

OpenFlow: abrindo portas para inovações nas redes de nossos campi

Leandro Haruo Aoyagi
 Universidade Federal de São Carlos, Campus Sorocaba
 Sorocaba, São Paulo
 Email: aoyagi.haruo@gmail.com

Resumo – A comunidade científica, depois de reconhecer a dificuldade que existe para conseguir realizar e testar novos experimentos em um ambiente de rede real trabalhou duro para encontrar uma alternativa. Diversos projetos estão sendo desenvolvidos, porém ou são de longo-prazo, ou são ambiciosos demais, ou muito custosos, ou não possuem o desempenho necessário. O Open Flow é um caminho para os pesquisadores executarem protocolos experimentais em uma rede real de pequena escala como a rede de uma Universidade.

Index Terms – Switch OpenFlow, tabela de fluxo, canal seguro, controlador, protocolo OpenFlow.

I. INTRODUCTION

AS redes de computadores se tornaram parte essencial da infraestrutura de nossas residências, escolas e empresas. Elas fazem parte do cotidiano de milhares de pessoas ao redor do mundo. Por causa dessa expansão, o trabalho dos pesquisadores da área se tornou muito mais importante, porém com o grande crescimento do número de equipamentos e protocolos instalados para suportar a expansão, surgiu uma enorme barreira que está dificultando a vida desses pesquisadores.

A maioria das ideias que surgem não consegue ser executada e nem testada por causa da falta de maneiras práticas que possibilitem a realização de experimentos com novos protocolos de rede em um ambiente suficientemente realista para ganhar a confiança necessária para uma implantação generalizada. Por esse motivo alguns pesquisadores estão dizendo que a rede está “ossificada”.

Com o objetivo de resolver esse enorme problema a comunidade de pesquisa está desenvolvendo redes virtualizadas programáveis, uma das propostas é o GENI [2].

As redes virtualizadas programáveis podem diminuir a barreira de entrada de novas ideias. O GENI, por exemplo, tem o intuito de facilitar a realização de experimentos com novas arquiteturas de redes e sistemas distribuídos, utilizando switches e roteadores que podem ser programados para encaminhar pacotes simultaneamente para múltiplas redes experimentais. Através da virtualização o GENI consegue

atribuir aos pesquisadores uma fatia dos recursos da rede, como enlaces, switches, roteadores e terminais para que eles possam configurá-los da maneira que eles desejarem.

A implantação dessa proposta seria muito interessante, mas devido a sua grande escala é um projeto muito ambicioso, custoso e levaria muito tempo para ser completado.

Então, para encontrar uma alternativa de curto prazo alguns pesquisadores pensaram em ambientes que se aproximam do nosso cotidiano e de escala menor, os nossos campi universitários. A partir daí surgiram algumas questões:

- Como realizar experimentos nas redes dos nossos campi universitários?
- Como ganhar a confiança dos administradores de rede dos campi para que eles se sintam confortáveis em permitir a introdução de equipamentos experimentais em sua rede?
- Como os pesquisadores poderiam controlar uma parte da rede local sem perturbar os outros que dependem dela?
- Quais funcionalidades seriam necessárias na rede de switches para permitir experiências?

Uma das alternativas seria convencer os fornecedores de equipamentos que já possuem nome no mercado a produzirem switches e roteadores com plataformas abertas, virtualizadas e programáveis. Assim, os administradores ficariam tranquilos, pois o equipamento pertence a uma marca de confiança e os pesquisadores conseguiriam testar novos protocolos. Mas, este resultado seria muito improvável em curto prazo, pois os equipamentos diferem de fornecedor para fornecedor com vários elementos ocultos ao cliente, além de que plataformas abertas diminuiriam a barreira de entrada para novos concorrentes.

Já existem algumas plataformas que possuem software aberto, mas elas não possuem o desempenho e nem a densidade de porta necessária. Um exemplo simples é um computador com diversas interfaces de rede e um sistema operacional que suporta o encaminhamento de pacotes entre as interfaces e os protocolos existentes e permite que o usuário

configure a maneira que os pacotes serão tratados, porém o problema é a falta de desempenho. Um computador não consegue suportar o número de portas necessárias para rede de uma universidade inteira e nem aproximar-se do desempenho que uma rede real pode chegar.

