ReVir – Programabilidade em Redes Virtualizadas

UFRGS

Liane Maria Rockenbach Tarouco; Ricardo Luis dos Santos; Wanderson Paim de Jesus

UFPR

Elias P. Duarte Jr.; Gustavo Bassil Heimovski

UFRJ

Luci Pirmez; Renato Pinheiro de Souza

Agenda

- Introdução
- Virtualização de Redes
- Programabilidade de Redes - Propostas Históricas
  - Redes Ativas
  - Agentes Móveis
  - MIBs DISMAN
- Programabilidade de Redes - Propostas Atuais
  - IOS (CISCO)
  - JunOS (Juniper)
  - Click
  - OpenFlow
- Considerações Finais
- *Status* do Projeto

Introdução

- Internet
  - É um dos principais alicerces da sociedade atual
  - Popularização dos serviços de Internet
  - Facilidade para implementação, aliado ao baixo custo das tecnologias
- Serviços da Internet
  - Borda
    - O “valor” da Internet, para o usuário final, está principalmente nas bordas
    - Aplicações (DropBox, Skype, BitTorrent, Twitter)
  - Núcleo
    - Comunicação

Introdução

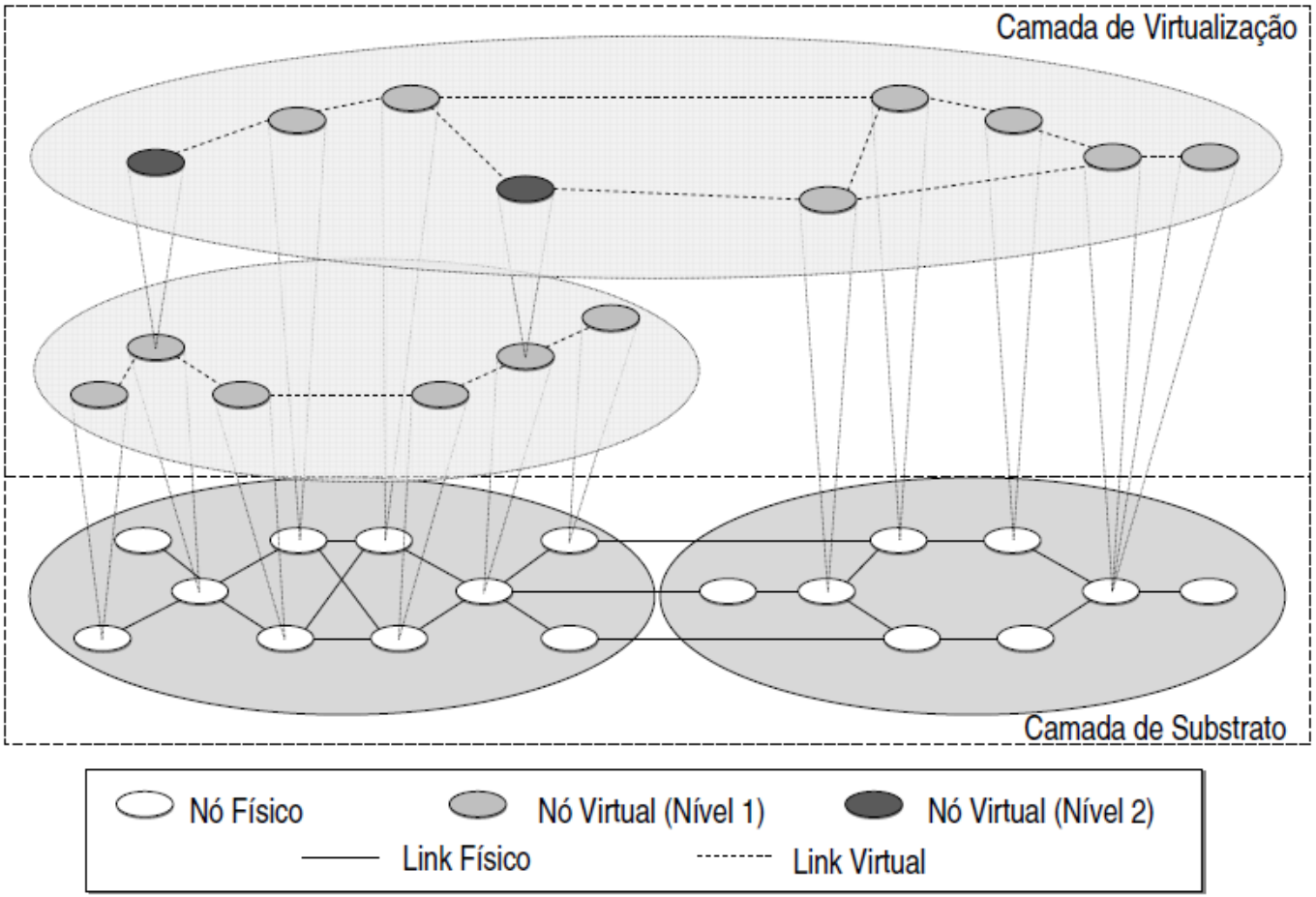
- Ossificação da Internet
- Programabilidade de Redes
  - Foi concebida como uma forma para desenvolver novos serviços
  - É definida como a capacidade de um dispositivo de rede (*e.g.*, um roteador) executar código no próprio dispositivo (LAZAR, 1997)
- Várias propostas que encontraram uma grande resistência, por parte dos administradores de rede
  - Impacto de possíveis erros na aplicação de novas soluções
  - Erros podem causar indisponibilidade de serviços importantes
  - Equipamentos e soluções proprietárias dificultam a implementação
  - Sem padronização

