

Beijing Forest Studio
北京理工大学信息系统及安全对抗实验中心



软件定义网络拓扑发现技术

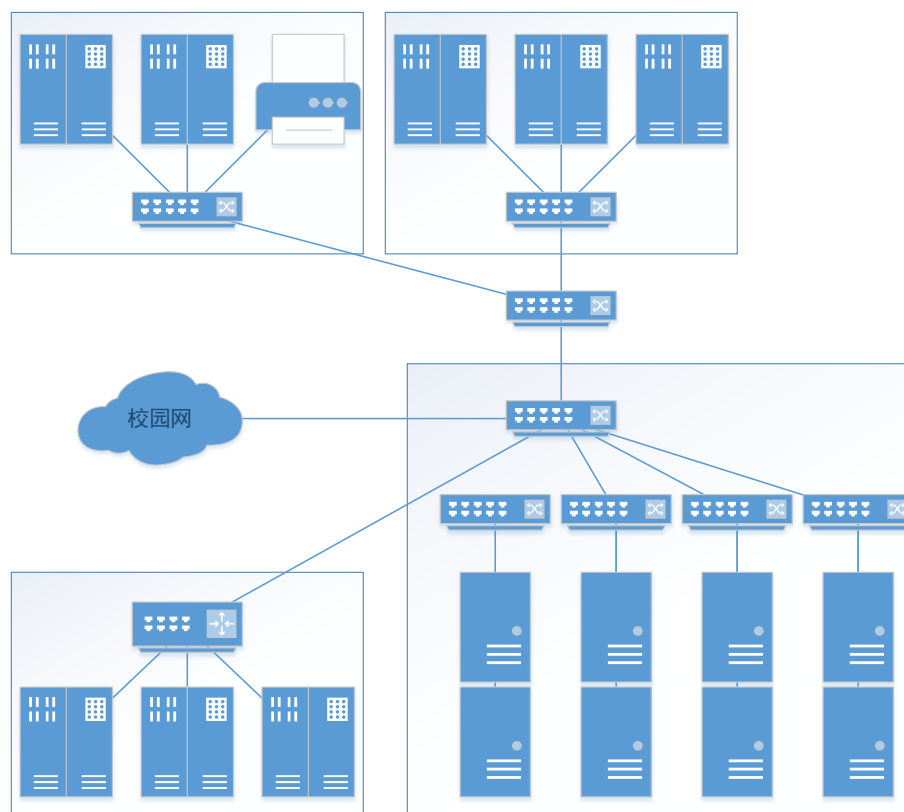
硕士研究生 门元昊

2020年7月26日

- 背景介绍
 - 网络拓扑发现
 - 软件定义网络（SDN）
- 基本概念
- 算法原理
- 优劣分析
- 应用总结
- 参考文献

- 了解网络拓扑发现和软件定义网络的概念
- 理解SDN中网络拓扑发现的原理

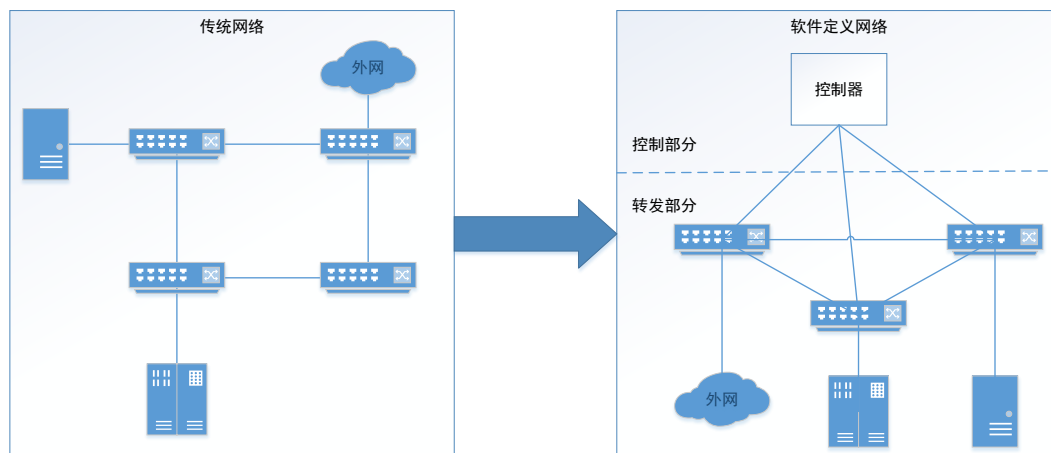
- 网络拓扑发现
 - 基本概念
 - 识别网络元素（主机、交换机等）之间的物理或逻辑连接关系，确定网络的拓扑结构



- **网络拓扑发现**
 - **评价指标**
 - **发现延时**: 发现网络拓扑结构时算法需要运行的时间
 - **网络负载**: 运行时占用网络和主机资源的多少
 - **完整性**: 发现的元素及连接关系占实际情况的百分比
 - **准确性**: 发现的元素及连接关系的准确率

- 网络拓扑发现
 - 拓扑发现方法
 - 基于SNMP协议的拓扑发现
 - 基于通用协议的拓扑发现
 - ARP
 - ICMP
 - ...
 - 基于路由协议的拓扑发现
 - RIP
 - OSFP
 - ...

