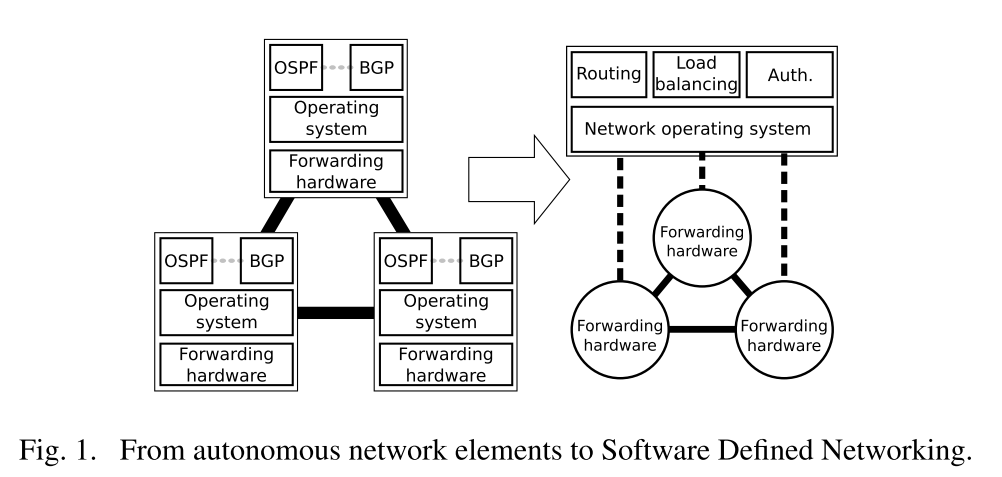
# Abstract

最近在行业中获得了巨大的动力，主要是由对数据中心应用程序感兴趣的 IT 公司推动的。然而，在本文中，我们将 SDN 应用于运营商领域，这对网络管理功能提出了额外的要求。作为一个特定用例，我们采用由多个客户共享的虚拟化运营商网络。我们考虑由开放网络基金会 (ONF) 定义的当前 SDN 模型，包括 OpenFlow 和 OF-config 协议。通过对配置和管理虚拟化网络所需程序的逐步讨论，我们分析了 ONF 指定的当前 SDN 模型的适用性。因此，我们确定了 ONF SDN 模型的缺点并提出了必要的扩展。突出显示的扩展包括控制网络引导注意事项、对 SDN 和 NOS 模型的更新，以及最重要的 OF-config 管理数据模型的扩展。

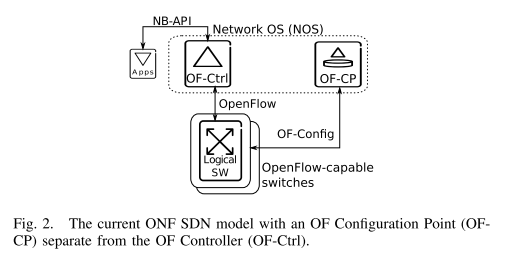
# INTRODUCTION

传统的网络元素被设计为自治实体（图 1，左），使用分布式控制平面与外部世界进行通信。各种协议允许自主决定采取什么行动。通常，这涉及在封闭操作系统 (OS) 内运行的多个进程调用专有 API，这又使 OS 再次使用专有 API 对专门的转发硬件进行编程。向网络元素添加新功能通常涉及对重新发明分发和信令等机制的新协议进行标准化，并等待供应商实施新协议。软件定义网络 (SDN) 通过在硬件之间创建开放 API 提出了一种新模型和操作系统，以及操作系统和网络应用程序之间。在 SDN 模型（图 1，右）中，网络操作系统 (NOS) 负责维护网络及其当前状态的最新视图 1。 NOS 不仅维护网络视图，还负责处理视图更改并将这些更改传输到网络硬件和网络应用程序。对视图的更改要么来自运行在操作系统之上的网络应用程序，要么来自底层网络硬件，例如在失败的情况下。网络应用程序是能够访问和修改由 NOS 维护的网络视图的软件模块，这大大简化了新功能的添加。只需利用 NOS 提供的 API 编写一个软件模块，由 NOS 负责更新网络和分发新状态。 SDN 的研究和开发目前以官方标准化机构 Open Networking Foundation2 为中心，该机构成立于 2011 年。 ONF 迄今为止主要关注 OpenFlow [1] 的规范，OpenFlow 是一种开放协议，旨在暴露网络的内部结构。网络元素并提供一个 API 来修改它们。该协议基本上将网络元素建模为流表。流表包含可用于匹配传入数据包并将它们与许多操作相关联的规则。如果传入的数据包与网络元素中的现有规则不匹配，则可以将数据包发送到 NOS，在那里网络应用程序可以进一步调查数据包并决定要做什么，例如，安装处理所有数据包的新规则在这个特定的数据包流中。 OpenFlow 协议主要用于通过以相对较高的频率安装永久或临时规则来管理流表。