VIRTUALIZAÇÃO DE REDES

Virtualização de Redes

- A virtualização de redes é vislumbrada como uma alternativa para experimentar e implementar novas funcionalidades sobre a rede de produção
- Alguns dos principais benefícios da utilização da virtualização de redes
  - Isolamento
  - Flexibilidade e disponibilidade
  - Escalabilidade
  - Redução de custos
  - Segurança

Virtualização de Redes



Virtualização de Redes

- Soluções que permitem a virtualização de *hosts*
  - VMWare
  - VirtualBox
  - Xen
  - …
- Alguns exemplos de sistemas operacionais de dispositivos de rede que podem ser utilizados para virtualização de redes
  - Open vSwitch – OvS
  - Quagga
  - Vyatta
  - …

PROGRAMABILIDADE DE REDES

Propostas Históricas

Redes Ativas

- Redes Ativas
  - São caracterizadas pela possibilidade dos nós da rede realizarem alterações ou computações no conteúdo de um pacote
  - Propõe-se que dispositivos executem aplicações
  - Os *apps* podem ser enviados aos nós através da própria rede
  - Pacotes ativos precisam ser diferenciados dos pacotes comuns
- Abordagens
  - Nós ativos
  - Pacotes ativos
  - Híbridas

Propostas Históricas

Redes Ativas

- Algumas aplicações possíveis
  - Gerência de Redes
    - O monitoramento atual exige *pooling*
    - Com o crescimento das redes isso é um problema
    - Com Redes Ativas diversos centros de gerenciamento poderiam ser configurados, deslocando o ponto de decisão para perto do nó
  - Implementação de *cache* para beneficiar *multicasting*
- Limitações
  - Segurança
    - Quais códigos podem ser executados?
    - *Trade-off* entre flexibilidade e segurança
    - Dependendo da solução seriam necessárias constantes atualizações nos nodos

Propostas Históricas

Agentes Móveis

- Agentes Móveis
  - Agente trafega livremente entre os *hosts* da rede, decidindo seu destino e ações
  - Transfere tanto o código como o *status* anterior para o novo *host*, continuando sua execução de onde havia parado
  - *Hosts* devem estar preparados para executar os agentes móveis
- Benefícios
  - Propõem mover o algoritmo para perto dos dados e não o contrário
  - Menor latência
  - Execução assíncrona e autônoma
  - Tolerância a falhas

Propostas Históricas

Agentes Móveis

- Limitações
  - Exigem *hosts* compatíveis para execução dos agentes
  - Equipamentos heterogêneos espalhados pela Internet (diferentes capacidades de processamento e memória)
  - Segurança
    - Uma vez disparados os agentes móveis não dependem do dispositivo que os originou
    - Agente trafega livremente entre os *hosts* da rede, decidindo seu destino e ações
    - Como definir o que executar na rede?

