

Aula 01 - Conceitos básicos e visão geral de OpenFlow/SDN

MATE18 – Oficina de OpenFlow/SDN
Universidade Federal da Bahia

Italo Valcy <italovalcy@ufba.br>

05 de julho de 2017

Licença de uso e atribuição



Todo o material aqui disponível pode, posteriormente, ser utilizado sob os termos da:

Creative Commons License:

Atribuição - Uso não comercial - Permanência da Licença



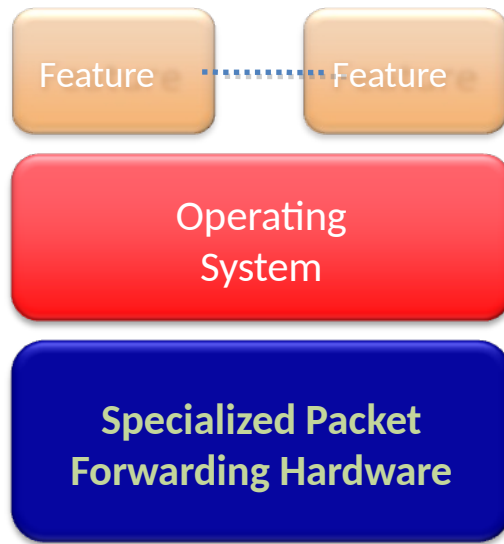
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

Agenda

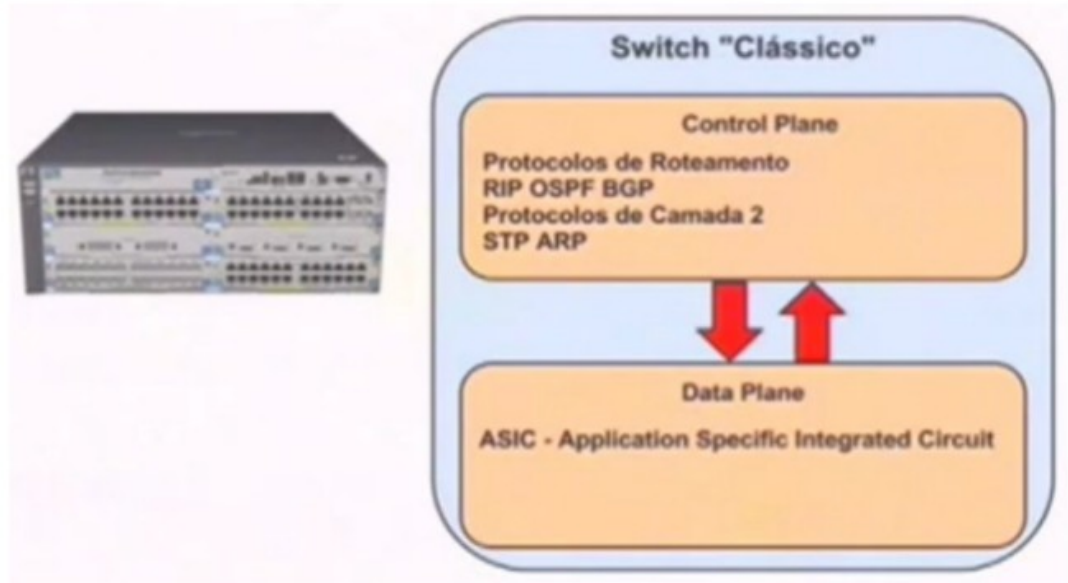
- ▶ Aula 01: conceitos de OpenFlow, prática de captura de pacotes, alteração do datapath de forma pró-ativa
 - Exercício: estudo sobre mininet, prática de criação de caminhos com ofctl
- ▶ Aula 02: controlador OpenFlow, exemplos, APIs, bibliotecas e aplicações de apoio
- ▶ Aula 03: construção de aplicação L2 multi-switch com Ryu/Mininet
- ▶ Aula 04: prática com switches reais, conceitos de slices

A rede atual

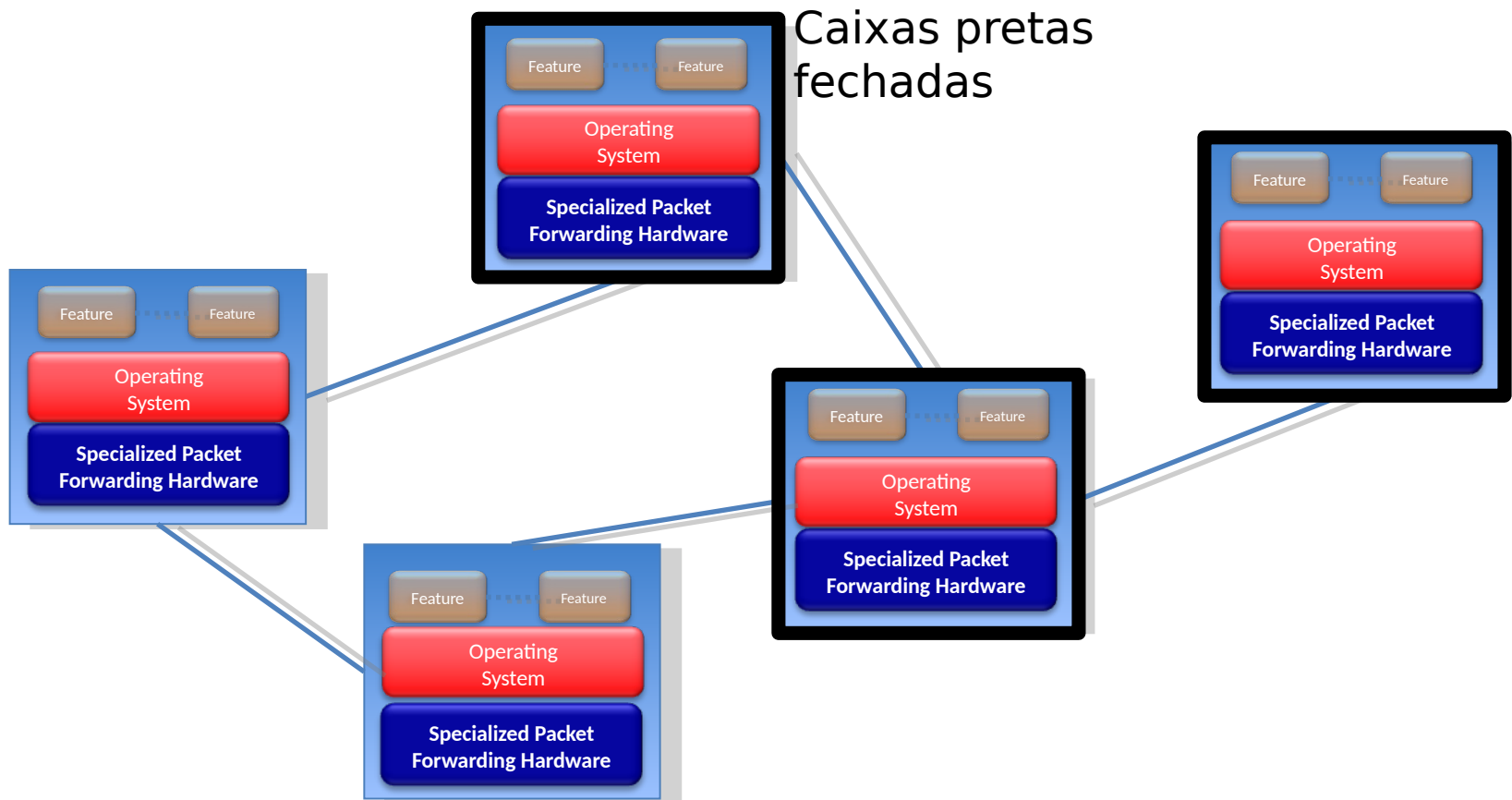
Roteamento, gerencia, mobilidade, controle de acesso, VPN, ...



Verticalização
Fechado, proprietário
Inovação lenta



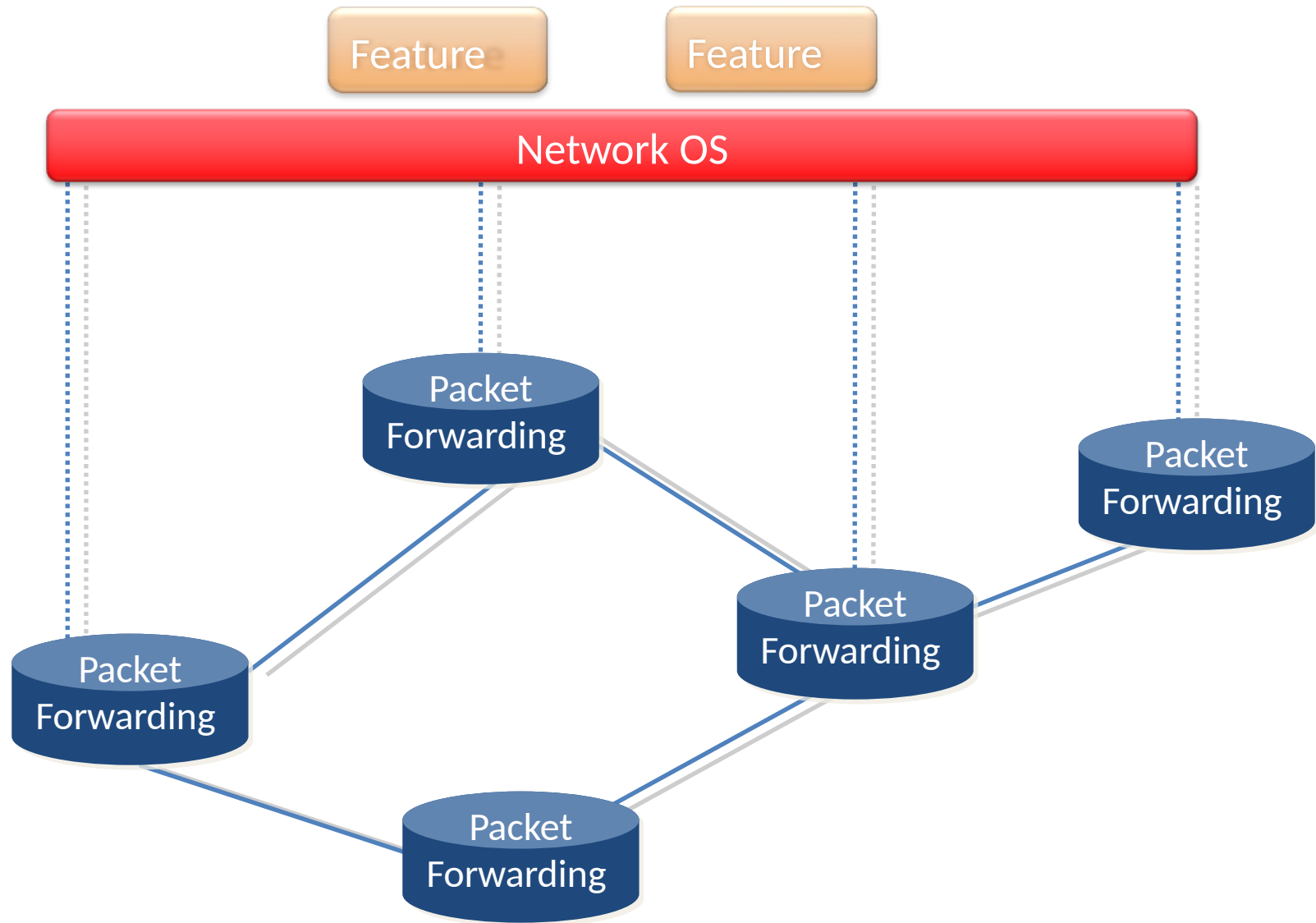
A rede atual



A rede atual

- ▶ Dificuldades com o modelo atual:
 - Múltiplas sintaxes de CLI;
 - Funcionalidades dependentes de fabricante – tempo de implantação;
 - Licenciamento por funcionalidade;
 - Impossibilidade de testar novas funcionalidades de rede (protocolos);
 - Customizações são restritas aos parâmetros de configuração;
 - Rede com pouca flexibilidade.

