

O livro do GNS3

Build Virtual

Usando o Network Labs

Cisco, Juniper e mais

Prefácio

Redes estão por toda parte. Eles conectam todos os tipos de negócios, de livrarias locais a grandes corporações e universidades, em várias cidades e continentes. As redes são conceitualmente simples de entender, mas estão se tornando cada vez mais complexas, com inovação em áreas como Redes Definidas por Software (SDN), Internet das Coisas (IoT) e outras tecnologias ao virar da esquina.

Para entender, projetar e gerenciar as redes complexas de hoje, os profissionais de rede devem não apenas dominar a teoria, mas também praticar e validar conceitos nesses ambientes em constante mudança. É aí que entra o GNS3: oferece aos usuários uma imensa flexibilidade para criar seus próprios laboratórios de rede, permitindo que eles experimentem novos recursos de rede, capturem pacotes para dissecar protocolos e verifiquem configurações para implantação posterior em dispositivos reais. Tudo isso é feito sem a necessidade de investir em hardware caro.

O GNS3 é uma ferramenta poderosa e adaptável, evoluindo para agora integrar vários fornecedores e interagindo para atender às crescentes necessidades dos profissionais da rede. Mas como você domina o GNS3 e por onde começar?

No livro do GNS3, Jason aborda tudo o que os engenheiros de rede, administradores e pessoas que estudam para obter certificações precisam começar, desde a instalação e configuração do GNS3 até a criação e o gerenciamento de seus projetos. Jason se aprofunda enquanto mostra a verdadeira amplitude do software, abordando tópicos como capturar pacotes de rede, conectar-se a redes reais e switches ao vivo e incluir sistemas avançados como o vSRX Firefly da Juniper e o IOS-XRv da Cisco em seus laboratórios. Ele passa um tempo significativo explicando conceitos e dando dicas que o tornarão um usuário experiente rapidamente.

O livro de Jason é ideal para aproveitar o GNS3 e tirar o máximo proveito do seu laboratório de rede. Seja você um iniciante no setor de redes ou um profissional experiente, posso garantir que você aprenderá algo novo.

Jeremy Grossmann
Co-founder of GNS3
May 2015

Agradecimentos

Dizem que é preciso uma vila para criar um filho, e o GNS3 é o bebê de todos. Gostaria de agradecer a todas as pessoas que ajudaram a criar e promover o GNS3 e torná-lo a ferramenta de software incrível que é. Vocês são ótimos! Agradecimentos especiais para:

- Minha esposa, Sharon, por sua paciência e por me permitir ser uma GNS3 übergeek
- Jeremy Grossmann, nosso benevolente ditador do GNS3
- Christophe Follot, o criador da Dynamips, o homem que começou tudo
- Julien Duponchelle, o mestre de código silencioso
- Stephen Guppy, que responde mais e-mail em um dia do que eu em um ano
- Mark Blackwell, extraordinário evangelista do GNS3
- Flávio J. Saraiva, guru do Dynamips
- Chris Welch, criador do controle de multidão GNS3 Workbench e Jungle
- Radovan Brezula, que pode fazer com que qualquer sistema operacional de rede seja executado no GNS3
- Daniel Lintott - podemos converter esse projeto, mas vamos usar o Debian!
- René Molenaar de gns3vault.com, u dobrou ranhura. Dank u veel!
- Chris Bryant, do Bryant Advantage, os Bulldogs se unem!
- Jeremy Cioara, extraordinário deus da Cisco (aderência nº 1)
- Keith Barker, extraordinário deus da Cisco (aderência nº 2)
- Andrew Coleman, super moderador do GNS3, durma um pouco!
- Os financiadores do GNS3 - você sabe quem você é!

Também gostaria de agradecer a todos da No Starch Press por toda a ajuda na criação do The Book of GNS3. Em particular, gostaria de agradecer:

- Jennifer Griffith-Delgado - você é a melhor!
- Serena Yang - você foi muito paciente comigo e é incrível!
- Bill Pollock, o senhor supremo do NSP

Por ser um imbecil, tenho certeza de que esqueci muitas pessoas importantes, mas tenha certeza de que também te agradeço! Deixe-me dizer agora a todas as suas almas sem nome: obrigado!

Introdução

Comecei a usar o GNS3 no início de seu desenvolvimento e o levei como um pato na água. Desde o início, pude ver que seria uma ferramenta de rede inestimável. Usei-o para obter experiência prática em sistemas operacionais como Cisco IOS, Junos OS e Arista, além de passar em alguns exames de certificação de rede. Até hoje, eu o uso regularmente para testar as configurações do roteador antes de implantar equipamentos reais no campo. O Livro do GNS3 é minha maneira de compartilhar esse ótimo recurso com outros profissionais de rede, como você.

Para quem é este livro

Este livro é para qualquer pessoa envolvida em roteadores, comutadores ou firewalls. Se você usa Cisco, Juniper, Arista, Vyatta ou algum outro sistema operacional de rede, o GNS3 é uma ótima alternativa para a construção de laboratórios físicos. Ao contrário dos laboratórios que usam equipamentos físicos, os laboratórios virtuais do GNS3 permitem criar e salvar configurações de rede ilimitadas, sem precisar desmembrar um laboratório existente. Este livro aborda todos os detalhes para colocar seus projetos em funcionamento rapidamente.

O que há neste livro

O Livro do GNS3 o orienta na instalação, configuração e execução do GNS3 no Windows, OS X e Linux, e mostra alguns truques nerds e divertidos ao longo do caminho. Se você está começando ou já usou o GNS3 antes, acho que encontrará uma nova apreciação pelo quanto é possível quando você tem a ferramenta certa. Não abordo os fundamentos da rede TCP / IP, mas forneço muitos exemplos de como configurar dispositivos GNS3.

Minha Abordagem

A maneira mais eficaz de aprender é fazendo. É por isso que uso uma abordagem baseada em tutorial para criar laboratórios de vários fornecedores totalmente funcionais usando o GNS3. Os tutoriais explicam como criar e configurar laboratórios usando os dispositivos virtuais apresentados nos capítulos. Fornecemos exemplos de configuração do Cisco IOS, Junos OS e Juniper vSRX Firefly, entre outros. Você não precisa ser especialista em sistemas operacionais de rede, porque eu o guio passo a passo nas configurações. Você pode passar dias ou até semanas pesquisando na Web para descobrir como configurar recursos como conectar-se a switches ativos, criar um servidor de acesso virtual ou conectar seus laboratórios virtuais à Internet. Mas não é necessário fazer isso depois de ler O Livro do GNS3.

Visão geral do livro

O Livro do GNS3 o guia pela instalação e uso do GNS3, e cada capítulo apresenta novos conceitos que se baseiam nas habilidades dos anteriores. Você aprenderá a criar e gerenciar projetos simples a complexos, usando apenas um único computador ou compartilhando a carga entre vários computadores.

- O Capítulo 1, Introdução ao GNS3, sobre o que é e como funciona o GNS3, fornece uma visão geral do GNS3, e discute os benefícios das redes virtuais.
- O Capítulo 2, Instalação de um sistema GNS3 básico, discute a instalação do GNS3 no Windows, OS X e Linux e explica os benefícios do uso de dispositivos virtuais para executar o GNS3 como uma alternativa para instalá-lo diretamente no seu PC.
- O Capítulo 3, Configuração, examina a instalação de uma imagem do Cisco IOS e configurando seu primeiro roteador virtual usando Dynamips. Você também aprenderá o importância de definir um valor Idle-PC para roteadores Dynamips.
- O Capítulo 4, Criando e gerenciando projetos, ensina a configurar um roteador virtual. Depois disso, você analisará todas as opções da barra de ferramentas e criará uma rede simples de dois roteadores.

- Capítulo 5, Integrando hosts e usando o Wireshark, mostra como instalar o VPCS e usá-lo para adicionar hosts simples do tipo PC aos seus projetos. Você aprenderá como adicionar PCs virtuais completos usando o VirtualBox e criar um laboratório usando um roteador Cisco IOS virtual e um PC Linux VirtualBox. Você aprenderá sobre a captura de pacotes usando o Wireshark.
- O capítulo 6, Juniper Olive e vSRX Firefly, explica como instalar QEMU e use-o para criar seu próprio roteador Juniper virtual. Você criará uma rede usando o Juniper e a Cisco, aprenderá como instalar o Juniper vSRX Firefly e configurar um firewall básico do vSRX.
- Capítulo 7, Nós de dispositivos, Switches ativos e Internet, demonstra os nós de dispositivo integrados no GNS3 e explica como eles podem ser usados para economizar recursos no seu PC. Você também aprenderá como conectar seus projetos GNS3 a switches ativos e à Internet.
- Capítulo 8, Cisco ASA, IDS / IPS e IOS-Xrv, leva você da configuração de dispositivos GNS3 para configurá-los. Você criará um firewall Cisco ASA e um IDS / IPS e criará um laboratório de rede usando o Cisco IOS-Xrv.
- O capítulo 9, Cisco IOS no Unix e NX-OSv, continua o tema de criação de dispositivo. Você aprenderá como instalar o Cisco IOS no Unix e criar um switch virtual NX OS usando o NX-Osv.
- Capítulo 10, Coisas legais para fazer em um dia chuvoso, apresenta algumas coisas divertidas que você pode fazer com seu novo conhecimento sobre o GNS3, como criar um servidor de acesso simulado para gerenciar seus dispositivos e implantar configurações de dispositivos virtuais GNS3 em roteadores Cisco reais.
- Apêndice A, Ajuda! Eu caí e não consigo me levantar, discute alguns problemas comuns que você pode encontrar no GNS3 e fornece soluções para corrigi-los.
- O Apêndice B, Cisco Hardware Compatible with GNS3, lista Cisco roteadores compatíveis com GNS3 e qual imagem do Cisco IOS arquivos funcionam melhor.
- Apêndice C, Limitações NM-16ESW e IOU L2, fornece informações sobre o IOS nos switches Cisco Unix e NM-16ESW usados no GNS3.

Agora, prepare-se para mergulhar no GNS3. Antes de embarcar nessa jornada, não se esqueça de dar um beijo de despedida na sua família, pois, assim que começar, você não poderá parar!

1 INTRODUÇÃO AO GNS3

O GNS3 é um simulador de rede gráfica multiplataforma que roda em Windows, OS X e Linux, e é o esforço colaborativo de alguns nerds super talentosos e de força industrial - pessoas como Christophe Fillot, Jeremy Grossmann e Julien Duponchelle, apenas para nomear alguns. Fillot é o criador do programa de emulação de processador MIPS (Dynamips) que permite executar o sistema operacional do roteador da Cisco, e Grossmann é o criador do GNS3. Ele pegou o Dynamips e o integrou, juntamente com outros softwares de código aberto, a uma interface gráfica de usuário fácil de usar. Duponchelle ajuda na codificação do GNS3, e suas contribuições ajudaram a aprimorar o software.

O GNS3 permite projetar e testar redes virtuais no seu PC, incluindo (mas não limitado a) Cisco IOS, Juniper, MikroTik, Arista e Vyatta redes e é comumente usado por estudantes que precisam de experiência prática com roteamento e comutação do Cisco IOS enquanto estudam para os exames Cisco Certified Network Associate (CCNA) e Cisco Certified Network Professional (CCNP). Mas isso apenas arranha a superfície do que o GNS3 pode fazer. Neste capítulo, discuto o que é o GNS3, bem como os benefícios e limitações do software.

Por que usar o GNS3?

Antes das maravilhas da virtualização, engenheiros de rede, administradores e estudantes tinham que construir laboratórios com hardware físico ou alugar tempo em um rack. Ambas as opções podem ser caras e inconvenientes e limitam o projetos de rede disponíveis para você. Programas de simulação de software como o RouterSim e o Boson NetSim já existem há muito tempo, mas esses aplicativos limitados apenas simulam os comandos do Cisco IOS.

O Cisco Education oferece aluguel de rack virtualizado mais barato, com base no Cisco IOS no Unix (IOU), mas permite praticar apenas em configurações de rede pré-configuradas específicas. Também requer que você tenha uma conexão ativa com a Internet para acessar os laboratórios. A Cisco também oferece um produto chamado Virtual

Internet Routing Lab (VIRL) que é semelhante ao GNS3, mas exige uma taxa anual, limita o número de objetos que você pode usar em seus laboratórios e usa apenas sistemas operacionais simulados da Cisco.

O GNS3, por outro lado, permite que você personalize seus laboratórios de rede para atender exatamente às suas necessidades, crie projetos ilimitados usando Cisco e tecnologia que não seja da Cisco, adicione objetos ilimitados a seus projetos e acesse-os a qualquer momento, independentemente da conectividade com a Internet. O GNS3 fornece flexibilidade máxima para seus projetos por meio de uma combinação de dispositivos de hardware emulados que executam sistemas operacionais de rede reais, como o Cisco IOS, sistemas operacionais simulados, como o NX-OSv, e a capacidade de compartilhar recursos em vários computadores.

Hardware emulado

A interface gráfica do GNS3 permite criar laboratórios de rede virtualizados com uma variedade de roteadores, comutadores e PCs, mas realmente brilha quando emparelhado com o Cisco IOS. Ao contrário de aplicativos semelhantes, o GNS3 não apenas imita comandos ou recursos do Cisco IOS. Em vez disso, ele usa um aplicativo hypervisor de back-end para emular o hardware que executa o Cisco IOS. Como apenas o hardware é emulado, você executa um arquivo de imagem IOS real no seu PC. Todos os comandos e saídas de configuração vêm de um IOS real e, teoricamente, todos os protocolos ou recursos que uma versão do IOS suporta estão disponíveis para uso em seus projetos de rede. Essa funcionalidade distingue o GNS3 de programas como RouterSim, Boson NetSim ou VIRL, que simulam toda a experiência e fornecem apenas ambientes, comandos e cenários limitados para você trabalhar.

Sistemas Operacionais Simulados

Além do hardware emulado, o GNS3 integra sistemas operacionais simulados e eles podem ser totalmente conectados em rede a outros dispositivos GNS3. Um exemplo é o Cisco IOU, abordado no capítulo 9. O IOU consiste em uma série de arquivos binários do Linux que simulam os recursos das imagens IOS e é totalmente suportado pelo GNS3.

Além do Cisco IOS, o GNS3 pode integrar o Quick Emulator (QEMU) e máquinas virtuais VirtualBox executando sistemas operacionais como Linux, BSD ou Windows. Por exemplo, para praticar a instalação e configuração de um servidor Web Apache no Linux, basta adicionar uma máquina virtual (VM) VirtualBox executando Linux e Apache ao GNS3 e testá-lo navegando para ele a partir de outro host do VirtualBox. Tudo isso é feito no ambiente de usuário do GNS3. Se você quiser lançar um firewall na frente do servidor Apache, poderá usar um roteador Cisco, um firewall ASA (Adaptive Security Appliance) ou mesmo um firewall baseado em Linux, como o Vyatta.

Escalabilidade com o servidor GNS3

GNS3 aproveita a tecnologia cliente-servidor; Assim como um navegador da web se conecta a um servidor da web para acessar e exibir páginas da web, o programa GNS3 interface gráfica do usuário (GUI) acessa um servidor GNS3, permitindo iniciar, parar e controlar os dispositivos GNS3. Isso permite que seus projetos sejam dimensionados porque não estão restritos à execução em um único computador. Se você trabalha com topologias grandes ou complexas, também pode executar o programa do servidor GNS3 em um PC diferente do programa GNS3 GUI. Se você tiver acesso a um servidor high-end com muita memória e poder de processamento, poderá instalar o programa do servidor GNS3 no hardware do servidor, mas controlar todos os dispositivos do programa GNS3 GUI em execução em um PC mais modesto.

Conectividade virtual

A verdadeira beleza do GNS3 reside na capacidade de conectar seus dispositivos virtuais em rede, geralmente usando protocolos como o Internet Protocol versão 4 (IPv4) e o Internet Protocol versão 6 (IPv6), para criar laboratórios que podem ser executados em apenas um único computador. Alguns dos projetos mais simples podem ter apenas alguns componentes, como o projeto mostrado na Figura 1-1.

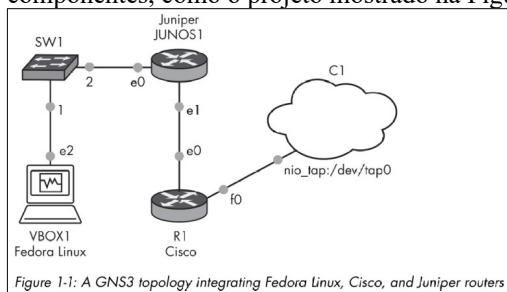


Figure 1-1: A GNS3 topology integrating Fedora Linux, Cisco, and Juniper routers

Figure 1-1: A GNS3 topology integrating Fedora Linux, Cisco, and Juniper routers

O projeto na Figura 1-1 permite que um host do Fedora Linux acesse a Internet ao vivo por meio de um switch, um roteador Juniper, um roteador Cisco e, finalmente, um nó da nuvem GNS3. Essa é uma rede simples, mas você pode criar redes complexas compostas por uma dúzia ou mais de roteadores, comutadores e PCs, como o design da Figura 1-2.

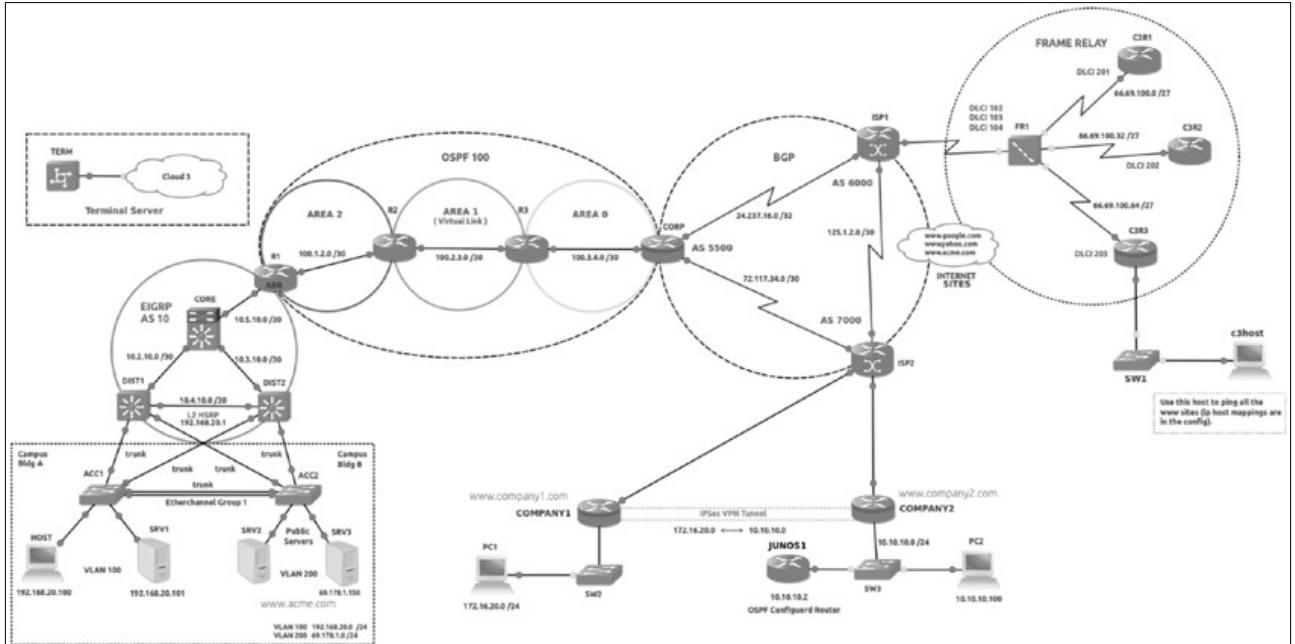


Figure 1-2: A complex, multiprotocol GNS3 topology

O projeto na Figura 1-2 é configurado com mais de 25 dispositivos, incluindo blocos de comutação redundantes, EtherChannel, HSRP (L2 Hot Standby Routing Protocol), Frame Relay, EIGRP (Enhanced Interior Gateway Routing Protocol), Open Shortest Path First (OSPF) e Border Gateway Protocol (BGP), mas o projeto pode ser executado em um PC modestamente configurado. Para manter seus dispositivos em ordem, você também pode anotar seus designs com texto colorido e escalável, como fiz neste exemplo. Se você possui um laptop, pode até levar projetos para apresentar aos clientes, resolver problemas de design ou estudar para exames de certificação. Os candidatos a CCNA ou CCNP também podem criar todos os laboratórios de treinamento necessários para aprender o material para exames da Cisco, praticar com sistemas operacionais reais e estudar de qualquer lugar.

O GNS3 tem a capacidade de conectar interfaces virtuais em seus dispositivos de laboratório para uma ou mais interfaces Ethernet físicas no seu PC. Isso permite que você conecte suas redes virtuais a hardware real, como roteadores, comutadores e outros PCs. Por exemplo, você pode executar duas ou mais redes GNS3 usando vários PCs e conecte-os usando um cabo cruzado Ethernet ou um comutador físico. Isso permite que você conecte todos os dispositivos GNS3 em todos os PCs. (Refiro-me carinhosamente a isso como uma ubernet GNS3!)

Integração de código aberto

O GNS3 realiza sua mágica aproveitando as tecnologias de código aberto, incluindo Dynamips, QEMU e VirtualBox. Pode executar Juniper, Arista e muitos outros sistemas operacionais de rede tão facilmente quanto o Cisco IOS.

O Hypervisor Dynamips

Para emular o hardware da Cisco, o GNS3 vem com o Dynamips, um aplicativo maravilhoso criado em 2005 por Christophe Fillot, da França, e mantido atualizado por contribuições de Flávio J. Saraiva e outros. O programa de hypervisor Dynamips pode emular o hardware do roteador das séries Cisco 1700, 2600, 3600, 3700 e 7200. Graças à Dynamips, você pode configurar rápida e facilmente esses modelos de roteador com uma variedade de placas de rede Cisco SLOT e WAN Interface Cards (WICs) emuladas no GNS3. As placas de entrada / saída virtual (E / S) permitem adicionar várias interfaces Ethernet, módulos de chave e portas seriais aos seus dispositivos. Você pode até adicionar ou remover memória por dispositivo, dependendo dos requisitos do seu projeto e da versão do Cisco IOS.

QEMU e VirtualBox

Você pode adicionar máquinas virtuais QEMU e VirtualBox ao GNS3 e usar em seus projetos. Esses dispositivos podem ser vinculados a outros dispositivos GNS3 para formar uma rede ponta a ponta completa.

Por exemplo, você pode conectar um host do VirtualBox a uma série de comutadores e roteadores e permitir que ele accesse recursos em outro host do VirtualBox nessa rede. Nesse cenário, você pode configurar e testar todos os tipos de protocolos de roteamento, além de recursos como conversão de endereços de rede (NAT), listas de controle de acesso (ACLs) e redes privadas virtuais (VPNs). Naturalmente, o hardware do seu computador físico impõe restrições aos seus recursos, mas os computadores modernos têm muitos recursos não utilizados esperando para serem acessados pelo GNS3.

Algumas limitações

O GNS3 não está isento de limitações. O Dynamips foi limitado de tal maneira que você não pode usá-lo em um ambiente de produção, tornando-o útil apenas para educação. Além disso, a comutação é limitada a um conjunto de comandos modesto, a menos que você integre um ou mais comutadores físicos do Catalyst nos seus projetos GNS3. Felizmente, o IOU ajuda a preencher parte dessa lacuna.

Alguma montagem necessária

Todas as grandes coisas têm um preço, e o GNS3 não é exceção. Mais notavelmente, o GNS3 exige que uma ou mais imagens do Cisco IOS sejam executadas nos roteadores Dynamips virtuais, e o GNS3 não as fornece. As imagens podem ser copiadas de um roteador que você possui ou através de uma conta Cisco connection online (CCO), se você tiver um contrato com a Cisco.

Emulação limitada

A Dynamips não consegue emular o hardware do circuito integrado específico do aplicativo (ASIC) dos switches Catalyst avançados da Cisco. Esse é um pequeno revés para o aspirante a CCNA ou mesmo ao CCNP, mas dificulta os aspirantes a Cisco Certified Internetwork Experts (CCIEs) que precisam dos recursos avançados dos comutadores.

No entanto, a versatilidade do GNS3 permite integrar seus laboratórios virtuais do GNS3 aos comutadores Catalyst reais. Isso pode reduzir bastante o custo de criação de um laboratório CCIE e, como a maioria do laboratório é virtualizada, permite maior flexibilidade em suas configurações. Quando você não precisa desses recursos avançados, pode adicionar um módulo de switch, como o Cisco NM-16ESW, para um dos roteadores Cisco virtuais para criar um switch de camada 3 simples. Este dispositivo deve satisfazer necessidades modestas de comutação, incluindo redes locais virtuais (VLANs), entroncamento 802.1Q, spanning tree, EtherChannel e roteamento multiprotocolo usando EIGRP, OSPF, BGP e outros protocolos. Por fim, as imagens Cisco IOU podem ser usadas para emular comutadores Cisco e fornecem mais comandos que o módulo de comutação Dynamips.

Desempenho de rede interrompido

Outra limitação do GNS3 é o desempenho da rede. Como o Dynamips é um emulador que não fornece nenhuma aceleração de hardware, a taxa de transferência é restrita de 1,5 Mb a 800 Mb por segundo, dependendo do IOS usado e da sua configuração. Isso pode parecer uma limitação, mas na verdade é uma coisa boa porque impede os usuários de virtualizar o hardware da Cisco e colocá-lo em ambientes de produção. Imagine se os dispositivos emulados funcionassem com a capacidade total: todo nerd de rede daqui para Timbuktu instalaria roteadores virtuais em PCs baratos e os usaria em redes de produção, roubando efetivamente a propriedade intelectual da Cisco. Se isso acontecesse, a Cisco teria procurado os desenvolvedores do Dynamips como uma tonelada proverbial de tijolos, e o GNS3 não existiria hoje. Essa limitação tem pouco ou nenhum efeito ao usar o GNS3 para treinamento e teste.

Pensamentos finais

Agora que cheguei aos destaques do GNS3, Espero que você esteja tão empolgado quanto eu em usá-lo em seu próprio computador. Diferente de aplicativos ou ferramentas semelhantes, o GNS3 oferece controle total, deixando você livre para usar sua imaginação para criar, aprender e desenvolver redes elaboradas que atendem às suas necessidades. Além disso, você pode fazer tudo isso sem gastar muito em roteadores e switches, apenas para acabar com uma sala cheia de hardware barulhento e que consome eletricidade. No próximo capítulo, mostrarei como instalar o GNS3. Vamos começar!

2

INSTALANDO UM SISTEMA BÁSICO GNS3

Diga adeus ao mundo do hardware e diga olá ao GNS3! É uma maneira totalmente nova de aprender networking. Neste capítulo, orientarei você no processo de instalação de um sistema GNS3 básico no Microsoft Windows, Mac OS X e Ubuntu Linux.

Uma instalação básica consiste do aplicativo GNS3 e alguns aplicativos auxiliares. No Windows e no OS X, todos os aplicativos de pré-requisito são fornecidos no pacote do instalador do GNS3, disponível no site do GNS3 (<http://www.gns3.com/>). Ao instalar no Linux, você pode baixar e instalar o GNS3 por meio de um gerenciador de pacotes específico da plataforma ou diretamente do código-fonte. Os princípios usados para instalar a partir do código fonte podem ser aplicados a praticamente qualquer sistema baseado em Unix, e é uma ótima maneira de garantir que você tenha o software mais recente.

Requerimentos gerais

Os requisitos para executar o GNS3 são amplamente determinados pelo sistema operacional em que você está instalando, o modelo e o número de roteadores que você deseja usar em seus projetos e se você integra programas externos como QEMU ou VirtualBox aos seus projetos. A maioria dos computadores adquiridos nos últimos anos deve poder executar esta instalação básica sem problemas.

Dito isto, se você decidir ir além da criação de projetos usando apenas roteadores Cisco e incorporando outros ambientes virtuais aos seus projetos GNS3 (como Linux, BSD, ASA, IDS ou Juniper), você precisará da maior potência possível. Quanto mais memória e poder de processamento você tiver, melhor será a execução de programas, como o QEMU e o VirtualBox, que requerem RAM para executar seus sistemas operacionais convidados e competem com o sistema operacional nativo pelo tempo de CPU. Você também precisará de espaço em disco adicional para armazenar seus sistemas operacionais convidados.

Você pode visitar o site do GNS3 para verificar os requisitos para o seu sistema operacional, mas uma boa regra geral para uma instalação básica simples é a seguinte:

- 1.5 GHz processor
- 4GB RAM
- 250MB free disk space

Essas são as especificações mínimas e um sistema que as possui deve ser capaz de executar uma topologia GNS3 simples usando um punhado de roteadores Cisco. Obviamente, à medida que seus projetos se tornam maiores e mais complexos, o GNS3 se beneficiará muito de um sistema mais poderoso.

Nota

Se as instruções de instalação parecerem impressionantes agora, não tenha medo! Vá para a seção “Dispositivos GNS3” na página 14 para aprender como baixar um dispositivo GNS3 pré-construído e mergulhe de cabeça.

Instalando no Microsoft Windows

Comparado a outros sistemas operacionais, a instalação do GNS3 no Windows é fácil. O pacote do instalador do Windows inclui quase todos os aplicativos que o GNS3 precisa, além de alguns extras não encontrados em outras plataformas, e tudo é instalado com pouca intervenção do usuário. O instalador do Windows inclui alguns aplicativos úteis adicionais, incluindo QEMU, usados para Juniper e ASA; Wireshark, um popular programa de monitoramento de rede; PuTTY, um programa de emulação de terminal do Windows; e VPCS, um simples simulador de comandos semelhante ao DOS para testar a conectividade usando os comandos ping e traceroute. O instalador contém uma versão de 32 bits e uma de 64 bits do GNS3, e deve instalar a versão correta automaticamente.

Siga estas etapas para instalar o GNS3 no Windows:

1. Faça o download do instalador do multifuncional GNS3 no site do GNS3 (<http://www.gns3.com/>) e inicie-o para iniciar a instalação.
2. Clique em Avançar na tela do Assistente de instalação e clique em Concordo na Tela Contrato de licença.

3. Selecione a pasta onde deseja que o instalador coloque um atalho para o aplicativo no Menu Iniciar e clique em Avançar. (A pasta padrão é GNS3.)

4. Você pode escolher os componentes a serem incluídos na sua instalação, como mostrado na Figura 2-1. A opção padrão instala todos os componentes para criar um sistema GNS3 totalmente funcional, incluindo Wireshark, VPCS e QEMU. Para economizar espaço em disco ou se você não precisar desses recursos adicionais, desmarque essas opções. O WinPCAP é necessário para conexões de nuvem NIO Ethernet e o Dynamips é necessário para criar projetos usando roteadores e switches Cisco. Faça suas seleções e clique em Avançar.

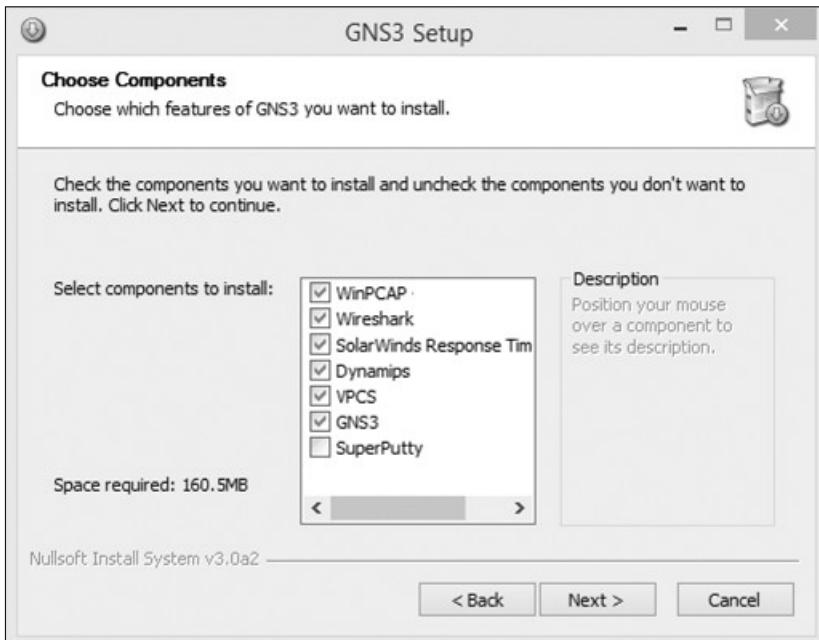


Figure 2-1: Choosing the GNS3 components to install

5. Você deve ver a tela Escolha o local de instalação, como mostrado na Figura 2-2. Para instalar o GNS3 em um local alternativo, digite o novo local no campo Pasta de destino e clique em Instalar.

6. Continue seguindo todas as instruções para concluir a instalação. Eu recomendo que você aceite todas as configurações padrão.

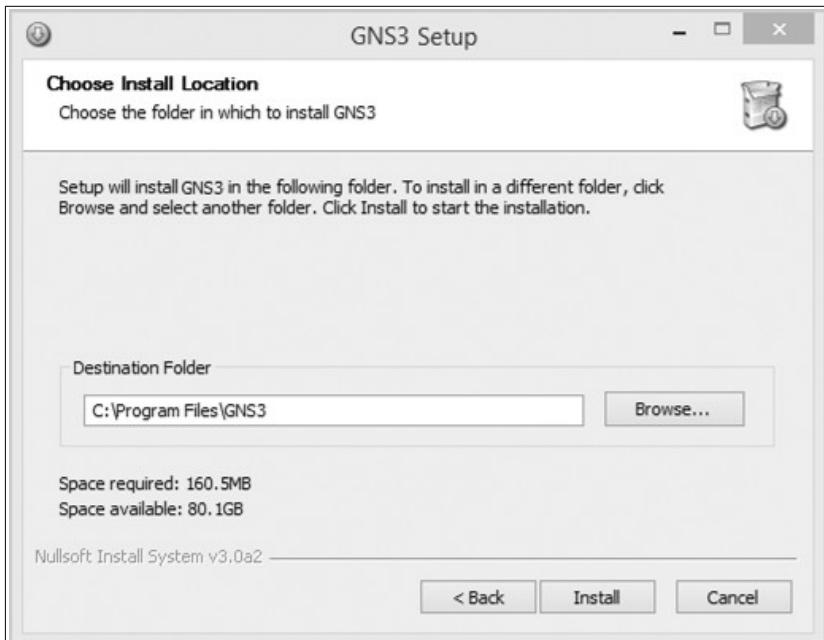


Figure 2-2: Choosing the destination folder location

Após a conclusão, o GNS3 deve colocar um ícone na área de trabalho.

Instalando no OS X

O GNS3 é suportado apenas em Macs baseados em Intel executando o OS X. Você provavelmente deve ter a versão mais recente do OS X antes de executar o GNS3. Para instalar o aplicativo GNS3 no OS X, faça o download do instalador apropriado no site do GNS3 (<http://www.gns3.com/>) e clique duas vezes no instalador e um arquivo de imagem de disco DMG será exibido na área de trabalho. Clique duas vezes no arquivo de imagem para abrir a pasta GNS3 e arraste o ícone GNS3 para a pasta Aplicativos, como mostra a Figura 2-3.

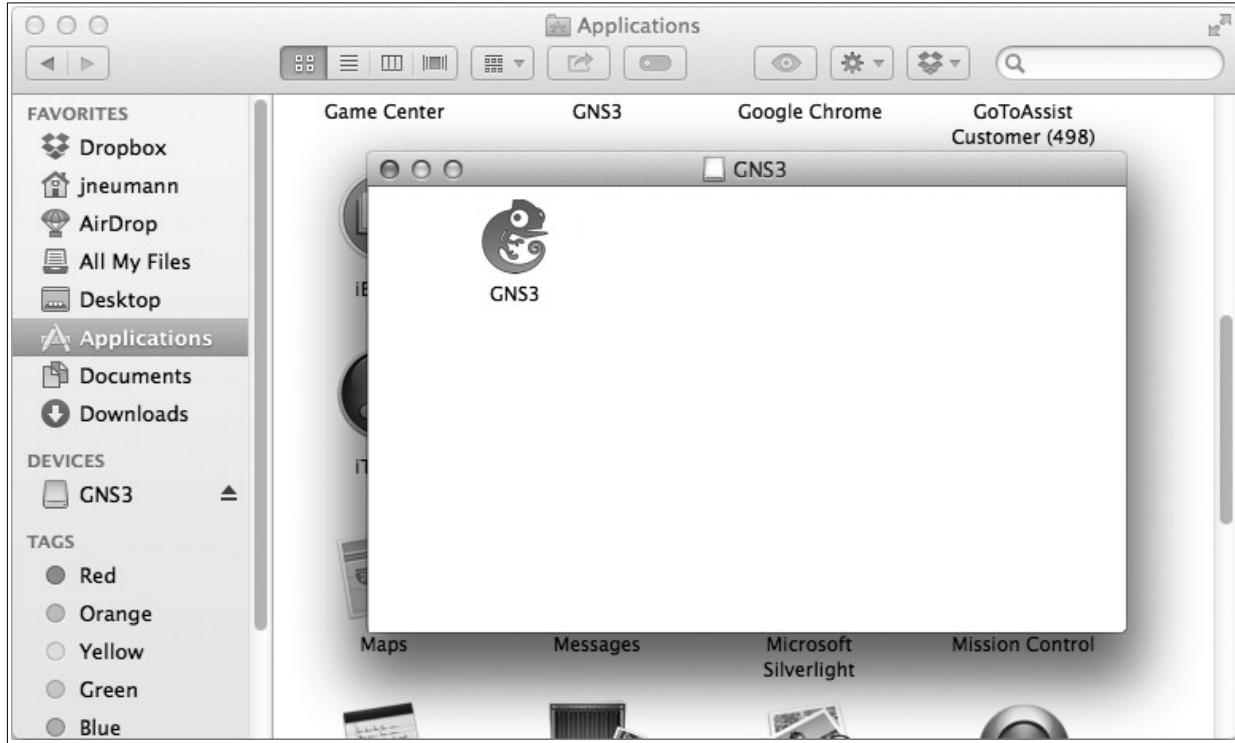


Figure 2-3: Dragging the GNS3 program icon to the Applications folder

Para executar o GNS3 nas versões atuais do OS X, talvez seja necessário clicar com o botão direito do mouse no ícone do aplicativo instalado e selecione Abrir na primeira vez em que o executar. Você será solicitado com uma caixa de diálogo avisando que o pacote é de um desenvolvedor não identificado e perguntando se você tem certeza de que deseja abrir o aplicativo. Clique no botão Abrir para contornar esse recurso do OS X Gatekeeper. O GNS3 começará normalmente a partir de então, sem nenhum aviso.

Instalando no ubuntu linux

O GNS3 funciona bem em muitas distribuições Linux diferentes, mas há uma infeliz falta de documentação para a maioria delas. Nesta seção, vou desvendar o mistério e mostrar como é simples executar o GNS3 em uma plataforma baseada em Unix. Eu escolhi cobrir o Ubuntu porque é uma das distribuições mais usadas.

Existem duas maneiras de instalar o GNS3 no Linux. Você pode instalar um pacote incluído no gerenciador de pacotes ou instalar a partir do código-fonte. O uso de uma instalação em pacote é rápido e fácil, mas a desvantagem é que você está preso a qualquer versão do GNS3 que foi portada para sua plataforma específica, que pode não ser a versão mais recente. É aqui que uma instalação de origem é útil. A instalação a partir da fonte requer apenas algumas etapas extras e fornece a versão mais recente do GNS3. Embora eu recomendo a instalação a partir do código-fonte, abordaremos os dois métodos aqui.

Instalando o GNS3 a partir de pacotes

Para instalar o GNS3 usando as Ferramentas avançadas de pacote, abra o programa do terminal e digite o seguinte comando:

```
$ sudo apt-get install gns3
```

Quando solicitado, digite sua senha. A saída deste comando exibe uma lista de pacotes que serão instalados e mostra quanto espaço em disco será usado pela instalação. O instalador solicita que você confirme se está tudo bem

antes de continuar. Quando confirmados, os pacotes estão instalados e o GNS3 está pronto para execução. Você pode iniciar o aplicativo a partir do programa do terminal digitando gns3 ou iniciando o GNS3 no menu de aplicativos do seu gerente de exibição. Agora você está pronto para configurar o GNS3.

Instalando o GNS3 a partir do código fonte

A instalação do código-fonte garante que você obtenha a versão mais recente do GNS3 e é, na minha opinião, a melhor maneira de instalar o GNS3 em sistemas baseados em Unix. Independentemente da versão do Linux que você estiver usando, você poderá usar estas instruções como um guia para colocar o GNS3 em funcionamento no seu sistema. No exemplo a seguir, usarei o Ubuntu Linux como uma estrutura, mas lembre-se de que essas instruções podem ser aplicadas a praticamente qualquer distribuição baseada em Unix. A principal diferença entre distribuições são as dependências necessárias e como você as instala. Verifique o site do GNS3 para obter os requisitos de dependência mais recentes.

Instalei o GNS3 no Solaris, FreeBSD, OpenBSD, Ubuntu, Mint, OpenSUSE, Fedora, Fuduntu, Debian, Arch, Gentoo, Kali, Netrunner e PCLinuxOS, por isso tenho certeza de que você também pode executá-lo no seu sistema! Baixe e descompacte os arquivos de instalação no site do GNS3 (<http://www.gns3.com/>).

Extraindo o código fonte

Ao baixar o GNS3 para Linux, você recebe um arquivo ZIP que contém o código-fonte do Linux. Ao extrair o arquivo, você verá arquivos ZIP individuais para cada programa que o GNS3 usa. Descompacte o arquivo de origem GNS3 usando o seguinte comando, substituindo x pela sua versão do arquivo:

```
$ cd ~/Download  
$ unzip GNS3-x-source.zip  
dynamips-x.zip  
gns3-gui-x.zip  
gns3-server-x.zip  
vpcs-x.zip  
iouyap-x.zip
```

Em seguida, você atualizará o gerenciador de pacotes Ubuntu.

Atualizando o Gerenciador de Pacotes

A atualização dos arquivos de índice do gerenciador de pacotes garante a instalação das versões mais recentes das dependências. No Ubuntu, abra o programa do terminal e digite:

```
$ sudo apt-get update
```

Instalando dependências

As dependências do GNS3 e os nomes dos pacotes são específicos para cada distribuição do Linux, portanto, você precisará fazer o download dos do seu sistema operacional. Você também pode consultar o site do GNS3 antecipadamente, pois as dependências podem mudar com o tempo. No Ubuntu, digite os seguintes comandos:

```
$ sudo apt-get install python3-dev  
$ sudo apt-get install python3-setuptools  
$ sudo apt-get install python3-pyqt4  
$ sudo apt-get install python3-ws4py  
$ sudo apt-get install python3-netifaces
```

Após instalar todos os pacotes python, vá para o Dynamips.

Instalando Dynamips

Você precisará instalar mais alguns pacotes no sistema Ubuntu antes de compilar o Dynamips:

```
$ sudo apt-get install libpcap-dev  
$ sudo apt-get install libelf-dev
```

```
$ sudo apt-get install uuid-dev
$ sudo apt-get install cmake
```

Em seguida, descompacte o arquivo de código-fonte, compile e instale o Dynamips usando os seguintes comandos. Substitua x pela sua versão do software.

```
$ unzip dynamips-x.zip
$ cd dynamips-x
$ mkdir build
$ cd build
$ cmake ..
$ make
$ sudo make install
```

Quando você terminar, você deve ter um arquivo chamado dynamips em seu diretório `/usr/local/bin/`. Altere a propriedade do programa para root e as permissões de arquivo para executável. Isso permite que os dispositivos Dynamips se conectem à Internet ou usem hardware ativo como switches Cisco usando o adaptador Ethernet do seu PC.

```
$ sudo chown root /usr/local/bin/dynamips
$ sudo chmod 4755 /usr/local/bin/dynamips
```

Para as pessoas preocupadas com a segurança, existe uma alternativa. Você pode obter a mesma funcionalidade sem fornecer permissões de nível raiz ao Dynamips. O seguinte funciona no Ubuntu e deve funcionar na maioria dos sistemas executando um kernel Linux 2.2 ou superior. Este método não funciona em sistemas baseados em BSD.

```
$ sudo apt-get install libcap2
$ sudo setcap cap_net_raw,cap_net_admin+eip /usr/local/bin/dynamips
```

Em seguida, você instalará o servidor GNS3 e os arquivos de origem da GUI.

