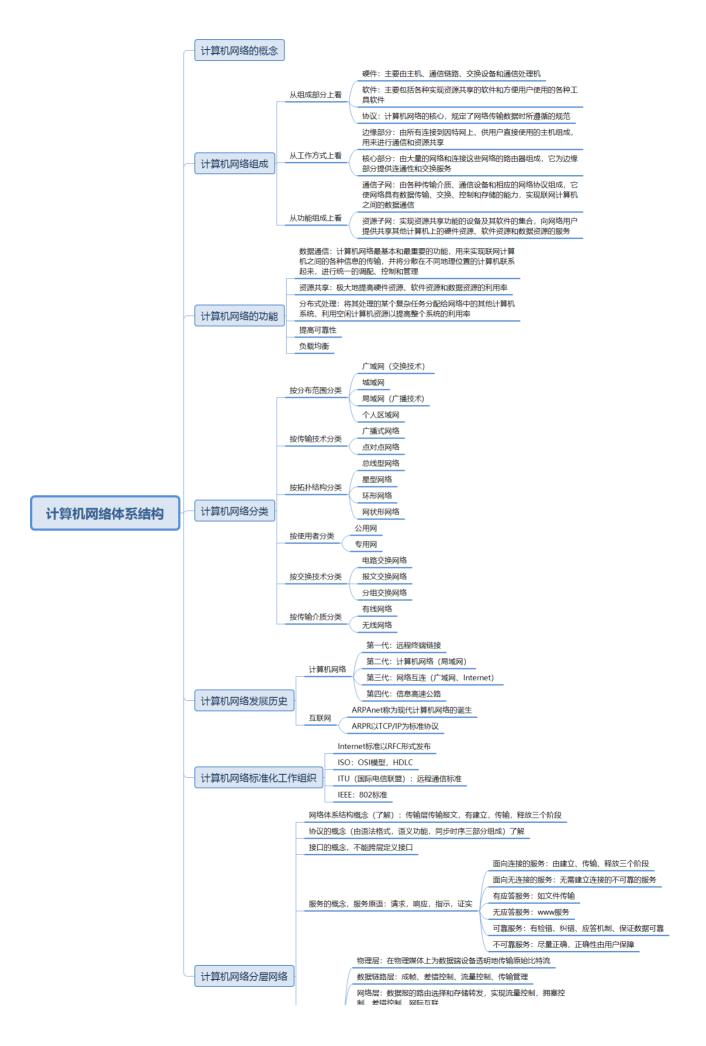
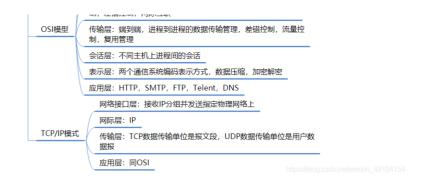
@TOC

相关课程链接

数据结构总结与知识网图 计算机网络知识总结及知识网图 操作系统总结及知识网图 计算机组成原理总结及知识网图 知识网图

第一章 计算机网络体系结构





计算机网络分成的基本原则:

1)每层都实现一种相对独立的功能,降低大系统的复杂度。 2) 各层之间界面自然清晰,易于理解,相互交流尽可能少。 3) 各层功能的精确定义独立于具体的实现方法,可以采用最适合的技术来实现。 4) 保持下层对上层的独立性,上层单向使用下层提供的服务。 5) 整个分层结构应能促进标准化工作。

TCP/IP模型和OSI参考模型的比较

相似点: 1) 二者都采取分层的体系结构,将庞大且复杂的问题划分为若干较容易处理的、范围较小的问题,而且分层的功能也大体相似。 2) 二者都是独立的协议栈的概念。 3) 二者都可以解决异构网络的互联,实现不同厂家的计算机之间的通信。不同点: 1) OSI参考模型精确定义了三个主要的概念:服务、协议和接口,这与现代面向对象程序设计思想很吻合,但TCP/IP模型并未明确区分这三个概念,不符合软件工程的思想。 2) OSI模型产生在协议发明之前俺,没有偏向于任何特定的协议,通用性良好。TCP/IP模型与之相反,先出现的是协议,模型是对已有协议的描述,不会出现与协议不匹配的情况,但不适用于任何塔器非TCP/IP的协议栈。 3) TCP/IP模型在设计之初就考虑到多种异构网络的互联问题,并将网际层作为一个单独的重要层次。OSI模型最初只考虑到用一种标准的公用数据网络将各种不同的系统互联。 4) OSI模型在网络层支持无连接和面向连接的通信,但在传输层仅有面向连接的通信。而TCP/IP模型在网际层仅支持无连接的通信模式,但传输层支持无连接和面向连接两种模式。

