BRENO MADURO MARCONDES PEREIRA

DESENVOLVIMENTO DE UMA APLICAÇÃO ALTERNATIVA AO PROTOCOLO PROPRIETÁRIO VTP PARA REDES SEM PADRONIZAÇÃO DE FORNECEDORES

INCONFIDENTES – MG
2016

BRENO MADURO MARCONDES PEREIRA

DESENVOLVIMENTO DE UMA APLICAÇÃO ALTERNATIVA AO PROTOCOLO PROPRIETÁRIO VTP PARA REDES SEM PADRONIZAÇÃO DE FORNECEDORES

Trabalho de Conclusão de Curso apresentado como pré-requisito de conclusão do curso de Graduação Tecnológica em Redes de Computadores no Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais – Campus Inconfidentes, para obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Kleber Marcelo da Silva Rezende

INCONFIDENTES-MG
2016

BRENO MADURO MARCONDES PEREIRA

DESENVOLVIMENTO DE UMA APLICAÇÃO ALTERNATIVA AO PROTOCOLO PROPRIETÁRIO VTP PARA REDES SEM PADRONIZAÇÃO DE FORNECEDORES

Data de aprovação:

27 de Outubro de 2016

Orientador: Prof. Kleber Marcelo da Silva Rezende
IFSULDEMINAS – Campus Inconfidentes

Prof. Vinícius Ferreira de Souza
IFSULDEMINAS – Campus Inconfidentes

Prof. Alessandro de Castro Borges
IFSULDEMINAS – Campus Inconfidentes

Instituto Federal de Educação, Ciência e Tecnologia
Sul de Minas Gerais
Campus Inconfidentes
Praça Tiradentes, 416 - Centro - CEP 37576-000
Telefone: (35) 3464-1200

Desenvolvimento de uma aplicação alternativa ao protocolo proprietário VTP para redes sem padronização de fornecedores

Breno M. M. Pereira[1], Kleber M. S. Rezende[1]

[1] Setor de Informática e Redes
IFSULDEMINAS – Campus Inconfidentes – Inconfidentes, MG – Brasil

breno.maduro@gmail.com, kleber.rezende@ifsuldeminas.edu.br

Abstract. *This paper presents the development of an application that reproduces part of the Cisco Systems protocol VTP (VLAN Trunk Protocol) for VLAN (Virtual LAN) management on networks without supplier standardization. With the growth of computer networks using together devices from different suppliers, the VLANs management can become complex and prone to faults, so that the proposed solution can turn the networks administrator's life easier. The application was developed in Shell Script, works on GNU/Linux systems and uses SNMP (Simple Network Management Protocol) as the foundation that provide compatibility with different network switch models. The application introduced capacity to reproduce the proposal functions and reduce the time of action of the network administrator, automating the management of VLANs.*

Resumo. *Este trabalho apresenta o desenvolvimento de uma aplicação que reproduz parte das funcionalidades do protocolo VTP (VLAN Trunk Protocol) da Cisco Systems para o gerenciamento de VLAN (Virtual LAN) em redes sem padronização de fornecedores. Com o crescimento de uma rede de computadores que utiliza equipamentos de marcas diversas, o gerenciamento de VLANs pode se tornar complexo e propenso a falhas, de forma que a solução proposta pode facilitar a vida de um administrador de rede. A aplicação foi desenvolvida em Shell Script, opera em sistemas GNU/Linux e o protocolo SNMP (Simple Network Management Protocol) é a base que proporciona a compatibilidade com diversos modelos de switches. A aplicação apresentou grande capacidade de reproduzir as funções propostas e reduziu o tempo de ação do administrador na rede, automatizando o gerenciamento de VLANs.*

1. Introdução

As VLANS (Virtual LANs) são mecanismos utilizados em redes de computadores com o objetivo de garantir maior desempenho, segurança e organização. Elas definem redes virtuais, segmentando a rede em diferentes domínios de difusão, com isso, oferecendo maior segurança e robustez.

A administração de VLANS em redes de computadores, mesmo que pequenas, pode ser um trabalho bastante complexo ao se considerar a quantidade de componentes envolvidos. O gerenciamento de VLANs, ao passo que a rede cresce, torna-se complicado e custoso, sendo indispensável otimizar o que for possível. Soluções como o VTP (VLAN Trunk Protocol) da Cisco Systems facilitam esse trabalho, mas por se tratar de um protocolo proprietário, esses benefícios não se aplicam em redes com equipamentos de múltiplos fornecedores (CISCO, 2008).