Instalando o servidor GNS3 e a GUI

O GNS3 consiste em dois aplicativos principais: um aplicativo para servidor e um aplicativo GUI. O aplicativo do servidor é executado em segundo plano no seu PC e geralmente não é visto pelos usuários normais. Ele executa e gerencia todos os aplicativos auxiliares, como Dynamips, QEMU e VirtualBox. O aplicativo GUI fornece a experiência do usuário front-end e é onde você interage com o GNS3.

```
$ unzip gns3-server-x.zip
$ unzip gns3-gui-x.zip
```

Para concluir a instalação, execute o script de configuração do GNS3 para cada aplicativo. Esta etapa requer privilégios elevados no nível da raiz, portanto, tenha sua senha de root à mão. Comece com o servidor GNS3.

```
$ cd gns3-server-x
$ sudo python3 setup.py install
```

Em seguida, instale o aplicativo GNS3 GUI.

```
$ cd gns3-gui-x
$ sudo python3 setup.py install
```

Quando a instalação termina, o aplicativo é instalado em `/usr/local/bin/`. Em seguida, instale o Virtual PC Simulator (VPCS) descompactando o arquivo ZIP do vpcs e executando o script do instalador mk.sh. Este software simula um PC host simples e pode ser usado para testar roteadores em seus projetos.

```
$ unzip vpcs-x.zip
$ cd vpcs-x/src
$ ./mk.sh
$ sudo cp vpcs /usr/local/bin
```

A etapa final é específica para o Ubuntu e algumas outras distribuições Linux, e é necessária devido à implementação do Gnome Desktop. Sem esse comando, o programa funcionará bem, mas alguns dos ícones do menu não serão exibidos no GNS3.

```
$ gconftool-2 --type Boolean --set /desktop/gnome/interface/menus_have_icons True
```

Para iniciar o programa, digite o seguinte comando do terminal:

```
$ gns3
```

É isso aí! Agora você está pronto para seguir em frente configurando o GNS3 e criando projetos.

GNS3 Appliances

Uma alternativa para instalar o GNS3 no seu PC é: use um dispositivo GNS3 pré-configurado. Um dispositivo GNS3 é simplesmente uma máquina virtual que vem com o GNS3 já instalado. Os appliances GNS3 são extremamente flexíveis porque são executados usando um aplicativo como o VirtualBox. O VirtualBox é gratuito e é executado na maioria dos sistemas operacionais (incluindo Windows, OS X, Linux e FreeBSD).

Alguns Prós e Contras

Existem várias vantagens em executar o GNS3 em um ambiente virtual. Os principais são facilidade e portabilidade. A maior parte do trabalho de configuração foi feita para você e você terá uma instalação portátil do GNS3 que pode ser movida de um PC para outro. Se você comprar um novo computador, poderá copiar o dispositivo para o novo PC e tudo deverá funcionar exatamente como antes, independentemente do hardware ou sistema operacional em que o novo computador esteja executando.

Por outro lado, sua máquina host precisa ter um processador rápido e bastante memória RAM, se você quiser que o sistema operacional convidado e o GNS3 funcionem bem, principalmente se você criar projetos grandes ou complexos. E como você está emulando o hardware do sistema operacional convidado, seu projeto pode sofrer um pequeno impacto no desempenho, dependendo do hardware subjacente.

GNS3 WorkBench

Existem vários dispositivos GNS3 para você escolher, mas eu recomendo o GNS3 WorkBench (<http://rednectar.net/gns3-workbench/>), mostrado na Figura 2-4. O desenvolvedor fez um bom trabalho ao tornar a interface limpa e a configuração é bastante direta. Construído sobre o Linux, o GNS3 WorkBench vem com GNS3, Wireshark e VPCS pré-instalados. Ele também vem com vários exercícios e laboratórios pré-configurados para ajudá-lo a se preparar para os exames de certificação CCNA da Cisco. Muitos laboratórios contêm problemas para solucionar, com os objetivos claramente definidos.



Figure 2-4: GNS3 WorkBench

O GNS3 WorkBench pressupõe que o usuário tenha um nível mínimo de experiência no Linux, mas alguma experiência anterior no Linux é útil. Os scripts de shell do Linux estão incluídos para ajudá-lo na instalação do Cisco IOS, e os laboratórios foram projetados para que eles precisem apenas de algumas imagens do IOS para funcionar. Como bônus, o desenvolvedor incluiu vários exercícios do GNS3 Vault.

O site do GNS3 Vault (<http://www.gns3vault.com/>) é dedicado a tudo o que o GNS3, tem um forte foco na educação da Cisco e fornece exercícios práticos para quem se prepara para a certificação Cisco CCNA ou CCNP.

Instalando o GNS3 WorkBench

O GNS3 WorkBench é gratuito e está disponível apenas como uma máquina virtual VMware. No entanto, você pode importar a Imagem de Disco virtual e executar o dispositivo usando o VirtualBox. Se você deseja executar o dispositivo de forma nativa usando o VMware, visite o site (<http://www.vmware.com/>) e verifique se a sua plataforma é suportada. Caso contrário, eu recomendo usar o VirtualBox (<http://www.virtualbox.org/>) porque suporta mais plataformas - especificamente Windows, Linux, FreeBSD e OS X - e é gratuito para todas elas. Antes de começar, verifique se sua estação de trabalho possui 10 GB de espaço livre no disco rígido e você instalou o VirtualBox. Para instalar o GNS3 WorkBench no VirtualBox, faça o download do appliance GNS3 WorkBench no site do GNS3 (<http://www.gns3.com/>) e siga estas etapas:

1. Inicie o VirtualBox e crie uma nova máquina virtual clicando em Novo na tela de inicialização. Após a abertura do assistente, clique em Continuar para começar.

2. Nomeie sua máquina virtual, escolha Linux como o sistema operacional e Ubuntu como a versão (como mostrado na Figura 2-5) e, em seguida, clique em Continuar.

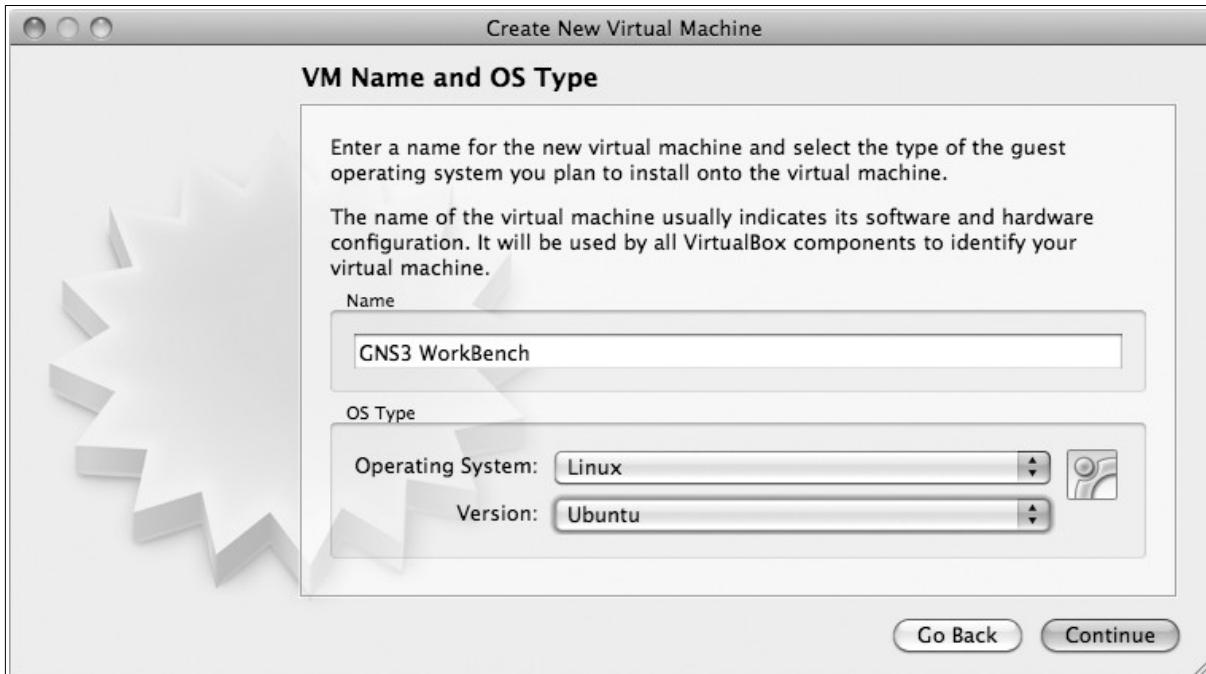


Figure 2-5: Creating a new Ubuntu Linux virtual machine for GNS3 WorkBench

3. Ajuste as configurações de memória conforme necessário e clique em Continuar para avançar para a caixa de diálogo Disco rígido virtual. Em seguida, marque o botão de opção Usar disco rígido existente, clique no ícone da pasta amarela e navegue até o local em que você salvou os arquivos do GNS3 Workbench. Selecione o arquivo chamado GNS3 WorkBench.vmdk, verifique se há uma verificação ao lado de Disco de inicialização e clique em Continuar, conforme mostrado na Figura 2-6. Isso é o equivalente virtual de remover um disco rígido de um PC e instalá-lo em outro.



Figure 2-6: Selecting the VMware Disk Image to use with VirtualBox

4. Clique em Avançar e Concluir para finalizar a instalação.

5. Finalmente, inicie o GNS3 WorkBench e instale as adições de convidado. Software de adições para convidados fornece os drivers de hardware para sua nova máquina virtual. Clique em **Devices ▾ Install Guest Additions** e siga as instruções na tela. No FreeBSD, adições de convidados são instaladas via pacote `virtualbox-ose-additions`.

Nota

Se o PC host tiver RAM extra, convém fornecer ao GNS3 WorkBench 2 GB de RAM (ou mais), em vez do padrão de 1 GB. 1 GB de RAM é mínimo para o GNS3. Aumentar a memória disponível melhorará o desempenho.

Depois de concluir a instalação, clique em Iniciar para inicializar o Ubuntu. Instruções sobre como configurar e usar o GNS3 WorkBench devem aparecer.

Pensamentos finais

Neste capítulo, você aprendeu que o GNS3 pode ser instalado em praticamente qualquer sistema operacional e que não precisa de um PhD em Ciência da Computação para fazer isso. Isso não quer dizer que seja instalado com facilidade em todos os sistemas. Algumas distribuições Linux, por exemplo, podem não ter um pacote GNS3 (ou o pacote disponível pode estar desatualizado demais para atender às suas necessidades), mas essa é a beleza do software de código aberto: você pode instalar diretamente a partir do código-fonte. Outra armadilha em potencial é que todas as dependências necessárias - ou a versão adequada dessas dependências - podem não estar disponíveis para a versão do seu sistema operacional, e isso é um impedimento garantido. Nesse caso, eu recomendo que você use um dispositivo como o GNS3 WorkBench ou use o VirtualBox e instale um sistema operacional convidado que, como o Ubuntu, suporte totalmente o GNS3. Com o GNS3 instalado, você estará pronto para o próximo capítulo, onde aprenderá a configurar o GNS3 e criar projetos.

3 Configuração

Instalando GNS3 é apenas o primeiro passo no caminho para a criação de projetos; o segundo passo é a configuração. Felizmente, o GNS3 nunca foi tão fácil de configurar, e você precisa executar apenas algumas tarefas. Neste capítulo, abordarei as opções básicas de configuração do GNS3 necessárias para colocar os roteadores IOS em funcionamento usando o Dynamips.

Adquirindo uma imagem de IoS

Os roteadores Dynamips virtuais fornecidos pelo GNS3 são dispositivos de hardware emulados. Como um disco rígido de PC recém-formatado, seus roteadores virtuais aguardam pacientemente a instalação de um sistema operacional para que possam fazer algo útil. O que eles precisam é do Cisco IOS!

Antes de inicializar um roteador, você precisará instalar e configurar pelo menos um arquivo de imagem do Cisco IOS no GNS3, embora esteja por conta própria quando se trata de adquirir um. O IOS é propriedade intelectual da Cisco Systems e normalmente não está disponível ao público. Além disso, como os desenvolvedores do GNS3 não têm afiliação com a Cisco, eles também não podem fornecer legalmente uma imagem do IOS (por isso, não pergunte).

A maneira mais simples de adquirir um arquivo de imagem do IOS é copiar uma imagem de um roteador Cisco que você possui. A vantagem dessa abordagem é que você não está roubando uma imagem; você já tem uma imagem do IOS licenciada para o seu roteador. A desvantagem é que o GNS3 suporta apenas alguns modelos dentre as centenas que a Cisco fabrica, e seu roteador pode não ser um deles. (Consulte o Apêndice B para obter uma lista completa de roteadores Cisco compatíveis e configurações de hardware.)

Para copiar um arquivo de imagem do IOS de um roteador para uma estação de trabalho, faça logon no roteador e use o comando Cisco copy para copiar o arquivo de imagem da memória flash do roteador para um servidor FTP. Se você não souber o nome do seu arquivo de imagem do IOS, poderá usar o comando show flash no seu roteador. No exemplo a seguir, o nome do arquivo da imagem IOS é c7200-ios-version.bin; meu servidor FTP está sendo executado em um PC com o endereço IP 192.168.1.25, e meu nome de usuário e senha FTP são jason e mypass, respectivamente.

```
# copy flash:c7200-ios-version.bin ftp://jason:mypass@192.168.1.25
```

Quando o comando é executado no roteador, o arquivo de imagem será ser copiado da memória flash do roteador para um servidor FTP em execução no 192.168.1.25 usando as credenciais fornecidas. Se você deseja usar o TFTP, faça o download de um servidor TFTP gratuito no site da Jounin (<http://tftpd32.jounin.net/>). Quando o servidor estiver instalado e em execução, use o seguinte comando tftp para copiar o arquivo do seu roteador para o servidor TFTP:

```
# copy flash:c7200-ios-version.bin tftp  
Address or name of remote host []? 192.168.1.25  
Destination filename [c7200-ios-version.bin]? <enter>
```

Pressione Enter após o nome do arquivo de destino [c7200-ios-version.bin] para completar a cópia.

Se, por outro lado, você não possui um roteador Cisco, existem mais maneiras desagradáveis de encontrar arquivos de imagem do IOS, como você certamente encontrará com uma simples pesquisa na Internet. Enquanto empresas como Cisco e Juniper fecharam os olhos para esse tipo de coisa no passado (desde que o software seja usado apenas para fins educacionais), talvez você não queira usar uma versão pirata do Cisco IOS. Essas imagens podem funcionar muito bem, mas sempre há a possibilidade de que elas contenham malware ou tenham sido adulteradas de maneiras inesperadas.

Por fim, se você trabalha para uma grande empresa que é parceira da Cisco, deve conseguir fazer logon no site da Cisco usando as credenciais do parceiro e obter a imagem do IOS desejada. Esteja ciente de que esse tipo de atividade pode ser motivo para levá-lo à força corporativa; portanto, obtenha permissão antes de usar sua conta corporativa.

No entanto, você obtém uma imagem do IOS, pode usar apenas arquivos de imagem que são projetados para modelos de roteador suportados pelo GNS3, e algumas versões do IOS para um determinado modelo podem funcionar melhor que outras. Se você achar que um roteador Dynamips está agindo de maneira persnickety, tente trocar o IOS por uma versão diferente, pois isso geralmente corrige o problema.

Nota

Em geral, fique longe das imagens c26xx porque elas parecem ser as menos estáveis!

A escolha da imagem correta do roteador e do IOS é fundamental para criar um ambiente estável projetos. As versões recomendadas do IOS são c36xx, c37xx e c7200 (mas não o c7200p) porque essas são as versões mais estáveis para Dynamips e GNS3. Considere também o número da versão do IOS. Embora as novas versões do IOS forneçam as

últimas informações, as versões mais antigas tendem a usar menos recursos do PC, como energia e memória do processador. Se você estiver criando projetos simples para o estudo do CCNA, convém usar um IOS mais antigo do que 12.2 ou 12.3 para economizar recursos, mas se estiver estudando para o seu CCIE, poderá precisar instalar o IOS mais novo disponível.

Configurando seu primeiro roteador IoS Depois de ter uma imagem IOS, você precisa fazer algumas coisas antes de começar a usar seus roteadores virtuais. Primeiro, verifique o caminho para Dynamips (isso é específico para Linux). Em seguida, copie suas imagens do IOS para uma pasta e adicione as imagens ao GNS3. Por fim, defina um valor de PC ocioso para cada imagem do IOS que você adicionou ao GNS3. Vou guiar você por essas etapas agora.

Configurando Dynamips

No Windows e no OS X, as preferências devem ser configuradas para você, mas no Linux você deve verificar se o caminho para o aplicativo Dynamips está correto. Vá para **Edit > Preferences**, selecione **Dynamips** e clique na guia **General settings**, como mostra a Figura 3-1.

Verifique se o caminho para Dynamips o campo aponta para `/usr/local/bin/dynamips`. Se você instalou o aplicativo Dynamips em outro diretório, defina o caminho para esse diretório.



Figure 3-1: Dynamips preferences, General settings tab

Em seguida, clique na guia Configurações avançadas para exibir as configurações na Figura 3-2.

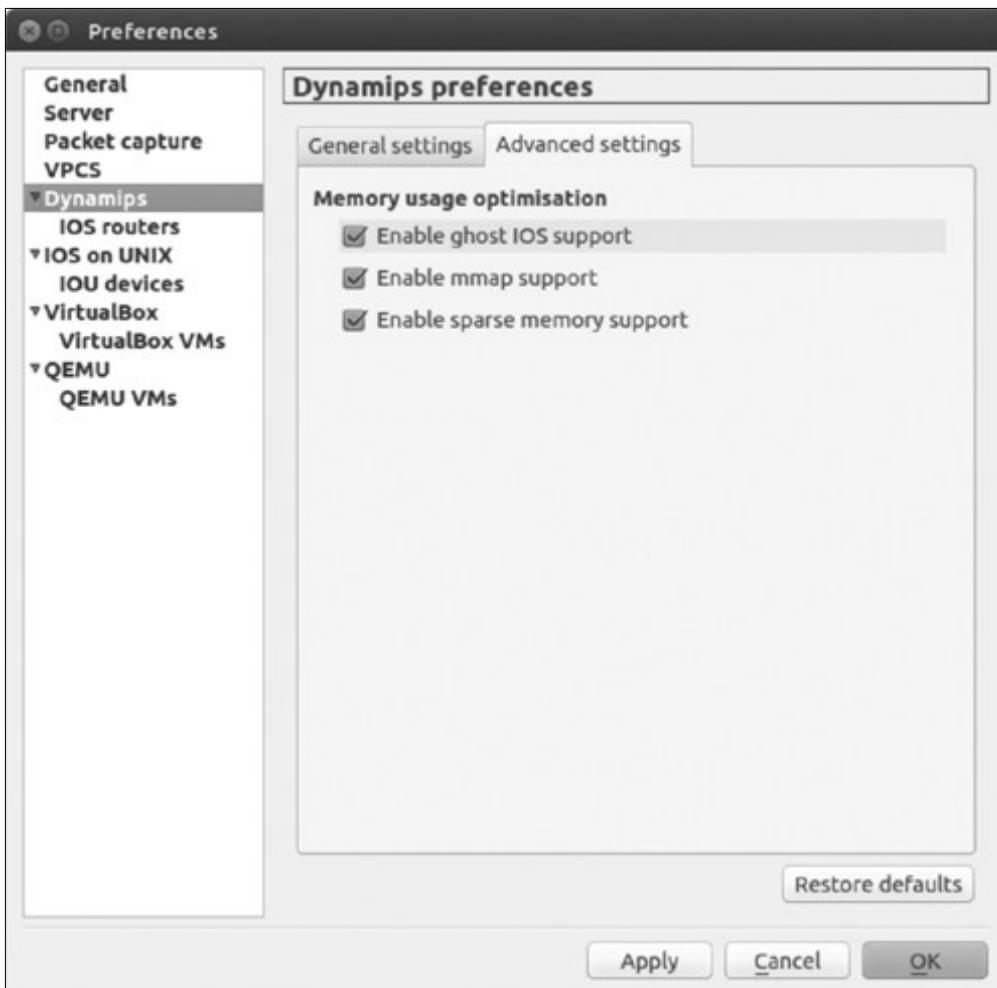


Figure 3-2: Dynamips preferences, Advanced settings tab

As opções de configurações avançadas do Dynamips relacionam-se principalmente à estabilidade do Dynamips e ao uso de memória. Como regra, você não deve alterá-las, mas discutirei as opções para que você possa decidir por si mesmo.

As configurações de otimização de uso da memória têm como objetivo conservar memória no seu PC. Quanto menos memória a Dynamips usa por roteador, mais roteadores você pode adicionar aos seus projetos. A opção Ativar suporte ao Ghost IOS reduz o consumo de memória no seu PC, alocando uma região compartilhada de memória que vários roteadores podem usar, desde que estejam executando a mesma imagem do IOS. Esse é um bom motivo para usar o mesmo modelo de roteador várias vezes em um projeto; o uso de vários modelos diferentes, com diferentes versões do IOS, consumirá mais memória do seu PC. A opção Ativar suporte a mmap permite que o conteúdo da memória do roteador seja gravado em um arquivo no disco rígido, semelhante a um arquivo de cache ou troca. A opção Ativar suporte à memória esparsa reduz a quantidade de memória virtual usada pelos roteadores, para que você possa executar mais instâncias do roteador por processo do Dynamips.

Adicionando imagens do IOS ao GNS3

Antes de começar a criar projetos usando roteadores IOS, adicione pelo menos uma imagem IOS ao GNS3. Para adicionar uma imagem do IOS, selecione **Edit ▶ Preferences** no Windows e Linux ou selecione **GNS3 ▶ Preferences** no OS X. Expanda **Dynamips** no painel à esquerda e clique em **IOS Routers**, como mostra a Figura 3-3.

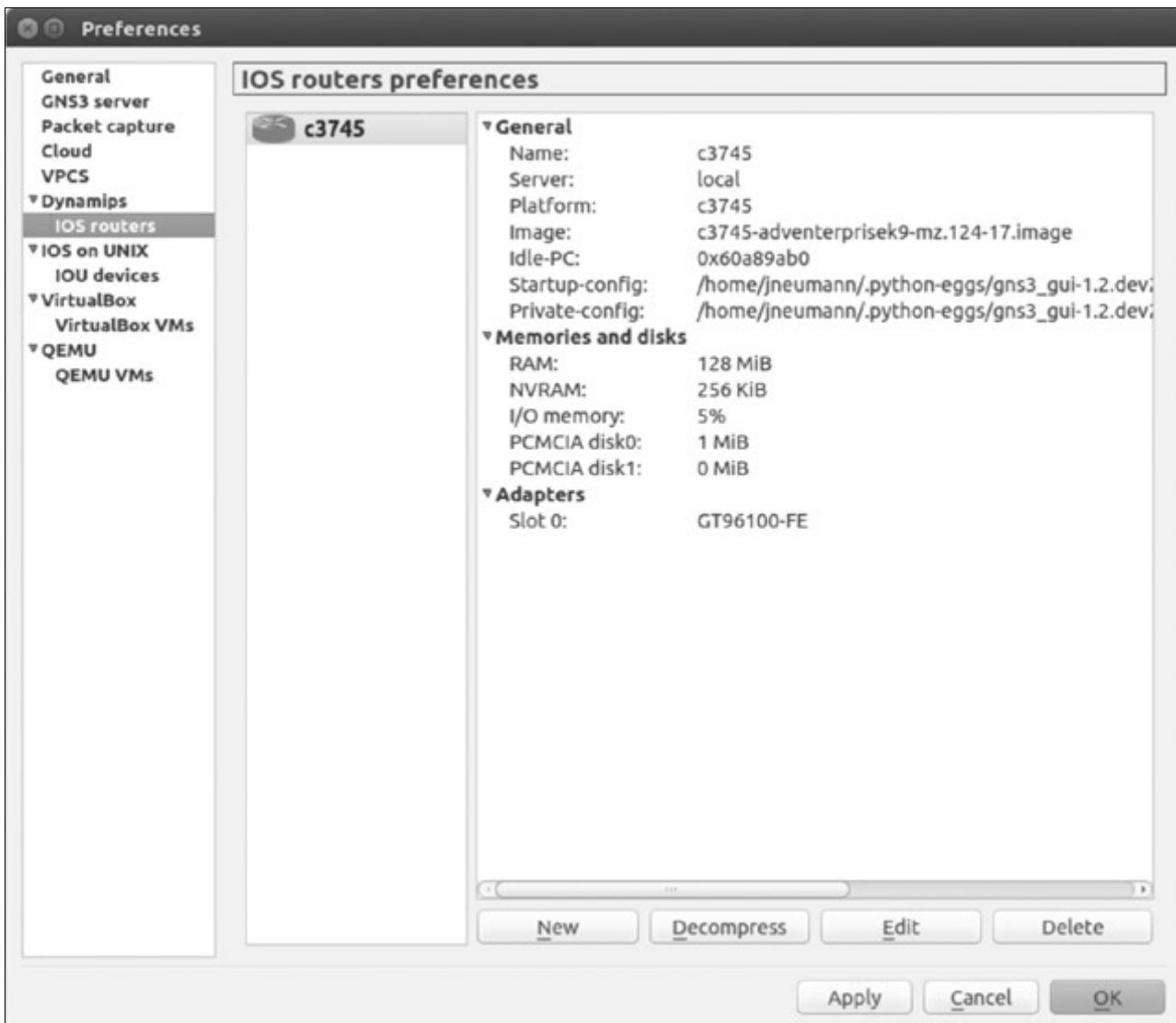


Figure 3-3: IOS routers preferences

Clique em **New** para iniciar o assistente e, em seguida, clique no botão **Browse** para localizar seu arquivo de imagem. Depois de selecionar seu arquivo de imagem, você será perguntado se deseja descompactar a imagem do IOS, como mostra a Figura 3-4.



Figura 3-4: Decidindo descomprimir o Imagem IOS

É uma boa ideia deixar o GNS3 descompactar seus arquivos de imagem; caso contrário, seus roteadores precisarão descompactar as imagens toda vez que um roteador for carregado. Descomprimir as imagens antecipadamente fará com que os roteadores sejam inicializados muito mais rapidamente. Após descompactar sua imagem, clique em Avançar e o GNS3 tentará reconhecer a plataforma do roteador à qual seu IOS pertence, conforme mostrado na Figura 3-5.

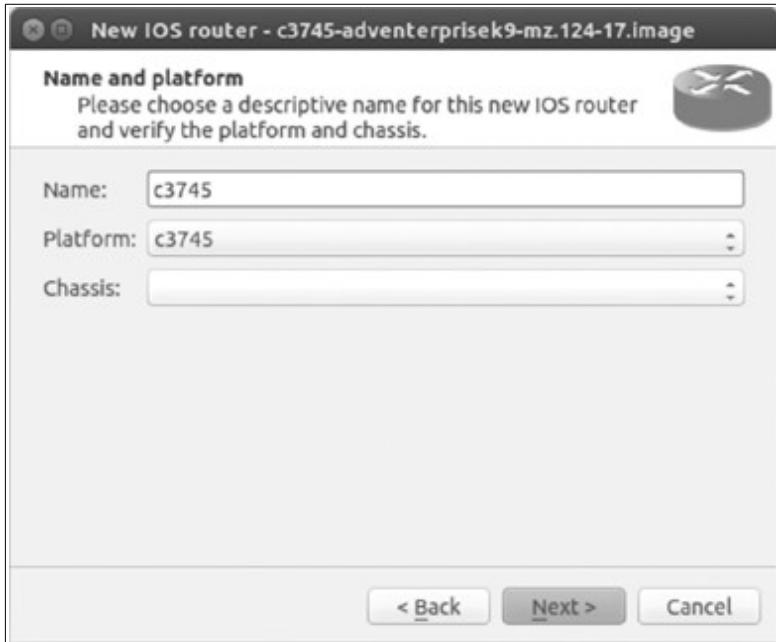


Figure 3-5: Name and platform screen

O GNS3 determinou que meu arquivo de imagem pertence a uma plataforma de roteador c3745 e o nomeou automaticamente de c3745. Se você acha que isso está incorreto, pode usar o menu suspenso Plataforma para escolher outra plataforma, mas, na minha experiência, o GNS3 faz um bom trabalho para corrigir isso. Você pode alterar o nome do seu roteador para o que quiser, digitando um nome no campo Nome.

Em geral, daqui, basta clicar em todas as definições de configuração para definir um modelo básico de roteador, mas o assistente oferece oportunidades para você personalizar a memória do roteador e outros recursos durante esse processo. Por enquanto, clique em Avançar para continuar. Você deve receber a tela Memória, mostrada na Figura 3-6.



Figure 3-6: IOS Memory screen

Seus roteadores devem funcionar bem com a configuração de memória padrão. Mas se você não tiver certeza, clique em Verificar requisitos mínimos de RAM e o GNS3 iniciará um navegador da Web e o levará à página da Web Cisco Feature Navigator em <http://www.cisco.com/>. A partir daqui, você pode procurar os requisitos de memória específicos da sua imagem IOS. Digite esse valor no campo RAM padrão. Quando terminar, clique em Avançar e você verá a tela Adaptadores de rede, como mostra a Figura 3-7.

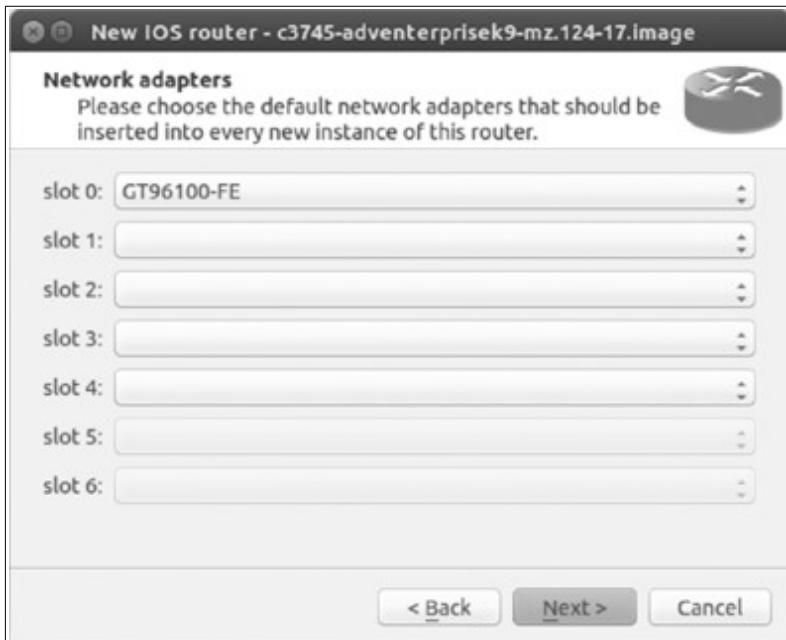


Figure 3-7: Network adapters screen

A configuração padrão configura seu roteador com as mesmas opções padrão fornecidas com um modelo real do mesmo roteador Cisco. Se você deseja adicionar mais interfaces, use o menu suspenso ao lado dos slots disponíveis e escolha os módulos de rede desejados. As opções de slot serão limitadas às opções reais disponíveis na versão real do roteador Cisco. Quando terminar, clique em Avançar e escolha os módulos WIC que você deseja instalar. Em seguida, clique em Avançar novamente para exibir a tela do Idle-PC, mostrada na Figura 3-8.



Figure 3-8: Idle-PC screen

Se você iniciar um roteador no GNS3 sem uma configuração de (Idle-PC)PC ocioso, o uso da CPU do computador aumentará rapidamente para 100% e permanecerá lá. Isso acontece porque a Dynamips ainda não sabe se o seu roteador virtual está fazendo algo que requer recursos do sistema, por isso é compensado demais, fornecendo todos os recursos possíveis. O GNS3 funcionará lentamente até que isso seja corrigido e, se o uso da CPU for mantido em 100% por um longo tempo, o processador do seu PC poderá superaquecer.

Você pode corrigir isso facilmente, fazendo com que o GNS3 procure lugares no código do programa IOS onde existe um loop inativo (loops inativos causam picos de CPU); o resultado desse cálculo é chamado de valor de PC ocioso. Quando o valor do PC inativo apropriado é aplicado, o Dynamips deve suspender o roteador periodicamente quando esses loops inativos são executados, o que reduz bastante o uso da CPU. Se você não se importa com todos os detalhes, lembre-se de que o valor do PC ocioso é o que impede a Dynamips de comer seu processador no almoço.

Para que o GNS3 encontre um valor automaticamente, clique no botão localizador de PC ocioso e o GNS3 tentará procurar um valor. Se o GNS3 encontrar um valor adequado, você está pronto. clique em Concluir. Se não der certo, deixe o campo em branco e clique em Avançar para salvar o roteador sem uma configuração de PC ocioso.

Definindo um valor manual para PC ocioso

Se o GNS3 não conseguir encontrar um valor de PC ocioso automaticamente, você precisará encontrá-lo manualmente. Você precisa calcular um valor de PC ocioso apenas uma vez por imagem do IOS. O GNS3 aplica essa configuração a todos os roteadores virtuais que usam esse arquivo de imagem. Feche a janela Preferências e arraste um roteador da barra de ferramentas Dispositivos para o espaço de trabalho do GNS3, como mostra a Figura 3-9.

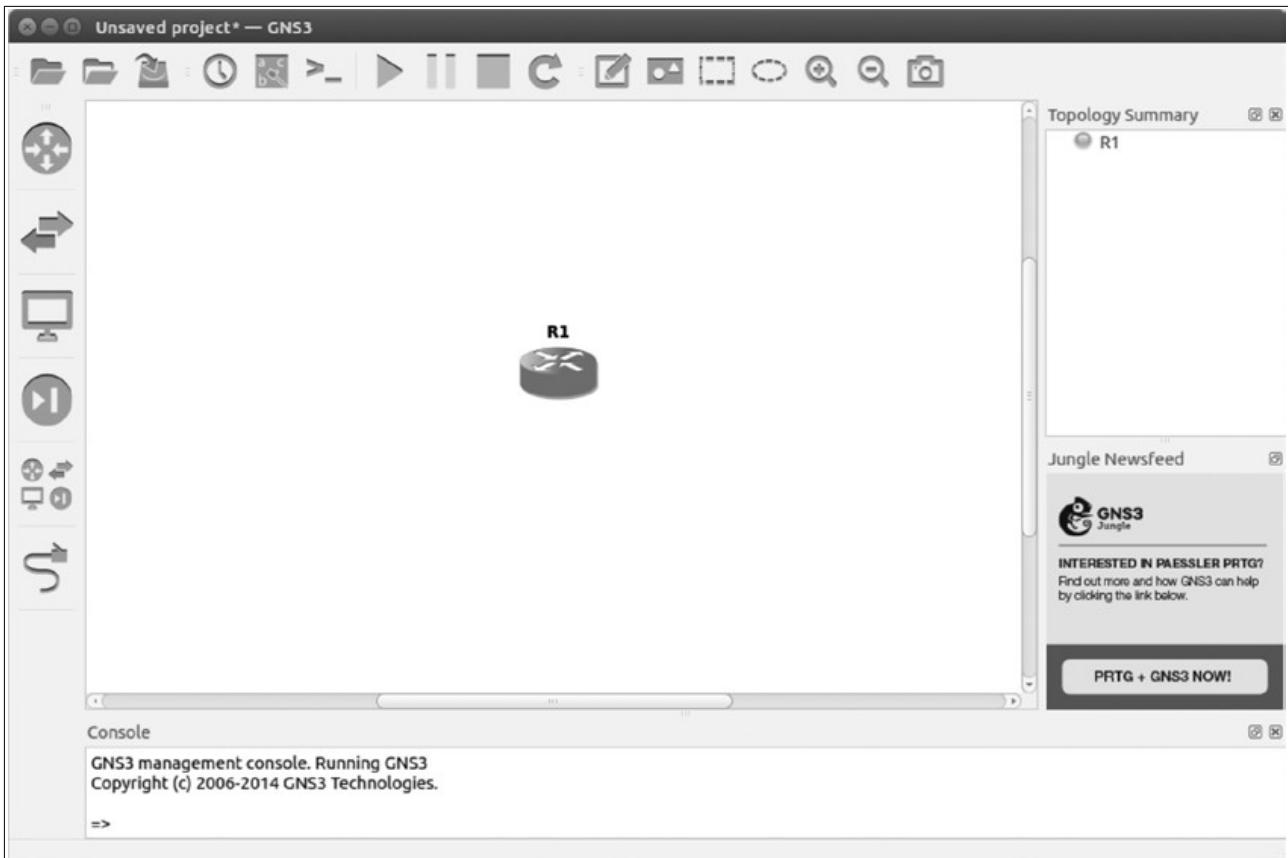


Figure 3-9: Adding a router to a blank workspace

Em seguida, initialize o roteador clicando com o botão direito do mouse no ícone do roteador e selecionando Começar; verifique se o IOS é carregado corretamente clicando com o botão direito do mouse imediatamente no roteador novamente e selecionando Console. Uma janela do console da Cisco deve abrir e exibir as mensagens de inicialização do roteador. Se o roteador inicializar corretamente, você estará pronto para iniciar o cálculo do PC ocioso. caso contrário, verifique se o modelo e as configurações padrão de RAM atribuídas ao roteador estão corretas ou tente uma imagem IOS diferente.

Se você estiver executando o Linux e um console Cisco não aparecer após selecionando Console, verifique as configurações do console GNS3. Vá para **Edit ▶ Preferences**, clique em **General** e selecione a guia **Console applications**, conforme mostrado na Figura 3-10.

Usando o menu suspenso Comandos pré-configurados, selecione seu Tipo de terminal Linux e clique em Definir, Aplicar e OK. Quando o roteador é inicializado, o uso da CPU do seu computador aumenta rapidamente para 100%. Monitore o uso da CPU para que, depois de definir um valor de PC ocioso, você possa verificar se o uso da CPU foi resolvido. No Windows, pressione ctrl-alt-del e clique em Gerenciador de tarefas para exibir o uso da CPU. No OS X, abra o programa Monitor de Atividade na pasta Aplicativos / Utilitários e clique em CPU.

Nos sistemas Linux, use o System Monitor ou digite *top* no terminal.

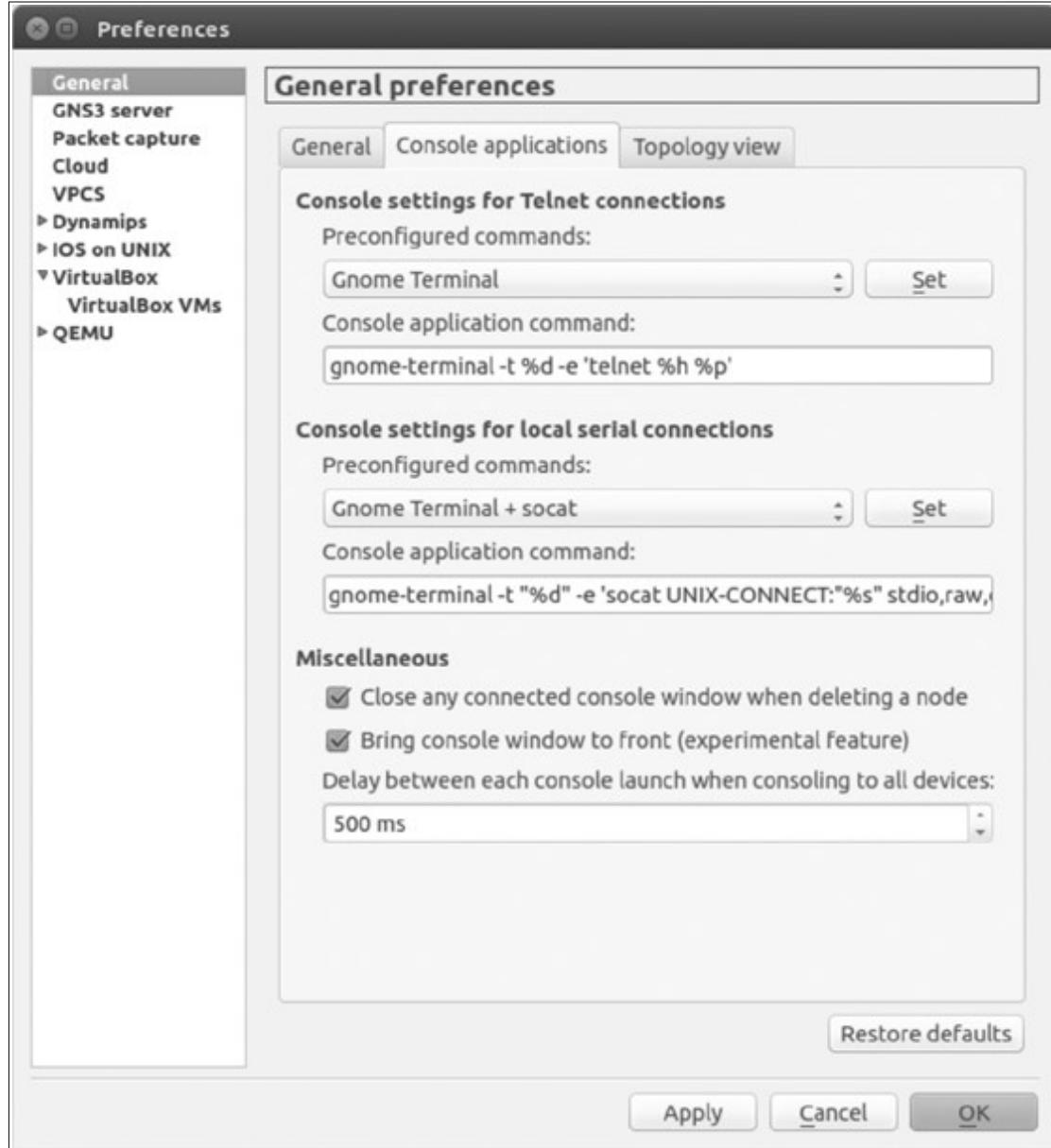


Figure 3-10: Choosing a Console application using Ubuntu Linux

Para começar a calcular um valor, clique com o botão direito do mouse no roteador e selecione PC ocioso no menu, como mostra a Figura 3-11.

O GNS3 agora deve calcular os valores do PC ocioso e fornecer um ou mais valores para você escolher. Isso pode levar um minuto, portanto, reserve um tempo para exibir os resultados na janela de valores do PC inativo, mostrada na Figura 3-12.

Se houver um asterisco (*) próximo a um determinado valor, o GNS3 determinou que esse valor é o melhor e você deve escolhê-lo. Clique em Aplicar para escolher o valor e verifique novamente o uso da CPU.

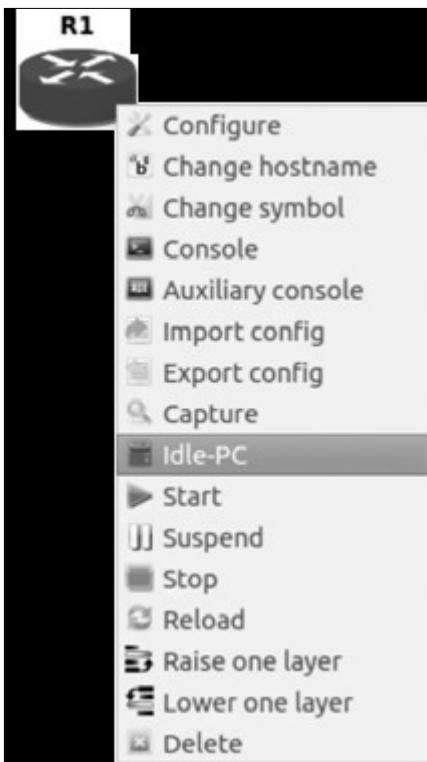


Figure 3-11: Manually calculating
Idle-PC values

Ocasionalmente, o GNS3 calcula mal o valor e o uso do processador permanece alto. Se isso acontecer, tente novamente usando um valor diferente no menu suspenso e clique em Aplicar novamente para escolher o novo valor. Se nenhum asterisco for exibido, você precisará encontrar um valor que funcione usando um método simples de tentativa e erro. Quando terminar, clique em OK para salvar o valor.