Propostas Históricas

MIBs DISMAN

- DISMAN (*Distributed Management*)
  - RFC 3165 (Script MIB)
  - RFC 2981 (Event MIB)
  - RFC 2982 (Expression MIB)
  - RFC 4560 (Remote Operations MIB)
  - RFC 3231 (Schedule MIB)

Propostas Históricas

MIBs DISMAN

- *Script* MIB
  - Define um ambiente de execução que permite a criação de operações mais complexas codificadas em *scripts*
  - Além de permitir a manipulação dos *scripts* através de requisições SNMP, o ambiente de execução possibilita
    - A instalação de *scripts* nos nós da rede através de requisições SNMP
    - Escrita destes *scripts* em qualquer linguagem de programação, desde que esta seja suportada pelo ambiente de execução

Propostas Históricas

MIBs DISMAN

- Permite a delegação de *scripts* para gerentes distribuídos fornecendo os seguintes atributos
  - Transferência de scripts para locais distribuídos (*push* ou *pull*)
  - Gerenciamento dos *scripts* (inicialização, suspensão, reinicialização e finalização)
  - Passagem de parâmetros
  - Monitoramento e controle dos *scripts* que estão em execução
  - Transferência para o gerente dos resultados produzidos
- Limitações
  - Necessidade de liberar acesso de administrador para inserir códigos nos dispositivos
  - Escopo limitado ao Gerenciamento de Redes

Propostas Atuais

JunOS (Juniper)

- JunOS
  - Baseado em FreeBSD
  - Está dividido em 3 camadas: Plano de Controle, Dados e Serviço
    - **Plano de Controle:** Gerenciar e controlar o funcionamento do equipamento como um todo, incluindo os dois outros planos
    - **Plano de Dados** ou *Packet Forwarding Engine* (PFE)**:** *Hardware* dedicado com a função de encaminhar ou filtrar o tráfego de acordo com a tabela de roteamento
    - **Plano de Serviço:** Extensão opcional do Plano de Dados que executa funções não nativas no PFE
  - Cada plano é executado em módulos de *hardware* instaláveis nos equipamentos Juniper

Propostas Atuais

JunOS (Juniper)

- JunOS SDK
  - Funciona integrado ao Sistema Operacional de Rede JunOS
  - Provê APIs que permitem a incorporação de aplicações no JunOS
  - Uma vez implantados, as aplicações rodam nativamente nos equipamentos
  - Com o objetivo de evitar possíveis conflitos, a área de instalação dos módulos é controlada
    - São instalados em locais diferentes
    - Precisam de um ID fornecido pela Juniper extraído de um certificado assinado

Propostas Atuais

IOS (CISCO)

- IOS (*Internetwork Operating System*)
  - Utilizado nos equipamentos da CISCO
  - Sistema operacional multitarefas que integra soluções de:
    - Roteamento
    - *Switching*
    - Interligação de redes *(Internetworking)*
    - Telecomunicações