- 软件定义网络
 - 基本概念
 - 能够通过软件编程的形式定义和控制网络的一种网络架构
 - 核心思想：通过**分层**，将**控制与转发进行分离**
 - 控制部分：使用可编程的控制器，便于管理和配置网络
 - 转发部分：OF交换机，仅提供简单的数据转发功能
 - 交互：通过统一接口（OpenFlow协议等）进行通信，由控制器向交换机下发转发规则



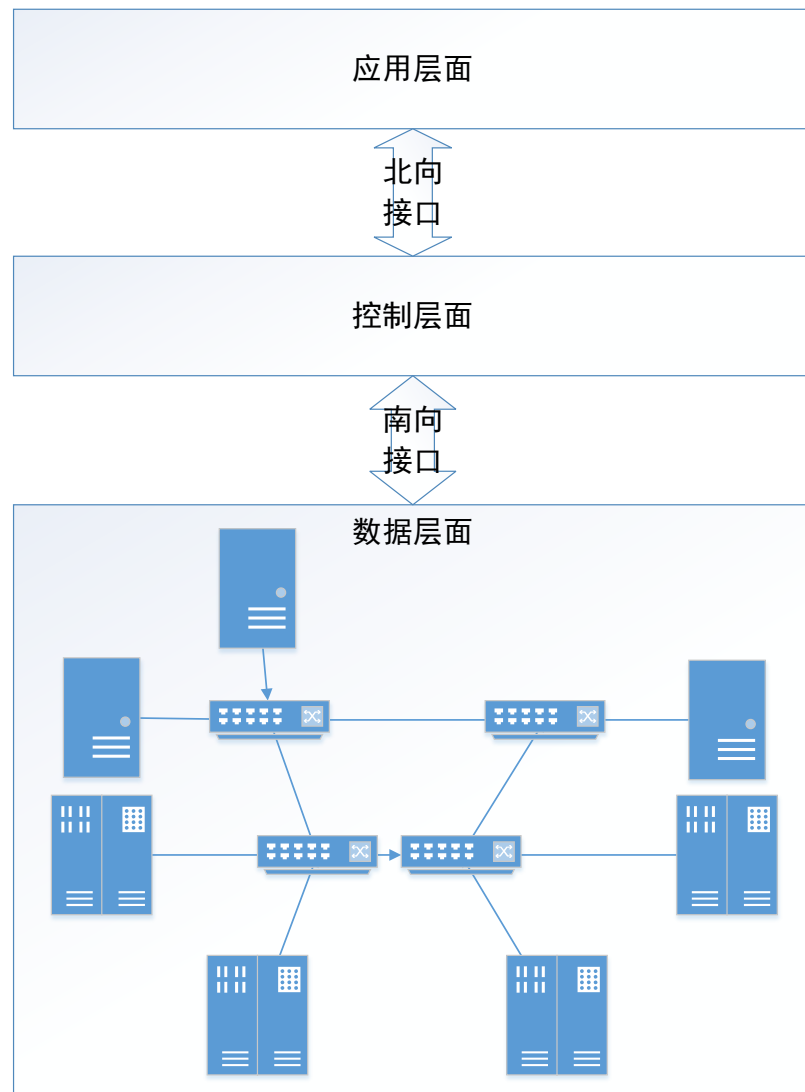
- 软件定义网络

- 体系结构

- 数据层面：交换机、服务器、PC等硬件设备
 - 控制层面：SDN控制器
 - 应用层面：基于SDN的各类网络应用

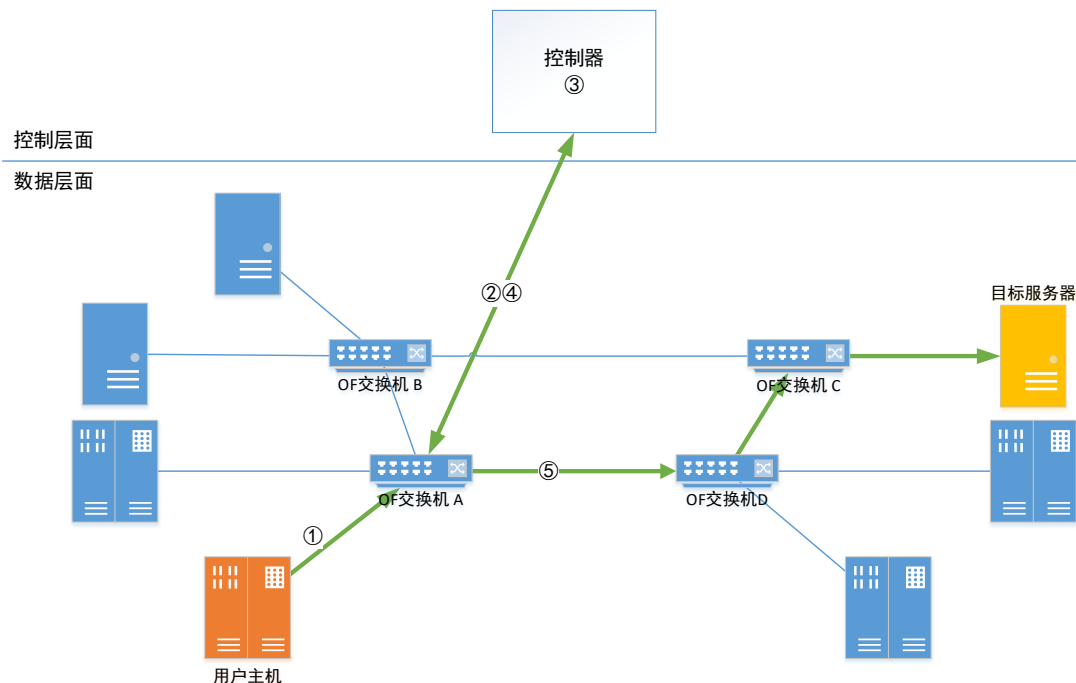
- 接口

- 南向接口：控制层与数据层的通信，具有统一的标准，最主流的就是OpenFlow协议