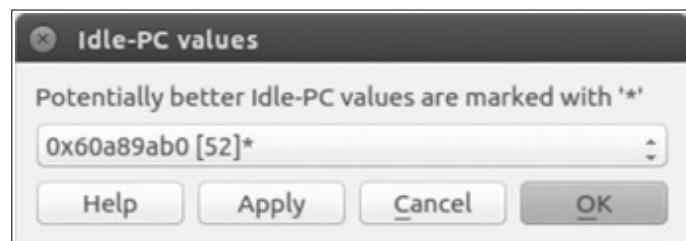


Figure 3-12: Idle-PC values

Após a aplicação de um valor de PC inativo, você está pronto para criar alguns projetos!

Pensamentos finais

Agora que você atribuiu um ou mais arquivos de imagem do IOS aos seus roteadores e configurou opções básicas no GNS3, está pronto para começar a trabalhar com seus roteadores. Você pode selecionar qualquer roteador virtual exibido na barra de ferramentas Routers Device. De uma chance. Arraste alguns roteadores para a área de trabalho, inicie-os e insira alguns comandos do IOS.

Assim como os roteadores Cisco reais, as limitações dos roteadores virtuais do Dynamips são determinadas pela versão do IOS em execução. Se você achar que está faltando um comando IOS no seu roteador ou que a sintaxe de um determinado comando não é o que você esperava, talvez seja necessário tentar uma versão diferente do IOS. Se você está estudando para o exame CCNA ou CCNP, isso não deve ser um problema, porque essas certificações exigem um conjunto bastante simples de comandos e recursos. Se você está estudando para obter uma certificação CCIE ou outra certificação avançada da Cisco, pode precisar do IOS mais recente que ofereça suporte a um conjunto de recursos mais robusto. Em caso de dúvida, visite o site da Cisco para descobrir quais recursos e recursos são suportados por um modelo de roteador ou IOS específico. A página da Web do Cisco Feature Navigator é uma ferramenta incrível que permite pesquisar informações do IOS por recursos, tecnologia, software, imagem ou código do produto, além de comparar versões de software.

Agora que você atribuiu uma imagem do IOS e configurou opções básicas no GNS3, vamos criar projetos!

4

Criando e Gerenciando Projetos

Agora que você pode configurar e iniciar um único roteador IOS, arregace as mangas e eu mostrarei como criar um projeto conectando dois ou mais roteadores em rede. Comparado ao trabalho com equipamentos de laboratório reais, é fácil criar redes virtuais e gerenciar dispositivos no GNS3. A interface do usuário funciona como uma sala de controle principal, permitindo manipular seus projetos e dispositivos de rede com apenas alguns cliques. Este capítulo mostra como usar o GNS3 para gerenciar centralmente sua rede, incluindo o hardware virtual.

Visão Geral do Gerenciamento de Projetos

Um forte recurso do GNS3 é o gerenciamento de projetos. Você pode criar um número ilimitado de designs de rede para salvar e usar sempre que precisar. Isso significa que você nunca precisará perder tempo destruindo um projeto existente para criar um novo, o que geralmente acontece quando você usa equipamento físico.

Não apenas você pode salvar vários projetos, mas também vários snapshots de uma configuração inteira do projeto. Um snapshots preserva o layout de rede do seu projeto e o estado de todas as configurações do roteador em um determinado momento. Você pode restaurar um snapshots sempre que desejar reverter todo o projeto para o estado em que estava quando o snapshots foi tirado.

NOTA

Os snapshots são úteis para a prática de exercícios de configuração CCNA ou CCNP. Você pode criar um laboratório, aplicar as configurações básicas do roteador necessárias para um drill (como endereços de rede, protocolos de roteamento etc.) e tirar um snapshots. Depois de ter um snapshots da configuração básica, você pode praticar a aplicação dos objetivos do cenário para a rede. Se você deseja praticar as mesmas tarefas novamente mais tarde, poderá reverter para o snapshots básico e seus roteadores deverão estar prontos sem configuração adicional.

O GNS3 também oferece a capacidade de gerenciar seu hardware virtual. Assim como nos roteadores reais, você pode usar os módulos de expansão da Cisco para atualizar seus roteadores virtuais. Você pode adicionar uma ampla variedade de funcionalidades, como memória RAM (Random Access Access) adicional, interfaces Ethernet, portas seriais, modo de transferência assíncrona (ATM) e portas de pacote sobre SONET (POS).

Terminologia

Antes de começar, vamos explorar algumas terminologias importantes. Você precisa saber a diferença entre uma topologia e um projeto. Um arquivo de topologia é um arquivo de texto que termina em `.gns3` e refere-se principalmente aos dispositivos e aos links entre eles. Um projeto é uma pasta de projeto definida pelo usuário (`MyLab`, por exemplo) armazenada dentro da pasta `GNS3/projects`. Uma pasta de projeto do usuário contém um arquivo de topologia denominado `<project_name>.gns3`, configurações do roteador, o conteúdo da NVRAM (memória de acesso aleatório não volátil) e outras informações salvas. Em outras palavras, representa uma rede inteira, incluindo a topologia e todas as configurações do dispositivo.

Outro termo com o qual você deve estar familiarizado é nó. Na rede de computadores, um nó é qualquer dispositivo conectado à sua rede. No GNS3, um nó é qualquer dispositivo encontrado na barra de ferramentas Dispositivos. Para ser eficiente no gerenciamento de dispositivos e projetos, você precisará de mais do que apenas vocabulário; você também precisa estar familiarizado com o layout da tela do GNS3.

Layout da tela

Vamos dar uma olhada no layout padrão do GNS3 (mostrado na Figura 4-1) e definir alguns conceitos usados pelo programa.

① GNS3 toolbar

Uma série de ícones para executar facilmente tarefas comuns.

② Devices toolbar

Usado para adicionar roteadores, comutadores, dispositivos finais e dispositivos de segurança, além de criar links entre dispositivos. Para criar topologias, selecione um tipo de dispositivo na barra de ferramentas e arraste os dispositivos da janela do dispositivo para o seu espaço de trabalho. Existem dois tipos de dispositivos: simulado e emulado. Um dispositivo simulado imita todas as características de um dispositivo real (como um nó do comutador Ethernet) e não executa um sistema operacional. Um dispositivo emulado emula o hardware de um dispositivo real e requer que um sistema operacional funcione (como roteadores Dynamips virtuais executando o Cisco IOS).

③ Console

A command line interface where you can manage aspects of your devices.

④ Topology Summary

Exibe o estado dos dispositivos em seu projeto. Um círculo verde de um dispositivo indica que ele foi iniciado, um círculo vermelho indica que um dispositivo está parado e um círculo amarelo indica que um dispositivo está suspenso. Os dispositivos simulados (como o nó do comutador Ethernet) estão sempre verdes. Para ver os links em uso em um determinado dispositivo, clique no triângulo ao lado do nome do dispositivo.

➊ Workspace

A área em que você projetará sua rede. Arraste os dispositivos da barra de ferramentas Dispositivos para a área de trabalho e os vincule.

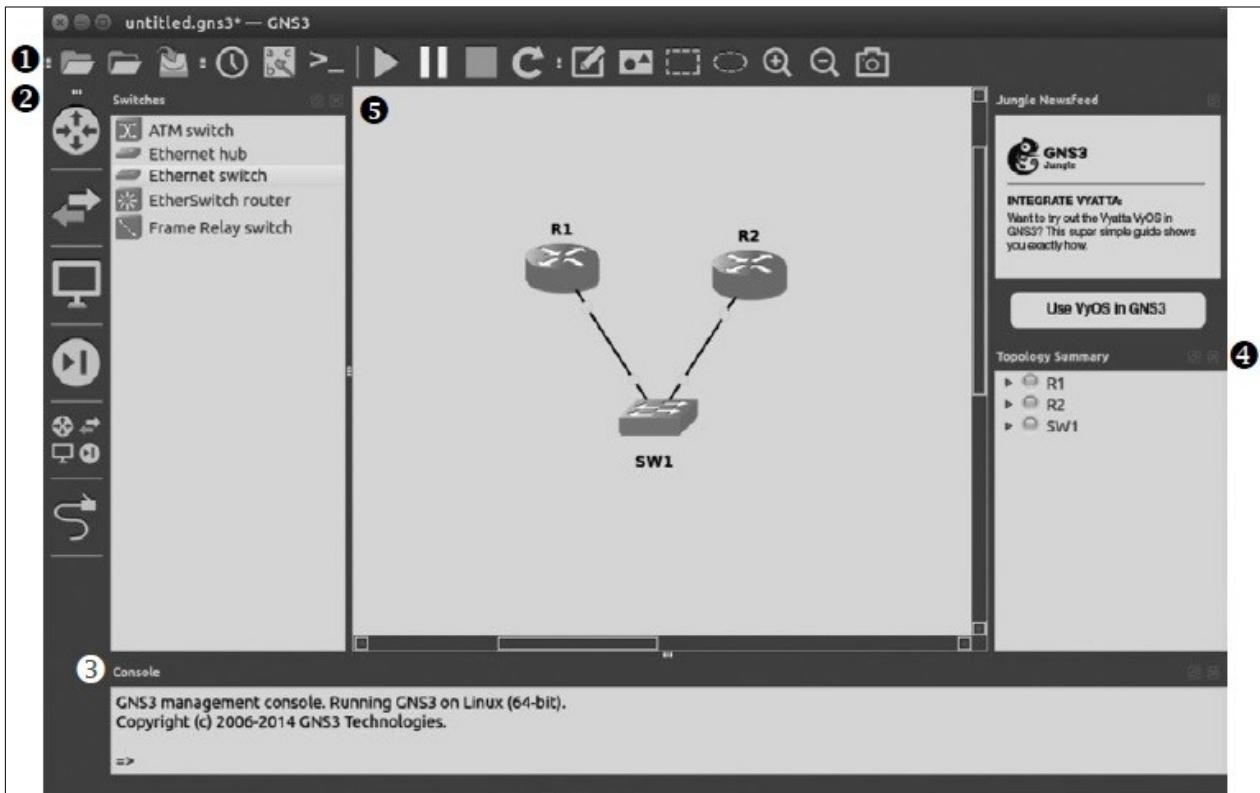


Figure 4-1: Screen layout showing two routers and a switch in the GNS3 workspace

Agora que você sabe como é a tela principal do GNS3, vejamos mais de perto nas opções que você encontrará lá.

Usando a barra de ferramentas GNS3

A barra de ferramentas do GNS3 contém vários grupos de ícones organizados aproximadamente por função e oferecem uma maneira simples de fazer as coisas. O primeiro grupo lida com projetos, o segundo com links, o terceiro com dispositivos e snapshots e o quarto com outras maneiras de organizar visualmente seus projetos.

Primeiro grupo da barra de ferramentas

O primeiro grupo de ícones da barra de ferramentas, mostrado na Figura 4-2, lida com ações que afetam projetos inteiros. Da esquerda para a direita, esses ícones são os seguintes:



Figure 4-2: First toolbar group

New blank project

Cria uma nova pasta do projeto e permite escolher o nome seu projeto.

Open project

Abre um projeto salvo anteriormente. Para abrir um projeto, escolha o nome da pasta do projeto e selecione o arquivo chamado `<project_name>.gns3`.

Save project

Salva um projeto completo na pasta de projetos GNS3. Por padrão, um arquivo de imagem PNG do seu espaço de trabalho é salvo com o seu projeto.

Segundo grupo da barra de ferramentas

Os botões no segundo grupo de ícones da barra de ferramentas, mostrados na Figura 4-3, permitem criar snapshots do projeto, mostrar ou ocultar rótulos de interface e conectar-se aos seus dispositivos usando a porta do console virtual em seus dispositivos. Da esquerda para a direita, esses ícones são os seguintes:



Figure 4-3: Second toolbar group

Snapshot

Cria um Snapshot de seus dispositivos, links, e configurações do IOS para registrar o estado do seu espaço de trabalho naquele momento. Você pode salvar mais de um Snapshot e reverter para um Snapshot salvo a qualquer momento. As opções são Criar, Excluir, Restaurar e Fechar.

Show interface labels

Mostra ou oculta os nomes de interface usados por um link. Esses rótulos são abreviados e exibidos com dispositivos em sua área de trabalho (por exemplo, f0/0 é exibido para FastEthernet0/0).

Console connect to all devices

Abre uma conexão de console para todos os roteadores em execução no seu espaço de trabalho.

NOTA

Quando você abre uma conexão de console a todos os dispositivos, sua tela pode ficar cheia de janelas abertas, a menos que o seu terminal suporte sessões com guias. Ao lidar com topologias grandes, talvez seja mais fácil abrir e fechar sessões únicas, conforme necessário, clicando com o botão direito do mouse em um nó do dispositivo e escolhendo Console.

Terceiro grupo da barra de ferramentas

O terceiro grupo de ícones da barra de ferramentas, mostrado na Figura 4-4, lida principalmente com dispositivos de controle. Da esquerda para a direita, esses quatro ícones são os seguintes:



Figure 4-4: Third toolbar group

Start/Resume all devices

Inicia todos os dispositivos parados ou retoma todos os dispositivos suspensos no seu espaço de trabalho.

Suspend all devices

Coloca todos os dispositivos com capacidade de suspensão em um estado suspenso.

Stop all devices

Pára todos os dispositivos.

Reload all devices

Recarrega todos os dispositivos. Certifique-se de salvar as configurações e o projeto do roteador antes de recarregar, caso contrário você poderá perder as configurações!

Quarto grupo da barra de ferramentas

O grupo final de ícones da barra de ferramentas, mostrado na Figura 4-5, fornece ferramentas para apresentar seus layouts de rede com mais clareza. Você pode adicionar objetos como retângulos e elipses ao seu projeto e até gerar uma captura de tela do seu espaço de trabalho.



Figure 4-5: Fourth toolbar group

Da esquerda para a direita, os ícones no último grupo da barra de ferramentas são os seguintes:

Add a note

Cria anotações de texto no seu espaço de trabalho. Clique duas vezes no texto para modificá-lo e clique com o botão direito do mouse no objeto de texto para alterar os atributos de Estilo (como tamanho e cor da fonte). Você também pode girar objetos de texto de 0 a 360 graus.

Insert a picture

Adiciona imagens e logotipos aos seus projetos. O GNS3 suporta os formatos de arquivo PNG, JPG, BMP, XPM, PPM e TIFF.

Draw a rectangle

Desenha retângulos dinamicamente redimensionáveis. Você pode clicar com o botão direito do mouse em um objeto retangular para alterar os atributos de estilo da borda e da cor da borda. Objetos retangulares podem ser girados de 0 a 360 graus.

Draw an ellipse

Desenha elipses dinamicamente dimensionáveis. Você pode clicar com o botão direito do mouse em um objeto de elipse para alterar o estilo e a cor da borda.

Zoom in

Aplica zoom no seu espaço de trabalho para ver detalhes.

Zoom out

Reduz o zoom da sua área de trabalho para uma maior visão aérea.

Screenshot

Gera uma captura de tela do seu espaço de trabalho. A imagem pode ser salva como um arquivo PNG, JPG, BMP, XPM, PPM ou TIFF e, por padrão, é salva na sua pasta *GNS3/projects*.

Estilos e encaixes de janelas

O GNS3 fornece vários estilos de janela para você escolher. Para alterar o estilo padrão, selecione **Edit ▶ Preferences** no Linux e Windows ou selecione **GNS3 ▶ Preferences** no OS X. Selecione a categoria **General**, selecione a guia **General** e use o menu suspenso em **Estilo** para escolher seu novo estilo padrão. Clique em **Aplicar** e em **OK** para ativar sua alteração. O GNS3 lembrará sua seleção entre as reinicializações do programa. As docas das janelas, por outro lado, são as janelas que cercam o espaço de trabalho do GNS3. O GNS3 exibe as docas de resumo do console e da topologia por padrão. Para visualizar ou ocultar um encaixe da janela, selecione **View ▶ Window Docks** e selecione o encaixe que deseja exibir; qualquer estação com uma marca de seleção ao lado do nome deve aparecer na tela. Para redimensionar uma doca, clique na borda da janela onde ela se conecta à área de trabalho e arraste a borda até atingir o tamanho desejado.

Objetos (anotações, figuras e formas) que você adicionar ao seu espaço de trabalho pode ser agrupado em camadas. Para aumentar ou diminuir um objeto, clique com o botão direito do mouse no objeto e selecione **Raise one layer** ou **Lower one layer**. Esse recurso permite manipular objetos em uma camada sem afetar outras. Você pode exibir posições de camada para seus objetos escolhendo **View ▶ Show Layers** no menu, o que é útil durante a manipulação avançada de camadas.

Adicionando formas e cores com esta barra de ferramentas, você pode dividir os componentes de rede em grupos lógicos. Com o texto, você pode adicionar notas e lembretes sobre como o seu projeto está configurado. A Figura 4-6 mostra como você pode apresentar informações mais claramente usando formas, cores e mensagens de texto anotadas.

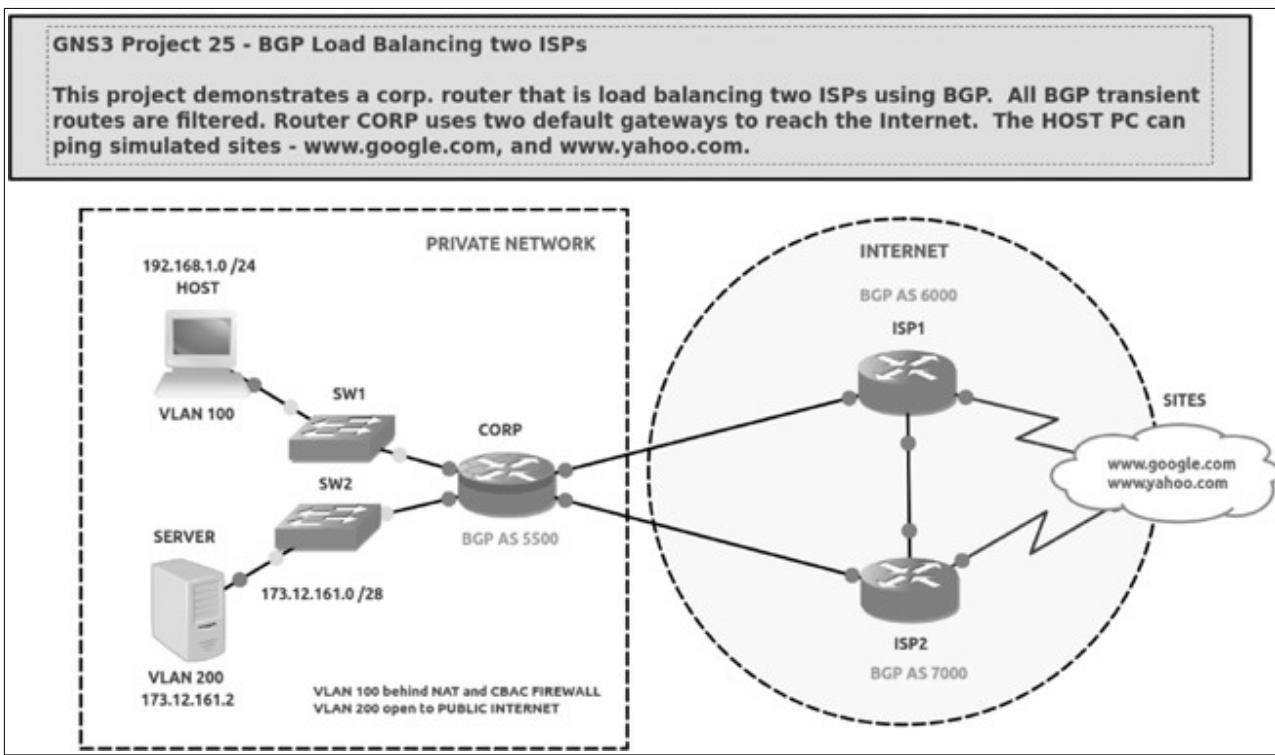


Figure 4-6: Sample project with annotations

Depois de criar vários projetos, é fácil esquecer como você os configurou ou quais eram seus objetivos. A adição de notas (como a útil na Figura 4-6) é uma maneira simples de se lembrar rapidamente dessas informações, especialmente depois de algumas semanas ou meses. As notas são incríveis-use-as!

Usando a barra de ferramentas Dispositivos

A barra de ferramentas Dispositivos (mostrada na Figura 4-7) organiza os dispositivos por função. Clique em um ícone na barra de ferramentas Dispositivos para ver todos os dispositivos nesse grupo de dispositivos.



Figure 4-7: Devices toolbar

Para adicionar um nó de dispositivo ao seu projeto, clique em um ícone na barra de ferramentas Dispositivos para exibir uma lista de dispositivos configurados e, em seguida, arraste um dispositivo para sua área de trabalho. Você pode pressionar **shift** para adicionar vários dispositivos idênticos. Da esquerda para a direita, os tipos de dispositivos na barra de ferramentas são os seguintes:

Routers

Exibe todos os nós do roteador Dynamips disponíveis que foram configurados com um arquivo de imagem IOS válido, bem como roteadores IOU L3.

Switches

Exibe todos os nós de comutador disponíveis, incluindo comutador Ethernet switch, Ethernet hub, ATM switch, Frame Relay switch, EtherSwitch router, e IOU L2 switches.

End Devices

Exibe todos os dispositivos finais disponíveis, incluindo convidados QEMU, convidados VirtualBox, host e cloud.

Security Devices

Exibe todos os dispositivos de segurança disponíveis, incluindo firewall ASA, IDS / IPS e todos os nós personalizados que você criou.

All Devices

Exibe todos os dispositivos disponíveis na barra de ferramentas Dispositivos.

Add a Link

Quando essa opção é selecionada, o ponteiro do mouse muda para uma cruz, indicando que você pode vincular dois dispositivos usando suas interfaces virtuais. Para vincular dispositivos, clique no primeiro dispositivo e selecione uma interface; depois repita para o segundo dispositivo para concluir a conexão.

Clique no ícone All Devices e agora você verá uma janela contendo todos os dispositivos configurados no GNS3. Você pode arrastar qualquer um dos dispositivos para o seu espaço de trabalho e usá-los em seu projeto.

Criando seu primeiro projeto

Agora que você conhece a interface do GNS3, vamos analisar alguns detalhes do gerenciamento de projetos. Abordarei a maneira mais fácil de fazer as coisas, mas lembre-se de que o GNS3 geralmente oferece mais de uma maneira de fazer as coisas.

Quando você inicia o GNS3, uma janela Novo projeto é exibida, conforme mostrado em Figura 4-8. A partir daqui, você pode abrir um projeto existente ou criar um novo.

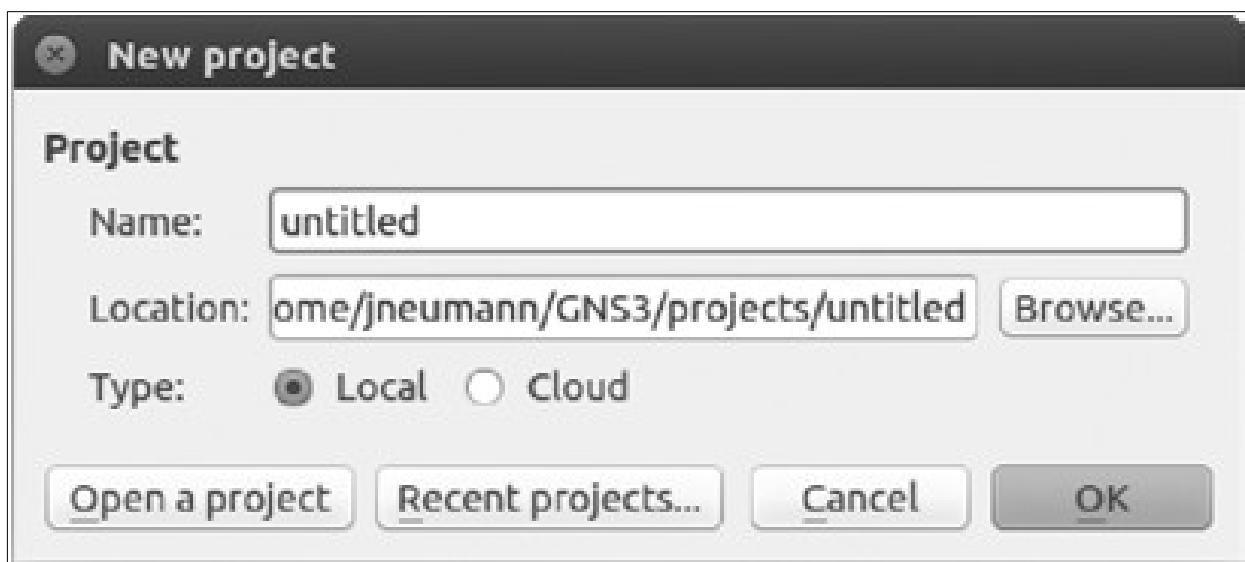


Figure 4-8: New project window

Para criar um novo projeto, substitua *untitled* pelo nome do seu projeto e clique em **OK**. Se você já está no GNS3, selecione **File ▶ New** para criar um novo projeto. Depois de criar um novo projeto GNS3, é hora de criar uma topologia, começando com alguns roteadores Dynamips.

Trabalhando com roteadores

Comece um projeto arrastando alguns roteadores da barra de ferramentas Dispositivos para o espaço de trabalho do GNS3. Se você pressionar **Shift** ao adicionar dispositivos, verá uma caixa de diálogo que permite adicionar vários dispositivos idênticos. Tente adicionar o primeiro par de roteadores dessa maneira. Se você não encontrar nenhum roteador na barra de ferramentas Dispositivos, consulte "Configurando o seu primeiro roteador IOS" na página 21 para saber como adicionar dispositivos ao GNS3.

Depois de adicionar os roteadores ao seu espaço de trabalho, eles devem ser nomeados R1 e R2 automaticamente. Os roteadores obtiveram seus nomes no comando *hostname% h* encontrado no arquivo GNS3 *ios_base_startup-config.txt*. Este arquivo contém configurações padrão do IOS aplicadas a todos os roteadores e atribuídas a um dispositivo quando ele é configurado com um arquivo de imagem do IOS. Para localizar os arquivos de configuração do Dynamips, vá para **Preferences**, escolha **Dynamips** no painel à esquerda e escolha **IOS Routers**. Selecione um roteador configurado e clique em **Edit** para exibir as opções de configuração do Dynamips IOS Router, mostradas na Figura 4-9.

A partir daqui, você pode verificar o caminho para a configuração de inicialização do seu dispositivo e arquivos de configuração privada. Quando um roteador é colocado em sua área de trabalho, o conteúdo do arquivo de configuração de inicialização *ios_base_startup-config.txt* é aplicado à configuração de inicialização do roteador e

carregado na configuração em execução do roteador quando o roteador é iniciado. Se você deseja criar parâmetros personalizados aplicados globalmente aos seus roteadores (por exemplo, para abrir automaticamente uma interface ou usar um nome de usuário e senha pré-atribuídos), use um editor de texto para modificar e salvar o arquivo *ios_base_startup-config.txt*. Você pode aplicar quaisquer comandos válidos do Cisco IOS ao arquivo, desde que o seu IOS os suporte, é claro. Você não precisa modificar o arquivo *ios_base_private-config.txt*. Este arquivo foi instalado pelo GNS3 para que você possa usar o Secure Shell (SSH) entre as reinicializações do roteador, sem precisar gerar novas chaves de criptografia nos roteadores.

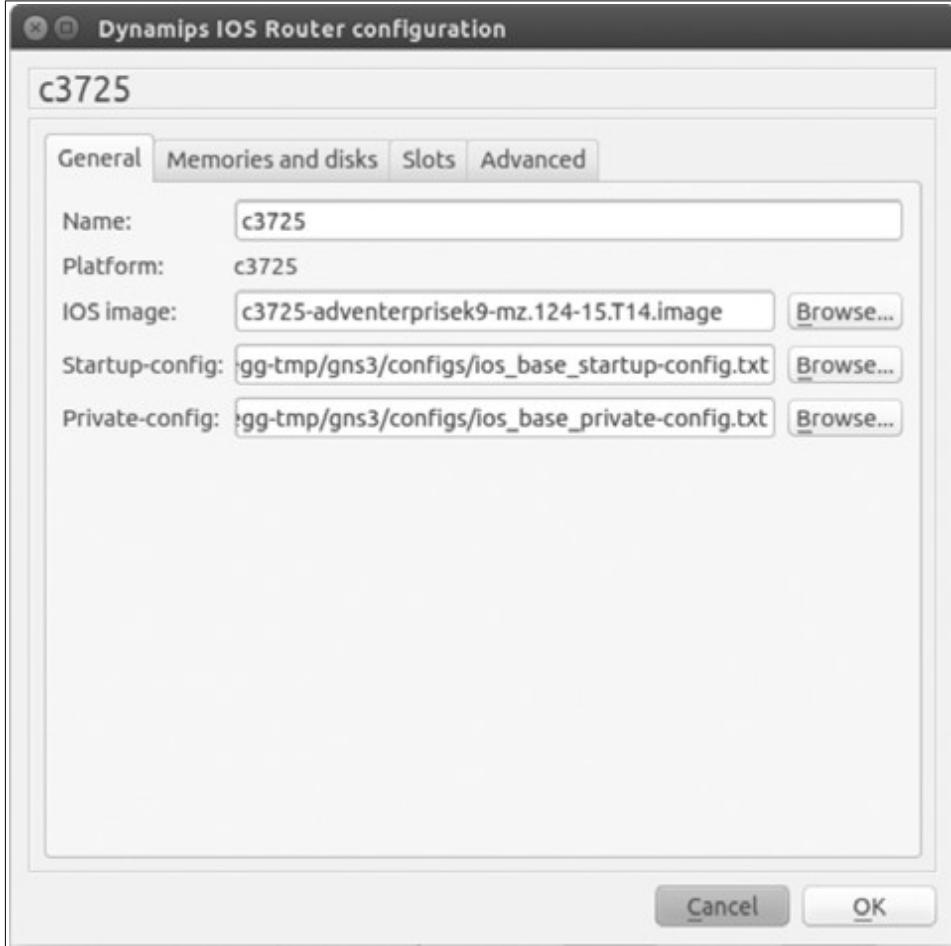


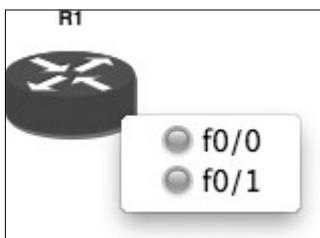
Figure 4-9: Dynamips IOS Router configuration dialog

É importante observar que as alterações que você faz são aplicadas apenas a roteadores adicionados a novos projetos e não podem ser aplicados retroativamente a roteadores em seus projetos salvos anteriormente.

AVISO

*Antes de modificar o arquivo *ios_base_startup-config.txt*, você pode salvar uma cópia de backup. Se você digitar comandos inválidos, seus roteadores poderão gerar erros e se comportar mal.*

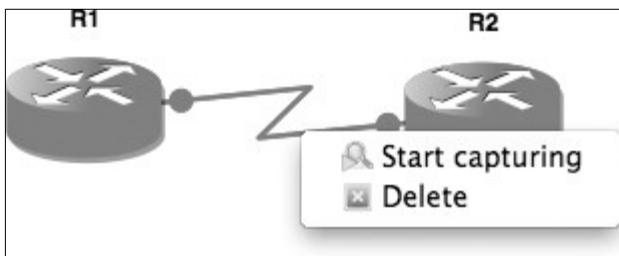
Criando links entre seus roteadores



Depois de colocar dispositivos no seu espaço de trabalho, você precisará adicionar links entre eles para criar uma rede totalmente funcional. Isso é equivalente a cabear uma rede real, exceto pelo fato de você estar usando cabos virtuais em vez de cabos físicos. Para adicionar links aos seus dispositivos, clique no ícone Adicionar um link na barra de ferramentas Dispositivos. Seu cursor deve mudar para uma mira, indicando que você pode selecionar dispositivos. Para criar um link, clique em um dispositivo. Você verá um menu suspenso de interfaces disponíveis, como mostra a Figura 4-10.

Figure 4-10: A router with two FastEthernet interfaces

Um círculo vermelho ao lado de uma interface indica que está disponível para uso; um círculo verde indica que a interface já está sendo usada por um link existente. Selecione qualquer interface disponível para estabelecer o link e, em seguida, selecione uma interface em outro dispositivo para concluir a conexão. Você pode criar conexões apenas entre dois tipos de interface compatíveis. Em outras palavras, assim como no hardware físico, você não pode conectar um cabo serial a uma interface Ethernet.



Em algum momento, você pode querer quebrar um link entre dois dispositivos para simular uma interrupção, reconfigurar sua rede ou por algum outro motivo. Para quebrar um link entre dois dispositivos, clique com o botão direito do mouse no link e selecione **Delete**, conforme mostrado na Figura 4-11. Para restabelecer um link, clique no ícone **Add a link** novamente e escolha os mesmos dispositivos.

Figure 4-11: Deleting links between devices

Configurando hardware virtual

Quando você coloca roteadores virtuais no seu espaço de trabalho, eles têm as mesmas opções de configuração que foram aplicadas quando você configurou a imagem IOS do dispositivo. Mas isso não significa que seus roteadores estão presos a essa configuração. Assim como os PCs, os roteadores Cisco possuem portas de expansão para fornecer funcionalidade adicional, e os roteadores GNS3 Dynamips oferecem as mesmas opções de expansão que suas contrapartes físicas. Para modificar a configuração de hardware de um roteador, clique com o botão direito do mouse no roteador e selecione **Configure**; depois clique no nome do nó (R1, por exemplo), como mostra a Figura 4-12.

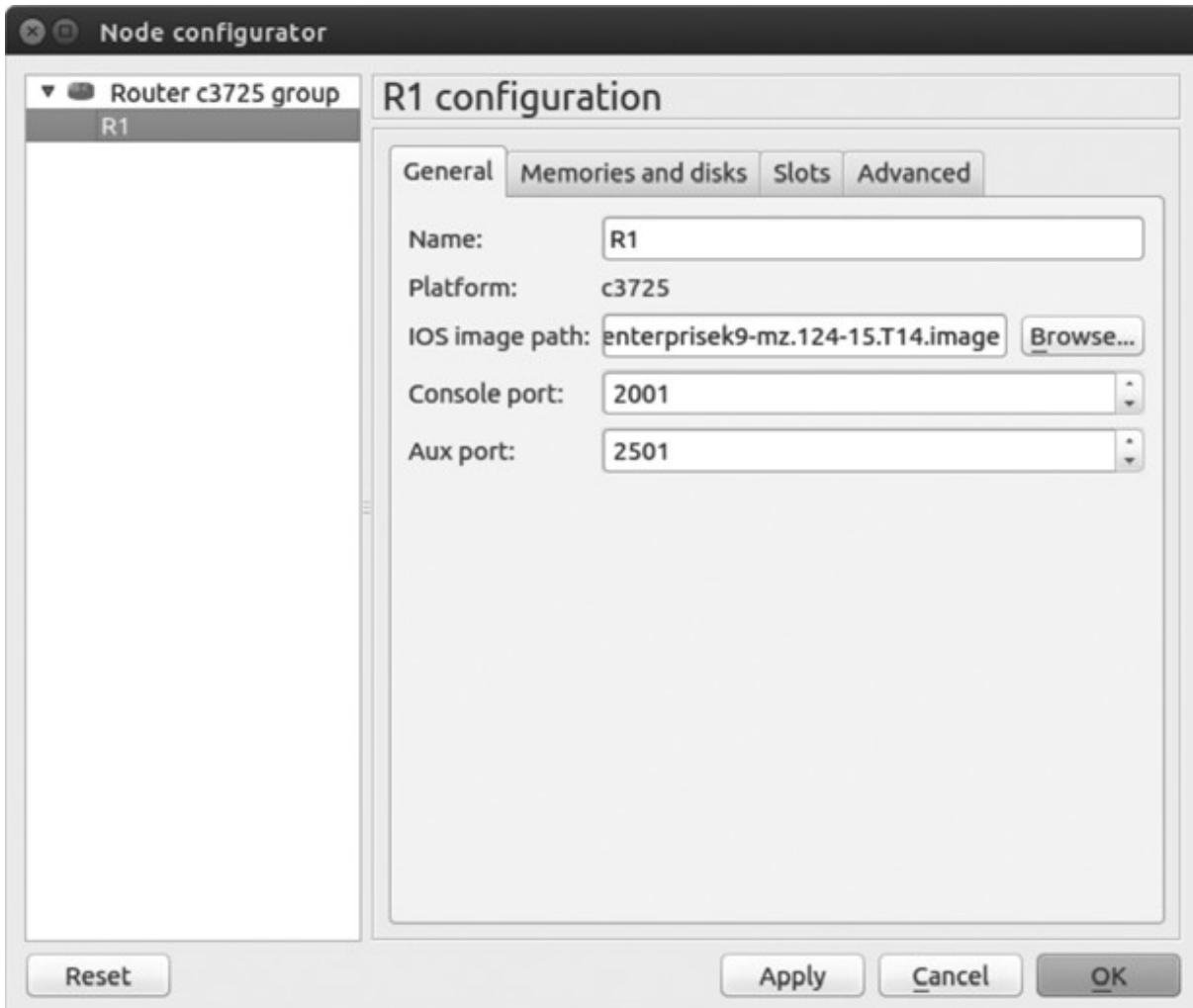


Figure 4-12: Cisco IOS router Node configurator dialog

Na caixa de diálogo Configurador do nó, você deve ver as opções de configuração disponíveis para esse modelo de roteador. Os modelos básicos permitem adicionar apenas opções simples, como placas Cisco SLOT, WIC ou RAM, enquanto os modelos mais avançados permitem definir recursos como o tipo de chassi ou um tipo NPE (Network Processing Engine) que pode ser encontrado no Cisco Roteadores da série 7200.

Você pode configurar e aplicar as mesmas opções de dispositivo para memória e slots que foram abordados no Capítulo 3, mas as alterações feitas aqui serão aplicadas apenas aos dispositivos ou grupo de dispositivos que você escolheu no seu projeto. Todos os outros dispositivos permanecerão inalterados.

Iniciando, parando e pausando roteadores

Eu mostrei como iniciar e parar os roteadores clicando com o botão direito do mouse em um roteador e escolhendo Iniciar ou Parar, mas você também pode suspender seu roteador clicando com o botão direito do mouse e escolhendo Suspender. Suspender um roteador é útil quando você deseja simular uma falha sem precisar passar pelo processo de salvar sua configuração, parar o roteador e reiniciá-lo. De fato, parar e reiniciar repetidamente os roteadores GNS3 pode causar falhas no Dynamips com algumas versões do IOS, por isso, recomendo suspender e continuar.

O recurso de suspensão realmente brilha nos testes de convergência de rede. Você pode simular rapidamente falhas e recuperações para testar protocolos de roteamento como o **RIP (Routing Information Protocol)**, **EIGRP** e **OSPF**, bem como protocolos de redundância como **HSRP**, **VRRP (Virtual Router Redundancy Protocol)** e **Gateway Load Balancing Protocol (GLBP)**. Para simular uma falha, clique em Suspender e monitore seus outros roteadores para verificar se ocorreu o failover ou a convergência.

Para simular uma recuperação, reinicie o roteador clicando com o botão direito do mouse no dispositivo e escolhendo Iniciar. Devido às limitações de taxa de transferência colocadas no Dynamips por causa da emulação, o failover ou a convergência podem demorar um pouco mais do que você costumava usar ao usar hardware real. Não se preocupe, isso é totalmente normal. É claro que, mesmo que você possa iniciar e interromper seus roteadores, não poderá fazer muito com eles até fazer logon em um console.

Fazendo logon em roteadores

Você faz logon nos roteadores usando a porta do console simulada. Se isso soa familiar, é porque também é assim que você faz logon no equipamento real da Cisco. Em um hardware físico, a porta do console é onde você conecta o pequeno cabo serial azul do console da Cisco. Verifique se o roteador foi iniciado antes de abrir uma conexão do console; caso contrário, você não verá uma tela de console.

Definindo as configurações do terminal

Esteja você executando o Windows, OS X ou Linux, existem vários tipos de terminais disponíveis para uso com o GNS3. Mas por que você prefere um ao outro? Um motivo pode ser que você instalou no seu sistema. No Linux, por exemplo, você pode estar usando o Gnome Desktop, que possui o gnome-terminal instalado por padrão. Se for esse o caso, convém modificar a configuração do terminal GNS3 para usar o gnome-terminal. Outro motivo é que alguns programas de terminal oferecem mais recursos que outros. Você pode escolher um tipo de terminal que permita o uso de janelas com guias, por exemplo, para poder abrir mais de um console por vez, sem um monte de janelas abertas bagunçando a tela. Para modificar as configurações do terminal, vá para Preferences, clique em General e, em seguida, clique na guia Console applications para exibir a janela mostrada na Figura 4-13. A partir daqui, você pode escolher um tipo de terminal predefinido e personalizar as configurações de comando em Comando do aplicativo de console. (Verifique a documentação do aplicativo do terminal para descobrir quais opções estão disponíveis no seu sistema.) Quando terminar, clique em Set, depois em Apply e em OK.