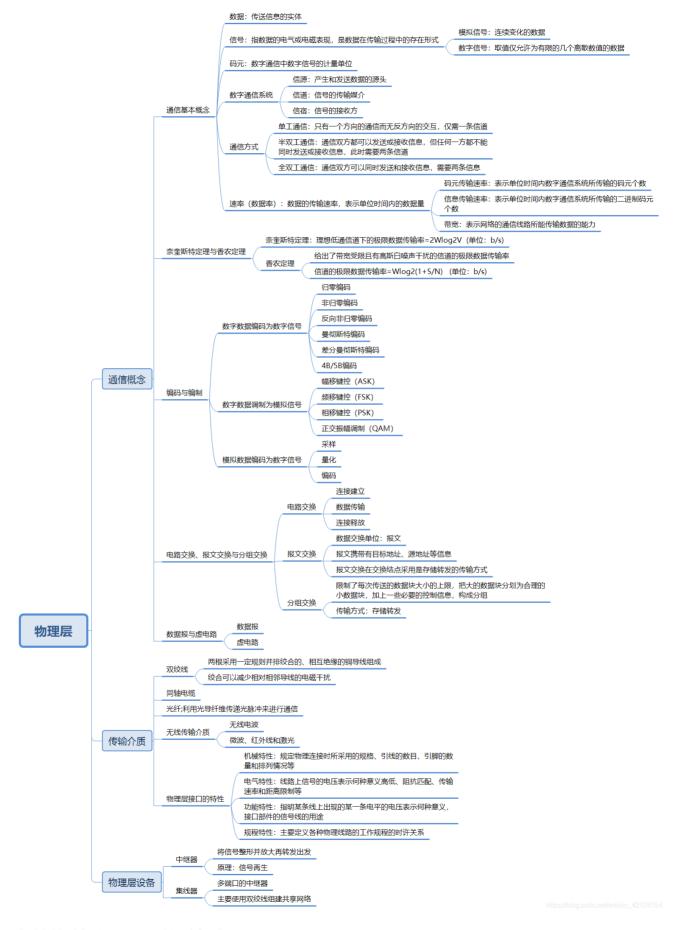
计算机网络与分布式计算机系统的主要区别

分布式系统主要的特点是,整个系统中的各个计算机对用户都是透明的。用户通过输入命令运行程序,但用户并不知道哪台计算机在为它运行程序。操作系统为用户选择一台最合适的计算机来运行其程序,并将运行的结果传送到合适的地方。 而**计算机网络**,用户必须先登录欲运行程序的计算机,然后按照计算机的地址,将程序通过计算机网络传送到该计算机上运行,最后根据用户的命令将结果传送到指定的计算机。 二者的区别主要在软件的不同。

端到端诵信与点到点诵信的区别

点到点通信 直接相连的结点之间的通信,只提供一台机器到另外一台机器之间的通信,不涉及程序或进程的概念。点到点通信不能保证数据传输的可靠性。 **端到端通信** 传输层为网络中的主机提供端到端通信。端到端通信是建立在点到点通信的基础上的,是由一段段的点到点通信通道构成的,是比点到点通信更高一级的通信方式,以完成应用程序(进程)之间的通信。"端"是指用户程序的端口,端口号标识了应用层中的不同进程。

第二章 物理层



1) 在任何信道中,码元传输的速率是有上限的。 2) 信道的频带越宽,就可用更高的速率进行码元的有效传输。 3) 奈氏准则给出了码元传输速率的限制,但并未对信息传输速率给出限制,即未对一个码元可以多少个二进制给出限制。

香农定理得到的结论

1) 信道的带宽或信道中的信噪比越大,信息的极限传输速率越高。2) 对一定的传输宽带和一定的信噪比,信息传输速率的上限是确定的。3) 只要信息的传输速率低于信道的极限传输速率,就能找到某种方法来实现无差错的传输。4) 香农定理得出的极限信息传输速率,实际信道能达到的传输速率要比它低不少。

电路交换的特点

优点 1) 通信时延小 2) 有序传输 3) 没有冲突 4) 使用范围广 5) 实时性强 6) 控制简单 **缺点** 1) 建立连接时间长 2) 线路独占 3) 灵活性差 4) 难以规格化

报文交换的特点

优点 1) 无需建立连接 2) 动态分配线路 3) 提高线路可靠性 4) 提高线路利用率 5) 提供多目标服务 **缺点** 1) 数据进入交换结点后要经历存储、转发这一过程,引起转发时延 2)报文交换对报文的大小没有限制,网络结点需要较大的缓存空间

分组交换的特点

- 1) 无建立时延 2) 线路利用率高 3) 简化了存储管理 4) 加速传输 5) 减少了出错概率和重发数据量 **缺点** 1) 存在传输时延。 2) 每块小数据块都需要加上源地址、目的地址和分组编号等额外信息。 3) 当分组交换
- 采用数据报服务时,可能会出现失序,丢失或重复分组,分组到达目的时需要对分组按序号进行排序等工作。

数据报服务

发送端发送一个报文时,再端系统中的高层协议先将报文拆成若干带有序号的数据单元,并在网络层加上地址等控制信息后形成数据分组。中间结点存储分组很短一段时间,找到最佳路由后,尽快转发每个分组。特点: 1) 发送分组前不需要建立连接。 2) 网络尽最大努力交付,传输不保证可靠性;为每个分组独立地选择路由,转发的路径可能不同,分组不一定按需到达目的结点。 3) 发送的分组中要包括发送端和接收端的完整地址,以便可以独立传输。 4) 分组在交换结点存储转发时,会带来一定的时延。 5) 网络具有冗余路径,对故障的适应能力强。 6) 存储转发的时延一般较小,提高网络的吞吐量。 7) 收发双方不独占某一链路,资源利用率较高。

虚电路

试图将数据报方式和电路交换方式结合起来,充分发挥两种方法的优点,以达到最佳的数据交换效果。再分组发送之前,要求再发送方和接收方建立一条逻辑上相连的虚电路,并且连接一旦建立,就固定了虚电路所对应的物理路径。分为三个阶段:虚电路建立,数据传输,虚电路释放 **特点**: 1) 虚电路通信链路的建立和拆除需要时间开销。 2) 虚电路的路由选择体现在连接建立阶段,连接建立后就确定了传输路径。 3) 虚电路提供了可靠的通信功能,能保证每个分组正确且有序到达。 4) 当网络中的某个结点或某条链路出现故障而彻底失效时,所有经过该结点或该链路的虚电路将遭到破坏。