 - 北向接口：应用层与控制层的通信，并无统一标准



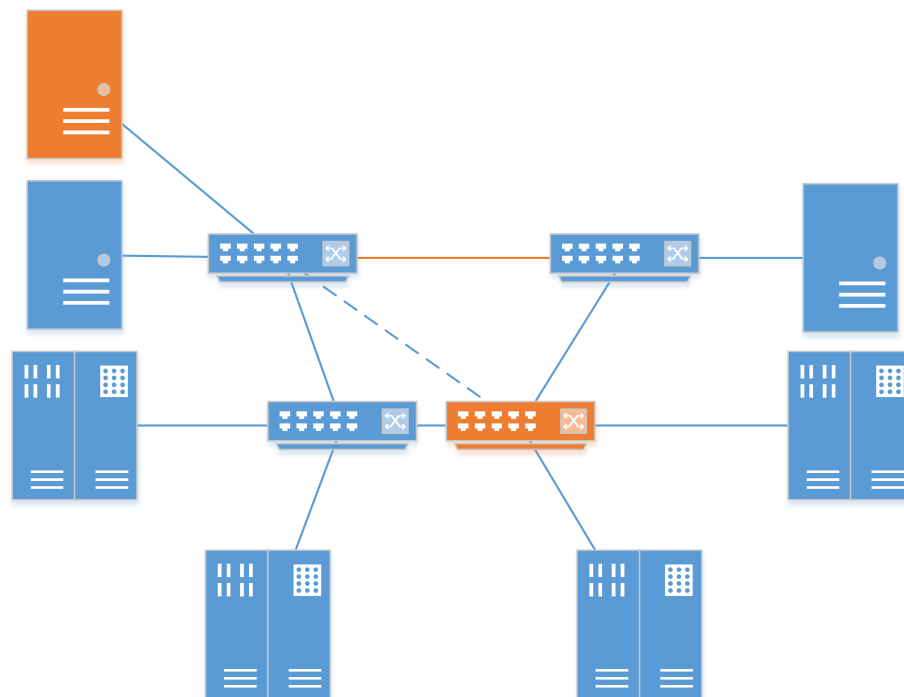
- 软件定义网络
 - 通信流程

- ①流量到达OF交换机A
- ②交换机向控制器发送Packet_In数据包，请求转发规则
- ③控制器根据用户的定义，生成转发规则
- ④控制器发送Packet_Out数据包，返回转发规则
- ⑤OF交换机将流量转发至下一目标
- ⑥后续的OF交换机都会重复上述步骤，直至流量到达目标服务器

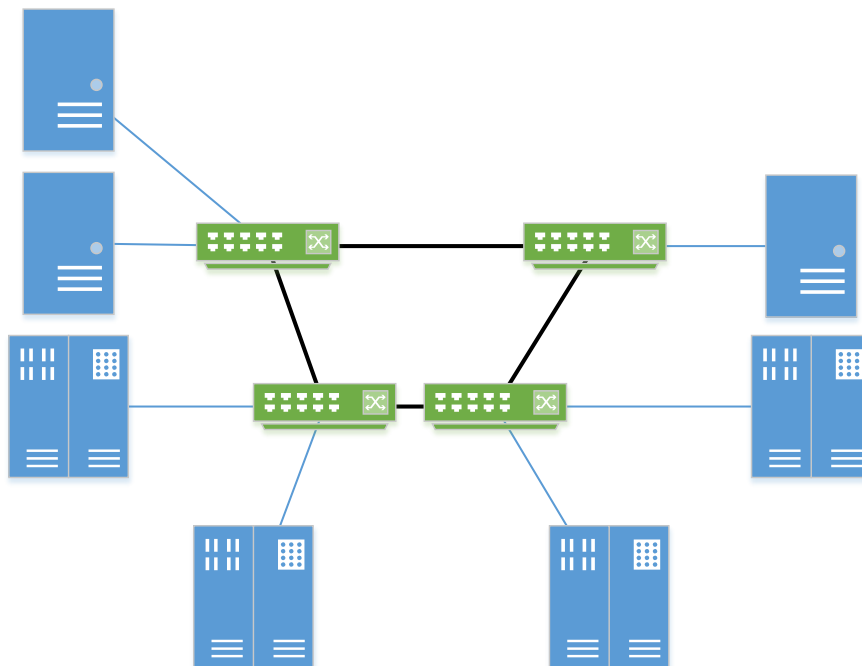


- 软件定义网络
 - 对拓扑发现的影响
 - 完整性、准确性：由于SDN的控制器要求对整个网络拓扑的全面准确掌控，因此在SDN架构下，对网络拓扑发现的完整性和准确性有极高的要求。

