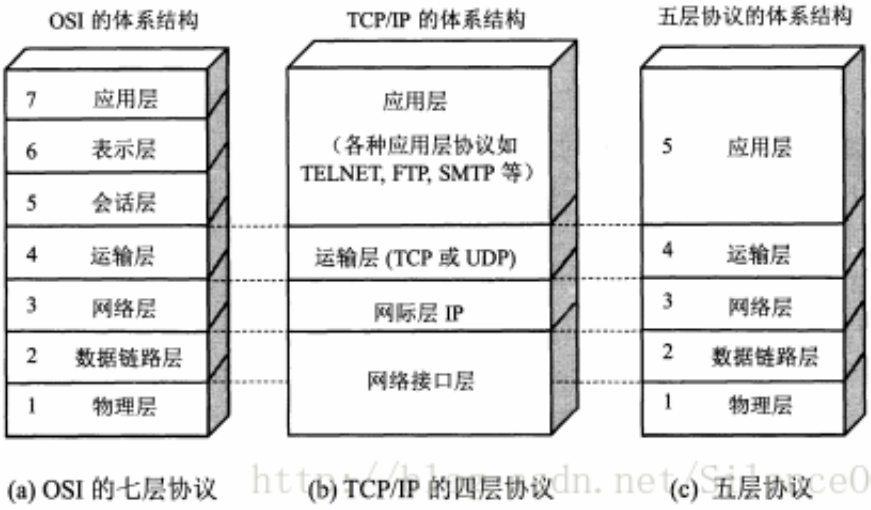
## 各层都有哪些常见协议?




| OSI七层网络模型 | TCP/IP四层概念模型 | 对应网络协议 |
| --- | --- | --- |
| 应用层（Application） | 应用层 | HTTP、TFTP, FTP, NFS, WAIS、SMTP |
| 表示层（Presentation） | | Telnet, Rlogin, SNMP, Gopher |
| 会话层（Session） | | SMTP, DNS |
| 传输层（Transport） | 传输层 | TCP, UDP |
| 网络层（Network） | 网络层 | IP, ICMP, ARP, RARP, AKP, UUCP |
| 数据链路层（Data Link） | 数据链路层 | FDDI, Ethernet, Arpanet, PDN, SLIP, PPP |
| 物理层（Physical） | | IEEE 802.1A, IEEE 802.2到IEEE 802.11 |

## 各层的作用

1、物理层：比特

主要定义物理设备标准，如网线的接口类型、光纤的接口类型、各种传输介质的传输速率等。它的主要作用是传输比特流（就是由1、0转化为电流强弱来进行传输,到达目的地后在转化为1、0，也就是我们常说的数模转换与模数转换）。这一层的数据叫做比特。

2、数据链路层：帧

定义了如何让格式化数据以进行传输，以及如何让控制对物理介质的访问。这一层通常还提供错误检测和纠正，以确保数据的可靠传输。

3、网络层：数据报

在位于不同地理位置的网络中的两个主机系统之间提供连接和路径选择。Internet的发展使得从世界各站点访问信息的用户数大大增加，而网络层正是管理这种连接的层。

4、运输层：报文段/用户数据报

定义了一些传输数据的协议和端口号（WWW端口80等），如： TCP（transmission control protocol –传输控制协议，传输效率低，可靠性强，用于传输可靠性要求高，数据量大的数据） UDP（user datagram protocol–用户数据报协议，与TCP特性恰恰相反，用于传输可靠性要求不高，数据量小的数据，如QQ聊天数据就是通过这种方式传输的）。 主要是将从下层接收的数据进行分段和传输，到达目的地址后再进行重组。常常把这一层数据叫做段。

5、会话层：

通过运输层（端口号：传输端口与接收端口）建立数据传输的通路。主要在你的系统之间发起会话或者接受会话请求（设备之间需要互相认识可以是IP也可以是MAC或者是主机名）

6、表示层：

可确保一个系统的应用层所发送的信息可以被另一个系统的应用层读取。例如，PC程序与另一台计算机进行通信，其中一台计算机使用扩展二一十进制交换码（EBCDIC），而另一台则使用美国信息交换标准码（ASCII）来表示相同的字符。如有必要，表示层会通过使用一种通格式来实现多种数据格式之间的转换。

7.应用层：报文

1 第五层——应用层(application layer)

- **应用层(application layer)**：是体系结构中的最高。直接为用户的应用进程（例如电子邮件、文件传输和终端仿真）提供服务。
- 在因特网中的应用层协议很多，如支持万维网应用的HTTP协议，支持电子邮件的SMTP协议，支持文件传送的FTP协议，DNS，POP3，SNMP，Telnet等等。

2. 第四层——运输层(transport layer)

- **运输层(transport layer)**：负责向两个主机中进程之间的通信提供服务。由于一个主机可同时运行多个进程，因此运输层有复用和分用的功能
- 复用，就是多个应用层进程可同时使用下面运输层的服务。
- 分用，就是把收到的信息分别交付给上面应用层中相应的进程。
- **运输层主要使用以下两种协议： (1) 传输控制协议TCP(Transmission Control Protocol)**：面向连接的，数据传输的单位是报文段，能够提供可靠的交付。 **(2) 用户数据包协议UDP(User Datagram Protocol)**：无连接的，数据传输的单位是用户数据报，不保证提供可靠的交付，只能提供“尽最大努力交付”。

