

# 高级计算机网络综述

袁铭潮

## 摘要

本文主要介绍了计算机网络中较为高级的技术，以及目前的发展方向，从现代网络的组成入手。较为传统的研究方面包括IPv6技术，主要为IPv6的各类协议和IPv6之于IPv4的优势;路由器方面，是主流协议与新型路由算法;QoS，主要是流分类以及服务模式;网络安全方面，介绍主流的网络威胁以及网络安全技术，以及当前的形式和新型网络的安全威胁。还结合了较为新的SDN和NFV的内容，以及这两种技术的关系以及在云计算和物联网中的应用。最后结合当前热点，介绍了深度学习与云计算等新型网络模式的结合应用。

## 1 概念解读

计算机网络是现代计算机技术与通信技术相互渗透，密切结合的产物，是随着社会对信息共享和信息传递的日益增强的需求而发展起来的，所谓计算机网络，就是利用通信设备和线路将地理位置不同的、功能独立的多个计算机系统互联起来，以功能完善的网络软件（网络通信协议、信息交换方式和网络操作系统等）实现网络汇总资源共享和信息传递的系统。

一个计算机网络是由资源子网和通信子网构成的，资源子网负责处理信息，通信子网负责全网中的信息传递<sup>[1]</sup>。

计算机网络的实现，为用户构造分布式的网络计算环境提供了基础，主要表现在三个方面：

(1) 硬件资源共享，可以在全网范围内提供对处理资源、存储资源、输入输出资源等昂贵设备的共享，从而使用户节省投资，也方便集中管理与均衡分担负荷。

(2) 软件资源共享，允许互联网尚的用户远程访问各类大型数据库，可以得到网络文件传送服务，远程进程管理服务和远程文件访问服务，从而避免软件研制上的重复劳动以及数据资源的重复存贮，也便于集中管理。

(3) 用户信息交换，计算机网络为分布各地的用户提供了强有力的通信手段，用户可以通过计算机网络传送电子邮件，发布新闻消息和进行电子商务活动等等。

计算机网络在资源共享和信息交换方面所具有的功能是其他系统所不能代替的，计算机网络所具有的高可靠性、搞性价比和易扩充性等优点，使得它在各个行业获得了越来越广范的应用。

所谓高级计算机网络是指计算机网络研究和应用领域中的一些高级主题、前沿主题和最新进展。本文包含了现代网络的组成、IPv6、路由、组播技术、QoS技术、网络安全等方面对计算机网络研究的内容进行综合阐述。

## 2 现代网络的组成

现代网络中使用的关键网络传输技术主要有以太网、Wi-Fi和4G/5G蜂窝网<sup>[2]</sup>。这些技术的每一种已经演化为支持非常高速的数据率，这些数据率支持许多多媒体应用，同时对网络交换设备和网络管理设施提出很多要求。

### 2.1 高速以太网

以太网是占主导地位的有线网络技术，被用于家庭、办公室、数据中心、企业和WAN中。当前以太网已经演化到支持数据率高达100Gbps，距离从几米到几十千米，已经称为大小组织机构中必不可少的网络。

现在的以太网已经能够支持高达100Gbps的数据率，已经能够满足所有领域的需求包括数据中心在内，一种同一协议方法是很有竞争力的。

以太网数据速率从1Gbps到10Gbps的主要驱动需求是内联网流量以及因特网流量的增长，造成流量增长的因素有：网络连接数量的增长、每个端工作站连接速率的增长、部署诸如高质量视频等带宽密集型应用的增长和网站托管和应用托管流量的增长。

IEEE 802.3委员会为支持因特网交换、高性能计算和按需视频交付等需求，发展出了两个不同数据率的新标准的需求，分别为40Gbps和100Gbps。

现如今，400Gbps的以太网协议也已经进入了部署阶段，IEEE的802.3cd标准为当前和将来的高速以太网接口定义了物理端口，预计50 Gbps、200 Gbps和400Gbps这几种速率将逐渐取代25 Gbps和100 Gbps。下一代是1Tbps标准已成广泛共识。

同时因为以太网的多用途，研发两种较低速率（2.5Gbps和5Gbps）的标准已经取得共识，主要希望支持IEEE 802.11ac无线流量进入有线网络。

### 2.2 Wi-Fi

Wi-Fi是一种处于支配地位的无线因特网接入技术，Wi-Fi成功的关键在于互操作性。Wi-Fi使能的设备必须能够于Wi-Fi接入点通信，而无论设备或接入点的生产商是谁。

Wi-Fi协议的从初始1997年的802.11到2014年的802.11ac。最新的802.11ac运行在5GHz频段，前一个版本为802.11ad协议，工作于60GHz频段，该频段能提供比5GHz频段宽得多的信道带宽，使得具有相对简单的信号编码和天线特征的高数据速率成为可能。

又由于60GHz频段的传输限制，802.11ad协议能支持高数据速率，但覆盖范围较小，所以适合在家庭娱乐系统中代替有线的应用或从蜂窝手机到电视转移高分辨率流。

目前这两种协议同时被广泛，在不同的场景中有各自的应用。

### 2.3 4G/5G蜂窝网

蜂窝技术是移动无线通信的基础，在不方便由有线网络提供服务的场所支持用户。蜂窝网络技术主要用于移动电话、个人通信系统、无线因特网和无线Web应用及更多应用的支撑技术。当前已经发展到第四代，第五代的部署已经展开。

第三代无线通信的目标是提供相当高速的无线通信，以除了支持语音外还支持多媒体、数据和视频。3G网络带宽被限制为5MHz，目标数据速率是144kbps和384kbps。通过多速率技术实现灵活的支持来自某个给定用户的多个并行的应用，并且能够通过为每个服务提供所要求的能力来有效的使用可用的能力。

4G系统为包括便携机、智能手机和平板电脑在内的各种移动设备提供了极宽的带宽的因特网接入。4G网络支持移动Web介入和高带宽应用，例如高分辨率移动TV、移动视频会议和游戏服务。这些需求导致了4G网络的发展，该移动无线技术设计用来最大化带宽和吞吐量，同时也最大化频谱的效率。

目前5G系统以及部署，但尚未普及，其峰值理论传输速度可达每8秒1GB，比4G网络的传输速度快10倍以上。5G的关注点是在网络中构建更多的智能，通过动态使用优先权、适应性的网络重配置和其他网络管理技术来满足服务质量需求。