## A. SDN 中网络管理的现状

SDN 框架能够集中控制数据路径元素，独立于用于连接来自不同供应商的这些设备的网络技术。集中控制嵌入了所有智能并维护数据路径元素和连接它们的链接的网络范围视图。这种集中的最新视图使 NOS 也适合执行网络管理 (NM) 功能。认识到 SDN 中需要明确的 NM 功能，ONF 最近提议 OF-config 作为除 OpenFlow 之外的附加配置和管理协议。 OF-config 基于 NETCONF [2]，这是一种事务性协议，它在安全传输通道（例如 SSL 和 SSH）之上使用远程过程调用 (RPC) 来管理远程设备上的配置。它提供了不仅在单个设备上而且在单个事务中的多个设备上安装、操作和删除配置的方法。虽然 NETCONF 本身是基于 XML 的，但数据模型 - 描述可以配置的内容以及不同的配置类如何相互关联 - 是用 YANG [3] 编写的。 OF-Config 采用 NETCONF 协议，扩展了特定的 YANG 模型。图 2 显示了 ONF [4] 定义的当前 SDN 架构。在此模型中，支持 OpenFlow 的交换机（物理或虚拟网络元素）托管一个或多个 OpenFlow 逻辑交换机。逻辑交换机代表实际的 OpenFlow 网络元素，它们由一个或多个 OF 控制器通过 OpenFlow 协议控制。 OF 控制器顶部的网络应用程序通过 OF 控制器的北向 API (NB API) 使用网络。最后，OF 配置点代表通过 OF-Config 协议与支持 OpenFlow 的交换机通信并在 OF 逻辑交换机（例如端口和队列）之间划分资源的服务。 OF控制器和OF配置点之间的关系目前没有由ONF特意定义，但是，在一般SDN术语中，这两个功能元素都可以被认为是NOS的一部分。

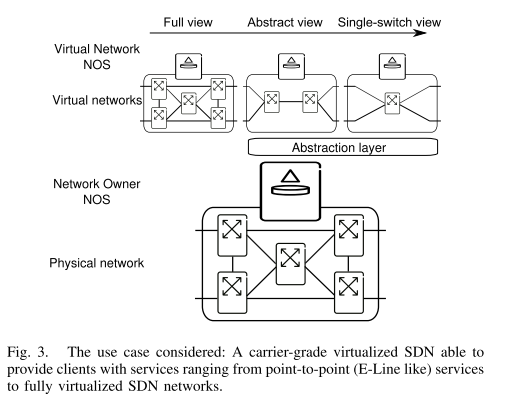


## B. 我们的贡献

SDN 在行业论坛上获得了动力，主要由专注于数据中心应用的领先 IT 公司推动。然而，本文的重点是现代运营商网络中的 SDN，正如在 EU FP7 SPARC 项目 3 的框架内所研究的那样。为了被视为电信级网络，SDN 解决方案需要提供网络和服务管理能力[5]、[6]。在本文中，我们通过将 ONF 模型应用于虚拟化运营商网络的用例来分析 ONF 模型。我们把重点放在网络配置上，但也考虑了故障和性能管理功能4。作为该分析的结果，我们推导出了 ONF 模型的更新视图，并提出了对 ONF 协议的扩展。我们在第 II 节中描述了虚拟化运营商级 SDN 的用例。然后，我们将在第 III 节中讨论用于配置和监控此类网络场景的程序。为了满足这些所需的功能领域，我们在第 IV 节中建议在 NOS 和协议扩展方面对 SDN 模型进行更新。最后，我们总结并总结了第五节的分析。

