别的作用  方法步骤：课堂讲解与实例介绍  器材保障：电脑、投影  教学内容与时间安排:  7.4实体鉴别  实体鉴别就是鉴别通信对端实体的身份，即验证正在通信的对方确实是所认为的通信实体，这需要使用鉴别协议。  鉴别协议通常在两个通信实体运行其他协议（例如，可靠数据传输协议、路由选择协议或电子邮件协议）之前运行。  最简单的实体鉴别过程：  A 发送给 B 的报文使用对称密钥 KAB的被加密，用共享对称密钥 KAB 进行解密，因而鉴别了实体 A 的身份。  该方法会遭受重发攻击。  使用不重数进行鉴别：  7.5 密钥分发和认证  由于密码算法是公开的，密钥系统的安全性依赖于密钥的安全保护。在对称密钥密码体制中，通信双方要共享同一个秘密的密钥，如何将密钥分发到通信的双方是一个需要解决的问题。  对于公钥密码体制，虽然不需要共享密钥，公钥可以发布在报纸或网站上，但如何验证该公钥确实是某实体真正的公钥仍然是一个问题。  7.5.1 对称密钥的分发  目前常用的密钥分发方式是设立密钥分发中心 KDC (Key Distribution Center)。  用户 A 和 B 都是 KDC 的登记用户，并已经在 KDC 的服务器上安装了各自和 KDC 进行通信的主密钥（master key）KA 和 KB  7.5.2 公钥的认证  需要有一个值得信赖的机构——即认证中心CA (Certification Authority)，来将公钥与其对应的实体（人或机器）进行绑定(binding)。  认证中心一般由政府出资建立。每个实体都有CA 发来的证书(certificate)，里面有公钥及其拥有者的标识信息。此证书被 CA 进行了数字签名。任何用户都可从可信的地方获得认证中心 CA 的公钥，此公钥用来验证某个公钥是否为某个实体所拥有。有的大公司也提供认证中心服务。  7.6 网络安全协议  7.6.1 网络层安全协议: IPsec  IPSec是为因特网网络层提供安全服务的一组协议。IPSec是一个协议名称，是IP Security （意思是IP安全）的缩写。  提供两种运行方式：  1. 传输方式    2. 隧道方式    7.7 系统安全：防火墙与入侵检测  恶意用户或软件通过网络对计算机系统的攻击已成为当今计算机安全最严重的威胁之一。  7.7.1 防火墙(firewall)  防火墙(firewall)是把一个组织的内部网络与其他网络（通常就是因特网）隔离开的软件和硬件的组合。根据访问控制策略，它允许一些分组通过，而禁止另一些分组通过。访问控制策略由使用防火墙的组织根据自己的安全需要自行制订。  防火墙技术一般分为两类:  (1) 分组过滤路由器——是一种具有分组过滤功能的路由器，它根据过滤规则对进出内部网络的分组执行转发或者丢弃（即过滤）。过滤规则基于分组的网络层或运输层首部的信息，例如：源/目的IP地址、源/目的端口、协议类型、标志位等等。  (2)应用网关——在应用层通信中扮演报文中继的角色。一种网络应用需要一个应用网关。在应用网关中可以实现基于应用层数据的过滤和高层用户鉴别。  7.7.2 入侵检测系统  入侵检测系统(Intrusion Detection System, IDS) 对进入网络的分组执行深度分组检查，当观察到可疑分组时，向网络管理员发出告警或执行阻断操作（由于IDS的“误报”率通常较高，多数情况不执行自动阻断）。  IDS能用于检测多种网络攻击，包括网络映射、端口扫描、DoS攻击、蠕虫和病毒、系统漏洞攻击等。  入侵检测方法一般可以分为基于特征的入侵检测和基于异常的入侵检测两种。  作业与思考题  （1）防火墙与入侵检测系统的差异？  本次课教学体会 | 板书  用启发的方式让学生发现使用简单加密进行鉴别会遭受重发攻击  用图示讲解使用不重数是如何抵御重发攻击的  板书  板书  结合图例讲解  板书  板书  板书  两种使用模式要对比教学(从用途，保护范围、封装方式等)  板书  板书  突出讲解为什么需要防火墙  板书  两种技术对比教学  板书  简单介绍  板书 |