## 3 IPv6

### 3.1 新一代网络协议

新一代IP协议的研究和提出源于对现有IPv4协议不足之处的认识，最主要的原因是IPv4地址几乎已经枯竭，无法应对Internet应用和用户数量的迅猛增长的需要，对满足未来的增长预期更是无能为力。根据最新报道，IPv4的地址已经枯竭。其次，骨干网络上庞大的路由表拖慢了数据交换的速度，维护工作量十分惊人，而且越来越像一颗炸弹，随时可能致Internet于死地。另外，IPv4具有对QoS缺乏支撑、安全性很弱、扩展选项过少、不支持即插即用等缺陷，这些都是受到广大开发者和使用者诟病的。

在1991年，IETF预见到了IPv4地址迅速消耗的问题，并采取了很多措施来减少对IPv4地址的使用，比如取消了临时地址分配（拨号、点对点协议（PPP）和动态主机配置协议（DHCP））、严格的分配政策、CIDR和网络地址转换（NAT）等等。

IETF于1995年正式发布了面向下一代互联网的数据包传送协议-IPv6（当时的版本是RFC 1883,当前版本是RFC 2460）。

能够满足多层结构化、层次化的网络拓扑，能很好地支持路由聚合，减少了路由表项的增长;能够方便地址的自动配置和管理;能够支持端到端的IPSec协议;包括地址在内的IPv6头部字段的固定长度方便了路由转发的快速处理。还在数据格式上为解决目前互联网面临的安全、高性能传送、服务质量控制和移动通信等重要技术挑战预留了设计空间<sup>[3]</sup>。

IPv6协议分别用固定128为长度的二进制位表示源地址和目的地址，与IPv4的32bit地址空间相比，IPv6拥有128bit的地址空间， $2^{128} \approx 3.4 \times 10^{38}$ ，足以使网络地址分配远离捉襟见肘的尴尬境地。

### 3.2 IPv6的过渡技术

IPv4升级到IPv6肯定不会是一蹴而就的，是需要经历一个十分漫长的过渡阶段（用我厂通用的术语说，就是IPv4升级IPv6这个灰度的时间非常长），要数十年的时间都不为过。现阶段，就出现

了IPv4慢慢过渡到IPv6的技术（或者叫过渡时期的技术）。过渡技术要解决最重要的问题就是，如何利用现在大规模的IPv4网络进行IPv6的通信。

目前的过渡技术主要有三种：双栈技术、隧道技术、转换技术。

隧道技术是比较好地解决了在很长期一段时间内还是IPv4网络是主流的情况下IPv6节点（或者双栈节点）间的通信问题。

协议转换技术是为了解决IPv6节点与IPv4节点通信的问题。协议转换技术的核心思路就是在IPv4和IPv6通信节点之间部署中间层，将IPv4和IPv6相互映射转换。

### 3.3 下一代互联网

IPv6协议不等于下一代互联网，但采用IPv6协议的大规模下一代互联网实验网必将是研究下一代互联网技术的重要基础措施。

值得说的是，目前我们接触得比较多的主流操作系统内核，已经很好地支持IPv6协议栈，例如：

Windows: windows 7、windows 8.x、windows 10，默认开启IPv6；

Linux: 内核2.6.x、内核3.x、内核4.x 已经支持IPv6（需要手动开启）；

iOS: IOS9开始已经支持IPv6 Only，2016年苹果已经强制要求app必须支持IPv6。

目前对下一代互联网的需求和基本特征还是有比较一致的看法的，就是希望下一代互联网“更大、更快、更安全、更及时、更方便、更可管理和更有效益”。

下一代互联网所面临的主要技术挑战可以归纳为扩展性、安全性、高效性、是实行、移动性和可管理性，其中，扩展性和安全性是目前互联网面临的首要技术挑战。

### 3.4 移动IPv6

移动IPv6充分利用了IPv6技术本身的特点，使IPv6设备具有移动性。移动节点由Home Network负责管理，当节点移动出Home Network后，接纳移动节点的网络称为该网络的Foreign Network。当节点移动到Foreign Network时，在保留Home Address的同时还需要获得Foreign Network的转交地址，移动IP需要构建Home Agent到移动节点之间隧道，通过隧道和转交地址来保持移动节点的连通性。

相对于移动IPv4，在移动IPv6中可通过邻居发现、自动配置等技术直接实现Foreign Network的发现以及转交地址的获得，，可以优化报文路径、减少迂回路由、解决了源地址过滤等问题，并使移动节点的应用层对转交地址透明处理，实现无缝的移动。

### 3.5 IPSec协议

IPSec（互联网协议安全性）是通过对IP协议的分组进行加密和认证来保护IP协议的网络传输协议族。由两大部分组成：（1）建立安全分组流的密钥交换协议；（2）保护分组流的协议。

前者为IKE（互联网密钥交换）协议，后者包括加密分布流的ESP（封装安全载荷）协议或AH（认证头部）协议，用于保证数据的机密性、来源可靠性、无连接的完整性并提供抗重播服务。

IPSec在IPv6中是必选的，也随着IPv6得到更为广泛的使用。

### 3.6 IPv6与IPv4的对比

本节通过对比IPv6相对与IPv4的优势，给出IPv6更新的必要性。如表1所示。

描述	IPv4	IPv6
IP数量	提供的地址数量为40多亿( $2^{32} - 1$ )。	提供 $3.4 \times 10^{38}$  $(2^{128} - 1)$ 个地址。
传输速度	根据提供的 IP 选项，有 20-60 个字节的可变长度。网络数据转发的效率较慢。	40个字节的固定报头，路由表小，聚合能力强，数据转发路径短，转发效率高。
安全性	没有强制使用 IPSec 加密数据，导致网站明文传输泄漏数据。	集成了 IPSec，在网络层认证与加密数据，为用户提供端到端的数据安全，保证数据不被劫持。
移动端	存在三角路由的问题，且需要外地代理，配置难度大。	增强移动终端的移动特性、安全特性、路由特性，同时降低网络部署的难度和投资。
即插即用	不能即插即用	IPv6 增加了自动配置以及重配置技术，对于 IP 地址等信息实现自动增删更新配置，提升 IPv6 的易管理性。

