**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？

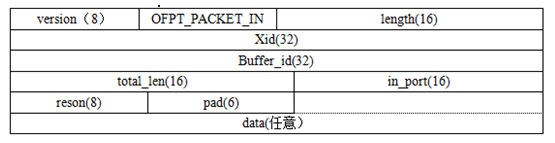
Nmap 可用来端口扫描http://nmap.org/

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：



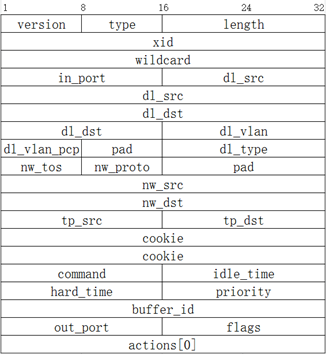
字段含议：



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

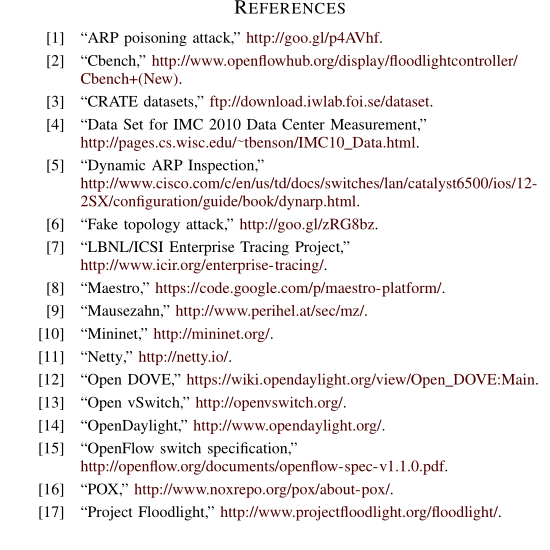
Java 的Netty库

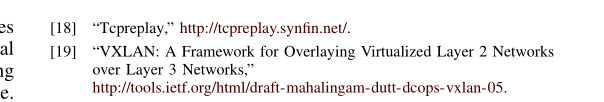
Controller DoS 利用Cbench http://www.openflowhub.org/display/floodlightcontroller/

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**

**入侵检测信息交换格式** RFC4765. The intrusion detection message exchange format

(idmef). [http://www.ietf.org/rfc/rfc4765.txt](informattion_format.txt)

**Snort**: open source intrusion prevention system capable of real-time traffic analysis and packet logging.网站：[Snort](https://snort.org/)

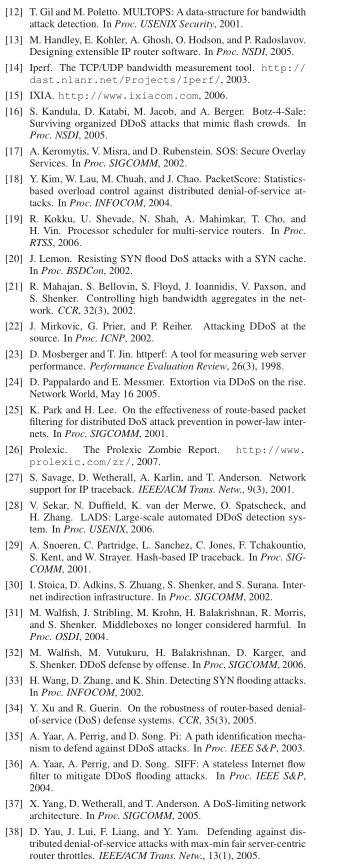
**Botnet**也就是我们所说的[僵尸网络](https://baike.baidu.com/item/%E5%83%B5%E5%B0%B8%E7%BD%91%E7%BB%9C/5391691)，是指采用一种或多种传播手段，将大量[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA/455151)感染bot程序（[僵尸程序](https://baike.baidu.com/item/%E5%83%B5%E5%B0%B8%E7%A8%8B%E5%BA%8F)），从而在控制者和被感染主机之间所形成的一个可一对多控制的网络。

Network Worm:通过网络传染的一种病毒，本质是一个程序勤务命令行文件。

**ANML. DDoS attack tools.** http://anml.iu.edu/ddos/tools.html, 2001.

**httperf**: A tool for measuring web serverperformance. Performance Evaluation Review

DdoS的文章，担是太老了，截图如下：



**D-ITG（Distributed Internet Traffic Generator）**:良性流量生成器，可生成各种协议，包大小和包率可以各种分布。

**TFN2K：**DdoS流量生成器，可以生成UDP flod,TCP/SYN flood,ICMP/flood,mix attackl

开源工具：

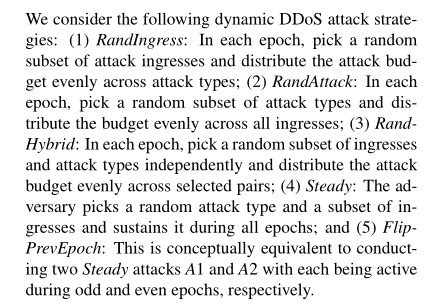
**iptables**. http://www.netfilter.org/projects/iptables/.