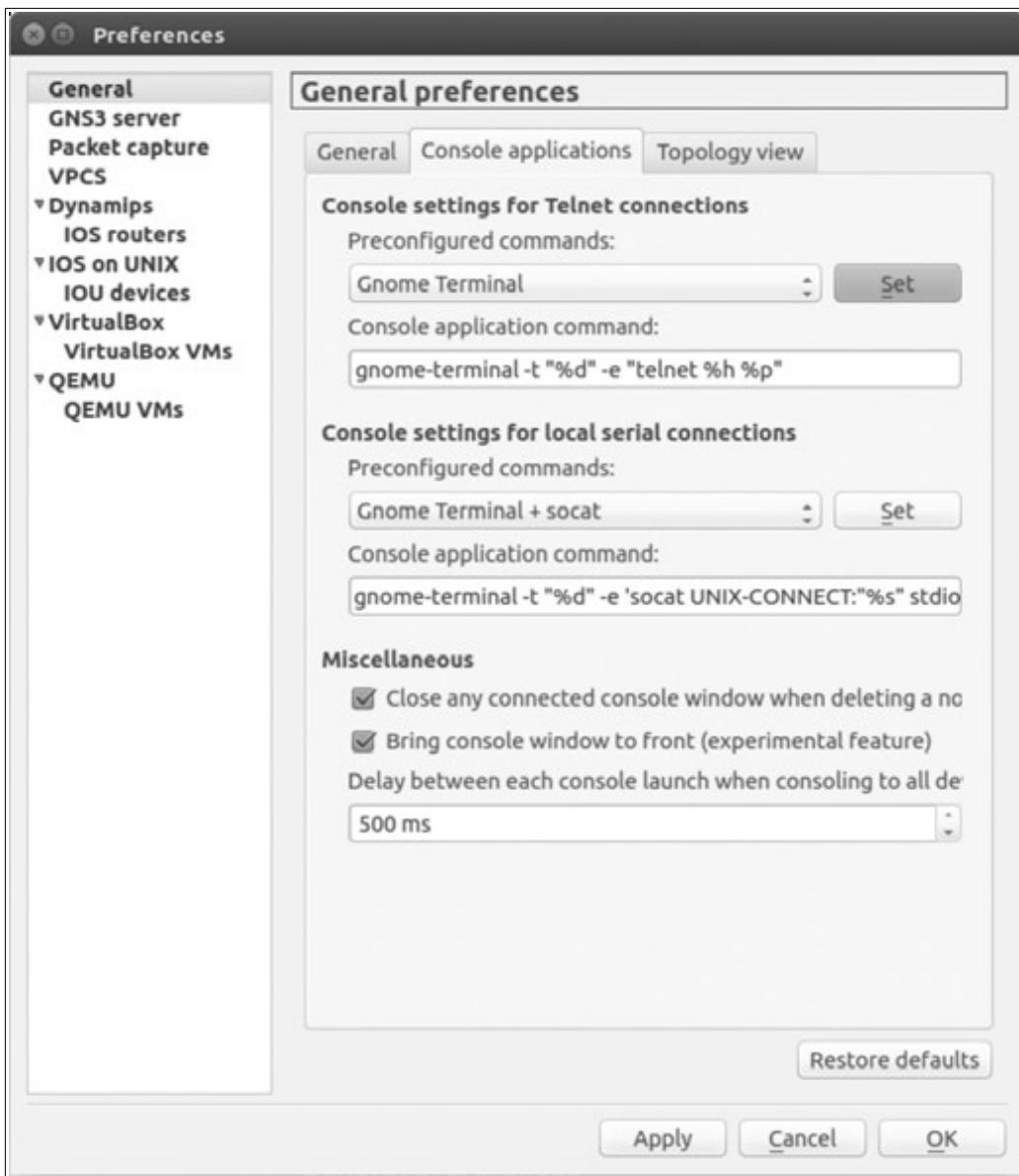
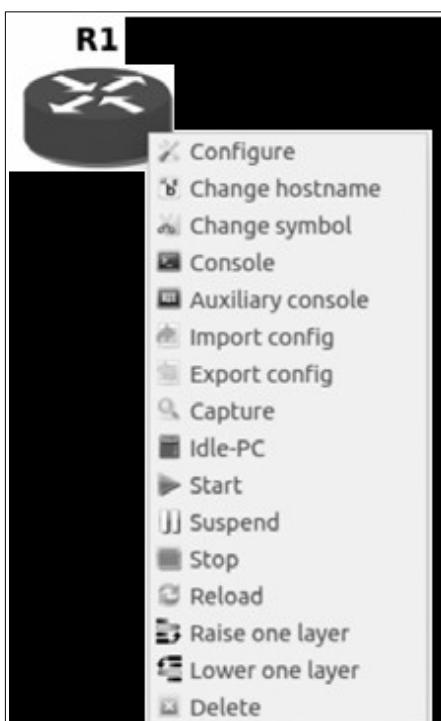


Figure 4-13: Terminal settings



Para fazer logon em todos os seus roteadores ao mesmo tempo, clique no ícone Console conectar a todos os dispositivos no segundo grupo da barra de ferramentas (consulte a Figura 4-3 na página 34). Para fazer logon em um único roteador, clique com o botão direito do mouse no nó do roteador no seu espaço de trabalho e selecione Console ou Console auxiliar no menu (veja a Figura 4-14).

Para alterar o número da porta TCP (Transmission Control Protocol) na qual o console de um roteador ou a porta AUX escuta, clique com o botão direito do mouse no dispositivo no seu espaço de trabalho, clique em **Configure** e selecione a guia **General**. O número da porta que você escolher deve ser exclusivo para todos os dispositivos no GNS3 e no seu PC. Como regra, tente não mexer com números de porta, a menos que seja necessário. O GNS3 faz um bom trabalho em mantê-los em linha reta, e sujar com eles pode causar dores de cabeça. Mas se algum outro aplicativo TCP/IP em execução no seu PC entrar em conflito com o GNS3, talvez seja necessário fazer algumas alterações antes de fazer logon no seu roteador.

Figure 4-14: Choose **Console** or **Auxiliary console** to connect to a router

NOTA

Use o comando netstat no seu PC para verificar quais portas TCP/IP já estão em uso.

Depois de estabelecer uma conexão do console ao roteador, você verá uma janela familiar do console da Cisco.

```
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^J'.
Connected to Dynamips VM "R1" (ID 1, type c3725) - Console port
Press ENTER to get the prompt.
ROMMON emulation microcode.
```

```
Cisco 1720 (MPC860) processor (revision 0x202) with 55206K/9830K bytes of memory.
Processor board ID FTX0945WOMY (4279256517), with hardware revision 000
M860 processor: part number 0, mask 0
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
4096K bytes of processor board System flash (Read/Write)
```

```
SETUP: new interface FastEthernet0 placed in "shutdown" state
```

```
Press RETURN to get started!
00:00:02: %LINK-5-CHANGED: Interface FastEthernet0, changed state to administratively down
00:00:03: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0, changed state to down
R1#
```

Neste ponto, você pode começar a usar comandos IOS padrão para configurar o roteador. Um comando que pode parecer estranho é o comando *show flash*. Normalmente, este comando exibe arquivos salvos na memória flash, como o arquivo de imagem IOS do roteador e outros arquivos padrão da Cisco. No GNS3, no entanto, você notará que não há arquivos salvos aqui por padrão. Além disso, a unidade flash pode não estar formatada; se for esse o caso, você precisará emitir o comando *erase flash*: antes de salvar os arquivos na memória flash. Caso contrário, você poderá receber um erro semelhante ao seguinte:

```
%Error opening slot0:router-config (Bad device info block)
```

NOTA

Se você usa um módulo de chave NM-16ESW, pode ser necessário apagar a memória flash do seu roteador antes de criar VLANs; caso contrário, o banco de dados da VLAN (*vlan.dat*) não poderá ser salvo.

Esta seção foi sobre roteadores Dynamips até agora, mas você pode também usar switches nos seus projetos GNS3, que abordarei a seguir.

Nós do comutador Ethernet

O nó do switch Ethernet é um switch virtual emulado que permite criar acesso à VLAN e portas de tronco. O nó do switch Ethernet suporta portas de acesso, portas de tronco 802.1Q padrão do setor e marcação QinQ. No entanto, ele não suporta o protocolo de enroncamento ISL (Inter-Switch Link) proprietário da Cisco.

Para usar um nó do switch Ethernet, arraste o nó para sua área de trabalho. Você nunca precisa iniciar um nó de switch Ethernet; eles estão sempre prontos para usar. Para configurar o switch, clique com o botão direito do mouse no ícone do nó do switch Ethernet e selecione Configurar. Usando a janela do configurador de Nó mostrada na Figura 4-15, clique no nome do switch (SW1, por exemplo) para modificar as portas do switch padrão ou adicionar novas portas. Por padrão, existem oito portas de acesso atribuídas à VLAN 1. Para alterar uma porta, clique no número da porta e modifique as configurações conforme necessário. Quando terminar, clique em Aplicar e OK. Para adicionar uma nova porta, defina as configurações da porta e clique no botão Adicionar; depois clique em Aplicar. Quando terminar de adicionar portas, clique em OK para concluir a configuração.

Uma alternativa ao nó do switch Ethernet é configurar um roteador Dynamips com um módulo de switch de rede. A vantagem de usar um módulo de switch é que ele suporta mais recursos (como o Spanning Tree Protocol); A desvantagem é que o uso de um módulo de switch de rede utiliza mais recursos do PC. Se você precisar das funções de

apenas um switch simples, recomendo que você ative o nó do switch Ethernet. Se você precisar de capacidade total de switch IOS, use um roteador com um módulo de switch instalado como o roteador EtherSwitch ou use uma imagem de switch IOU L2 (discutida no Capítulo 9).

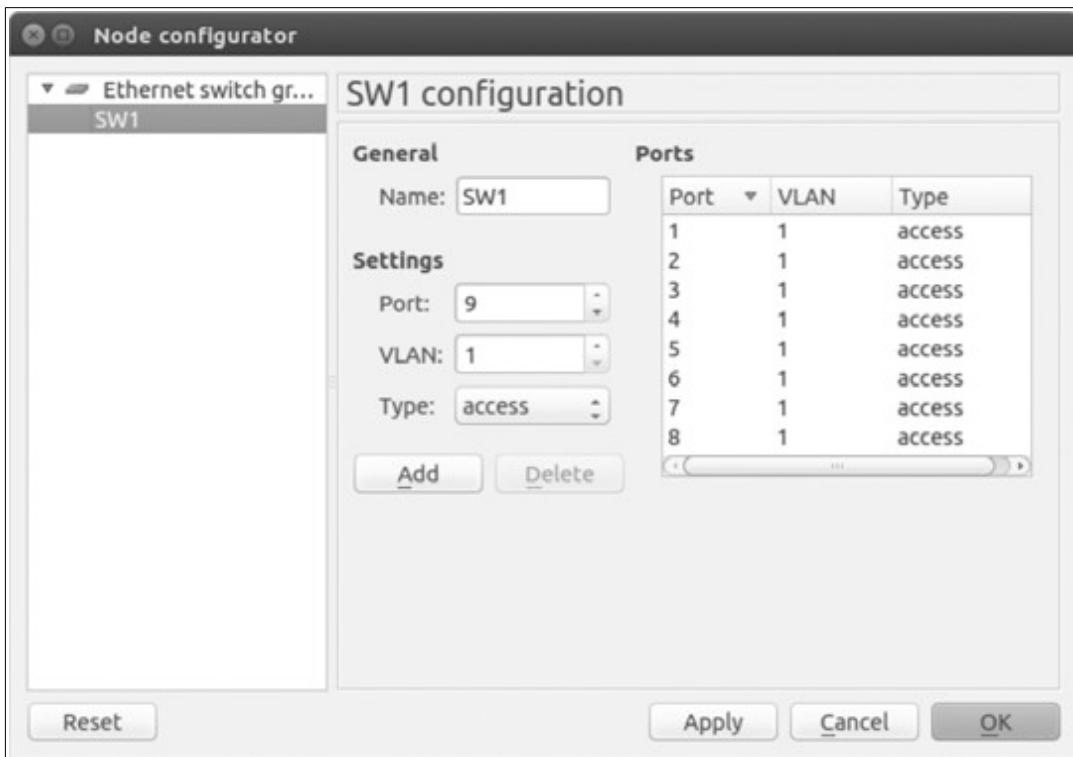


Figure 4-15: Ethernet switch Node configurator window

Alterando símbolos e organizando seus dispositivos

Você pode alterar os símbolos usados para representar dispositivos em seu espaço de trabalho e escolher onde seus dispositivos estão localizados na barra de ferramentas Dispositivos. Digamos que você queira alterar o símbolo de um roteador IOS. Para alterar o símbolo do dispositivo, selecione **Edit ▶ Preferences** no Linux e Windows ou selecione **GNS3 ▶ Preferences** no OS X. Em seguida, vá para o dispositivo que deseja alterar, clique com o botão direito do mouse no ícone do dispositivo e selecione **Change symbol**, como mostra a Figura 4-16

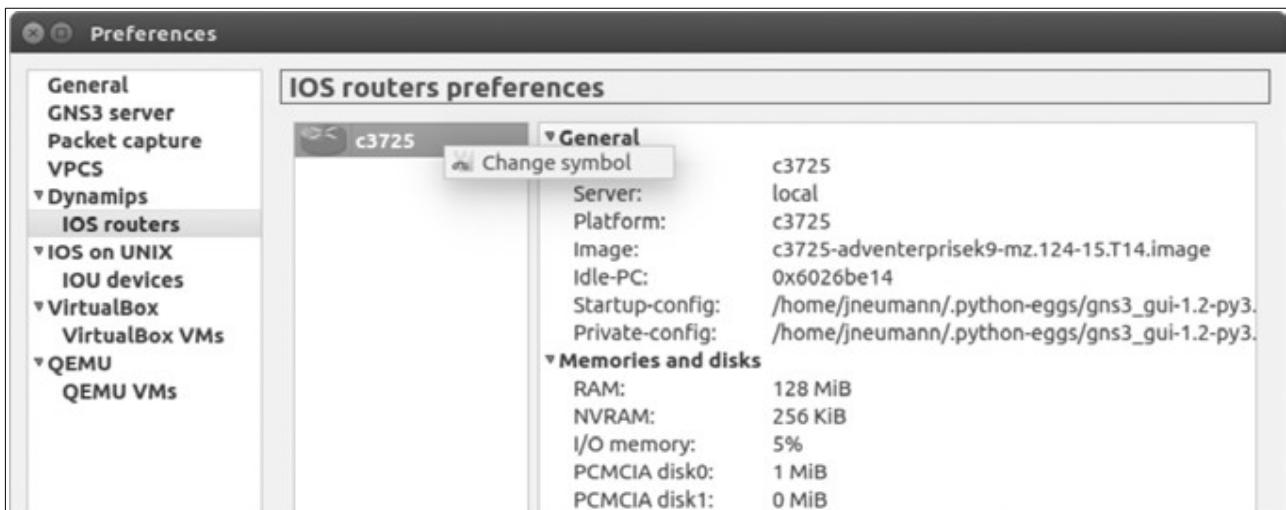


Figure 4-16: Changing the symbol

Você pode alterar o símbolo para dispositivos IOU, Máquinas virtuais VirtualBox e máquinas virtuais QEMU da mesma maneira. A janela de seleção Symbol, como mostra a Figura 4-17, deve aparecer após você clicar em **Change symbol**.



Figure 4-17: Symbol selection and device category

Comece criando a rede na Figura 4-1. Depois de criar a topologia, faça logon nos roteadores, configure suas interfaces e tente executar ping entre eles. Simule uma falha e recuperação usando o recurso de suspensão e retomada ou iniciando e parando um dispositivo. Depois de explorar alguns comandos do IOS e os recursos do GNS3, tente criar um laboratório simples de CCNA com três ou mais roteadores; existem muitos laboratórios de exemplo do CCNA e do CCNP on-line.

Uma última palavra de cautela: se você criar grandes topologias que usam roteamento multiprotocolo, poderá achar que precisa aumentar os temporizadores de protocolo do roteador para impedir que suas interfaces subam e desçam repetidamente. (É raro, mas às vezes acontece.) O problema é causado pelos efeitos inerentes à latência no Dynamips. Conexões seriais são outra área problemática comum; algumas imagens do roteador podem ser esquisitas quando executadas em portas seriais emuladas. Se você achar que a porta serial de um roteador está travando ou travando a conexão, tente outro modelo de roteador ou imagem IOS diferente. Em geral, as imagens c36xx, c37xx e 7200 IOS são as mais estáveis com o Dynamips e devem ser usadas sempre que possível. No capítulo 5, você explorará o básico da captura de pacotes de rede com o Wireshark e expandindo suas redes adicionando hosts usando VPCS, VirtualBox e Linux.

5 Integrando hosts e usando o Wireshark

Até esse momento, você aprendeu a criar redes usando dispositivos Cisco, mas o GNS3 pode fazer muito mais! Ele usa um conjunto robusto de ferramentas de rede que permitem integrar aplicativos externos aos seus projetos GNS3. Neste capítulo, você explorará algumas dessas ferramentas aprendendo a integrar hosts de PC a projetos usando o Virtual PC Simulator e o VirtualBox. O capítulo também abordará o sniffing básico de pacotes usando o Wireshark.

Virtual PC Simulator

Uma maneira de adicionar hosts aos seus projetos é com o VPCS, um pequeno aplicativo que simula até nove PCs do tipo DOS. Os hosts VPCS têm um conjunto limitado de comandos, mas são adequados para testar a conectividade de ponta a ponta nas redes GNS3. O VPCS usa muito poucos recursos do PC, o que permite adicionar vários hosts aos projetos sem atrapalhar o seu PC.

Instalando o VPCS

Se você estiver executando o Windows ou OS X, o VPCS deveria ter sido incluído quando você instalou o GNS3. Se você estiver usando um sistema Linux, o código-fonte do VPCS deveria ter sido incluído no seu download do

Para alterar um símbolo do dispositivo, role para baixo na janela de seleção Symbol e selecione o símbolo que deseja usar. Em seguida, use o menu suspenso para escolher uma categoria. Essa é a categoria em que o dispositivo será colocado na barra de ferramentas Dispositivos. As categorias incluem comutadores, roteadores, dispositivos finais e dispositivos de segurança. Quando terminar, clique em **OK** para concluir a alteração.

Pensamentos finais

Neste capítulo, você aprendeu o básico da configuração de uma rede GNS3. Agora é um bom momento para criar alguns laboratórios e praticar o que aprendeu. Se você estuda para obter uma certificação Cisco, gastar o máximo de tempo possível com o equipamento Cisco é a única maneira de obter experiência suficiente para passar nos exames. (Eles são difíceis!)

GNS3 para Linux, mas ele precisará ser compilado antes de você poder usá-lo. Compile e instale-o usando os seguintes comandos, substituindo x pelo número da versão do seu arquivo de origem VPCS:

```
$ unzip vpcs-x.zip  
$ cd vpcs-x/src  
$ sh mk.sh  
$ sudo cp vpcs /usr/local/bin/
```

Para usar o VPCS, arraste um nó do host VPCS de End Devices na barra de ferramentas Devices para o seu espaço de trabalho. Antes de iniciar um host VPCS, ele deve estar conectado a outro dispositivo no seu projeto. Depois de iniciar um host VPCS e abrir um console, você verá uma janela semelhante à Figura 5-1.

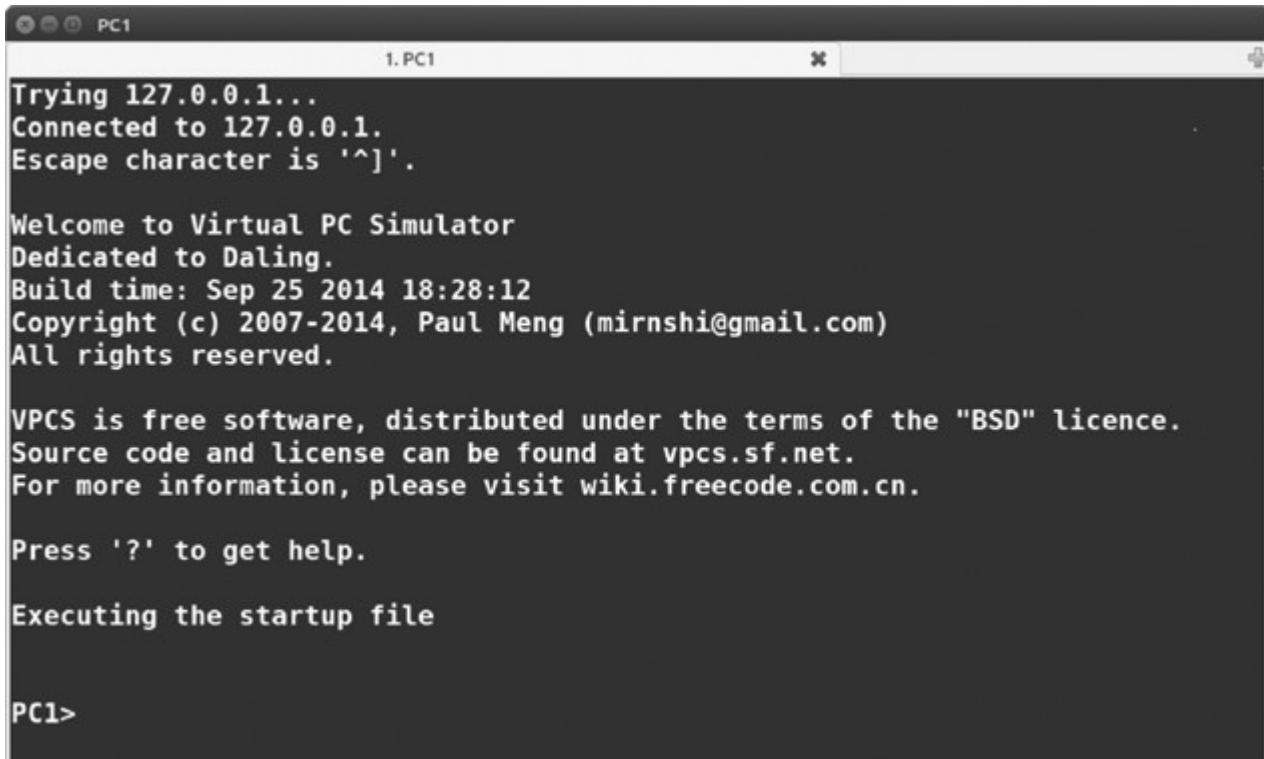


Figure 5-1: The VPCS console

Se você não vir o console do VPCS ou se o seu aplicativo exibir erros, verifique se o programa reside em /usr/local/bin/ (no Linux) e se o caminho foi definido corretamente nas preferências do GNS3. O desenvolvedor fornece muito pouco em termos de suporte ou documentação; portanto, se você continuar com problemas, visite os fóruns do GNS3 (<http://community.gns3.com/>) para obter uma possível solução.

Comandos VPCS

Os comandos no VPCS são na sua maioria auto-explicativos, mas abordarei alguns deles aqui para você começar. Para ver uma lista completa dos comandos suportados, você pode inserir um ponto de interrogação, ?. Para exibir a configuração de seus hosts, você pode inserir o comando show. Para exibir os parâmetros para um comando específico, digite o nome do comando seguido por um ponto de interrogação. Por exemplo, inserindo ping? exibirá todas as opções do comando ping.

NOTA

Como o Cisco IOS, o VPCS suporta sintaxe de comando abreviada. Por exemplo, o comando ping pode ser inserido como p. Você pode abreviar qualquer comando VPCS, mas você deve digitar letras suficientes do comando para que seja exclusivo de outros comandos que começam com as mesmas letras.

Endereçamento IP VPCS

Após iniciar o VPCS, você precisa configurar o host para uso com o GNS3. Normalmente, isso requer apenas a configuração do endereço IP, máscara de sub-rede e endereço do gateway. O VPCS suporta endereçamento IPv4 e IPv6.

Você pode configurar manualmente um endereço IP ou adquirir um automaticamente se um servidor DHCP (Dynamic Host Configuration Protocol) estiver sendo executado no seu projeto GNS3. Para configurar manualmente um endereço IPv4, insira o *ip-address mask gateway*. O exemplo a seguir define um endereço IPv4 para 192.168.1.50 usando uma máscara de sub-rede 255.255.255.0 e define o gateway padrão para 192.168.1.1:

```
PCI> ip 192.168.1.50 255.255.255.0 192.168.1.1
```

Você pode inserir o mesmo endereço IPv4 usando Notação *Classless Inter-Domain Routing-CIDR* (Roteamento entre Domínios sem Classe) no lugar de uma máscara de sub-rede padrão, como mostrado aqui:

```
PCI> ip 192.168.1.50 /24 192.168.1.1
```

Para configurar manualmente um endereço IPv6, digite o comando *ip* seguido por um endereço e máscara IPv6 válidos. O exemplo a seguir define o endereço IPv6 como 2014: 12: 1a :: 50 usando uma máscara de sub-rede de 64 bits:

```
PCI> ip 2014:12:1a::50 /64
```

Para configurar um host automaticamente usando o DHCP, digite o comando *dhcp* para cada host que requer um endereço, como neste exemplo:

```
PCI> dhcp
```

Use o comando *save* para salvar suas configurações de VPCS com seu projeto GNS3.

```
PCI> save  
.done
```

As configurações serão salvas na pasta de projetos GNS3 em *GNS3/projects/<project_name>/project-files/vpcs/<vpcs_uuid>*. Mais tarde, quando você carrega seu projeto GNS3, as definições de configuração serão aplicadas automaticamente ao host.

Para testar o VPCS, crie um projeto usando um nó host VPCS e vincule-o a algum outro dispositivo, como um roteador. Atribua um endereço IP ao host VPCS e ao outro dispositivo e use ping ou trace para testar a conectividade. Se tudo correr bem, você deve receber uma resposta como a deste exemplo:

```
PCI> ping 192.168.1.1  
192.168.1.1 icmp_seq=1 ttl=255 time=35.821 ms
```

Após executar o ping com êxito nos dispositivos, você pode examinar o cache do ARP (Endereço MAC para a tabela IP) usando o comando *arp*, conforme a seguir:

```
PCI> arp  
cc:00:05:a9:00:00 192.168.1.1 expires in 114 seconds
```

Se um ping não tiver êxito, o VPCS exibirá uma mensagem "host não acessível":

```
PCI> ping 192.168.1.1  
host (192.168.1.1) not reachable
```

Você pode solucionar isso verificando se as interfaces do roteador estão ativadas no GNS3 e verificando se todos os endereços IP e máscaras de sub-rede foram atribuídos corretamente. Outra causa pode ser as configurações de

firewall do seu PC, especialmente se você estiver usando um PC com Windows. Em geral, desabilitar completamente o firewall enquanto trabalha com o GNS3 é uma boa ideia e pode resolver esse e outros problemas.

VirtualBox

O VPCS é uma ótima ferramenta para adicionar hosts simples ao GNS3 e testar a conectividade, mas às vezes você precisa de um host que esteja executando um sistema operacional real, em vez de um simulado. É aqui que entra o VirtualBox. O VirtualBox pode executar a maioria dos sistemas operacionais baseados em PC, incluindo Windows, Linux, FreeBSD e outros. Também é útil para executar sistemas operacionais de rede como Arista vEOS, Juniper Firefly e NX-OSv. A vantagem de usar o VirtualBox é que ele fornece hosts executando sistemas operacionais reais;

A desvantagem é que esses sistemas operacionais podem precisar de recursos substanciais do seu PC. Se tudo o que você precisa fazer é testar a conectividade, fique com o VPCS, mas se precisar de um host que forneça um conjunto robusto de utilitários de rede (para testar a segurança da sua rede GNS3, por exemplo) ou para executar outro roteador ou switch Sistema operacional, convém usar o VirtualBox.

Instalando no Windows

Para instalar o VirtualBox no Windows, baixe o instalador apropriado no site do VirtualBox (<http://www.virtualbox.org/>). Inicie o instalador e clique em Avançar quando vir a tela Bem-vindo para abrir uma janela de personalização. Faça as personalizações desejadas aqui e siga as instruções na tela para concluir a instalação. Eu recomendo aceitar os valores padrão para garantir que o VirtualBox seja executado corretamente com o GNS3. Após a conclusão da instalação, você pode iniciar o aplicativo usando o menu Iniciar do Windows ou clicando no ícone VirtualBox.

Instalando no OS X

Para instalar o VirtualBox no OS X, faça o download do instalador apropriado no site VirtualBox (<http://www.virtualbox.org/>) e inicie-o. Quando a tela de instalação do VirtualBox aparecer, clique duas vezes no ícone VirtualBox.pkg e siga as instruções na tela. A instalação requer privilégios elevados, portanto, tenha sua senha de administrador à mão. Depois que o pacote estiver instalado, você poderá iniciá-lo na pasta Aplicativos, clicando duas vezes no ícone VirtualBox.

Instalando no Linux

O VirtualBox é suportado na maioria das distribuições Linux, mas verifique seu gerenciador de pacotes Linux para verificar se ele é suportado em sua plataforma específica. No Ubuntu e na maioria dos outros sistemas Linux baseados no Debian, use o utilitário apt-get para atualizar seu gerenciador de pacotes e instalar a versão mais recente do VirtualBox. Verifique se você tem acesso à Internet e digite o seguinte em uma janela do terminal:

```
$ sudo apt-get update  
$ sudo apt-get install virtualbox
```

Depois que o utilitário estiver instalado, você pode iniciá-lo abrindo uma janela do terminal e entrando no virtualbox ou iniciando-o no seu gerenciador de janelas Linux.

Importando Appliances

Um dispositivo VirtualBox é uma máquina virtual pré-configurada, geralmente executando uma distribuição Linux personalizada, que você pode usar em seus projetos GNS3. O uso de um sistema operacional real oferece mais comandos e maior flexibilidade do que o uso de um simulador como o VPCS. Você pode fazer o download de dispositivos VirtualBox pré-configurados no site do GNS3, na seção Download. Os equipamentos precisam ser importados para o VirtualBox antes que você possa usá-los. Os nomes dos pacotes de aplicativos terminam em .ova, que significa Open Virtual Appliance, e geralmente são chamados de arquivos OVA. Para importar um dispositivo, inicie o VirtualBox e você verá a janela do VirtualBox Manager. No VirtualBox Manager, você pode importar ou criar novos convidados da máquina virtual e gerenciar todos os seus sistemas operacionais convidados instalados. A importação de um appliance é uma maneira rápida e fácil de adicionar um convidado, pois a configuração e instalação do sistema operacional já foi feita para você.

Os aparelhos encontrados no site do GNS3, muitas vezes são otimizados para usar menos recursos do PC do que uma instalação padrão do mesmo sistema operacional. Infelizmente, isso significa que seu dispositivo pode não ter

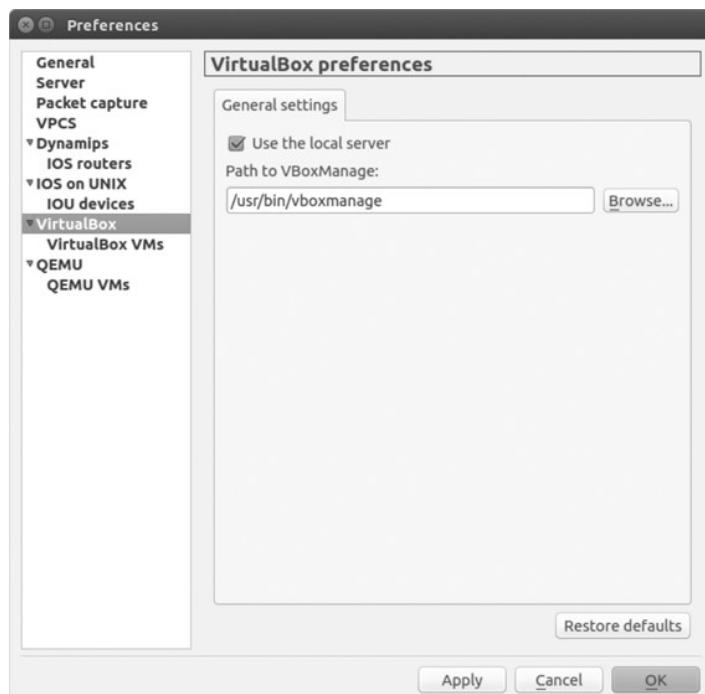
todos os comandos ou ferramentas necessárias, mas você deve poder atualizar ou instalar software adicional através do gerenciador de pacotes de software. Na Figura 5-2, você pode ver que o VirtualBox foi configurado com um convidado (Linux Microcore).



Figure 5-2: VirtualBox Manager showing an imported Linux guest OS

Selecionando o SO convidado exibe informações básicas sobre a configuração do convidado, como a memória base e quanto espaço em disco foi atribuído à máquina virtual. Para modificar as configurações de uma máquina virtual, realce o convidado e clique em Configurações na barra de ferramentas. Assim como PCs reais, os convidados de PC virtual geralmente funcionam melhor quando recebem mais recursos, como memória ou núcleos adicionais de CPU.

Para importar um dispositivo convidado do VirtualBox, baixe um arquivo de imagem e copie-o para uma pasta no seu diretório de usuário. Inicie o VirtualBox e selecione **File** ▶ **Import Appliance**; depois clique em **Open Appliance** e navegue até o local em que você salvou o arquivo. Selecione o arquivo de imagem e clique em **Continue** seguido de **Import** para concluir o processo. Para testar seu convidado do VirtualBox, clique em **Start** e seu sistema operacional deve inicializar e executar como um PC normal. Depois de testar seu sistema operacional importado recentemente, você está pronto para configurar as preferências do GNS3 VirtualBox.



Preferências do VirtualBox

Para gerenciar convidados do VirtualBox, o GNS3 usa o aplicativo VboxManage. Este programa é instalado automaticamente quando você instala o VirtualBox. Antes de adicionar um convidado do VirtualBox ao GNS3, verifique o caminho para o VboxManage. Inicie o GNS3, selecione **GNS3** ▶ **Preferences** no OS X ou **Edit** ▶ **Preferences** no Windows e Linux e clique em **VirtualBox** para acessar a janela mostrada na Figura 5-3.

Figure 5-3: VirtualBox General Settings tab

No Ubuntu Linux, o caminho na guia Configurações Gerais deve ser definido para `/usr/bin/vboxmanage`. Ajuste o caminho conforme necessário e clique em Aplicar e OK. No Windows e no OS X, o caminho do VBoxManage não precisa ser alterado. Desmarcando **Use the local server** permitirá escolher um local ou servidor GNS3 remoto ao criar um host do VirtualBox. Deixando a caixa marcada garante que o convidado do VirtualBox sempre seja executado localmente no seu PC. Se você tiver problemas ao iniciar um host do VirtualBox ou abrir uma conexão de console a um host, um ou mais números de porta padrão do console já podem estar em uso por outro aplicativo em execução no seu PC. Para corrigir isso, tente fechar o aplicativo incorreto ou desativar o firewall do PC. Outra causa possível pode ser que o convidado do VirtualBox que você está usando não esteja configurado para aceitar conexões de console.

Configurações da máquina virtual do VirtualBox

Após configurar (ou pelo menos revisar) as preferências do VirtualBox no GNS3, você precisa configurar um ou mais hosts do VirtualBox para usar em seus projetos. Comece selecionando **VirtualBox VM** no painel esquerdo. Clique em **New** e selecione sua máquina virtual VirtualBox no menu suspenso da lista de VMs, como mostra a Figura 5-4.



Figure 5-4: New VirtualBox VM screen

Clique em **Finish** para concluir a instalação. Você deve ver as configurações atualmente atribuídas à máquina virtual, como mostra a Figura 5-5.

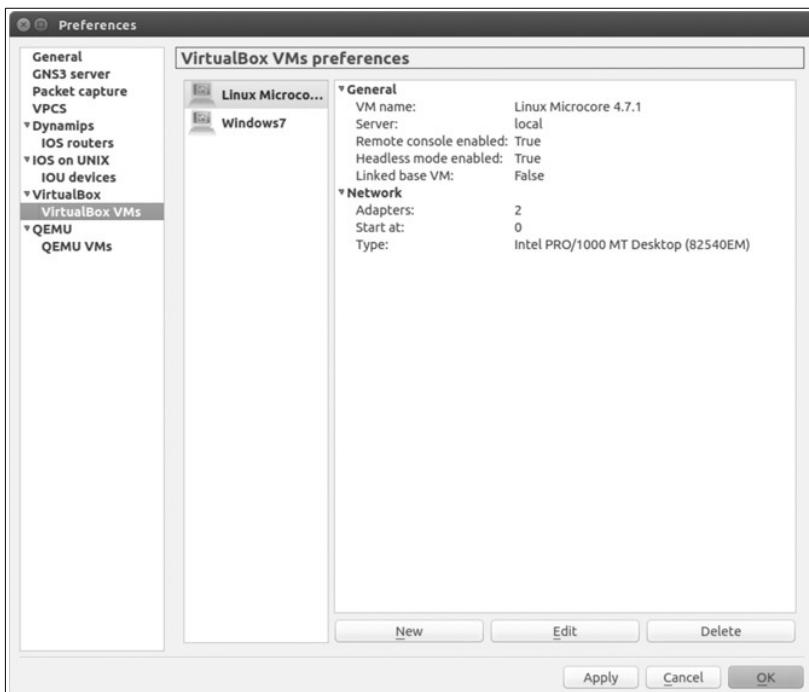


Figure 5-5: VirtualBox VMs preferences

Por padrão seu dispositivo de máquina virtual pode ser encontrado em Dispositivos finais na barra de ferramentas Dispositivos. Ao clicar com o botão direito do mouse no ícone da máquina virtual na janela Preferências (Linux Microcore neste exemplo), você pode atribuir um ícone diferente à máquina virtual e escolher onde ela residirá na barra de ferramentas Dispositivos. Isso permite que você organize melhor todos os seus dispositivos GNS3.

Para modificar as configurações de uma máquina virtual, selecione a máquina virtual e clique em **Edit**. Na maioria dos casos, você deseja ir para a guia Configurações gerais e selecionar as caixas **Enable remote console** e **Start VM in headless mode**, como mostra a Figura 5-6. A primeira opção permite acessar o console de uma máquina virtual em execução a partir do aplicativo de terminal atribuído ao GNS3; a segunda opção impede o VirtualBox de abrir uma janela do console quando você inicia uma máquina virtual no GNS3.

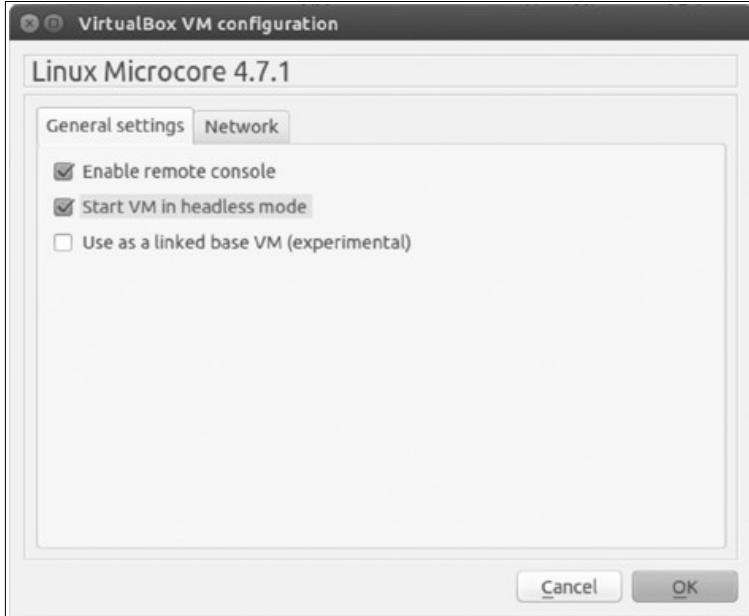


Figure 5-6: VirtualBox VM configuration's General settings tab

Para modificar as configurações de rede, clique na guia **Network**. Você pode mudar o número de adaptadores instalados na máquina virtual, o índice número do adaptador (geralmente 0 ou 1) e o tipo de adaptador instalado na máquina virtual. Quando terminar, clique em **Apply** e **OK** para salvar as modificações. Depois de configurar um sistema operacional convidado da máquina virtual, você pode usá-lo em seus projetos GNS3.

Usando hosts VirtualBox em um projeto

Para adicionar um host do VirtualBox a um projeto, arraste um ícone do nó do host do VirtualBox da janela End Devices para o espaço de trabalho do GNS3. Um host do VirtualBox pode ser usado apenas uma vez por projeto GNS3. Se você deseja usar um host VirtualBox específico mais de uma vez, inicie o VirtualBox e use o recurso Clone para criar uma cópia clonada da máquina virtual.

Em seguida, inicie o GNS3 e siga as mesmas etapas descritas anteriormente para configurar o host clonado em Preferências do VirtualBox. Na próxima vez que você adicionar um nó de host do VirtualBox à sua área de trabalho, o sistema operacional clonado estará disponível. Depois que um nó host do VirtualBox for adicionado ao seu espaço de trabalho, você estará pronto para vinculá-lo a outros dispositivos GNS3.

Vinculando nós de host do VirtualBox a outros dispositivos

Para adicionar um link entre um nó host do VirtualBox e outro dispositivo, clique no ícone da barra de ferramentas **Add a Link**; clique no nó do host do VirtualBox e escolha uma interface a ser usada para o link. Selecione outro dispositivo e escolha uma interface para concluir a conexão. Para inicializar o host, clique com o botão direito do mouse no ícone do nó do host VirtualBox e selecione **Start**. Teste a conexão configurando um endereço IP no host do VirtualBox e no dispositivo ao qual está vinculado; em seguida, use o comando ping para verificar a conectividade. Na maioria dos sistemas Linux, como o Microcore, você pode configurar manualmente um endereço IP e um gateway padrão usando os comandos ifconfig e route. Para ver uma lista de placas de interface de rede (NICs) disponíveis no Linux, use o comando ifconfig sem nenhuma opção de configuração.

```
$ ifconfig
```

```
eth0      Link encap:Ethernet      HWaddr 08:00:27:7F:91:0A
          UP BROADCAST MULTICAST  MTU:1500      Metric:1
          RX packets:0      errors:0 dropped:0      overruns:0 frame:0
          TX packets:0      errors:0 dropped:0      overruns:0 carrier:0
          collisions:0      txqueuelen:1000
          RX bytes:0 (0.0 B)    TX bytes:0 (0.0 B)
          Interrupt:10     Base address:0xd020

eth1      Link encap:Ethernet      HWaddr 08:00:27:C5:FC:66
          UP BROADCAST MULTICAST  MTU:1500      Metric:1
          RX packets:0      errors:0 dropped:0      overruns:0 frame:0
          TX packets:0      errors:0 dropped:0      overruns:0 carrier:0
          collisions:0      txqueuelen:1000
          RX bytes:0 (0.0 B)    TX bytes:0 (0.0 B)
          Interrupt:9      Base address:0xd060
```

Nota

Nem todos os sistemas Linux usam o comando `ifconfig` ou `route` para configurar o TCP / IP, mas a maioria usa. Se esses comandos não estiverem disponíveis na sua distribuição, verifique a documentação do Linux para ver como configurar uma interface.

Se você estiver usando uma máquina virtual para PC com Windows, poderá configurar manualmente um endereço IP, abrindo o Centro de rede e compartilhamento e clicando em Alterar configurações do adaptador. Clique com o botão direito do mouse no adaptador que você deseja configurar e selecione Propriedades para modificar as configurações de TCP / IP, conforme mostrado na Figura 5-7.

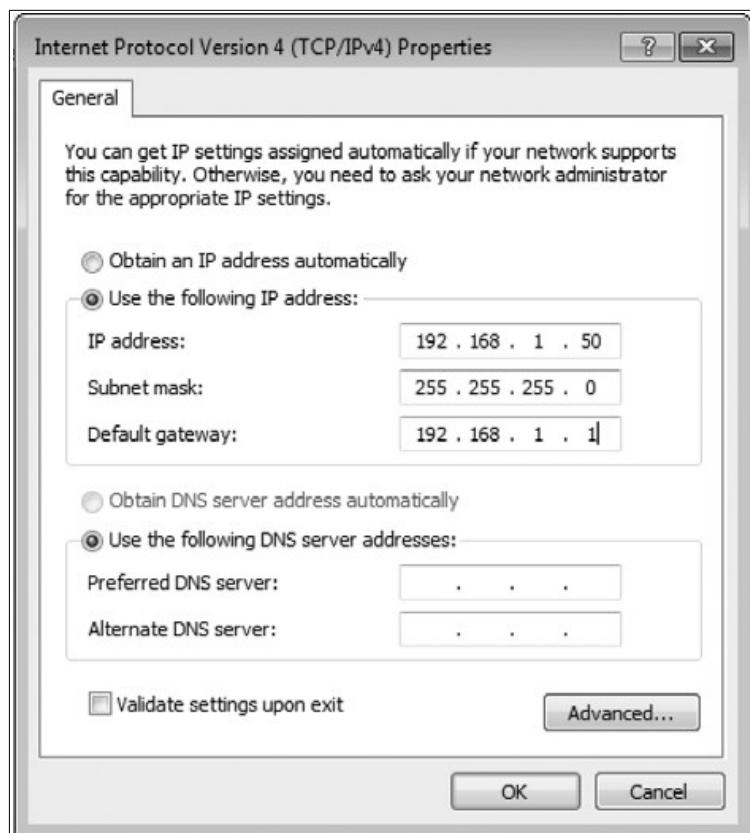


Figure 5-7: Windows TCP/IP interface properties

Digite as informações do seu endereço IP e clique em OK quando terminar. Se você tiver um servidor DHCP configurado no seu projeto GNS3, poderá deixar os campos em branco e escolher Obter um endereço IP automaticamente.

Projeto VirtualBox simples usando uma máquina virtual Linux

Agora que você adicionou uma máquina virtual Linux VirtualBox ao GNS3, vamos criar um projeto simples que conecte o host a um roteador Cisco IOS. Comece criando o projeto na Figura 5-8. Arraste um host do VirtualBox Linux e o roteador Dynamips para o seu espaço de trabalho e vincule-os usando um nó Ethernet switch.