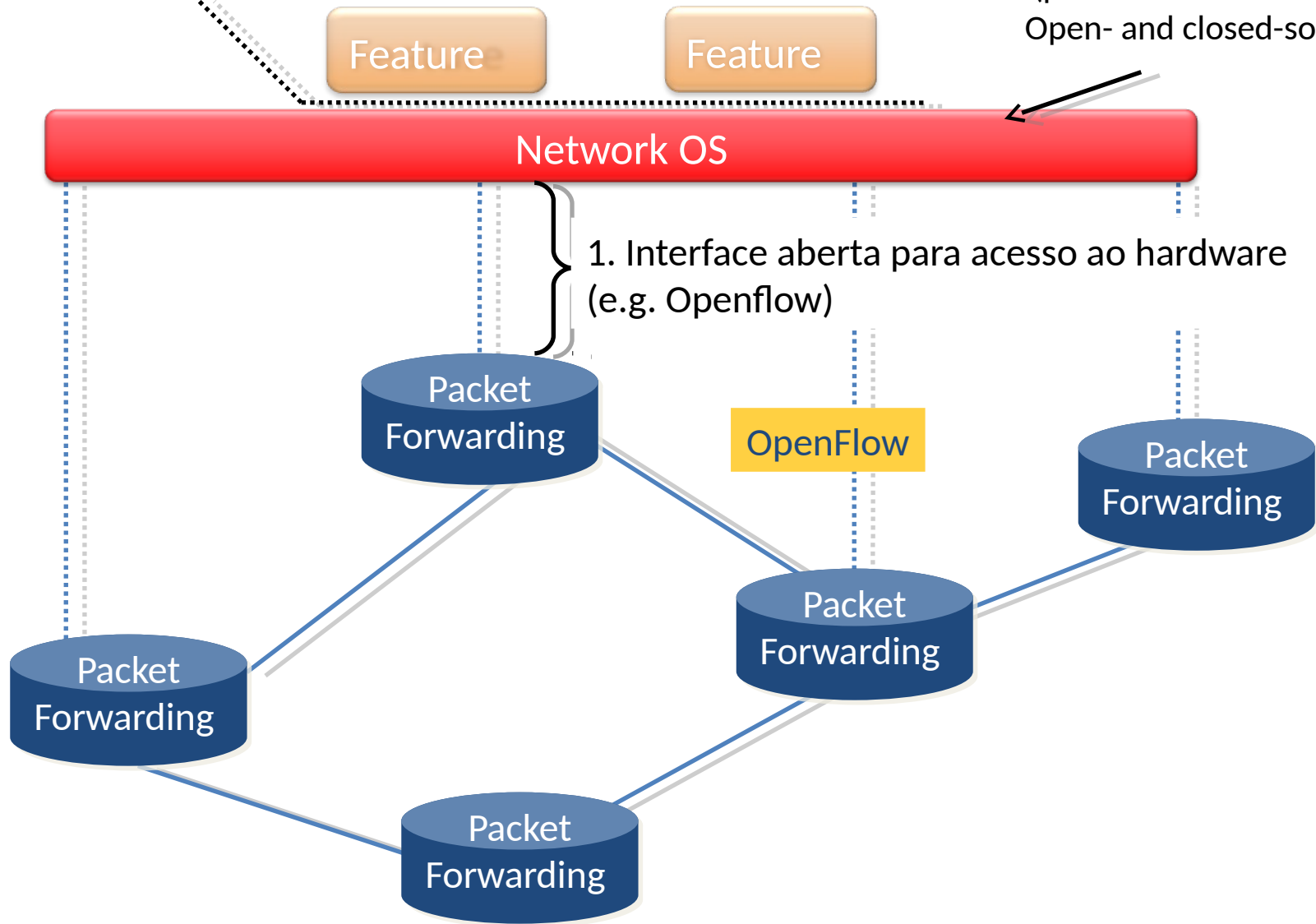
A “Rede definida por software”



A “Rede definida por software”

3. API aberta bem definida

2. Pelo menos um SO de rede
(provavelmente muitos)
Open- and closed-source

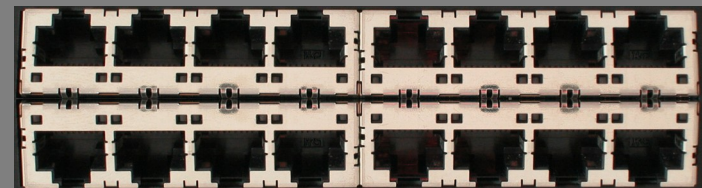
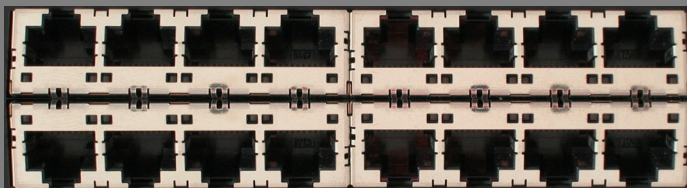


Openflow

*Openflow é uma **interface aberta** para **controlar remotamente a tabela de encaminhamento** de equipamentos de rede como switches, roteadores e access points.*

- ▶ A partir dessa primitiva de baixo nível, pesquisadores podem construir redes com novas propriedades de alto nível.

Ethernet Switch/Router



Fonte: Nick McKeown (Stanford), SDN CIO Summit 2010

Control Path (Software)

Data Path (Hardware)

Fonte: Nick McKeown (Stanford), SDN CIO Summit 2010

OpenFlow Controller

OpenFlow Protocol (SSL)



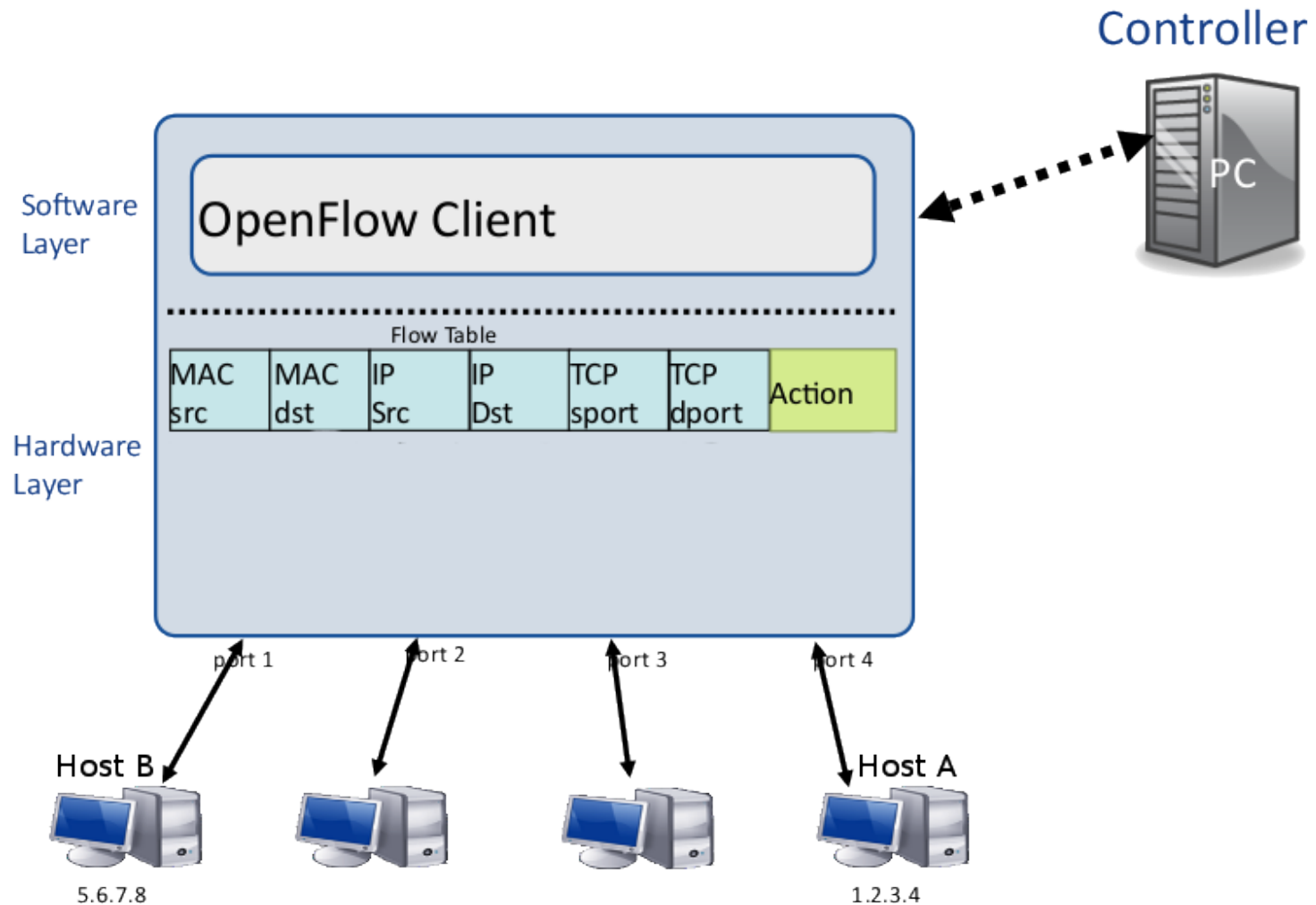
Control Path

OpenFlow

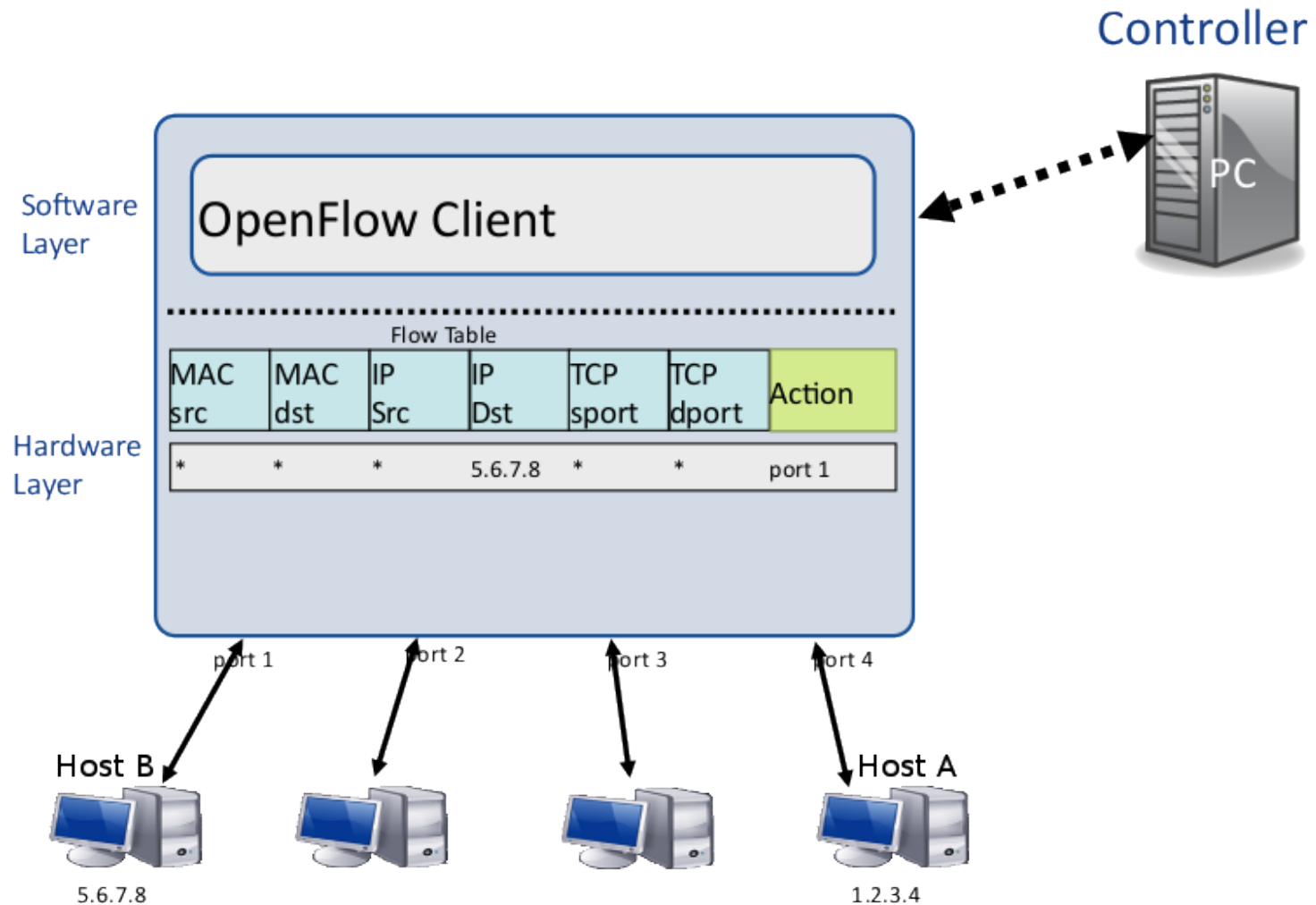
Data Path (Hardware)