3. 第三层——网络层(network layer)

- **网络层(network layer)主要包括以下两个任务：**
- **(1) 负责为分组交换网上的不同主机提供通信服务。在发送数据时，网络层把运输层产生的报文段或用户数据报封装成分组或包进行传送。在TCP/IP体系中，由于网络层使用IP协议，因此分组也叫做IP数据报，或简称为数据报。**
- **(2) 选中合适的路由，使源主机运输层所传下来的分组，能够通过网络中的路由器找到目的主机。**
- 协议：IP,ICMP,IGMP,ARP,RARP

4. 第二层——数据链路层(data link layer)

- **数据链路层(data link layer)**：常简称为链路层，我们知道，两个主机之间的数据传输，总是在一段一段的链路上传送的，也就是说，在两个相邻结点之间传送数据是直接传送的(点对点)，这时就需要使用专门的链路层的协议。
- 在两个相邻结点之间传送数据时，数据链路层将网络层交下来的IP数据报组装成帧(framing)，在两个

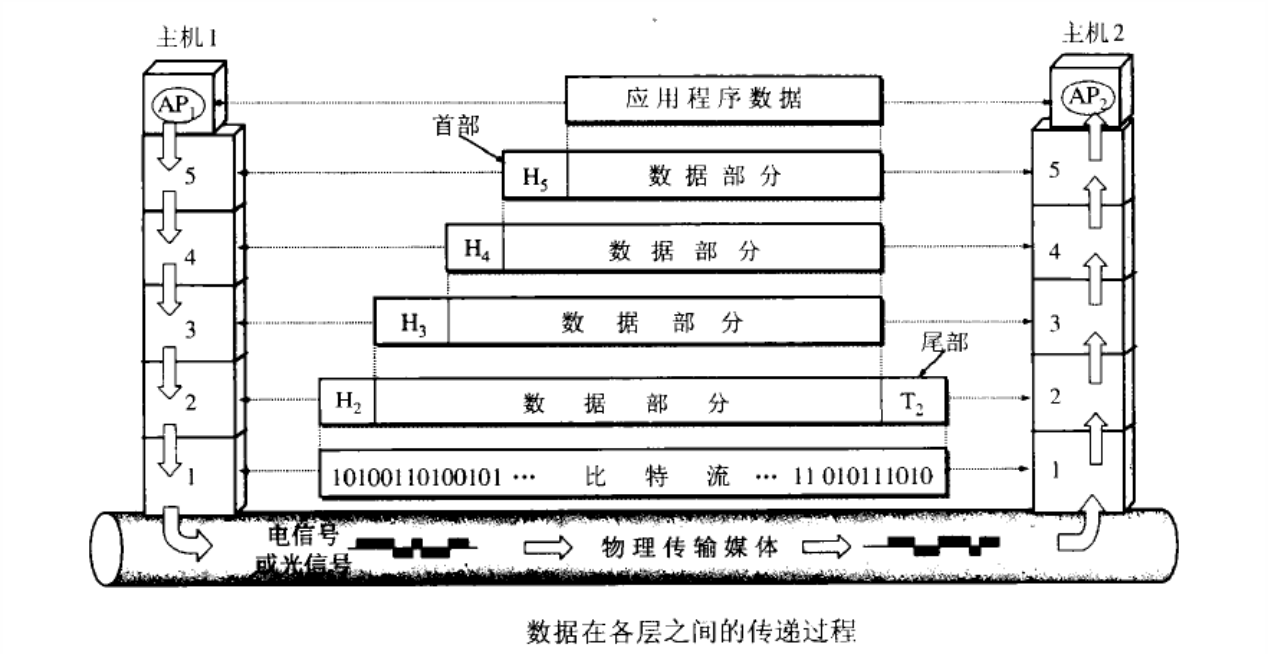
相邻结点之间的链路上“透明”地传送帧中的数据。

- 每一帧包括数据和必要的控制信息(如同步信息、地址信息、差错控制等)。典型的帧长是几百字节到一千多字节。
- 注：”透明”是一个很重要的术语。它表示，某一个实际存在的事物看起来却好像不存在一样。”在数据链路层透明传送数据”表示无力什么样的比特组合的数据都能够通过这个数据链路层。因此，对所传送的数据来说，这些数据就“看不见”数据链路层。或者说，数据链路层对这些数据来说是透明的。(1)在接收数据时，控制信息使接收端能知道一个帧从哪个比特开始和到哪个比特结束。这样，数据链路层在收到一个帧后，就可从中提取出数据部分，上交给网络层。(2)控制信息还使接收端能检测到所收到的帧中有无差错。如发现有差错，数据链路层就简单地丢弃这个出了差错的帧，以免继续传送下去白白浪费网络资源。如需改正错误，就由运输层的TCP协议来完成。

5. 第一层——物理层(physical layer)

- 物理层(physical layer)：在物理层上所传数据的单位是比特。物理层的任务就是透明地传送比特流。

## 数据在各层之间的传递过程




数据在各层之间的传递过程

## 什么是ARP协议?

地址解析协议，即ARP（Address Resolution Protocol），是根据IP地址获取物理地址的一个TCP/IP协议。主机发送信息时将包含目标IP地址的ARP请求广播到局域网络上的所有主机，并接收返回消息，以此确定目标的物理地址；收到返回消息后将该IP地址和物理地址存入本机ARP缓存中并保留一定时间，下次请求时直接查询ARP缓存以节约资源。