**Snort,Bro**

**Npdump：检测工具**

**OpenDNS server with BIND：DNS amplification攻击。**

**DDOS攻击策略：**



|  |
| --- |
| MAWI 标签数据集：MAWILab: combining diverse anomaly detectors for automated anomaly labeling and performance benchmarking |

**BGP消息数据集：**“RIPE Network Coordination Centre.” [Online]. Available: https://www.ripe.net/

**开源BGP模拟器：**“Chaos: BGP-4 Simulator.” [Online]. Available: https://github.com/VolSec/chaos

**路由策略：**P. Gill, M. Schapira, and S. Goldberg, “A survey of interdomain routingpolicies,” ACM SIGCOMM CCR, 2013.

**僵尸网络：**“Understanding the mirai botnet,” in USENIX Security, 2017

“Netlab360’s Mirai Scanner.” [Online]. Available: http://data.netlab.360.com/mirai-scanner/

**网络拓扑：**“SSFNet.” [Online]. Available: http://ssfnet.org+BRITE.” [Online]. Available: http://www.cs.bu.edu/brite

**网络拓扑：**<http://www.topology-zoo.org/index.html>

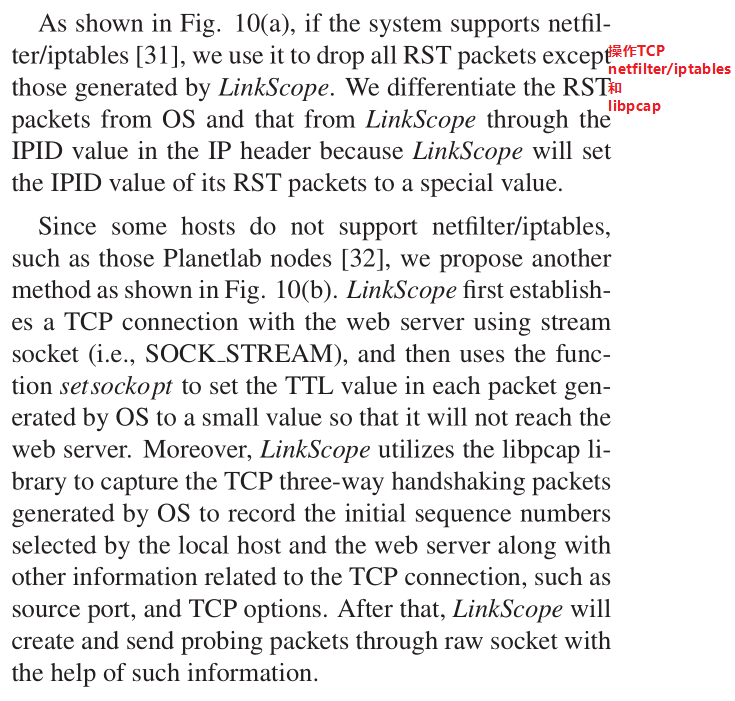
**正常流量：**

1. 工具：<http://tcpreplay.appneta.com/>

2.数据集：<http://pages.cs.wisc.edu/~tbenson/IMC10_Data.html>；<http://www.caida.org/data/passive/trace_stats/chicago-B/2015/?monitor=20150219-130000.UTC>；<http://traffic.comics.unina.it/Traces/ttraces.php>

**测拓扑：pair traceroute;rocketfuel**

**操作TCP**



**Netperf：测网络性能的，**Netperf工具以client/server方式工作。server端是netserver，用来侦听来自client端的连接，client端是netperf，用来向server发起网络测试。在client与server之间，首先建立一个控制连接，传递有关测试配置的信息，以及测试的结果；在控制连接建立并传递了测试配置信息以后，client与server之间会再建立一个测试连接，用来来回传递着特殊的流量模式，以测试网络的性能。在《the design and implementation of Open vSwitch》中用它来来测一分钟建立了多少次TCP从而测OVS的性能。