Fonte: Nick McKeown (Stanford), SDN CIO Summit 2010

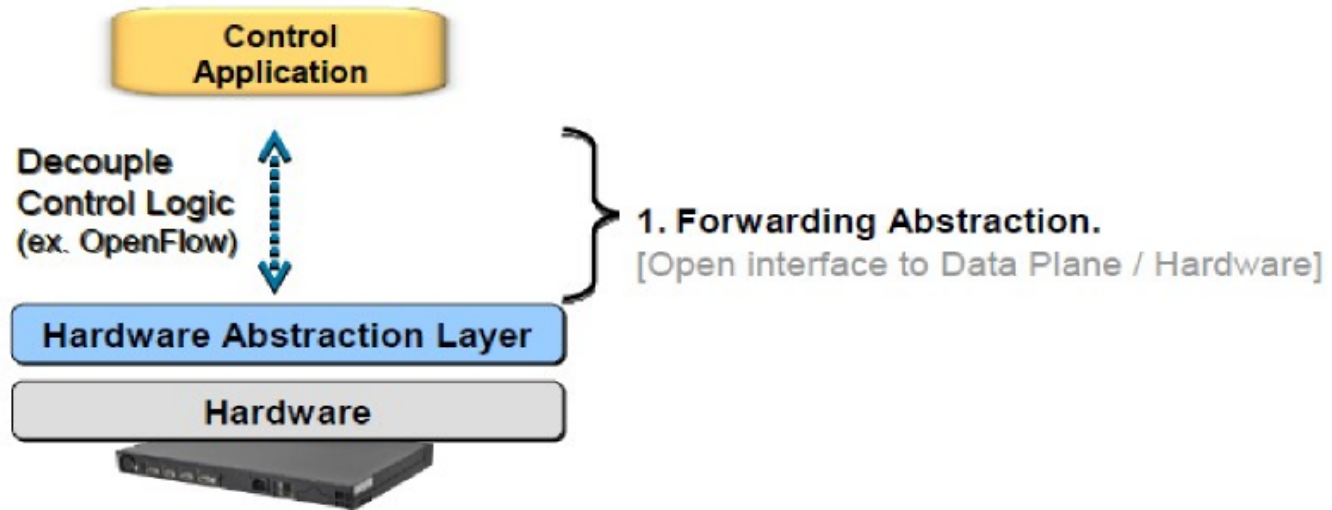
Exemplo do OpenFlow



Exemplo do OpenFlow

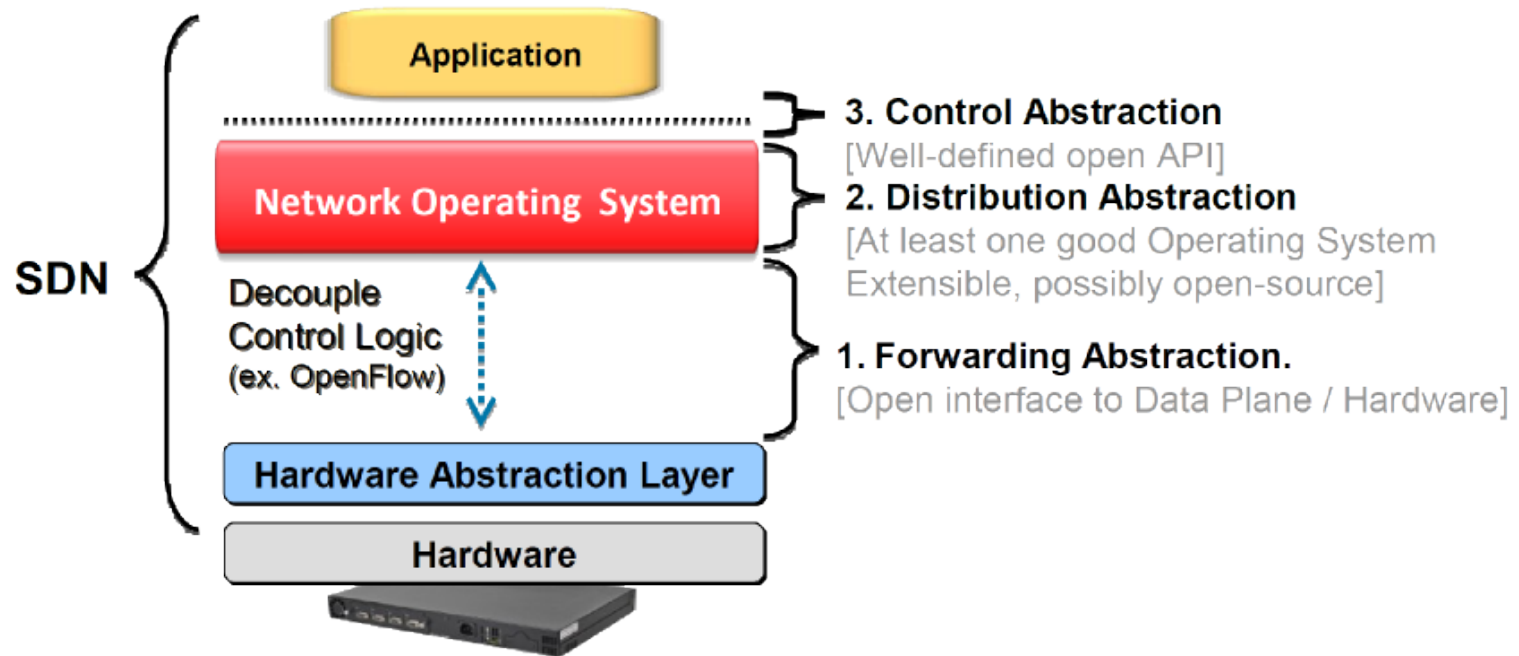


OpenFlow é um protocolo, SDN é uma arquitetura



- ▶ Redes Definidas por Software (SDN) refatoram o relacionamento entre os dispositivos de rede e o software que os controla
- ▶ OpenFlow é uma interface aberta que permite um controle mais flexível e previsível da rede, tornando fácil estender sua função. [HotSDN'12 CFP]

OpenFlow é um protocolo, SDN é uma arquitetura



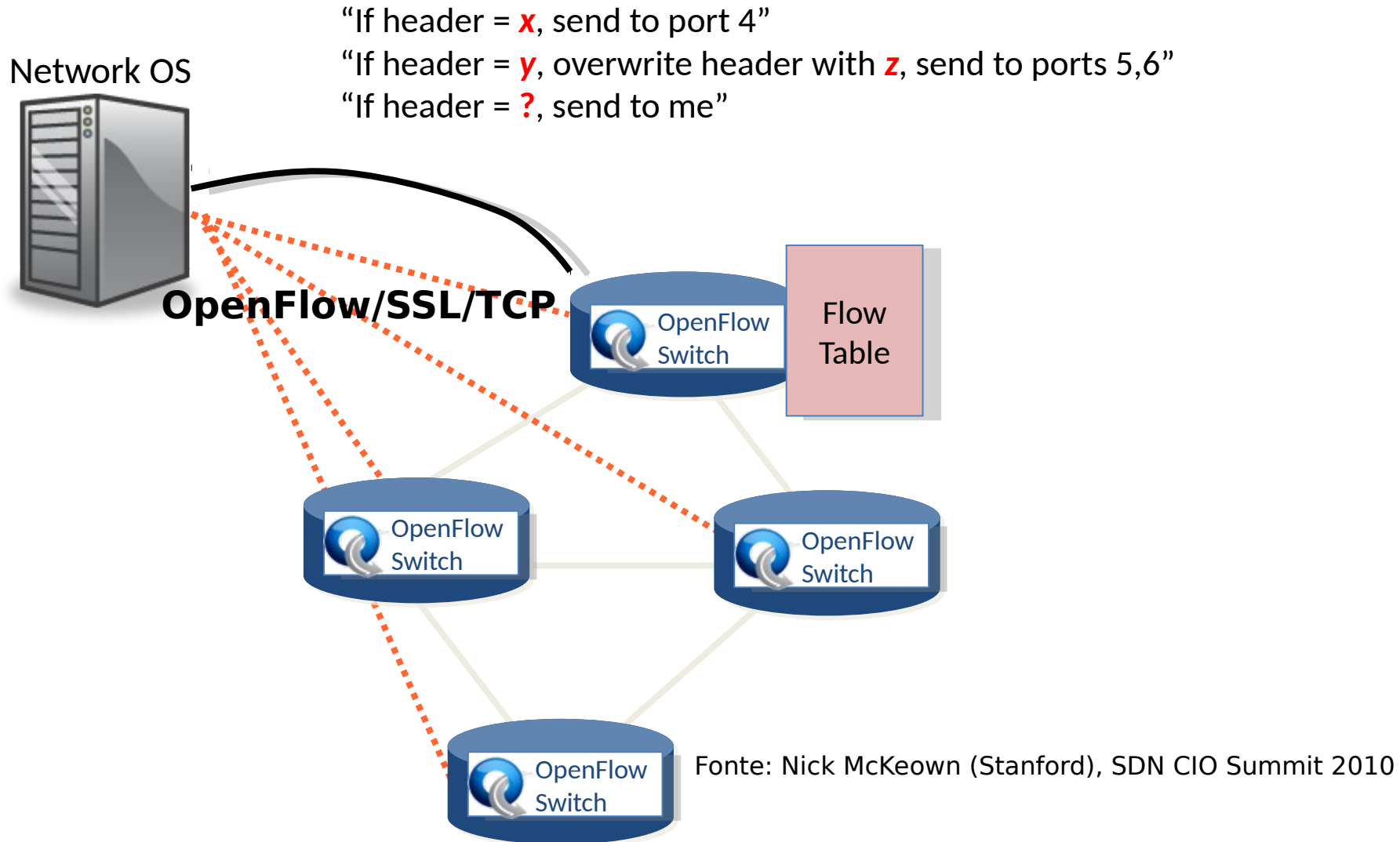
- ▶ Redes Definidas por Software (SDN) refatoram o relacionamento entre os dispositivos de rede e o software que os controla
- ▶ OpenFlow é uma interface aberta que permite um controle mais flexível e previsível da rede, tornando fácil estender sua função. [HotSDN'12 CFP]

Exercício de fixação 1

- ▶ Como SDN/OpenFlow trata as seguintes questões?
 - Múltiplas sintaxes de CLI;
 - Funcionalidades dependentes de fabricante – tempo de implantação;
 - Licenciamento por funcionalidade;
 - Impossibilidade de testar novas funcionalidades de rede (protocolos);
 - Customizações são restritas aos parâmetros de configuração;
 - Rede com pouca flexibilidade.

Como funciona o Openflow?

Como Openflow funciona



Como OpenFlow funciona

- ▶ A principal abstração utilizada na especificação do OpenFlow é o conceito de fluxo
- ▶ Um fluxo é constituído pela combinação de campos do cabeçalho do pacote a ser processado pelo dispositivo.

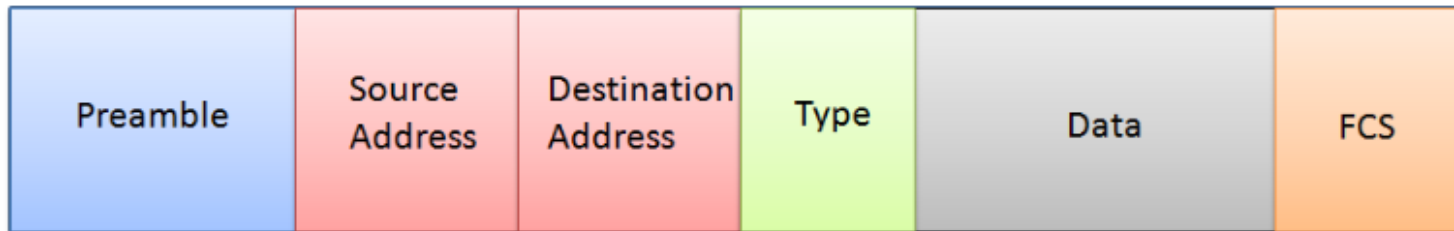
Como Openflow funciona

- ▶ Definição: fluxo
 - É uma **sequência unidirecional** de pacotes na qual todos os pacotes compartilham **um conjunto de valores de cabeçalho comum**
- ▶ Exemplos:
 - Fluxo 1: pacotes com destino 192.168.0.0/24
 - Fluxo 2: pacotes com interface de entrada 2, VLAN ID 10 e MAC de destino X:X:X:X:X:X
 - Fluxo 3: pacotes com IP de origem X.X.X.X, IP de destino Y.Y.Y.Y e porta TCP de destino 80
 - ...

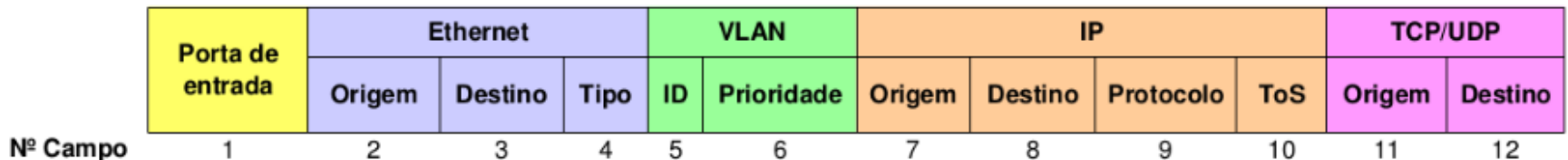
Como Openflow funciona

- ▶ Exemplos de campos para definição do fluxo:

Ethernet frame

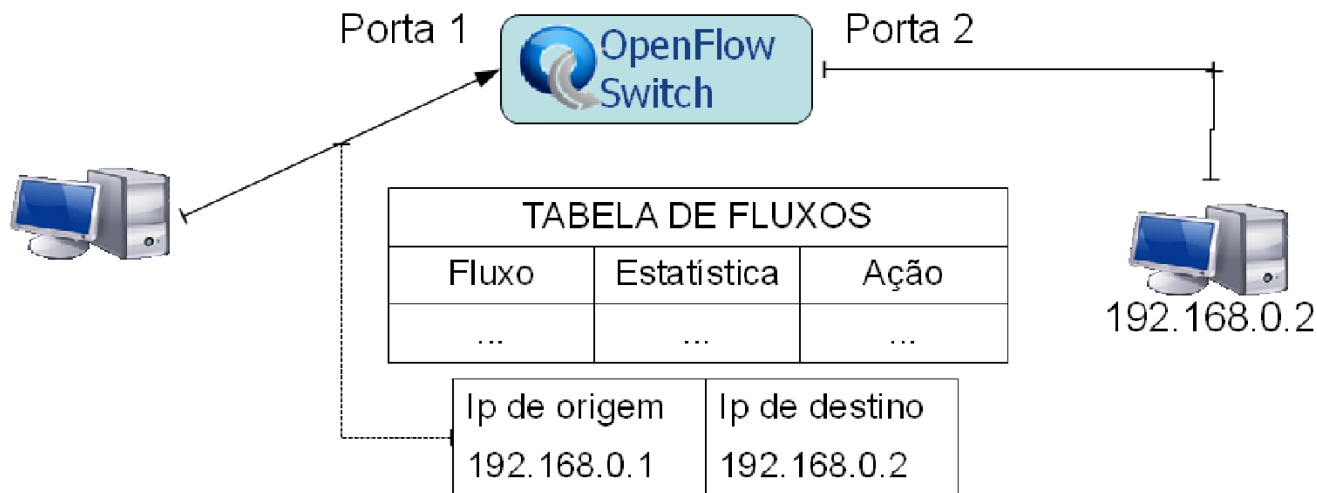


Cabeçalho dos *frames* do protocolo OpenFlow



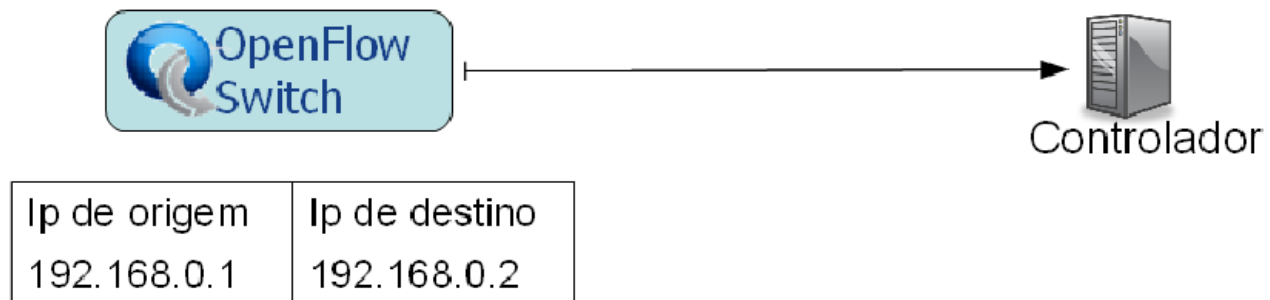
Como Openflow funciona

- ▶ Quando o switch recebe um pacote ele deve compará-lo com sua tabela de fluxo



Como Openflow funciona

- ▶ Se o cabeçalho não for compatível com nenhum fluxo em sua tabela, o switch deve encaminhar o cabeçalho (ou pacote todo) para o controlador