## 单播、多播（组播）、广播

一、单播：

主机之间“一对一”的通讯模式，网络中的交换机和路由器对数据只进行转发不进行复制。网络中的路由器和交换机根据其目标地址选择传输路径，将IP单播数据传送到其指定的目的地。 单播的优点：

1. 服务器及时响应客户机的请求

2. 服务器针对每个客户不通的请求发送不通的数据，容易实现个性化服务。

单播的缺点：

1. 每个客户机流量大的流媒体应用中服务器不堪重负。

2. 现有的网络带宽是金字塔结构，将造成网络主干不堪重负。

二、 广播：

主机之间“一对所有”的通讯模式，网络对其中每一台主机发出的信号都进行无条件复制并转发，所有主机都可以接收到所有信息（不管你是否需要），由于其不用路径选择，所以其网络成本可以很低廉。 广播的优点：

1. 网络设备简单，维护简单，布网成本低廉

2. 由于服务器不用向每个客户机单独发送数据，所以服务器流量负载极低。

广播的缺点：

1.无法针对每个客户的要求和时间及时提供个性化服务。

2. 无法向众多客户提供更多样化、更加个性化的服务。

3. 广播禁止在Internet宽带网上传输。

三、组播：

主机之间“一对一组”的通讯模式，也就是加入了同一个组的主机可以接受到此组内的所有数据，网络中的交换机和路由器只向有需求者复制并转发其所需数据。主机可以向路由器请求加入或退出某个组，网络中的路由器和交换机有选择的复制并传输数据。 组播的优点：

1. 需要相同数据流的客户端加入相同的组共享一条数据流，节省了服务器的负载。具备广播所具备的优点。

2. 由于组播协议是根据接受者的需要对数据流进行复制转发，所以服务端的服务总带宽不受客户接入端带宽的限制。

3. 此协议和单播协议一样允许在Internet宽带网上传输。

组播的缺点：

1．与单播协议相比没有纠错机制，发生丢包错包后难以弥补，但可以通过一定的容错机制和QOS加以弥补。

2．现行网络虽然都支持组播的传输，但在客户认证、QOS等方面还需要完善，需要逐步推广应用到现存网络当中。

## TDMA介绍

**时分多址**（Time division multiple access，缩写：**TDMA**） 是一种为实现共享传输介质（一般是无线电领域）或者网络的通信技术。它允许多个用户在不同的时间片（时隙）来使用相同的频率。

缺点：

- 信道利用率低
- 强假设各机器时间同步
- 强假设网络拓扑是静态的不变的

## RTT(Round-Trip Time)

往返时延。是指数据从网络一端传到另一端所需的时间。通常，时延由发送时延、传播时延、排队时延、处理时延四个部分组成。

# 广播路由选择算法

1、N次单播

如果有N个目的结点，那么在源结点中就产生N个分组副本，然后将这N份分组传到N个目的结点，这种方法看上去十分简单，而且是可以利用单播的协议进行N次传送。但是这方法有很多致命的缺点，比如：N次单播的第一段路径都相同，那么这段路径就是被利用了N次，第二个路由器也收到了N个重复的分组。那么，如果从第二个路由器开始发送这N个分组会不会更好点呢？所以这种方法会使得效率变得很低。

2、无控制的洪泛

洪泛是：每个结点收到了广播分组之后向它的所有邻居（除了发送给他分组的那个邻居）发送分组。这个方法看起来是挺好的，但是却存在这两个问题：第一个问题是如果这个拓扑中有圆，那么在这个圆中传播的分组将要无休止地循环下去。第二个问题是路由器将会收到很多重复的分组。

3、受控的洪泛

受控的洪泛主要是通过两种方法进行控制的。

第一种方法是**序号控制洪泛**（sequence - number - controlled flooding）中，对需要洪泛的分组添加一个广播序号，然后每个路由器都维护一个序号列表。当每个路由器收到一个分组的时候，先检查是否已经存在于序号列表中，如果不在，则记录该序号，然后转发分组，如果在的话，就直接丢弃分组并不转发分组。

第二种方法是**反向路径转发**（Reverse Path Forwarding，RPF）（也可以称为反向路径广播）。如果一台路由器接收到一个分组的时候，需要做一件事情，查看一下分组的源地址，检查这个分组是否是从源结点到此结点的最短路径上。如果是的话，就进行继续转发，如果不是，则直接丢弃分组。

4、生成树广播

现在已经研制出了很多种生成树的算法，这里我们只研究一种简单的算法，采用基于中心的方法（center - based approach）建立一颗生成树。首先需要定义一个中心结点，然后其他结点都向中心结点单播“加入树报文”，如果路径还未在树中，那么就直接加入树，如果路径中的某些部分已经在树中，例如该路径是B -> A -> F -> C -> G，但是F已经在树中了，那么就将B -> A加入到树中。通过这样的方法创建一颗生成树。