Se pensarmos nas plataformas que possuem hardware especializado em encaminhamento também chegaríamos a conclusão de que elas não são adequados para a rede de uma universidade. A Universidade de Washington está desenvolvendo uma abordagem baseada em roteadores virtualizados programáveis chamado Supercharged PlanetLab Platform que é uma abordagem muito promissora a longo prazo, mas é cara demais para ser implantada em uma rede de uma universidade, ela é mais indicada para grandes centros de comutação. Por outro lado existe uma abordagem que utiliza uma placa PCI de baixo custo com um FPGA programável para o processamento de pacotes e quatro portas que é o NetFPGA[3], ele é indicado para laboratórios de pesquisa e para o ensino, porém o NetFPGA só suporta quatro interfaces de rede e esse número é insuficiente.

Então, para permitir a experimentação de novas propostas para as redes em uma escala menor foi proposto o switch OpenFlow, que tem o objetivo de abrir as portas para que os pesquisadores consigam executar seus experimentos na rede real de sua própria universidade, através de mecanismos que permitem a divisão do tráfego em fluxo de produção (fluxo real) e fluxo de pesquisa. Outro objetivo também é permitir a adição das funcionalidades do OpenFlow nos switches e roteadores comerciais já existentes sem que seja exposto o projeto de suas plataformas.

Para se tornar uma abordagem mais promissora o projeto do OpenFlow se compromete a ser flexível para atender certos requisitos como:

- Ser passível a implementações de baixo custo e alto desempenho;
- Ter capacidade de suportar uma ampla gama de pesquisas científicas;
- Garantir isolamento entre o tráfego de pesquisa e o tráfego de produção;
- Consistir com a necessidade dos fabricantes de não expor o projeto de suas plataformas.

Neste artigo será abordado o switch OpenFlow, uma proposta que tem como objetivo, abrir as portas para as inovações nas redes de computadores.

II. OS SWITCHES OPENFLOW

A maioria dos switches e roteadores modernos possuem uma tabela de fluxo que possibilitam a implementação de funcionalidades como firewalls, *Quality of Service* (QoS) e a coleta de estatísticas. As tabelas de fluxo desses equipamentos diferem de uma marca para outra, porém existe um conjunto de funções comuns à maioria dos switches e roteadores. A

ideia básica do OpenFlow é explorar esse conjunto de funções comuns de manipulação de tabelas de fluxo, tornando-se compatível com um maior número de equipamentos.

O OpenFlow fornece um protocolo aberto para programar a tabela de fluxo desses equipamentos. Dessa maneira, o administrador de rede consegue dividir o tráfego em fluxo de produção e fluxo de pesquisa. Os pesquisadores conseguem controlar o seu próprio fluxo, escolhendo a rota e o tratamento que cada pacote deve receber. Enquanto na mesma rede o tráfego de produção é isolado e processado normalmente.

Dessa maneira os pesquisadores conseguem testar seus experimentos como novos protocolos de roteamento e modelos de segurança, na mesma rede que o tráfego do fluxo de produção e sem interferir no seu bom funcionamento.

O data path de um switch OpenFlow é formado por uma tabela de fluxos com uma ação associada a cada um desses fluxos. Permitindo que os fluxos sejam tratados de maneira diferente. Por isso o administrador consegue manter o isolamento do tráfego do fluxo de pesquisa do fluxo de produção.

O conjunto de ações de um switch OpenFlow é extensível, mas esses equipamentos devem conter um requisito mínimo. O seu data path deve ser flexível para garantir alto desempenho e baixo custo.

O switch OpenFlow é composto por, no mínimo, três partes:

1. Uma tabela de fluxo com uma ação associada a cada fluxo que indica ao switch como tratar o fluxo;
2. Um canal seguro que conecta o switch ao controlador da rede. Essa conexão permite que comandos e pacotes possam ser enviados entre o controlador e o switch; e
3. O protocolo OpenFlow, que permite que o controlador se comunique com o switch de maneira padrão.

Através do protocolo OpenFlow os pesquisadores conseguem configurar a tabela de fluxo sem precisar programar o switch.