Como Openflow funciona

- ▶ Ao receber o pacote, o controlador deve tomar uma decisão e
 - Enviar uma requisição de **mudança da tabela de fluxos do switch**
 - Devolver o pacote (ou o cabeçalho + buffer-id)
 - Indicar uma **ação** para o pacote
 - Ou.. descartar

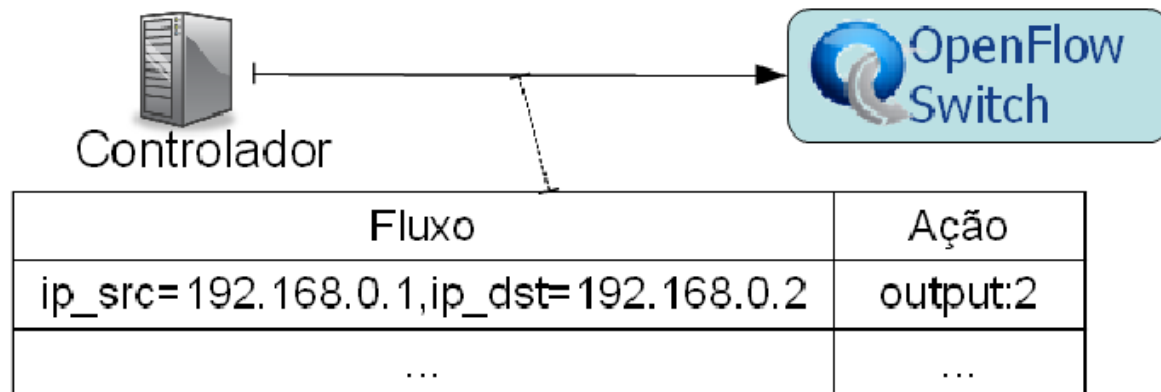


Tabela de fluxos

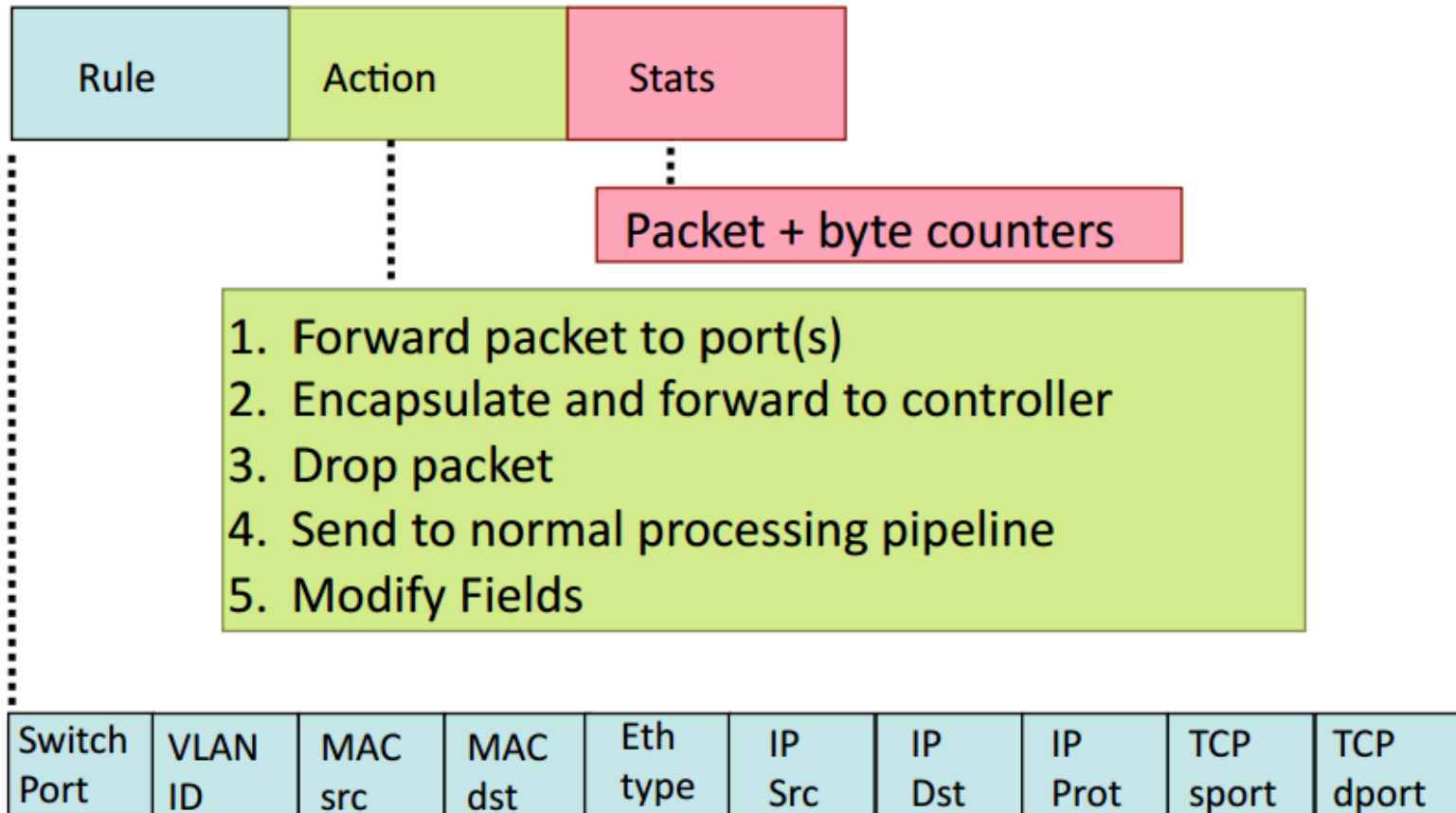


Tabela de fluxos - Exemplos

Switching

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	00:1f:..	*	*	*	*	*	*	*	port6

Flow Switching

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
port3	00:20..	00:1f..	0800	vlan1	1.2.3.4	5.6.7.8	4	17264	80	port6

Firewall

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	*	*	*	*	*	*	*	22	drop

Routing

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	*	*	*	*	5.6.7.8	*	*	*	port6

VLAN Switching

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	00:1f..	*	vlan1	*	*	*	*	*	port6, port7, port9

Componentes do OpenFlow

- ▶ **Tabela de fluxo:** realiza pesquisas em pacotes:
 - Todos os pacotes são comparados com a tabela de fluxo (match)
 - A ação a ser tomada depende das regras de match encontrada na tabela de fluxo
- ▶ **Canal seguro:** comunicação com o controlador externo.
- ▶ **Protocolo OpenFlow:** padroniza a comunicação do equipamento de rede com um sistema externo. Diversas versões: 1.0, 1.1, 1.2, 1.3, 1.4, 1.5, 1.6
- ▶ **Controlador:** software responsável pelas decisões de encaminhamento e atualização da *flow table*, conforme definido pelas aplicações

Exercício de fixação 2

- ▶ O que é um fluxo? O que é uma tabela de fluxos? Qual equivalente da tabela de fluxos em switches convencionais?
- ▶ Em qual camada do modelo TCP/IP o protocolo OpenFlow atua?
- ▶ Qual o papel do controlador?

Protocolo OpenFlow – Tipos de mensagem

- ▶ O protocolo OpenFlow suporta três tipos de mensagem (cada um com outros sub-tipos):
 - **Controller-to-switch**: iniciadas pelo controller e usadas para gerenciar ou inspecionar o estado do switch
 - **Asynchronous**: iniciadas pelo switch e usadas para atualizar o controller dos eventos da rede e mudanças no switch
 - **Symmetric**: podem ser iniciadas pelo controller ou pelo switch sem solicitação

Protocolo Openflow – Tipos de mensagem

- ▶ Controller-to-switch (algumas):
 - **Features**: quais capabilities o switch suporta?
 - **Modify-state**: add/delete/modify flows na tabela de flows do switch
 - **Read-State**: obter estatísticas da tabela de flows, portas ou flows individuais
 - **Send-Packet**: usado pelo controller para enviar pacotes para uma porta do switch

Protocolo Openflow – Tipos de mensagem

- ▶ Asynchronous (algumas):
 - **Packet-in**: switch encaminha pacote (ou cabeçalho) para o controller se não houver uma entrada correspondente previamente instalada na tabela de flows
 - **Flow-removed**: quando o timeout do flow expirou e ele foi removido da tabela de flows
 - **Port-Status**: switch informa ao controller sobre mudanças na configuração do estado das portas
 - **Error**: informa ao controller sobre erros diversos

Protocolo Openflow – Tipos de mensagem

- ▶ Symmetric (algumas):
 - **Hello**: usados no estabelecimento da conexão do switch com o controller
 - **Echo**: Echo request/reply usado para checar latência, largura de banda e/ou conexões ativas

Protocolo Openflow - Ações

Na versão 1.0:

- ▶ Required:
 - Forward (ALL, CONTROLLER, IN_PORT)
 - Drop
- ▶ Optional:
 - Enqueue
 - Forward (NORMAL)
 - Modify-field (set VLAN ID, strip VLAN header, modify src/dst MAC, modify src/dst IPv4, modify src/dst transport port, etc.)

Protocolo Openflow - Contadores

Na versão 1.0:

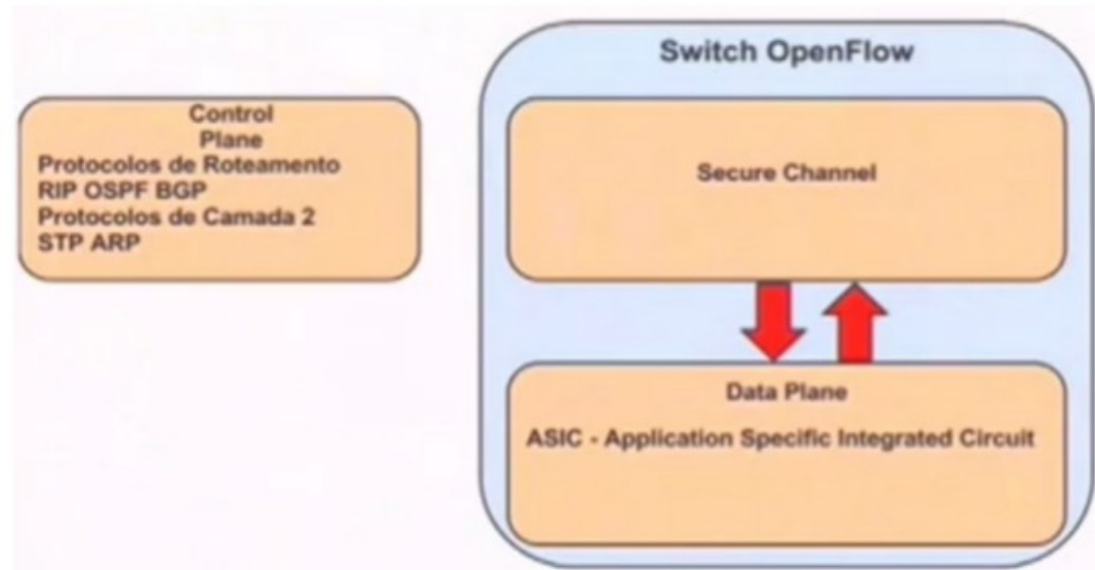
Counter	Bits
Per Table	
Active Entries	32
Packet Lookups	64
Packet Matches	64
Per Flow	
Received Packets	64
Received Bytes	64
Duration (seconds)	32
Duration (nanoseconds)	32

Per Port	
Received Packets	64
Transmitted Packets	64
Received Bytes	64
Transmitted Bytes	64
Receive Drops	64
Transmit Drops	64
Receive Errors	64
Transmit Errors	64
Receive Frame Alignment Errors	64
Receive Overrun Errors	64
Receive CRC Errors	64
Collisions	64
Per Queue	
Transmit Packets	64
Transmit Bytes	64
Transmit Overrun Errors	64