# 链路状态路由选择算法

见书246页

## 距离向量路由选择算法

见书248页

## IPv4数据报分片

该表配合书P217食用：

表 4-2　IP 片

| 片 | 字节 | ID | 偏移 | 标志 |
| --- | --- | --- | --- | --- |
| 第 1 片 | IP 数据报的数据字段中的 1480 字节 | identification = 777 | offset = 0（表示插入的数据开始于字节 0） | flag = 1（表示后面还有） |
| 第 2 片 | 1480 字节数据 | identification = 777 | offset = 185（表示插入的数据开始于字节 1480。注意 185 × 8 = 1480） | flag = 1（表示后面还有） |
| 第 3 片 | 1020 字节数据（= 3980 − 1480 − 1480） | identification = 777 | offset = 370（表示插入的数据开始于字节 2960。注意 370 × 8 = 2960） | flag = 0（表示这是最后一个片） |

## 循环冗余校验

见书P291

## ALOHA协议

ALOHA协议和它的后继者CSMA/CD都是随机访问或者竞争发送协议。随机访问意味着对任何站都无法预计其发送的时刻；竞争发送是指所有发送的站自由竞争信道的使用权。广播信道具有反馈性，因此发送方可以在发送数据的过程中进行冲突检测，将接收到的数据与缓冲区的数据进行比较，如果发送方检测到冲突，那么它可以等待一段时间后重发该帧。

## 转发(forwarding)和路由选择(routing)

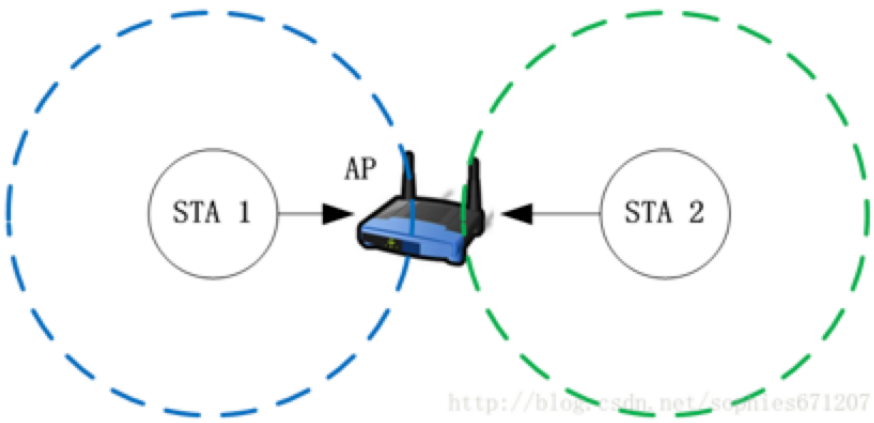
见书P200

## 隐藏终端和暴露终端

隐藏终端和暴露终端都是由于CSMA/CA中所采用的LBT机制所引起。隐藏终端是由于监听到的信道空闲而不是真的空闲，故引发冲突。而暴露终端是由于监听到的信道忙而不是真的忙，故其可以传输而不传输。

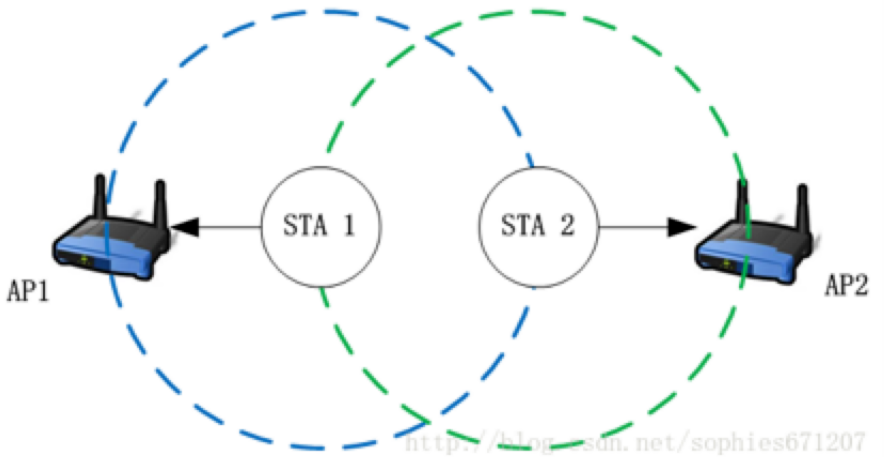
隐藏终端：

隐藏终端问题可以简单定义为：节点之间无法互相监听对方。但当其不可以同时传输时，其同时传输，从而导致冲突发生。隐藏终端在单个AP（或者单个Receiver）时就有可能发生。




暴露终端：

暴露终端问题可以简单定义为：节点之间能够互相监听对方。但其可以同时传输时，其不传输，从而造成浪费。暴露终端在多个AP（或者多个Receiver）时才有可能发生。




## 传输速率 带宽 吞吐量

1.传输速率：

定义：在数据传输中，两个设备之间数据流动的物理速度成为传输速率，单位为bps。

计算：比特是数据量最小单位，秒是时间的最小单位， 所以速率单位为bps。类似的，有kb/s，Mb/s(M=10^6), Gb/s（G=10^9）, Tb/s(t=10^12) 1Byte=8bit 一字节=8bit， 所以1Bps=8bps

我们平常说的速率是额定速率

2.带宽:

定义：计算机网络中的主机在数字信道上，单位时间内从一段传送到另一端的最大数据量，即最大速率。

类比：一个供水管，假设管子中有流动的水，这里的水为数据。单位时间内，从管子的某个横截面就是速率，即单位时间内传送的数据量。当管子充满水的时候，管子的某个横截面就是最大速率，即带宽计算：单位同速率一样，为bps

3.吞吐量:

主机之间实际的传输速率，被称为吞吐量，不仅仅衡量带宽，还衡量CPU的处理能力，网络拥堵程度及报文中数据字段的占有份额。说的通俗一点，就是单位时间内某个（信道。端口）实际的数据量，可以理解为实际的带宽。

# 网络术语

## SDN

软件定义网络 (SDN) 是一种网络虚拟化方法，致力于优化网络资源，使网络快速适应不断变化的业务需求、应用程序和流量。它的工作方法是分离网络的控制平面和数据平面，创建与物理设备不同的软件可编程基础架构。

有了 SDN，网络编排、管理、分析和自动化功能就成了 SDN 控制器的工作。由于这些控制器不属于网络设备，因此它们可以利用现代云计算和存储资源的规模、性能和可用性。SDN 控制器越来越多地建立在开放平台之上，采用开放标准和开放式 API，使它们能够编排、管理和控制来自不同供应商的网络设备。

SDN 带来诸多业务优势。控制层和传输层的分离，提高了灵活性并加快了新应用程序的上市时间。能够更快地应对问题和故障，从而提高了网络可用性。此外，可编程性更便于 IT 组织实现网络功能的自动化，进而降低运营成本。

SDN 可以和另一项技术即网络功能虚拟化 (NFV) 协同工作。NFV 可以用来虚拟化基于设备的网络功能，例如防火墙、负载平衡器和 WAN 加速器；而 SDN 提供的集中化控制可以有效地管理和编排 NFV 实现的各种虚拟网络功能。

## CDN

全称:Content Delivery Network或Content Ddistribute Network，即内容分发网络

基本思路：尽可能避开互联网上有可能影响数据传输速度和稳定性的瓶颈和环节，使内容传输的更快、更稳定。通过在网络各处放置节点服务器所构成的在现有的互联网基础之上的一层智能虚拟网络，CDN系统能够实时地根据网络流量和各节点的连接、负载状况以及到用户的距离和响应时间等综合信息将用户的请求重新导向离用户最近的服务节点上。

目的：解决因分布、带宽、服务器性能带来的访问延迟问题，适用于站点加速、点播、直播等场景。使用户可就近取得所需内容，解决 Internet网络拥挤的状况，提高用户访问网站的响应速度和成功率。控制时延无疑是现代信息科技的重要指标，CDN的意图就是尽可能的减少资源在转发、传输、链路抖动等情况下顺利保障信息的连贯性。CDN就是扮演者护航者和加速者的角色，更快准狠的触发信息和触达每一个用户，带来更为极致的使用体验。

## NFV

网络功能虚拟化（英语：Network Functions Virtualization，缩为 NFV），一种对于网络架构（network architecture）的概念，利用虚拟化技术，将网络节点阶层的功能，分割成几个功能区块，分别以软件方式实作，不再拘限于硬件架构。

网络功能虚拟化（NFV）的核心是虚拟网络功能。它提供只能在硬件中找到的网络功能，包括很多应用，比如路由、CPE、移动核心、IMS、CDN、饰品、安全性、策略等等。

但是，虚拟化网络功能需要把应用程序、业务流程和可以进行整合和调整的基础设施软件结合起来网络功能虚拟化（NFV）技术的目标是在标准服务器上提供网络功能，而不是在定制设备上。虽然供应商和网络运营商都急于部署NFV，早期NFV部署将不得不利用更广泛的原则，随着更多细节信息浮出水面，这些原则将会逐渐被部署。

为了在短期内实现NFV部署，供应商需要作出四个关键决策：部署云托管模式，选择网络优化的平台，基于TM论坛的原则构建服务和资源以促进操作整合，以及部署灵活且松耦合的数据/流程架构。

网络功能虚拟化(NFV)是由服务提供商推动，以加快引进其网络上的新服务。通信服务提供商(CSPs)已经使用了专用的硬件元素，使其可以频繁快速提供新的服务。对于传输网络而言，网络功能虚拟化(NFV)的最终目标是整合网络设备类型为标准服务器、交换机和存储，以便利用更简单的开放网络元素。

## 5G

5G移动网络与早期的2G、3G和4G移动网络一样，5G网络是数字蜂窝网络，在这种网络中，供应商覆盖的服务区域被划分为许多被称为蜂窝的小地理区域。表示声音和图像的模拟信号在手机中被数字化，由模数转换器转换并作为比特流传输。蜂窝中的所有5G无线设备通过无线电波与蜂窝中的本地天线阵和低功率自动收发器（发射机和接收机）进行通信。收发器从公共频率池分配频道，这些频道在地理上分离的蜂窝中可以重复使用。本地天线通过高带宽光纤或无线回程连接与电话网络和互联网连接。与现有的手机一样，当用户从一个蜂窝穿越到另一个蜂窝时，他们的移动设备将自动“切换”到新蜂窝中的天线。