物理接口的特性

1) 机械特性。规定物理连接时所采用的规格、引线的数目、引脚的数量和排列情况等。 2) 电气特性。线路上信号的电压高低、阻抗匹配、传输速率何距离限制等。 3) 功能特性。指明某条线上出现的某一电平的电压表示何种意义,接口部件的信号线的用途。 4) 规程特性。主要定义各种物理线路的工作规程和时序关系。

基带传输、频带传输和宽度传输的比较

基带传输:可以不经过调制就在信道上直接进行的传输方式,通常用于局域网。 **频带传输**:用数字信号对特定 频率的载波进行调制,将其变成适合于传送的信号后再进行传输。 **宽带传输**:借助频带传输,可将链路容量 分解成两个或多个信道,每个信道可以携带不同信号。

数据链路层

将物理层可能出差错的物理连接改造成逻辑上无差错的数据链路 发送帧不建立连接,收到帧不反馈;丢失帧由上层处理 无确认的无连接服务 应用: 实时通信或误码率较低的信道, 如以太网 发送帧不建立连接,接收帧必须发回确认 为网络层提供服务 有确认的无连接服务 适用于误码率较高的通信信道, 如无线通信 帧传输要建立数据链路、传输帧、释放数据链路 有确认的有连接服务 适用于可靠性实时性要求较高的场合 数据链路层连接的建立、维持和释放过程 链路管理 初始化帧序号,建立并维持连接 数据链路层的功能 帧定界: 将一段数据前后添加首部和尾部构成帧,首部和 尾部由控制信息确定帧的界限,即帧定界 帧定界、帧同步和透明传输 帧同步:接收方能从接受的二进制比特流中区分出起始和终止 透明传输: 无论所传数据是什么样的比特组合都能在链路上传送 限制发送方的数据流量,使其不超过接收方的接受能力 流量控制 数据链理财提供的是相邻两个节占间的流量控制 确认接收方接收的数据是否出错,错误包括位错与帧错 差错控制 通过CSC校验等发现位错,通过自动重传请求方式重传该错误的帧 帧错:指帧的丢失,重读,失序等。 字符计数法: 在帧头部使用一个计数字段来标明帧内字符数 字符填充的首尾定界符法: 使用一些特定的字符来定界帧的开始和结束 组帧 零比特填充的首尾标志法:使用特定的比特模式,即01111110来标志一帧的开始与结束 违规编码法: 借用违规编码序列来定界帧的起始和终止 奇偶校验码 检错编码 循环冗余码 差错控制 纠错编码 海明码 流量控制的基本方法: 由接收方控制发送方发送数据的速率 停止-等待协议;每次只允许发送一帧,等待接收方确认信息后再发 流量控制 接收窗口: 发送方维持一组连续的允许发送的帧的序列 滑动窗口协议 接收窗口:接收方维持一组连续的允许接收帧的序号 数据链路层的可靠传输通常使用确认和超时重传两种机制来完成 停止-等待协议 可靠传输机制 退后N帧协议 选择重传协议 频分多路复用 (FDM) 时分多路复用 (TDM) 信道划分介质访问控制 波分多路复用 (WDM) 码分多路复用 (CDM) 纯ALOHA协议: 当网络中的任何一个站点需要传送数据时, 可以 不进行任何检测就发送数据 ALOHA协议 时隙ALOHA协议:只能在每个时隙开始时才能发送一个帧 1-坚持CSMA: 一个结点要发送数据时, 首先侦听信道, 若信道空 闲则立即发送数据,若信道忙则等待,同时继续侦听直至信道空 介质访问控制 闲;若发生冲突,则随机等待一段时间后再继续侦听信道 非坚持CSMA:一个结点要发送数据,先侦听信道,若信道空闲,则立即发送数据,若忙则放弃侦听,等待一个随机时间后再重复上 CSMA协议 p-坚持CSMA:若信道忙,则继续侦听直到信道空闲;若信道空闲,则以概率p发送数据,以概率1-p推迟到下一个时隙,重复上诉 随机访问介质控制 先听后发, 边听边发, 冲突停发, 随机重发 CSMA/CDt办议 最小帧长=总线传播时延*数据传输率*2 用于无线局域网 CSMA/CA协议 预约信道