Existem dois tipos de switches OpenFlow, um é o switch OpenFlow dedicado, que não suporta o encaminhamento comum das camadas 2 e 3 e o outro é o roteador ou switch ethernet comercial com OpenFlow habilitado.

A. Switches OpenFlow dedicados

Um switch OpenFlow dedicado apenas encaminha os pacotes entre as portas do switch de acordo com a Tabela de Fluxos configurada remotamente. Neste contexto os fluxos podem ser definidos de diferentes maneiras. Por exemplo, um fluxo pode ser definido como todos os pacotes provenientes de um endereço MAC ou um endereço IP. Além disso, alguns comutadores OpenFlow podem tratar pacotes que não são IPv4, verificando os campos arbitrários do cabeçalho. Isso mostra a flexibilidade do OpenFlow para suportar diferentes tipos de experimentos.

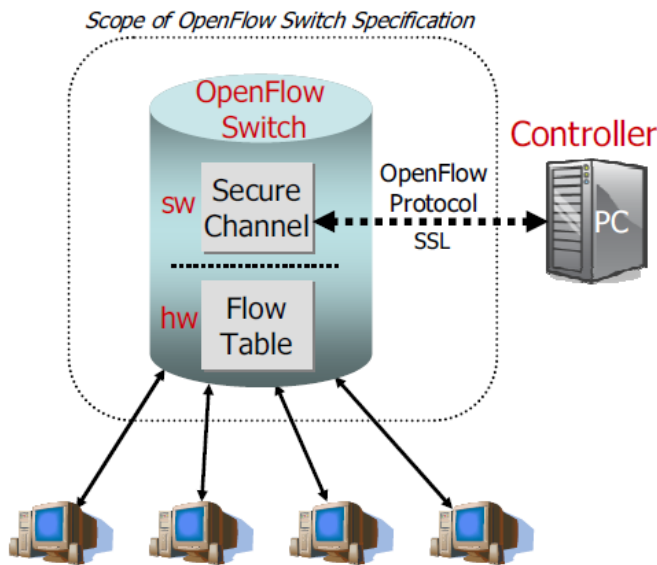


Figura 1 - Switch OpenFlow dedicado. A tabela de fluxo é controlada por um controlador remoto através de um canal seguro. Retirado de [1].

Como foi dito anteriormente, cada entrada de fluxo possui uma ação associada a ela. As três ações mais básicas são:

1. Encaminhamento dos pacotes do fluxo para uma determinada porta (ou portas). Isso permite que os pacotes sejam encaminhados pela rede.
2. Encapsulamento dos pacotes do fluxo e transmissão para um controlador através do canal seguro. Normalmente isso é feito com o primeiro pacote de um fluxo novo, assim o controlador pode verificar se o fluxo deve ser adicionado à tabela de fluxo. Essa ação pode ser utilizada também, para o envio dos pacotes ao controlador para o recebimento de tratamentos adicionais.
3. Descartar os pacotes do fluxo. Essa ação pode ser utilizada em casos de segurança, para impedir ataques de negação de serviço.

Uma entrada da tabela de fluxo possui três campos:

1. Um campo para o cabeçalho de pacote, que define o fluxo;
2. Outro para a ação, que define como o pacote deve ser tratado; e
3. Por fim um campo para as estatísticas, que mantém o controle do número de pacotes e bytes de cada fluxo e o tempo decorrido desde que o último pacote pertencente ao fluxo foi identificado pelo switch, essa última estatística auxilia na remoção de fluxos inativos.

Nos switches “tipo 0” que são a primeira geração de switches OpenFlow, o cabeçalho é uma tabela 10-tupla como mostrado na Figura 2. Um fluxo pode ser definido por todos os dez campos da tabela ou por campos arbitrários, isso varia de acordo com o tipo do experimento.

In Port	VLAN ID	Ethernet			IP			TCP	
		SA	DA	Type	SA	DA	Proto	Src	Dst

Figura 2 - Campos do cabeçalho de um de fluxo de um switch OpenFlow “tipo 0”. Retirado de [1].

B. Switches com OpenFlow habilitado

Esses switches são os switches, roteadores e pontos de acesso comerciais reforçados com os recursos do OpenFlow. São adicionados a esses equipamentos a tabela de fluxo, o canal seguro e o protocolo OpenFlow.