A Cisco Systems fornece em suas soluções o VTP que se trata de um protocolo que estabelece uma relação hierárquica entre switches que compõem uma LAN, permitindo a definição de um deles como servidor de domínio e os demais como clientes. Quando se configura uma nova VLAN em um servidor VTP, ela é distribuída por todos os switches no domínio, reduzindo a necessidade de se configurar a mesma VLAN nos switches clientes (CISCO, 2008). O VTP utiliza em seus mecanismos, Quadros de Resumo, onde as informações de atualização das VLANs são enviadas aos switches clientes na rede, na Figura 01, o formato do quadro é exibido.

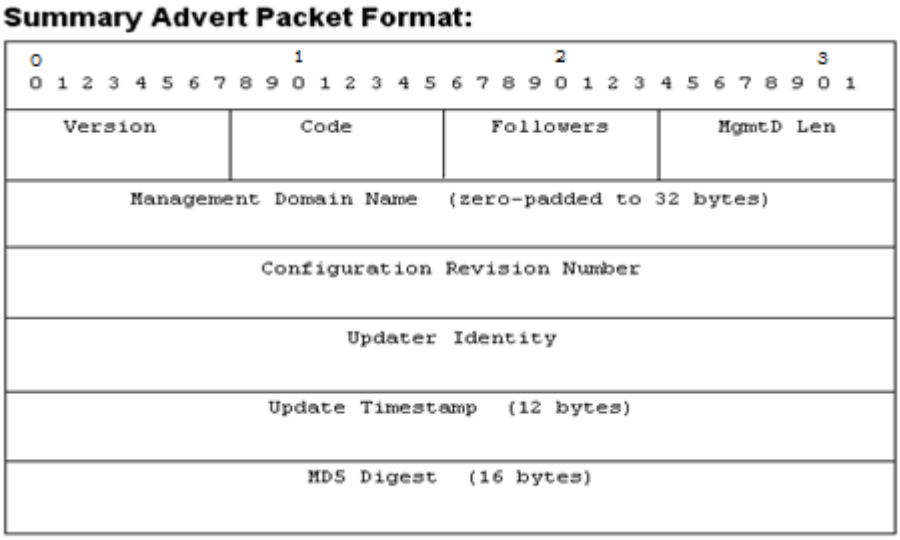

Figura 01. Formato do quadro de anúncio de resumo VTP. Fonte: CISCO 2009.

Ainda que o VTP proporcione facilidades no gerenciamento de redes com equipamentos Cisco, esse protocolo é proprietário e não entrega os mesmos benefícios para redes compostas por equipamentos de marcas diferentes. Mesmo que algumas etapas da configuração de uma rede ainda precisem ser executadas manualmente, a

automatização do gerenciamento de VLANs, como proporcionado pelo VTP, contribui para a otimização do tempo dos administradores.

A aplicação alvo deste trabalho destina-se a proporcionar otimização no gerenciamento de VLANs. Por ser escrita em Shell Script, a aplicação funciona em qualquer distribuição GNU/Linux. Para proporcionar compatibilidade com switches de diversas marcas e modelos, a solução proposta utiliza o protocolo SNMP (*Simple Network Management Protocol*) como mecanismo principal de interação com os switches, mas deve-se notar que não há limitações para utilização de outras formas de interação, como acesso à CLI (Command Line Interface) do equipamento através de SSH (Secure Shell) ou TELNET.

O gerenciamento da rede através do SNMP permite o acompanhamento simples e fácil do estado, em tempo real, da rede, podendo ser utilizado para gerenciar diferentes tipos de sistemas.

O SNMP é um protocolo de gerência definido no nível de aplicação, é utilizado para obter informações de servidores SNMP - agentes espalhados em uma rede baseada na pilha de protocolos TCP/IP. Os dados são obtidos através de requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte UDP (User Datagram Protocol) para enviar e receber suas mensagens através da rede.

Diante do exposto, o presente trabalho buscou desenvolver uma solução que automatize parte do gerenciamento de VLANs em redes com equipamentos de diferentes marcas, baseando-se no protocolo SNMP, amplamente adotado em equipamentos de rede, e em Shell Script, uma linguagem de programação aberta e com interpretador incluído na maioria das distribuições GNU/Linux.