5G网络的主要优势在于，数据传输速率远远高于以前的蜂窝网络，最高可达10Gbit/s，比当前的有线互联网要快，比先前的4G LTE蜂窝网络快100倍。另一个优点是较低的网络延迟（更快的响应时间），低于1毫秒，而4G为30-70毫秒。由于数据传输更快，5G网络将不仅仅为手机提供服务，而且还将成为一般性的家庭和办公网络提供商，与有线网络提供商竞争。以前的蜂窝网络提供了适用于手机的低数据率互联网接入，但是一个手机发射塔不能经济地提供足够的带宽作为家用计算机的一般互联网供应商。

## NGN

下一代网络（Next Generation Network），又称为次世代网络。主要思想是在一个统一的网络平台上以统一管理的方式提供多媒体业务，整合现有的市内固定电话、移动电话的基础上（统称FMC），增加多媒体数据服务及其他增值型服务。其中话音的交换将采用软交换技术，而平台的主要实现方式为IP技术，逐步实现统一通信其中voip将是下一代网络中的一个重点。为了强调IP技术的重要性，业界的主要公司之一思科公司（Cisco Systems）主张称为IP-NGN。

NGN是一个分组网络，它提供包括电信业务在内的多种业务，能够利用多种带宽和具有QoS能力的传送技术，实现业务功能与底层传送技术的分离；它允许用户对不同业务提供商网络的自由接入，并支持通用移动性，实现用户对业务使用的一致性和统一性。它是以软交换为核心的，能够提供包括语音、数据、视频和多媒体业务的基于分组技术的综合开放的网络架构，代表了通信网络发展的方向。NGN具有分组传送、控制功能从承载、呼叫/会话、应用/业务中分离、业务提供与网络分离、提供开放接口、利用各基本的业务组成模块、提供广泛的业务和应用、端到端QoS和透明的传输能力通过开放的接口规范与传统网络实现互通、通用移动性、允许用户自由地接入不同业务提供商、支持多样标志体系，融合固定与移动业务等等特征。

## DetNet

确定性网络（Deterministic Networking），DetNet是一项帮助实现IP网络从“尽力而为（best-effort）”到“准时、准确、快速”， 控制并降低端到端时延的技术。2015年，IETF成立DetNet工作组，专注于在第2层桥接和第3层路由段上实现确定传输路径，这些路径可以提供延迟、丢包和抖动的最坏情况界限，以此提供确定的延迟。DetNet工作组的目标在于将确定性网络通过IP/MPLS等技术扩展到广域网上。

确定性网络是由网络提供的一种特性，这里的网络指的是主要由网桥、路由器和MPLS标签交换机组成的尽力而为的分组网络。确定性网络的基本特征是：

1.时钟同步。所有网络设备和主机都可以使用IEEE 1588精确时间协议将其内部时钟同步到1$\mu$s-10 ns的精度。大多数（不是全部）确定性网络应用程序都要求终端站及时同步。一些队列算法还要求网络节点同步，而有些则不需要。

2.零拥塞丢失。拥塞丢失是网络节点中输出缓冲区的统计溢出，是尽力而为网络中丢包的主要原因。通过调整数据包的传送并为临界流（critical flow）分配足够的缓冲区空间，可以消除拥塞。

3.超可靠的数据包交付。丢包的另外一个重要原因是设备故障。确定性网络可以通过多个路径发送序列数据流的多个副本，并消除目的地处或附近的副本。不存在故障检测和恢复周期 - 每个数据包都被复制并被带到或接近其目的地，因此单个随机事件或单个设备故障不会导致丢失任何一个数据包。

4.与尽力而为（best-effort）的服务共存。除非临界流的需求消耗了过多的特定资源（例如特定链路的带宽），否则可以调节临界流的速度，这样，尽力而为的服务质量实践，例如优先级调度、分层QoS、加权公平队列等仍然按照其惯常的方式运行，但临界流降低了这些功能的可用带宽。

从某种意义上说，DetNet只是尽力而为网络提供的另一种QoS。 DetNet服务最大的作用在于整个网络的大部分流量都是尽力而为的。

## TSN

下一代工业通信—TSN（时间敏感网络），工业物联网的助推器

TSN是一项从视频音频数据领域延伸至工业领域、汽车领域的技术。TSN最初来源于音视频领域的应用需求，当时该技术被称为AVB，由于针对音视频网络需要较高的带宽和最大限度的实时，借助AVB能较好的传输高质量音视频。

TSN是以以太网为基础的新一代网络标准，具有时间同步、延时保证等确保实时性的功能。TSN是一组以太网标准，允许通过802网络实现时间同步的低延迟流服务。通过标准以太网，TSN创建了分布式，同步，硬实时系统的机制。这些系统使用相同的基础架构来提供实时控制并传达所有标准IT数据，从而为控制、测量、配置、UI和文件交换基础架构的融合提供动力。通过基于时间定义队列，TSN可确保通过交换网络的流量具有有限的最大延迟。这意味着标准以太网现在可以：

- 通过交换网络保证消息延迟

- 关键和非关键流量可以在一个网络中融合
- 更高层协议可以共享网络基础结构
- 实时控制可以远离操作区域
- 子系统可以更容易地集成
- 可以在不进行网络或设备更改的情况下添加组件
- 可以更快地诊断和修复网络故障