Switch OpenFlow

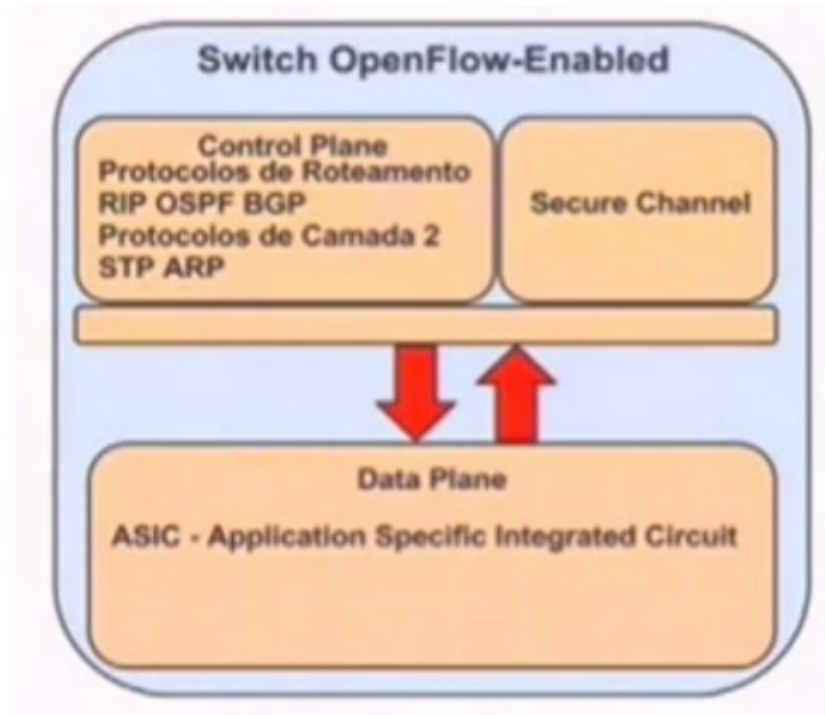
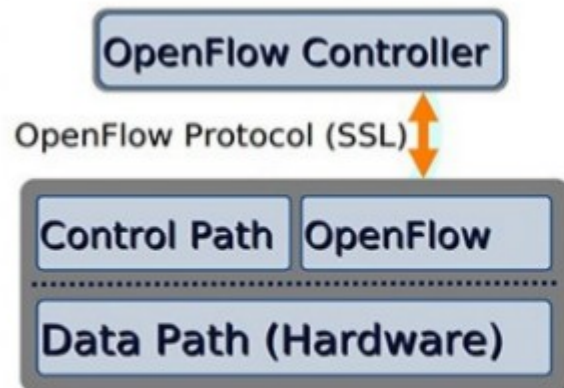
- ▶ O protocolo OpenFlow define dois tipos de switches:
 - Switch OpenFlow (only);
 - Switch OpenFlow – Enabled (hybrid).

Ex Switch OpenFlow only:



Switch OpenFlow

- ▶ Switch OpenFlow híbrido



Controlador OpenFlow

- ▶ O controlador OpenFlow se comunica com os switches através de um canal seguro
 - Objetivo: atualização da tabela de fluxo
 - A lógica é executada pelo controlador
- ▶ Fornece API (*Application Programming Interface*) para implementação de aplicações.
- ▶ Canal de controle: tcp ou ssl; in-band ou out-of-band

Exercício de fixação 3

- ▶ Qual a função das seguintes mensagens e como elas são processadas no controlador?
 - Packet-In
 - Modify-state
 - Send-Packet
 - Features
- ▶ Qual a diferença de controle *in-band* versus *out-of-band*?

OpenFlow em ação

- ▶ Quando um pacote chega a um equipamento com OpenFlow habilitado, os cabeçalhos do pacote são comparados às regras das entradas das tabelas de fluxos, os contadores são atualizados e as ações correspondentes são realizadas.

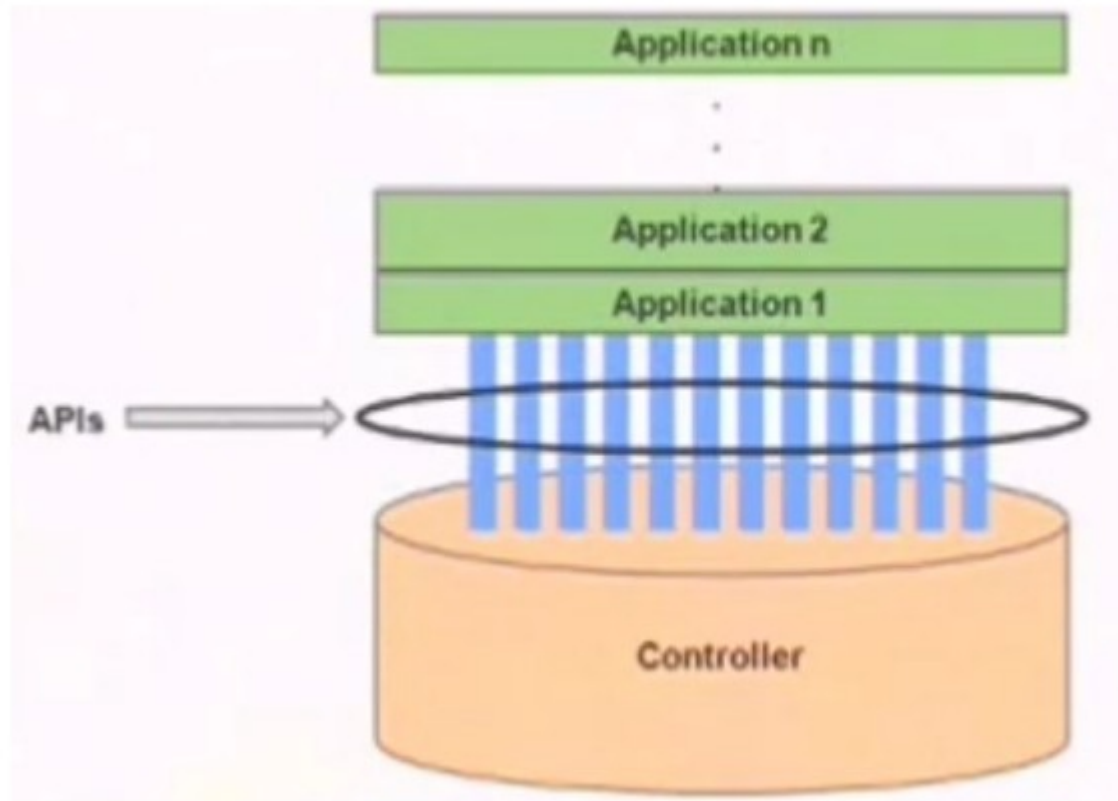
OpenFlow em ação

- ▶ Se não houver correspondência entre o pacote e alguma entrada da tabela de fluxos, o pacote é encaminhado, por completo, ao controlador.
- ▶ Alternativamente, apenas o cabeçalho encaminhado ao controlador mantendo pacote armazenado no buffer do hardware.

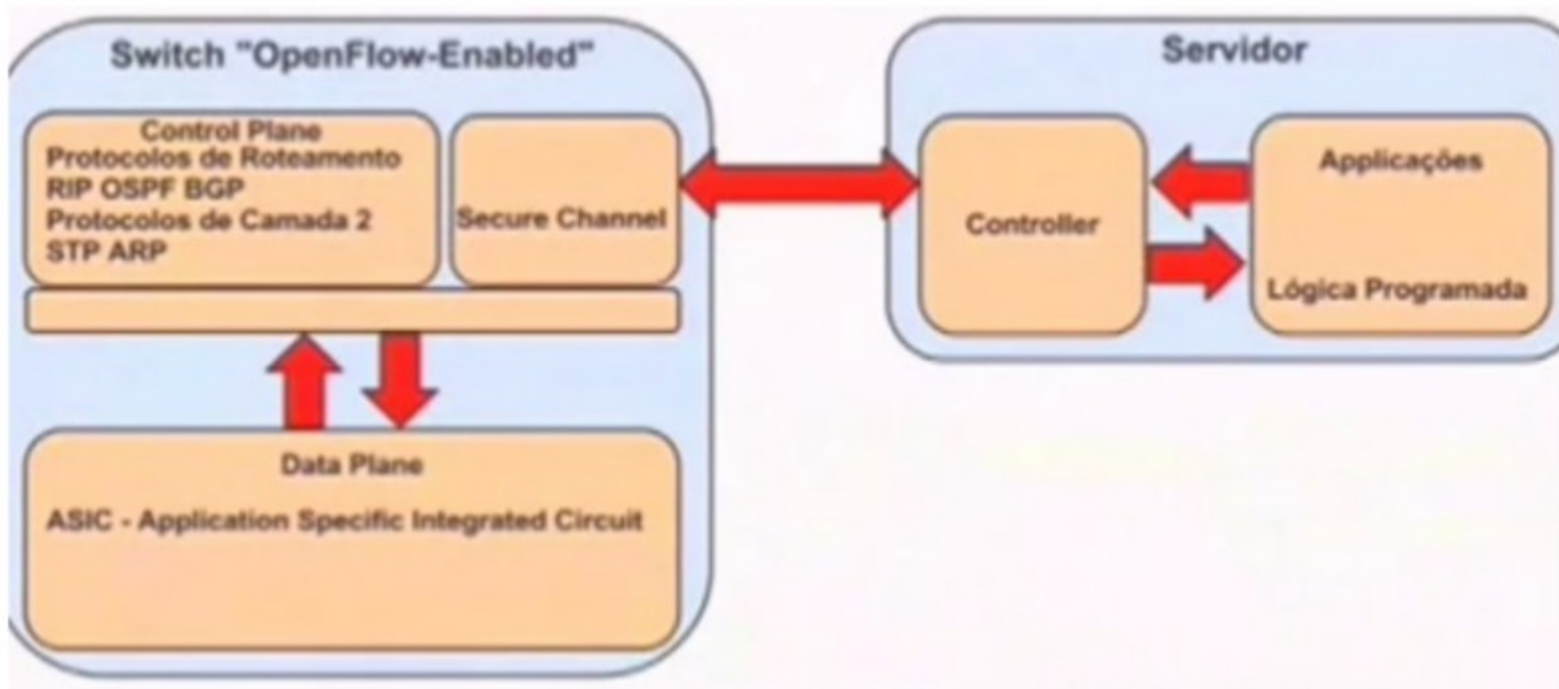
OpenFlow em ação

- ▶ As ações associadas aos fluxos incluem:
 - a) encaminhar o fluxo de pacotes para determinada porta(s);
 - b) modificar os campos do cabeçalho;
 - c) encapsular e transmitir o pacote para o controlador;
 - d) descartar os dados, como medida de segurança, com a implementação de firewalls, ou ainda para inibir ataques de negação de serviço;
 - e) encaminhar o pacote para o processamento normal do equipamento nas camadas 2 ou 3.