表 1: IPv6对比IPv4

有个问题是，IPv6有众多优点，为什么却迟迟没有普及？

阻碍 IPv6 普及，一方面是技术原因，还一方面是资源分配不平均：

1、IPv6 与 IPv4 的兼容性存在问题，双方之间很难做到完整的互联互通，目前的技术是在双方通信时经过隧道，建立隧道的成本太高；

2、美国、欧洲等手里拥有大量闲置的 IPv4 地址资源，它们现在还无需担心地址枯竭，所以也迟迟不肯推进 IPv6 的普及。

## 4 路由

### 4.1 路由器体系结构

路由器是计算机网络的核心设备，其主要功能是完成路由和转发。此外，由于应用领域的多样性和应用环境的复杂性，在很多情况下，路由器还要完成额外的控制与管理功能，比如安全、策

略、计费等。在骨干网络中，路由器的转发能力仍然是核心路由器最重要的性能指标。

随着计算机行业的快速发展，光纤通信技术的成熟，路由器的转发速率是目前网络速度提高的主要瓶颈。

路由策略可由自治系统（AS）自行决定，有些路由算法和协议适用于子网接入AS，有些适用于AS内部，还有些适用于AS之间的互连，最终构成整个Internet。

## 4.2 路由算法与协议

依据路由算法和协议应用的网络位置，协议可分为内部网关协议和外部网关协议。

内部网关协议的主要协议有：路由信息协议（RIP），RIP采用UDP进行传送；开放式最短路径优先协议（OSPF）采用分布式的链路状态协议，基于Dijkstra算法实现。

外部网关协议是自治系统之间使用的，边界网关路由协议（BGP）是最主要的一种，功能为同其他的BGP系统交换网络可达信息。BGP使用TCP作为传输协议。

随着Internet的发展，对于路由分组转发的要求越来越高，分组转发的一个重要步骤就是查找路由表，因此快速的路由查找算法是实现高速分组转发的关键。目前主要有严格匹配和最长前缀匹配两种算法。

### （1）严格匹配查找算法

在两层以太网交换中，以目标MAC地址按端口转发的方式是采用严格匹配查找算法。使用的方法为相联存储（CAM），能够并行查找。还可以采用Hash的办法进行查找。

严格匹配查找算法的优点是简单，而且查找开销较少。缺点是内存使用率不高，查找时间不确定。

### （2）最长地址前缀匹配查找算法

最长地址前缀查找可以从地址前缀值以及地址前缀长度两个方面考虑。

基于地址前缀值路由查找算法的特点是通过对整个地址前缀空间进行地址关键字穷局来消除地址前缀长度对查找的影响。方法主要有线性匹配查找算法、地址区域二分法甚至基于CAM的硬件实现方法也算。

基于地址前缀长度的路由查找算法的出发点就是在前缀长度空间内进行查找，可以使用线性遍历法（比如二进制Trie树查找算法和多分支Trie查找算法）、二分法遍历法。

## 4.3 新型路由查找算法的研究

近年来，随着对路由器研究的逐步深入以及对于路由器性能要求的不断提高，提出了多种较为新颖的地址前缀查找算法。为了提高算法的效率，大多使用了一些辅助策略。

1、前缀扩展。地址前缀是一系列主机地址或者网络地址的合并，地址前缀的转发信息涵盖了所有这些主机或者网络的转发信息，所以可以将一条长度较短的地址前缀展开成多条地址长度较长的前缀集，其中这些前缀集的转发信息就是原来地址前缀所对应的转发信息。

2、独立前缀转化。最精确转发信息的方法是将地址前缀集转化为一些完全独立的前缀集。独立的前缀集中各个前缀之间不存在相互包含关系，使用二分支Trie树结构实现。

3、压缩技术。试图从编码中删除数据的冗余信息，对Trie树使用压缩技术主要是考虑到Trie树的扩展转化过程大大增加了信息的冗余度，使用一定的压缩算法将信息的冗余度降低。

4、优化技术。能够使在一定显示条件的前提下找到满足约束条件的最佳前缀集，比如在查找速度的约束下尽量减少算法的存储空间等。

## 5 QoS技术

服务质量（QoS）是一个综合指标体系，用以衡量网络对于各种类型网络应用及其需求的支撑能力。这些指标必须是可提供的、可计量的、可验证的和可管理的，而且在使用时是始终如一的、可预测的，有些方面甚至是起决定性作用的。

常见的指标包括一下几个方面：吞吐量、时延、时延抖动、误码率、丢包率、优先级、可用性和安全性。

### 5.1 QoS基本框架

为了保证端到端应用的服务质量，QoS首先需要进行流分类，然后根据网络状况进行处理，具体处理形式包括流量监管、流量整形、拥塞管理及拥塞避免等。

#### （1）流分类

无论采用哪种技术手段实现QoS，都需要路由器能够根据事先规定的规则对报文头的某些字段进行分类标识，判断其对应的流量规范，设置不同优先级以便实现不同的转发处理。

这是实现QoS服务的前提条件与基础，目的是将报文映射到不同的服务类别。流分类的核心是查找算法，需要满足速度快、消耗资源小、易于更新等需求，在上文路由相关内容中包含。

#### （2）流量监管

如果不限用户发送的流量，网络中可能出现大量的突发报文导致拥塞和数据丢弃，QoS策略可以检测或主动限制进入某一网络的某一连接的流量，当某个连接的流量过大以致超过约定带宽时，就可以根据报文的类别采取不同的方式进行处理。

#### （3）流量整形

流量监管多用于入口的流量控制，而流量整形则用于限制出口方向的流量速率。流量监管的目的在于控制流量。而流量整形则用于调整分组传输的平均速率，尽量避免流量因突发的特性而造成网络拥塞的发生。

对于超出部分，不丢弃，而是进行缓存。缓冲区队列饱和时，多余的分组会被丢弃。

#### （4）队列调度

队列调度机制有助于QoS根据不同的优先级进行数据的重新排序，这对于拥塞控制管理非常重要。数据达到出口时，路由器根据分组的优先级或基于分类决定数据包是否丢弃或分配到不同的队列进行缓冲，然后通过队列调度机制进行传输。