在一个较小的地理范围内,将各种计算机、外部设备和数据库系统等通过双绞线、同轴电缆等连接介质相互连接起来,组成资源何信息共享的计算机互联网络

碰撞避免机制

轮询访问介质访问控制: 令牌传递协议

ACK帧 RTS/CTS帧

适用于负载很高的广播信道

拓扑结构

决定要系 传输分质 介质访问控制方式 以太网:逻辑拓扑:总线型结构,物理拓扑:星型或拓展星型结构 数据链路层 =种特殊的局域网 令牌环:逻辑拓扑:环形结构,物理拓扑:星型结构 FDDI (光纤分布数字接口): 逻辑拓扑: 环形结构, 物理拓扑: 星型结构 以太网逻辑上采用总线性拓扑结构,所有计算机共享同一条总线,信息以广播方式发送 以太网尽最大努力交付数据,提供不可靠服务,差错的纠错由高层完成 粗缆 细缆 传输介质 双绞线 以太网的传输介质与网卡 光纤 以太网与IEEE802.3 図卡 局域网 每个网络适配器 (网卡) 都有一个地址,即MAC地址 (物理地址) 以太网的MAC地址 网卡从网络上每接收一个MAC帧,首先要用硬件检查MAC帧中的 MAC地址,若是发往本站的帧,则收下,否则丢弃 速率达到或超过100Mb/s的以太网称为高速以太网 100BASE-T以太网 高速以太网 吉比特以太网 10吉比特以太网 是无线局域网的一系列协议标准,包括802.11a和802.11b,制定了MAC层协议,运行在多个物理层标准上 有固定基础设施无线局域网:包含一个基站和若干个移动站 无线局域网类型 IFFF802.11 由一些平等状态移动站相互通信组成的临时网络 无固定基础设施无线局域网自组织网络 各节点之间地位平等,中间结点都为转发结点,都具有路由器功能 媒体接入控制机制采用分布式控制模式的循环方法 今牌环网的基本原理 今牌实际是一个特殊格式的MAC控制帧 逻辑上是环形拓扑结构,物理上是星型拓扑结构 指覆盖范围很广的长距离网络,连接广域网各结点交换机的链路都是高速链路。 广域网使用的协议主要在网络层 广域网有一些结点交换机及连接这些结点交换机的链路组成。结点交换机功能是将分组存储并转发 使用串行线路通信的面向字节的协议,该协议应用在直接连接两个 结点的链路上 PPP协议 链路控制协议 (LCP) : 用于建立、配置、测试和管理数据链路 组成部分 网络控制协议 (NCP) : 为网络层协议建立和配置逻辑连接 广域网 一个将IP数据报封装到串行链路的方法。 非平衡配置: 由一个主站控制整个链路的工作 配置方式 平衡配置: 链路两端的两个站都是复合站,每个复合站都可以平等地发起数据传输 正常相应方式: 一种非平衡结构操作方式, 即主站向从站传输数 据,从站响应传输,但从站只有在收到主站的许可后,才可进行响 HDLC (高级数据链路控制) 协议 异步平衡方式: 一种平衡结构操作方式, 每个复合站都可以进行对 数据操作方式 另一站的数据传输 异步响应方式: 一种非平衡结构操作方式, 从站即使未受到主站的 允许,也可进行传输 HDLC帧 网桥工作在数据链路层的MAC子层,与高层协议无关 网桥有过滤帧以及存储转发帧的作用,可以隔离冲突域,但不能隔离广播域 具备寻址和路径选择的能力,确定帧的送方向 从源网络接收帧,根据MAC地址向目的网络转发帧 特点 网桥能连接不同的局域网,能进行对应的数据链路层协议转换和帧格式修改 网桥要有足够大的存储空间来存储转发 帧过滤,隔离网段 网桥 自由主题 优点 扩大物理范围 可使用不同物理层,连接不同局域网,可靠性高,性能好 增加延时,不同MAC子层会有帧格式转换 缺点 MAC子层无流量控制的功能,不能阻止广播风暴 诱明网桥 生成树算法生成路由表 数据链路层设备 对主机不透明,主机必须知道网桥标识和目标网桥,路由选择由源 源路由网桥 站点浮躁,源站向目的站发送探测真来寻找最佳路由 相当于多端口的网桥,端口隔离冲突域,但不隔离广播域,用交换机能实现虚拟局域网,VLAN既能隔离冲突域也能隔离广播域

原理:根据源MAC地址和目的MAC地址查找表,若MAC地址不在

表中,则加入表中并转发目的端口

交换机

存储转发式:缓存帧,差错检测,丢弃或转发,延迟较长

停止等待协议中可能出现差错的情况

1) 数据帧丢失 2) 到达目的站的帧可能已遭破坏 应对措施: 超时重传 3) 数据帧正确但确认帧被破坏 应对措施: 超时重传,发送方将重传的同样数据帧丢弃,并重传一个对应的确认帧

CSMA/CD与CSMA/CA的区别

1) CSMA/CD可以检测冲突,但无法避免;CSMA/CA发送报的同时不能检测到信道上有冲突,本结点上没有冲突不意味着在接收结点处就没有冲突,只能尽量避免。 2) 传输介质不同。CSMA/CD用于总线型以太网,CSMA/CA用于无线局域网。 3) 检测方式不同。CSMA/CD通过电缆中的电压变化来检测;CSMA/CA通过能量检测、载波检测和能量载波混合检测三种方式检测信道是否空闲。 4) 在本结点处有无冲突,并不意味着接收结点处就有无冲突。

局域网的主要特点

1) 为一个单位所拥有,且地理范围和站点数目有限。2) 所有站点共享较高的总带宽。3) 较低的时延和较低的误码率。4) 各站为平等关系而非主从关系。5) 能进行广播和组播。

今牌环网中令牌和数据的传递过程

1) 网络空闲时,环路中只有令牌帧在循环传递。 2) 令牌传递到有数据要发送的站点处时,该站点就修改令牌中的一个标志位,并在令牌中附加自己需要传递的数据,将令牌变成一个数据帧,然后将这个数据帧发送出去。 3) 数据帧沿着环路传输,接收到的站点一边转发数据,一边查看帧的目的地址。若目的地址和自己的地址相同,则接收站就复制该数据帧以便进一步处理。 4) 数据帧沿着环路传输,直到到达该帧的源站点,源站点接收到自己发出去的数据帧后便不再进行转发。同时发送方可以通过检验返回的数据帧来查看数据传输过程中是否有错,若有错则重传该帧。 5) 源站点传送完数据后,重新产生一个令牌,并将令牌传递给下一个站点,以交出对媒体的访问权限。