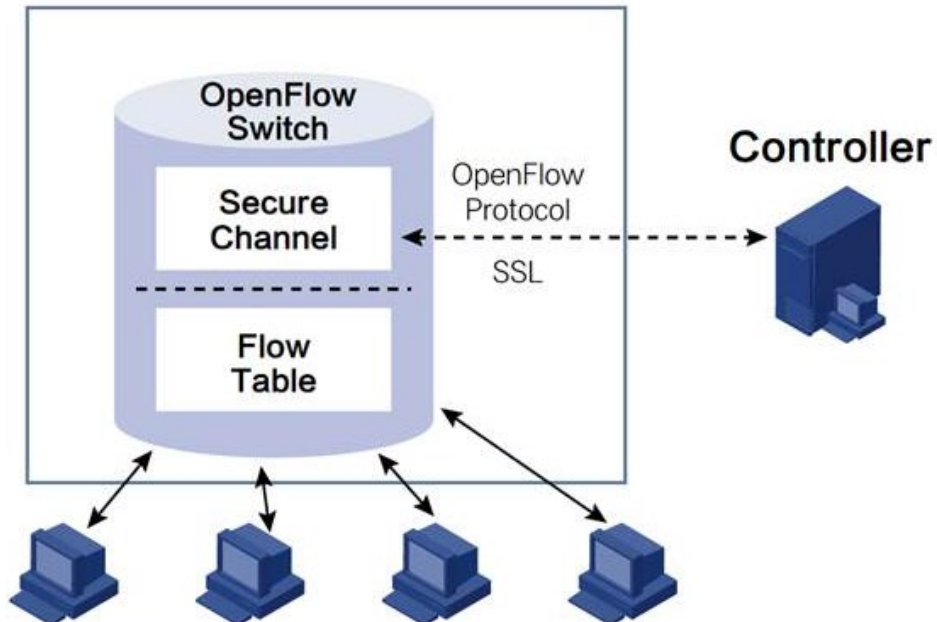
- 主机发现错误
- 交换机发现错误
- 链路发现错误



- 拓扑发现实体
 - 主机：连接到交换机的物理或虚拟系统
 - 交换机：OF交换机，只具有简单的转发功能
 - 互联链路：交换机之间的物理或虚拟链接



- Openflow协议
 - Openflow组件
 - 控制器：根据管理员的设置，生成流量的转发规则
 - OF交换机：依据控制器的转发规则，转发流量
 - 安全通道：交换机与控制器的通信通道
 - 流表：存放转发规则



- Openflow协议

- 流表

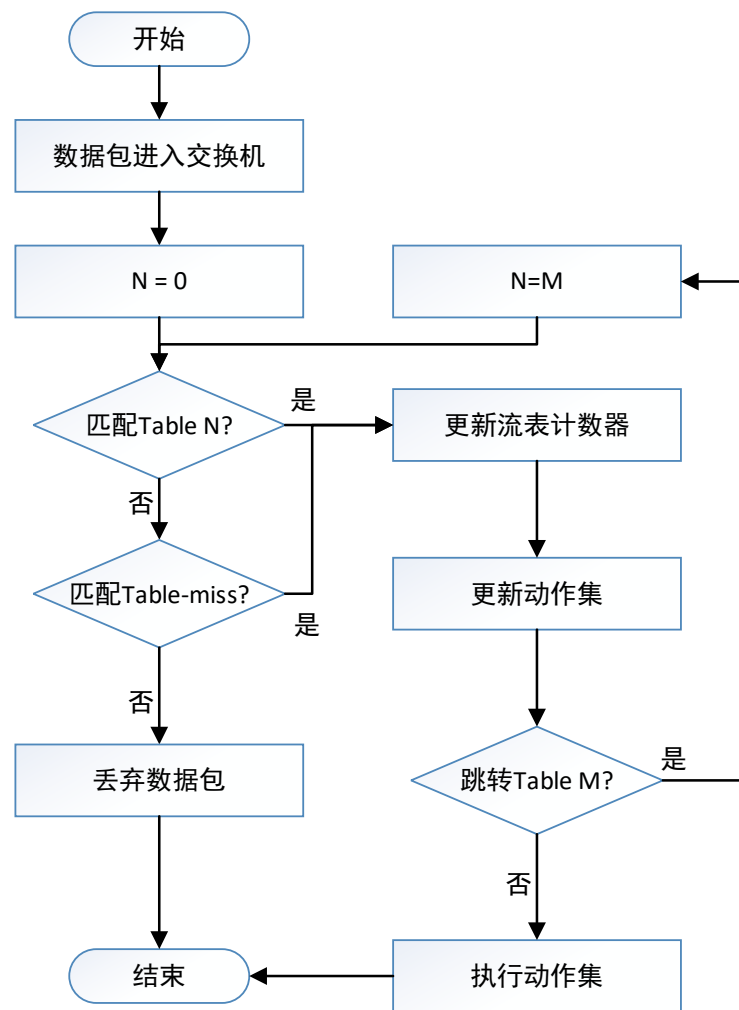
- Match Fields: 流表项匹配规则
 - Priority: 优先级, 流表的匹配顺序
 - Counter: 计数器, 统计报文数和字节数
 - Instructions: 流表项动作指令集, 定义匹配到该流表项的报文需要进行的处理
 - Timeouts: 流表项的超时时间
 - Cookie: 控制器下发的流表项的标识



