SDN概述1.1SDN研究背景及意义随

1 SDN概述  
1.1 SDN研究背景及意义  
随着终端计算处理能力的提高、网络传输能力的不断扩大，网络所承载的信息急剧膨胀，网络不再单纯以通信为目的，而是朝着尽可能满足人们需求的方向发展。因此，在现代社会，网络已经成为一个信息承载和分发的平台。然而，传统的网络架构在经历30年的发展后，因其由不同技术标准、不同厂商的交换机、路由器、终端等设备组成，而这些网络设备又使用着封闭、专有的内部接口，并运行着提供网络拓扑发现，流量监控和访问控制功能的大量分布式协议。这些设备将数据平面和控制平面高度集中，因网络操作员必须对每个独立的设备的每个协议进行独立配置，在这种情况下，传统的网络架构对处理日益庞大的数据已经显得力不从心，常常难以满足当今企业、运营商以及用户的需求。在这种封闭式的网络环境下，给网络功能扩展和管理带来了巨大挑战，网络创新已经成为了一大难题。  
2006年，斯坦福大学启动了“Clean-Slate Design for the Internet”项目[1]，该项目旨在研究提出一项新的网络技术，突破当前互联网基础架构的限制，以更好地支持新的技术应用和创新。其核心理念是使网络软件化，并充分实现网络开放，从而使得网络能够像软件一样便捷、灵活，以提高网络创新能力。  
为了支持这个项目的实现，2008年斯坦福大学的Nick Mckeown教授将其命名为OpenFlow，其核心思想是将传统网络设备的数据平面（Data Plane）和控制平面（Control Plane）分离，通过集中控制器以标准化接口对各种网络设备进行分配和管理。后经由斯坦福Clean State项目推广，以及GENI（Global Environment for Network Innovations）项目中的应用，这个概念被逐渐扩展并成为了SDN。  
在OpenFlow的网络中，集中的控制器取代了传统设备的路由决策，并且直接决定了数据包在整个网络的传输路径。数据平面只需提供对OpenFlow协议的支持，部署到不同的网络中去，而不再需要专有的网络互连设备，从而将网络创新完全转移到控制平面的控制策略开发上来。这样的设计大大加速了新协议的开发、测试和部署。因为这些优点，基于OpenFlow的软件定义网络（Software-Defined Network，SDN）成为了近年来业界热议的焦点。  
1.2 SDN概念及定义  
SDN作为一项最有希望实现网络虚拟化的新兴技术，允许控制平面和数据平面分离，从而实现集中化，控制平面可编程和数据平面抽象化。因而，网络运营商能够直接控制和管理自己的虚拟资源，且在广播时无需对网络设备硬件进行识别。控制平面和数据平面的分离，使得控制平面能够直接进行集中化的编程和管理，数据平面也更简易化和抽象化，而不是使用代价高昂的特殊网络硬件。  
  
图1 SDN基本原理  
图1是SDN的基本原理说明。SDN采用数据抽象转发模型，将网络资源虚拟化，使得计算机可以摆脱网络的束缚，把交换机的转发过程抽象为“流表”(Flow Table)。控制设备为NOS（网络操作系统），通过OpenFlow或者其他协议控制转发平面的SDN转发设备。  
SDN转发设备本身并没有智能，而是完全按照NOS下的流表进行流量转发。流表包含匹配规则和行为，按规则转发数据流。除此之外，SDN转发设备将网络时间转发给NOS，供NOS作决策。  
SDN的出现，使得数据中心网络具备了可编程性，数据中心网络流量优化、支持多租户、虚拟机迁移成为可能。  
1.2.1 可编程控制平面  
对SDN来说，控制平面和数据平面是分离开来的，而控制平面可以直接进行集中化编程。这就要求SDN有3个开放的接口：控制平面的南向接口，北向接口和东西向接口。  
（1）南向接口：位于可编程控制平面和数据平面之间的接口。SDN控制器通过利用SDN提供的转发平面抽象来构建全局网络视图，因为不再需要理解和处理成千上万个协议标准，只需接受来自SDN控制器的指令，从而极大简化了网络的设计和运行。  
（2）北向接口：位于应用程序/服务和网络基础设施（或控制器）之间的接口。逻辑上集中的基于软件的SDN控制器，负责维护全局网络视图，网络可看成一个逻辑或者虚拟是实体，并向上层应用提供用于实现网络服务的可编程接口。  
（3）东西向接口：控制器之间的接口。这个接口可以把整个网络定义为一个逻辑的交换机，同时，利用控制器提供的应用程序编程接口（API），网络操作人员可以在这上面灵活地编写多种网络应用程序，如接入控制、快带管理、服务质量（QoS）、流量工程等形式的策略管理。  
  