以太网交换机的特点

1)以太网交换机的每个端口都直接与单台主机相连,并且一般都工作在全双工方式。2)以太网交换机能同时连通多对端口,使每对相互通信的主机都能像独占通信媒体那样无碰撞传输数据。3)以太网交换机是一种即插即用的设备,其内部的帧的转发也是通过自学习自动地逐渐建立起来的。4)使用专用的交换结构芯片,交换速率较高。5)独占传输媒体的带宽。

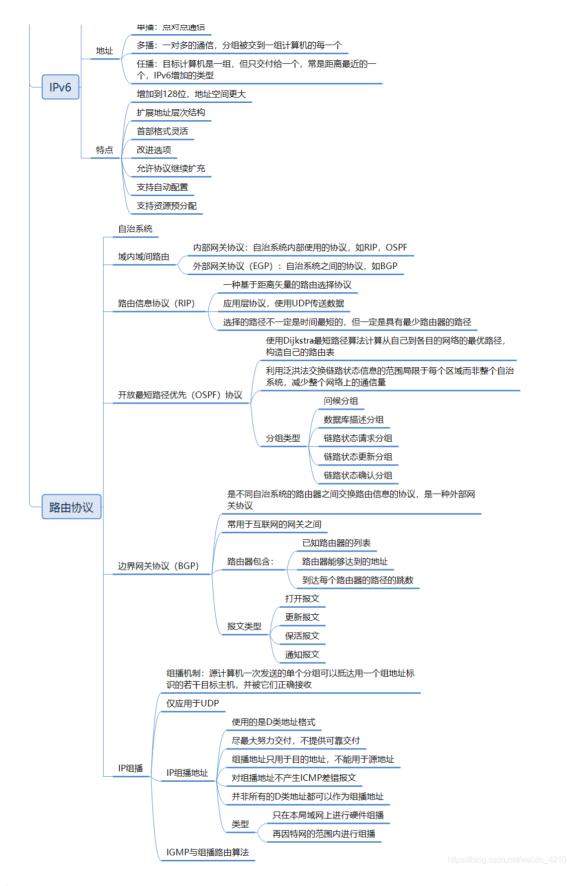
第四章 网络层

使异构的网络实现互联 路由与转发 网络层的功能 开环控制 拥塞控制 闭环控制 静态路由:由网络管理员手工配置的路由信息 动态路由:路由器上的路由表项是通过相互连接的路由器之间彼此 分类 交换信息,按照一定的算法优化出来的,路由信息在一定时间间隙 内不断更新,以适应不断变化的网络,随时获得最优的寻路效果 所有结点都定期将它们的整个路由选择表传送给所有与之直接相邻 的结点 每条路径的目的地 距离-向量路由算法 路由表 路径的代价 RIP算法 路由算法 要求每个参与该算法的结点都具有完全的网络拓扑信息 主动测试所有邻接结点的状态 链路状态路由算法 定期地将链路状态传播给所有其他结点 OSPF算法 内部网关协议 (IGP) : 一个自治系统内部所使用的路由选择协议 层次路由 外部网关协议 (EGP) : 自治系统之间所使用的路由选择协议 版本: IP的版本 首部长度 总长度: 首部和数据之和的长度 标识: 是一个计数器, 每产生一个数据报就+1 MF=1, 表示后面有分片 标志 MF=0,表示最后一个分片 IP首部的部分重要字段 片偏移 首部检验和 生存时间 (TTL) 协议 源地址字段:表示发送方的IP地址 目的地址字段:标识接收方的IP地址 IP首部大小为20B,IP数据报总长度不超过65535B 当分组长度超过MTU时, 必须分片 数据报的格式 校验和只校验分组首部,不校验数据部分 IPv4分组 路由器转发分组前,TTL-1,当TTL=0时丢弃分组 协议字段6标识TCP,17标识UDP MTU表示数据链路层能承载的最大数据量,是最大传输单元,用来 限制IP数据报长度 分片后的数据报在目的地址网络层合并,依据是首部的标识,标志 和片偏移 数据报分片 每个分片有相同的标识。标志有MF和DF两位,MF表示是否最后一 片,DF表示该数据报能否分片,通过片偏移确定该片在原始报文中 的位置,片偏移以8B为单位 1.提取目的地址,得到目的网络地址N 2.若地址直接与路由器相连,则直接将数据报交给主机 网络层转发分组 3.若路由表中有到达网络N的路由,则根据路由表转发该数据报 4.若路由表中有默认路由,则发送到默认路由器。若234都失败, 则报告分组出错 IP地址由网络号和主机号组成,网络号在全因特网是唯一的,主机 号在该网络是唯一的,5类IP地址 主机全0表示本网络本身 主机号全1表示本网络广播地址 127.0.0.1用于环路自检,该报文不会出现在任何网络上 特殊IP地址 32位全0表示本主机 IPv4地址 32位全1表示整个网络广播地址。由于路由器对广播域隔离,实际