- Openflow协议

- 流表工作流程

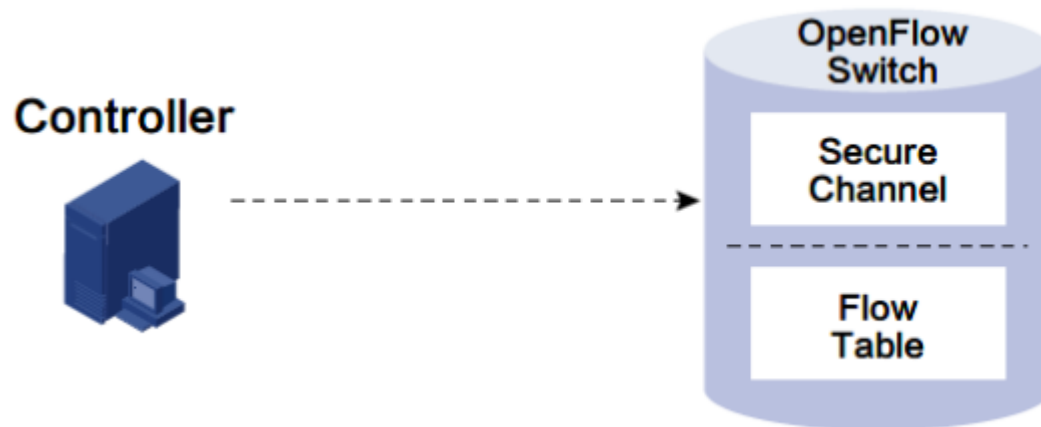
- 按顺序由小到大匹配流表
 - 若匹配到流表，先更新计数器
 - 根据匹配到的流表更新数据包对应的动作集
 - 若有流表跳转，则跳转到对应流表执行上述操作，否则直接执行动作集
 - 若无流表匹配，且存在Table-miss项，则该行该项
 - 若未匹配到任何一项，则丢弃该数据包



- Openflow协议

- 消息类型

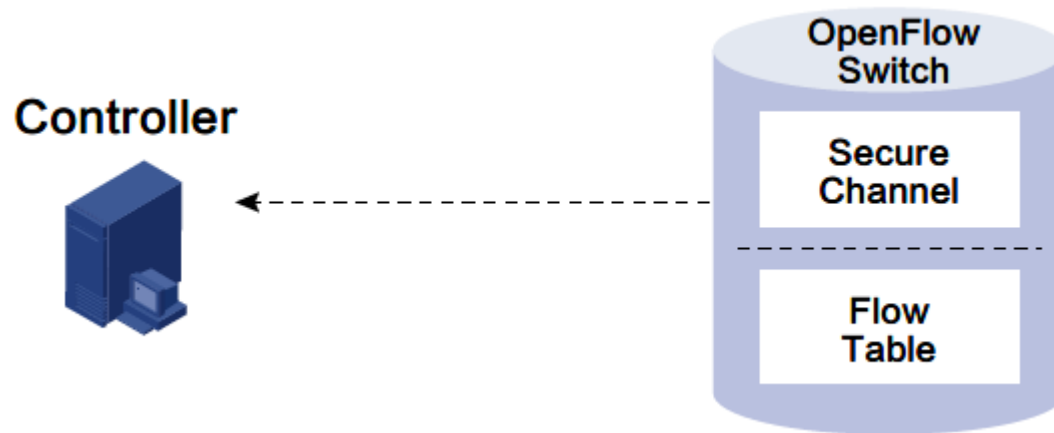
- OpenFlow协议支持三种消息类型，分别为：
controller to switch, asynchronous(异步)和
symmetric(同步/对称)，每一类消息又有多个子消息类型
 - controller to switch消息：由控制器发起的，主要用于
控制器对交换机进行状态查询和修改配置等管理操作



- Openflow协议

- 消息类型

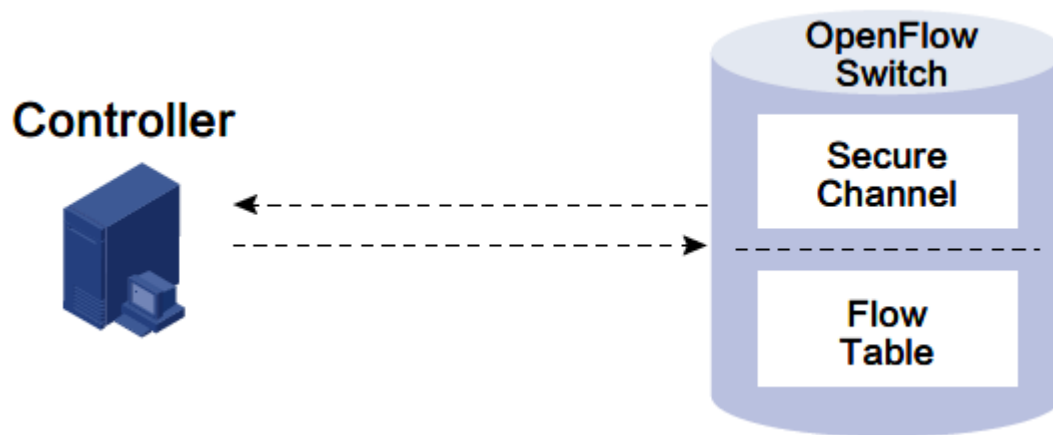
- asynchronous消息：由交换机发送给控制器，用来通知交换机上发生的某些异步事件的消息



- Openflow协议

- 消息类型

- symmetric消息：双向对称的消息，主要用来建立连接、检测对方是否在线等，是控制器和OpenFlow交换机都可以在无请求情况下发送的消息



- Openflow协议
 - 消息类型举例
 - **Features:** 用于请求交换机身份和能力信息
 - **Packet-Out:** 用于控制交换机在指定端口转发数据包
 - **Packet-In:** 交换机收到一个网络数据包，在流表中没有匹配项，则发送Packet-In消息给控制器
 - **Flow-Removed:** 流表因为超时或者修改等原因被删除掉，会发送flow-removed消息给控制器
 - **Hello:** 用于交换机和控制器建立连接
 - **Echo:** 测量延迟、带宽等
 - ...