图2 SDN参考架构和应用程序接口  
1.2.2 数据平面抽象化  
数据平面的抽象化要求SDN能够很好的定义一般的数据平面模型[2]，而不是使用特殊的硬件，所用到的SDN的数据平面抽象模型包括：  
（1) 数据包转发抽象模型（Ethernet,Ipv4,Ipv6等）。Ipv4、Ipv6等是现在最常用到的数据包转发模型，主要用于提供互联网地址空间。在现有的具体转发协议基础上，对其进行抽象化，有助于SDN数据平面技术的进一步探索。  
（2）电路交换抽象模型（光学，多协议标签交换（MPLS））。  
（3）分组核心演进（Evolved Packet Core, EPC），支持LTE，是4G长期演进（LTE）网络上提供汇聚语音的架构。2G和3G架构处理并转换通过两个子域的声音和数据：电路交换（CS）针对声音，分组交换针对数据。分组核心演进在互联网协议（IP）服务架构上统一声音和数据，而数据就作为另一个互联网协议应用。使得操作者针对2G、3G、WLAN、LTE和固定接取（以太网，DSL，光缆和光纤）部署并运行分组网络。  
1.3 SDN特点  
SDN的基本特征如下：  
（1）控制与转发分离。转发平面受控转发的设备组成，转发方式以及业务逻辑由运行在分离出去的控制面上的应用程序所控制。  
（2）转发平面之间的开放接口。SDN为控制平面提供开放的网络操作接口（也称为“可编程接口”。通过这种方式，控制应用只需要关注自身逻辑，而不需要关注底层的实现细节。  
（3）逻辑上的集中控制。逻辑上的集中控制面可以控制多个转发设备，也就是控制整个物理网络。因此，可以获得全局的网络状态视图，并根据全局网络状态视图实现对网络的优化控制。  
总之，SDN将网络从硬件转移到软件，用户不需要更新已有的硬件设备就可以为网络增加新的功能。这样不仅简化和整合了控制功能，让网络变得更加可靠，还有助于降低设备的购买和运营成本。控制平面和数据平面分离之后，厂商可以单独开发控制平面，并能与ASIC、商业芯片或服务器技术相集成。由于SDN具有上述特点，因此SDN的发展能为将来网络产业格局带来重大调整，这就意味着，传统的通信设备业将面临着重大挑战，同时也将为IT和软件企业迎来新的市场机遇。因此，SDN的出现可能会彻底颠覆目前的互联网产业现状。  
  
2 SDN研究现状  
2.1 SDN的体系架构  
图3是SDN体系架构模型[3]。该模型分为3层，其中基础设施层主要由OpenFlow协议的SDN交换机组成。控制层主要包含OpenFlow控制器和网络操作系统（Network Operation System, NOS）。NOS是利用网络底层所提供的数据传输功能为高层网络用户提供各种服务软件及相关规程的集合。控制器是一个平台，平台下可以直接与OpenFlow交换机进行会话；平台上，为应用层软件提供开放接口，用于检测网络状态，并下发控制策略。位于顶层的应用层由众多应用软件组成，这些应用软件可以根据控制器提供的网络信号执行特定的控制算法，并将结果通过控制器转化为流量控制命令，下发到基础设施层的实际设备中。  
  
在这一架构下，开发和标准化是核心的关键。标准化数据平面和控制平面的接口，屏蔽网络基础设施在类型、协议等方面的异构性，使得数据平面的网络资源设施能够无障碍地接收控制平面的指令，承载网络的数据转发业务；标准化控制层和应用层的接口，为上层应用提供了统一的管理视图和编程接口，使用户可以通过软件从逻辑上定义网络控制和网络服务。  
2.2 SDN基础理论  
2.2.1 OpenFlow协议  
OpenFlow协议是SDN的核心协议。OpenFlow协议OpenFlow 交换机和控制器通信提供了开放的标准化接口。借助于定义好的API，控制器就可以接受交换机的请求，发送指令修改交换机的流表，从而控制数据流的走向。  
2.2.2 网络虚拟化  
随着虚拟服务器、桌面、应用、存储等虚拟化技术的广泛应用，网络虚拟化已成为数据中心技术发展的一大助力。网络虚拟化的目的是为了共享同一物理网络资源上划出的独立的网络，以满足多租户、流量隔离和逻辑网络自由管控的应用趋势。成熟的虚拟局域网（VLAN）就是一种典型的网络虚拟化技术，但最多只能够划分出4096个逻辑网络，在拥有成千上万台物理主机的大环境下显然是不可能满足人们实际需求的。  
网络虚拟化是基于软件结合网络硬件和软件集网络资源和网络功能为一体的功能性实体，网络虚拟化有如下几个要求：  
（1）可编程能力，其中包括可编程控制面和转发面。  
（2）已知的拓扑结构，不仅是提供连接，还需要知道相关的拓扑结构。  
（3）可快速重构，能够对快速进行重新配置。  
SDN网络对基础网络硬件设施进行抽象，应用层只看到控制器抽象过的网络视图，为网络虚拟化提供了天然优势[4]。在这种情况下，SDN网络就相当于主机服务器，基础网络设施相当于服务器硬件资源，控制器是NOS，SDN应用相当于主机应用程序，网络虚拟化可以在NOS之下设计网络超级管理者实现[5]，也可以在控制器增加虚拟抽象层实现。  
2.3 SDN研究热点  
2.3.1 FlowVisor  
FlowVisor是建立在 OpenFlow 之上的网络虚拟化平台，引入 FlowVisor 后的OpenFlow网络架构如图4所示。  
  