# Use-case

在本文中，我们考虑了运营商级网络的虚拟化，以便在多个虚拟网络运营商 (VNO) 之间共享物理基础设施（见图 3）。除了为管理如此复杂的网络节省预期的 OPEX 和 CAPEX 之外，使用 SDN 来控制整个基础设施还可以通过为客户提供不同的抽象级别来超越 ELine 或 E-LAN​​ 等传统服务。例如，一些客户可能需要托管连接服务（例如 E-Lines），将底层网络视为黑匣子。其他人可能需要更细粒度地暴露网络细节以获得对网络的完全控制，例如用于高级流量工程 (TE) 目的。我们希望 SDN 设计能够提供完整的网络虚拟化，客户可以通过该设计将自己的 NOS 连接到逻辑交换机。此外，我们提出了一个抽象层，它提供了运行在物理基础设施之上的虚拟网络的抽象视图。抽象视图的一个例子可以是由多个虚拟交换机和端口组成的抽象交换机。在客户和交换机之间拥有这样一个层的优点是它提供了任何级别的客户控制，从完整的数据平面暴露到单交换机接口。在这个用例中，虚拟化直接在物理网络之上完成 [7]-[10]。具体来说，我们考虑了 [9] 中描述的数据路径虚拟化，因为它通过让每个 VNO 访问完整的流空间来提供最高级别的灵活性。这种虚拟化方法应用了基于封装的链路分离，结合流表分区和严格的资源隔离。虚拟连接由隧道提供，可以使用适用于 SDN/Openflow [11] 的 OAM 工具（例如，BFD 或性能监控工具）进行监控。在网络详细信息向客户（即 VNO）公开的情况下，网络通过 VNO 自己的 NOS 进行控制。这种场景的优势包括通过客户控制的 TE 和将控制权委托给使用网络的应用程序（例如，over-the-top、网络感知应用程序）来更有效地利用网络。此外，所提出的方法还减少了物理网络所有者的管理任务量。这种方法的优势已经在数据中心/云环境 [12] 中得到体现，但我们认为这个概念可以推广到任何类型的网络，包括运营商级接入/聚合和固定移动融合 (FMC)。虚拟网络所需的拓扑、抽象级别、交换机功能、网络带宽和交换机资源在 VNO 和网络所有者之间的协议中指定。 SLA 也是本协议的一部分。



# CONFIGURATION PROCEDURES

在本节中，我们将根据用例讨论在一个物理基础设施之上配置虚拟 SDN 的分步过程列表。对于许多步骤，可能存在多种替代解决方案 - 在这些情况下，我们尝试详细说明允许最高级别自动化的解决方案。请注意，ONF SDN 模型目前并不支持列出的所有步骤。缺失的函数将在后面的第四节中列出。过程列表从引导设备和物理网络的配置开始。为了满足 SLA，我们在物理网络上配置了性能和故障监控。当虚拟网络拓扑被计算、配置、验证并移交给客户时，该过程就完成了。

1) 设备配置和网络引导：

a) 新连接的交换机请求连接标识符以连接到 OF 配置点 5。所需的连接标识符至少是本地地址和 OF 配置点的地址。如果使用非默认值，这也可能包括传输协议和端口号。例如，在基于 IP 的控制网络地址（自动）配置中，可以通过 DHCP [13]（见图 4）来完成。此外，如果需要来自身份验证服务的证书，则还需要提供此服务的连接标识符。

b) 可以在设备上预先配置与 OF 配置点和 OF 控制器的安全连接的凭据。对于更动态的引导过程，可以从身份验证和授权服务 (AA) 请求凭据。在这种情况下，使用身份验证机制（例如，通过向数据库添加唯一的交换机标识符）与 AA 服务建立初始信任。建立信任后，所需的证书（例如 SSH 密钥和 X.509 证书）将传输到交换机。

c) 交换机发起与 OF 配置点的 OF-Config 会话。他们使用获得的证书来相互验证自己。

2）物理网络配置：

a) OF 配置点使用新建立的 OF-config 会话发现物理资源和能力。物理资源的示例包括交换机 CPU、内存和端口。具有 OF 能力的交换机的能力是硬件和软件能力，例如支持的 OAM 工具列表、OpenFlow 操作和 QoS 功能。