- Openflow协议

- 流表下发（控制器与交换机的通信）

- 交换机请求

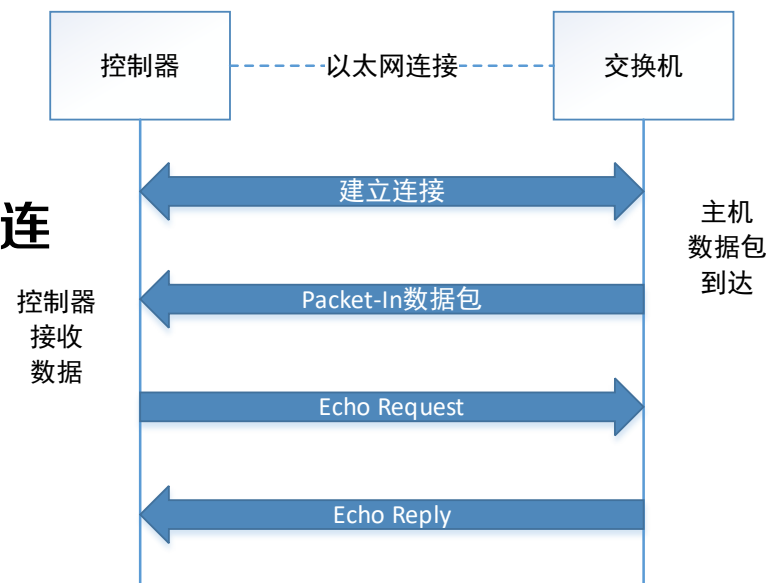
- 双方建立通信连接（初始化、Hello消息）

- 主机数据包到达交换机

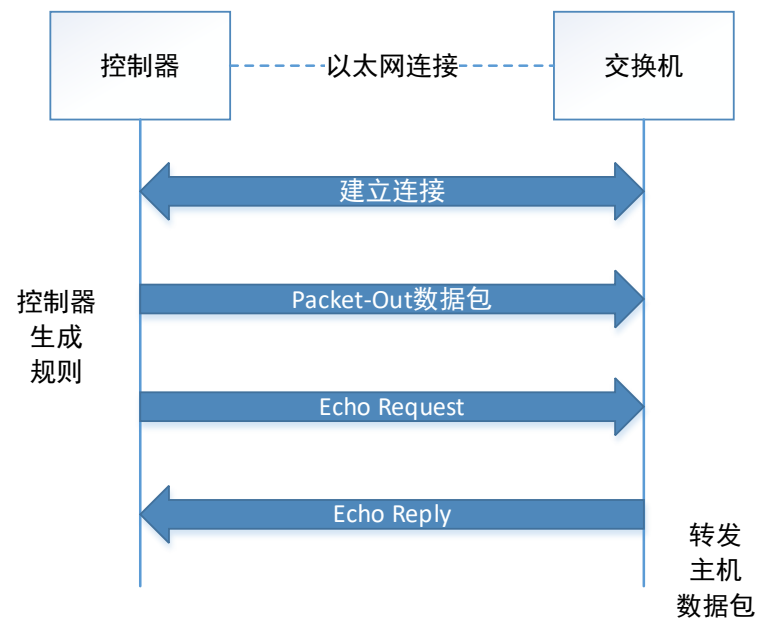
- 交换机发送Packet_In消息

- 控制接受消息并处理

- 双方使用Echo消息再次确认连接



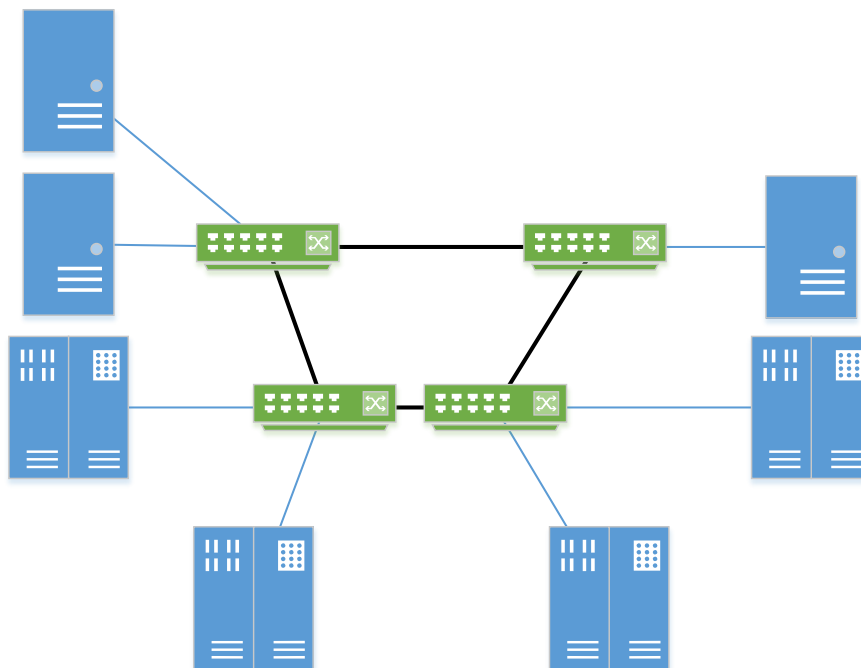
- Openflow协议
 - 流表下发（控制器与交换机的通信）
 - 控制器响应
 - 双方建立通信连接（初始化、Hello消息）
 - 控制器生成规则
 - 控制器发送Packet_Out消息
 - 双方使用Echo消息再次确认连接
 - 交换机转发主机数据包