O objetivo do trabalho foi desenvolver uma aplicação com, no mínimo, as funcionalidades a seguir:

- Detecção das ações do administrador da rede de criação, alteração ou remoção de VLANs no switch servidor;
- Replicação automática dessas ações nos demais switches da LAN;
- Funcionamento uniforme independente de fabricante;
- Interação do usuário através de CLI (Command Line Interface);
- Suporte a execução de tarefas agendadas (com utilitário CRON do Linux).

A arquitetura da solução abrange o servidor da aplicação, o switch servidor e os switches clientes. A aplicação funciona como um orquestrador, monitorando constantemente o switch modelo para identificar eventos de modificação das VLANs para replicar nos switches clientes configurados. Eventos de criação e exclusão de VLANs, assim que identificados, são reproduzidos para os demais switches, desobrigando o administrador da rede de executar essa ação manualmente.

2. Material e métodos

Considerando a inviabilidade de se utilizar equipamentos reais para o desenvolvimento do trabalho proposto, optou-se por emular os equipamentos necessários através da solução GNS3 (*Graphical Network Simulator 3*), que emula os mais diversos equipamentos de redes, roteadores, switches, PC's e firewalls, de diversos fabricantes.

O simulador GNS3 oferece um método fácil para arquitetar e construir redes de qualquer tamanho, sem a necessidade de equipamentos físicos (GNS3, 2016). A tela inicial do simulador é exibida na Figura 02.

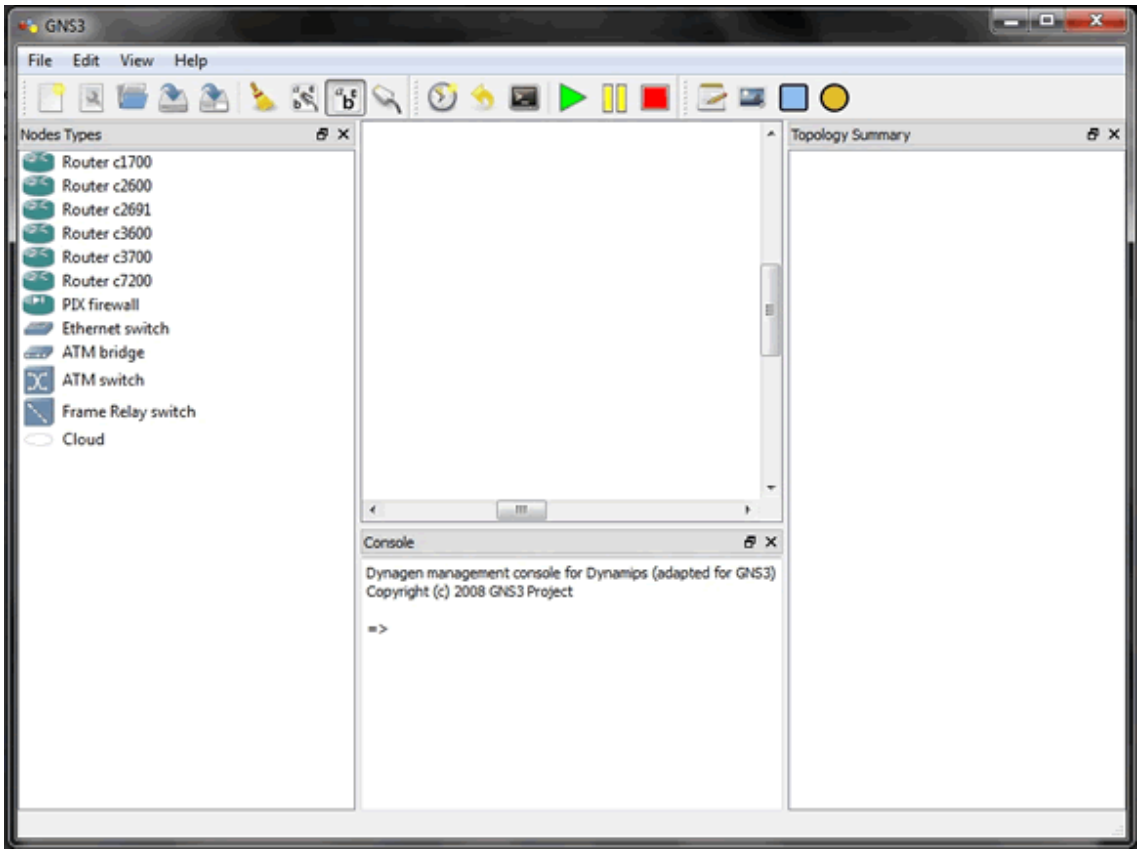

Figura 02. Tela inicial do software GNS3. Fonte: GNS3 2016.