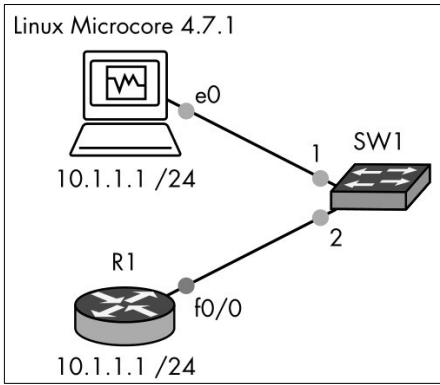


Figure 5-8: VirtualBox host and Cisco IOS router project

Inicie os dispositivos e comece a configurar seu projeto atribuindo um endereço IP à interface eth0 do host do VirtualBox Linux. Clique com o botão direito do mouse no nó Linux Microcore e selecione **Console** para abrir o terminal. No shell do terminal Linux, digite o seguinte comando para atribuir o endereço IP:

```
$ sudo ifconfig eth0 10.1.1.1 netmask 255.255.255.0 up
```

Em seguida, abra um console para o roteador R1, atribua um endereço IP à interface f0/0 e abra a interface.

```
R1# configure-terminal
R1(config)# interface f0/0
R1(config-if)# ip address 10.1.1.2 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# exit
R1#
```

Finalmente, teste a conectividade executando o ping do endereço IP do host Linux do roteador R1.

```
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/16/32 ms
```

Agora vamos ver como você pode usar o Wireshark para analisar pacotes nas suas redes GNS3.

Wireshark

O Wireshark é uma das ferramentas de análise de pacotes mais robustas disponíveis para os engenheiros de rede e é grátis! Um analisador de pacotes, às vezes chamado de sniffer de pacotes, é um software que permite capturar pacotes IP à medida que eles atravessam sua rede. Você pode abrir os pacotes para revelar e analisar seu conteúdo. Os farejadores de pacotes como o Wireshark são usados para solucionar problemas de protocolos de rede, impedir hackers e até identificar vírus, mas geralmente são ignorados pelos iniciantes. Se você é um aspirante a engenheiro de rede, usar o GNS3 e o Wireshark juntos é uma excelente maneira de aprender os meandros da rede e como os protocolos de rede funcionam.

Instalando no Windows

Se você instalou o GNS3 usando o instalador multifuncional do Windows, o Wireshark já deve estar instalado. Se você estiver usando o OS X ou Linux, precisará fazer o download e instalar o Wireshark manualmente.

Instalando no OS X

Antes de instalar o Wireshark no OS X, é necessário instalar o XQuartz, uma versão do OS X do sistema X Window semelhante ao X.Org nos sistemas Linux. Faça o download da versão apropriada do XQuartz no site do Mac OS Forge (<http://xquartz.macosforge.org/>). Clique duas vezes no instalador e clique no pacote do instalador do *XQuartz.dmg*. Clique em **Continue** até chegar à tela de boas-vindas e clique em **I Agree** e **Install** para concluir a instalação. Em seguida, baixe e instale o Wireshark no site do desenvolvedor (<http://www.wireshark.org/>). Clique duas vezes no arquivo baixado, seguido pelo pacote do instalador do *wireshark.dmg*. Na tela de boas-vindas, clique em **Continue**, **I Agree** e **Install** para concluir a instalação. Na primeira vez que você inicia o Wireshark, o OS X solicita a localização do programa X Window. Na janela **Browse**, clique em Procurar, navegue até a pasta *Applications/Utilities* e selecione **Xquartz**.

Nota

Na primeira vez que você inicia o Wireshark, o XQuartz abre uma janela do Xterm, mas não o Wireshark. Essa estranha peculiaridade é facilmente corrigida fechando o XQuartz e reiniciando o Wireshark. Pode levar um momento para abrir, mas isso é normal. Quando o aplicativo iniciar, você deverá ver a tela de boas-vindas do Wireshark.

Agora que o Wireshark está instalado, vamos ver como capturar pacotes de dispositivos em seus projetos.

Instalando no Linux

Para instalar a versão mais recente do Wireshark usando as Ferramentas Avançadas de Pacotes no Ubuntu Linux, abra um programa de terminal e digite os seguintes comandos:

```
$ sudo apt-get update  
$ sudo apt-get install wireshark
```

Confirme a instalação quando solicitado, e o pacote será instalado. Após a conclusão do processo, o Wireshark deve estar pronto para uso.

Capturando pacotes no GNS3

Para começar a capturar pacotes, clique com o botão direito do mouse em um link entre dois dispositivos e selecione Iniciar captura, como mostra a Figura 5-9. (Para interromper uma captura, clique com o botão direito do mouse no mesmo link e selecione Parar captura.)

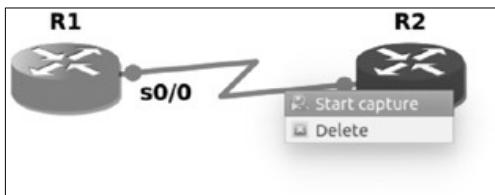


Figure 5-9: Start capturing packets.

O GNS3 solicita o dispositivo de origem, o nome da interface e o tipo de encapsulamento a ser usado para capturar dados. Você pode capturar dados nas interfaces Ethernet e serial. Nas conexões Ethernet, você pode escolher apenas o encapsulamento Ethernet: DLT_EN10MB, mas nas conexões seriais, você pode escolher o encapsulamento Cisco HDLC: DLT_C_HDLC, encapsulamento Cisco PPP: DLT PPP_SERIAL ou encapsulamento Frame Relay: DLT_FRELAY. Para capturar dados seriais padrão da Cisco (controle DataLink de alto nível), escolha HDLC; para capturar dados seriais do protocolo ponto a ponto, escolha PPP; e para capturar dados do Frame-Relay, selecione FRELAY. Use o menu suspenso para fazer sua seleção, como mostra a Figura 5-10.

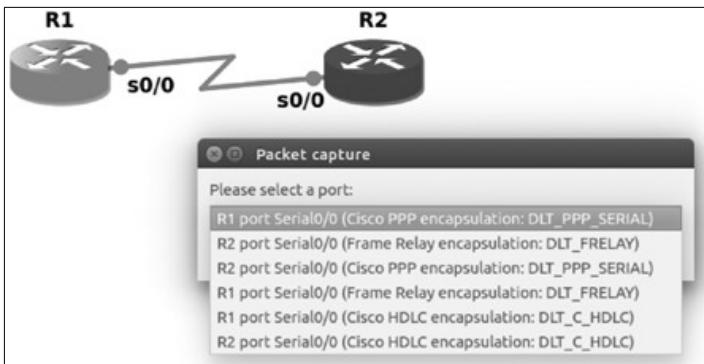


Figure 5-10: Source selection for capturing serial packets

Depois de fazer uma seleção e clicar em OK, o GNS3 abrirá o Wireshark e comece a capturar pacotes, como mostra a Figura 5-11. Observe que a janela do Wireshark está dividida em três painéis distintos.

1 Painel Lista de Pacotes

O painel superior da janela é dedicado à exibição de pacotes individuais à medida que eles são capturados. Os campos de pacote são exibidos na parte superior e incluem o número de sequência do pacote (Nº), carimbo de data / hora (Hora), endereço IP de origem (Origem), endereço IP de destino (Destino), nome do protocolo (Protocolo), tamanho do quadro (Comprimento), e campo de informações (informações). Pacotes contendo diferentes tipos de protocolo são exibidos em cores diferentes para ajudar a identificá-los.

2 Painel Detalhes do Pacote

Depois que um pacote é selecionado na lista de pacotes, detalhes sobre os protocolos e campos de protocolo do pacote são exibidos no painel do meio. Você pode expandir e recolher os campos para mostrar ou ocultar seus detalhes. Os nomes dos campos exibidos são específicos para o tipo de pacote que está sendo capturado e serão alterados de um tipo para outro.

3 Painel Bytes de Pacote

O painel inferior da janela principal exibe os dados brutos em formato hexadecimal, com caracteres ASCII exibidos à direita. É assim que os dados se parecem nativamente quando atravessam a rede. O Wireshark permite visualizar essas informações em hexadecimal ou binário.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	c2:02:27:8b:00:00	c2:02:27:8b:00:00	LOOP	60	Reply
2	0.5164380000	c2:01:27:79:00:00	c2:01:27:79:00:00	LOOP	60	Reply
3	3.0978270000	10.1.1.2	224.0.0.10	EIGRP	74	Hello
4	3.5405910000	10.1.1.1	224.0.0.10	EIGRP	74	Hello
5	7.4261160000	10.1.1.2	224.0.0.10	EIGRP	74	Hello
6	8.0801390000	10.1.1.1	224.0.0.10	EIGRP	74	Hello
7	9.9860590000	c2:02:27:8b:00:00	c2:02:27:8b:00:00	LOOP	60	Reply
8	10.5030610000	c2:01:27:79:00:00	c2:01:27:79:00:00	LOOP	60	Reply
9	12.2073860000	10.1.1.2	224.0.0.10	EIGRP	74	Hello
10	12.6865100000	10.1.1.1	224.0.0.10	EIGRP	74	Hello

Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

►Ethernet II, Src: c2:02:27:8b:00:00 (c2:02:27:8b:00:00), Dst: IPv4mcast_00:00:0a (01:00:5e:00:00:0a)

►Internet Protocol Version 4, Src: 10.1.1.2 (10.1.1.2), Dst: 224.0.0.10 (224.0.0.10)

►Cisco EIGRP

Version: 2
Opcode: Hello (5)
Checksum: 0xeeec2 [correct]
Flags: 0x00000000
Sequence: 0
Acknowledge: 0
Virtual Router ID: 0 (Address-Family)
Autonomous System: 10
►Parameters
►Software Version: EIGRP=12.4, TLV=1.2

Frame (frame), 74 bytes

Figure 5-11: Simple Wireshark capture from GNS3

Se você não encontrar nenhum pacote exibido na lista de pacotes, feche o Wireshark e pare a captura. Verifique se as interfaces do roteador estão ativadas e se foram atribuídos endereços IP, reinicie uma captura e inicie o Wireshark novamente.

Nota

Para saber mais sobre o uso do Wireshark, recomendo a leitura de *Practical Packet Analysis, 2^a Edição*, de Chris Sanders (No Starch Press, 2011). Você pode até se tornar um Wireshark Certified Network Analyst (WCNA).

Para alterar o comportamento padrão do Wireshark no GNS3, vá para **Preferences** e selecione **Packet Capture**. Para impedir que o GNS3 inicie automaticamente o Wireshark ao capturar pacotes, desmarque **Automatically start the packet capture application**, conforme mostrado na Figura 5-12. Você tem a opção de salvar capturas de pacotes e analisá-las posteriormente. Para fazer isso, selecione **Wireshark Traditional Capture** no menu suspenso (em Comandos pré-configurados da leitora de captura de pacotes) e clique em **Set**, **Apply** e **OK**. Agora, quando o GNS3 captura dados, ele salva automaticamente os arquivos capturados em um diretório denominado capturas dentro da pasta do projeto, como no *GNS3/projects/<project name>/project-files/captures/*. Para revisar capturas de pacotes salvos, inicie o Wireshark no seu PC, selecione **File ▶ Open**, navegue até a pasta capturas e selecione um arquivo de captura. Os arquivos de captura *.pcap* receberão o nome dos dispositivos GNS3 envolvidos na captura, como em *R1_FastEthernet0-0_to_R2_FastEthernet0-0.pcap*.

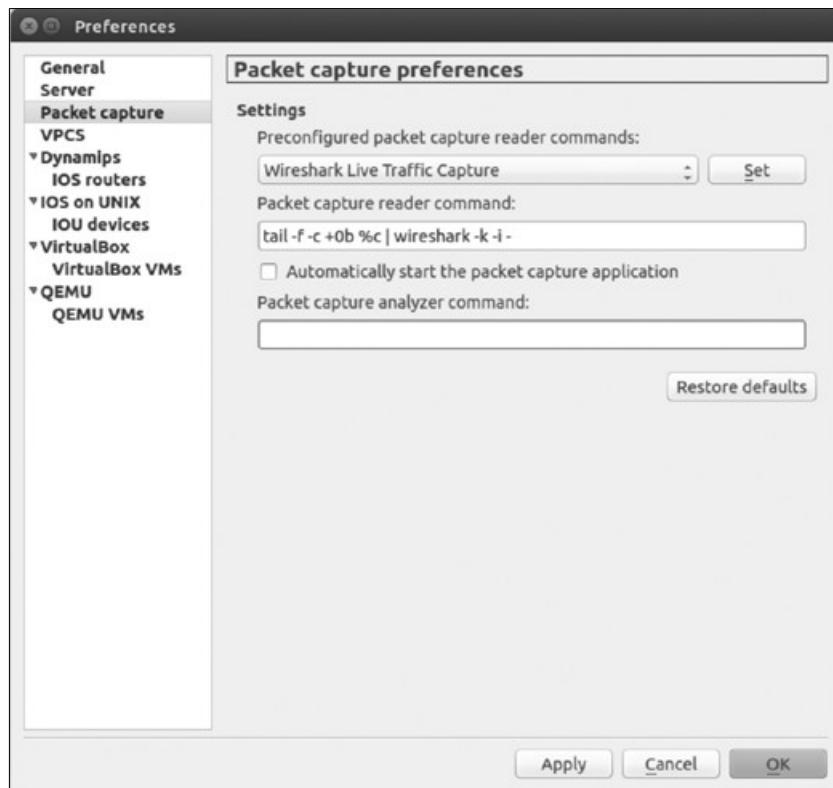


Figure 5-12: Wireshark capture preferences

Para saber mais sobre o Wireshark, confira o Guia do usuário on-line (http://www.wireshark.org/docs/wsug_html_chunked/). É bem organizado e fornece muitas informações sobre o uso do software.

Pensamentos finais

Um aspecto importante do GNS3 é o design modular e a capacidade de expandir projetos usando outro software de código aberto. Usando o VPCS, você pode adicionar um grande número de hosts de PC simples e, com o VirtualBox, você pode executar hosts usando sistemas operacionais completos, como o Linux. Esse recurso torna o GNS3 muito expansível, pois qualquer sistema operacional de rede executado no VirtualBox pode ser adicionado aos seus projetos GNS3.

O Wireshark é uma das ferramentas mais subutilizadas do mercado, mas também é um dos mais poderosos. Com o Wireshark, você pode se aprofundar e realmente ver o que está acontecendo em suas redes. Se você é novato em

redes ou já possui certificação de rede, desmembrar o Wireshark e examinar pacotes é uma ótima maneira de aprimorar suas habilidades e aumentar sua compreensão dos protocolos de rede.

No capítulo 6, você examinará o Quick Emulator, outro emulador de PC de código aberto, e o usará para criar uma versão especial para PC do Junos OS da Juniper, conhecido como Juniper Olive. O Juniper Olive permite adicionar roteadores Juniper totalmente funcionais aos seus projetos GNS3.

6

JUNIPER OLIVE e VSR X FIREFLY

Você pode instalar e executar roteadores Juniper com o GNS3 de várias maneiras. Neste capítulo, mostro como usar o VirtualBox e o Quick Emulator (QEMU) para criar dispositivos Juniper prontos para GNS3 e depois instalar o firewall vSRX Firefly da Juniper.

O QEMU é um emulador de PC de código aberto semelhante ao VirtualBox. É menos polido, mas possui muitos recursos poderosos e é totalmente integrado ao GNS3. Usando o QEMU, você pode executar muitos sistemas operacionais de rede, incluindo Cisco ASA, IDS, IOS-XR, NX-OSv e uma versão especial do Junos OS da Juniper, conhecida como Juniper Olive. Neste capítulo, concentro-me apenas no Juniper.

Instalando o Qemu no Windows e no OS X

Se você instalou o GNS3 no Windows ou no OS X, o QEMU já deveria estar instalado para você. O instalador do GNS3 pode ter instalado duas versões do QEMU: uma versão estável configurada automaticamente durante a instalação do GNS3 e uma versão mais recente que contém recursos adicionais não testados. Se você precisar que seus projetos sejam completamente estáveis, recomendo usar apenas a versão pré-configurada.

Se você instalou o GNS3 usando os padrões descritos no Capítulo 2, você deve encontrar os aplicativos QEMU em *C:\ Program Files\GNS3\qemu-0.13.0* nos sistemas Windows de 32 e 64 bits, mas lembre-se de que esse diretório será alterado conforme novas versões do QEMU forem introduzidas e adicionadas para o GNS3. No OS X, você deve encontrar o QEMU em */Applications/GNS3.app/Contents/Resources/qemu/bin/*.

Instalando o Qemu no Linux

O QEMU no Ubuntu pode ser instalado usando um pacote ou compilado a partir do Código fonte. Para instalar a partir de um pacote, atualize seu gerenciador de pacotes e instale o QEMU na linha de comandos.

```
$ sudo apt-get update  
$ sudo apt-get install qemu
```

Como alternativa, você pode instalar o pacote *qemu-system-x86*. Essa é uma instalação muito menor que deve ser capaz de executar qualquer sistema operacional que você deseja usar com o GNS3. Para instalar a versão somente para arquitetura x86 do QEMU, use os seguintes comandos:

```
$ sudo apt-get install qemu-system-x86  
$ sudo apt-get install qemu-utils
```

Convém compilar o QEMU a partir do código-fonte, dependendo de qual versão do QEMU está disponível para o seu sistema. Embora existam pacotes pré-compilados de QEMU em muitas distribuições Linux, eles podem não ser a versão mais recente disponível e podem não incluir o kit de ferramentas GTK que fornece a interface gráfica com o usuário do QEMU. Nesse caso, você pode acessar a interface QEMU instalando um programa visualizador VNC, como o GNC Viewer.

Ao instalar a partir do código-fonte, você também precisa instalar outros pacotes exigidos pelo QEMU antes de compilar o código-fonte. Atualize seu gerenciador de pacotes e instale estes pacotes agora:

```
$ sudo apt-get update  
$ sudo apt-get install flex  
$ sudo apt-get install bison
```

```
$ sudo apt-get install zlib1g-dev
$ sudo apt-get install libglib2.0-dev
$ sudo apt-get install libgtk2.0-dev
$ sudo apt-get install libncurses5-dev
$ sudo apt-get install libpcap-dev
$ sudo apt-get install dh-autoreconf
```

Em seguida, faça o download do código fonte do QEMU no site do QEMU (<http://www.qemu-project.org/>) e descompacte o arquivo, conforme mostrado aqui:

```
$ wget http://www.qemu-project.org/download/qemu-2.1.2.tar.bz2
$ bunzip2 qemu-2.1.2.tar.bz2
$ tar xvf qemu-2.1.2.tar
```

Após descompactar os arquivos, vá para o diretório de instalação do QEMU e insira os comandos *configure* e *make* para compilar o código-fonte.

```
$ cd qemu-2.1.2
$ ./configure
$ make
```

Por fim, conclua o processo instalando os arquivos compilados no seu sistema. Isso deve ser feito usando privilégios elevados de root.

```
$ sudo make install
```

Quando a instalação estiver concluída, você encontrará binários QEMU em */usr/local/bin/*, e os arquivos de suporte QEMU devem estar no diretório */usr/local/share/qemu/*. Com o QEMU instalado, você está pronto para começar a criar e usar dispositivos QEMU no GNS3.

Apresentando o Juniper

A maioria das pessoas já ouviu falar da Cisco, mas relativamente poucas ouviram falar da Juniper Networks. Como a Cisco, a Juniper produz uma ampla variedade de hardware de rede, e os provedores de serviços de Internet usam seus dispositivos de alto rendimento para rotear com eficiência bilhões de pacotes para seus clientes.

Todos os dispositivos Juniper são projetados em torno de uma base de código comum do FreeBSD, embora nem todo dispositivo Juniper execute o sistema operacional FreeBSD. Em vez disso, eles usam seu kernel apenas como uma estrutura para outro sistema operacional conhecido como Junos OS. No entanto, como o Junos OS foi desenvolvido com o FreeBSD, você pode executar uma versão especial do software em seu PC, chamada Juniper Olive.

Juniper Olive é uma versão funcional do Junos OS. Por ser executado em um PC comum e não em um chassis Juniper real, não possui o hardware ASIC proprietário para obter o alto rendimento de um dispositivo Juniper real. Caso contrário, é o negócio real e não uma simulação do sistema operacional. Isso o torna adequado para estudar para a certificação Juniper Networks Certified Associate (JNCIA) e outras certificações de nível de entrada.

Nota

A Juniper fornece outro roteador virtual chamado vMX que roda em hardware x86 bare-metal ou como uma máquina virtual usando QEMU, VirtualBox ou VMware, que permite a integração no GNS3. É o que a Juniper chama de uma solução escalável de "pagamento à medida que cresce".

JUNIPER EXTENDS E OLIVE BRANCH

Há rumores de que o Juniper Olive é uma versão interna do Junos OS que deve ser usada apenas pelos desenvolvedores do Juniper e não se destina ao consumo público, mas apenas o Juniper sabe ao certo. Se você entrar em contato com a empresa, será informado de que é uma "versão não suportada". A Juniper não fornecerá o software e a Juniper certamente não fornecerá nenhum suporte. No entanto, o GNS3 suporta totalmente a integração do Juniper Olive, permitindo adicionar roteadores Juniper aos seus projetos GNS3.

Instalando o Juniper

Dizem que se você dá a uma pessoa um peixe, você a alimenta por um dia, mas se você ensina uma pessoa a pescar, você a alimenta por toda a vida. Esse ditado é verdadeiro ao criar uma Juniper Olive, então vamos pescar! Embora existam muitas maneiras de configurar e instalar o Olive (incluindo scripts que automatizam o processo ou máquinas virtuais pré-configuradas que podem ser encontradas na Internet), aprender a fazê-lo manualmente permite ajustar os parâmetros conforme necessário quando novas versões do Olive estiverem disponíveis. Quando usado com o GNS3, o software Juniper Olive geralmente é instalado usando o VirtualBox ou o QEMU. Nesta seção, você trabalhará com o QEMU, mas antes de criar um Olive, seu sistema deverá atender aos seguintes requisitos:

- 8 GB de espaço disponível em disco
- 1024 MB de memória disponível para QEMU / Juniper
- QEMU instalado no seu sistema
- FreeBSD-4.11 mini ISO
- Software Juniper Olive

Vamos ver como criar uma Olive e onde obter o software para fazê-lo.

Visão geral do processo

O software de instalação Juniper Olive funciona muito como um parasita comum, com o FreeBSD como seu host inocente. Para criar um Olive, você instala uma cópia do FreeBSD usando QEMU ou VirtualBox. Em seguida, você copiará um arquivo compactado gzip do software Juniper Olive para sua máquina virtual FreeBSD.

Lá, você descompactará o pacote e fará uma pequena modificação e depois compactará os arquivos novamente em um pacote instalável do FreeBSD. Por fim, você instala o pacote e reinicia o sistema FreeBSD. É onde as coisas começam a ficar interessantes. A primeira vez que você inicializa seu sistema, o software Juniper Olive invade seu host FreeBSD. Ele reparticionará o disco rígido do FreeBSD, copiará novos arquivos para o sistema e manterá os arquivos do FreeBSD necessários. Quando terminar, você deverá ter um roteador Juniper funcional.

Adquirindo o FreeBSD

Uma imagem de CD do FreeBSD é necessária para instalar o FreeBSD com QEMU. Estão disponíveis várias versões adequadas para a criação de Juniper Olive, mas eu recomendo um mini ISO. Ele contém todos os arquivos necessários e é o download mais rápido. Faça o download do arquivo 4.11-RELEASE-i386-miniplain.iso do arquivo FreeBSD (<ftp://ftp-archive.freebsd.org/>). Eu recomendo esta versão do FreeBSD em vez das mais recentes, porque parece funcionar bem com quase todas as versões do Olive.

Nota

Você pode encontrar uma imagem pronta para uso do QEMU (e VirtualBox) com o FreeBSD já instalado no site do GNS3 (<http://www.gns3.com/>) na seção Download, em appliances QEMU.

Adquirindo o Software Juniper Olive

Em seguida, você precisa adquirir o software Juniper Olive. O software está disponível como um pacote instalável do FreeBSD e deve ter um nome como *jinstall-12.1R1.9-domestic-olive.tgz*. Como o Juniper Olive não é suportado pelo Juniper, você não pode obter uma cópia do software diretamente do Juniper.

Criando um arquivo de imagem Juniper olive cd

Depois de ter o software Juniper Olive, você precisa de uma maneira de copiar o pacote para sua máquina virtual FreeBSD para instalá-lo. Há mais de uma maneira de fazer isso, mas a maneira mais simples é montar um arquivo de imagem ISO em sua máquina virtual FreeBSD, da mesma forma que faria em um CD comum. Antes de fazer isso, você deve criar sua própria imagem ISO do software Olive.

Criando um ISO no Windows

Para criar um arquivo de imagem ISO usando o Windows, você precisa primeiro instalar o software de criação de imagem ISO. Eu recomendo o ISO Recorder (<http://isorecorder.alexfeinman.com/isorecorder.htm>). É gratuito, fácil de instalar e funciona bem. Faça o download do software e inicie o instalador. Em seguida, clique em Avançar e siga as instruções para concluir a instalação. Após a instalação do ISO Recorder, você poderá criar uma imagem ISO do software Juniper Olive. Crie uma pasta e copie o arquivo Olive compactado para a pasta (chamada juniper-olive, por exemplo). Em seguida, clique com o botão direito do mouse na pasta e selecione Criar arquivo de imagem ISO.

O Assistente de criação do gravador ISO é exibido, como mostra a Figura 6-1.

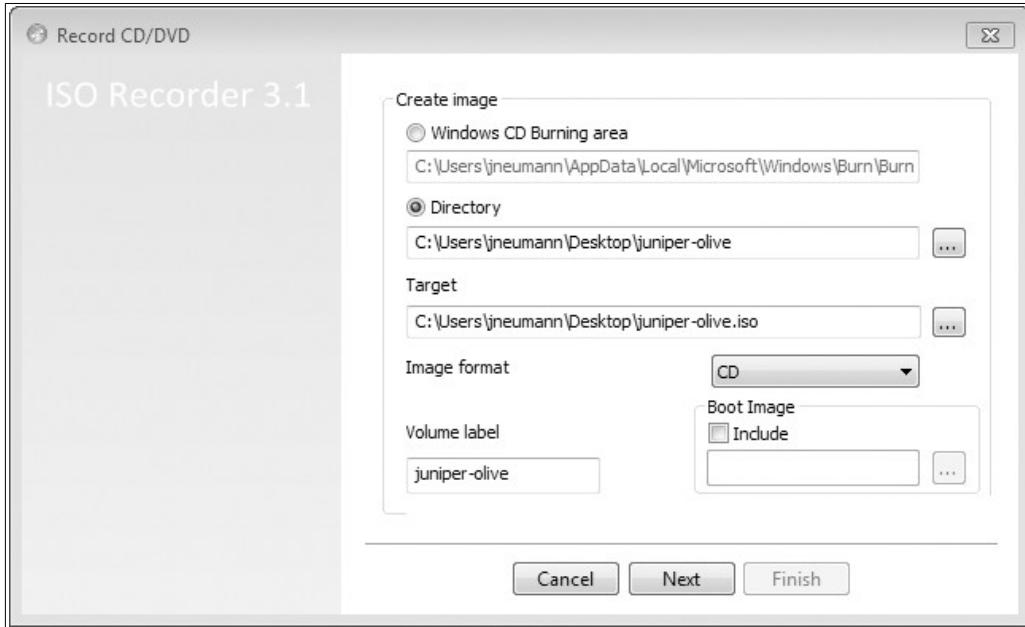


Figure 6-1: ISO Recorder Creation Wizard

Em Criar imagem, selecione o botão de opção Diretório, altere o Formato da imagem no CD, clique em Avançar e siga as instruções para criar sua imagem ISO. Depois de ter um Juniper ISO, você estará pronto para instalar o Juniper Olive no Windows.

Criando um ISO no OS X

Em computadores executando o OS X, copie o arquivo de imagem do Juniper para uma pasta e use o *hdiutil* para criar uma imagem ISO do conteúdo da pasta. Na listagem a seguir, criei um arquivo de imagem ISO chamado *juniper-olive.iso* usando uma pasta chamada *JUNOS*:

```
$ mkdir JUNOS
$ cp jinstall-12.1R1.9-domestic.tgz JUNOS
$ hdiutil makehybrid -iso -joliet -o juniper-olive.iso JUNOS
```

Agora que você possui um ISO adequado do software Olive, você está pronto para instalar o Juniper Olive no OS X.

Criando uma ISO no Linux

Criar uma imagem ISO no Ubuntu Linux é quase a mesma que no OS X, exceto pelo uso do aplicativo *mkisofs*. Copie o arquivo de imagem do Juniper para uma pasta (*JUNOS*, por exemplo) e digite os seguintes comandos para criar o ISO:

```
$ mkdir JUNOS
$ cp jinstall-12.1R1.9-domestic.tgz JUNOS
$ mkisofs -o juniper-olive.iso JUNOS
```

Agora que você tem seu ISO, faltam apenas algumas coisas antes de criar uma Juniper Olive.

Instalando e configurando o freeBSD usando o Qemu

O primeiro passo na criação de um Juniper Olive é criar uma máquina virtual QEMU do FreeBSD. O QEMU não possui uma interface gráfica do usuário, portanto, você fará tudo na linha de comando. Você usará o programa qemu-img para criar um arquivo de imagem de disco virtual e o programa qemu para instalar e testar sua máquina virtual.

Nota

Nem todas as instalações do QEMU são iguais. Em algumas instalações, o arquivo do aplicativo QEMU pode ser denominado qemu-system-i386 ou qemu-system-x86_64 ou os dois podem estar instalados. Se não tiver certeza, verifique o diretório de instalação do QEMU.

Preparando o diretório de compilação

Comece criando um diretório de construção e copie os arquivos ISO de instalação do FreeBSD e Juniper Olive ISO para o diretório, como no exemplo a seguir:

```
$ mkdir Juniper
$ cp 4.11-RELEASE-i386-mininst.iso Juniper
$ cp juniper-olive.iso Juniper
```

Se você estiver usando o Windows, abra uma janela do prompt de comando e insira os seguintes comandos:

```
c: mkdir Juniper
c: copy 4.11-RELEASE-i386-mininst.iso Juniper
c: copy juniper-olive.iso Juniper
```

Agora que tudo está preparado no diretório de construção, você pode começar a instalar o sistema.

Instalando um sistema FreeBSD compatível com o Junos

Nesta seção, você criará um disco rígido virtual usando o qemu-img e instalará o FreeBSD no disco virtual. Abordarei apenas o básico da preparação do FreeBSD para Olive e não entrarei em muitos detalhes sobre o próprio FreeBSD.

Verificações preliminares para Windows e OS X

Se você é usuário do Windows, instale o aplicativo Cliente Telnet a partir do Painel de controle de programas e recursos antes de começar. Se você é um usuário do OS X, você deseja adicionar o diretório de arquivos QEMU a seu caminho de pesquisa do OS X. Verifique o caminho da instalação para seus arquivos QEMU. Se você instalou o QEMU manualmente, procure o arquivo qemu-img em `/opt/local/bin` ou `/usr/local/bin`. Se você estiver usando o QEMU instalado com o GNS3, deverá encontrar o arquivo em `/Applications/GNS3.app/Contents/Resources/qemu/bin/`. Digite os seguintes comandos para adicionar os binários QEMU ao caminho de pesquisa do OS X. Faça uma cópia de backup do seu arquivo `.bash_profile` antes de começar.

```
$ cd ~
$ cp .bash_profile .bash_profile-backup
$ sudo echo 'export PATH=/Applications/GNS3.app/Contents/Resources/qemu/
bin:$PATH' >> .bash_profile
```

Depois de inserir os comandos, feche e reabra uma janela do terminal para ativar o novo caminho de pesquisa. Para verificar se seu caminho está correto, digite o seguinte comando:

```
$ echo $PATH
```

O comando anterior exibirá sua configuração de caminho. Se não estiver correto, pode ser necessário restaurar o arquivo `.bash_profile-backup` e tentar novamente. Se estiver correto, você está pronto para seguir em frente.

Começando

Comece a instalação criando um arquivo de imagem de disco virtual de 8 GB chamado juniper.img no seu diretório de construção. As opções de comando qemu-img usadas aqui devem funcionar em todos os sistemas similares ao Unix.

```
$ cd Juniper  
$ qemu-img create juniper.img 8G
```

Em seguida, inicialize o QEMU a partir do FreeBSD mini ISO usando o seguinte comando:

```
$ qemu-system-i386 -m 512 -hda juniper.img -localtime -cdrom 4.11-RELEASE-i386-miniinst.iso
```

Os usuários do Windows devem abrir um janela do prompt de comando e use os seguintes comandos. Certifique-se de inserir o comando path se o QEMU ainda não estiver no seu caminho do Windows.

```
c: cd Juniper  
c: path="c:\program files\GNS3\qemu-0.13.0"  
c: qemu-img create juniper.img 8G  
c: qemu-system-i386w -m 512 -hda juniper.img -localtime -cdrom 4.11-RELEASE-i386-miniinst.iso
```

Quando o FreeBSD é inicializado, o Menu de Configuração do Kernel aparece, como mostrado na Figura 6-2.

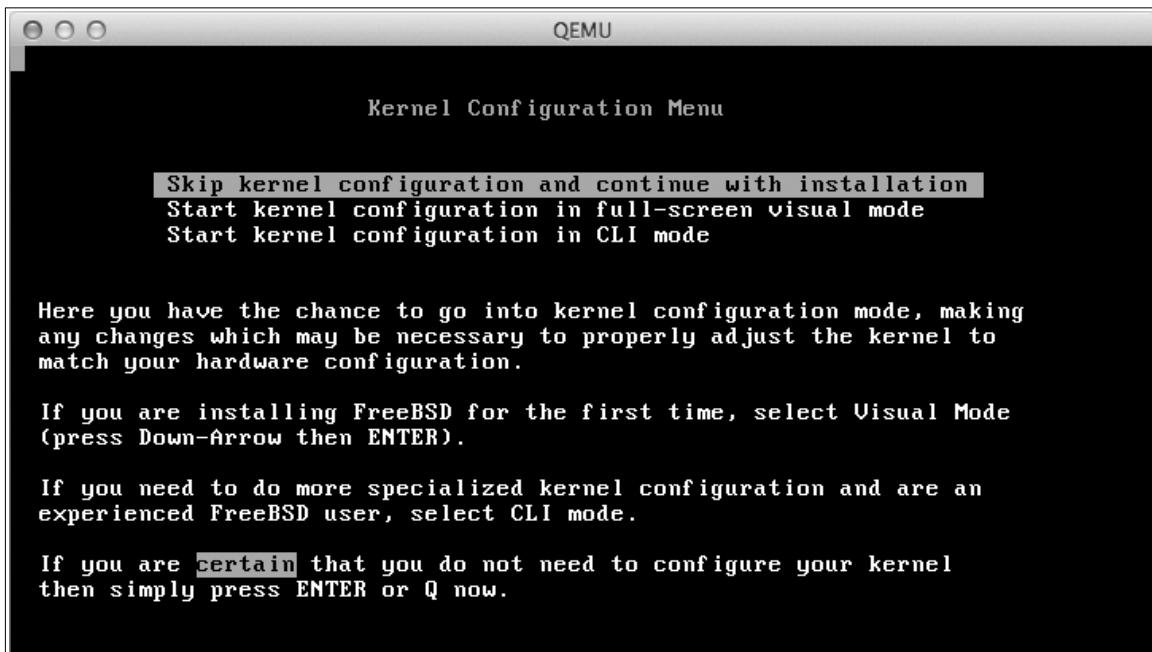


Figure 6-2: FreeBSD Kernel Configuration Menu

Pressione enter para pular a configuração do kernel e continue com a instalação. A seguir, o Menu Principal do sysinstall do FreeBSD aparece, mostrado na Figura 6-3.

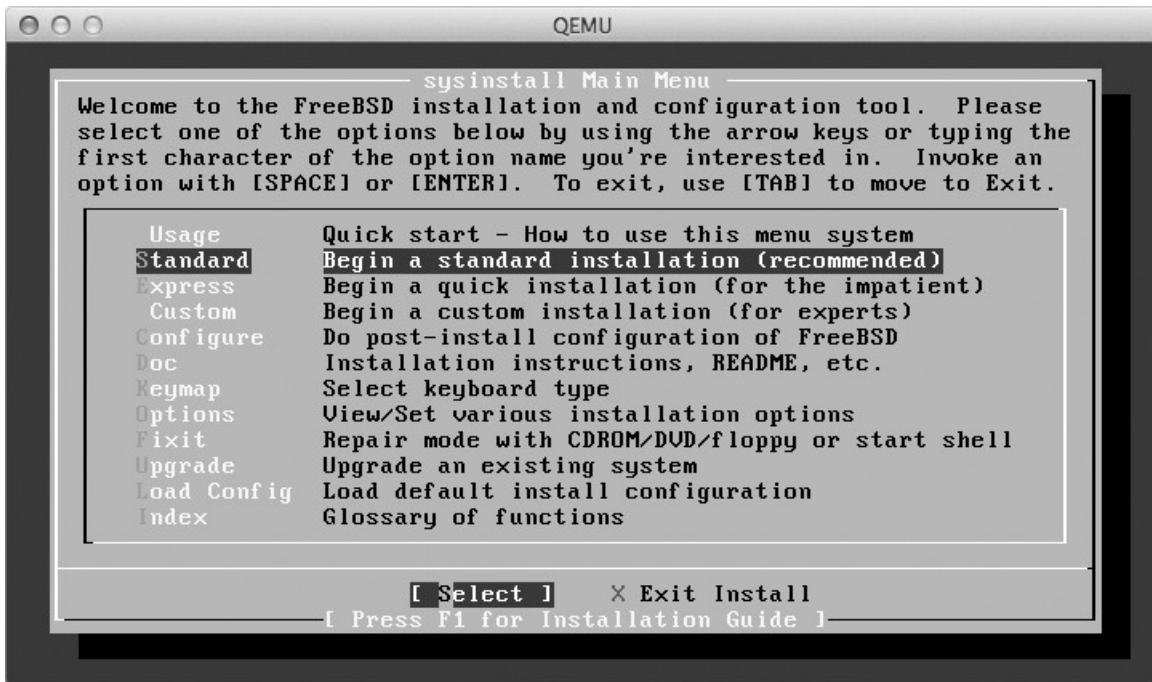


Figure 6-3: sysinstall Main Menu

Use a seta para descer, selecione Padrão para iniciar uma instalação padrão e pressione Enter para continuar.

Particionando o sistema de arquivos

A próxima tela, mostrada na Figura 6-4, exibe informações básicas sobre o uso do FDISK Partition Editor.

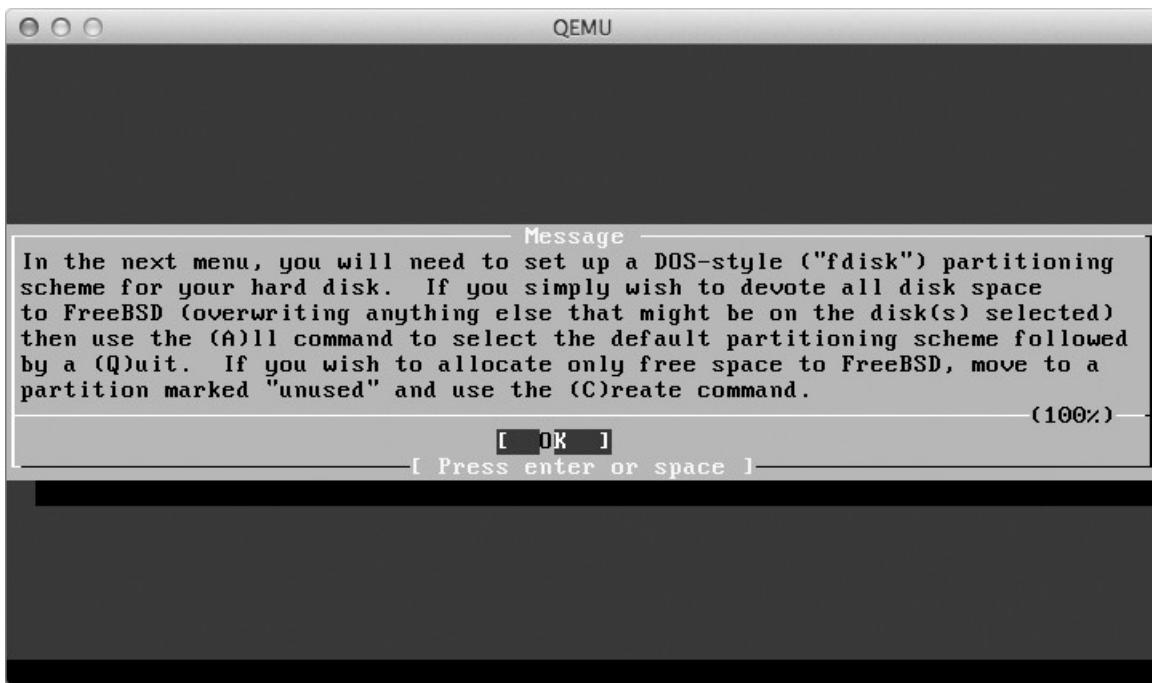


Figure 6-4: FDISK partitioning message screen

Leia as instruções e pressione Enter para continuar no FDISK Menu Editor de Partições, mostrado na Figura 6-5.

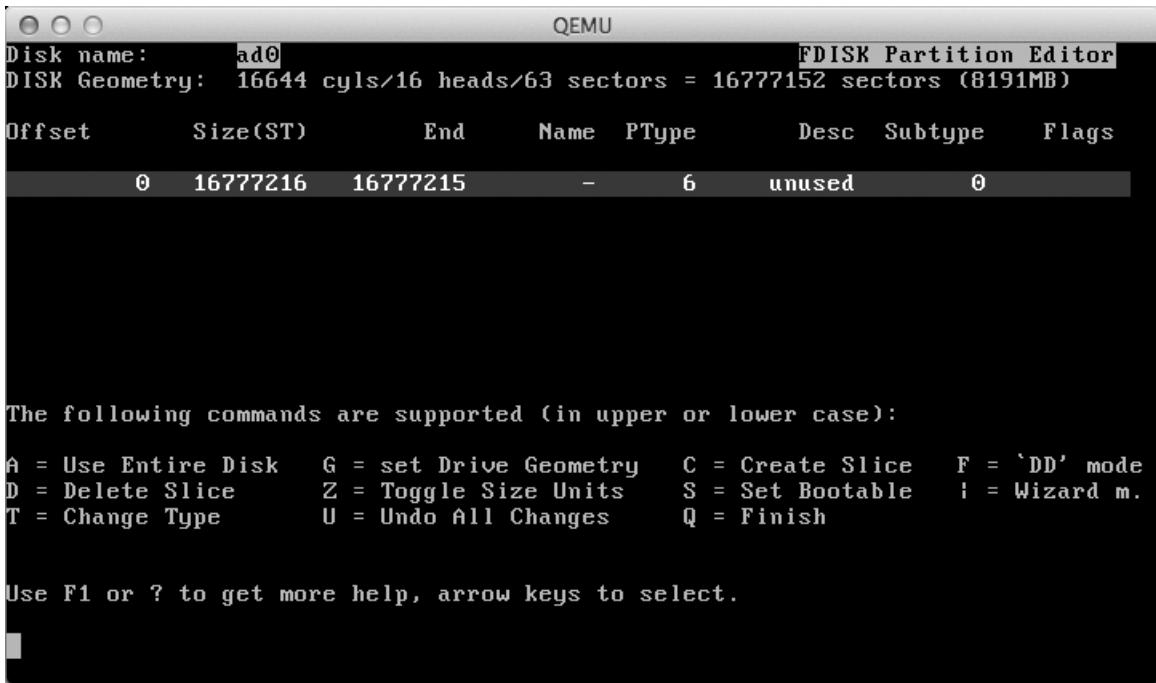


Figure 6-5: FDISK Partition Editor menu

O Editor de Partições FDISK permite escolher quanto espaço em disco você deseja alocar para o FreeBSD. Escolha *A* para usar o disco inteiro e selecione *Q* para concluir. O menu Install Boot Manager deve aparecer a seguir, como mostrado na Figura 6-6.