图4 FlowVisor的OpenFlow网络架构  
对于控制器而言，FlowVisor是普通的交换机；从 OpenFlow 交换机的角度来看，FlowVisor 就是一个控制器。总的来说，FlowVisor 就是位于硬件结构元件和软件之间的网络虚拟层。 FlowVisor将物理网络分成多个逻辑网络， 从而允许多个控制器同时控制一台 OpenFlow 交换机，但是每个控制器仅仅能够控制经过这个OpenFlow交换机的某一个虚拟网络（即网络切片）。因此，通过FlowVisor建立的实验平台可以允许多个网络实验在不同的虚拟网络上同时进行。  
网络切片（Slice）是FlowVisor实现管理功能的要素，Slice由一组文本配置文件定义。文本配置文件包含控制各种网络活动的规则，如允许，只读和拒绝等，规则范围的表达范围包括流量的来源IP地址、端口号和数据分组的表头信息。  
由于FlowVisor是建立在OpenFlow控制器基础上的，因此，FlowVisor与一般交换机是兼容的。目前FlowVisor正处于试验阶段，主要部署在校园网（如斯坦福大学）。  
2.3.2 NOS  
在SDN中，NOS特指允许在控制器上的网络控制平台。控制器的控制功能就是由NOS来实现的。NOS类似于OpenFlow网络的操作系统，通过交换机操作来管理流量。图5为NOS在网络中的位置。  
  
图5 NOS在网络中的位置  
从整个网络的角度来看，网络操作系统是抽象网络中的各种资源，从而为网络管理提供易用的接口。由此，可以建立网络管理和控制的应用。因此，NOS本身并不完成对网络的管理任务，而是通过其运行的各种应用来实现各种管理任务。管理者和开发者可以专注与这些应用的开发，而不必花费心思在底层的开发细节上。为此，NOS则需要提供尽可能多的通用接口，以满足各种不同的需求。  
NOS上运行的应用软件通过流量信息来建立网络视图（Network View），并确定流量的行为。正是有了NOS，SDN才能针对不同的应用建立不同的逻辑网络，并实施不同流量管理策略。目前，较为流行的NOS有NOX、Beacon、Trema、Maestro等。  
2.3.3 支持多租户  
因为SDN的可编程能力，SDN NOS可以加载应用模块，识别不同租户的网络流量。通过流量表的控制，使得数据流只能在同一租户的虚拟机之间转发。租户通过所分配的虚拟数据中心，资源按需分配；租户资源隔离，独立分配IP、MAC地址和网络策略。  
2.3.4 网络流量优化  
根据每个虚拟机所在的位置，SDN的NOS通过探测网络拓扑，能计算出每两个虚拟机之间的最佳路径，使流量按最佳路径转发。而且，SDN的NOS还能支持多路径转发、基于约束条件的最短路径转发、服务器负载的流量工程调度，从而实现广播抑制，通过支持ARP减少宽带消耗。SDN架构能灵活修改设备流表，从而改变数据报文转发路径。  
2.3.5 SDN和Non-SDN网络互通  
SDN作为一种新的网络架构，必须考虑到实际部署过程中与传统非SDN（Non-SDN）网络共存的问题。对于这个问题，有三种可能会出现的情况：  
（1）全由OpenFlow交换机组建的SDN网络。在这种情况下，可以将整个网络抽象成为单台交换机或者路由设备；  
（2）OpenFlow交换网络中间连接有传统交换机或路由设备。SDN控制器就无法跨越多个传统Non-SDN网络设备；  
（3）整个网络存在多个SDN网络和多个传统Non-SDN网络。SDN控制器之间分配一条带QoS保证的链路问题。  
目前，已经有研究采用多层封装和隧道技术来解决这个问题，但在SDN上层业务确定之前，SDN和Non-SDN网络边界的确定也是一个值得深究的问题。  
2.3.6 SDN在BDP网络设备交付和吞吐量优化  
今天，数据传输需要经过大型宽带延时乘积（Bandwidth-Delay Product, BDP）网络。由于这种传输方式需要极其特殊的配置，这便增加了复杂性和额外的费用。这是一个典型的SDN应用案例。在SDN范畴中，控制器能够通过报文的报头字段来进行转发控制、重写和丢包。用软件定义的方式来处理数据包，对提高效率、节省成本和提高用户体验有着显著的影响。  
随着互联网的全球化，两端的数据传输常常需要经过更远的距离，在这个过程中，往往导致更长的往返时间（RTT）和更高的丢包率。传输控制协议（TCP），是事实上在互联网上提供可靠传输的协议。然而，不幸的是，由于TCP的先天性不足，在性能严重降低的情况下，RTT和丢包率都很高。因此，为了提高TCP在大型BDP网络中的性能，SDN也能被用来作为在BDP网络优化吞吐量的解决方案。但由于就目前情况来说，大多数用户还并不了解眼前的问题，SDN在BDP网络中的探索也还有很长的路。  
如前面所提到的， SDN一个可以分离任意一组以太网交换机控制平面和数据平面的网络架构。这就意味着，控制平面可以通过软件来控制数据平面来转发数据包。其中，OpenFlow是支持软件控制器与以太网交换机数据包处理规则（数据平面工作）通信的通信协议（控制平面协议）。OpenFlow的SDN，软件定义网络能够轻松的做出转发决策，甚至可以只是数据平面上的数据包进行数据包报头重写。这就使得服务供应商能够通过编程无缝地部署新的任务，改善用户体验，同时保持传统协议与网络服务的兼容。  
OpenFlow是一个集中化的连接到控制器的交换机模式（也被称为数据通路），并告诉其如何处理数据包。OpenFlow使用交换机内的流表来匹配数据包。当数据包进入OpenFlow交换机，交换机首先检查数据包是否匹配现有的流条目。如果不匹配，则通过控制平面将数据包转发至控制器[3]。  
控制器通过流输入现在已经有能力交换机如何处理这些类型的数据包。每个流输入都有个动作指令，范围从丢弃，输出端口到重写数据包报头。一旦控制器在交换机建立了流输出，数据包匹配则不再发送到控制器而是交给交换机直接以线速处理。  
OpenFlow容许多个研究人员通过切片尝试不同的转发方法。切片是通过一个名为FlowVisor的特殊的控制器来完成的。研究人员利用FlowVisor通过特殊报头或物理端口号来控制流量子集；然后FlowVisor透明的发送匹配特定研究人员自身的软件控制器的流量匹配。此外，OpenFlow使得生产网络成为了测试平台。例如，在同一网络的一个生产切片可以用来处理一般流量，以及实验性的切片则能够使研究人员测试出更多新的想法，而无需冒着破坏网络稳定性的风险。  
  