Dada à natureza do trabalho, a utilização de componentes livres e gratuitos foi considerada prioridade. Além de proporcionar a continuidade do trabalho sem novos investimentos, essa abordagem permitiu o desenvolvimento sem a geração de custos e uma manutenção mais sustentável. Para o desenvolvimento da aplicação foi utilizada a distribuição Ubuntu, que se baseia na distribuição Debian e utiliza o núcleo Linux. O Ubuntu apresenta-se como uma das distribuições Linux que mais se desenvolveu nos últimos anos e oferece boa estabilidade. (COSTA, 2009)

A Figura 04 apresenta o cenário utilizado para o desenvolvimento e testes da aplicação. Observa-se que o computador com Ubuntu na versão 14.04 conecta-se diretamente à rede na qual estão hospedados os switches. Em cenários mais complexos, o computador pode não estar na mesma rede dos switches, dependendo de roteamento

de camada 3 para alcançá-los, onde roteadores teriam papel fundamental como gateway das diferentes sub-redes, realizando o encaminhando de pacotes entre elas, buscando na tabela de rotas o destino a ser enviado. Outro formato aceitável seria utilizar uma VLAN específica para conectar o servidor da aplicação aos equipamentos gerenciados. Uma vez que essas variáveis não afetam o desenvolvimento da aplicação, um cenário mais simples foi utilizado.

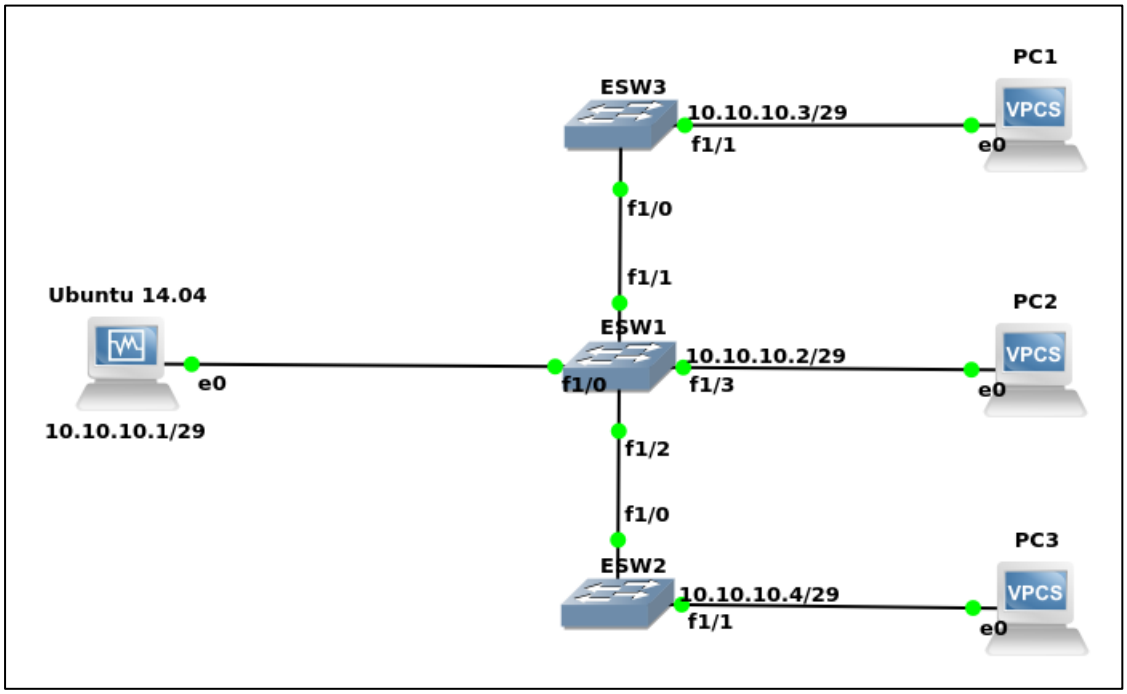

Figura 03. Topologia de rede virtual emulada pelo software GNS3. Fonte: Autores 2016.