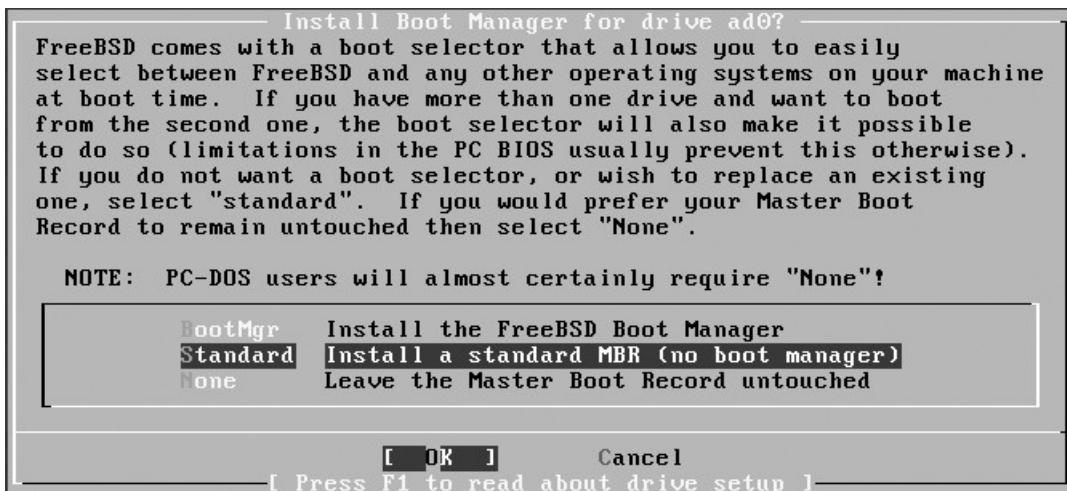


Figure 6-6: Install Boot Manager menu

Use a seta para descer, selecione *Standard* para instalar um registro mestre de inicialização padrão (MBR) e pressione Enter para continuar. O FreeBSD exibe uma mensagem sobre a criação de partições BSD dentro da sua partição FDISK recém-criada, como mostra a Figura 6-7.

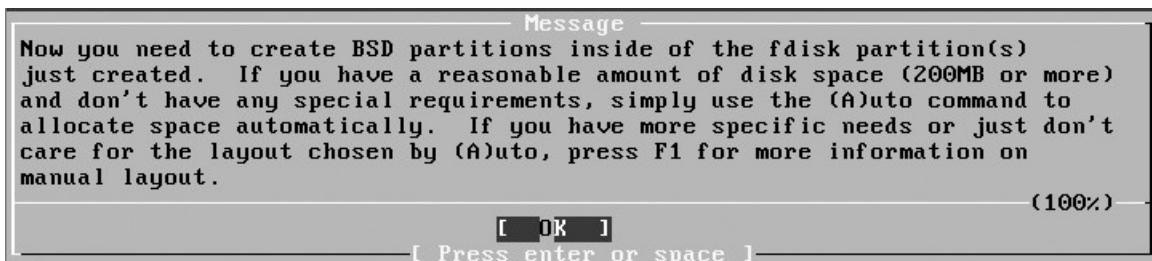


Figure 6-7: BSD partition message

Após ler a mensagem, pressione enter para continuar no FreeBSD Editor de disco. O próximo passo é criar partições compatíveis com o Juniper. É importante prestar muita atenção em como você partitiona o disco rígido virtual, porque o pacote Juniper Olive deve ver as partições corretas do FreeBSD ou a instalação falhará. Você também deve criar suas partições em uma ordem específica. Para criar sua primeira partição, selecione C e digite o tamanho da partição no campo fornecido, como mostra a Figura 6-8.



Figure 6-8: Specify a partition size.

Entrei com 1024M para criar uma partição de 1 GB. Pressione enter para aceitar esse valor e você verá a tela de opções do tipo de partição, mostrada na Figura 6-9.



Figure 6-9: Choose a partition type.

Pressione enter para criar um tipo de partição do sistema de arquivos (FS), e você terá a opção de escolher o ponto de montagem da partição, como mostra a Figura 6-10.



Figure 6-10: Choose a mount point for the partition.

Para criar um ponto de montagem para sua partição raiz, digite uma barra (/) e pressione enter para concluir a configuração da sua primeira partição. Usando a Tabela 6-1, siga o mesmo procedimento para criar o layout completo do sistema de arquivos. A ordem é importante! Após criar sua partição raiz (/), desça a lista, terminando com a partição /var. Quando você chegar à partição swap, escolha swap e não FS como seu tipo de partição. A partição /var é a última; portanto, quando você a cria, aceite o tamanho padrão do bloco de partição. Este valor usa o espaço livre restante na sua partição. Lembre-se, se as partições não forem criadas em ordem seqüencial, o os nomes das partições não corresponderão aos pontos de montagem e o Juniper Olive não será instalado corretamente.

Table 6-1: FreeBSD Partitioning for Juniper Olive		
Part	Mount	Size
ad0s1a	/	1024 MB
ad0s1b	swap	1024 MB
ad0s1e	/config	1024 MB
ad0s1f	/var	remaining space

Existem várias maneiras de particionar o FreeBSD em preparação para a instalação do Olive, mas achei esse método o mais confiável nas diferentes versões do Juniper Olive. Quando terminar, o sistema de arquivos deve ser exatamente igual ao da Figura 6-11.



Figure 6-11: Fully configured partition layout suitable for Juniper Olive

Depois de configurar todas as partições, escolha Q para concluir o processo de particionamento e, em seguida, escolha seu conjunto de distribuição, como mostra a Figura 6-12.

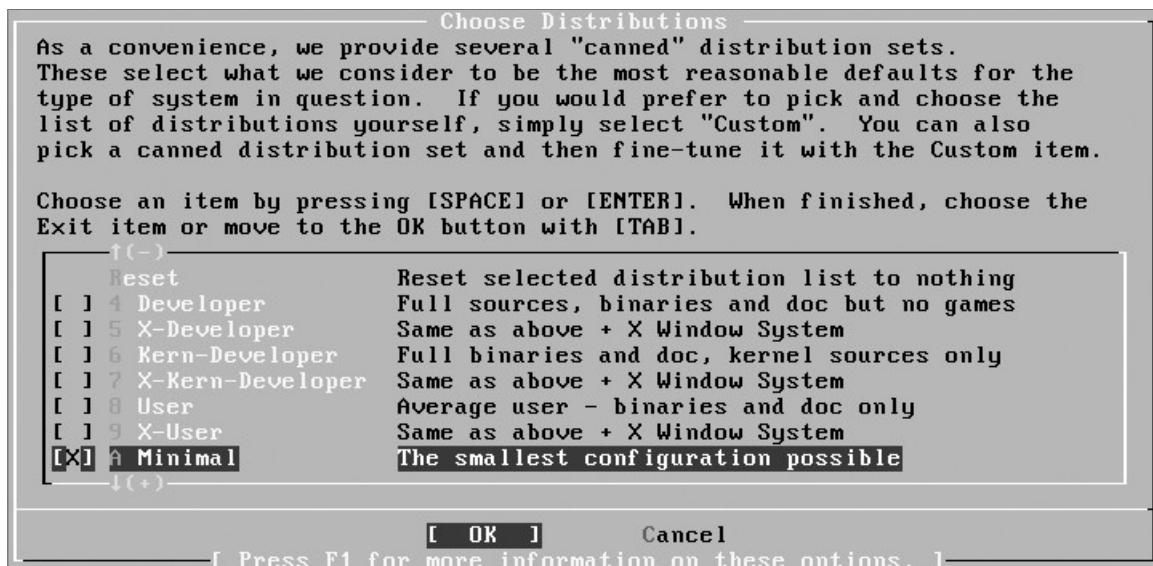


Figure 6-12: FreeBSD distribution choices

Use as teclas de seta para rolar para baixo, selecione *Minimal* e pressione o botão barra de espaço para fazer a seleção. Agora pressione tab para selecionar OK e pressione enter para concluir.

Finalizando a instalação do FreeBSD

Em seguida, escolha sua mídia de instalação, como mostra a Figura 6-13.

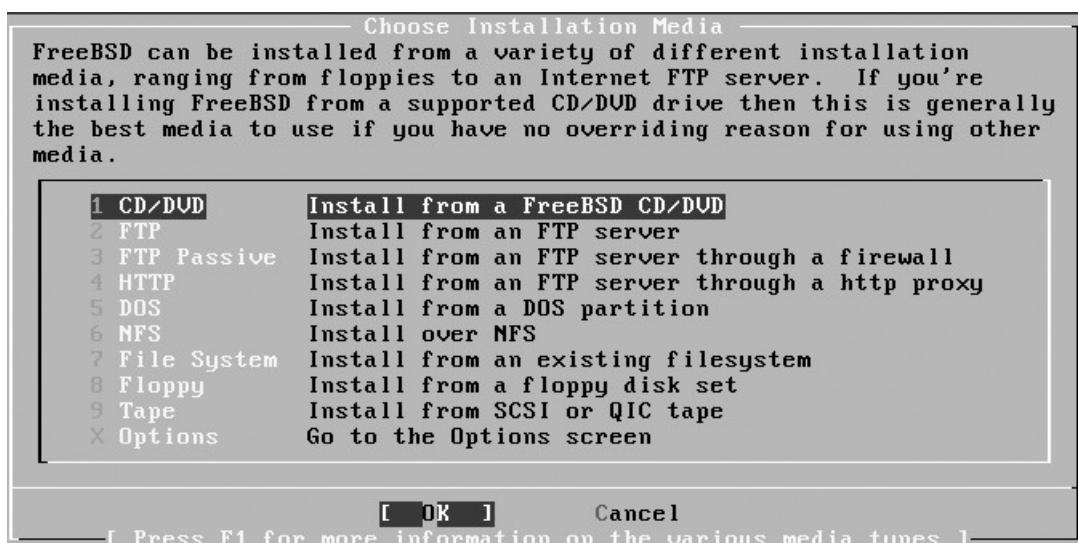


Figure 6-13: Choosing an installation media

Pressione enter para escolher CD / DVD como sua mídia de instalação, e a instalação começará. Quando terminar, a mensagem mostrada na Figura 6-14 aparece.

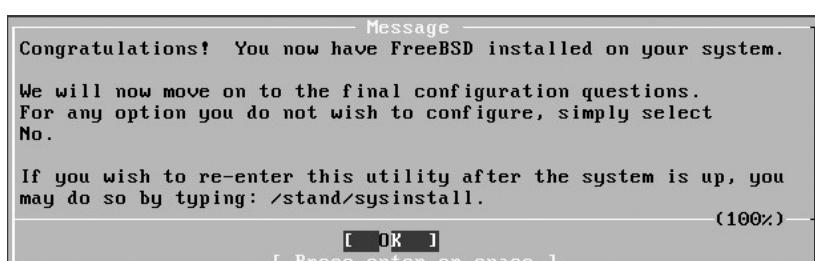


Figure 6-14: File installation complete message

Como você está usando o FreeBSD como host para o Junos OS, não precisa se preocupar com nenhuma das perguntas de configuração do FreeBSD que seguem esta tela. Responda “não” a todas as perguntas restantes e, quando solicitado a criar uma senha para a conta raiz, pressione enter para deixá-la em branco. Quando terminar de responder às perguntas, permita que o sistema reinicie, faça logon como root e encerre o FreeBSD usando o comando halt. Em seguida, feche a janela e feche o programa QEMU.

Instalando o pacote Juniper olive no FreeBSD

Agora que a instalação do FreeBSD está concluída, você pode instalar o pacote Juniper Olive.

Getting Your Olive Up and Running

Inicie o FreeBSD usando QEMU com o seguinte comando para garantir que você possa montar o arquivo de imagem do CD juniper-olive.iso que você criou anteriormente. (No Windows, substitua *qemu-system-i386* por *qemu-system-i386w*.)

```
qemu-system-i386 -m 512 -hda juniper.img -localtime -cdrom juniper-olive.iso
```

Se o FreeBSD for carregado corretamente, um prompt de login deve aparecer. Efetue login como root no prompt; você não precisa digitar uma senha, então pressione enter. Em seguida, use o comando mount para montar a imagem do CD *juniper-olive.iso*.

```
# mount /cdrom
```

Crie um diretório temporário chamado olive na partição */var* e extraia o pacote Juniper Olive para o diretório temporário.

```
# mkdir /var/tmp/olive  
# cd /var/tmp/olive  
# tar zxvf /cdrom/jinstall-12.1R1.9-domestic.tgz
```

Em seguida, modifique o Junos OS para permitir a instalação do software na sua Máquina virtual QEMU.

```
# mkdir temp  
# cd temp  
# tar zxvf ../pkgtools.tgz  
# cp /usr/bin/true bin/checkpic
```

Extraia o diretório *pkgtools* de *pkgtools.tgz* para outro diretório temporário no diretório olive e substitua o arquivo *checkpic* pelo arquivo *true* do FreeBSD. Isso remove a proteção *checkpic* do sistema operacional Junos. Após a modificação, gzin o conteúdo do diretório *temp* novamente em um *tarball* chamado *pkgtools.tgz* e remova o diretório temporário que você criou.

```
# tar zcvf ../pkgtools.tgz *  
# cd ..  
# rm -rf temp
```

Em seguida, crie uma nova instalação do Olive empacote e instale-o no seu sistema FreeBSD. Na lista a seguir, chamei o pacote de instalação de *olive.tgz*:

```
# tar zcvf ../olive.tgz *  
# pkg_add -f ../olive.tgz
```

Depois de instalar o pacote Olive, você verá uma mensagem de erro seguida de algumas mensagens de aviso, informando que o pacote apagará todos os arquivos que não são arquivos de configuração do Junos e que você precisa reiniciar para carregar o software Junos OS. Quaisquer outras instruções exibidas na tela podem ser ignoradas porque eles se aplicam a um roteador Juniper real, não a uma instalação do Olive em um PC. No entanto, antes de continuar, você precisa desligar o sistema FreeBSD usando o comando *halt* e sair do QEMU.

```
# halt
```

O passo final na instalação do Olive é reiniciar o sistema e dê tempo ao pacote para concluir sua aquisição do FreeBSD. Neste ponto, você deve fornecer ao instalador memória extra ou a instalação falhará. Embora o Junos OS funcione confortavelmente com 512 MB de RAM, o instalador precisa de 1024 MB de RAM para criar o disco RAM que ele usa durante a instalação. No Linux e OS X, inicialize o Juniper Olive com 1024 MB de RAM para concluir a instalação, da seguinte maneira:

```
$ sudo qemu-system-i386 -m 1024 -hda juniper.img -serial telnet:127.0.0.1:1001,server;nowait,nodelay -localtime
```

Os usuários do Windows devem digitar o seguinte comando:

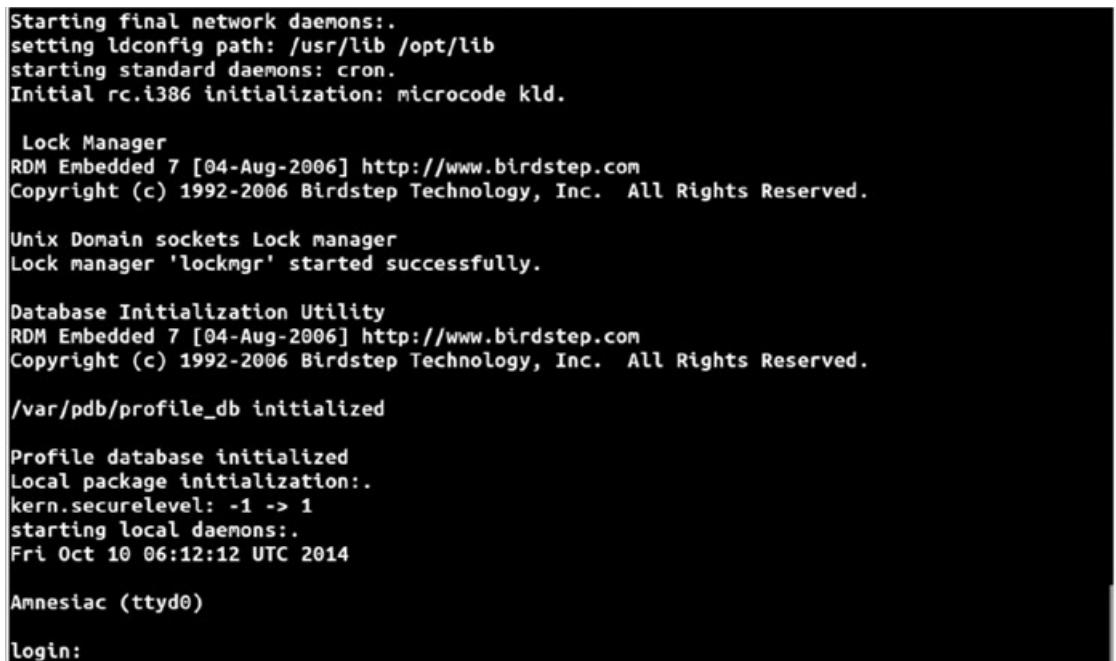
```
c: qemu-system-i386w -m 1024 -hda juniper.img -serial telnet:127.0.0.1:1001,server;nowait,nodelay -localtime
```

Depois de inicializar o sistema, você pode assistir o software Olive sendo instalado usando o telnet para conectar-se à porta 1001 do seu host local. (No Windows, talvez seja necessário instalar o programa Cliente Telnet primeiro no Painel de Controle de Programas e Recursos.) Abra um segundo prompt de comando ou janela do terminal do Windows e digite o seguinte comando para ver a saída da instalação exibida no console:

```
telnet localhost 1001
```

Eu recomendo monitorar sua instalação. É uma ótima maneira de solucionar problemas se algo der errado. Caso contrário, você não saberá por que uma instalação falhou. Um problema comum é que não há memória suficiente alocada para sua máquina virtual; outra é que os tamanhos das partições são muito pequenos ou foram criados incorretamente.

A instalação do Juniper Olive pode levar 15 minutos ou mais, dependendo no seu hardware, porque o instalador executa muitas tarefas, como reparticionar o disco rígido do FreeBSD e extrair vários pacotes. Quando tudo estiver completo, o sistema deve reiniciar automaticamente, carregar o Junos OS e apresentar o que parece ser um prompt de login do FreeBSD, mostrado na Figura 6-15.



```
Starting final network daemons..
setting ldconfig path: /usr/lib /opt/lib
starting standard daemons: cron.
Initial rc.i386 initialization: microcode kld.

Lock Manager
RDM Embedded 7 [04-Aug-2006] http://www.birdstep.com
Copyright (c) 1992-2006 Birdstep Technology, Inc. All Rights Reserved.

Unix Domain sockets Lock manager
Lock manager 'lockmgr' started successfully.

Database Initialization Utility
RDM Embedded 7 [04-Aug-2006] http://www.birdstep.com
Copyright (c) 1992-2006 Birdstep Technology, Inc. All Rights Reserved.

/var/pdb/profile_db initialized

Profile database initialized
Local package initialization:.
kern.securelevel: -1 -> 1
starting local daemons:.
Fri Oct 10 06:12:12 UTC 2014

Amnesiac (ttyd0)

login:
```

Figure 6-15: Successful Junos OS boot messages and login

Esse prompt é onde você faz login no Junos OS. Se você vir as mensagens anteriores e o prompt de login, o seu roteador Juniper estará pronto para uso.

Fazendo backup Juniper Olive

Depois de criar um Olive funcional, faça uma cópia de segurança da imagem para proteção. Afinal, quem quer passar por todo esse trabalho novamente? Eu não! Primeiro, desligue corretamente o Junos OS para impedir o acionamento de um sistema de arquivos sujo. Um sistema de arquivos sujo ocorre quando os arquivos não foram fechados corretamente. Essa condição pode causar corrupção de arquivo e pode até quebrar o sistema operacional Junos. Se o sistema de arquivos estiver marcado como sujo, uma verificação do sistema de arquivos será acionada na próxima vez em que você iniciar o Junos OS, e pode demorar mais que o normal para inicializar até que o sistema seja verificado e marcado como limpo novamente (o que significa que nenhum erro foi encontrado ou todos os erros foram corrigidos). Para desligar o Junos OS, efetue login como root (nenhuma senha é necessária) e insira os seguintes comandos:

```
Login: root
root@% cli
root> request system halt
Halt the system ? [yes,no] (no) yes
```

É seguro sair do QEMU depois de ver uma mensagem indicando que o sistema operacional foi interrompido, conforme mostrado aqui:

```
The operating system has halted.
Please press any key to reboot.
```

Para fazer uma cópia de backup da sua imagem Juniper, digite o seguinte comando no diretório em que seu arquivo de imagem está salvo:

```
$ cp juniper.img backup-juniper.img
```

Os usuários do Windows podem usar este comando:

```
c: copy juniper.img backup-juniper.img
```

Agora que você tem um roteador Juniper, você precisa configurar o GNS3 para que ele possa ser usado em seus projetos.

Configurando um roteador Juniper no GNS3

Para configurar um roteador Juniper no GNS3, selecione **Edit ▶ Preferences** em Windows e Linux ou **GNS3 ▶ Preferences** no OS X. Clique duas vezes em **QEMU** na barra lateral e selecione **QEMU VMs** para abrir a janela de preferências de QEMU VMs, mostrada na Figura 6-16.

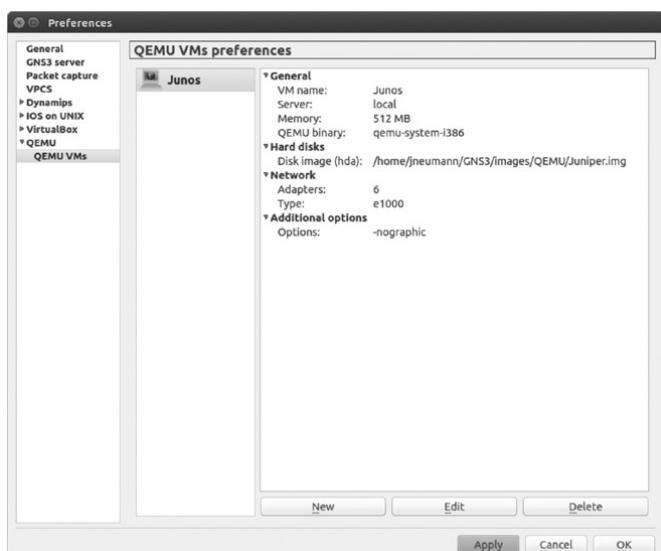


Figure 6-16: QEMU VMs preferences window

A partir daqui, você pode criar, editar e excluir máquinas virtuais QEMU, permitindo que você leve sua máquina virtual Juniper para o GNS3.

Adicionando a Juniper Virtual Machine ao GNS3

Para adicionar sua máquina virtual Juniper ao GNS3, clique em **New** para iniciar o assistente de Nova VM QEMU. Digite um nome para sua máquina virtual e deixe Tipo definido como **Default**. Clique em **Next** para definir as opções binárias e de memória do QEMU, mostradas na Figura 6-17.

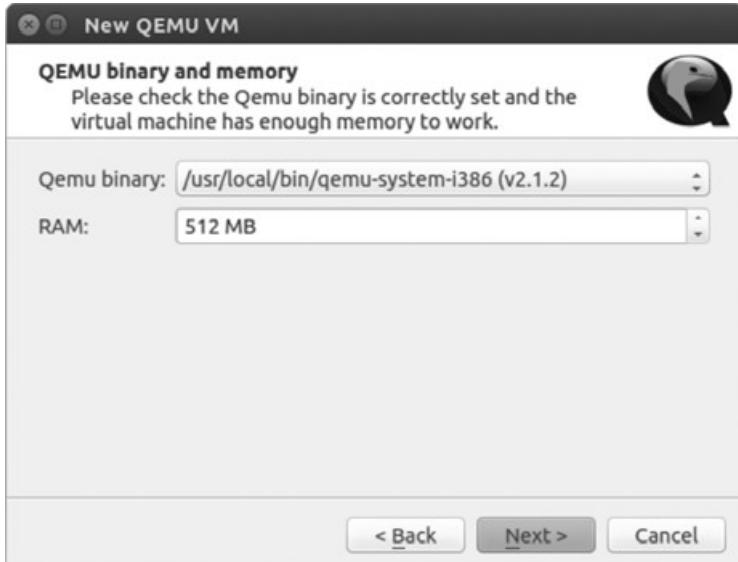


Figure 6-17: Setting QEMU binary and memory

Selecione **qemu-system-i386** no menu suspenso binário do Qemu. Você está escolhendo este programa QEMU porque o Juniper Olive é executado em uma versão de 32 bits do FreeBSD. Dê ao Olive 512MB de RAM e clique em **Next**. Clique em **Browse** para localizar e selecionar o arquivo *juniper.img* que você criou anteriormente e clique em **Finish**.

Nota

Dois aplicativos binários QEMU são frequentemente usados no GNS3: *qemu-system-i386* e *qemu-system-x86_64*. A diferença entre eles é que o *qemu-system-i386* foi projetado para emular a arquitetura de 32 bits, e o *qemu-system-x86_64* foi projetado para emular a arquitetura de 64 bits. O aplicativo *qemu-system-x86_64* deve ser compatível com versões anteriores de 32 bits, mas não é compatível com todas as máquinas virtuais de 32 bits (incluindo o IOS-XRv, por exemplo).

Adicionando interfaces Ethernet

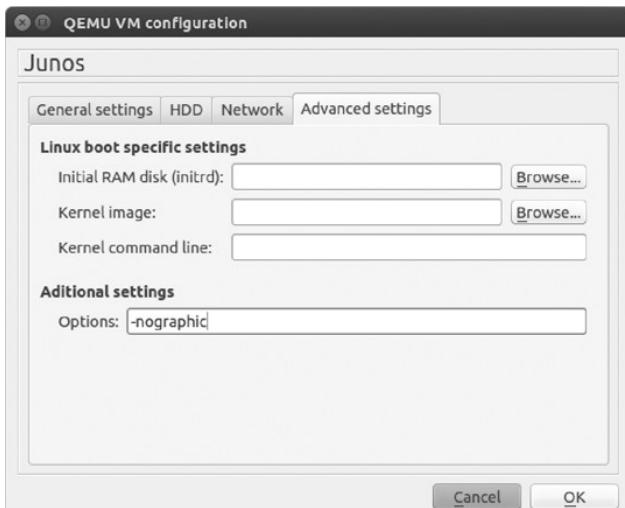


Figure 6-18: QEMU advanced options

Depois de criar sua máquina virtual, volte e adicione mais interfaces Ethernet. Eu recomendo o uso de seis interfaces. Destaque sua máquina virtual e selecione **Edit**. Clique na guia **Network** e altere o número de interfaces para 6.

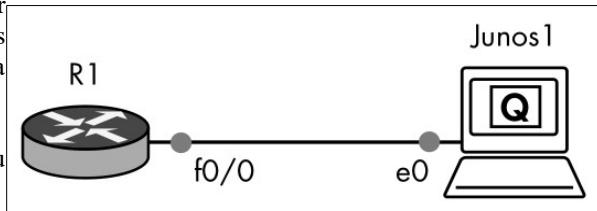
Agora selecione a guia **Advanced settings** e insira a opção **-nographic** em Configurações adicionais, como mostrado na Figura 6-18.

A opção **-nographic** impede a interface QEMU GUI da exibição quando você inicia sua máquina virtual QEMU. Embora a GUI possa ser útil na solução de problemas de uma máquina virtual, costuma ser um incômodo e deve ser desativada. Esta opção pode ser usada com qualquer máquina virtual QEMU, não apenas com o Juniper. Quando terminar, clique em **OK** para fechar a janela e clique em Aplicar e **OK** para salvar todas suas alterações.

Testando um roteador Juniper

Antes de criar projetos que incluem roteadores Juniper, é uma boa ideia testar a conectividade entre um roteador Cisco e um roteador Juniper. Se você não conseguir executar o ping com êxito entre os dispositivos, pode haver um problema com sua instalação e é melhor descobrir antes que você gaste horas projetando um projeto que não funciona.

Arraste um nó do roteador Cisco e um nó do roteador Juniper para seu espaço de trabalho na barra de ferramentas Dispositivos e crie um link do roteador Cisco para fazer a interface e0 do roteador Juniper, como mostra a Figura 6-19. Inicie os roteadores e abra um console para o roteador Cisco. Atribua um endereço IP à interface que está conectada ao seu roteador Juniper (f0/0, neste exemplo).



```
R1> enable
R1# configure-terminal
R1(config)# interface f0/0
R1(config-if)# ip address 10.10.10.1 255.255.255.0
R1(config-if)# no shutdown
```

Agora abra um console no seu roteador Juniper, faça logon e configure um endereço IP usando a mesma sub-rede que o seu roteador Cisco.

```
Login: root
root@% cli
root> edit
root# set system root-authentication plain-text password
New password: olive1
Retype new password: olive1
root# set interfaces em0 unit 0 family inet address 10.10.10.2/24
root# commit
commit complete
```

Por segurança, o Junos OS exige que você atribua uma senha raiz u antes de confirmar outras alterações na configuração do roteador, faça isso agora. Defino a senha como olive1, mas você pode inserir qualquer senha que desejar.

Nota

Neste exemplo, você pode ver que a sintaxe do Juniper é totalmente diferente da sintaxe da Cisco. Se a sintaxe do Juniper for nova para você, visite o site da Juniper (<http://www.juniper.net/>) para obter informações detalhadas sobre a configuração de roteadores Juniper.

Depois de configurar os dois dispositivos, execute ping no seu roteador Cisco para testar a conectividade.

```
root# exit
root> ping 10.10.10.1
```

Se o teste de ping falhar, pode haver um problema com seus endereços IP ou instalação QEMU. Se você compilou o QEMU a partir do código-fonte, verifique se você instalou uma versão conhecida por funcionar com o Juniper Olive. Se necessário, compile e reinstale o QEMU novamente. Se o problema persistir, tente instalar ou compilar outra versão do QEMU. Você também pode criar um Olive usando o VirtualBox. O procedimento é basicamente o mesmo que o QEMU, mas você usará as ferramentas da GUI do VirtualBox em vez da linha de comando. Ao criar sua máquina virtual VirtualBox, defina Type como BSD e Version como FreeBSD (32 bits).

Executando o Juniper vSrX firefly

Além do Junos OS, você pode executar uma versão virtual do SRX Firewall da Juniper, chamada *vSRX Firefly*. Se você se registrar no Juniper, poderá fazer o download de uma avaliação do Firefly no site gratuitamente (<http://www.juniper.net/>). Você deseja fazer o download do pacote Firefly VMware Appliance - PARA AVALIAÇÃO!

Como você pode ver pelo nome, ele foi projetado para ser executado no VMware, mas você pode ajustá-lo para ser executado no VirtualBox ou QEMU. Estou abordando o VirtualBox aqui. Verifique se o programa VirtualBox está instalado no seu sistema antes de começar. Depois de baixar o software Firefly, observe que é um arquivo OVA (Open Virtual Appliance), chamado algo como *junos-vsrx-ver.x-domestic.ova*. Um arquivo OVA é um arquivo de pacote especial que pode ser desarquivado usando o comando tar. Para extrair o conteúdo do arquivo no Linux ou OS X, use o seguinte comando:

```
$ tar xvf junos-vsrx-ver.x-domestic.ova
```

Nota

Se você estiver executando o Windows, poderá usar o aplicativo 7-zip (<http://www.7-zip.org/>) para extrair os arquivos.

Após a extração de todos os arquivos, você precisa converter o arquivo de disco da máquina virtual VMware (o arquivo com extensão .vmdk) em um arquivo de imagem de disco virtual (VDI) que pode ser usado pelo VirtualBox. Para converter o arquivo, use o utilitário *vboxmanage* que acompanha o VirtualBox.

```
$ vboxmanage clonehd -format VDI junos-vsrx-ver.x-domestic-disk1.vmdk junos-vsrx-ver.x-domestic-disk1.vdi
```

Após converter a imagem do disco, é possível excluir todos os arquivos Firefly, exceto o novo arquivo de imagem VDI (neste exemplo, *junos-vsrx-ver.x-domestic-disk1.vdi*). Este é o arquivo de imagem do disco rígido que você importará para o VirtualBox.

Criando uma máquina virtual Firefly com o VirtualBox

Você precisa criar uma nova máquina virtual no VirtualBox e importar o Arquivo de imagem do disco rígido Firefly. Inicie o VirtualBox e clique em **New** para abrir a caixa de diálogo **Create Virtual Machine**, mostrada na Figura 6-20.



Figure 6-20: Create Virtual Machine dialog

Atribua um nome à máquina virtual (Firefly neste exemplo), defina Type para BSD e Version para FreeBSD (32 bits). Quando terminar, clique em Avançar para atribuir o tamanho da memória, como mostra a Figura 6-21.

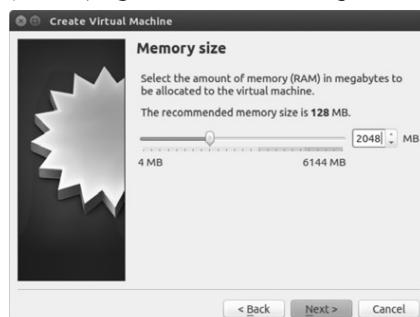


Figure 6-21: Adjust the memory size.

Siga as instruções do Juniper para definir o tamanho de memória adequado. Neste exemplo, escolhi 2048 MB, porque é isso que a Juniper recomenda para minha versão do Firefly. Quando terminar, clique em **Next** e marque **Use an existing virtual hard drive file**, como mostra a Figura 6-22. Use o ícone de navegação para localizar e escolher o arquivo de imagem VDI criado anteriormente. Quando terminar, clique no botão **Create** para criar a máquina virtual.



Figure 6-22: Choose the Junos vSRX Firefly VDI hard disk image file.

Dando à sua máquina virtual mais processadores

Depois de criar a máquina virtual, você deve aumentar o número de processadores para dois porque o vSRX Firefly precisa de dois processadores para funcionar corretamente. Se sua máquina virtual estiver configurada com apenas um processador, o Firefly será inicializado e executado, mas você não poderá ver nem configurar nenhuma interface Ethernet. Selecione o nome da sua máquina virtual no VirtualBox, vá para **Settings** ▶ **System** e clique na guia **Processor**, mostrada na Figura 6-23.

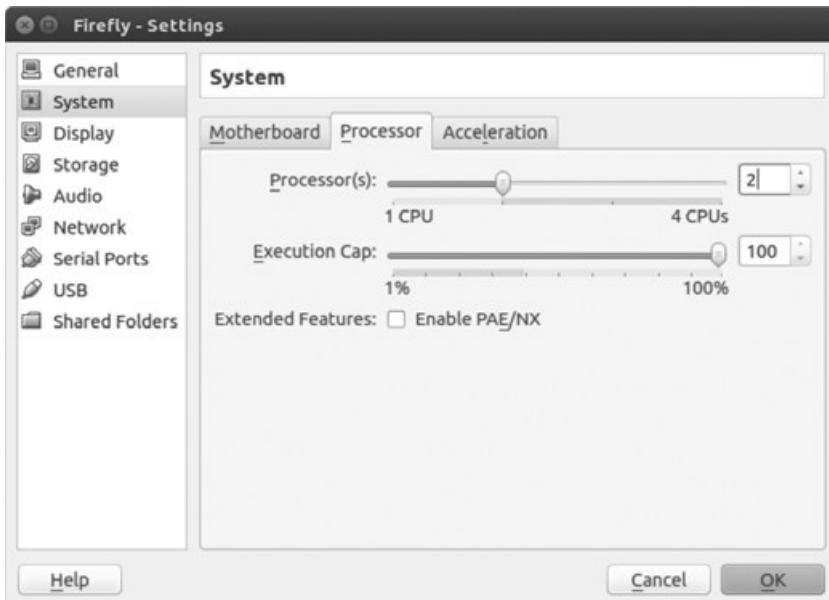


Figure 6-23: The Processor tab under System

Use a ferramenta deslizante para selecionar dois processadores e clique em **OK**. Depois de configurar sua máquina virtual Firefly, clique com o botão direito do mouse em sua máquina virtual no VirtualBox e selecione **Clone** para criar uma cópia para trabalhar no GNS3. A máquina virtual original permanecerá sem uso e você sempre terá um mestre limpo e não configurado da sua máquina virtual. Depois de criar a máquina virtual Firefly, você precisará adicioná-lo ao GNS3 antes de poder usá-lo em seus projetos.

Adicionando vSRX Firefly ao GNS3

Inicie o GNS3 e selecione **Edit** ▶ **Preferences** no Windows e Linux ou **GNS3** ▶ **Preferences** no OS X.

Clique duas vezes em **VirtualBox** no painel à esquerda e selecione **VirtualBox VMs** para abrir a janela de preferências das VMs do VirtualBox, mostrada na Figura 6-24. Para adicionar sua máquina virtual Firefly VirtualBox ao GNS3, clique em **New** para iniciar o assistente para Nova VM virtual. Selecione sua máquina virtual Firefly no menu suspenso e clique em **Finish**. Em seguida, clique em **Edit**.

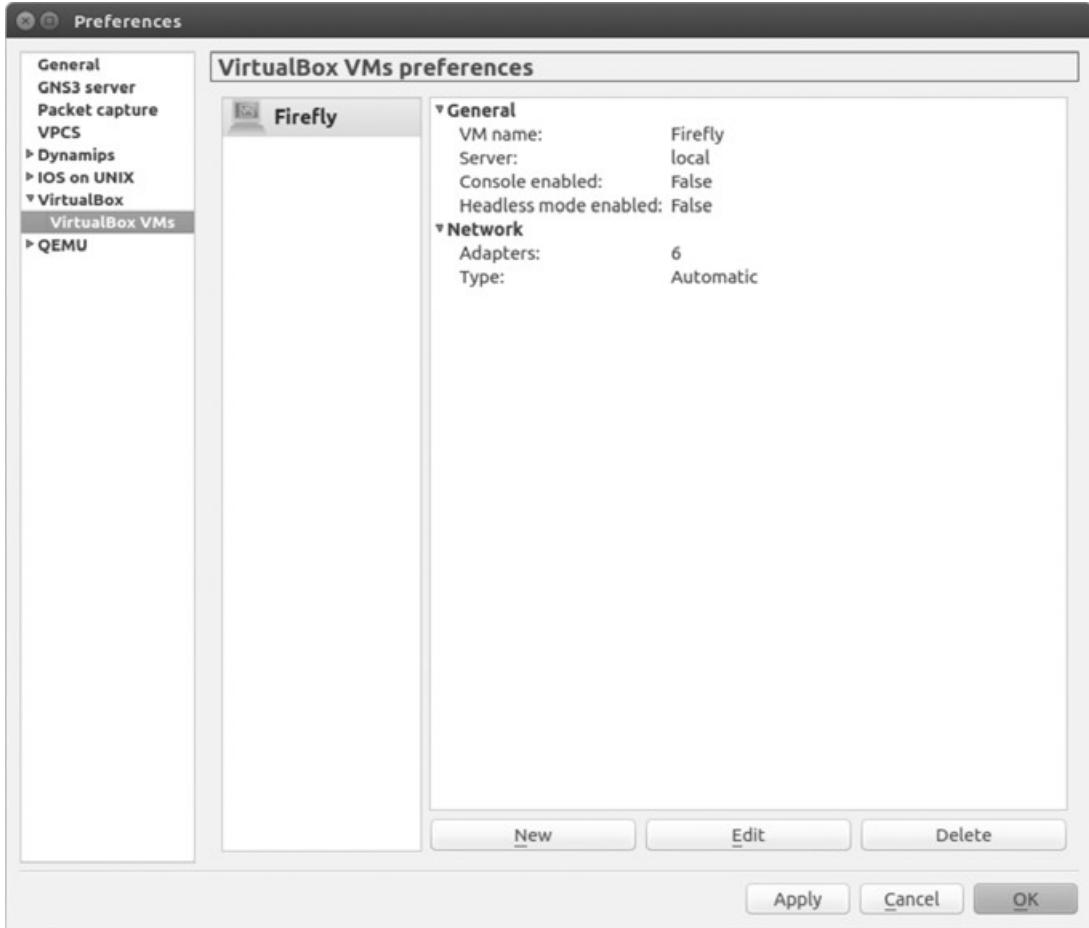


Figure 6-24: VirtualBox VMs preferences window

Na guia Configurações gerais, marque **Enable remote console** e **Start VM in headless mode**. Isso permitirá que você use o console para fazer logon no Firefly. Por fim, clique na guia **Network**, altere o número de interfaces para 6 e defina o tipo de rede como **Paravirtualized Network (virtio net)**. Agora você está pronto para criar um projeto usando o Firefly.

Criando um projeto com um firewall baseado em região

Nesta seção, você criará um projeto simples usando o vSRX Firefly como um firewall de rede. O Firefly é semelhante em funcionalidade ao firewall ASA da Cisco, mas é diferente de configurar. Eu não vou entrar em muitos detalhes, mas este projeto deve começar. Se você quiser saber mais sobre o Juniper SRX, pode encontrar muitos documentos detalhados no site da Juniper (<https://www.juniper.net/>). Vamos começar criando o projeto GNS3 mostrado na Figura 6-25. Arraste um dispositivo Firefly da barra de ferramentas **End Devices** para o seu espaço de trabalho. Em seguida, arraste dois roteadores Cisco para o seu espaço de trabalho e vincule os dispositivos. Vincule a interface f0/0 de R1 à interface e1 do vSRX Firefly. Vincule a interface f0/0 do R2 à interface e0 do vSRX Firefly.

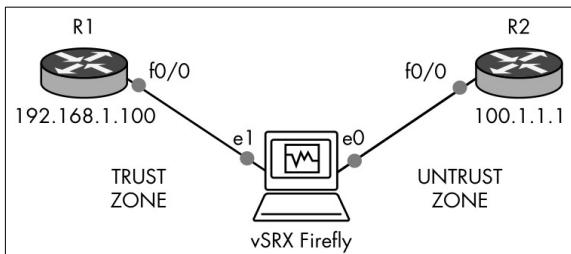


Figure 6-25: vSRX Firefly project

O roteador R1 será configurado para usar uma zona de confiança Firefly. R1 representa um host confiável na sua LAN. O roteador R2 será configurado para usar uma zona não confiável do Firefly. A zona não confiável representa uma rede não confiável, como a Internet. Você configurará o Firefly para que seu host confiável (R1) possa executar ping no host não confiável (R2) através do firewall vSRX Firefly usando NAT. Comece configurando o roteador R1 com um endereço IP e um gateway padrão.

```
R1(config)# interface f0/0
R1(config-if)# ip address 192.168.1.100 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Em seguida, configure um endereço IP no roteador não confiável R2. Nenhuma configuração de gateway é necessária aqui.

```
R2(config)# interface f0/0
R2(config-if)# ip address 100.1.1.1 255.255.255.0
R2(config-if)# no shutdown
```

Com os endereços IP do roteador configurados, você pode voltar sua atenção para Firefly. Faça logon usando a conta root para configurar o firewall vSRX Firefly. Por se tratar de uma nova instalação, não é necessário solicitar uma senha. Após o logon, digite os seguintes comandos para criar seu firewall; você começará criando uma senha e definindo as configurações de rede:

```
root@%cli
root>edit
1 root#set system root-authentication plain-text-password
New password:firefly1
Retype new password:firefly1
2 root#set interface ge-0/0/0.0 family inet address 100.1.1.2/24
3 root#set interface ge-0/0/1.0 family inet address 192.168.1.1/24
4 root#set routing-options static route 0.0.0.0/0 next-hop 100.1.1.1
```

Como um roteador Juniper, você não pode salvar nenhuma alteração na configuração de um dispositivo SRX até atribuir uma senha à conta root **1**; portanto, comece no modo de edição e crie uma senha raiz. Eu inseri o *firefly1*, mas você pode escolher qualquer senha que desejar. Em seguida, em **2**, você define o endereço IP na interface WAN (ge-0/0 / 0.0), e em **3**, você define a interface da rede local (ge-0/0 / 1.0). Por fim, em **4**, defina o endereço de gateway padrão usando o endereço IP do roteador não confiável (100.1.1.1). Conclua a configuração definindo suas zonas de segurança e políticas de confiança de segurança.