Propostas Atuais

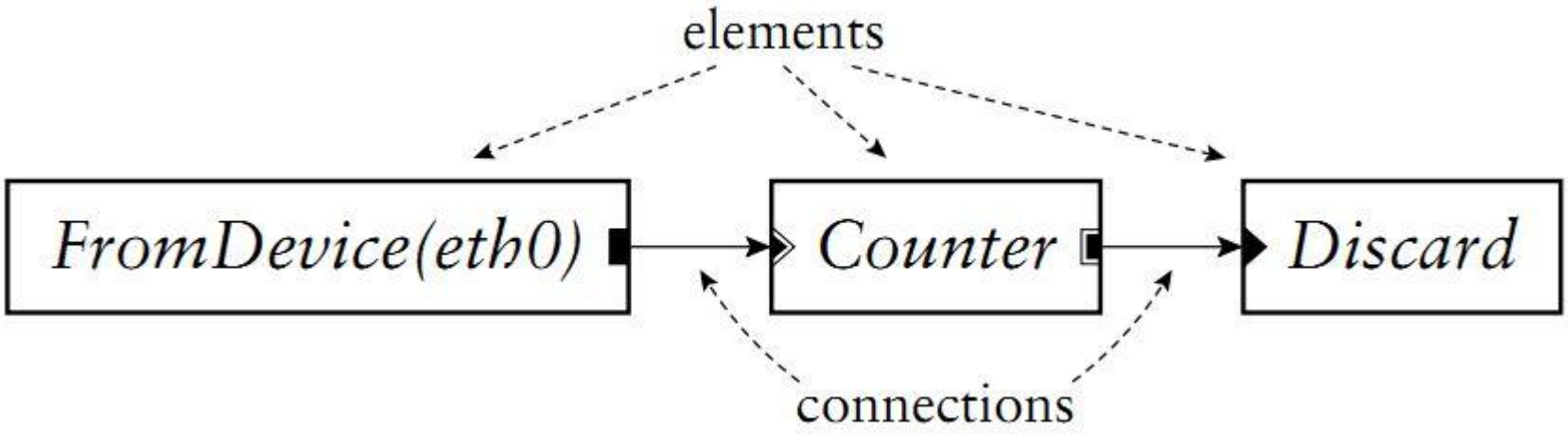
IOS (CISCO)

- Cisco AON (*Application-Oriented Networking*)
  - Atua na camada de aplicação
  - Permite alterações no conteúdo dos pacotes
  - Exige equipamento dedicado (CADE – *Cisco Application Deployment Engine*)
  - *Switches* ou roteadores redirecionam o tráfego para o equipamento AON de maneira transparente, o qual aplica as políticas definidas
- Aplicações
  - Pode atuar como *gateway* entre empresas parceiras, tratando autenticação e autorização de acesso
  - Pode assumir papel de IDS, criar *logs* de ataques
  - Controlar qualidade de serviço, atribuindo prioridades

Propostas Atuais

Click Modular Router

- Click Modular Router
  - Roteador baseado em *software* que implementa as funcionalidades de um roteador através de módulos
  - Os módulos podem ser escritos em C/C++
- Exemplo Contador de Pacotes



Propostas Atuais

Click Modular Router

- Modos de operações
  - *Kernel* (alto desempenho para um roteador baseado em *software*)
  - *UserLevel* (nível de aplicação)
  - Simulação (módulo do NS-2 NSClick)
- Novos elementos podem ser desenvolvidos ou baixados da biblioteca de elementos prontos no *site* do Click
- Ferramenta gratuita e de código aberto
- Limitações
  - Não suporta migração de código e estado de execução
  - Carece de mecanismos que garantam seu funcionamento em caso de falha na rede