b) 为了将交换机连接到 OF 控制器，OF 配置点首先需要实例化一个可以访问所有物理端口的逻辑交换机，我们将其称为主逻辑交换机 6。为主逻辑交换机分配了最少量的资源（例如 CPU、带宽）和高优先级，以确保在高负载期间也能进行控制。 OF 配置点然后将 OpenFlow 会话的连接标识符和凭证分配给主 OF 控制器，即基础设施所有者的控制器。结果是已建立的 OpenFlow 会话可以访问所有物理端口。

c) 物理拓扑的发现可以基于控制器 (i) 或分布式方式 (ii) 完成。 (i) 当考虑纯 OpenFlow 交换机时，需要 OF 控制器参与物理拓扑发现。连接到主逻辑交换机的主 OF 控制器使用基于控制器的方法启动物理拓扑发现，例如NOX 发现模块中使用的集中式 LLDP 机制。发现的物理拓扑与主OF配置点共享。(ii)物理拓扑的发现也可以分布式方式完成，其中交换机自主使用诸如LLDP或生成树协议的方法。然后可以通过 OF-config 点检索本地邻接，以创建拓扑的全局视图。这种方法假设支持交换机（即混合交换机）中的传统协议。

3）物理故障和性能监控：发现物理拓扑后，验证物理链路和资源是否正确实例化并持续监控其性能很重要。为此，需要用于故障检测和性能监控的 OAM 工具。

a) 在支持 OF 的交换机上配置用于物理链路故障检测和性能监控的 OAM。此外，还配置了对其他交换机资源（例如 CPU 和内存）的监控。对于每个 OAM 工具，可以配置以下参数：用于调度测量和报告的参数、阈值和交换机本地操作。测量和报告的调度包括测量类型（主动、被动）、监控周期（即执行测量的频率）和报告方法（定期、按需、更改或何时违反阈值） .阈值是根据性能指标配置的，例如带宽性能下降或特定链路状态变化。交换机本地操作在阈值违规时触发，可以是纠正操作，例如故障转移、流表操作或通过 OpenFlow 会话发送到 NOS 的警报。

b) 当 NOS 收到警报或测量数据时，它可以通过多种方式做出反应，例如通过网络恢复、物理资源重新分配或逻辑交换机到另一个物理交换机的潜在迁移。有关 NOS 的警报和测量处理的详细信息超出了本文的范围。

4) 虚拟网络设置：

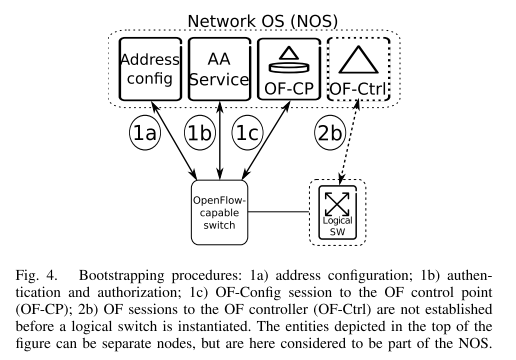
a) 使用发现的物理拓扑和交换能力，结合预先建立的虚拟网络拓扑和 SLA 客户协议，可以计算虚拟拓扑。基于这些虚拟拓扑结构，主控配置点可以创建虚拟链路。虚拟链路是需要使用 OpenFlow 配置隧道端点（即逻辑端口）和相应流表配置的隧道。带宽隔离是通过对虚拟链路应用 QoS 来实现的。

b) 创建虚拟链路后，主OF 配置点准备为虚拟网络实例化逻辑交换机。它通过对物理资源进行分区并将功能分配给每个逻辑交换机来实现。这定义了通过 OpenFlow 协议呈现给 VNO 的资源和能力的视图。此外，此处还指定了通过 OF-config 协议呈现给 VNO 的资源和能力视图，例如定义可以使用哪些隧道协议。

c) 在将新创建的虚拟网络移交给客户之前，应验证拓扑和功能。为了获得客户视图，一个特殊的测试-NOS 连接到虚拟SDN。在 test-NOS 的帮助下，网络所有者执行能力发现和基于控制器的拓扑发现。获得的发现结果可以与虚拟网络参数进行比较，以验证它们是否满足客户的要求。 SLA 的初始验证是通过 OAM 性能测量工具执行的。

d) 可选地，可以配置抽象层，例如定义公开的抽象级别（参见图 3）。抽象系统在交换机的外部，作为单独的实体运行，作为网络所有者 NOS 的一部分（如果它作为服务提供）或在服务提供商 NOS 中运行。如何配置抽象系统超出了本文的范围。