Em uma rede de switches e pontos de acesso comerciais com OpenFlow habilitado todas as tabelas de fluxo são tratadas pelo mesmo controlador, o protocolo OpenFlow possui um recurso que permite que dois ou mais controladores controlem um switch auxiliando no aumento do desempenho e da robustez.

Esses equipamentos com o OpenFlow habilitado tem como objetivo tornar possível o isolamento do tráfego experimental, que utiliza os mecanismos do OpenFlow, do tráfego de produção que utiliza os mecanismos normais de um switch. Esse isolamento pode ser garantido através de duas opções, uma seria adicionar uma quarta ação, o encaminhamento dos pacotes através do pipeline normal do switch. Assim, o fluxo que for identificado como não referente ao OpenFlow será processado utilizando-se o encaminhamento normal. Outra opção para garantir que o tráfego de produção seja processado normalmente pelo switch é através do uso de VLANs, definindo conjuntos separados de VLANs para o tráfego de produção e para o tráfego experimental.

Todos os switches com OpenFlow habilitado precisam conter uma dessas duas ações, alguns equipamentos suportam as duas.

C. Controladores

O controlador é quem adiciona e remove as entradas de fluxo em uma tabela de fluxo para os experimentos. Por exemplo, um controlador estático é uma simples aplicação rodando em um computador que, durante um experimento, decide estaticamente quais fluxos pertencem ou não a um conjunto de computadores de teste. Para este caso podemos comparar os fluxos com as VLANs das redes atuais, que fornecem um mecanismo simples de isolamento de tráfego, isolando o tráfego experimental do tráfego de produção. Por esse motivo alguns pesquisadores dizem que o OpenFlow é uma versão generalizada das VLANs.

Alguns pesquisadores imaginaram controladores mais sofisticados que poderiam adicionar e remover dinamicamente os fluxos durante um experimento. Normalmente, um pesquisador consegue controlar toda a rede de switches OpenFlow e configurar a maneira de como os fluxos serão tratados, esses controladores mais potentes conseguem suportar vários pesquisadores, onde cada um possui uma conta e permissões diferentes, os pesquisadores podem então executar seus experimentos independentes em diferentes conjuntos de fluxos. Os fluxos que forem identificados como sendo de um determinado pesquisador é entregue a um

programa de controle de nível de usuário que decide se o novo fluxo de entrada pode ou não ser adicionado à rede de acordo com as permissões do usuário.

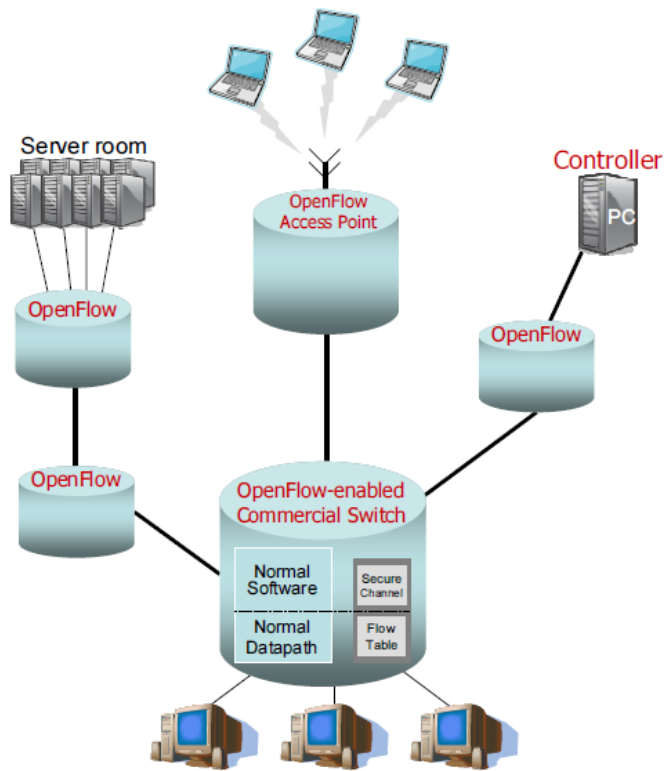


Figura 3 - Exemplo de uma rede de switches e roteadores com OpenFlow habilitado. Retirado de [1].