**实验一**

| **内 容** | **备 注** |
| --- | --- |
| 实验题目：局域网组网  实验时间：2学时  目的要求：1.深入理解局域网基本概念  2.了解局域网组网中的软硬件以及传输介质  3.掌握双绞线的制作方法  重点难点：掌握双绞线的制作方法  方法步骤：学生根据实验步骤自行完成所有练习后教员进行检查  器材保障：电脑、网络测试器、压线钳、水晶头、双绞线  实验内容与步骤：  一、常见网络设备  1.集线器（HUB）：  是扩充网络、连接更多工作站的网络设备，采用共享媒体方式，只具有放大和重发数据的功能。  2.交换机：  具有处理数据的功能，支持点对点全双工交换模式，数据传输能力比HUB要强。  3、RJ45接头：双绞线的接头，俗称水晶头。  4、网卡  网卡的功能  （1）数据的封装与解封：发送、接收  （2）链路管理：实现CSMA/CD协议  （3）编码与译码：曼彻斯特编解码  二、制作工具和材料  1.制作工具  网线制作工具是RJ-45压线钳，该工具上有三处不同的功能，最前端是剥线口，它用来剥开双绞线外壳。中间是压制RJ-45头工具槽，这里可将RJ-45头与双绞线合成。离手柄最近端是锋利的切线刀，此处可以用来切断双绞线，见下图。    RJ-45压线钳  2.制作所需材料  网线制作材料是RJ-45头和双绞线。由于RJ-45头像水晶一样晶莹透明，所以也被俗称为水晶头，每条双绞线两头通过安装RJ-45水晶头来与网卡和集线器(或交换机路由器等)相连。而双绞线是指封装在绝缘外套里的由两根绝缘导线相互扭绕而成的四对线缆，它们相互扭绕是为了降低传输信号之间的干扰。  三、实验步骤  1.网线制作  (1)剪断:  利用压线钳的剪线刀口剪取适当长度的网线。    (2)剥皮:  压线钳的剪线刀口将线头剪齐,再将线头放入剥线刀口,让线头角及挡板,稍微握紧压线钳慢慢旋转,让刀口划开双绞线的保护胶皮,拔下胶皮。如下图所示    (注意:剥与大拇指一样长就行了，一般2～3cm，有一些双绞线电缆上含有一条柔软的尼龙绳，如果您在剥除双绞线的外皮时，觉得裸露出的部分太短，而不利于制作RJ-45接头时，可以紧握双绞线外皮，再捏住尼龙线往外皮的下方剥开，就可以得到较长的裸露线。)见下图。  剥线完成后的双绞线电缆如下图所示。  【小提示】网线钳挡位离剥线刀口长度通常恰好为水晶头长度，这样可以有效避免剥线过长或过短。剥线过长一则不美观，另一方面因网线不能被水晶头卡住，容易松动；剥线过短，因有包皮存在，太厚，不能完全插到水晶头底部，造成水晶头插针不能与网线芯线完好接触，当然也不能制作成功了，见下图。  (3)排序:  小心的剥开每一对线，因为我们是遵循EIA／TIA 568B的标准来制作接头，所以线对颜色是有一定顺序的，每对线都是相互缠绕在一起的,制作网线时必须将4个线对的8条细导线一一拆开,理顺,捋直,然后按照规定的线序排列整齐。如下图所示。    (4)剪齐：  把线尽量抻直（不要缠绕）、压平（不要重叠）、挤紧理顺（朝一个方向紧靠），然后用压线钳把线头剪平齐  (5)插入：  一手以拇指和中指捏住水晶头，使有塑料弹片的一侧向下，针脚一方朝向远离自己的方向，并用食指抵住；另一手捏住双绞线外面的胶皮，缓缓用力将8条导线同时沿RJ-45头内的8个线槽插入，一直插到线槽的顶端，见下图。    (6)压制：  确认所有导线都到位，并透过水晶头检查一遍线序无误后，就可以用压线钳制RJ-45头了。将RJ-45头从无牙的一侧推入压线钳夹槽后,用力握紧线钳(如果力气不够大,可以使用双手一起压),将突出在外面的针脚全部压入水晶并头内，见下图。    至此，这个RJ-45头就压接好了。下图是已完成的水晶头。  2.测试  把水晶头的两端都做好后即可用网线测试仪进行测试，如果测试仪上8个指示灯都依次为绿色闪过，证明网线制作成功。如果出现任何一个灯为红灯或黄灯，都证明存在断路或者接触不良现象，此时最好先对两端水晶头再用网线钳压一次，再测，如果故障依旧，再检查一下两端芯线的排列顺序是否一样，如果不一样，随剪掉一端重新按另一端芯线排列顺序制做水晶头。如果芯线顺序一样，但测试仪在重夺后仍显示红色灯或黄色灯，则表明其中肯定存在对应芯线接触不好。此时只好先剪掉一端按另一端芯线顺序重做一个水晶头了，再测，如果故障消失，则不必重做另一端水晶头，否则还得把原来的另一端水晶头也剪掉重做。直到测试全为绿色指示灯闪过为止。对于制作的方法不同测试仪上的指示灯亮的顺序也不同，如果是直通线测试仪上的灯应该是依次顺序的亮，如果做的是双绞线那测试仪的一段的闪亮顺序应该是3、6、1、4、5、2、7、8。  本次课教学体会 | 板书  板书  板书  板书  2~3人一把，结合实物进行介绍  本节课的重点  边操作边演示  然后学生自己操作  本节课的难点  此处要注意提醒学生压制到位  此处可提问学生，如有部分指示灯未亮怎么办  让学生制作完毕后挑几个人的作品进行讲评 |