相当于本网络广播地址 网络信息中心分配IP时只分配网络号,由得到IP的单位分配主机号 路由器转发IP数据报的依据是网络号,不考虑主机号,可减小路由 当一台主机连接两个网络时,必须同时有两个网络网络号对应的IP 特点 地址 (外网地址、内网地址)。每个路由器必然至少具备两个IP地 址,每个端口至少分配一个地址 用集线器,交换机,网桥连接的若干局域网同属一个网络,其网络 号都相同, 主机号都不同 网络地址转换,将专用网络地址转换为公用网络地址,从而对外隐 藏内部管理地址。NAT节省了IP地址的消耗隐藏内部网络细节,降 低收攻击的风险 私有地址不能直接用于Internet, 要通过NAT转换为全球IP地址后 才能用Internet。所有路由器对目的地址是私有地址的数据报一律 NAT 使用NAT时需要连接到因特网的路由器有NAT软件,且至少一个有 效外网地址。NAT映射表存放着内网地址:端口号-》外网地址: 端口号的肿射 IPv4 普通路由器转发数据报时不改变源IP地址和目的IP地址,而NAT路 中器转发数据报要根据地址转换表更换IP地址 在IP地址中增加一个"子网号"字段,使IP地址变成3级,这叫子网划分 {<网络号>, <子网号>,<主机号>} 子网划分 原子网不能全为0或全1,现随着CIDR的广泛使用,子网号也可以 全为0或1 用子网掩码表达对源网络中主机号的借位,进行子网划分 子网掩码中1的部分对应网络号和子网号,O的部分对应主机号。IP 地址和子网掩码相与得到子网的网络号 子网 主机除了设置IP地址,必须设置子网掩码 子网掩码 使用子网掩码特征 一个子网下的所有主机和路由器对应端口,有相同子网掩码 路由表中记录:目的网络地址;子网掩码;下一跳地址 路由转发方法 无类编址 (CIDR) 网络层只能看到抽象的IP数据报分组 IP地址与MAC IP首部有完整的源IP地址和目的IP地址,路由选择只需要目的IP地 发送方是主机时,要把IP数据报发送本网络上的另一主机,用ARP 找到目的主机的硬件地址 ARP 发送方是主机时,要把IP数据报发送到另一个网络上的一台主机。用ARP找到本网络上的一 个路由器的硬件地址,剩下的工作由这个路由器来完成 ARP的4种典型情况 发送方是路由器时,要把IP数据报转发到本网络上的一台主机。用 ARP找到目的主机的硬件地址 发送方是路由器,要把IP数据报转发到另一个网络上的一台主机。 用ARP找到本网络上的一个路由器的硬件地址,剩下的工作由找到 的这个路由器完成 动态主机配置协议,是应用层协议,基于UDP的,用来动态分配IP DHCP 申请主机广播请求报文,DHCP服务器响应报文并分配IP 网际控制报文协议, 网络层协议, 使主机和路由器可以报告差错和 异常情况 ICMP也是IP分组,其报文作为IP分组的数据字段 终点不可达:源点抑制(减缓发送速率),时间超时(TTL到0) ICMP差错 参数问题(首部参数);改变路由(重定向) ICMP报文出错 **ICMP** 分片的数据报的后续分片 不发送ICMP差错 具有多播地址的数据报 127.0.0.1或0.0.0.0特殊地址的报文 ping:应用层协议,直接使用ICMP协议而不使用TCP和UDP协 议,用到ICMP的回送ICMP的回送请求和回答报文 应用 tracert:工作在网络层,使用ICMP的超时报文 解决IP消耗的方法: CIDF, NAT, IPv6 (最根本方法)

77.140 F-37 F-7-2-15

网络层



路由与转发

1)路由选择。指按照复杂的分布式算法,根据从各相邻路由器所得到的关于整个网络拓扑的变化情况,动态地改变所选择的路由。 2) 分组转发。指路由器根据转发表将用户的IP数据报从合适的端口转发出去。

流量控制与拥塞控制

流量控制 流量控制是发送端和接收端之间的点对点通信量的控制。流量控制所要做的是抑制发送端发送数据的速率,以便使接收端来的接收。 拥塞控制 拥塞: 因出现过量的分组而引起网络性能下降的现象。 判断网路是否进入拥塞状态的方法是观察网络的吞吐量与网络负载的关系。若网络负载的增加,网络吞吐量明显小于正常的吞吐量,则网络已进入"拥塞"状态。 确保通信子网能够待传送的数据,是一个全局性的问题,涉及网络中所有的主机、路由器及导致网络传输能力 拥塞控制必须确保通信子网能够传送待传送的数据,是一个全局性的问题,涉及网络中所有的主机、路由器及导致网络传输能力下降的所有因素。

拥塞控制的两种方法

1) 开环控制 在设计网络时事先将有关发送拥塞的因素考虑周到,力求网络在工作室不产生拥塞。是一种静态的预防方法。一旦整个系统启动并运行,中途就不再需要修改。 2) 闭环控制 事先不考虑有关发生拥塞信息传到合适的地方,采用监测网络系统去监视,及时检测哪里出现拥塞,再将拥塞信息传到合适的地方,以便调整网络系统的运行,并解决出现的问题。是基于反馈环路的,是一种动态的方法。

网络层转发分组的流程 (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,得到目的地址N。2) 若网络N与此路由器直接相连,则把数据报直接交付给目的主机D,即路由器的直接交付;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条路由器;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)。报告转发分组出错。

使用子网掩码时路由器的分组转发算法:

1)从收到的分组的首部提取目的IP地址,记为D。 2) 先判断是否为直接交付。对路由器直接相连的网络逐个进行检查:用各网络的子网掩码和D逐位相"与",看结果是否与相应的网络地址匹配。若匹配,则将分组直接交付,否则间接交付,执行3)。 3) 若路由表中有目的地址为D的特定主机路由,则将分组传送给路由表中所指明的下一跳路由器;否则执行4)。 4) 对路由表中的每一行中的子网掩码和D逐位相"与",其结果为N。若N与该行的目的网络地址匹配,则将分组传送给该行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,则将分组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。