3 OpenFlow协议  
3.1发表情况及运行原理  
从SDN的技术背景可以看出，OpenFlow协议是SDN实现控制与转发分离的基础。为了推动SDN的发展并统一OpenFlow标准，业界组建了标准化组织开放网络基金会（Open Networking Foundation, ONF）。目前，ONF已经成为SDN标准制定的重要推动力量，其宗旨就是使基于OpenFlow协议的SDN成为网络的新标准。自2009年10月发布OpenFlow标准的第一个版本以来，ONF先后发布了1.1，1.2，1.3等版本。表1是OpenFlow协议发表详情[12]。  
表1 OpenFlow协议发表详情   
  
  
图6 OpenFlow运行原理  
一个OpenFlow交换机包括一个或者多个流表（Flow Table）和一个组表（Group Table）。流表中的每个流条目包括以下3个部分。  
（1）匹配（Match）：根据数据分组的输入端口、报头字段以及前一个流表传递的信息 ，匹配已有的流条目。  
（2）计数（Counter）：对匹配成功的分组进行计数。  
（3）指令（Instruction）：包括输出分组到端口、封装后送往控制器、丢弃等操作。  
如前文所述，OpenFlow的设计目标之一就是将网络设备的控制功能与转发功能进行分离，进而将控制功能全部集中到远程的控制器上完成，而OpenFlow交换机只负责在本地做简单高速的数据转发。在OpenFlow交换机的运行过程中，其数据转发的依据就是流表。  
所谓流表，其实可被视作是OpenFlow对网络设备的数据转发功能的一种抽象。在传统网络设备中，交换机和路由器的数据转发需要依赖设备中保存的二层MAC地址转发表或者三层IP地址路由表，而OpenFlow交换机中使用的流表也是如此，不过在它的表项中整合了网络中各个层次的网络配置信息，从而在进行数据转发时可以使用更丰富的规则。  
SDN交换机在接收到数据分组后，首先在本地的流表上查找是否有匹配的流条目。数据分组从第一个流表开始匹配，之后经过多个流表，这种方式叫做流水线处理（Pipeline Processing）。如果某个数据分组成功匹配到了流表中的某个流条目，则更新这个流条目中的 “计数”，同时执行这个流条目中的“指令”；如果没有匹配到，则将该数据流的第一条报文或者报文转发到控制器，由控制器转发决定转发端口。  
3.2 OpenFlow交换机  
OpenFlow是基于流来定义的。OpenFlow的流定义是指，具有某种特征、需要进行相同处理的一系列数据包，如来自特定MAC地址或者IP地址的数据包、具有相同的VLAN 标签的数据包、同一个交换机端口的数据包等。  
OpenFlow的交换机可以分两类。  
（1）纯OpenFlow交换机：专门为支持OpenFlow而设计，不支持现有商业交换机。交换机不再具有控制逻辑，而是作为一个数据路径部件在端口转发数据包。  
（2）支持OpenFlow的交换机：在商业交换机的基础上添加流表、安全通道和OpenFlow协议来获得OpenFlow特性。既有商业交换机的转发模块，又有OpenFlow的转发逻辑，可以采用不同的方式来接收数据包。  
3.3 OpenFlow技术架构  
OpenFlow技术是SDN实现转发抽象的核心。OpenFlow的主要组件有OpenFlow交换机，控制器和OpenFlow协议。图7是OpenFlow规范的技术架构，主要定义了交换机的功能模块以及控制器之间的通信信道接口。通过这些接口，OpenFlow控制器将制定好的转发测量通过安全的通信信息到转发给交换机，对交换机处理流的方式进行控制。具体的控制策略由是由图8所示的流表（Flow Table）来表示的[13]。  
  