5) 虚拟网络运营：一旦虚拟网络被网络所有者创建和验证，虚拟网络就移交给客户。 如图 3 所示，为客户提供了完整视图或抽象视图。虚拟网络可以具有由网络所有者配置的预先分配的客户定义地址和凭据。 或者，客户可以选择以类似于步骤 1a 中针对物理网络所述的方式引导其网络。 从客户的角度来看，连接的虚拟网络就像任何物理 SDN 网络，使虚拟服务提供商能够使用自己的 NOS 执行控制和管理操作。 典型的服务提供商操作包括转发配置、隧道创建、OAM 和 QoS 配置等。



# DERIVED EXTENSIONS

为了执行上面列出的过程，需要对 ONF 模型和协议进行一些扩展。 这些包括引导注意事项、修改后的 SDN 架构以及对 ONF 协议的扩展。

A. 控制网络引导

当前的 ONF OpenFlow 规范没有描述初始地址分配和控制信道设置是如何执行的。 在本文中，我们没有提出特定的方法，而是指出自动引导需要用于控制网络设置、地址分配、身份验证和凭据传输的机制。 这些机制需要 OpenFlow 交换机和 NOS 支持。 计划在未来的工作中详细讨论引导程序。

B. SDN 架构和 NOS 模型

当前 ONF 控制器模型定义了 OF 配置点 (OF-CP) 和 OF 控制器 (OF-Ctrl) 作为单独的实体。 从程序中我们可以看出，这些实体之间需要共享数据。 在步骤 2a 中第 III 部分描述的程序列表中，OF-CP 获得物理能力。 但是，OF-Ctrl 负责通过拓扑发现（步骤 2c）和 OAM 数据（步骤 3b）获取和更新物理拓扑。 该数据的组合可能是易失性的，并且是虚拟网络的实例化和维护所必需的。 我们认为，为了快速对这些数据做出反应，需要一个紧密耦合 OF-CP 和 OF-Ctrl 的系统。 我们在图 5 中用 NOS 中的共享数据存储来表示这一点。

此外，我们看到需要能够将具有不同视图和功能的多个 OF-CP 连接到支持 OF 的交换机。 在 ONF 模型中，网络所有者拥有完整的管理能力，能够实例化逻辑交换机、配置物理链路级 OAM 等。但是，客户可能还需要一个 OF-config 接口来配置自己的隧道端点、OAM 工具、 因此，我们建议通过OF-config接口为客户提供交换机的缩小视图和减少的配置权限。 例如，通过这种简化的 OF-config 界面，客户只会看到一个逻辑交换机，它似乎直接连接到物理端口。

C. 协议要求

根据配置程序，我们确定了当前 ONF 协议中缺少的一些功能。这些主要是自然适合 OF-Config 协议的配置相关功能。此外，我们建议处理快速变化信息的函数更适合 OpenFlow 协议。在 OF-Config 中，我们看到四个需要扩展的领域： (i) 物理资源发现目前只能使用 OF-config 模型 [4] 中的 OpenFlow Resource 结构，该结构由有关物理端口、队列、流表和证书。这里缺少的信息包括支持的 OAM 工具、CPU 和内存资源以及这些资源的上限。对于 OAM 工具，我们需要发现支持的 OAM 工具类型以及可以激活的最大 OAM 工具实例数。此外，如果我们要在交换机上运行多个 OpenFlow 协议实例（具有不同的优先级），我们希望为它们分配硬件资源。许多物理资源的上限值缺失。虽然可以配置 OpenFlow 资源，但没有关于所报告资源的最大数量的信息。但是，此信息对于实例化逻辑交换机和计算虚拟网络拓扑至关重要。我们建议更新现有的 OpenFlow 资源结构并在模型中添加两​​个新结构（见图 6）： OpenFlow Resource：现有的 OpenFlow 资源结构（[4] 中的第 7.6 节）扩展了组表和仪表。物理交换机资源：内存和CPU资源；可用的 OAM 工具列表；支持的隧道类型列表。 Physical Switch Capabilities：支持 OF 的交换机上的最大逻辑交换机数量；每个逻辑交换机的物理资源上限。