Durante a operação, a aplicação se conecta ao switch servidor 24 vezes ao dia, num intervalo de uma hora pré-definido. Esse agendamento se dá através da ferramenta CRON, também incluída em todas as distribuições GNU/Linux. Durante a conexão, é verificada a existência de novas VLANs através da leitura da base de informações de gerenciamento (MIB) do switch servidor ou switch modelo. Essa base é um banco de dados hierárquico onde cada entrada é endereçada através de um identificador de objeto. A Figura 04 representa a hierarquia da MIB.

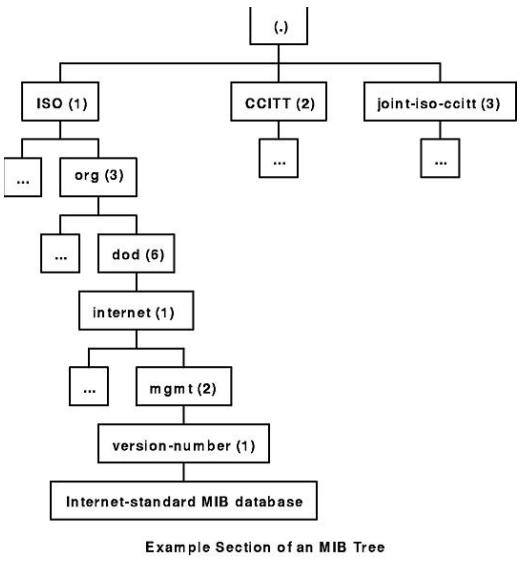

Figura 04. Estrutura hierárquica da MIB. Fonte: SourceDaddy 2013.

A MIB Q-BRIDGE-MIB é um banco de dados hierárquico contendo informações de gerência de VLAN, que são definidas seguindo a RFC 4363 (LEVI, 2016). Esta MIB armazena as informações de nome, estado e ID, sobre as VLANS dos equipamentos de rede que possuam suporte ao padrão 802.1Q. Com essas informações é possível fazer a verificação da existência ou não das VLANs no switch servidor e transferir para os switches clientes da topologia, caso seja necessário.

É realizada também uma comparação das informações existentes no switch servidor com as informações nos switches clientes, onde as VLANs não utilizadas no switch servidor são imediatamente excluídas nos demais switches clientes da rede, obedecendo aos comandos SNMP enviados pelo controlador.

Com o desenvolvimento da topologia de testes apresentada na Figura 01, o switch denominado “ESW1” foi selecionado para executar a função de switch servidor. Quando o administrador da rede realiza uma alteração nas VLANs desse switch, o script instalado no servidor com a distribuição Ubuntu é capaz de detectar, por meio dos comandos SNMP de consulta, esta alteração, seja ela de criação, exclusão ou modificação e armazená-la em variáveis. A partir da detecção, a aplicação replica as alterações nos demais switches por meio das chamadas de escrita do protocolo SNMP.

Os switches da rede são vinculados a uma comunidade SNMP e possuem endereços IP conforme mostrado na Figura 01, já que a comunicação via SNMP exige esses parâmetros. A partir de uma base de dados, a aplicação verifica se uma série de estruturas de condições são satisfeitas, com o objetivo de determinar se as modificações nos switches serão realizadas ou não. Deve-se observar que esta aplicação não é um protocolo, mas sim um script que reproduz algumas funcionalidades do VTP.

As estruturas de condição possuem papel fundamental na aplicação, pois são elas quem automatizam as operações, determinando se as alterações serão feitas ou não, por meio dos comandos de estrutura de repetição e condição da linguagem Shell script.

3. Resultados e discussões

No ambiente virtual emulado a aplicação entregou os resultados esperados, de forma que as funções de detecção de criação, alteração, remoção e replicação foram executadas com sucesso.