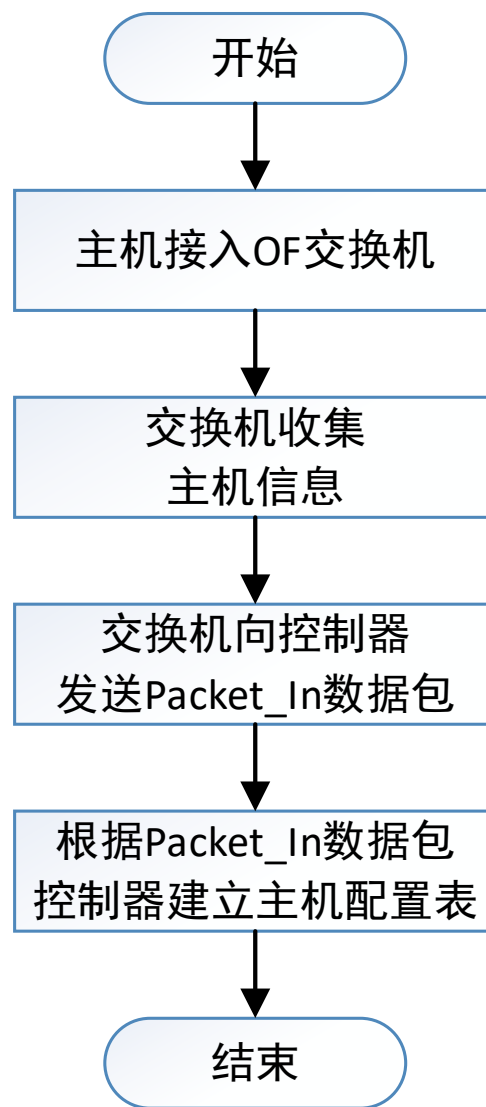
T	获得给定SDN的拓扑结构
I	SDN网络
P	1.主机实体发现 2.OF交换机发现 3.交换机链路发现
O	SDN网络拓扑结构

P	全面准确的获取SDN的网络拓扑结构
C	SDN网络，且不存在传统交换机
D	提高拓扑发现效率、降低拓扑发现开销
L	ICSPCS 2014 （ OFDPv2 ）

- SDN网络拓扑发现
 - 主机发现
 - OF交换机发现
 - 交换机互联链路发现

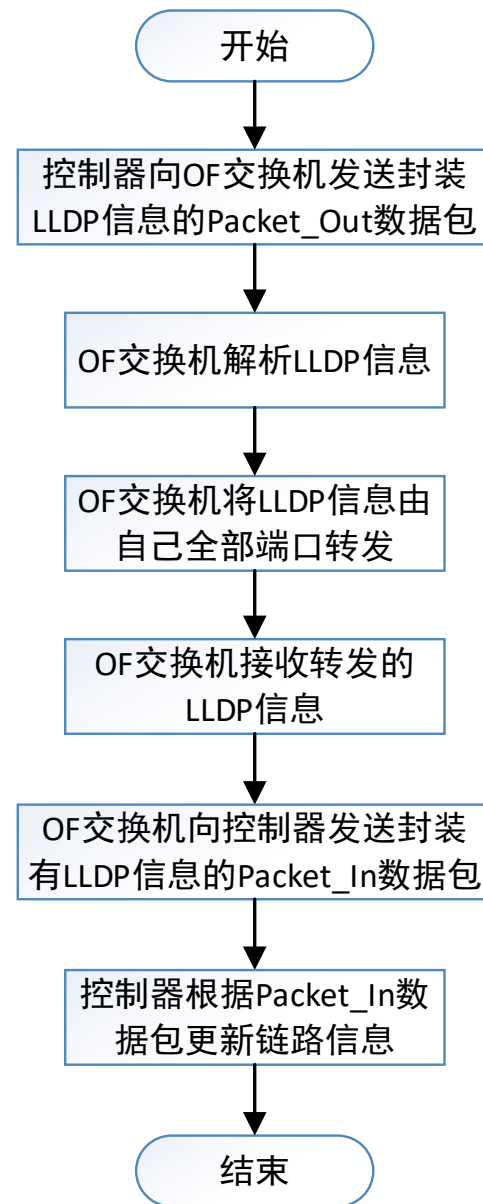


- 主机发现
 - 主机接入
 - Packet_In数据包中包括IP, MAC, 接入的交换机端口等信息
 - 主机配置表在对应主机接入期间一直存在, 直至主机离开网络时删除, 或者主机迁移时进行更新