(ii) OF-Config 支持逻辑链路配置

然而，通过 OpenFlow Tunnel 结构，仅适用于少数基于 IP 的隧道协议和有限的 QoS 能力。一个逻辑链路被表示为一个逻辑端口，它实际上是一个隧道端点。逻辑端口可以设置为特定的比特率，但缺少其他 QoS 配置，例如优先级或物理端口队列。 OpenFlow Tunnel：现有的 OpenFlow Tunnel 结构（[4] 中的第 7.7 节），扩展了额外的隧道类型； QoS 配置参数（优先级、队列）。

(iii) 目前正在考虑逻辑开关实例化

超出 OF-Config 的范围，但是，使用 OpenFlow 逻辑交换机功能中的现有（当前只读）参数，逻辑交换机实例化应该是可能的。除了现有参数之外，我们还建议添加更多硬件资源（参见 (i)）、支持的 OAM 工具的掩码以及支持的隧道协议。此外，需要为多个逻辑交换机之间共享的逻辑交换机资源指定上限。 OpenFlow Logical Switch：OpenFlow Resource结构（[4]中的7.6节），扩展了CPU和内存预留； OAM工具列表；隧道类型列表；米，组表。逻辑交换能力：逻辑交换能力结构（[4] 中的第 7.4 节），扩展了流和组表条目、队列、隧道、OAM 工具和仪表的数量上限。(iv) 设备和链路 OAM 配置是目前不支持。我们考虑的 OAM 功能是监控各种参数，例如设备上的 CPU 负载和内存使用情况、路径连通性验证、丢失率、延迟和链路上的带宽测量。对于 OAM 工具，有许多特定于工具的配置参数，例如 BFD 会话的时间间隔和标识符、延迟测量情况下的单向或双向测量等。 然而，OAM 工具也共享许多参数，例如，如何执行测量的频率（按需或定期），报告测量的频率（按需或定期），以及指定条件的阈值，当达到时应触发发送警报或由交换机执行自主操作。 OAM：OAM参数：OAM实例标识、OAM工具类型、测量类型；被管实体：资源类型、资源标识；测量和报告的安排：监测期；报告方式；阈值：阈值类型；阈值；行动清单；切换本地动作：动作类型；特定于动作的参数；可选参数：OAM 工具特定参数。

除了 OF-Config，我们的程序还需要对 OpenFlow 协议进行扩展。 虽然 OAM 工具是由 OF-Config 配置的，但由于 OpenFlow 协议的实时性，其结果和警报的报告更适合于 OpenFlow 协议。 OpenFlow 目前缺乏专用的监控消息，因此我们建议为异步警报消息和周期性测量结果添加新的消息类型。 这些消息结构的确切规范将高度依赖于特定的警报和 OAM 工具。

# SUMMARY AND CONCLUSIONS

ONF 目前指定了 SDN 环境的两种协议，这两种协议都将网络元素与网络操作系统 (NOS) 接口，后者代表集中控制和管理平面。这些协议是 OpenFlow，用于在流和数据包时间尺度中对流表进行编程；以及最近的 OF-config，主要任务是在人类时间尺度上对网络元素进行网络范围的配置。在本文中，我们将基于这两个规范的 ONF SDN 模型应用于由多个客户 (VNO) 虚拟化和共享的运营商网络的用例。我们概述了配置和管理此类虚拟化 SDN 所需的步骤，从设备和网络引导到虚拟网络的设置，再到最终移交给 VNO。对该过程的每一步分析使我们能够识别缺点并在网络管理功能方面对 ONF SDN 模型提出必要的扩展。突出显示的扩展包括控制网络引导注意事项、对 SDN 和 NOS 模型的更新，以及最重要的对 OF-config 管理数据模型的扩展。我们认为，这种特定于用例的分析对于验证 ONF SDN 模型及其协议在网络管理功能方面的适用性和有用性很重要。