**Raft** Introduction. Accessed: Jun. 2, 2017. [Online]. Available:http://infinispan.org/ https://raft.github.io

**Infinispan** Introduction. Accessed: Sep. 15, 2016. [Online]. Available:http://infinispan.org

**Mininet** Introduction. Accessed: Jun. 2, 2017. [Online]. Available:http://mininet.org

**NTP** Introduction. Accessed: Jun. 2, 2017. [Online]. Available:https://www.opendaylight.org

**IPERF** Introduction. Accessed: Jun. 2, 2017. [Online]. Available:http://www.ntp.org

入侵攻击：RPC buffer overflow是什么鬼？

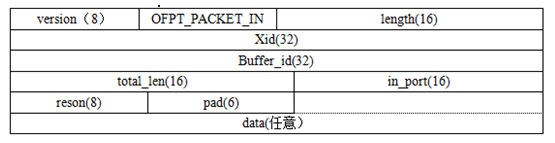
Nmap 可用来端口扫描http://nmap.org/

PACKET\_IN消息：将到达OF switch的message转给Controller,这么做的原因：

1.流表No\_MATCH

2.匹配有的action为“发往控制器”。

消息格式：



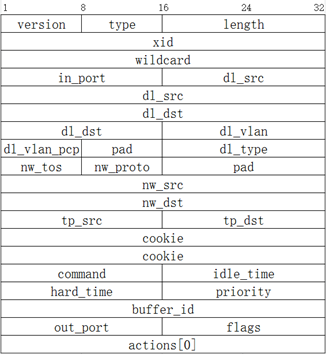
字段含议：



FLOW\_MOD消息：

触发：自动下发流表，手动下发流表（下发流表意思是对switch流表进行增删改查）

消息格式：



字段含义：



STATS\_REPLY:

这个回应跟请求是一起的



简单列出一下格式，学的时候再看OF文档。

FEATURES\_REPLY:

Features消息用于查询交换机特性，request与reply成对出现。



更具体的只有查文档了。

ARP poisoning 如：A请求：“Who has B,tell C”but with A's MAC address http://goo.gl/p4AVhf

LLDP spoofing 创建假的边

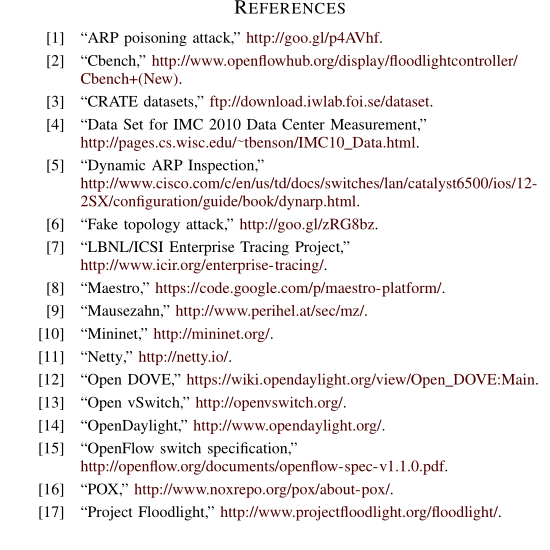
Java 的Netty库

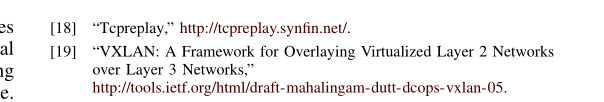
Controller DoS 利用Cbench http://www.openflowhub.org/display/floodlightcontroller/

Cbench+(New).

Tcpreply 使packet\_in率发生变化 http://tcpreplay.synfin.net/.

Mausezahn控制TCP包率 http://www.perihel.at/sec/mz/.





Link flooding attack: **看The Crossfire Attack为A类论文**