图7 OpenFlow技术架构  
  
图8 OpenFlow流表实例  
每个交换机可以有一个或者多个流表，从0开始依次编号。编号的大小表示流表的跳转顺序，只能从编号小的流表依次或越级跳转至编号大的流表。每个流表包含一系列的流表项，每条流表项由匹配域（Match Field）、计数域（Counter）和指令（Instruction）等字段组成。当数据分组进入流表后，必须从流表0开始向后进行匹配。如果数据分组与流表的某条表项匹配成功，则首先更新该表项队友的计数器，然后根据表项定义的数据进行数据分组处理，包括启动后续流表的匹配、执行数据分组操作等等。如果数据分组已经处于最后一个流表，且仍然未匹配任何规则，则执行默认设置，转发数据分组到控制器或者丢弃。  
在OpenFlow的SDN中，控制和转发平面功能是解耦的。底层的网络设备被上层的控制和应用抽象化。OpenFlow控制器的网络控制和管理功能可以被逻辑上的集中或分散，独立于底层网络。因此，SDN可以提供更高性能、灵活的网络管理，以及对多个厂商网络设备的精确的流量控制。  
3.4 Steroid OpenFlow服务  
Steroid OpenFlow服务（Steroid OpenFlow Service,SOS）是完全由幕后操作，以提高大型BDP网络吞吐量为目的的服务。SOS是无缝解耦终端用户网络协议选择的一个例子。SOS为了做到这一点，需要操纵网络中的流量。然而，这是由网络中以太网交换机OpenFlow协议的软件控制器来完成的。除了检测和选择SOS的候选流量，SOS OpenFlow控制器还负责处理网络中所有类型的流量。除此之外，OpenFlow软件的交换机转发路径的终端主机还配备了SOS的代理。  
当SOS控制器检测到SOS的候选流量时，SOS首先检查终端主机每一侧的连接附近是否有代理。如果是，则控制器通知有关该链接的代理，并安装交换机两端链接的流入口（Flow Entry），以便将流量重定向到附近的代理。代理之间依赖于客户端链接中高吞吐量的数据。远程代理则通过TCP连接到所需的终端主机来交付数据。由于报头重写，整个过程对于客户端来说是完全无缝的。  
为了提供终端用户更好的体验，通过软件定义网络的用户协议选择，解耦网络供应商所使用的协议。SOS经过了多次测试，检测的性能结果显示，SOS能克服TCP的缺憾，并缓解用户配置的复杂性。  
SOS是使用软件定义网络进行吞吐量优化的一个实际案例。在未来的工作中，还会有许多优化工作加入到SOS当中。如压缩、缓存、和自动性能调整等，以防止过饱和网络。今后，利用软件定义网络，探索其他的方法来为用户提供更好的服务。  
3.5 OpenFlow技术的发展趋势  
目前，随着OpenFlow规范的不断更新，支持OpenFlow标准的硬件交换机日益丰富。如NOX,侧重学术研究，尚未出现成熟的商用控制器产品。在应用平面，部署在控制器的网络应用较少，已有的应用多为学术研究模型，因此，功能完善的控制器和上层应用有待于进一步研究和丰富。  
虽然OpenFlow是SDN的核心技术，但实际上OpenFlow并不等于SDN，OpenFlow是SDN体系结构里南向接口的实例。OpenFlow的重要性在不同领域中是不同的，然而就目前来看，OpenFlow的具体的实际应用只在SDN体系结构得到了体现。从目前的发展情况来看，OpenFlow技术的应用还需要较长时间的发展和普及。从技术角度分析，已有的SDN网络架构上，还应该关注复杂问题进一步简化的方法，如转发模型简化，网络操作系统简化等问题。   
  