**实验二**

| **内 容** | **备 注** |
| --- | --- |
| 实验题目：分析Web应用中的协议交互  实验时间：2学时  目的要求：1.掌握使用wireshark分析协议的基本方法  2.通过有目的地访问网络站点，分析web应用中的协议交互，掌握DNS协议的域名解析过程和HTTP协议的工作机制  重点难点：掌握使用wireshark分析协议的基本方法  方法步骤：学生根据实验步骤自行完成所有练习后教员进行检查  器材保障：连接校园网的计算机、Wireshark软件  实验内容与步骤：  一、几种协议简介  1.DNS协议与报文  DNS协议: 查询和应答报文，都有相同的报文格式，使用UDP。  2.HTTP协议  HTTP：超文本传输协议是万维网的应用层协议，客户机/服务器模式，一般有两种连接方式：非持久连接方式和持久连接方式  二、使用WireShark分析web中的协议交互  1.安装WireShark软件。  2.运行WireShark软件，阅读帮助文件user-guide-a4.pdf，配置过滤数据包。  三、请自主设计实验过程，完成下列内容：  （1）分析Web应用中域名解析的过程  （2）分析利用HTTP协议请求基本HTML文件的过程  （3）分析利用HTTP持久连接请求一个包含对象的网页的过程  （4）分析利用HTTP非持久连接请求一个包含对象的网页的过程  （5）分析利用HTTP协议进行有条件获取(Conditional GET)网页的过程  本次课教学体会 | 进行简要的理论讲解  引导学生安装软件并提醒注意事项  学生一边实验一边进行答疑 |

**实验三**

| **内 容** | **备 注** |
| --- | --- |
| 实验题目：配置路由器  实验时间：2学时  目的要求：1.学会使用网络模拟器软件Packet Tracer  2.掌握两级简单网络的设计与IP地址规划方法  3.掌握静态路由的配置  4.掌握RIP动态路由的配置  重点难点：掌握IP地址规划方法  方法步骤：学生根据实验步骤自行完成所有练习后教员进行检查  器材保障：连接校园网的计算机、Packet Tracer仿真软件  实验内容与步骤：  一、实验原理讲解  路由器可以使位于不同网段的主机进行通信，但是能通信的前提是对路由器进行正确配置，通常采用的路由选择可以分为哪两类呢？  1.静态路由选择：  人工编辑路由器的转发表  2.动态路由选择：  根据动态路由选择协议（如RIP）自动选择路径  二、使用Packet Tracer软件进行路由器配置  1.安装并运行Packet Tracer软件。  2.在Packet Tracer软件中搭建仿真模型。  3.在配置选项卡中选择CLI，进行IOS配置界面  4．观察RIP通信过程  三、请自主设计实验过程，完成下列内容  （1）设计交换机、路由器两级简单网络  （2）对网络中的各个网段进行IP地址规划  （3）配置路由器的静态路由，并观察分组的通信过程  （4）配置路由器的动态路由，并观察分组的通信过程  本次课教学体会 | 板书  板书  板书  带学生简单回忆相关原理  引导学生安装软件并提醒注意事项  让学生熟悉软件的应用  配置路由时注意与学生互动，加深映像  学生自主进行，教员进行辅导 |