接口发生拥堵时，通过队列调度机制就可以保证实时性要求较高的分组的传输。常见的队列调度机制包括FIFO、公平排队算法（FQ）、加权公平队列（WFQ）等。

### 5.2 QoS服务模式

单纯一项技术的应用可能无法切实保障QoS，而需要综合多种技术，同样，为了避免QoS技术用于网络时出现问题，端到端的原则是QoS设计者必须遵循的路线。为了使协议相互配合，在每个传输

环节上落实QoS保障机制，QoS技术框架上可采用Intserv、Diffserv和两者结合三种服务模型。

Intserv需要面向连接，这与IP技术本身无连接的特性是不相符的，且需要全网设备都能提供一致的技术才能实现QoS，实施难度大，所以在IP网络中利用技术提供IP QoS时，为了达到规模化和适应性，往往会采用Diffserv体系结构。

## 6 网络安全

网络安全问题主要分为两类，一为网络本身及计算机系统的安全：保护端系统和网络自身的可用性和功能的完整性，防止计算资源或通信资源的非法使用；二为信息安全：为网络中的信息提供保密与完整性传播、抗抵赖等安全服务。

网络安全要保护的对象实际上是网络中的资产，即网络中的信息、信息传输和处理系统等资源。攻击者通过多种手段实现自己的非法目的，从攻击方式来区分，可以分为被动攻击和主动攻击两种方式。

### 6.1 网络安全威胁技术

当前的网络安全威胁技术有扫描攻击、陷阱攻击、感染攻击、陷阱攻击等四种类型。

#### (1) 扫描攻击

扫描攻击泛指那些通过有针对性的扫描方法对特定对象进行的攻击行为。攻击对象包括登录口令、信息内容、网络地址、设备配置、软件版本、程序缺陷等。

主要方式有：口令破解、通信窃听、漏洞扫描等。

#### (2) 缺陷攻击

缺陷攻击通常是利用网络系统、软件系统等存在的漏洞、差错和故障，以达到实现攻击目的的行为。

拒绝服务（DoS）通过耗尽目标系统的资源危害目标系统的正常使用，有效的DoS攻击一般采用分布式拒绝服务（DDoS）攻击方法，大致利用协议漏洞、软件缺陷、资源比拼等三类方法。

溢出攻击，用于攻击非常普遍、非常隐蔽、非常危险的缓冲区溢出错误，在各种操作系统、应用软件中广泛存在，如今大约80

注入攻击，利用网络应用系统用户访问界面的输入机制，输入事先严密设计的内容，并达到攻击目的，往往针对SQL数据库访问操作，故常称为SQL注入攻击。

(3) 感染攻击，计算机和计算机网络中感染宿主并进行攻击的恶意代码，具有极大的危害性。有病毒、蠕虫、木马、恶意脚本等。

#### (4) 陷阱攻击

陷阱攻击是以欺骗为核心、以谋取利益为最终目的，利用网络覆盖性及网络用户的不设防、网络知识薄弱、网络意识薄弱、防范意识松懈、贪图小便宜等因素，步步为营、引人入钩的方式。主要为网络欺诈、劫持攻击、域名攻击、垃圾邮件等。

### 6.2 网络安全关键技术

当前网络安全服务以认证服务、保密服务为主，还有数据完整性保护、访问控制、可用性服务

等。

验证、授权和记账（AAA）用于提供系统的访问控制功能，在网络与信息系统中应用广泛，是保障网络安全的重要环节。AAA的应用包括但不限于：安全协议的通信验证、网络信息系统访问登录中的用户身份验证、网络设备互连的合法性验证、操作系统或数据库管理系统登录与存取操作验证、Internet接入验证。

加密技术分为对称密钥加密和非对称密钥加密。

对称密钥加密技术是面向大数据量的加密的，密钥越长强度越大，具有很高的计算效率，但密钥的生成、发布、存储带来较大的管理工作量。

主要的对称密钥加密技术有RC4、DES、IDEA等。

非对称密钥加密是使用一对密钥来加密和解密的，其中一个是密钥的拥有者秘密保存的私钥，另一个是可以对任何人公开的公钥。用公钥加密的数据只能用对应的私钥解密，而用私钥加密的数据只能用对应的公钥解密。

由于公钥加密技术的效率通常很低，所以不适用对大量的数据进行加密，一般用来加密会话密钥。公钥加密算法有RSA、ECC等。

上文中所提到的IPSec协议是IP协议的一个子层，可以看作是IP的一个安全补丁。

### 6.3 网络安全新技术及趋势

在美国，“动态目标防御”(MTD, MovingTargetfense)是美国国家科学技术委员会(NSTC)提出的网络空间“改变游戏规则”的革命性技术之一。这种新的网络安全技术首先由美国空军提出并得到美国军方的认可、推动、实施。014年，美国空军发展指挥和控制能力以实现动态目标防御(MovingTargetDefense)<sup>[4]</sup>。

2015年美国新型动态防御公司崛起，动态防御概念的3家公司获得超过6000万美元的融资，其中CrowdStrike获得3000万美元融资，Morphisec获得800万美元融资，ShapeSecurity获得2600万美元融资。

美国阿贡国家实验室于2016年3月22日报道，更多的动态防御技术被美国国家专利局授权，特别是专利号为9294504的技术已经开始商用。

在我国，“拟态安全防御”理论的研究和实验取得阶段性成果，其中拟态安全防御主要针对基于未知的可利用漏洞或后门的攻击进行防御，通过变化的多样性、随机性、快速性，实现了网络安全动态性、主动性的效果。2013年我国科学家邬江兴院士基于“拟态计算”提出“拟态安全防御”理论，与十余家院校、科研院所及国内信息技术企业合作，在2016年年初研制成功“Web服务器拟态防御原理验证系统”和“路由器拟态防御原理验证系统”。

## 7 软件定义网络SDN

随着大数据、云计算、和移动流量等大需求数据源的出现，网络中产生了海量种类繁多的流量，为了实现网络的适应性和可扩展性，软件定义网络（SDN）和网络功能虚拟化（NFV）在各种网络服务和应用中得到了快速部署<sup>[5]</sup>。