4 SDN应用  
4.1 SDN应用背景  
早在2012年，SDN就已经被列为未来影响10年的10项技术之一。近年来SDN更是成为业界热议的焦点，业内热议SDN技术走向，应用场景和产业发展趋势。  
SDN最受关注的是商业前景。预测，从2013年到2016年，SDN产业将达到20亿美元以上[7]。Google在开放网络基金会（Open Networking Foundation，ONF）上宣布内部骨干网已经全部实现SDN全面部署，见证了SDN商业化的重要里程碑。此外，VMWare宣布以12.6亿美元收购SDN服务商，正式向商业化迈入重要一步。  
2012年SDN峰会上，国内外多家芯片厂商推出了支持OpenFlow协议的新功能芯片，宣告了主流芯片厂商们已经把OpenFlow提上产品日程。2013年，SDN峰会宣布设立SDN专业技术培训板块，得到了国际权威组织ONF的全面支持。此外，本次峰会国内三大运营商中国电信、中国移动、中国联通齐聚，共同探讨SDN在运营商层面的挑战和机遇。至此，SDN将带来一个网络新时代，网络与应用之间的关系将变得更加微妙。  
4.2 SDN的应用广泛  
随着近几年SDN技术的发展，虽然目前SDN具体的应用尚未普及，但随着研究的不断深入以及技术的进步，SDN关键技术将趋于完善，未来的网络将会越来越依赖于软件。SDN能够在多种网络环境中得到应用，如数据中心网络、广域网、以及移动网络等。因此，互联网将可能进入SDN时代。  
在数据中心网络环境中使用SDN，可以将网络和资源更紧密地联系在一起，从而实现高效的控制。在数据中心内部，利用SDN的优势，可以有效得进行数据中心的路径优化和负载均衡，提高数据中心资源的利用率，降低能量消耗。同时，在多个数据中心利用SDN网络虚拟化技术，可以轻松实现虚拟专用网（VPN）的映射以及虚拟机的迁移。  
同时，在广域网以及移动网中使用SDN技术，对提高网络服务质量也有许多好处。SDN逻辑上的集中控制能够更好地实现网络融合，使网络的统一管理成为可能。利用SDN技术可以在固定网络和移动网络中实现无缝控制，提高VPN管理的灵活性等。已有企业利用OpenFlow技术对移动网络进行高效灵活的网络管理，实现了多种移动通信方式之间的实时动态切换。在运营商网络中利用SDN技术，不但能有效降低网络管理难度[8]，还能加快网络业务部署进度，提供网络服务的适应能力。  
4.3 通信网络中的SDN应用场景  
与现有通信网络相比，SDN架构在网络的控制层的智能边缘转发能力、骨干网络的承载能力、以及网络的开发协同能力具有很强的优越性。从通信网络的架构来看，SDN技术体系可以在云计算中心、通信网络骨干层面、接入层甚至传输层面上引入[9]。  
4.3.1 数据中心的SDN应用场景  
数据中心是全球协作的特定设备网络，用来在ernet网络基础设施上加速信息的传递。通过在数据中心引入SDN，可以在物理网络基础上对资源进行虚拟化，从而解决大规模云计算数据中心在承载多租户业务的时候面临的扩展性[10]和灵活性问题[11]，提升了网络整体的运营能力，从而实现数据中心间的网络智能化承载。  
目前，所使用的SDN数据中心应用方案是Google的全球数据中心网络。Google采用OpenFlow技术，通过10G网络链接分布全球12个数据中心。经过详细的流量工程和优先次序控制，Google将互联的链路使用率从原来的30%到40%提升至将近100%。同时，在全球范围内进行网络拓扑和通信路径的动态调整，以避免故障链路，从而提高网络的可用性和容错能力。  
4.3.2 城域骨干网的SDN应用场景  
城域骨干网是在一个城市范围内所建立的计算机通信网。城域骨干网中，边缘控制设备（如宽带接入服务器BRAS和业务路由器SR）是用户和业务接入的核心控制单元，不仅具备了丰富的网络接口，还实现了业务接入到骨干网络，进行业务交换等功能。边缘控制设备作为用户接入网络的第一跳网关，维护了用户相关的业务熟悉、配置和状态，如用户IP地址、路由寻址表、DHCP地址绑定表、PPPOE会话、QoS等。  
在城域网SDN应用场景中，网络控制器（NOS）需要支持各种远端设备的自动发现和注册，支持远端节点之间的保持连接（Keep Alive）功能，能够接受不同厂商远端设备的信息格式。NOS能够将规划后的转发策略下放给远端设备进行转发，支持下发的策略包括IP地址、基本路由协议参数、QoS策略等，并保证策略下发的一致性。网络边缘设备与NOS之间还支持OpenFlow协议以及其他标准协议。  
4.3.3 接入网的SDN应用场景  
所谓接入网是指骨干网络到用户终端之间的所有设备。其长度一般为几百米到几公里，因而被形象地称为"最后一公里"。由于骨干网一般采用光纤结构，传输速度快，因此，接入网便成为了整个网络系统的瓶颈。在日常运维中，接入网的网络节点工作量异常巨大。业务发放时，要对这些节点进行一一配置，当有新的业务需求要部署时，这些节点则要进行一一升级和更新，延长了新业务的部署周期。显然，项工作的工作量是非常巨大，而且非常容易出错的。  
  