TSN并非涵盖整个网络，TSN其实指的是在IEEE802.1标准框架下，基于特定应用需求制定的一组“子标准”，旨在为以太网协议建立“通用”的时间敏感机制，以确保网络数据传输的时间确定性。而既然是隶属于IEEE802.1下的协议标准，TSN就仅仅是关于以太网通讯协议模型中的第二层，也就是数据链路层（更确切的说是MAC层）的协议标准。请注意，是一套协议标准，而不是一种协议，就是说TSN将会为以太网协议的MAC层提供一套通用的时间敏感机制，在确保以太网数据通讯的时间确定性的同时，为不同协议网络之间的互操作提供了可能性。

## 参数敏感，怎么面对，怎么调?

- 选择合适的激活函数，对于输出层，多分类任务选用softmax输出，二分类任务选用sigmoid输出，回归任务选用线性输出。对于中间隐层，则优先选择relu激活函数。构建序列神经网络（RNN）时要优先选用tanh激活函数。
- 一般学习率从0.1或0.01开始尝试，不可太大或太小；
- 防止过拟合，使用L1正则项、L2正则项、dropout、提前终止、数据集扩充等；
- 使用Grid Search、Random Search等自动调参方法；
- 参数随机初始化与数据预处理，参数初始化很重要，它决定了模型的训练速度与是否可以躲开局部极小；

## 人工智能技术在计算机网络中的优势

随着计算机网络技术的突飞猛进，当前的计算机网络环境具有很多鲜明的特点，如信息的瞬时性、传输速度的高速性等特点。结合这些特点，为了更合理、高效、稳定地管理好网络系统，具有一套成熟的网络管理技术与管理方法是必不可少的。而结合人工智能技术管理网络系统，其具备非常突出的优势。

**学习能力**

通过人工智能超强的学习能力，机器系统能够利用已有的训练数据通过数据挖掘来处理海量数据，并通过对低层次信息的学习、分析和推理等环节，提升相关概念的层次和等级获取更有价值的信息，从而可以提高分析的准确性，并进一步实现网络与服务的智能化管理。

**理解和推理能力**

利用人工智能其特有的推理、协作能力和模糊逻辑处理方式，可以最大限度优化计算机网络的环境，进一步提升网络管理和信息处理的能力。

**协同合作的能力**

利用人工智能的非线性协作能力可以有效地协调网络中的不同层级的关系，实现网络各层之间的协同管理。

**降低成本**

人工智能技术所采用的控制算法可以快速、高效且一次性完成最优的计算任务，不但节省了计算资源，还可以实现对计算机网络管理的高效处理。

## 人工智能在计算机网络安全管理技术中的应用

### 智能反垃圾邮件系统

人工智能应用在反垃圾邮件系统中，除了可以保护用户数据的安全外，最主要的是可以检测扫描用户邮件并进行智能识别，及时发现其中的敏感信息，同时采取有效防范措施阻止恶意邮件，使用户免受垃圾邮件骚扰之忧。

### 智能防火墙系统

防火墙智能防火墙引用的识别技术，可以很好地自行分析和处理相应的数据，同时又能巧妙地融合代理技术和过滤技术，不但可以降低计算机对数据的运算量，还能拓宽监控范围，有效地拦截对网络有害的数据流，从而更好地保障网络环境的安全。

### 智能入侵检测系统

智能入侵检测系统借助人工智能中的模糊信息识别、规则产生式专家系统、数据挖掘和人工神经网络等技术，提升入侵检测效率，并且可以最大程度地抵御来自于各方病毒入侵所带来的潜在威胁。

### 网络监测与控制

通过从DPI采集到的海量数据，人工智能技术可以利用其强大的理解和推理能力快速分析并判断信息中是否存在异常。如果出现新的病毒攻击或黑客入侵，人工智能还可以利用自身的学习能力将相关记录写在安全数据库中。

## 基于机器学习的网络系统面临的机遇和挑战之展望

提升对网络系统的理解，在端到端的网络系统设计原则下，各种终端协议复杂多样。借助机器学习方法，可以通过后验的方法分析学习算法的输出，了解网络的行为和影响因素，从而为算法设计提供帮助和指导

挑战之一是机器学习算法往往以尽力而为的方式工作，而网络系统要求算法能够进行满足硬约束的结构化输出，并提供最差性能保证。挑战之二是为了满足动态网络环境和差异化用户需求，机器学习算法需要具有较强的泛化能力和多目标决策的特性。最后，机器学习算法的问责性和可解释性的缺失，对其实际应用产生了很大的障碍。许多学习模型，特别是深度学习模型，往往是黑盒。

分布式机器学习与计算卸载，随着机器学习应用规模的增加，机器学习应用本身的发展再次需要网络侧的辅助。另一方面，移动设备受到计算能力和能耗的限制，很难完成神经网络的计算任务，此时可以利用网络将该计算卸载到云或边缘计算节点，实现网络资源与计算资源的整合。