软件定义网络SDN是由美国斯坦福大学Clean State课题调研组提出的一种新型网络创新架构，是网络虚拟化的一种实现方式。它利用OpenFlow协议将路由器的控制平面（control plane）从数据平面（data plane）中分离，改以软件方式实现。该架构可使网络管理员在不更新硬件设备的前提下，以中央控制方式用程序重新规划网络，为控制网络流量提供了新方案，也为核心网络和应用创新提供了良好平台<sup>[6]</sup>，SDN的体系结构如图1所示。

Facebook与Google都在他们的数据中心中使用OpenFlow协议，并成立了开放网络基金会来推动这个技术。

## 7.1 OpenFlow

OpenFlow是一种网络通信协议，属于数据链路层，能够控制网络交换器或路由器的转发平面，借此改变网络数据包所走的网络路径。被认为是SDN标准之一。它最初在SDN环境中定义了通信协议，使SDN控制器能够与物理和虚拟的交换机和路由器等网络设备的转发平面直接进行交互，从而更好地适应不断变化的业务需求。

OpenFlow允许从远程控制网络交换器的数据包转送表，透过新增、修改与移除数据包控制规则与行动，来改变数据包转送的路径。比起用访问控制表(ACLs) 和路由协议，允许更复杂的流量管理。同时，OpenFlow允许不同供应商用一个简单，开源的协议去远程管理交换机（通常提供专有的接口和描述语言）。

## 7.2 数据平面

SDN数据平面也称为基础设施平面，是网络转发设备的根据SDN控制平面的决策来执行数据传输和处理所处的平面。SDN网络中网络设备的重要特征是这些设备只完成简单的转发功能，不需要内嵌软件来执行自治决策。

数据平面网络设备的主要功能包括：控制支撑功能、数据转发功能。如图所示这些网络设备的转发表必须根据上层协议来定义表象，网络设备进行转发决策时通过检查IP首部，也可以包括分组的其他首部信息来完成。

一个重要的数据流是应用程序编程接口（API），包括OpenFlow协议数据单元（PDU）或其他类似的API协议数据流。

## 7.3 控制平面

SDN控制层将应用层服务请求映射为特定的命令和正式指令并传达数据平面交换机，并且向应用程序提供数据平面拓扑和活动性的信息。控制层作为服务器或服务器的协同操作集合来实现，称为SDN控制器。

SDN控制器提供的功能可以被看作网络操作系统，提供基本的服务、通用的API和对研发者的低层元素的抽象。目前一些商业和开源SDN控制器已经实现，如OpenDaylight、开放网络操作系统、POX等等。

其中OpenDaylight是一个由Linux基金会主持的开源项目，实际上包括每个主要的网络组织、SDN技术的用户和SDN产品的厂商参与。其目的是生产一个可扩展、开源、虚拟化的网络

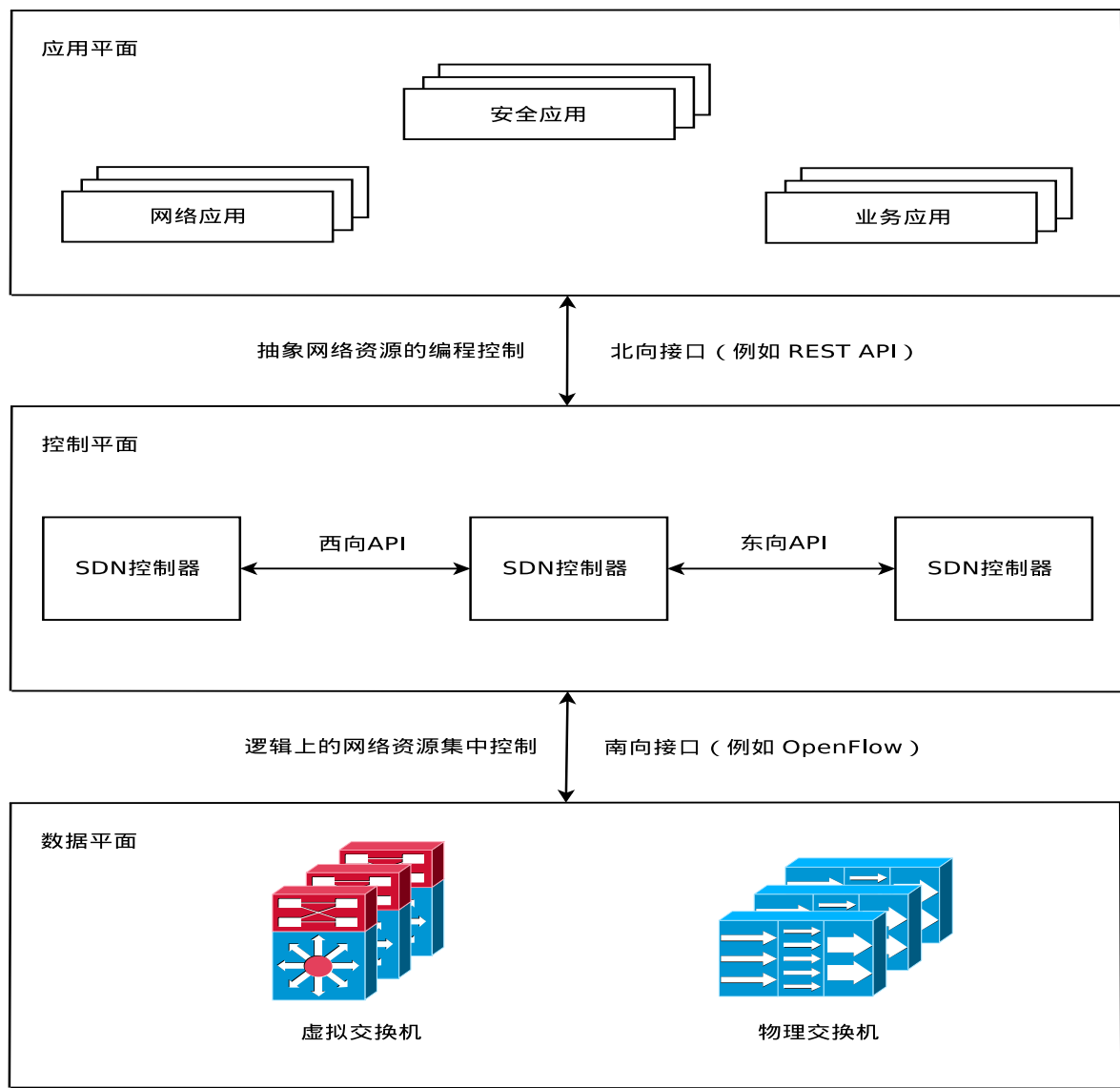


图 1: SDN体系结构

平台，为研发者利用、贡献和建造商业产品与技术提供共同的和开放的SDN平台。

## 7.4 应用平面

SDN是当前网络领域最热门和最具发展前途的技术之一。鉴于SDN巨大的发展潜力，学术界深入研究了数据层及控制层的关键技术，并将SDN成功地应用到企业网和数据中心等各个领域。