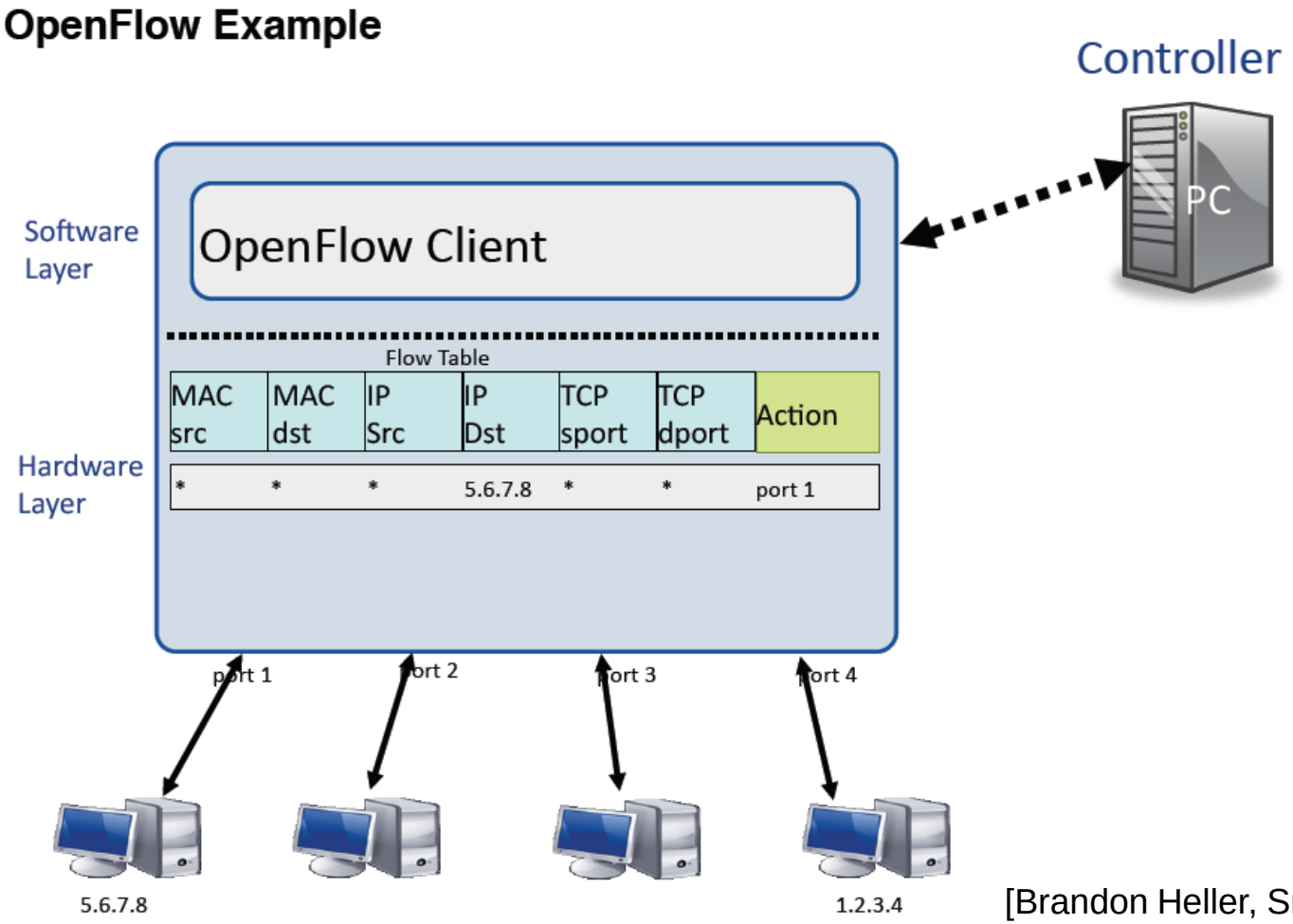
Propostas Atuais

Openflow

- OpenFlow
  - Utiliza tabelas de fluxo internas e uma interface padronizada para adicionar e remover fluxos
  - Exige que os dispositivos de rede tenham suporte à OpenFlow
  - Utiliza modelo em camadas
    - Camada de controle
    - Camada de dados
  - Componentes
    - OpenFlow Switch/Router
    - Controlador
    - Protocolo

Propostas Atuais

Openflow



[Brandon Heller, Srini Seetharaman]

Propostas Atuais

Openflow

- Vantagens
  - Visão geral da topologia de rede
  - Por ser uma solução livre, pode reduzir os custos finais dos equipamentos
  - Segurança
  - Aplicações podem ser desenvolvidas em Java, C/C++ e Python
- Limitações
  - O controlador é um ponto de falha centralizado
  - Não suporta processamento por pacotes, apenas por fluxos
  - Escalabilidade limitada, devido à exigência de equipamentos de rede com suporte à OpenFlow