地址解析协议 (ARP) 工作原理

主机A想向本局域网上的某台主机B发送IP数据报时,先在其**ARP高速缓存**中查看有无主机B的IP地址。若有,则查出其对应的**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。若无,则通过使用目的MAC地址为FF-FF-FF-FF-FF-FF的帧来封装并广播ARP请求分组,使同一个局域网里的所有主机收到ARP请求。主机B收到该ARP请求后,向主机A发出响应ARP分组,分组中包含主机B的IP与MAC地址的映射关系,主机A在收到后将此映射写入ARP缓存,然后按查询到的硬件地址发送MAC帧。

DHCP交换过程

1) DHCP客户机广播"DHCP发现"消息,试图找到网络中的DHCP服务器,以便从DHCP服务器获得一个IP地址。2) DHCP服务器收到"DHCP发现"消息后,向网络中广播"DHCP提供"消息,其中包括提供DHCP客户机的IP地址和相关配置信息。3) DHCP客户机收到"DHCP提供"消息,若接收DHCP服务器所提供的相关参数,则通过广播"DHCP请求"消息向DHCP服务器请求提供IP地址。4) DHCP服务器广播"DHCP确认"消息,将IP

不发送ICMP差错报告报文的情况

1) ICMP差错报告报文 2) 第一个分片的数据报片的所有后续数据报片 3) 具有组播地址的数据报 4) 具有特殊地址的数据报

ICMP询问报文的四种类型

回送请求和回答报文 时间戳请求和回答报文 掩码地址请求和回答报文 路由器询问和通告报文

RIP

1)网络中的每个路由器都要维护从它自身到其他每个目的网络的距离记录。 2) 距离(跳数)规定从一个路由器到直接连接网络的距离为1.没经过一个路由器,则距离+1。 3) RIP优先选择跳数少的路径。 4) RIP规定一条路径最多包含15个路由器,RIP=16,则表示网络不可达。 5) RIP默认在任意两个使用RIP的路由器之间每三十秒广播一次RIP路由更新信息,以便动态建立并维护路由表。 6) 在RIP中不支持子网掩码的RIP广播,所有RIP中每个网路的子网掩码必须相同。 特点 1) 仅与相邻路由器交换信息。 2) 路由器交换的信息是当前路由器所知道的全部信息,即自己的路由表。 3) 按固定的时间间隔交换路由信息。

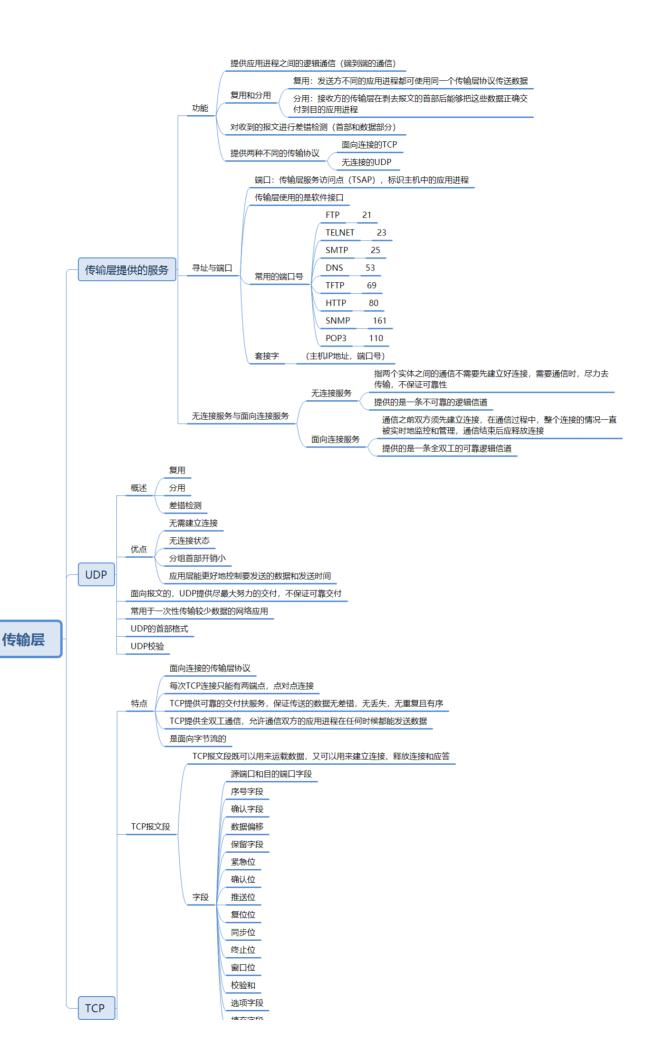
OSPF

1)对不同的链路可根据IP分组的不同服务类型而设置成不同的代价。 2) 若到同一个目的网络有多条相同代价的路径,则可以将通信量分配给这几条路径,即多路径间的负载平衡。 3) 所有OSPF路由器之间交换的分组都具有鉴别功能,保证了仅在可信赖的路由器之间交换链路状态信息。 4) 支持可变长度的子网划分和无分类编址CIDR。 5) 每个链路状态都带上一个32位的序号,序号越大,状态越新。