III. USANDO O OPENFLOW

Como foi citado anteriormente, o OpenFlow é uma abordagem que abre as portas para a evolução das redes, dando a um controlador o poder de modificar o comportamento dos equipamentos da rede através de um conjunto bem definido de instruções de encaminhamento de pacotes.

Atualmente, o crescente ecossistema do OpenFlow já possui roteadores, switches, switches virtuais e pontos de acesso de uma série de fornecedores. O conjunto de experimentos que podem ser executados em redes OpenFlow ainda não é certo, pois por ser uma plataforma experimental o OpenFlow pode suportar muitos tipos de experimentos. Alguns dos exemplos de como uma rede com OpenFlow habilitado pode ser usada para o experimento de novas aplicações e arquiteturas de rede são:

A. Exemplo 1: Novos protocolos de roteamento

Vamos pensar em um cenário onde um pesquisador quer testar um novo protocolo de roteamento utiliza uma rede de switches OpenFlow sem realizar modificações nos terminais. Para isso o novo protocolo deve ser configurado para ser executado no controlador, a cada hora que um novo pacote

chegar ao switch o protocolo irá traçar uma rota pelos switches OpenFlow e adicionar um fluxo de entrada em cada switch dessa rota. Para executar o experimento no tráfego de uma rede OpenFlow o pesquisador não pode perturbar os outros que dependem dela. Então o pesquisador precisa definir que um fluxo seja todo o tráfego que está entrando no switch OpenFlow pela porta do switch que está conectada ao seu computador e adicionar um fluxo de entrada com a ação “Encapsulamento e envio de todos os pacotes ao controlador”. Assim, quando os pacotes enviados pelo pesquisador chegarem ao controlador, o protocolo irá traçar uma rota e adicionar um fluxo de entrada a todos os switches dessa rota. Dessa forma, os próximos pacotes que chegarem serão processados rapidamente pela tabela de fluxo.

B. Redes não IP

Anteriormente foi citado que um switch OpenFlow pode analisar campos arbitrários do cabeçalho de um pacote, permitindo que os pacotes assumam vários formatos.

Dessa maneira, poderão ser testados novos esquemas de endereçamento, encaminhamento e nomeação.

Existem várias maneiras de um switch com OpenFlow habilitado reconhecer um tráfego “não IP”. Os fluxos poderiam ser identificados pelo endereço MAC de origem e destino, um novo tipo de Ethernet ou uma nova versão do IP.

C. Mobilidade

Uma rede OpenFlow suporta pontos de acesso sem fio, permitindo que clientes móveis se conectem a servidores e a Internet por meio de sua infraestrutura. Neste exemplo o controlador é programado para rastrear a localização do cliente, que alterando dinamicamente as tabelas de fluxo reencaminha conexões de acordo com a movimentação do usuário possibilitando um perfeito handoff de um ponto de acesso a outro.

D. VLANs

Assim como as VLANs o OpenFlow consegue facilmente fornecer ao usuário a sua própria rede isolada. Uma maneira simples é declarar estaticamente um conjunto de fluxos que especificam as portas acessíveis ao tráfego de uma determinada VLAN ID. Então o tráfego que for enviado de uma porta específica do switch ou de um determinado endereço MAC será marcado com uma VLAN ID apropriada.

E. Processamento de pacotes

De acordo com os exemplos que vimos anteriormente sobre experimentos que trabalham com fluxos, sempre que um fluxo começa o controlador toma as suas decisões quanto a ele. Alguns experimentos necessitam que cada pacote seja processado. Podemos pensar em um experimento de um mecanismo de controle de congestão, ou em experimentos em que o conteúdo dos pacotes precisa ser alterado, ou quando é necessário converter os pacotes de um formato de protocolo

para outro ou até mesmo um sistema de detecção de intrusos que inspeciona todos os pacotes.

Em uma rede com OpenFlow habilitado é possível processar os pacotes de duas diferentes maneiras. Uma seria forçar que todos os pacotes de um fluxo passassem por um controlador. Para fazer isso, um controlador permite que o switch realize o encaminhamento de cada pacote ao controlador do modo padrão. Esta flexibilidade fornece uma maneira prática de, por exemplo, realizar testes das funcionalidades de um novo protocolo, porém essa flexibilidade custa desempenho então essa maneira não seria muito interessante em uma grande rede.