```
1 root#set security zones security-zone trust interfaces ge-0/0/1.0
2 root#set security nat source rule-set interface-nat from zone trust
3 root#set security nat source rule-set interface-nat to zone untrust
4 root#set security nat source rule-set interface-nat rule rule1 match source-address 0.0.0.0/0 destination-address 0.0.0.0/0
5 root#set security nat source rule-set interface-nat rule rule1 then source-nat interface
6 root#set security policies from-zone trust to-zone untrust policy permit-all match source-address any destination-address any application any
7 root#set security policies from-zone trust to-zone untrust policy permit-all then permit
8 root#commit
```

Atribua sua interface LAN à zona confiável **1**. Defina a zona de origem da interface-nat para confiar em **2** e a zona de destino da interface-nat para não confiar em **3** e crie uma regra que corresponda a qualquer endereço IP de origem e de destino (0.0.0.0/0) **4**. Em um ambiente de produção, você reforçaria um pouco isso, mas para o laboratório GNS3, tudo bem. Agora configure sobrecarga de NAT na interface WAN **5**.

Nota

O comando **interface-nat** do vSRX Firefly é usado para obter o equivalente à **NAT/PAT overloading**.

Para concluir a configuração, defina o tipo de tráfego permitido para ir entre as zonas **6**. Nesse caso, você está permitindo todos os protocolos e aplicativos da zona confiável para a zona não confiável. Por fim, crie a política de segurança **7** e confirme suas alterações **8** e pronto! Verifique sua configuração digitando o comando *show security nat source summary*.

```
root>show security nat source summary
Total port number usage for port translation pool: 0
Maximum port number for port translation pool: 33554432
Total pools: 0
```

Total rules: 1				
Rule name	Rule set	From	To	Action
rule11	interface-nat2	trust3	untrust4	interface5

Esta informação indica que a regra **1** permite pacotes via NAT **2** da zona confiável **3** para a zona não confiável **4**, e os dados IP provenientes da zona confiável serão sobrecarregados na interface não confiável **5**. Por padrão, essa é a interface ge-0/0 / 0.0 (sua interface WAN). Se o seu resumo corresponder ao deste livro depois de inserir o comando, você estará pronto para testar a conexão. Se sua saída parecer diferente, você provavelmente digitou algo incorretamente, então você precisa voltar e verificar todas as suas definições de configuração. Faça logon no roteador R1 e insira o comando ping para testar a conectividade com o roteador R2.

```
R1#ping 100.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/10/24 ms
```

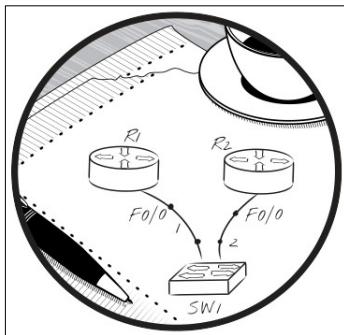
Se o seu ping for bem-sucedido, como indicado por **!!!!!**, então você fez tudo corretamente. Se falhar, pode ser necessário voltar e verificar as configurações. Você também deve garantir que seus roteadores Cisco tenham os endereços IP e máscaras de sub-rede corretos e que as interfaces Ethernet não sejam desligadas.

Considerações finais

Neste capítulo, você aprendeu sobre o Juniper e o Juniper Olive e eu mostrei como criar um Juniper Olive usando o QEMU e o VirtualBox. Também apresentei o vSRX Firefly e forneci algumas dicas sobre como configurar um firewall básico baseado em zona usando um dispositivo SRX. Na maioria dos casos, o Juniper executa um pouco mais lentamente usando o QEMU do que usando o VirtualBox. No entanto, o QEMU permite que você adicione um número ilimitado de roteadores Juniper aos seus projetos sem clonar, e o GNS3 armazenará suas configurações do Juniper nos seus projetos. Como regra, o VirtualBox carrega e executa dispositivos mais rapidamente que o QEMU, mas suas configurações são salvas com cada instância da máquina virtual no VirtualBox, não no GNS3. Por isso, é necessário criar uma instância única de máquina virtual dos seus dispositivos usando o recurso de clone do VirtualBox. Os dispositivos clonados são usados nos seus projetos GNS3.

O Juniper é menos popular que a Cisco no mundo corporativo, mas é um grande participante em ambientes maiores, como sites de campus e o mercado de roteamento e comutação de ISP. Se você levar sua carreira de rede para um desses domínios, a certificação Juniper poderá diferenciá-lo de outros candidatos, e o GNS3 é uma ótima maneira de aprender roteadores Juniper e dispositivos SRX! Você deve começar com a certificação JNCIA, que é a certificação Juniper básica (a Juniper equivale ao Cisco CCNA) e é um pré-requisito para certificações mais avançadas. O site de treinamento da Juniper (<http://www.juniper.net/us/en/training/>) fornece todas as informações necessárias para você começar.

DEVICE NODES, LIVE SWITCHES, AND THE INTERNET



Neste capítulo, demonstrarei como os nós do dispositivo GNS3 são usados com os roteadores Cisco IOS. O GNS3 fornece um nó Hub e vários nós do Switch, incluindo um switch Ethernet, roteador EtherSwitch, switch ATM e switch Frame Relay. Além disso, veremos como criar seu próprio switch Frame Relay usando um roteador Cisco IOS.

Também exploraremos um recurso muito poderoso conhecido como *Cloud node*. Um Cloud node é usado para expandir suas redes além do programa GNS3. Com os nós da nuvem, em breve você poderá conectar seus projetos GNS3 a switches da Cisco e acessar a Internet usando roteadores GNS3.

Nós de dispositivo integrados

Nós de dispositivo integrados simulam os recursos de um tipo de dispositivo específico (como um Switch). Eles são fáceis de configurar e podem ser úteis se você precisar economizar tempo e recursos do PC ou se quiser fazer algo sem conhecer todos os detalhes da tecnologia subjacente. Se você criar uma topologia que usa VLANs, você pode arrastar um nó do switch Ethernet GNS3 para sua área de trabalho e usar um menu simples para criar rapidamente VLANs ou troncos de VLAN. Obviamente, se você estiver estudando para um exame da Cisco que envolva switch, precisará saber como configurar os switches Cisco IOS reais.

Configurador de nó

Até agora, você já sabe que o configurador do Nó pode ser usado para configurar os recursos de um único nó do dispositivo, mas também pode ser usado para modificar vários dispositivos ao mesmo tempo. À medida que seus projetos crescem e você usa mais dispositivos, esse recurso pode economizar muito tempo. Para abrir vários dispositivos ao mesmo tempo, use o mouse para selecionar nesses dispositivos no seu espaço de trabalho, clique com o botão direito do mouse em qualquer dispositivo e escolha **Configure**. Os dispositivos selecionados são exibidos no configurador do nó, como mostrado na Figura 7-1.

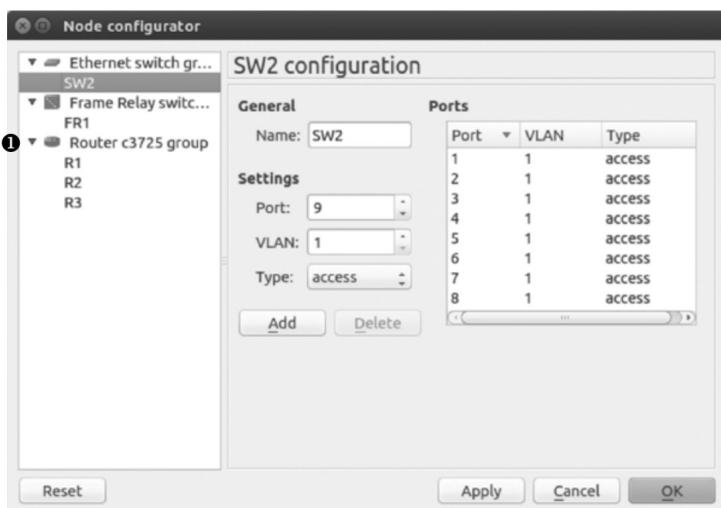


Figure 7-1: Modifying multiple devices using the Node configurator

Para configurar um único dispositivo, selecione esse dispositivo na coluna à esquerda. Configure cada dispositivo e clique em **Apply**. Quando você terminar de configurar todos os dispositivos, clique em **OK** para concluir o processo.

Para modificar vários dispositivos, use a tecla Shift para selecionar vários de uma vez da coluna à esquerda e configure-os da mesma maneira que faria com um único dispositivo. Digamos que você tenha dez roteadores da série

7200 e deseja adicionar o mesmo módulo de rede ao slot 0 em todos os 10 roteadores. Use a tecla Shift para selecionar todos os roteadores, adicione o módulo ao slot 0 e clique em Aplicar e OK para fazer a alteração nos 10 dispositivos.

Você também pode selecionar um grupo inteiro de roteadores clicando no grupo nome. Na figura anterior, você pode configurar R1, R2 e R3 no mesmo tempo, selecionando o nome do grupo *Router c3725 group* ①.

Ethernet hub

O GNS3 fornece um hub Ethernet (consulte a Figura 7-2) como uma ferramenta que os instrutores de rede podem usar para ensinar aos alunos os perigos dos loops Ethernet, difusões excessivas e repetição de várias portas.

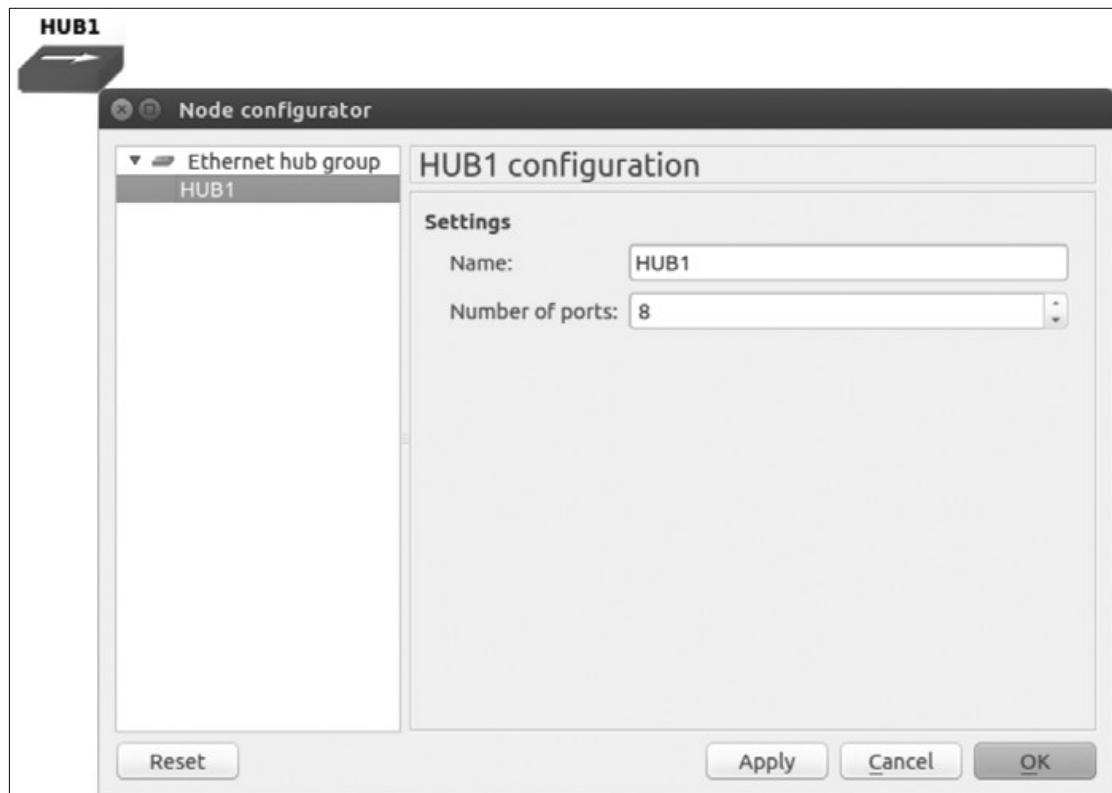


Figure 7-2: Ethernet hub Node configurator

Como regra geral, você deve seguir os switches GNS3 e evitar a inclusão de hubs em seus projetos. Mas se você precisar usar um hub Ethernet, poderá alterar o número de portas Ethernet disponíveis, puxando o configurador do Nó e selecionando seu hub na lista à esquerda. O valor padrão é oito portas, portanto, se você quiser uma quantidade diferente, insira esse número no campo Configurações à direita.

Roteador EtherSwitch

O GNS3 fornece dois tipos de Switch Dynamips, o nó do Switch Ethernet e o roteador EtherSwitch. Eu discuti o nó do Switch Ethernet no capítulo 4, portanto, abordarei apenas o roteador EtherSwitch aqui. Um roteador EtherSwitch não é um dispositivo simulado como um hub Ethernet ou Nó do comutador Ethernet. Em vez disso, é um roteador Dynamips executando o Cisco IOS que foi configurado com um módulo de chave de 16 portas (NM-16ESW). Este é o mesmo módulo de chave que pode ser instalado em um roteador Cisco real e possui os mesmos recursos e limitações (consulte o Apêndice C para obter detalhes). Embora o módulo de chave tenha funcionalidade limitada, é perfeitamente adequado para o CCNA e para muitos estudos do CCNP. Para recursos de Switch mais avançados, você precisa integrar Switches reais em seus projetos GNS3 ou usar Switches Cisco IOU.

Nota

O roteador EtherSwitch exige que você configure um roteador c3745 com um IOS.

Para adicionar portas de switch adicionais ao seu roteador EtherSwitch, clique com o botão direito do mouse no ícone do Switch e selecione Configurar, conforme mostrado na Figura 7-3. O roteador EtherSwitch permite adicionar módulos de chave adicionais. A adição de outro módulo NM-16ESW no slot 2 aumenta o número de portas do Switch para 32.

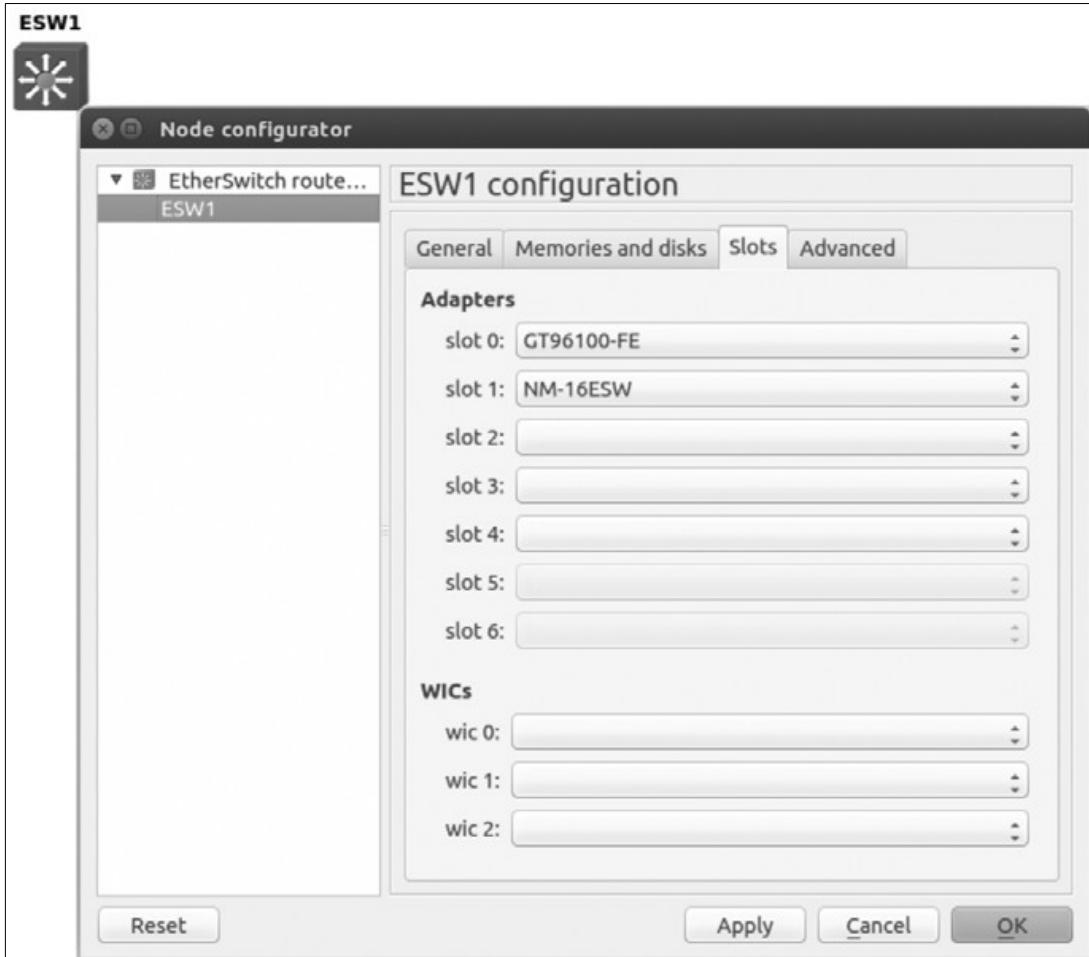


Figure 7-3: EtherSwitch router Node configurator

Frame Relay Switch

O GNS3 fornece um nó de switch Frame Relay simples, capaz de emular o básico de um switch Frame Relay genérico. O bom do nó do switch GNS3 Frame Relay é que ele requer muito pouca configuração. A desvantagem é que às vezes pode ser instável.

Atenção

Apenas o nó do switch Frame Relay GNS3 suporta o tipo de ANSI LMI e Cisco é o tipo de LMI padrão no Cisco IOS. Você deve usar o comando frame-relay lmi-type ansi nas interfaces do roteador. Caso contrário, sua nuvem de quadros não funcionará. Você pode verificar seu tipo de LMI usando o comando show frame-relay lmi (depois de configurar o encapsulamento do Frame Relay).

No Frame Relay, os DLCIs (*data link connection identifiers*) (*identificadores de conexão de link de dados*) são usados para atribuir quadros a um (*permanent virtual circuit*) *círcuito virtual permanente (PVC)* usando conexões de porta serial. Para configurar o DLCI para mapeamentos de porta serial, clique com o botão direito do mouse no ícone do comutador Frame Relay e abra o configurador de Nô. Use os campos Origem e Destino para criar um mapeamento e clique em **Add**. Quando terminar, clique em **Apply** e **OK** para concluir a configuração.

A configuração de exemplo na Figura 7-4 será usada posteriormente para criar uma rede simples do Frame Relay. No painel Mapeamento, à direita, observe que o FR1 está configurado usando duas portas seriais. Cada porta serial é usada para vincular o switch Frame Relay a um roteador no seu projeto GNS3.

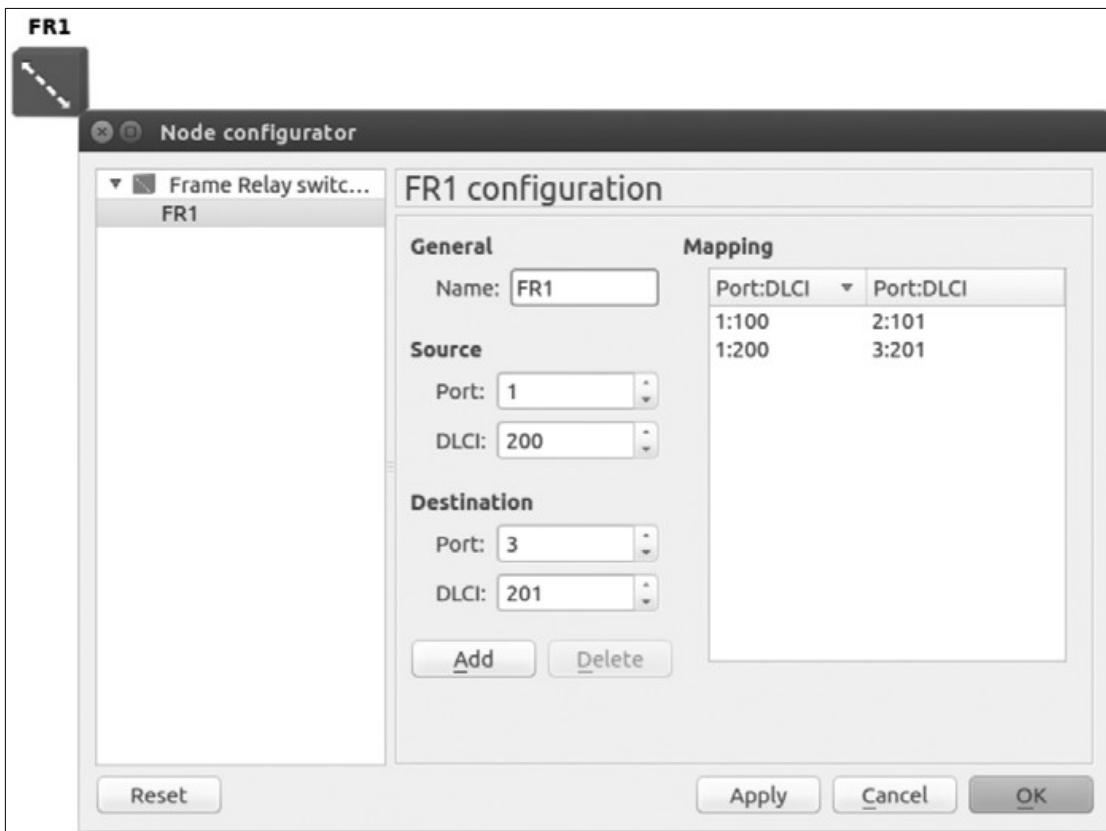


Figure 7-4: Frame Relay switch Node configurator

A porta 1 recebeu dois números DLCI (100 e 200). Cada DLCI na porta 1 é mapeada para um número DLCI em outra porta serial e cada mapeamento forma um PVC de Frame Relay. O mapeamento é lido da esquerda para a direita, portanto, na primeira linha, a porta 1 DLCI 100 é mapeada para a porta 2 DLCI 101 e, na segunda linha, a porta 1 DLCI 200 é mapeada para a porta 3 DLCI 201. Usaremos esses mapeamentos para configurar uma rede simples do Frame Relay.

Simple Frame Relay Hub e Configuração Spoke

Existem várias maneiras de configurar uma rede Frame Relay, e entender o DLCI para mapeamento de porta serial é fundamental para entender e configurar qualquer uma delas. Para entender melhor a relação de mapeamento, vamos configurar uma rede simples usando o DLCI discutido anteriormente para mapeamentos de porta serial. Não vou abordar muita teoria, mas explicarei o suficiente para você começar. Criaremos nossa rede de amostra usando a topologia da Figura 7-5. A rede é dividida em duas sub-redes, 10.10.10.0 e 10.10.10.32, usando a máscara de sub-rede 255.255.255.224.

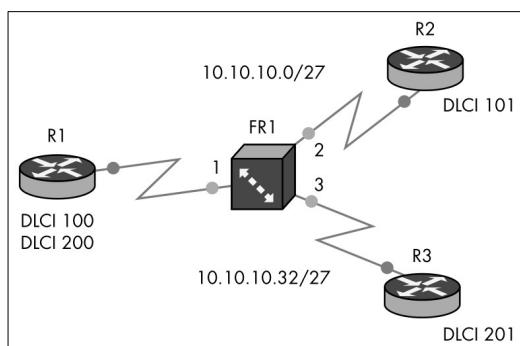


Figure 7-5: Sample hub and spoke Frame Relay network

Essa rede simples é um exemplo de um hub Frame Relay e topologia spoke e deve fornecer uma boa idéia de como os mapeamentos DLCI funcionam em uma rede Frame Relay. O roteador R2 estará na sub-rede 10.10.10.0 e o roteador R3 estará na sub-rede 10.10.10.32. O roteador R1 é o hub em nossa topologia hub e spoke. Ele será conectado às duas sub-redes e encaminhará pacotes entre elas através do switch Frame Relay. Essa configuração permitirá que o roteador R2 faça ping no roteador R3 e vice-versa.

Para criar o projeto, adicione um nó do switch Frame Relay ao seu espaço de trabalho e configure-o da maneira que fizemos na Figura 7-4. Adicione três roteadores e configure cada um deles com uma placa de interface serial, como WIC ou NM-4T. Conecte os roteadores ao switch FR1, como mostrado. Verifique se R1 está conectado à porta 1 no FR1, R2 está conectado à porta 2 e R3 está conectado à porta 3. Após conectar os dispositivos e configurar o mapeamento Port: DLCI no switch FR1, configure o roteador de hub R1, conforme mostrado no código a seguir.

```
R1(config)# interface Serial0/0
① R1(config-if)# encapsulation frame-relay
② R1(config-if)# frame-relay lmi-type ansi
③ R1(config-if)# clock rate 64000
R1(config-if)# no shutdown
R1(config-if)# no ip address
```

Na interface serial, ative o encapsulamento Frame Relay ① e defina o tipo de LMI como ANSI ②. Embora não seja obrigatório para o GNS3, também defini a taxa de clock ③ porque, dependendo do seu IOS, o comando pode ser necessário em um comutador Frame Relay real. Em seguida, configure interfaces ponto-a-ponto e DLCIs.

```
① R1(config-if)# interface Serial0/0.100 point-to-point
② R1(config-subif)# frame-relay interface-dlci 100
③ R1(config-subif)# ip address 10.10.10.1 255.255.255.224
④ R1(config-subif)# interface Serial0/0.200 point-to-point
⑤ R1(config-subif)# frame-relay interface-dlci 200
⑥ R1(config-subif)# ip address 10.10.10.33 255.255.255.224
```

Configurar uma subinterface ponto a ponto ① na interface serial Serial0 / 0.100 usando DLCI 100 ② e atribua à interface um endereço IP da primeira sub-rede ③ (10.10.10.0/27). Conclua a configuração adicionando uma segunda subinterface ponto a ponto ④ da mesma maneira, mas use o DLCI 200 ⑤ e atribua à interface um endereço IP da segunda sub-rede ⑥ (10.10.10.32/27). Neste exemplo, usarei o primeiro endereço válido da sub-rede, que é 10.10.10.33.

Nota

É uma prática recomendada da Cisco usar o número DLCI para o seu número de subinterface. Serial0 / 0.100 é um exemplo de uma subinterface para o DLCI 100.

A lista a seguir contém todos os comandos necessários para configurar o roteador R2.

```
R2(config)# interface Serial0/0
① R2(config-if)# encapsulation frame-relay
② R2(config-if)# frame-relay lmi-type ansi
③ R2(config-if)# clock rate 64000
R2(config-if)# no shutdown
R2(config-if)# no ip address
④ R2(config-if)# interface Serial0/0.101 point-to-point
⑤ R2(config-subif)# frame-relay interface-dlci 101
⑥ R2(config-fr-dlci)# ip address 10.10.10.2 255.255.255.224
R2(config-subif)# exit
⑦ R2(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.1
```

Para configurar o R2, acesse a interface serial e ative o encapsulamento Frame Relay ①, defina o tipo LMI como ANSI ②, defina a taxa de clock ③ e abra a interface. Configure uma subinterface ponto a ponto ④ usando o DLCI 101 ⑤ e atribua à subinterface um endereço IP da primeira sub-rede ⑥ (10.10.10.0 / 27 neste exemplo). Por fim, defina o gateway padrão do roteador usando o endereço IP configurado na interface DLCI 100 do roteador R1 ⑦ (endereço IP 10.10.10.1). Como o R1 é o hub de nossa topologia de hub e Frame Relay, é usado como gateway padrão para nossas duas sub-redes, para que os dados possam ser roteados entre os roteadores R2 e R3. Por fim, adicione uma configuração ao roteador R3 para concluir o projeto.

```

R3(config)# interface Serial0/0
R3(config-if)# encapsulation frame-relay
R3(config-if)# frame-relay lmi-type ansi
R3(config-if)# clock rate 64000
R3(config-if)# no shutdown
R3(config-if)# no ip address
R3(config-if)# interface Serial0/0.201 point-to-point
① R3(config-subif)# frame-relay interface-dlci 201
② R3(config-fr-dlci)# ip address 10.10.10.34 255.255.255.224
R3(config-subif)# exit
③ R3(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.33

```

O roteador R3 é configurado quase da mesma maneira que o R2, mas usa o DLCI 201 ① e um endereço IP ② da segunda sub-rede. Além disso, você precisa definir o gateway padrão usando o endereço IP configurado na interface DLCI 200 do roteador R1 ③ (endereço IP 10.10.10.33).

É isso aí! Todos os três roteadores agora devem poder executar ping um ao outro. Em poucas palavras, cada roteador encapsula quadros de dados e os identifica com um número DLCI do Frame Relay à medida que eles deixam suas interfaces seriais. Quando o switch Frame Relay recebe dados de um roteador, os quadros de dados são encaminhados para outros roteadores através do switch, com base no mapeamento da porta DLCI para serial. Como o R1 é configurado como um hub Frame Relay e conhece as duas sub-redes, ele pode encaminhar dados entre as duas sub-redes usando os dois PVCs. Neste exemplo, um PVC é composto pelo DLCI 100 mapeado para o DLCI 101 e o outro é composto pelo DLCI 200 mapeado para o DLCI 201. Para verificar se o seu circuito Frame Relay está ativo, digite o comando *show frame-relay pvc* em cada um dos seus roteadores.

```
R1# show frame-relay pvc
```

PVC Statistics for interface Serial0/0 (Frame Relay DTE)

	<i>Active</i>	<i>Inactive</i>	<i>Deleted</i>	<i>Static</i>
<i>Local</i>	①2	0	0	0
<i>Switched</i>	0	0	0	0
<i>Unused</i>	0	0	0	0

Se você configurou tudo corretamente, seus PVCs devem ser exibidos em **Active**①.

Criando um comutador de Frame Relay usando o IOS

Por mais útil que seja o nó do comutador Frame Relay, às vezes você pode precisar criar seu próprio comutador Frame Relay usando um roteador IOS. Talvez você queira usar um tipo LMI diferente (como Cisco ou q933a), ou talvez seus estudos exijam conhecer os detalhes de um switch Cisco Frame Relay real. De qualquer forma, um switch IOS é bastante fácil de configurar. A lista a seguir cria um switch IOS Frame Relay usando DLCI mapeamentos idênticos ao nó do switch GNS3 Frame Relay que você configurou anteriormente. Pode parecer intimidador à primeira vista, mas não é; você só precisa entender como os comandos de conexão do Frame Relay são usados para configurar o DLCI para mapeamentos de porta serial.

```

① FRSW(config)# frame-relay switching
FRSW(config)# interface Serial0/0
FRSW(config-if)# description Serial connection to Router R1 (Hub)
FRSW(config-if)# no shutdown
FRSW(config-if)# no ip address
② FRSW(config-if)# encapsulation frame-relay
③ FRSW(config-if)# clock rate 64000
④ FRSW(config-if)# frame-relay lmi-type ansi
⑤ FRSW(config-if)# frame-relay intf-type dce
FRSW(config-if)# interface Serial0/1
FRSW(config-if)# description Serial connection to Router R2 (Spoke)
FRSW(config-if)# no shutdown

```

```

FRSW(config-if)# no ip address
FRSW(config-if)# encapsulation frame-relay
FRSW(config-if)# clock rate 64000
FRSW(config-if)# frame-relay lmi-type ansi
FRSW(config-if)# frame-relay intf-type dce
FRSW(config-if)# interface Serial0/2
FRSW(config-if)# description Serial connection to Router R3 (Spoke)
FRSW(config-if)# no shutdown
FRSW(config-if)# no ip address
FRSW(config-if)# encapsulation frame-relay
FRSW(config-if)# clock rate 64000
FRSW(config-if)# frame-relay lmi-type ansi
FRSW(config-if)# frame-relay intf-type dce
FRSW(config-if)# exit
⑥FRSW(config)# connect PVC1 Serial0/0 100 Serial0/1 101
⑦FRSW(config)# connect PVC2 Serial0/0 200 Serial0/2 201

```

Ao configurar um switch Frame Relay, você deve primeiro ativar o Frame Relay switch com o comando *frame-relay switching* ①. Você também configurará o encapsulamento do Frame Relay em cada interface serial com o comando *encapsulation frame-relay* ②. Em seguida, use o comando *clock rate* ③ para configurar o clock, escolha um tipo de LMI com *frame-relay lmi-type* ④ e defina o tipo de interface para o DCE usando o comando *frame-relay intf-type dce* ⑤. Após exibir as interfaces, você estará pronto para definir seus PVCs.

Nota

Em algumas versões do IOS, o comando clock rate pode precisar ser inserido como clockrate

O DLCI para mapeamento de porta está configurado usando os comandos *connect connection-name interface dlci interface dlci*. Os dois últimos comandos nesta configuração definem um mapeamento de conexão entre dois PVCs do Frame Relay. O comando *connect PVC1 Serial0/0 100 Serial0/1 101* ⑥ define um PVC entre os roteadores R1 e R2 e é usado para criar nossa primeira sub-rede. A interface de origem é Serial0/0 e o DLCI de origem é 100. O PVC é concluído usando a interface Serial0/1 e o DLCI 101 configurado no roteador R2. O comando *connect PVC2 Serial0/0 200 Serial0/2 201* ⑦ usa a mesma sintaxe para criar um segundo PVC entre os roteadores R1 e R3 (usado para a segunda sub-rede). Isso é tudo o que há para criar seu próprio switch Frame Relay. Ao configurar um switch Frame Relay com o Cisco IOS, o tipo LMI pode ser definido como cisco, ansi ou q933a, mas você deve ser consistente em todos os roteadores que participam da rede Frame Relay.

ATM Switch

O GNS3 fornece uma maneira fácil de configurar um *switch de modo de transferência assíncrona (Asynchronous Transfer Mode-ATM)*. O ATM é semelhante ao Frame Relay, pois é um protocolo de camada 2 que mapeia portas físicas para circuitos lógicos. Para configurar um VPI/VCI para mapeamento de porta, clique com o botão direito do mouse no ícone switch ATM e selecione **Configure**, como mostra a Figura 7-6. Aqui, configurei um circuito virtual simples usando duas portas no nó do switch ATM1.

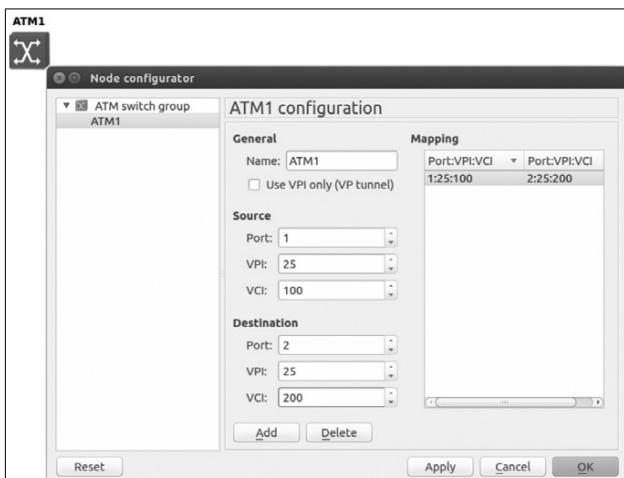


Figure 7-6: Node configurator

Use os campos **Source** e **Destination** para criar seu mapeamento de portas e clique em **Add**. Quando terminar o mapeamento de portas, clique em **Apply** e em **OK** para concluir a configuração. Agora vamos ver um exemplo rápido de criação de um simples conexão WAN ponto a ponto usando um switch ATM. Comece criando a topologia mostrada na Figura 7-7.

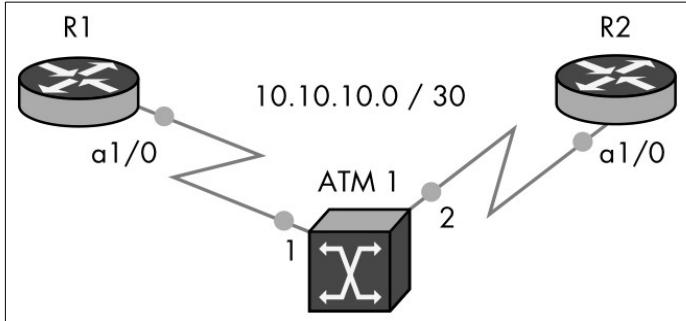


Figure 7-7: Sample ATM network

Adicione um switch ATM ao seu espaço de trabalho e configure-o usando as informações da Figura 7-6. Em seguida, adicione dois roteadores e crie um link entre cada roteador e o switch. Você precisa usar os *roteadores da série 7200*, cada um configurado com um *adaptador de porta ATM* (PA-A1) no slot 1. Crie um link de *a1/0* em cada roteador para o switch ATM, como mostra a Figura 7-7, e depois digite os seguintes comandos para configurar o ATM no roteador R1.

```
R1(config)# interface ATM1/0
R1(config)# no shutdown
R1(config)# interface ATM1/0.100 point-to-point
R1(config-subif)# ip address 10.10.10.1 255.255.255.252
R1(config-subif)# pvc 25/100
R1(config-if-atm-vc)# protocol ip 10.10.10.2 broadcast
R1(config-if-atm-vc)# encapsulation aal5snap
```

Em seguida, aplique uma configuração semelhante ao roteador R2.

```
R2(config)# interface ATM1/0
R2(config)# no shutdown
R2(config)# interface ATM1/0.200 point-to-point
R2(config-subif)# ip address 10.10.10.2 255.255.255.252
R2(config-subif)# pvc 25/200
R2(config-if-atm-vc)# protocol ip 10.10.10.1 broadcast
R2(config-if-atm-vc)# encapsulation aal5snap
```

Para verificar se o seu circuito ATM está ativo, digite o comando *show atm pvc*.

```
R1# show atm pvc
```

Se o status do PVC exibir UP, agora os dois roteadores devem poder executar ping um ao outro.

Cloud Nodes

O nó da nuvem é um nó de dispositivo altamente configurável que não simula uma peça de hardware específica. Em vez disso, fornece uma ampla variedade de opções de conexão de entrada/saída de rede (*Network Input/Output NIO*) que permitem que dispositivos virtuais GNS3 se comuniquem com outros programas ou hardware real, como o adaptador Ethernet do seu PC.

Você se conecta a um Cloud Node criando um link padrão de um dispositivo GNS3 (como um roteador) para a Cloud. Feito isso, todos os dados que saem de uma interface virtual passam pela conexão NIO do nó Cloud para um destino fora do GNS3, como um adaptador Ethernet físico. Lembre-se de que as limitações de taxa de transferência apresentadas no GNS3 também se aplicam à interface virtual conectada ao modo Cloud, o que significa que essas limitações afetarão seu desempenho geral. Para configurar uma conexão NIO (mostrada na Figura 7-8), clique com o botão direito do mouse no Ícone de Cloud e selecione **Configure**.

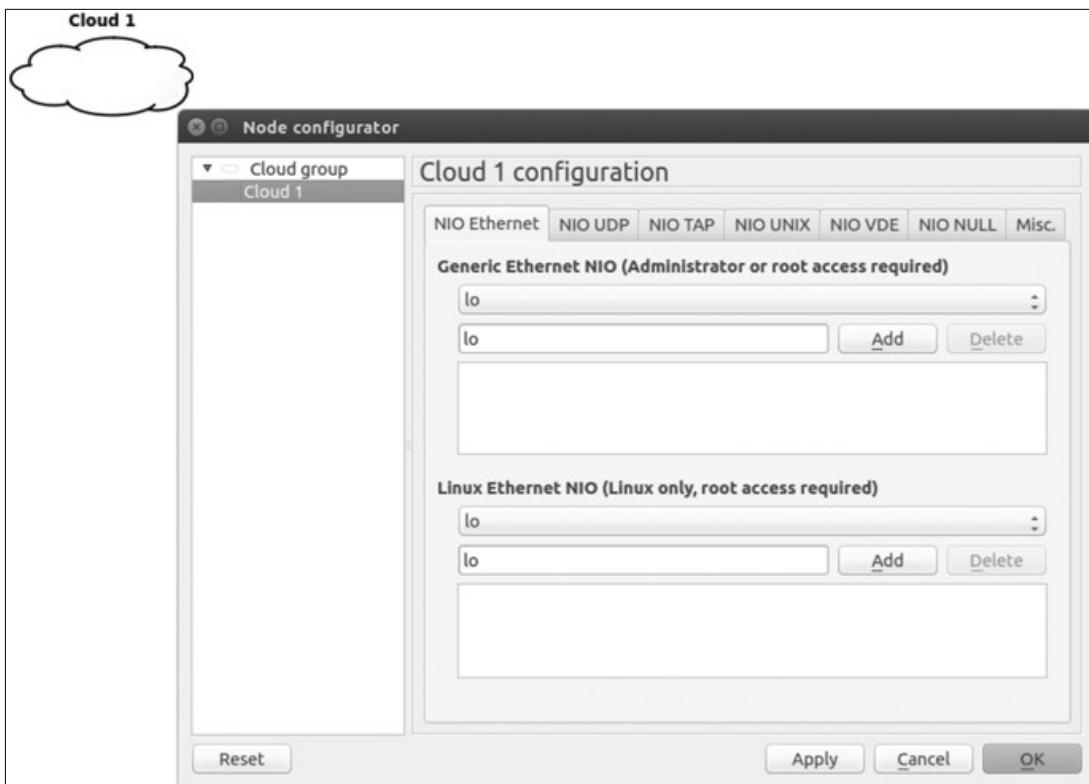


Figure 7-8: Cloud Node configurator

O configurador node fornece seis opções de conexão:

NIO Ethernet Cria uma conexão com um ou mais interfaces físicas ou lógicas no seu PC. A configuração da NIO Ethernet permite configurar uma NIO genérica e uma NIO somente para Linux.

NIO UDP Cria um soquete UDP para formar um link entre GNS3 e outros programas.

NIO TAP Cria uma conexão com uma interface TAP virtual. As interfaces TAP são frequentemente conectadas às interfaces físicas no seu PC.

NIO TAP Cria uma conexão com uma interface TAP virtual. As interfaces TAP são frequentemente uma bridged para interfaces físicas no seu PC.

NIO UNIX Cria uma conexão de soquete UNIX entre GNS3 e alguma outra aplicação.

NIO VDE Cria um link entre o GNS3 e um dispositivo Ethernet distribuído virtual(*Virtual Distributed Ethernet*).

NIO NULL Cria um link entre o GNS3 e um dispositivo NULL para formar um link fictício.

Misc. Permite renomear um Cloud Node.

Para configurar uma conexão, selecione o tipo de conexão NIO, escolha as opções desejadas e selecione **Add**. Você pode configurar mais de uma conexão por nó da nuvem, permitindo vincular vários dispositivos GNS3, assim como você pode usar várias interfaces em um switch ou roteador GNS3. Nos sistemas Linux, convém usar uma conexão NIO genérica, que pode funcionar de maneira mais confiável que uma NIO específica do Linux. Um motivo é que o NIO específico do Linux pode remover as tags de VLAN recebidas. Se você está tendo dificuldades com uma conexão no Linux, tente as duas para ver qual funciona melhor.

Conectar dispositivos GNS3 ao hardware físico

A capacidade de conectar projetos ao hardware físico é o que transforma o GNS3 de um diamante bruto para a Grande Estrela da África. Usando o Cloud Node, você pode estabelecer links de tronco com switches Cisco ativos e até acessar a Internet a partir de seus dispositivos GNS3. Isso oferece ao GNS3 possibilidades de rede quase ilimitadas.

Conectar o GNS3 a dispositivos reais é mais fácil em alguns sistemas do que em outros, mas deve funcionar em todos os principais sistemas operacionais.

Permissões Dynamips

Antes de conectar dispositivos GNS3 a um adaptador Ethernet físico, pode ser necessário fazer algumas alterações no seu PC. Se o seu Cloud Node estiver configurado usando a NIO Ethernet em um sistema Windows, execute o GNS3 usando privilégios de administrador clicando com o botão direito do mouse no ícone GNS3 e selecionando Executar como Administrador. Para tornar essa opção permanente, clique com o botão direito do mouse no ícone GNS3 e escolha Propriedades. Selecione a guia Compatibilidade e marque a opção Executar este programa como administrador. Em sistemas baseados em Unix, você precisa elevar as permissões do Dynamips antes de usar as conexões NIO Ethernet ou NIO TAP. Se você pular esta etapa, precisará executar o GNS3 usando a conta root. Caso contrário, as conexões NIO falharão e o GNS3 exibirá uma mensagem de erro na janela do console do GNS3. Para definir as permissões corretas do Dynamips no OS X, use os seguintes comandos:

```
$ sudo chown root /Applications/GNS3.app/Contents/Resources/dynamips*
$ sudo chmod 4755 /Applications/GNS3.app/Contents/Resources/dynamips*
```

Definir permissões na maioria das distribuições Linux funciona da mesma maneira; substitua o caminho do arquivo pelo local correto para o seu arquivo dynamips, conforme mostrado no código a seguir. Se você estiver executando um sistema Linux baseado no Debian como o Ubuntu, use o comando setcap porque é mais seguro.