SDN的应用领域十分广泛，比如对网络流行为进行动态分析、管控和预测的流量工程，流量工程中的典型为自动化的QoS策略实施框架PolicyCop。

最主要的是在数据中心的应用，由于数据中心的网络需求，传统的网络体系很难全部满足，SDN则在一定程度上对这些进行优化改进。

目前最新的成果分别为<sup>[7]</sup>：

基于SDN的大数据：HotSDN'12会议论文中溢出的一种利用SDN对数据中心网络的大数据应用进行优化的方法。

基于SDN的云网络：云网络即服务（CloudNaaS）是一种云网络系统，充分利用OpenFlow和SDN功能为云客户提供对云网络功能高度控制。

基于SDN的信息中心网络：目前尚未对SDN和信息中心网络如何结合达成一致，已经提出的方法包括对OpenFlow协议进行加强和修改、使用OpenFlow交换机和信息中心网络路由器之间的抽象层等。

## 8 网络功能虚拟化NFV

### 8.1 NFV概念及架构

网络功能虚拟化（NFV）是一种对于网络架构的概念，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。目前被定义为运行在虚拟机上且利用软件实现网络功能的虚拟化技术，将NAT、防火墙、入侵检测、域名服务、高速缓存等网络功能从专用硬件设施中分离出来，以软件的形式在虚拟机中运行和实现<sup>[8]</sup>，如图2所示。

NFV和SDN彼此之间没有必然联系。NFV即使脱离SDN，也能实现，在传统的网络架构中，将PNF（Physical Network Function）替换成虚拟化的NF，再辅以传统的NF连接方式，也能实现NFV。而SDN更是可以脱离NFV实现。

但是，另一方面，NFV和SDN如果相互结合，又可以是互补的存在。借助SDN，不仅传统的NF连接方式都能支持，SDN还能提供更高效的NFV实现方式。SDN提供的管理层和转发层的分离，使得网络变得极其灵活。反过来，NFV也能够提供SDN的运行环境，帮助SDN的实现<sup>[9]</sup>。

ETSI和Linux基金会都在积极地开发和培育NFV框架的参考架构和标准体系。ETSI管理下的OSM（Open Source MANO）和LF管理下的ONAP（Open Network Automation Platform）是目前由服务运营商和网络厂商们所支持的、最重要的开源NFV项目。

在ETSI NFV架构中，NFV MANO提供核心操作功能，并由四个部分组成：NFV编排器（VNF Orchestrator）、VNF管理器（VNF Manager）、虚拟化基础设施管理器（VI Manager, Virtualized Infrastructure Manager）以及这些功能模块与其他操作系统之间的互通。

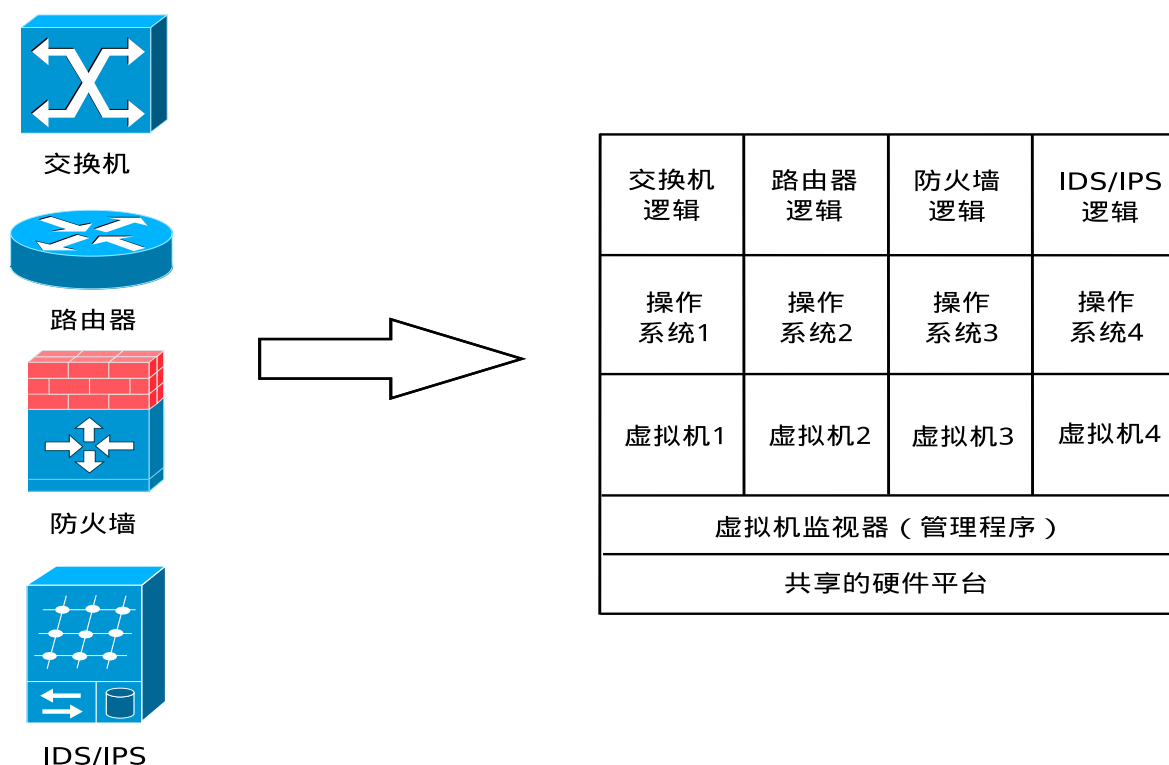


图 2: 网络功能虚拟化

在ETSI NFV框架下，NFV编排器、VNF管理器和VI管理器提供了主要的NFV MANO功能。NFV MANO主要有四个方面的职责，为服务提供商们带来相应的好处，譬如快速的业务创新、弹性的网络功能部署、提升的资源利用率、资本性支出和运营成本的降低；