Controlador OpenFlow

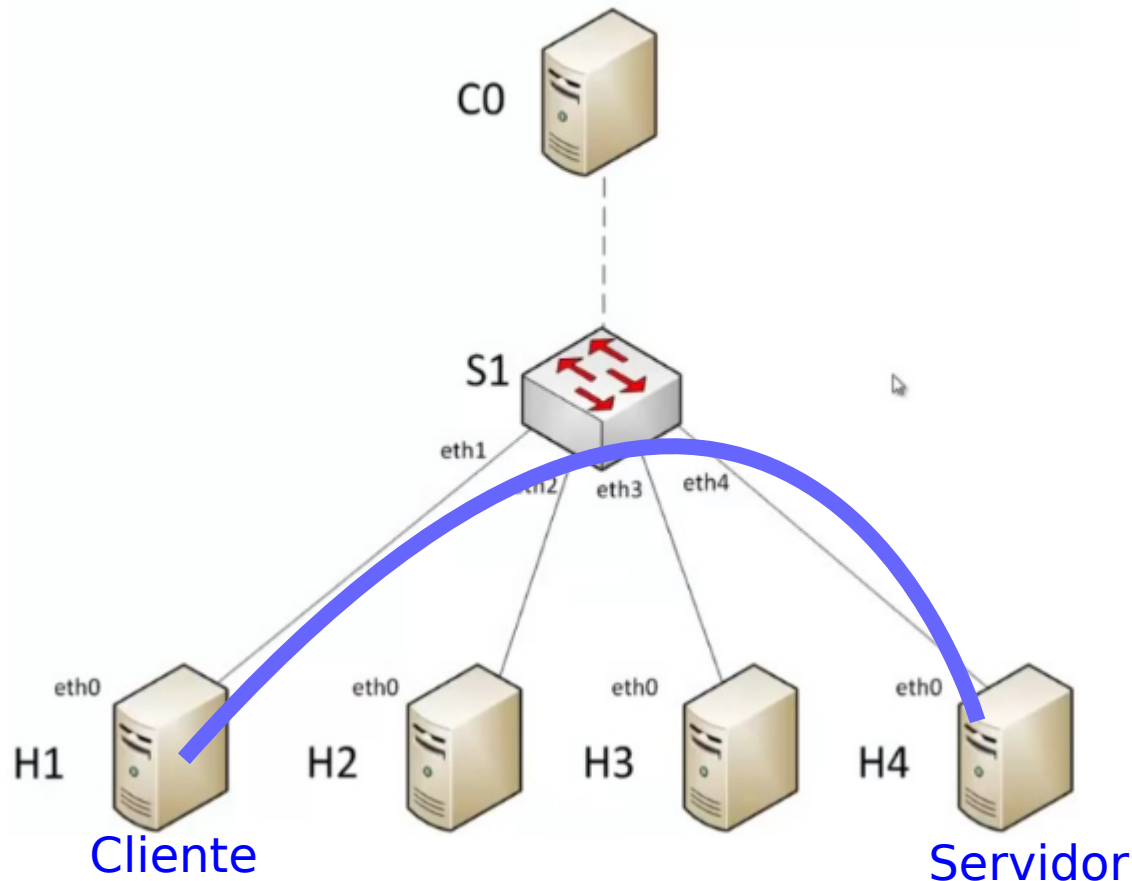


Controlador OpenFlow

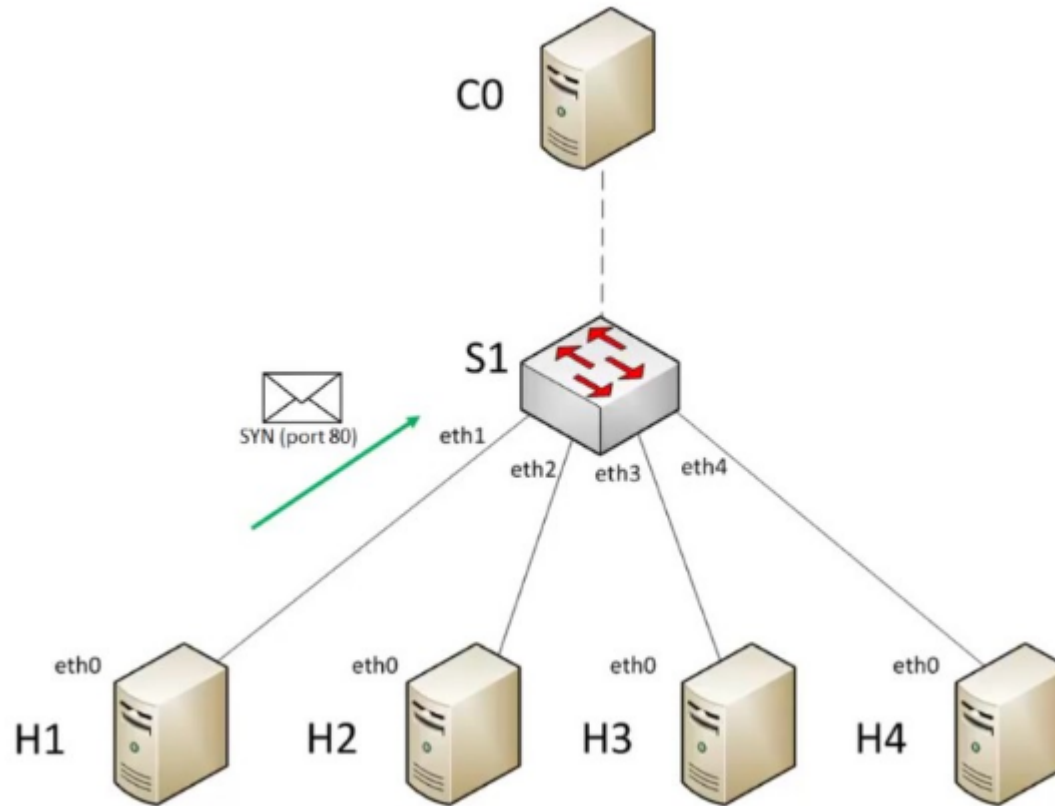


Exemplo com OpenFlow

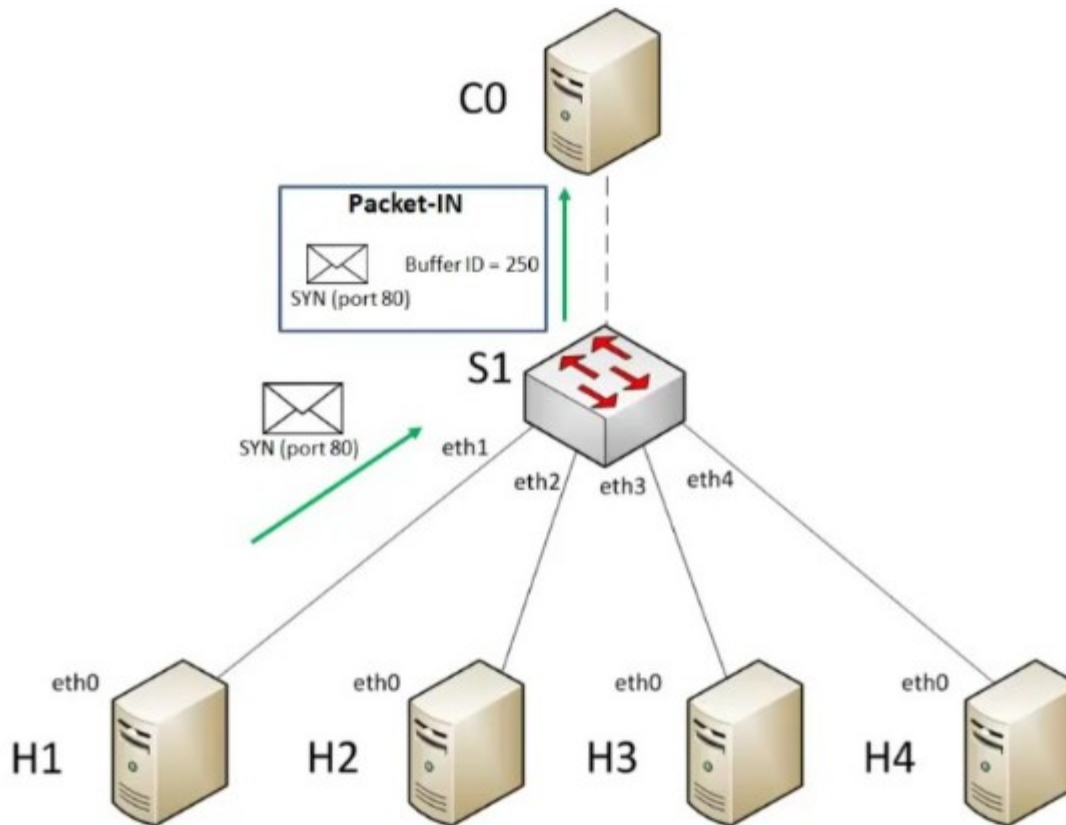
- ▶ Simulação de requisição HTTP em rede com OpenFlow (como funciona na rede legada?)