  
5 SDN安全  
安全性是信息时代一个永恒的研究课题。信息作为一种资源，其普遍性、共享性、可处理性和多效用性对人类具有极其重要的意义。信息安全的本质是保护信息系统中的信息免受外界的威胁、干扰和破坏，即保证信息安全。信息安全的含义主要包括信息的完整性、可用性、保密性和可靠性。因此，信息安全是任何国家与组织不可忽略的问题。SDN作为一个新兴的信息产业技术，安全尤为重要。  
5.1 SDN安全特点  
SDN架构实现了网络架构的创新，将传统网络架构中的网络管理功能集中起来，开辟了未来网络的新格局。这种创新除了带来网络管理、运营等方面的灵活性，也使得SDN安全性特点一一呈现出来。  
（1）集中式的网络管理使得网络配置、网络服务访问控制、网络安全服务等问题都集中在SDN控制器上[14]。攻击者一旦成功控制住了SDN控制器，将会造成SDN网络的大面积瘫痪，影响控制器所在的整个网络。在SDN架构下，攻击者的攻击对象越来越集中，极大降低了攻击难度。同时，云计算的发展为攻击者提供了大规模的计算能力，对于原本只有资金雄厚的大企业才能支付得起的网络攻击任务，普通人在云平台上也能轻而易举地实现。  
（2）SDN的开放性使得SDN能够实现统一管理、配置异构网络设备、提供可编程性，但同时也让SDN面临着更多的安全性问题。首先，开放性使得SDN控制器的安全漏洞暴漏在攻击者面前，提供给了攻击者足够的攻击策略素材；其次，SDN架构通过SDN控制器给应用层提供大量的可编程接口，这个层面上的开发性可能会导致接口的滥用，如DDOS攻击等；最后，开放性使得SDN控制器需要谨慎评估开放的接口，以防止攻击者利用这些接口来进行网络监听、网络攻击等。  
5.2 SDN的安全现状及挑战  
随着SDN的研究深入，SDN的问题越来越受到业界的重视。由于各种条件限制，目前的安全问题仍然停滞不前，SDN安全成为SDN蓬勃发展下的一大制约因素。  
尽管SDN架构可以解决网络管理、运营维护和成本问题，但从目前来看，SDN技术应用还需要很长的一段时间的发展和普及，尤其是SDN的安全性问题，将成为制约SDN架构商用化和推广的一个重要因素。从SDN架构来看，Hartman S等人认为SDN的安全问题需求主要集中在控制平面和应用平面之间[15]。  
控制平面和转发平面之间，在一个交换机被一个控制器控制的情况下，安全威胁模型比较简单，现有的OpenFlow中的相关规范基本可以满足相关安全需求；而在一个交换机在被多个控制器控制的情况下，安全威胁模型比较复杂，这正是现有OpenFlow规范所缺乏的。  
5.2.1 控制平面的安全  
集中化的控制平面承载网络环境中所有的控制流，其安全性直接关系网络服务的可用性、可靠性和数据安全性。是SDN首要解决的安全问题。控制平面中，主要面临的威胁包括：  
（1）网络监听。攻击者从网络上获取控制器的切入点后，对控制器上控制指令进行伪造和修改，威胁网络资源的安全。  
（2）IP地址欺骗。攻击者通过网络监听，将控制指令的IP地址修改为控制器的地址，骗取交换机的信任后将其破坏。  
（3）DDOS攻击。攻击者向控制器发送多个服务请求，这些请求的返回地址都是伪造的，直到控制器因过载而拒绝提供服务。  
（4）蠕虫、病毒以及木马攻击。攻击者通过控制器中存在的漏洞，获取控制器的控制权，执行恶意代码。  
5.2.2 应用平面的安全  
随着SDN的发展，应用层提供应用提供各种网络服务，安全问题也随之而来。主要包括以下两种情况。  
（1）恶意应用：通过应用层植入蠕虫等病毒，达到窃取网络信息、更改网络配置、占用网络资源等目的，从而干扰控制平面正常工作的进程，影响网络的可靠性和可用性。  
（2）应用的安全规则冲突：为了提高各类网络服务，应用层需要制定网络安全规则，以访问控制器的安全接口。随着应用的复杂化，多个应用之间会出现安全规则冲突，从而给网络服务带来混乱，增加网络管理的复杂度。  
5.3 SDN对网络隐私的保护   
随着数据挖掘、地理位置服务（GPS）、定向广告的无孔不入，特别是每个数据包上的互联网地址标记，使得网络的个人隐私受到了极大的威胁。事实上，现在对网络用户隐私最大的威胁是各种过分热心的网络服务，而不是网络基础设施供应商。对于网络供应商而言，他们是非常乐意保护用户潜在的隐私安全问题的，如身份盗窃、网络入侵等。虽然之前已经有了一些尝试去争取供应商对用户的隐私保护服务，然而不足的是，之前的工作是基于数据流的，使用的是关键字轮转的加密方法来预防某些网络攻击。这样的方法会造成长时间的网关流量短供，从而无法跟踪一个固定时间段里每个流的状态。  
对此，SDN卸载了交换机的路由判定，提供了一个可以部署新协议和服务的框架。从SDN的观点出发，可以大大的简化这个问题。由其部署的服务可以完全被软件定义而不需要专门的网关，从而也不会造成网关流量供应短缺的问题。而许多早期的分布式解决方案所面临的为都会被一个集中的视图所解决。  
在Marc Mendonca的解决方案[16]中，实验了SDN如何在服务供应商的部署下保护终端隐私。介绍并引入了AnonyFlow匿名服务，为用户隐私提供了一种无缝的高效的通信服务。Marc实现、设计并评估了相关的标准化模型，使得终端用户匿名且不受吞吐量和延迟的影响。  
  