移动IP的基本通信流程

1)移动结点在本地网时,按传统的TCP/IP方式进行通信。 2) 移动结点漫游到一个外地网络时,仍使用固定的IP地址进行通信。为了能够接收到通信对端发给他的IP分组,移动结点需要向本地代理注册当前的位置地址,即转交地址。 3) 本地代理接受来自转交地址的注册后,会构建一条通向转交地址的隧道,将截获的发给移动结点的IP分组通过隧道送到转交地址处。 4) 在转交地址处解除隧道封装,恢复原始的IP分组,最后送到移动结点,使移动结点在外网就能够接收这些发给它们的IP分组。 5) 移动结点在外网通过外网的路由器或外部代理向通信对端发送IP数据包。 6) 移动结点在外网通过外网的路由器或外部代理向通信对端发送IP数据包。 6) 移动结点有外网通过外网的路由器或外部代理向通信对端发送IP数据包。 7) 移动结点回到本地网时,移动结点向本地代理注销转交地址,此时移动结点又将使用传统的TCP/IP方式进行通信。

第五章 传输层





TCP连接管理

TCP连接分为三个阶段:连接建立,数据传输,连接释放。在TCP连接建立的过程中,要使每一方都能够确知对方的存在,允许双方协商一些参数,并能够对运输实体资源进行分配。TCP连接的建立采用客户机/服务器方式。TCP连接的建立 1)客户机的TCP首先向服务器发送一个连接请求报文段(SYN=1,seq=x)2)服务器的TCP收到连接请求报文段后,向客户机发回确认,并为该TCP连接分配TCP缓存和变量(SYN=1,ACK=1,seq=y,ack=x+1)3)当客户机收到确认报文段后,还要向服务器给给出确认,并为该连接分配缓存和变量(ACK=1,seq=x+1,ack=y+1)TCP连接的释放1)客户机打算关闭连接时,向其TCP发送一个连接释放报文段,并停止发送数据,主动关闭TCP连接(FIN=1, seq=u)2)服务器收到连接释放报文段后即发送确认,此时,从客户机到服务器这一方向的连接被释放,TCP连接处于半关闭状态(ACK=1,seq=v.ack=u+1)3)若服务器已经没有要向客户机发送的数据,就通知TCP释放连接(FIN=1,ACK=1,seq=w,ack=u+1)4)客户机收到连接释放报文段后,必须发送确认(ACK=1,seq=u+1,ack=w+1)

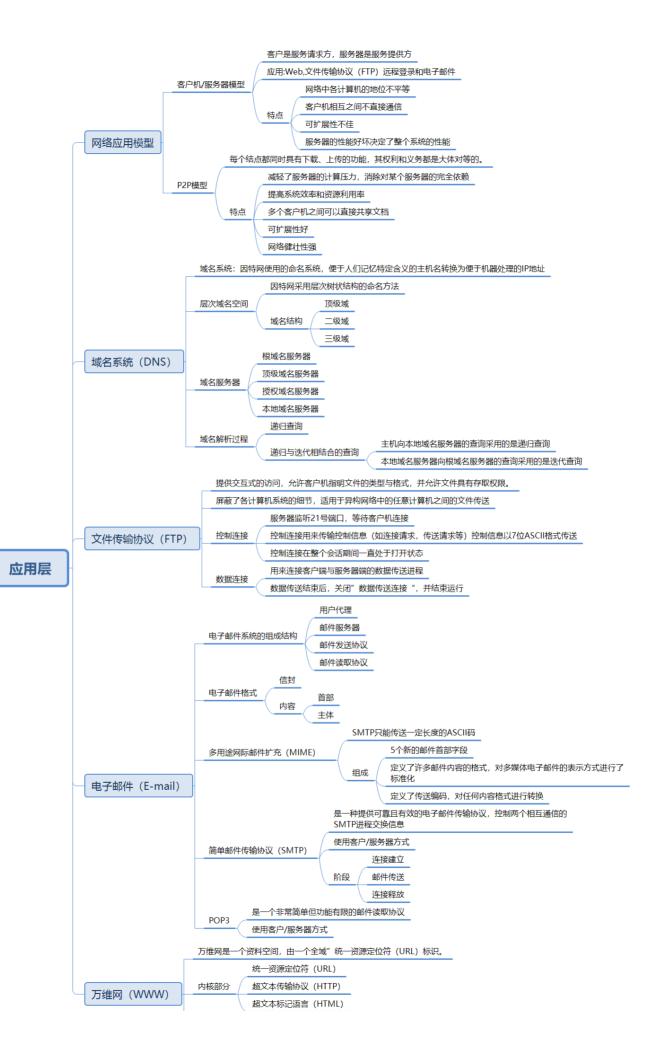
慢开始和拥塞避免

使用慢开始算法,TCP刚连接好并开始发送TCP报文段时,先令拥塞窗口cwnd=1,即一个最大报文段长度 MSS。每收到一个对新报文段的确认后,将cwnd+1,即增大一个MSS。 使用慢开始算法后,每经过一个传输轮次,拥塞窗口cwnd会加倍,即cwnd的大小指数式增长。当拥塞窗口增大至慢开始门限后,则改用拥塞避免算法 使用拥塞避免算法,发送端的拥塞窗口cwnd每经过一个往返时延RTT就增加一个MSS的大小,而不是加倍,使cwnd按线性规律缓慢增长,当出现一次超时时,令慢开始门限等于当前cwnd的一半。

快重传和快恢复

快重传技术使用冗余确认来检测丢包的发生。同时,冗余确认也用于网络拥塞的检测。当发送方连续收到三个重复的ACK报文时,直接重传对方尚未收到的报文段,而不必等到重传计时器超时。 **快恢复技术**是当发送端收到连续三个冗余确认时,执行"乘法减小"算法,把慢开始门限设置为出现拥塞时发送方的一半,跳过了cwnd从1开始的慢开始过程。

第六章 应用层



知识网图

链接: https://download.csdn.net/download/weixin 42104154/16486720.