与操作系统、OSS/BSS系统的交互；在网络服务中编排VNF，在虚拟资源上部署和运营VNF和网络服务实例，并对VNF和网络服务实例进行生命周期管理；与网元管理（EM）进行交互，从而管理其逻辑功能，并确保VNF服务包括VNF故障、配置、计帐、性能和安全管理（FCAPS）；与网络功能虚拟化基础设施（NFVI）交互，从而在VNF部署的地方，实现分配、管理和编排虚拟资源，包括计算资源、存储资源、网络资源等。

## 8.2 SDN与NFV

介绍了上述两种技术后，存在一个问题，那就是SDN与NFV能否共用？

SDN与NFV有许多共同的特征，它们的目标都是：

- (1) 将功能迁移到软件中实现。
- (2) 使用商用硬件平台来替代专用平台。
- (3) 使用标准化或开放的应用程序编程接口（API）。
- (4) 支持更高效的网络功能演化、部署和位置调整。

NFV和SDN是独立而又互补的机制。SDN将网络流量控制的数据平面和控制平面分离开来，使得数据流的控制和路由变得更加灵活和高效。而NFV则利用虚拟化技术将网络功能从特定硬件平台

分离出来，从而使这些功能更加高效和灵活地实现。虚拟化技术可以应用到路由器的数据转发功能和其他网络功能上，包括SDN控制器的功能等，这样两种技术可以单独使用，也可以结合起来取得更大的收益。

归根结底，网络服务提供商最终所关心的还是网络设备和这些设备所实现功能的控制和管理。

如果采用NFV技术，这些网络功能都以软件的形式实现，并运行在虚拟机中。而如果这些网络功能在专用设备上完成，并且采用SDN技术，那么中央控制器将完成控制功能，它会与网络设备进行交互。

然而，SDN和NFV技术并不是互斥的，如果网络同时采用了SDN和NFV，那么它们之间要保持下述关系：

- (1) 网络的数据平面功能在虚拟机上实现。
- (2) 控制平面的功能可以在专用的SDN平台或者SDN虚拟机上实现。

无论采用上述哪种控制平面实现方法，SDN控制器都要与运行在虚拟机上的数据平面进行交互。

目前，实现QoS的常见案例都没有采用NFV和SDN的。如果采用两NFV而没有使用SDN，QoS的设置由虚拟机来完成。如果采用两SDN，无论是否采用了NFV，SDN控制器都将负责实施QoS参数。

## 9 云和物网络

### 9.1 云计算

#### 9.1.1 云计算概念

目前许多组织机构越来越倾向于将其部分或者全部信息技术操作移植到具有因特网连接的基础设施上，并称为企业云计算。PC和移动设备用户也越来越以来云计算技术来备份数据、同步设备并进行共享。

应用最广的是NIST所定义的云计算，包括五种特性：广泛的网络接入、快速的弹性、可测量的服务、按需服务、资源池化；三种服务模型：软件即服务Saas、平台即服务PaaS、基础设施即服务IaaS；四种部署模式：公有、私有、混合、社区。

#### 9.1.2 云计算新进展

同样有很多其他的云服务，比如ITU-T Y.3500中提出的通信即服务CaaS、计算即服务CompaaS、数据存储即服务DSaaS、网络即服务NaaS等。

XaaS是云服务配置中的最新进展，表示X即服务，X可以表示任何可能的云服务类型。能够对服务类型进行一站式采购。

由于云计算出现的时间早于SDN和NFV，这两种技术出现后，对于云计算有很多的吸引力。这两种技术与现有云计算模型的结合成了研究的热点。

比如：在各种情况下研究了周期性数据流在真实SDN硬件上的性能。这项工作使用抢先式流安装机制（PFIM），通过预测何时可能需要特定规则来限制控制器查找的数量，从而提高SDN周期性

通信的性能。实验结果表明，该系统可以检测到大多数临时周期性流量并抢先安装流量规则，从而提高了与第二层交换速度相当的性能<sup>[10]</sup>。

## 9.2 物联网

### 9.2.1 物联网概念

物联网（IOT）是指通过 各种信息传感器、射频识别技术、全球定位系统、红外感应器、激光扫描器等各种装置与技术，实时采集任何需要监控、连接、互动的物体或过程，采集其声、光、热、电、力学、化学、生物、位置等各种需要的信息，通过各类可能的网络接入，实现物与物、物与人的泛在连接，实现对物品和过程的智能化感知、识别和管理。

被广泛应用与物联网的射频识别技术（RFID）是一种简单的无线系统，由一个询问器（或阅读器）和很多应答器（或标签）组成。标签由耦合元件及芯片组成，每个标签具有唯扩展词条一的电子编码，附着在物体上标识目标对象，它通过天线将射频信息传递给阅读器，阅读器就是读取信息的设备。

同样还有基于无线自组织网络的无线传感器网络、以及专门为无线传感器网络所研发的ZigBee协议，特点为短距离、低复杂度、低功耗、低数据速率、低成本。

### 9.2.2 物联网最新进展

2015年，思科推出了一套被称为思科IoT系统的集成和协调产品，通过基础设施来解决数字化的复杂性，旨在管理由多样化的端节点和平台组成的大型系统以及他们创建的海量数据。

目前物联网的安全问题被广为关注，在近几年网络安全业内加强对物联网安全研究，将物联网风险观察分析推动到解决方案研究之际，2016年10月，发生了导致半个美国互联网陷入瘫痪的物联网安全事件：数个品牌、不同类型的、数量巨大的物联网设备因端口及口令缺陷成为对美国最大域名服务商发起大规模DDoS攻击的攻击源。

思科2015年的一份IoT安全方面的白皮书，提出了一个安全的IoT框架，目前仍未部署。

## 9.3 云计算与物联网的联系

作为IT业界的两大焦点，其实云计算、物联网两者之间区别比较大，不过它们之间也是息息相关的，首先物联网通过传感器采集到海量数据，然后云计算对海量数据进行智能处理和分析。