Encaminhar os pacotes para um switch programável que realiza o processamento dos pacotes seria a segunda maneira. Temos como exemplo, um roteador NetFPGA programável que processa os pacotes de acordo com as definições de um usuário. O switch com OpenFlow habilitado opera como um patch panel para fazer com que o pacote alcance o NetFPGA. Podemos ver um exemplo de como isso acontece na figura 4.

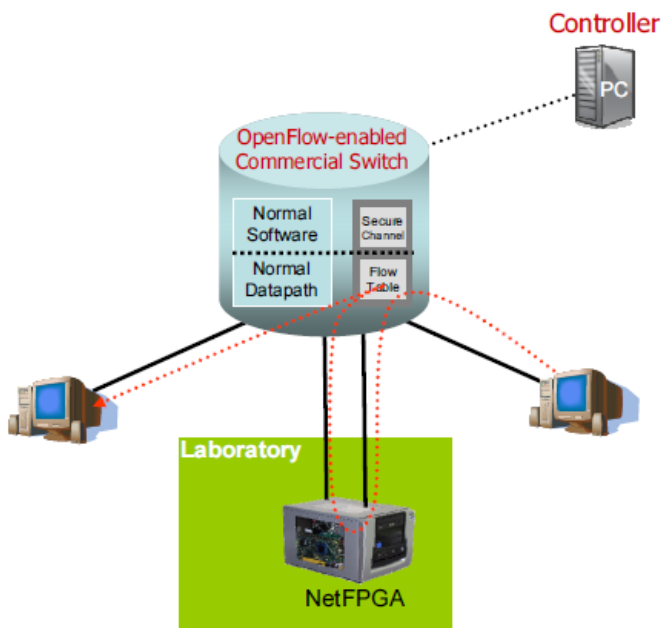


Figura 4 - Exemplo do processamento de pacotes através de um dispositivo de processamento de pacotes, o roteador NetFPGA programável

IV. CONCLUSÃO

O OpenFlow tem a capacidade de fornecer aos pesquisadores um ambiente de testes em uma rede como a rede local de nossas Universidades. Assim ele abre as portas para que os pesquisadores possam testar suas inovações e garantir que seus experimentos sejam testados em um ambiente suficientemente semelhante ao de uma rede real qualquer, conseguindo assim, ganhar a confiança para uma implantação generalizada, tirando a necessidade de os fornecedores exporem o projeto interior de seus produtos e também a necessidade do pesquisador de encomendar um equipamento com um software específico de controle para a realização de seus testes.

Como o OpenFlow é uma plataforma experimental ele permite a execução de diversos tipos de experimentos. Por suportar essa grande variedade de experimentos essa ferramenta pode possibilitar um grande avanço na área de Redes de Computadores.

Esta abordagem é muito interessante e quanto mais inovações forem surgindo com a ajuda do OpenFlow mais Universidades espalhadas pelo mundo todo irão implantar o OpenFlow em suas redes, aumentando a quantidade de redes que suportam experimentos. Além disso, com o aumento do número de universidades com redes OpenFlow, futuramente, poderão ser realizados acordos para que essas redes se interconectem e aumentem ainda mais a escala desses ambientes de teste. Um dos exemplos de projetos que estão sendo realizados no Brasil que fazem uso do OpenFlow é o Horizon[5], um projeto que aborda a Internet do Futuro nas universidades e empresas brasileiras e francesas.

REFERENCIAS

- [1] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. "OpenFlow: enabling innovation in campus networks", ACM SIGCOMM Computer Communication Review, 38(2):69–74, 2008.
- [2] GENI: Global Environment for Network Innovations, Web site: <http://www.geni.net/> - Acessado em Abril/2011.
- [3] NetFPGA: Programmable Networking Hardware. Web site: <http://netfpga.org> – Acessado em Abril/2011.
- [4] The OpenFlow Switch Specification. Web Site: <http://OpenFlowSwitch.org> – Acessado em Abril/2011.
- [5] Horizon Project: A New Horizon to The Internet, Web site: <http://www.gta.ufrj.br/horizon/> - Acessado em Abril/2011.