## 物联网机器学习的机遇和挑战

无数的分布式设备会产生连续的、大量的、各种类型和有大量噪声的数据。

物联网数据也是高度可变的，存在时间模式。因此在收集培训数据时捕捉所有可能的情景在实践中是不可行的。

大量物联网应用需要使用监督机器学习，需要在模型可以被训练之前标记数据。但是物联网数据通常是独一无二的，不能保证现有的开源数据集随时可获得。

在机器学习方面，通过群体感知，物联网允许以前所未有的方式收集非常独特的数据集。由于每个设备生成的数据通常都是人为的，因此用户可以标记或验证它。收集最接近用户位置的数据也变得可能。

最好的模型需要接受大量数据的训练，而大多数物联网设备仍然受限于存储空间和处理能力。 另一个挑战是物联网设备可能无法连续连接到云端。

由于互联网连接设备技术通过提供物理和网络世界之间的连接来扩展当前的互联网，因此它生成的数据是通用的，所以会导致严重隐私问题。

物联网机器学习提供高度个性化的应用和服务，有真正成为以人为本的机器学习的资格。

# 本组论文分析

## 条件随机场增强图卷积神经网络

图数据中不同结点具有相似的信息，对于图卷积神经网络的隐藏层来说保存这些相似信息是非常重要的。论文提出了图卷积神经网络的CRF（条件随机场）层，它具有以下特点：

CRF层易于计算和优化。

CRF层要易于嵌入到已存在的图卷积神经网络中。

能够保存结点间的相似信息。

## 已有方法的不足

对于图数据来说，‘边’代表不同节点之间的相似关系，相连的节点有相似关系，不相连的节点没有相似关系。以上两种图卷积神经网络方法不能充分利用图的特性。

半监督图卷积网络方法聚合了一跳邻域节点，相关信息被编码进了新的特性中，尽管卷积神经网络能够聚合信息相关性，但是仍旧不能够保证获得的隐藏特性准确的保存相似关系。如果这种关系违反了隐藏的特性，那么后面阶段的任务将会严重退化。

为了解决上述的问题，在新特性中保存相似关系的方法大量被提出。然而这些方法都要求昂贵的特征分解，所以不适合大规模的神经网络。

## 本文方法

既然我们需要加强图卷积神经网络的隐藏层从而去满足相似性约束，那么就有必要去使用计算开销小并且通过反向传播易于优化的轻量级操作。所以限制图卷积神经网络隐藏层的表现是一个挑战。

为解决以上问题：我们提出了一个易于插入的条件随机场层去调整标准图卷积神经网络，利用条件随机场模型去限制图卷积层的隐藏特性，使它保存相似信息。

## 总结

本文，我们为图卷积神经网络提出了一个新颖的条件随机场。具体来讲就是，对于图卷积神经网络的隐藏层，我们通过条件随机场模型探索相似性关系，条件随机场层能够使隐藏特性保存不同节点之间的相似性关系。除此之外，CRF层很容易计算和优化以至于能够被插入现存的图卷积神经网络从而去提高它们的性能。大量的实验结果证明了我们的方法很有效。

## P193 P40

a. TCP慢启动运行时的时间间隔为[1 , 6]和[23 , 26]。

b. TCP拥塞避免运行时的时间间隔为[6 , 16]和[17 , 22]。

c. 在第16个传输轮回之后报文段的丢失是根据3个冗余ACK检测出来的。因为拥塞窗口长度没有降到1个MSS而是减半。

d. 在第22个传输轮回之后报文段的丢失是根据超时检测出来的。因为拥塞窗口长度降到了1个MSS。

e. 在第1个传输轮回里，ssthresh的初始值设置成32个MSS，因为在第6轮传输时到达了阈值32。然后拥塞窗口开始以线性速度爬升，直到在第16轮传输后出现3个冗余ACK。

f. 在第18个传输轮回里，ssthresh的值被设置成21个MSS，因为当第16个周期丢包事件发生时，拥塞窗口值为42个MSS，所以ssthresh的值被设置成0.5 × cwnd = 21 × MSS。

g. 在第24个传输轮回里，ssthresh的值被设置成14.5个MSS，因为当第22个周期丢包事件第二次发生时，拥塞窗口值为29个MSS，所以ssthresh的值被设置成0.5 × cwnd = 14.5 × MSS。

h. 在前6个传输周期中已经发送了1 + 2 + 4 + 8 + 16 + 32 = 63 个报文段，第7个传输轮回要发送32 + 1 = 33个报文段，即第64 - 96个报文段，所以第70个报文段在第7个传输轮回中发送。

i. 在第26个传输轮回时，拥塞窗口值为8个MSS，因此通过收到3个冗余ACK检测出有分组丢失时ssthresh的值被设置成0.5 × cwnd = 4 × MSS。拥塞窗口长度应当为4 + 3 = 7个MSS。

j. 假定使用TCP Tahoe（不管是发生超时指示的丢包事件，还是发生3个冗余ACK指示的丢包事件，都无条件地将拥塞窗口减至1个MSS，并进入慢启动阶段），并假定在第16个传输轮回收到3个冗余ACK。在第19个传输轮回，ssthresh的值被设置成21个MSS，因为当第16个周期丢包事件发生时，拥塞窗口值为42个MSS，所以ssthresh的值被设置成0.5 × cwnd = 21 × MSS。但是此时拥塞窗口值为1个MSS。

k. 第17个传输轮回到第21个轮回分别传送了1 + 2 + 4 + 8 + 16 = 31个分组，第22个轮回传送分组为阈值21个，所以一共传送了52个分组。