云计算与物联网二者相辅相成，其中云计算是物联网发展的基石，同时作为云计算的最大用户，物联网又不断促进着云计算的迅速发展。

在云计算技术的支持下，物联网能够进一步提升数据处理分析能力，不断完善技术。假如没有云计算作为基础支撑，物联网工作效率便大大降低。那么其相比传统技术的优势也不复存在。由此可见，物联网对云计算的依赖性是很强的。物联网业务量逐渐增加，从而对数据存储、分析计算的能力提出更高要求，由此便有了云计算技术。

实际上，云计算是真正实现物联网应用的核心技术，人类运用云计算的模式，能够进行物联网中不同业务的实时动态的智能分析和决策。同时，在为物联网提供便捷和按需应用时，云计算做出了重大贡献。

一般来说，云计算可以为物联网的海量数据提供足够大的存储空间，而云存储则可通过网格技术、分布式技术等将不同类型的设备集合应用起来，协同起来对外提供数据存储以及业务分析等功能。

## 10 新型无线网络

随着应用需求的增加，越来越多的新型网络面世，在多种网络中，得到广泛应用的并不多，结合应用介绍几种较为新型的网络。

### 10.1 无线自组织网络

无线自组织网络即(Mobile Ad Hoc Network)，是一种不同于传统无线通信网络的技术。

传统的无线蜂窝通信网络，需要固定的网络设备如基站的支持，进行数据的转发和用户服务控制。而无线自组织网络不需要固定设备支持，各节点即用户终端自行组网，通信时，由其他用户节点进行数据的转发。这种网络形式突破了传统无线蜂窝网络的地理局限性，能够更加快速、便捷、高效地部署，适合于一些紧急场合的通信需要，如战场的单兵通信系统。但无线自组织网络也存在网络带宽受限、对实时性业务支持较差、安全性不高的弊端。国内外有大量研究人员进行此项目研究。

无线自组织网络(mobile ad-hoc network)是一个由几十到上百个节点组成的、采用无线通信方式的、动态组网的多跳的移动性对等网络。其目的是通过动态路由和移动管理技术传输具有服务质量要求的多媒体信息流。通常节点具有持续的能量供给。

应用上无线自组织网络最典型的是与物联网相结合，构建无线传感器网络。传感器网络使用无线通信技术，由于发射功率较小，只能采用多跳转发方式进行通信。分布在各处的传感器节点自组织成网络，以完成各种应用任务。

### 10.2 无线mesh网络

与传统无线网络不同的是在无线Mesh网络中，任何无线设备节点都可以同时作为AP和路由器，网络中的每个节点都可以发送和接收信号，每个节点都可以与一个或者多个对等节点进行直接通信。

种结构的最大好处在于：如果最近的AP由于流量过大而导致拥塞的话，那么数据可以自动重新路由到一个通信流量较小的邻近节点进行传输。依此类推，数据包还可以根据网络的情况，继续路由到与之最近的下一个节点进行传输，直到到达最终目的地为止。这样的访问方式就是多跳访问。

与传统的交换式网络相比，无线Mesh网络去掉了节点之间的布线需求，但仍具有分布式网络所提供的冗余机制和重新路由功能。

在部署安装、非视距传输、网络稳定性等方面有着传统无线网络所不能比拟的巨大优势。

## 11 深度学习与现代网络

我们正在从事的深度学习的研究与当前的网络发展也息息相关。

基于网络本身的,有深度学习应用协议识别技术<sup>[11]</sup>,通过创建一个网络协议分析库,深入网络数据包,进行深度学习的应用层协议分类与分析识别,以提高协议检测的准确性。根据大量主流应用程序的流特征进行深度学习,建立应用协议特征库,通过算法实现应用层协议的识别。研究一种应用于APT攻击防御系统、网络入侵检测系统与Web审计系统的应用层协议识别技术,可提高对APT攻击防御判断的准确性。

云计算对于深度学习,除了物联网用到的云计算之外,较为重要的是云计算平台实现的计算资源的共享,随与深度学习的发展起到了极大的推进作用,很多因为算力限制的研究者能够通过云计算实现自身的想法。

同样与云计算息息相关的物联网,IoT的一大部分应用场景中,输入深度学习的数据是图片或视频。每天,每个人都在用手机的高清摄像头拍摄者图片和视频,除此之外,家居、校园或工厂也在使用智能摄像头。所以,图像识别、分类、目标检测是这类设备的基础应用。随着智能手机和可穿戴设备的普及,语音识别也成了人们和自己的设备互动的一种自然而方便的方式。

在智能家居、智慧城市、智能交通系统等方面,物联网与深度学习的结合已经相当深入,已经得到了很好的应用。

随着网络的发展与深度学习的发展,两者相结合的应用将会越来越多,也将是未来发展值得期待的一个方向。

## 参考文献

- [1] 徐恪,徐明伟,陈文龙.高级计算机网络[M].北京:清华大学出版社,2012.10.
- [2] 凌力.高级网络概论[M].北京:清华大学出版社,2011.7.
- [3] 田果,刘丹宁,余建威.高级网络技术[M].北京:人民邮电出版社,2017.11.
- [4] 卜哲.网络安全新技术及发展趋势[J].世界电信,2016.4.
- [5] William Stallings.Foundations of Modern Networking[M].北京:机械工业出版社,2018.1.
- [6] 张朝昆,崔勇,唐, et al. 软件定义网络(SDN)研究进展[J]. 软件学报, 2015, 26(1):62-81.
- [7] 张顺淼,邹复民. 软件定义网络研究综述[J]. 计算机应用研究, 2013, 30(8):2246-2251.
- [8] 唐宏,欧亮. 网络功能虚拟化中的网络转发性能优化技术研究[J]. 电信科学, 2014, 30(11):135-139.
- [9] 赵慧玲,解云鹏,史凡. 网络虚拟化及网络功能虚拟化技术探讨[J]. 中兴通讯技术, 2014.3:12-15.
- [10] Bull P, Murphy S, Junior N, Austin R, Sharma M. A flow analysis and preemption framework for periodic traffic in an SDN network. Concurrency Computat Pract Exper. 2018.
- [11] 叶松. 基于现代网络的深度学习应用协议识别技术研究是实现[J]. 软件导刊, 2018, 17(10):198-203.