Considerações Finais

- Propostas da comunidade científica
  - Recentemente, Agentes Móveis e OpenFlow têm sido foco de um grande número de pesquisas
  - As MIBs do DISMAN foram atualizadas diversas vezes ao longo da ultima década e muitos equipamentos oferecem suporte
  - A Script MIB permite a execução de *scripts* desenvolvidos em diferentes linguagens de programação, porém limita-se ao escopo do gerenciamento de redes
  - O OpenFlow possui a capacidade de separar os fluxos isolando as aplicações que compartilham os mesmos equipamentos
  - Porém, todas as tecnologias estudadas pecam na segurança, pois para executar os programas desenvolvidos nos dispositivos de rede, o administrador deverá fornecer acesso total aos equipamentos

Considerações Finais

- Tecnologias disponíveis no mercado
  - Por serem soluções proprietárias, tanto o Cisco IOS quanto o JunOS SDK, possuem diversas semelhanças
    - Possuem otimizações e funcionam perfeitamente nos *hardwares* que oferecem suporte
    - Exigem equipamentos de um fabricante específico
    - Custo tanto dos equipamentos, quanto do suporte é elevado
  - O JunOS SDK destaca-se por limitar o que cada aplicação pode realizar, bem como a maneira como estas afetam o tráfego
  - O Click peca pela falta de mecanismos que garantam seu funcionamento em caso de falha na rede, bem como em relação a segurança

Considerações Finais

- Tendências
  - OpenFlow
  - Apoio de diversas empresas
    - Google, IBM, Yahoo!, Juniper, CISCO, HP ... ONF (*Open Networking Foundation*)
  - Economia na compra de *software* de rede
  - *Testbeds* com suporte à OpenFlow: Ofelia, GENI
  - Ponto de falha central (controlador)
- Apesar de inserir "inteligência" nos dispositivos de rede, ainda são necessárias pesquisas para disponibilizar uma plataforma de rede programável pelo usuário final

Status do Projeto

- Atividades concluídas
  - Estudo Teórico sobre virtualização e programabilidade de redes
- Atividades em desenvolvimento
  - Projeto de uma plataforma para programabilidade em redes virtualizadas
- Próximas atividades
  - Avaliação do projeto da plataforma – uma avaliação do *design* da plataforma será realizada por operadores de rede afim de aprimorar o projeto
  - *Implementação* – de posse de um projeto preliminar consistente com a opinião dos operadores, na etapa de implementação serão criados protótipos de roteadores e *switches* programáveis

Status do Projeto

- Próximas atividades
  - *Implantação/piloto* – nesta etapa os protótipos desenvolvidos serão colocadas em um ambiente próximo ao ambiente de produção, de forma a analisar o comportamento da solução
  - *Avaliação* – a etapa de avaliação será de fato contínua e fornecerá resultados intermediários para que os desenvolvimentos nas etapas anteriores possam ser constantemente aprimorados

Status do Projeto

- Pesquisas Ativas
  - **Gustavo Bassil Heimovski (UFPR)**

    Utilizando Redes Programáveis oferecer suporte à Anycast
  - **Renato Pinheiro de Souza (UFRJ)**

    Análise da influência na rede, ocasionada pela separação dos planos de controle e de dados em redes com suporte à OpenFlow
  - **Ricardo Luis dos Santos (UFRGS)**

    Desenvolver uma solução para programabilidade que habilite o desenvolvimento de serviços e aplicações sobre a rede núcleo
  - **Wanderson Paim de Jesus (UFRGS)**

    Desenvolver uma solução que permita disponibilizar para o cliente uma infraestrutura de rede virtual baseada em suas especificações

ReVir
Programabilidade em Redes Virtualizadas

Perguntas?