**实验四**

| **内 容** | **备 注** |
| --- | --- |
| 实验题目：电子邮件服务器部署  实验时间：2学时  目的要求：1.掌握电子邮件服务器及客户端的配置与使用方法  2.通过实现本地电子邮件服务器用户与校园网电子邮件服务器用户之间邮件传输  重点难点：掌握电子邮件服务器及客户端的配置与使用方法  方法步骤：学生根据实验步骤自行完成所有练习后教员进行检查  器材保障：连接校园网的计算机、MDaemon电子邮件服务器软件  实验内容与步骤：  一、实验原理讲解  当我们从一个邮件服务器邮箱向另一个邮件服务器邮箱发送电子邮件（例如新浪邮箱向163邮箱发送邮件），邮件的传送过程是怎样的？  我们是否可以自己架设邮箱服务器呢？架设邮箱服务器又需要配置哪些元素呢？  二、DNS配置  配置邮箱服务器所需要的DNS域及相关资源记录（如smtp、pop3、邮件交换器MX）    三、MDaemon配置  注意域(电子邮件服务器所在域，如网易163.com)，端口(STMP:25、POP3:110)及IP地址 (邮件服务器)的配置。  提问：我们目前都比较熟悉使用浏览器访问邮箱的方式，那么怎样配置MDaemon才能让用户使用浏览器访问呢？  四、Outlook Express配置  帐户设置(通过此客户端收发邮件)，用户的电子邮件地址，邮件服务器（SMTP和POP3）的IP地址，端口。    五、请自主设计实验过程，完成下列内容  1.为自己所在的局域网部署电子邮件服务器；  2.通过自己的邮件服务器，使用Outlook Express客户端给teacher@lgdx.mtn邮箱发送邮件，并告知邮件服务器域名；  3.收到回复后，将回复再次回复(如何成功，说明接收邮件功能正常)；  4.采用Web方式（使用80端口）收发电子邮件；  5.通过Web方式访问邮件服务器时能创建邮箱帐户。  本次课教学体会 | 板书  提问讨论  板书  引导学生完成实验，并提醒学生做DNS的测试验证  板书  引导学生完成实验  引导学生去探索  板书  引导学生完成实验  学生自主完成 |

**实验五**

| **内 容** | **备 注** |
| --- | --- |
| 实验题目：无线局域网  实验时间：2学时  目的要求：1.掌握无线局域网基本组成和设备连接关系  2.学习使用无线路由器配置无线局域网的基本技能  重点难点：使用无线路由器配置无线局域网  方法步骤：学生根据实验步骤自行完成所有练习后教员进行检查  器材保障：连接校园网的计算机、Packet Tracer软件  实验内容与步骤：  一、通过Packet Tracer软件搭建无线接入实验网络  二、进行路由配置  三、验证是否能连通  四、学生自行重新组网练习  本次课教学体会 | 板书  让学生比较与家庭无线网络的异同，并  引导学生完成实验  提问，每个配置参数背后的原理，为什么要配置，如果配置不正确会出现什么问题  学生自主完成 |

**实验六**

| **内 容** | **备 注** |
| --- | --- |
| 实验题目：编写web代理服务器程序  实验时间：2学时  目的要求：1.掌握web代理的原理  2.深入理解套接字的概念  3.了解使用java语言进行网络编程  重点难点：了解使用java语言进行网络编程  方法步骤：学生根据实验步骤自行完成所有练习后教员进行检查  器材保障：连接校园网的计算机、Eclipse软件  实验内容与步骤：  一、实验原理讲解  1.用户配置浏览器: 通过代理服务器访问Web  参考实验指导书第99页相关设置。如果实验室机器上安装有Firefox、Chrome等其它浏览器，也可以向学生演示各种其它浏览器的设置位置。  2.浏览器发送HTTP 请求到代理服务器  3.代理服务器向原始服务器转发HTTP请求  4.代理服务器收到原始服务器的响应后再转发给客户机  提问：代理能不能基于网络层、运输层或者应用层开发，有什么区别？  二、Eclipse安装  在解压eclipse 压缩包后，双击eclipse.exe 即可运行eclipse  **二、Eclipse的使用**  先编译和运行 java 程序，保存后，eclipse 会自动对代码进行编译并生成类文件，右键选择需要运行的java 类，选择“Run As->Run…”。  把实验指导书上的代码复制粘贴到Eclipse中，然后运行ProxyCache.java。  此处如果学生之前没有学习过Java语言，那么就略过以下问题，如果学生学习过，那么有下列问题让学生思考并回答（可以写到实验报告上）：  ProxyCache.java：指导书第92页的6个问题；  HttpRequest.java：指导书第95页的5个问题；  HttpResponse.java：指导书第96页的4个问题；  三、请自主设计实验过程，完成下列内容  两个人一个小组，合作完成实验，独立撰写报告。  1.两个人相互配合，访问校园网的网页，并用WireShark抓包分析HTTP的交互过程  2.不使用代理服务器直接访问网页，并用WireShark抓包，并与之前的交互过程对比  本次课教学体会 | 此处主要是教员演示+板书  引导学生完成实验  引导学生完成实验  学生自主完成 |