6 SDN未来展望  
SDN的提出，迅速成为了业界的关注焦点，相继出现一系列的相关标准和设备。SDN通过修改流表改变交换机的行为，给予网络运营商在网络中宽泛的控制范围选项，特别是在校园、企业和数据中心中。为此，VMware公司推出vCloud，提供了一套完整的云计算基础设施解决方案，可用于构建和管理满足IT最重要的云计算基础架构。借助VMware vCloud Director，客户可以将基础架构资源整合成虚拟数据中心资源池，并允许用户按需消费这些资源，从而构建安全的多租户混合云。2013年3月14日，VMware宣布收购软件定义网络技术到vCloud套件，同时，该公司还公布了新的混合云服务计划，该计划将为客户提供VMware公有云。  
今天的网络，通信需求如多宿主、移动性、安全性以及组播都是开放性的问题，许多研究小组正在从事于未来网络设计，以满足这些应用需求。因而，如前文所提到的，OpenFlow是一项有利于支持未来网络体系结构研究与实验的技术。  
6.1 未来技术难题  
尽管SDN在网络、服务部署等方面有明显的技术优势，尤其是对云计算和虚拟化等业务的支持，其未来的应用前景值得期待 [17]。但从目前SDN的发展水平来看，其实际应用还不多，一些技术挑战和应用问题有待于研究和解决。  
（1）SDN的控制平面网络构建。  
传统网络的控制平面是分布式结构，对经过网络设备的数据包执行转发操作，设备需要获取与其互联网设备或网关相关的信息，建立数据包转发规则，如BGP，OSPF等P2P协议。然而，因为SDN网络设备是由控制器统一执行控制面功能、集中控制到控制层的，网络设备与客户端之间采取类似客户端/服务器模式，网络设备基本依靠控制器下发的指令进行数据包操作，而无需了解整个网络和相邻网络设备。控制层是SDN的核心，其构建方式对基础设施层响应能力和网络性能有直接的影响。因此，需要研究和构建合理的控制层网络，才能正确发挥SDN技术在网络控制、服务部署等方面的技术优势。  
（2）SDN建设复杂度和运营维护成本。  
SDN将数据平面和控制平面分离，逻辑上的集中控制的理念被推广到网络中所有的网络设备，以简化网络设备和网络管理。但是，网络设备在得到简化的同时，软件化的网络控制层将出现高度的复杂化。这是因为数量庞大的网络设备要接受控制层的集中管理，基于软件的高复杂度控制层需要大量代码的编写和维护，给网络带来了不稳定性，得不到安全保障。简化了的网络设备在一定程度上能降低网络运营成本，网络的自动化程度提高也有助于网络运营商减少在网络设备维护方面的人力物力。  
但目前技术还不够成熟，控制层庞大的复杂度使得运营商不得不加大人力物力在控制层的研发和运营维护中，运营商的支出成本很有可能会上升。因此，在对SDN的研究中，控制层的构建复杂度和运营维护成本要进行更合理的综合考虑。  
(3)SDN的安全防护。  
在SDN架构下，安全防护的需求主要在控制层和应用层。SDN网络控制功能集中在控制器，在集中管理的模式下，一旦控制器收到网络攻击将直接影响整个网络的运行，所以，控制器的安全防护有着更高的要求。同时，应在应用层和控制层部署安全应用的防护措施，以应对新的安全需求。由于目前SDN应用还处于摸索阶段，对架构安全、应用安全等方面开展研究，是保障SDN应用的基础。  
(4)SDN在电信中的应用。  
现有的电信网IP网和传输网是相互分离、独自管理的，两者之间在管理方面没有重叠。SDN的引入，可以为现有的电信网络提供智能化网络和业务控制能力。将SDN引入电信网，将面临着一个问题，即在同一个管理平台下实现对报文交换网络和电路交换网的统一管理和两个网络之间的动态调度问题。由于报文交换网络和电路交换网络的结构不同，SDN在引入电信网只是，首先要解决这个问题。同时，SDN应用于电信网，需要具备电信级业务处理能力，如拓扑发现、网络故障检测、网络警告响应等，而目前SDN标准工作尚未考虑在电信网中的应用技术需求。  
6.2 未来展望  
传统的网络架构已经难以应对当前的网络信息传输需求，而SDN所体现的控制平面与转发平面分离的理念为未来网络发展提供了全新的思路，顺应了当前网络的应用趋势，具有很大的潜力和应用市场空间。SDN对现有的网络抽象简化，使得网络逐渐趋向“傻瓜型”，面向用户实现可编程。通过控制和转发分离，SDN能够降低网络控制的复杂度，提高了网络的安全性和可靠性，并加速了网络创新和发展进程。  
毫无疑问，SDN对网络格局的影响是革命性的，从应用角度上看，SDN很可能对整个通信产业产生巨大的冲击和影响。对于传统的通信设备制造商而言，SDN技术的出现改变了网络产业软硬件一体化的生产方式，转变为底层高性能转发/存储以及上层智能灵活调度的架构。所以，网络设备将变为低利润设备，而对现有占据市场主要份额的公司将造成巨大冲击。厂商为了适应这个趋势，一方面，以更低廉的价格优势占据市场，夺得市场份额；另一方面，积极储备与研发相关技术，适时推出相关技术产品，以满足市场需求。  
SDN并非适用所有的网络场景，也非解决网络问题的万全之策。SDN的首要应用场所一般在于IT定制化需求比较集中的地方，如数据中心和大型企业网络等。而另一个可能的应用场所是运营商的接入网络，用作多接入融合的统一控制。因此，SDN所带来的市场新的产业链将改变整个网络和应用之间的关系。  
对于网络运营商而言，现有的网络硬件的控制与转发架构将发生改变，运营维护模式也必须做出相应的调整策略。网络的核心将向网络操作系统转移，SDN的管理和控制也将成为运营商的一个新的探索研究方向。

<http://doc.mbalib.com/view/eb830e8bde2de0355832e51dd52e0edf.html>