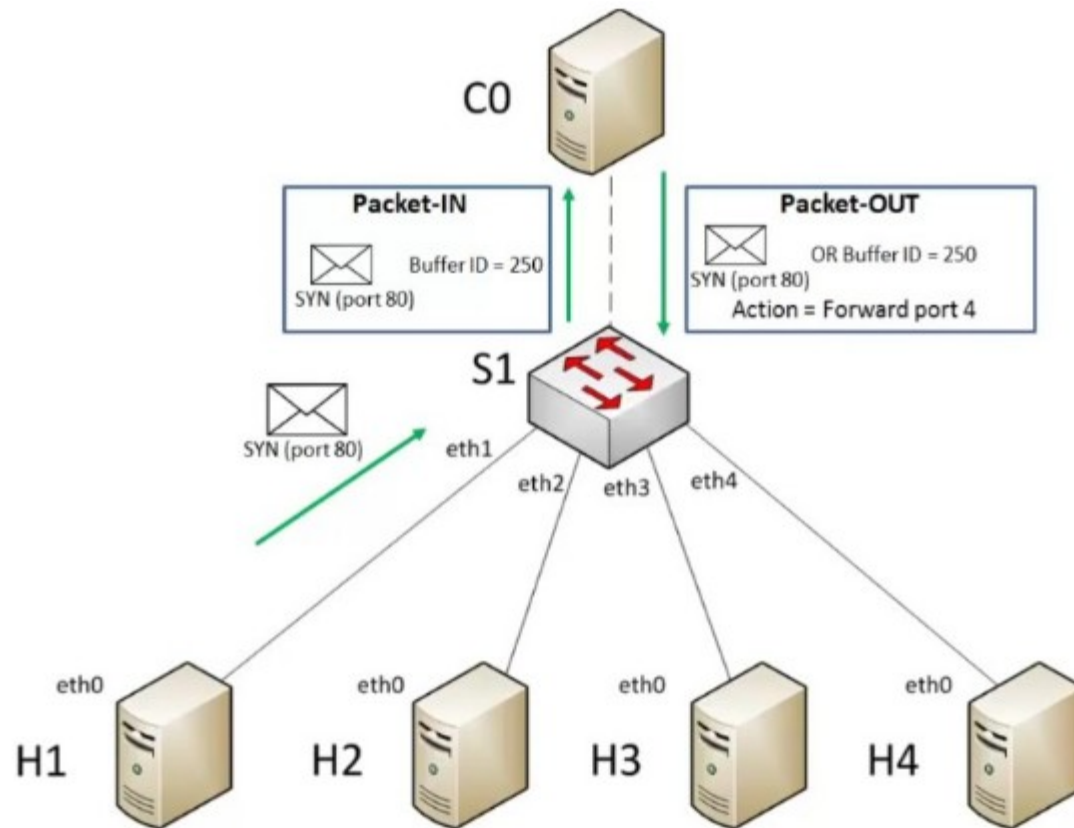
Exemplo com OpenFlow



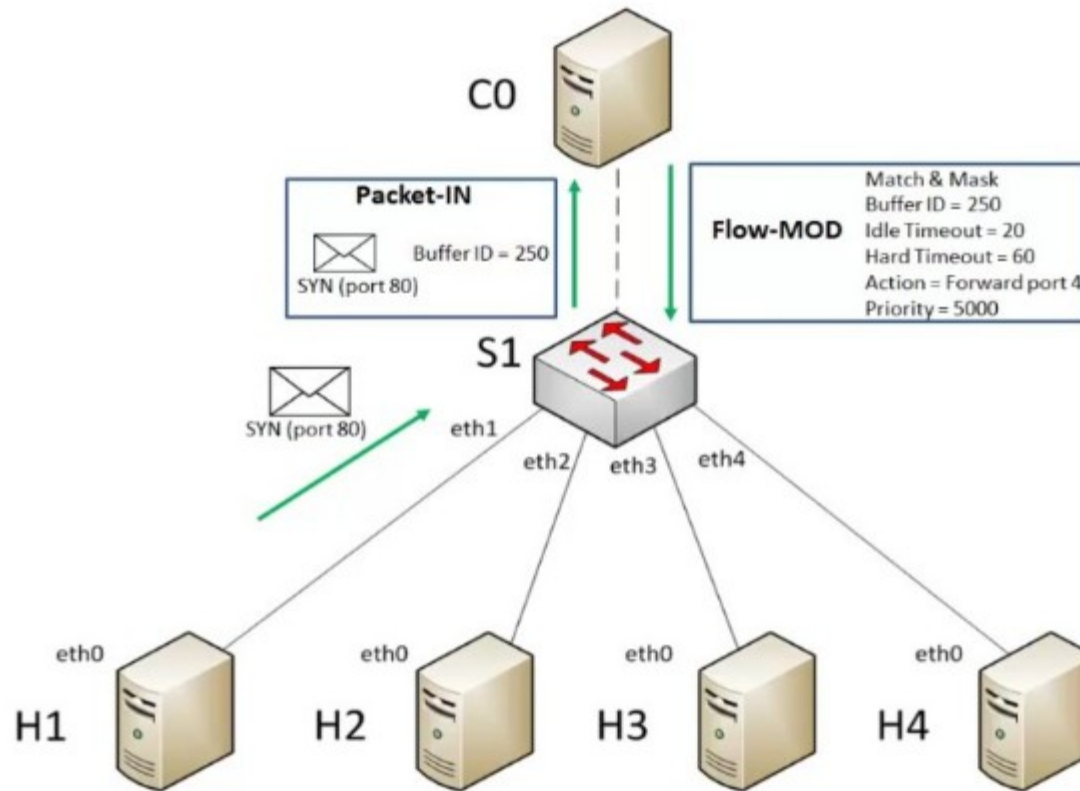
Exemplo com OpenFlow



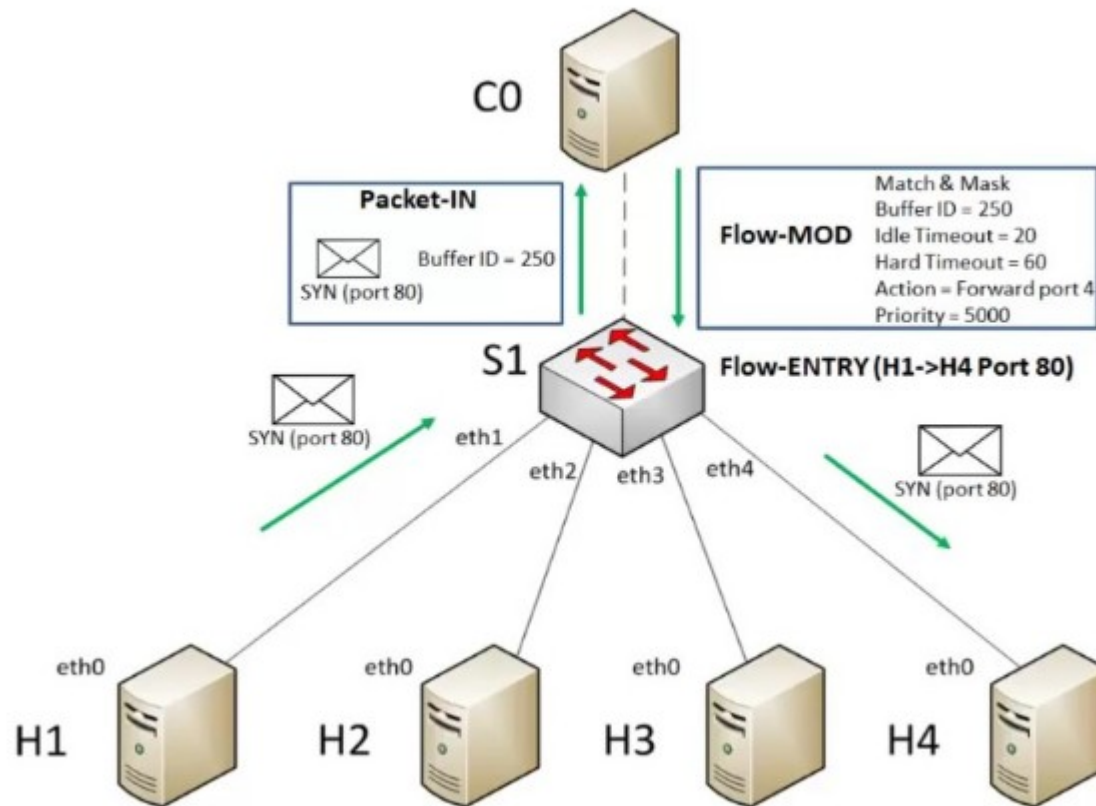
Exemplo com OpenFlow



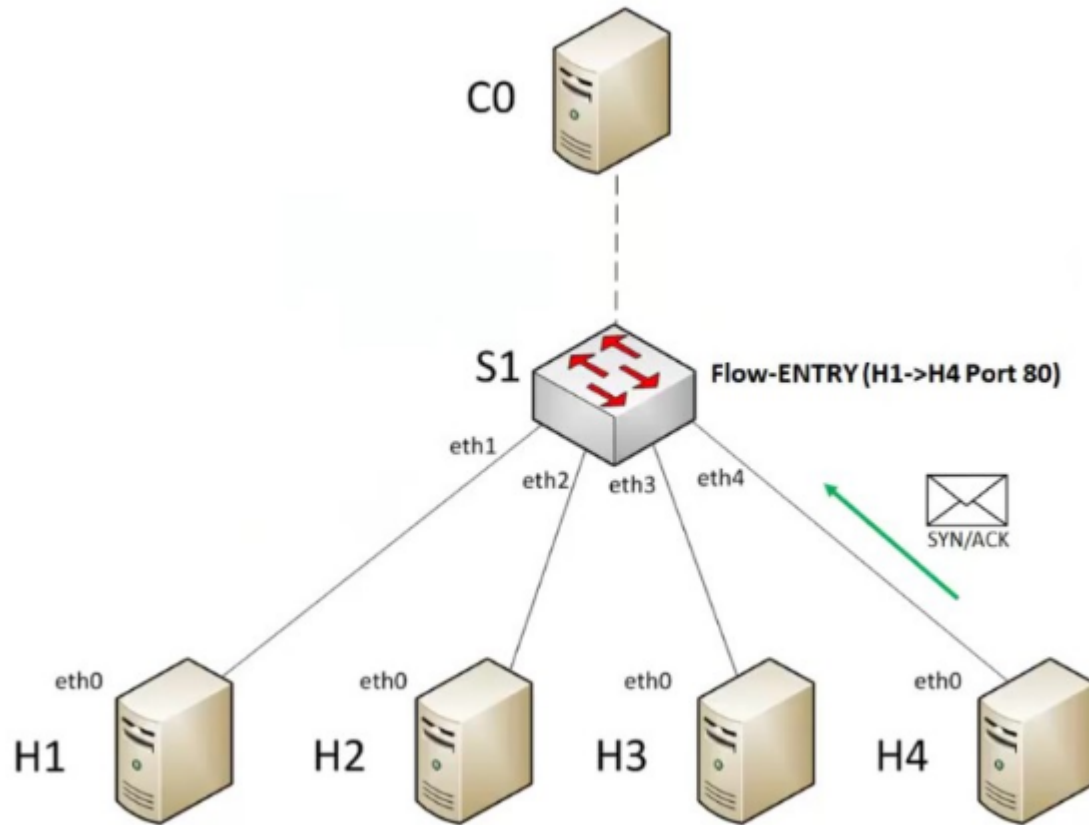
Exemplo com OpenFlow



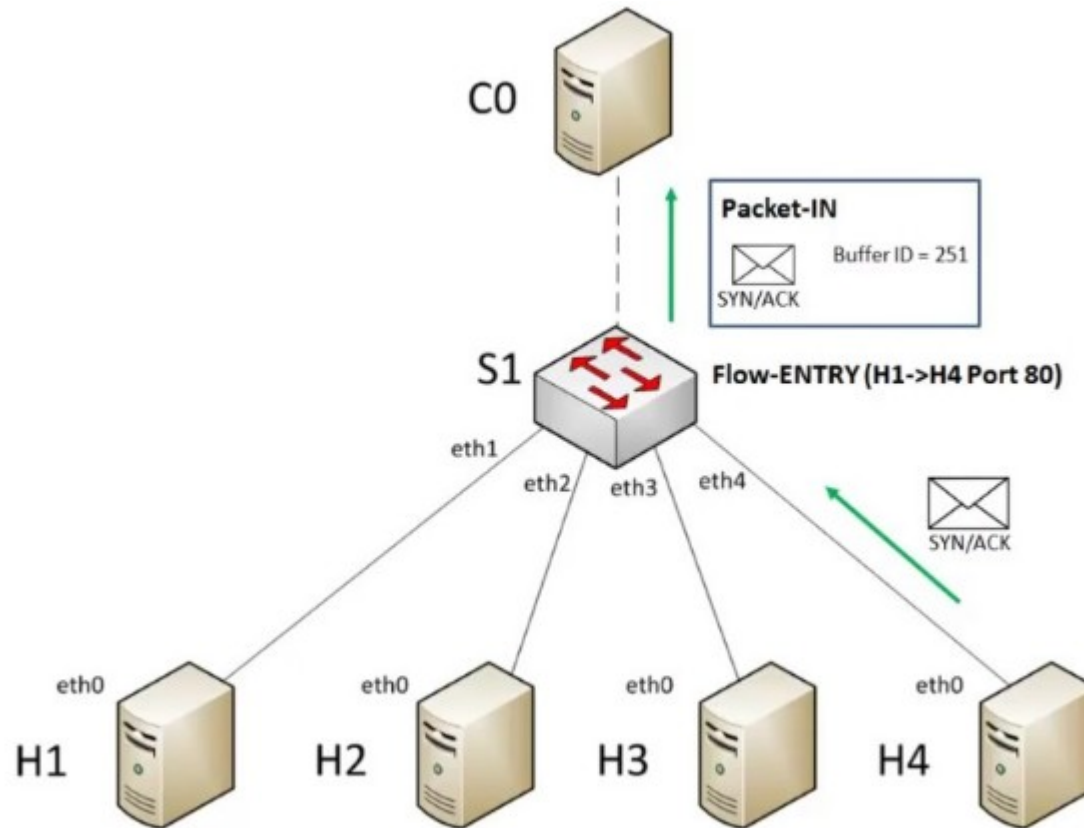
Exemplo com OpenFlow



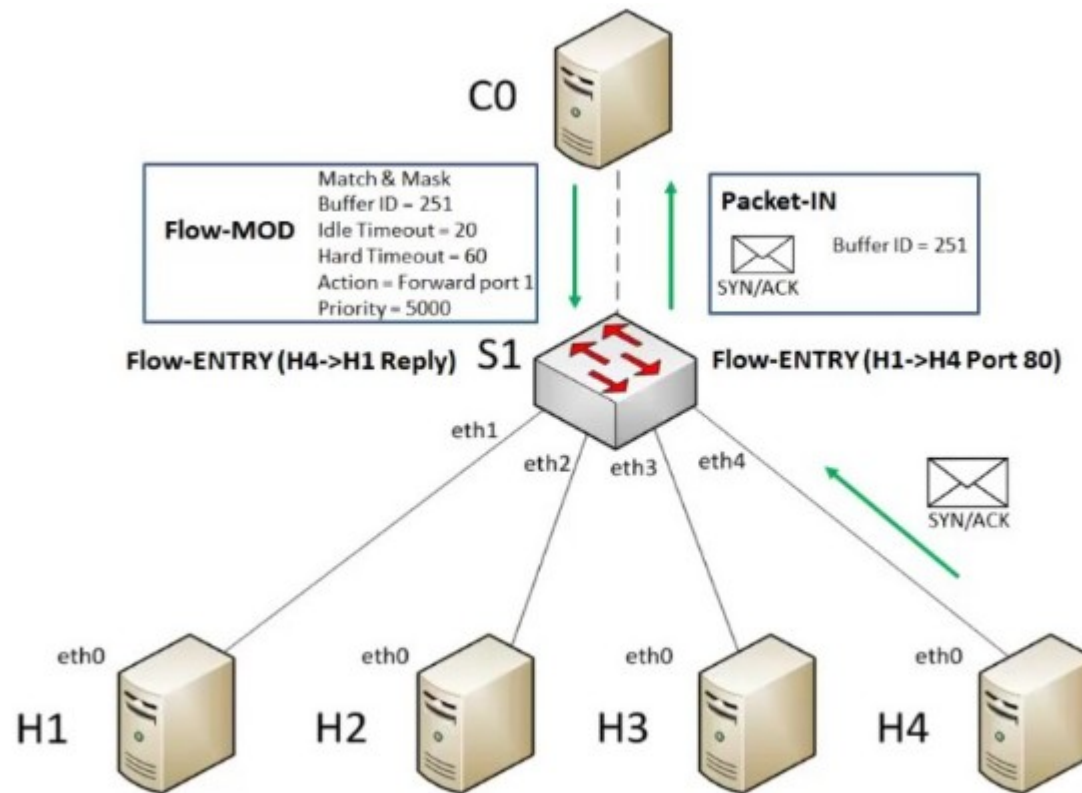
Exemplo com OpenFlow



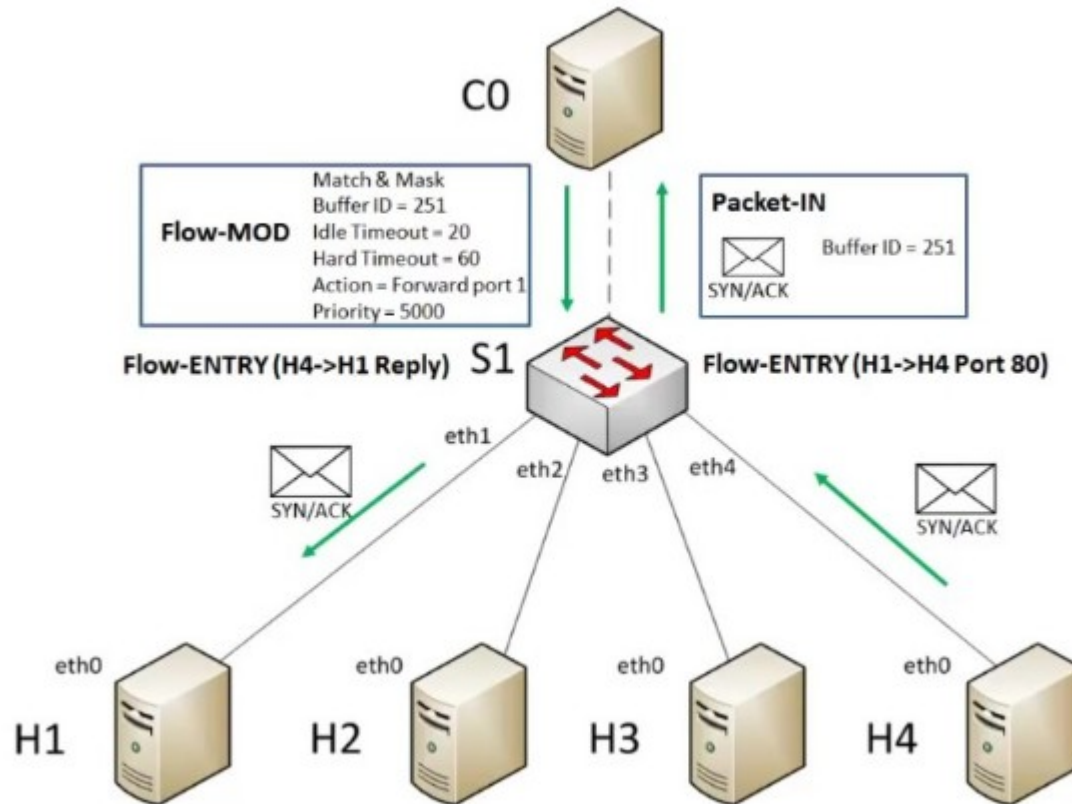
Exemplo com OpenFlow



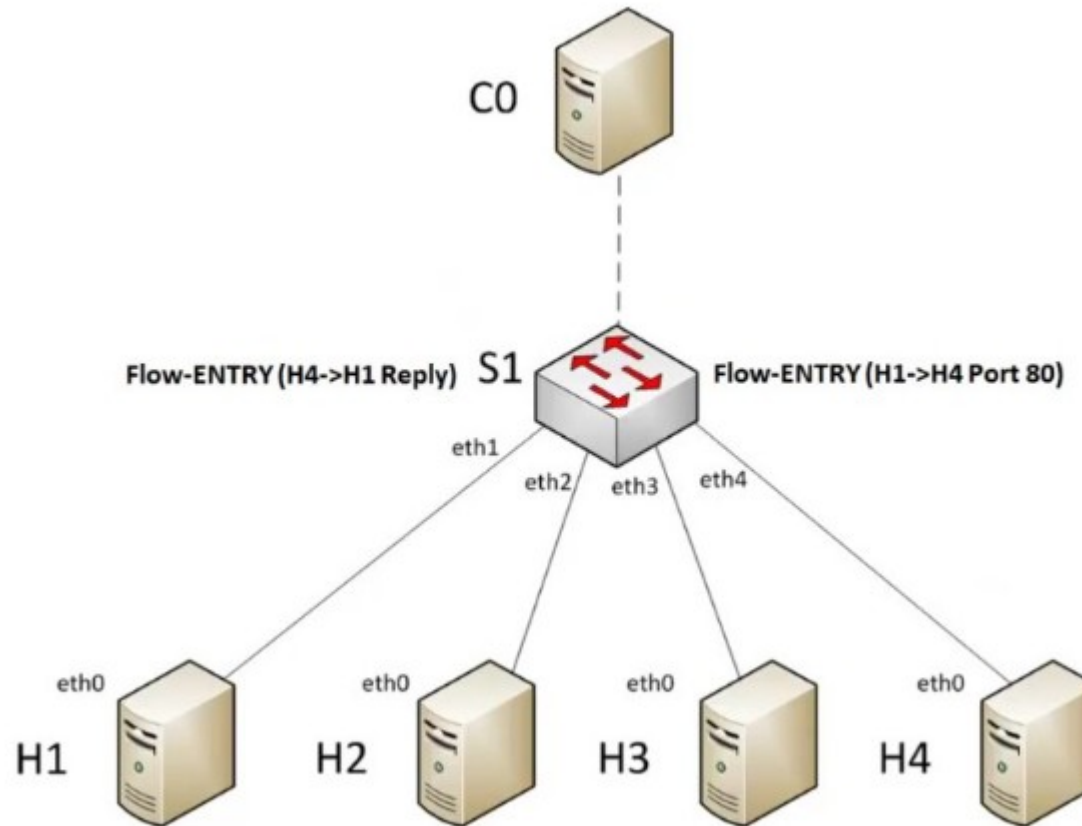
Exemplo com OpenFlow



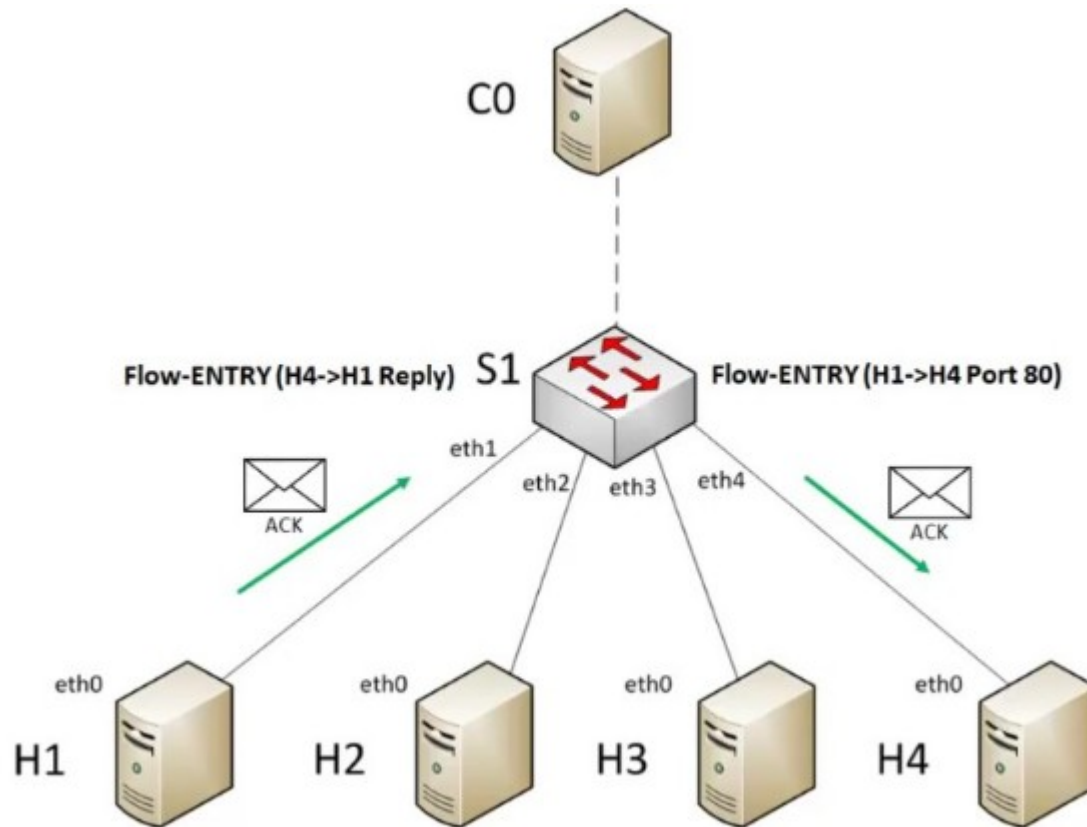
Exemplo com OpenFlow



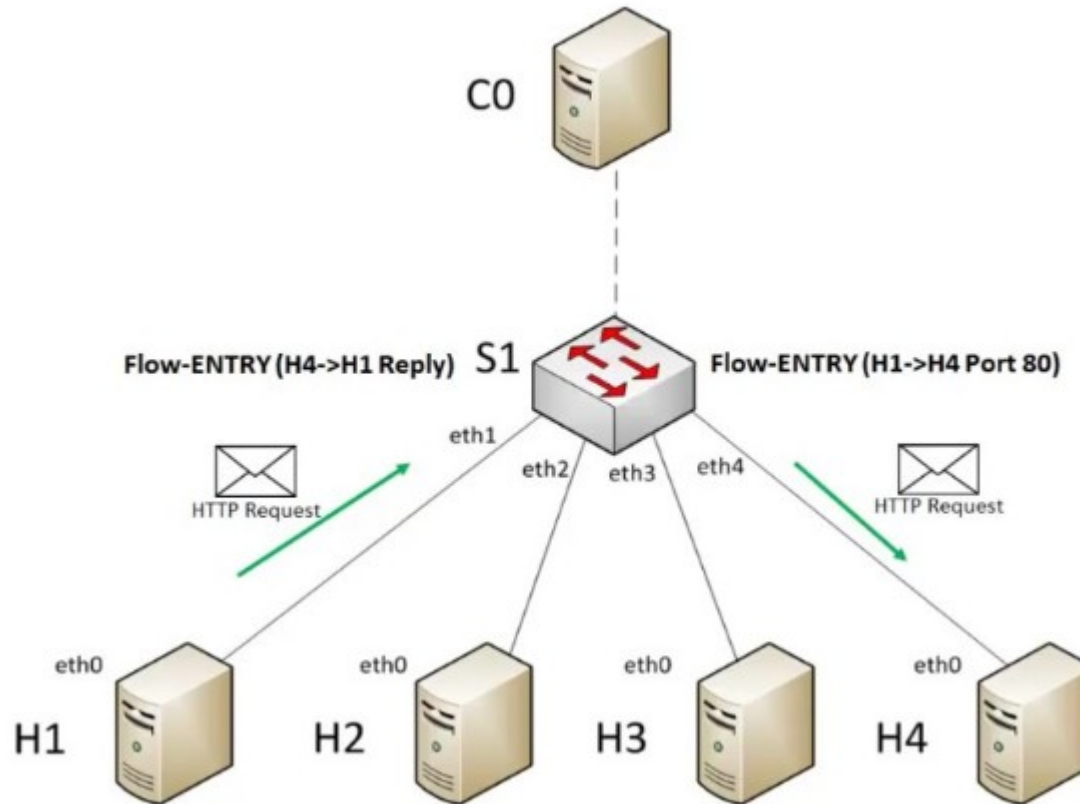
Exemplo com OpenFlow



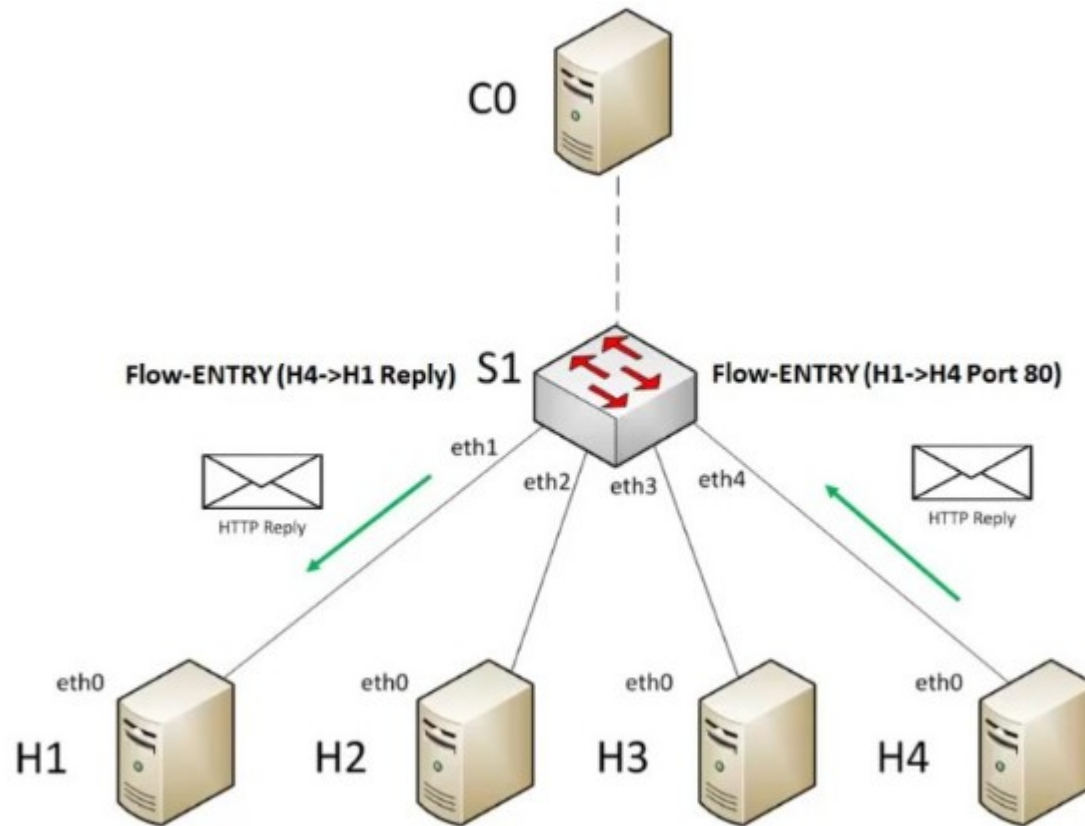
Exemplo com OpenFlow



Exemplo com OpenFlow



Exemplo com OpenFlow



Prática 01

- ▶ Captura de pacotes do protocolo openflow com wireshark e identificação de cada tipo de mensagem
 - No terminal:
 - ❑ sudo mn
 - No wireshark, fazer a captura no “Loopback” e colocar o filtro:
 - ❑ of
- ▶ Captura de requisição PING com OpenFlow

Open vSwitch



- ▶ Open vSwitch é um switch virtual *open source* tipicamente utilizando em ambientes de virtualização (locais e distribuídos)
- ▶ Também é utilizado em alguns equipamentos com hardware dedicado
- ▶ Muito utilizado em soluções SDN

Open vSwitch

- ▶ Visibilidade de comunicação inter-VM: NetFlow, sFlow(R), IPFIX, SPAN, RSPAN e mirrors baseados em túneis GRE
- ▶ LACP (IEEE 802.1AX-2008)
- ▶ Standard 802.1Q VLAN model with trunking
- ▶ BFD and 802.1ag link monitoring
- ▶ STP (IEEE 802.1D-1998)
- ▶ OpenFlow (1.0 ... 1.6)
- ▶ IPv6
- ▶ Multiple tunneling protocols (GRE, VXLAN, IPsec, GRE and VXLAN over IPsec)
- ▶ Remote configuration protocol with C and Python bindings
- ▶ Kernel and user-space forwarding engine

Utilitários OVS

- ▶ **ovs-ofctl** – utilitário de gerenciamento para openflow