O algoritmo abaixo mostra a etapa de detecção da criação e replicação das VLANs do switch modelo para os seus pares na topologia de testes. Utilizando a faixa de IP da sub-rede definida no projeto e a comunidade SNMP “private”.

```
for (( i=1; i<=4096; i++ ))

do

      csVlanState=$(snmpget –Oqv –v 2c –c private 10.10.10.2 VlanState.1.$i)

      csVlanName=$( snmpget –Oqv –v 2c –c private 10.10.10.2 VlanName.1.$i)

      csVlanId=$( snmpget –Oqv –v 2c –c private 10.10.10.2 VlanDot10Said.1.$i)

       if [[ $csVlanState == “operational” ]] && [[ $sVlanState != “operational” ]]; then

       when read ip

              do

                     sVlanState=$(snmpget –Oqv –v 2c –c private $ip VlanState.1.$1)

              done < ip.txt

        while read ip

              do

                     snmpset –v 2c private $ip VlanEditOperation.1 i 2

                     snmpset –v 2c private $ip VlanEditRowStatus.1.$i i 4
VlanEditType.1.$ i 1 VlanEditName.1.$i s “$csVlanName” VlanEditDot10Said.1.$i x
‘echo ${csVlanId:1:11} | tr –d [:blank:]’ VlanEditOperation.1 i 3

                    snmpset –v 2c private $ip VlanEditOperation.1 i 4

             done < ip.txt

done
```

Diferente do VTP, a aplicação não adota o conceito de domínios para segmentar redes, porém utiliza a divisão de endereços IP para este fim. O controlador possui classes de IP diferentes para cada grupo de switches.

No ambiente virtual de testes, o script foi capaz de reproduzir as funções propostas e minimizar o tempo de ação do administrador da rede, pois a configuração de

VLAN dos switches clientes “ESW2” e “ESW3” foram efetuadas de forma automática, sem intervenção do administrador.

Na versão atual, a aplicação executa uma parte do trabalho de um administrador de rede no gerenciamento de VLANs. Após a criação das VLANs, o administrador deve ainda identificar em quais portas aquelas VLANs serão utilizadas. Em futuras versões, a aplicação pode automatizar também parte dessa tarefa, identificando quais os switches adjacentes e configurando as VLANs utilizadas nos links entre eles automaticamente.

4. Conclusões

A aplicação resultado do trabalho atendeu aos requisitos definidos, apresentando resultados satisfatórios no ambiente emulado. A adoção de tecnologias livres em sua concepção viabiliza inclusive que outros formatos de acesso, como interação com a CLI do equipamento através de SSH (Secure Shell) ou TELNET, sejam adotados no futuro.

Deve-se observar que para a utilização da aplicação faz-se necessário executar a configuração inicial dos switches a serem utilizados, incluindo as configurações do SNMP e as configurações de endereçamento IP. Mesmo que essa etapa exija um trabalho manual e individual nos equipamentos, ela viabiliza o uso da aplicação para gerenciamento de VLANs, economizando potencialmente o tempo do administrador da rede no futuro.

Para trabalhos futuros, destaca-se a oportunidade de desenvolvimento de uma nova funcionalidade que permita automatizar a vinculação de portas a uma VLAN, criação de portas tronco entre as interfaces dos switches e testes em dispositivos de outros fabricantes.

Considerando que a aplicação é executada num intervalo pré-definido, para determinados cenários, o tempo de resposta para consolidação das configurações pode ser insatisfatório. Assim, registra-se a oportunidade de configurar gatilhos que serão acionados quando alguma alteração for feita no switch servidor. Para tal, o emprego do recurso de traps (armadilhas) do SNMP apresenta-se como oportunidade de estudo para expansão da aplicação.

A aplicação apresentou resultados satisfatórios, além de um amplo campo de oportunidades de expansão para trabalhos futuros, de forma que novas versões podem otimizar ainda mais o trabalho de administradores de redes sem padronização de fornecedores.

5. Referências

CISCO. **Compreendendo o VLAN Trunk Protocol (VTP).** 2008. Disponível em: <http://www.cisco.com/cisco/web/support/BR/8/83/83259_21.html>. Acesso em: 18 maio 2016.

COSTA, E. **O Ubuntu abraça a nuvem**. Info Exame. 286: 12(2009) 75

GNS3. **What is GNS3?** 2016. Disponível em: < https://www.gns3.com/software>. Acesso em: 30 maio 2016.

LEVI, David et al. **Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions**. RFC 4363. 2006. Disponível em: <https://tools.ietf.org/html/rfc4363>. Acesso em: 26 maio 2016.

SOURCEDADDY. **Management Information Base.** 2013. Disponível em: < http://sourcedaddy.com/networking/management-information-base.html>. Acesso em: 20 Outubro 2016.