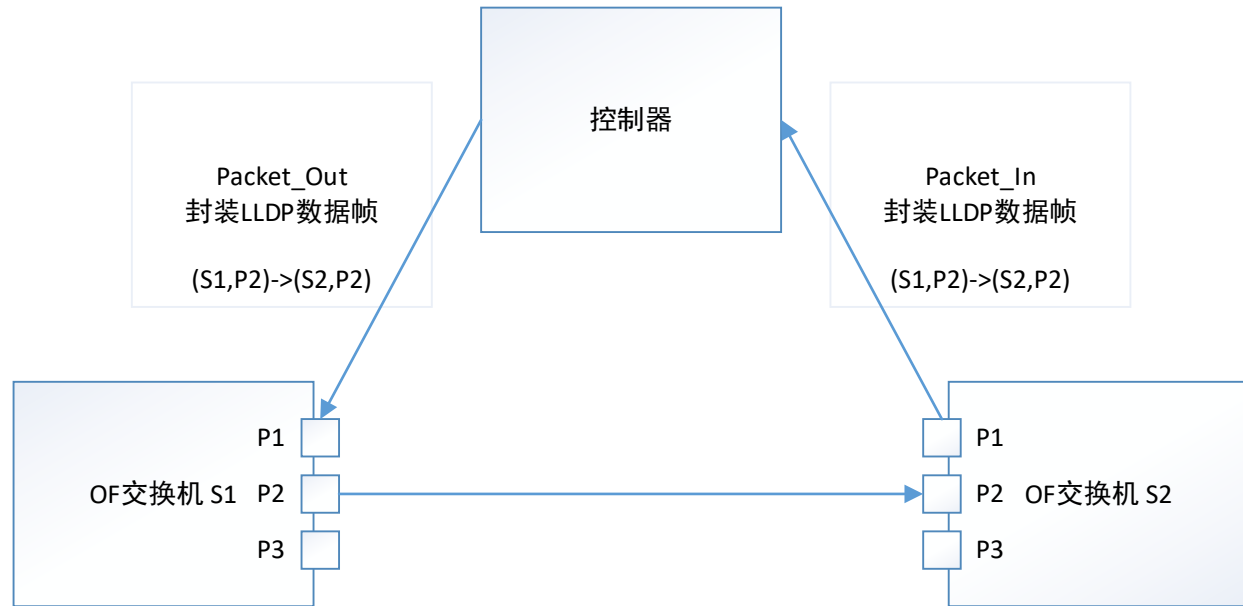


- OF交换机发现
 - OF交换机初始化时通过Hello消息建立连接
 - 控制器使用Features消息获取交换机信息
 - 使用Echo消息进行定期通信联立检查
 - OF交换机无需额外的协议保障发现

- 互联链路发现
 - OFDP协议
 - LLDP信息（数据帧）中包括了OF交换机更新链路所需要信息
 - OF交换机接收Packet_Out数据包并解析LLDP信息后，会根据其中的交换机编号和端口号更新互联链路
 - Packet_In数据包中带有源交换机和当前交换机的编号端口号等信息，用于控制器的链路信息更新



- 互联链路发现
 - 示例



- Packet_Out消息包含LLDP数据帧，以及指令(S1,P2)->(S2,P2)，即由S1的P2端口向S2的P2端口发送LLDP数据
- S1向S2发送数据
- S2接收到数据后，发送Packet_In消息给控制器，声明自己在P2端口接收到来自S1的P2端口的数据
- 控制器接收到Packet_In消息，确认S1P2和S2P2之间存在互联链路

- 优点
 - 简洁：充分利用现有协议，无需重新设计复杂的发现协议，便于实现
 - 全面：能够完全覆盖全部的活跃交换机及其链路
- 缺点
 - 高开销
 - 对网络中每一个活跃端口，控制器都需要发送一个 Packet_Out 数据包
 - 对网络中每一条活跃链路，控制器都会接收到两个 Packet_In 数据包
 - 低安全性
 - 缺乏数据认证机制，无法区分恶意伪造的虚假信息

- **网络可视化**
 - 拓扑发现能够帮助控制器实时的获取整个SDN的节点和连接关系
 - 基于节点和连接关系可以画出动态的网络拓扑，以达到运维和管理的可视化
- **流量监控**
 - OF交换机的流量统计功能，可以帮助控制器实时掌握网络中的流量情况
- **访问控制**
 - 通过更改流表规则，能够对主机的访问进行管理和限制
- **入侵检测**
- ...

- McKeown N , Anderson T , Balakrishnan H , et al. OpenFlow: Enabling Innovation in Campus Networks[J]. Acm Sigcomm Computer Communication Review, 2008, 38(2):69–74.
- Pakzad F , Portmann M , Tan W L , et al. Efficient topology discovery in software defined networks[C]// 8th International Conference on Signal Processing and Communication Systems (ICSPCS), 2014. IEEE, 2014.

- Azzouni A , Mai Trang N T , Boutaba R , et al. Limitations of OpenFlow Topology Discovery Protocol[C]// 2017 16th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net). IEEE, 2017.
- http://www.h3c.com/cn/d_201811/1131080_30005_0.htm
- http://www.h3c.com/cn/d_200805/605853_30003_0.htm

谢谢！

大成若缺，其用不弊。大盈
若冲，其用不穷。大直若屈。
大巧若拙。大辩若讷。静胜
躁，寒胜热。清静为天下正。