- ▶ **ovs-dpctl** – utilitário de gerenciamento do Open vSwitch datapath
- ▶ **ovs-vsctl** – gerenciamento de switches virtuais com *ovsdb-server*

Utilitários OVS

ovs-vsctl show	Mostra informações sobre os switches virtuais
ovs-vsctl list Controller	Mostra informações da conexão OF do switch

Utilitários OVS

ovs-ofctl show SWITCH	Exibe informações do SWITCH
ovs-ofctl dump-flows SWITCH	Verifica a Flow Table do SWITCH
ovs-ofctl del-flows SWITCH	Limpa a Flow Table do SWITCH
ovs-ofctl add-flow SWITCH action=normal	Deixa o SWITCH operando em modo “normal” (L2)
ovs-ofctl mod-port SWITCH IFACE ACT	Realiza a ação ACT (up, down) na interface IFACE do SWITCH

Utilitários OVS

**ovs-ofctl add-flow SWITCH
priority=XXXX,in_port=YYY,
actions=output:Z**

Adiciona um fluxo no SWITCH, com prioridade XXXX, entrando pela porta YYY, e realizando a ação de sair pela porta Z

**ovs-ofctl add-flow SWITCH
dl_src=MAC1,dl_dst=MAC2,
actions=output:X**

Adiciona um fluxo no SWITCH, com origem o MAC1, com destino o MAC2, realizando a ação X

**ovs-ofctl add-flow SWITCH
priority=XXX,ip,nw_src=IP1,
nw_dst=IP2,actions=normal**

Adiciona um fluxo no SWITCH, com prioridade XXX, que seja do tipo IP, com o origem o IP1 e destino IP2, realizando a opção normal (L2).

Prática 2

- ▶ Criar uma topologia linear (3 switches) e configurar regras de encaminhamento baseado em L2. Iniciar o mininet com:
 - **sudo mn --topo linear,3 --mac --arp --controller none**
- ▶ Objetivo: pingall

Exercício

- ▶ Tarefa 1: Estudar sobre o mininet conforme Aula02_Mininet no Moodle e fazer exercícios propostos
- ▶ Tarefa 2: Fazer script python para criar topologias em anel com “n” switches/hosts (um host em cada switch). Utilizar comandos ovs-ofctl para criar o menor caminho entre cada nó; além de encaminhar o tráfego, modificar o MAC de destino para o MAC do próximo salto.