```
$ sudo apt-get install libcap2
$ sudo setcap cap_net_raw,cap_net_admin+eip /usr/local/bin/dynamips*
```

Após alterar as permissões do Dynamips, você pode executar o GNS3 como um usuário regular, mas o Dynamips será tratado como se estivesse sendo executado pela conta root.

Preparando seu PC para uma Bridge

Alguns sistemas operacionais não permitem que o GNS3 se comunique diretamente com o hardware Ethernet do seu PC, e os adaptadores Wi-Fi geralmente também não funcionam. Antes de usar o GNS3 com um adaptador Ethernet nesses sistemas, pode ser necessário instalar um software adicional para fazê-lo funcionar. Uma solução comum é instalar um driver de interface virtual e usar uma Bridge para associá-lo ao adaptador Ethernet físico do seu PC. O GNS3 passa os dados da rede para a interface virtual, que os entrega à interface Ethernet física via ponte. Em sistemas baseados em Unix, as interfaces virtuais geralmente são fornecidas usando drivers TUN/TAP. No Windows, você usará um adaptador de loopback conectado ao seu adaptador Ethernet físico. Mesmo que o hardware Ethernet do seu PC funcione diretamente com o GNS3, os métodos a seguir são maneiras recomendadas e previsíveis de conectar o GNS3 ao mundo externo.

Usando um adaptador de loopback no Windows

No Windows, um driver de adaptador de loopback fornece uma interface de rede virtual que pode ser conectada a um adaptador Ethernet físico no seu PC. Para adicionar um adaptador de loopback ao Windows, vá ao **Control Panel** ▶ **Device Manager**. Clique com o botão direito do mouse no nome do computador na lista e selecione **Add legacy hardware**. Clique em **Next**, selecione **Install the hardware that I manually select from a list (Advanced)** e clique em **Next** novamente. Escolha **Network Adapters** na lista e clique em **Next**. No assistente Adicionar Hardware, mostrado na Figura 7-9, selecione **Microsoft** em Fabricante e role para baixo e selecione o Adaptador de Rede chamado **Microsoft Loopback Adapter**. Clique em **Next** e em **Finish** para concluir a instalação. Você deve reiniciar o Windows após instalar o Microsoft Loopback Adapter. O adaptador de loopback da Microsoft também pode ser instalado executando o comando `loopback-manager.cmd` do diretório de instalação do GNS3. Para criar uma ponte entre o adaptador de loopback e o adaptador Ethernet, vá para o Painel de controle ▶ Centro de rede e compartilhamento e escolha Alterar configurações do adaptador. Selecione os dois adaptadores e clique com o botão direito do mouse para exibir o menu mostrado na Figura 7-10. Selecione Conexões de ponte para criar a interface de ponte entre os dois adaptadores. Quando terminar, reinicie o Windows para permitir que as alterações entrem em vigor.

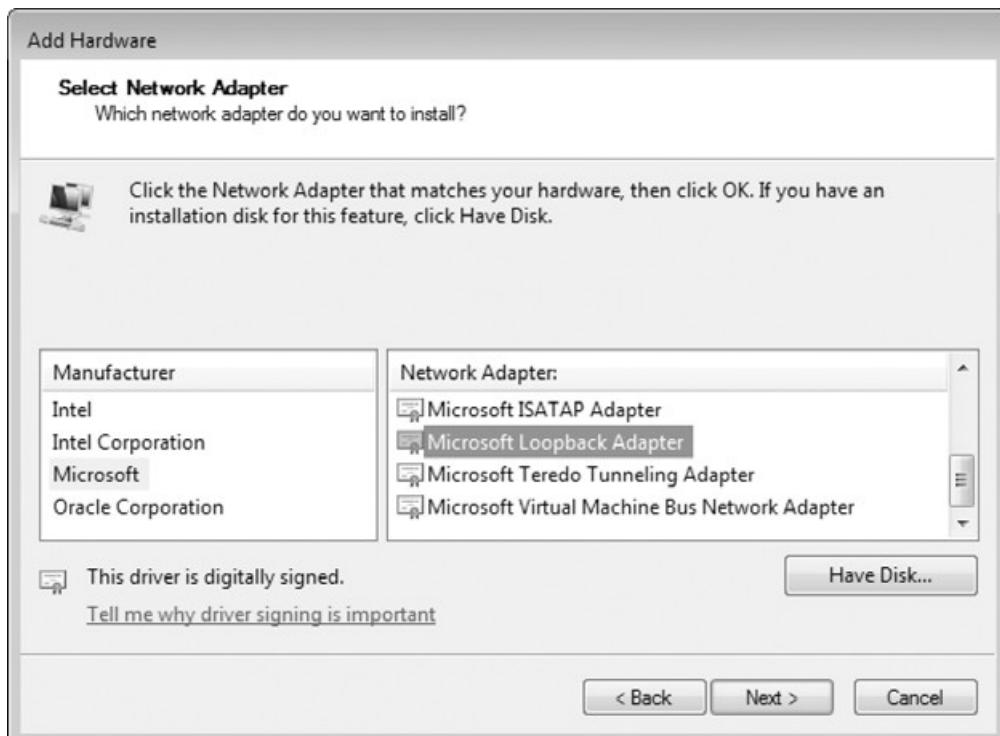


Figure 7-9: Selecting the Microsoft Loopback Adapter

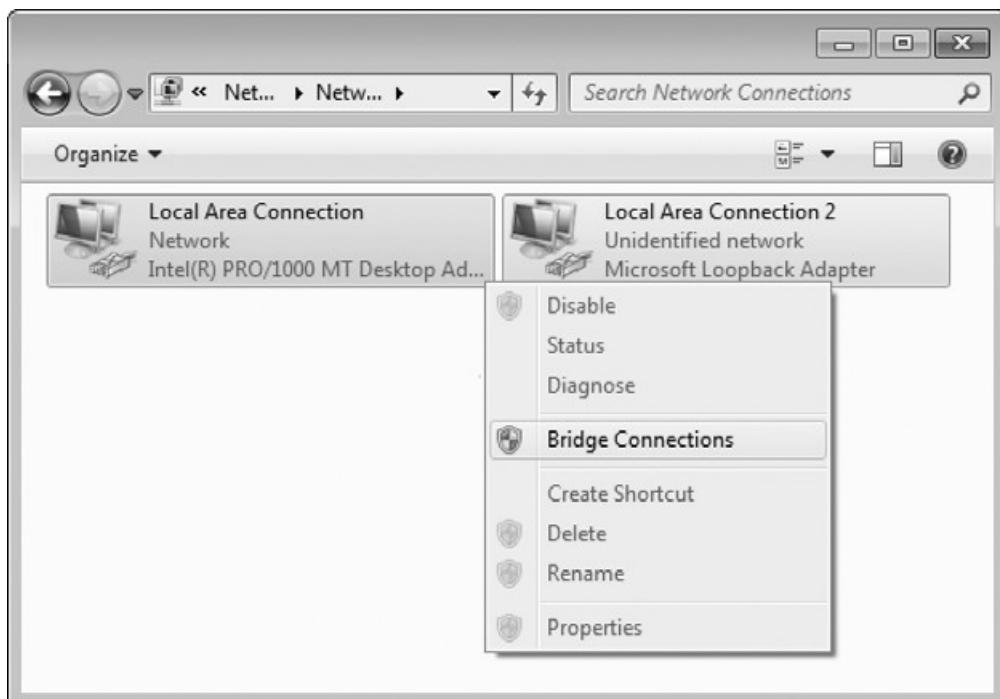


Figure 7-10: Creating a bridge using a Microsoft Loopback Adapter and an Ethernet adapter

Para permitir que o GNS3 use seu adaptador Ethernet físico em um sistema Windows, você precisará configurar um nó Cloud com o adaptador de loopback (consulte “Conectando dispositivos GNS3 ao hardware físico” na página 105). É uma boa ideia renomear seu adaptador de loopback, para que ele possa ser claramente identificado no GNS3. Neste exemplo, eu recomendo alterar a *Local Area Connection 2* para *Loopback*.

Drivers TUN / TAP no OS X

Se você estiver usando o OS X, você precisa instalar um driver de interface virtual antes que o GNS3 possa acessar uma interface Ethernet física. Para instalar drivers TUN/TAP no OS X, faça o download do software de driver da sua versão do OS X no SourceForge (<http://tuntaposx.sourceforge.net/>), execute o instalador e siga as instruções. Os

drivers devem ser instalados em */Library/Extensions* e devem carregar automaticamente quando você reiniciar o sistema. Para carregar o driver manualmente, vá para o diretório */Library/Extensions* e digite o seguinte:

```
$ sudo kextload tap.kext
```

Antes de lançar o GNS3, digite o seguinte comando para definir permissões em suas interfaces TAP. Você precisará digitar o comando sempre que reiniciar o Mac.

```
$ sudo chown $(id -un):$(id -gn) /dev/tap*
```

Para ativar uma interface TAP e realizar uma bridge com a porta Ethernet física no seu PC, você deve inserir os seguintes comandos após adicionar uma Cloud e conectar um roteador à interface *nio_tap*, configurada usando */dev/tap0*. Se você digitar os comandos com antecedência, eles falharão e sua ponte não funcionará. Você precisará inserir esses comandos toda vez que carregar um projeto que inclua uma cloud node.

```
$ sudo ifconfig bridge0 create  
$ sudo ifconfig bridge0 addm en0  
$ sudo ifconfig bridge0 addm tap0 up
```

Depois de inserir os comandos de um terminal, O OS X deve criar uma bridge da interface *tap0* à interface Ethernet física no seu Mac, que é *en0* neste exemplo. Você deve usar o comando *ifconfig* para verificar o nome da interface Ethernet do seu Mac e substituir *en0* por esse nome.

Nota

Se você alterar o maximum transmission unit (MTU) de uma interface, poderá ver o erro "ifconfig:BRDGADD tap0: Invalid argument" ao criar a bridge. Nesse caso, você precisa garantir que o tamanho da MTU da sua interface física corresponda ao tamanho da MTU da interface TAP.

Eu recomendo adicionar uma anotação ao seu projeto que inclua esses comandos como um lembrete para criar a ponte quando você abrir um projeto. Depois de abrir o projeto, você pode copiar a anotação e colá-la em uma janela do terminal para economizar tempo. Não se esqueça de inserir esses comandos toda vez que você abrir um projeto que conecte a Ethernet a uma interface TAP, ou não funcionará.

Drivers TUN/TAP no Ubuntu Linux

No Linux, você deve poder conectar um Cloud Node diretamente à sua interface Ethernet usando a guia NIO Ethernet no configurador Cloud, mas se achar que precisa de drivers TUN/TAP para Ubuntu, atualize seu gerenciador de pacotes e digite o seguinte comando para instalar o pacote.

```
$ sudo apt-get install uml-utilities
```

Se você estiver executando outra versão do Linux, poderá ser necessário instalar um pacote diferente, mas esse pacote deve funcionar na maioria das distribuições baseadas no Debian.

Conectando a Switches ativos

O GNS3 é um ótimo software, mas tem algumas limitações. Por exemplo, o módulo de Switches NM-16ESW não inclui todos os recursos avançados de um Switches de camada 2 ou 3 real. Se você deseja trabalhar com Switches avançados, é necessário usar software adicional como Cisco IOU ou usar Switches Cisco físicos. Se você estiver criando laboratórios CCNA, um switch Cisco ativo poderá ser suficiente, mas se estiver criando laboratórios CCNP ou CCIE, provavelmente usará vários Switches ativos. Frequentemente, o objetivo é ter um roteador GNS3 conectado a cada switch externo. Isso é complicado porque a maioria dos PCs possui apenas um adaptador de rede Ethernet. Felizmente, o GNS3 e o IOS resolvem isso. Suas opções são encaminhar VLANs para o switch em um único adaptador Ethernet no seu PC ou instalar vários adaptadores Ethernet no seu PC. Nesta seção, abordarei duas maneiras de conectar dispositivos GNS3 a switches Cisco ativos.

Standard 802.1Q Trunk

Esse método usa um tronco 802.1Q padrão para permitir que os dispositivos GNS3 se comuniquem com um switch Cisco ativo por meio do adaptador Ethernet do seu PC.

Switch Breakout Este método usa um Switch Ethernet especialmente configurado chamado breakout switch para permitir que os dispositivos GNS3 se conectem a vários comutadores ativos usando apenas um único adaptador Ethernet no seu PC. Para criar um breakout switch, você deve ter um segundo switch Ethernet físico disponível para usá-lo como o breakout switch.

A opção que você escolhe depende de quantos switches você possui, sistema operacional do seu PC e quais adaptadores Ethernet já estão instalados no seu PC. Vamos começar analisando como um tronco 802.1Q funciona para alcançar um switch Cisco.

Configurando um 802.1Q Trunk padrão

Na minha opinião, um 802.1Q Trunk é a melhor maneira de conectar switches reais aos seus projetos GNS3. As vantagens de um 802.1Q Trunk padrão são que é fácil de configurar e funciona da mesma maneira que conectar um switch a uma rede física. A desvantagem é que o sistema operacional do seu PC ou os drivers Ethernet do seu PC podem não ser compatíveis. Frequentemente, eles removem as tags 802.1Q dos pacotes provenientes do switch para o seu PC. Sem as tags adequadas, o GNS3 não tem como saber a quais VLANs seus pacotes pertencem e, por sua vez, não sabe para onde encaminhar os pacotes, o que interrompe sua rede. Se você vasculhar a Internet, encontrará todos os tipos de soluções criativas criadas pelas pessoas para contornar esse problema, mas elas geralmente são específicas da plataforma e variam de máquina para máquina.

Nota

Uma maneira de impedir a remoção de tags no OS X e Linux é usar um adaptador Ethernet USB que suporte tags 802.1Q e jumbo frames. Um desses adaptadores que funciona bem é o adaptador StartTech USB31000SW, mas qualquer adaptador que use o chipset ASIX AX88772A deve funcionar.

Neste exemplo, você colocará um roteador EtherSwitch ou Ethernet switch node no seu espaço de trabalho e configurará com o protocolo de 802.1Q Trunk. Em seguida, você adiciona um Cloud Node ao seu espaço de trabalho e o configura usando uma interface NIO e vincula-o ao comutador GNS3. O nó da nuvem pode ser conectado diretamente, ou em bridged, ao adaptador Ethernet do seu PC (dependendo do seu sistema operacional). Em seguida, você conecta um cabo Ethernet do adaptador Ethernet do seu PC a uma porta no switch Cisco ativo. A porta do switch que você escolher também precisa ser configurada com o entroncamento 802.1Q. Após a configuração do switch GNS3 e do switch físico, você poderá rotear pacotes de VLAN gerados pelo GNS3 através do tronco para o switch ativo. Nesta seção, criaremos um projeto simples que conecta nossa rede GNS3 a um switch c3550 ativo usando duas VLANs (10 e 20). Comece criando a topologia mostrada na Figura 7-11. Ao configurar o Cloud Node, escolha o nome do adaptador Ethernet do seu PC, encontrado na guia NIO Ethernet.

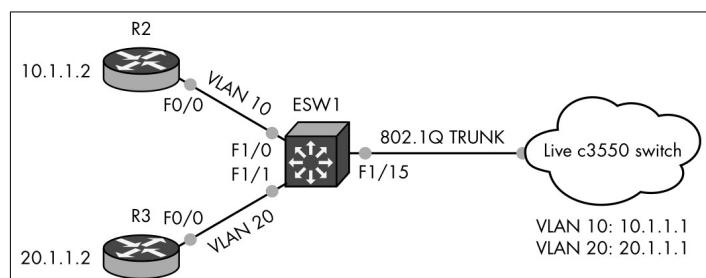


Figure 7-11: Sample topology using a standard dot1q trunk to live switch

Para configurar VLANs e um 802.1Q trunk usando o roteador EtherSwitch, abra um console no ESW1 e digite os seguintes comandos:

```
ESW1# vlan database
① ESW1(vlan)# vlan 10
② ESW1(vlan)# vlan 20
ESW1(vlan)# apply
ESW1(vlan)# exit
ESW1# configure terminal
ESW1(config)# int f1/15
③ ESW1(config-if)# switchport mode trunk
④ ESW1(config-if)# switchport trunk encapsulation dot1q
ESW1(config-if)# int f1/0
ESW1(config-if)# switchport mode access
```

```

⑤ ESW1(config-if)# switchport access vlan 10
ESW1(config-if)# int f1/1
ESW1(config-if)# switchport mode access
⑥ ESW1(config-if)# switchport access vlan 20

```

Os comandos anteriores criam VLAN 10 ① e 20 ② no comutador, configure uma porta trunk ③ usando o protocolo dot1q ④ e atribua portas de acesso à VLAN 10 ⑤ (para o roteador R2) e VLAN 20 ⑥ (para o roteador R3). Se você optar por usar um Ethernet switch node, configure uma porta como um tronco 802.1Q e as outras como portas de acesso à VLAN, conforme mostrado na Figura 7-12.

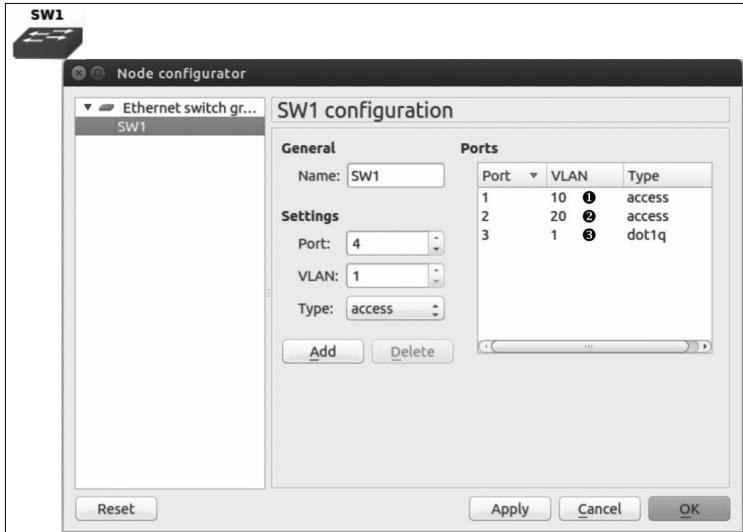


Figure 7-12: Ethernet switch node configured with a dot1q trunk port

As portas 1 e 2 são configuradas como portas de acesso usando VLAN 10 ① e 20 ②, e a porta 3 é a porta trunk dot1q ③ conectada ao Cloud Node. Em seguida, faça logon no seu switch Cisco ativo e crie as mesmas VLANs. Em seguida, configure a porta trunk 802.1Q e conecte-a ao adaptador Ethernet do seu PC. A lista a seguir é um exemplo de como configurar um switch c3550, usando comandos que você viu ao longo do capítulo.

```

c3550# configure-terminal
c3550(config)# ip routing
c3550(config)# interface vlan 10
c3550(config-vlan)# ip address 10.1.1.1
c3550(config-vlan)# interface vlan 20
c3550(config-vlan)# ip address 20.1.1.1
c3550(config-vlan)# exit
c3550(config)# Interface f0/1
c3550(config-if)# switchport trunk encapsulation dot1q
c3550(config-if)# switch port mode trunk
c3550(config-if)# switchport trunk allowed vlan all
c3550(config-if)# speed 100
c3550(config-if)# duplex full

```

Para concluir o projeto, configure os roteadores R2 e R3. Faça logon no roteador R2 e configure um endereço IP e um gateway padrão para a VLAN 10.

```

R2(config)# interface f0/0
R2(config-if)# description Using VLAN 10
R2(config-if)# ip address 10.1.1.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.1

```

Agora, faça logon no roteador R3 e configure um endereço IP e um gateway padrão para a VLAN 20.

```
R3(config)# interface f0/0
R3(config-if)# description Using VLAN 20
R3(config-if)# ip address 20.1.1.2 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)# ip route 0.0.0.0 0.0.0.0 20.1.1.1
```

Teste o roteamento de VLAN através do switch digitando um comando ping de uma VLAN para outra.

```
R3# ping 10.1.1.2
!!!!
```

Quando você terminar o projeto, poderá verificar ainda mais a configuração usando ferramentas como CDP ou Wireshark.

Criando a opção Elusive Breakout Switch

Um Breakout Switch é outra maneira de conectar switches reais a projetos GNS3, e é comum configurar um usando o Ubuntu Linux. Embora um Breakout Switch funcione em outros sistemas, é mais fácil configurar no Linux. Como mencionado anteriormente, outros sistemas operacionais como Windows e OS X podem remover informações de VLAN dos pacotes. Por esse motivo, é melhor instalar o Ubuntu em hardware real se você planeja criar um breakout switch.

Se você usa uma máquina virtual, o sistema operacional host subjacente pode remover as tags VLAN e o breakout switch não funcionará. Às vezes, você pode contornar isso usando um adaptador Ethernet USB, como o StartTech USB31000SW mencionado em “Configurando um trunk 802.1Q padrão” na página 109.

Esse método de comutação requer no mínimo dois switches Cisco reais; um é o switch breakout e o outro é um ou mais switches Cisco ativos que são usados no seu projeto GNS3. O switch breakout é usado para enganar os switches Cisco ativos, pensando que cada um dos seus roteadores GNS3 está diretamente conectado a um switch ativo com um cabo Ethernet. Na realidade, apenas um adaptador Ethernet é usado no seu PC para conectar todos os seus roteadores GNS3 aos switches ativos, e esse adaptador está conectado ao switch breakout. O switch breakout é então configurado para dividir todas as VLANs em interfaces individuais que você conecta a outros switches Cisco ativos usando cabos Ethernet (um por VLAN). Eu chamo esses cabos de *breakout cables*. A Figura 7-13 mostra o layout físico do seu PC e switches.

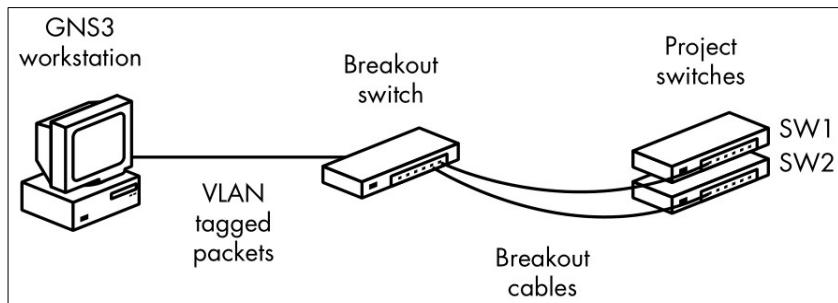


Figure 7-13: Physical layout using a breakout switch and live Cisco switches

Aqui está a visão rápida de como funciona. VLANs breakout estão configuradas no seu adaptador Ethernet Linux usando o pacote vlan e um 802.1Q trunk está configurado no breakout switch. No GNS3, você adiciona um ou mais Cloud Nodes configurados com as Linux breakout VLANs usando as interfaces Ethernet NIO. No seu projeto GNS3, um roteador é conectado a cada uma das interfaces de VLAN do Cloud Node (um roteador por interface). Os pacotes que saem dos roteadores vão para o Cloud Node, onde o Linux os identifica com um ID de VLAN e os passa para o switch breakout usando o adaptador Ethernet do seu PC. O switch breakout recebe os pacotes em uma porta de trunk 802.1Q padrão. A partir daí, o switch breakout usa os IDs de VLAN para identificar e passar os pacotes de forma transparente para um (ou mais) switches Cisco ativos. O que torna isso tão engenhoso é que cada roteador GNS3 possui um cabo Ethernet separado, conectado a uma porta no switch Cisco ativo, mesmo que o seu PC possua apenas um único adaptador Ethernet. Os switches breakout são bastante simples de configurar no Linux. Comece atualizando o gerenciador de pacotes e instalando o suporte à VLAN no sistema Ubuntu.

```
$ sudo apt-get install vlan
```

Agora, ative o módulo **8021q** Linux usando o comando **modprobe**.

```
$ sudo modprobe 8021q
```

Em seguida, aumente o tamanho do quadro MTU na interface Ethernet e crie suas breakout VLANs usando o comando **vconfig**. Certifique-se de substituir eth0 pelo nome da sua interface.

-
- ① \$ sudo ifconfig eth0 mtu 1546
 - ② \$ sudo vconfig add eth0 10
 - ③ \$ sudo vconfig add eth0 20
-

Nota

Seu adaptador Ethernet deve suportar tamanhos de quadro acima do padrão máximo de 1500 bytes.

O tamanho do quadro aumentado ① abre espaço para as tags VLAN adicionais. Crie uma breakout VLAN para cada roteador no seu projeto. Na listagem anterior, criei duas breakout VLAN (10 ② e 20 ③) na interface eth0 do meu PC Linux.

Nota

Não confunda breakout VLANs com VLANs criadas em seus projetos GNS3. É importante entender que as breakout VLANs devem ser usadas apenas pelo Linux e pelo switch breakout - elas não devem ser usadas no seu projeto GNS3 ou nos switches Cisco ativos.

Comece a configurar o breakout switch aumentando o tamanho da MTU em todo o sistema. Depois que o comando é inserido, você deve recarregar o switch para que a alteração entre em vigor.

```
Breakout(config)# system mtu 1546
```

Após a reinicialização do switch, faça logon e configure um link de trunk 802.1Q do seguinte modo:

```
Breakout# configure terminal
Breakout(config)# interface FastEthernet 0/1
① Breakout(config-if)# switchport trunk encapsulation dot1q
② Breakout(config-if)# switchport mode trunk
③ Breakout(config-if)# switchport trunk allowed vlan all
```

A interface que você configura como trunk é então conectada ao adaptador Ethernet físico do seu PC usando um cabo Ethernet. Como mostrado aqui, o encapsulamento dot1q ① é configurado na porta de tronco ②, e todas as VLANs ③ são permitidas através do trunk. Em seguida, vá em cada interface que você planeja conectar a um switch ativo e configure uma breakout VLAN e um túnel dot1q para cada VLAN, conforme mostrado na lista a seguir:

```
Breakout(config)# vlan 10
Breakout(config-vlan)# vlan 20
Breakout(config-vlan)# exit
Breakout(config)# interface FastEthernet 0/2
Breakout(config-if)# description GNS3 R1 Physical Uplink to Live Switch SW1
① Breakout(config-if)# switchport access vlan 10
② Breakout(config-if)# switchport mode dot1q-tunnel
③ Breakout(config-if)# l2protocol-tunnel cdp
Breakout(config-if)# interface FastEthernet 0/3
Breakout(config-if)# description GNS3 R2 Physical Uplink to Live Switch SW2
④ Breakout(config-if)# switchport access vlan 20
Breakout(config-if)# switchport mode dot1q-tunnel
```

```
Breakout(config-if)# l2protocol-tunnel cdp
```

Aqui, a interface FastEthernet0/2 do nosso breakout switch está configurada para VLAN 10 ①, dot1q tunneling ② e túnel de protocolo de descoberta Cisco ③. O FastEthernet0/3 está configurado da mesma maneira, mas para a VLAN 20 ④. Essas são as interfaces usadas para conectar os roteadores GNS3 aos seus switches Cisco ativos. Já sabemos que o Cisco Discovery Protocol (CDP) é usado para compartilhar e reunir informações com equipamentos Cisco conectados diretamente, geralmente chamados *neighbors*. No entanto, nosso switch Cisco real não está diretamente conectado ao GNS3; em vez disso, está conectado ao breakout switch. Nesse caso, a única maneira de usar o CDP é encapsulando o protocolo através do switch breakout para um switch Cisco ativo com o comando *l2protocol-tunnel cdp*. (Vocês também pode encapsular o STP e o VTP.) É aqui que as coisas ficam complicadas porque o encapsulamento do CDP não funciona em todos os comutadores. Se você precisar usar o CDP, escolha uma opção de breakout switch que suporte totalmente o encapsulamento do CDP. A Tabela 7-1 lista alguns comutadores Cisco comuns e seus recursos de encapsulamento CDP.

Table 7-1: Common Cisco Switches and Their CDP Tunneling Compatibility

Switch	CDP tunneling compatibility
Cisco 2950	CDP não funcionará em nenhuma direção. O encapsulamento da camada 2 não é suportado neste switch.
Cisco 3550	CDP funciona apenas em uma direção. Os vizinhos não podem ser vistos nos switches, independentemente da versão do IOS.
Cisco 3560	CDP funciona apenas em uma direção. Os vizinhos não podem ser vistos nos switches, independentemente da versão do IOS.
Cisco 3750	CDP bidirecional e totalmente funcional (camada 2 e camada 3) usando a imagem de serviços IP. A imagem IP Base não suporta encapsulamento.
Cisco 4948	CDP bidirecional e totalmente funcional (camada 2 e camada 3) usando uma imagem mínima de serviços IP.

O switch Cisco 3750 funciona bem, tanto como switch breakout quanto para tunelamento CDP, mas não é o switch mais barato disponível. Se você não tiver dinheiro para este modelo, poderá escolher um modelo mais barato que funcione como uma opção de switch breakout, mas não terá total transparência no seu projeto GNS3. Antes de continuar, verifique se Fa0/1 no switch breakout está conectado à porta Ethernet do seu PC e que Fa0/2 e Fa0/3 estejam conectados às portas Ethernet nos seus switches de projeto ao reais. Após verificar essas conexões, inicie o GNS3 e configure um Cloud Node usando as VLANs do Linux que você criou anteriormente, como mostra a Figura 7-14.

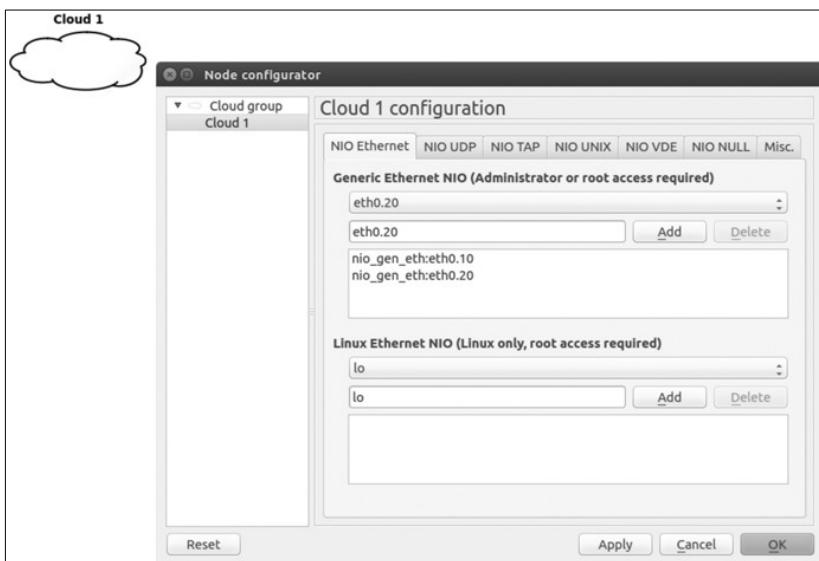


Figure 7-14: Configuring a Cloud node using Linux VLANs

Nota

Embora você esteja usando o Linux, é importante usar o Generic Ethernet NIO e não o Linux Ethernet NIO. Caso contrário, a marcação de VLAN pode não funcionar.

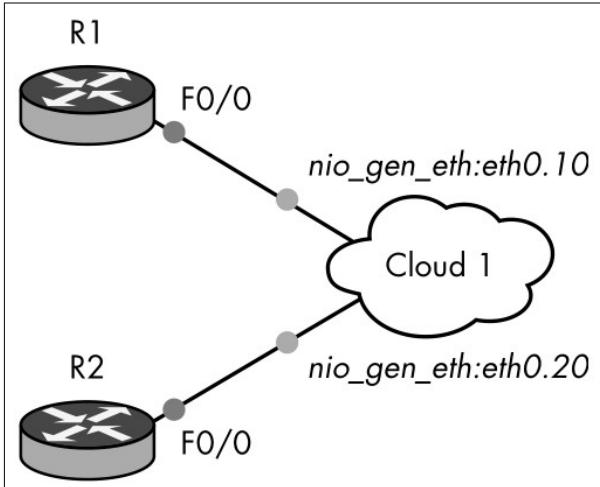


Figure 7-15: Virtual routers connected to Linux VLANs using a Cloud node

Nota

Se você criar grandes projetos usando várias VLANs, poderá atribuir apenas uma interface de VLAN do Linux por Cloud node para ajudar a esclarecer o layout em sua área de trabalho.

Seus roteadores GNS3 agora deve poder se comunicar com um ou mais switches Cisco reais.

Configuração opcional do switch breakout

Se você estiver executando o Windows ou OS X, poderá usar um GNS3 Switch node para vincular seu projeto a um switch breakout, como mostra a Figura 7-16. Nesta configuração, o breakout switch está configurado da mesma maneira que anteriormente, mas você precisará fazer alguns ajustes no seu PC. O Ethernet switch node se conecta a um Cloud node usando uma interface NIO configurada com um adaptador de loopback no Windows ou uma interface TAP no OS X. O adaptador virtual é conectado ao adaptador Ethernet físico do seu PC. Isso permite que a Cloud 1 se conecte ao breakout switch usando o adaptador Ethernet do seu PC.

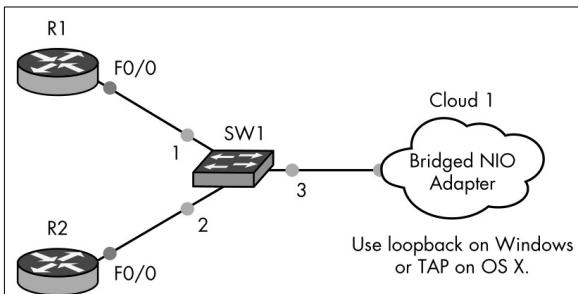


Figure 7-16: Breakout switch configuration using an Ethernet switch node

Para que o breakout switch funcione, você deve aumentar o tamanho da MTU no adaptador Ethernet físico do seu PC, mas nem todos os adaptadores são compatíveis com esse recurso. Se você é um usuário do OS X, o tamanho da MTU deve ser aumentado no adaptador físico e no adaptador virtual. Para aumentar o tamanho da MTU na linha de comando, use o seguinte exemplo:

```
$ sudo ifconfig en0 mtu 1546
$ sudo ifconfig tap0 mtu 1546
```

Nota

No OS X, configure o adaptador virtual e físico usando o mesmo tamanho de MTU ou a criação da bridge falhará.

Pode ser necessário verificar a documentação do adaptador Ethernet para configurá-lo no Windows. Em muitos adaptadores, no entanto, a configuração da MTU pode ser encontrada nas propriedades Avançadas do adaptador, conforme mostrado na Figura 7-17. Neste exemplo, o valor do pacote jumbo é definido como 9014 bytes em uma placa Intel PRO/1000 MT.

Quando você terminar de adicionar breakout VLANs ao Cloud node, adicione alguns roteadores ao seu espaço de trabalho e crie um link de cada roteador para uma breakout VLAN no Cloud node. Na Figura 7-15, o roteador R1 (F0/0) está vinculado à VLAN 10 na Cloud usando `nio_gen_eth:eth0.10` e R2 (F0/0) está vinculado à VLAN 20 usando `nio_gen_eth:eth0.20`.

Como o switch breakout é usado apenas para dividir VLANs em várias portas físicas, ele não requer configuração adicional. Neste exemplo, o roteador R1 agora está vinculado a qualquer switch ativo conectado à porta de switch breakout f0/2 e R2 deve ser vinculado a qualquer switch ativo conectado à porta f0/3.

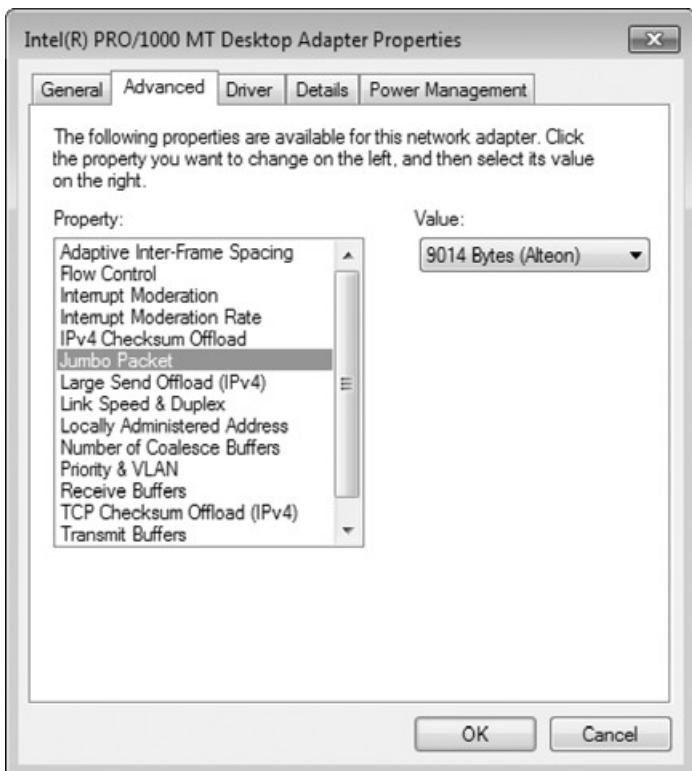


Figure 7-17: Setting the Jumbo Packet size on Windows

Em seguida, abra o **Node configurator** para o **Ethernet switch node** para definir VLANs e a porta de trunk dot1q, como mostra a Figura 7-18.

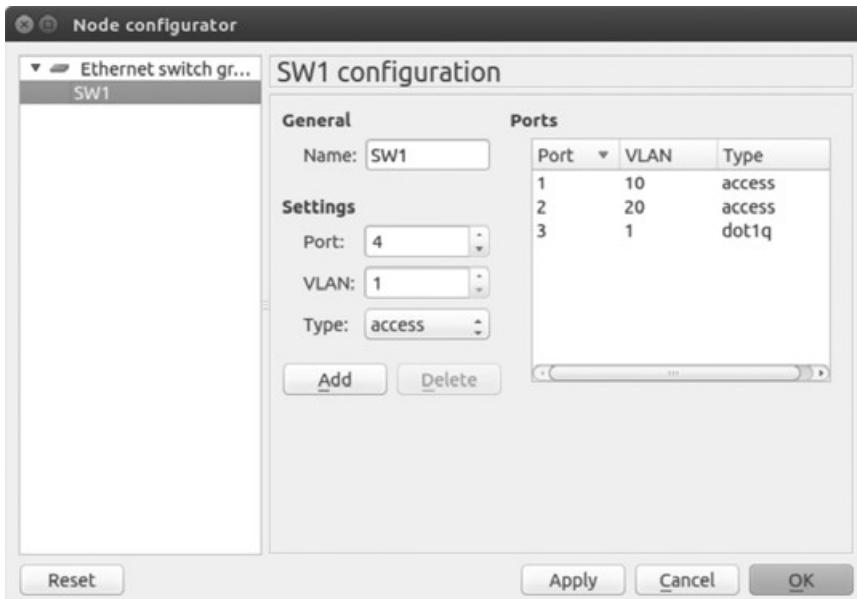


Figure 7-18: Ethernet switch node configured for breakout switch

Neste exemplo, R1 está conectado para acessar a Porta 1 (VLAN 10), R2 está conectado para acessar a porta 2 (VLAN 20) e a porta 3 é o dot1q trunk do breakout switch. Depois que tudo estiver configurado no GNS3, você poderá fazer logon e configurar o switch breakout com VLANs e tunelamento dot1q conforme descrito anteriormente.

Usando vários adaptadores no seu PC

Em vez de usar um tronco 802.1Q ou um breakout switch, você pode usar uma interface Ethernet física para cada roteador no GNS3. Se você tiver um laptop, poderá usar um hub USB e conectar vários adaptadores USB Ethernet ao seu PC; com um desktop, você pode usar o método do hub USB ou adquirir uma placa Ethernet de várias portas. A Figura 7-19 mostra o layout físico do design.

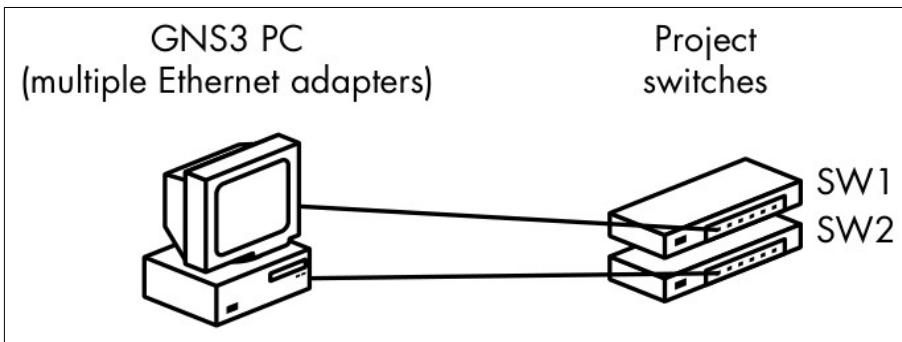


Figure 7-19: Physical layout using multiple adapters in a PC

Conecte cada adaptador Ethernet no seu PC a uma porta física em um switch Cisco real. Faça logon em cada switch e configure uma porta de acesso usando o comando `switchport mode access`. Em seguida, atribua um número VLAN exclusivo à porta digitando a porta de acesso de switch `vlan {número da vlan}`, como nas listagens a seguir.

Comece com o primeiro switch (c3550_sw1):

```
c3550_sw1(config)# interface f0/1
c3550_sw1(config-if)# description VLAN used for PC Ethernet Adapter 1
c3550_sw1(config-if)# switchport mode access
c3550_sw1(config-if)# switchport access vlan 10
```

Em seguida, configure o switch dois (c3550_sw2):

```
c3550_sw2(config)# interface f0/1
c3550_sw2(config-if)# description VLAN used for PC Ethernet Adapter 2
c3550_sw2(config-if)# switchport mode access
c3550_sw2(config-if)# switchport access vlan 20
```

Para conectar dispositivos GNS3 aos switches, adicione um Cloud Node ao seu Workspace e atribua uma interface Ethernet NIO para cada adaptador Ethernet no seu PC. Conecte seus roteadores GNS3 a cada interface NIO usando um roteador por interface.

Nota

Os usuários do OS X precisarão criar uma interface bridge exclusiva para cada adaptador e conectar cada interface Ethernet a uma interface TAP exclusiva. O OS X suporta até 16 dispositivos TAP (tap0 a tap15).

Depois que todos os dispositivos em seu projeto foram configurados, seus dispositivos GNS3 devem poder se comunicar com os switches Cisco ativos. É necessária uma configuração adicional nos switches para permitir o roteamento entre roteadores GNS3 e é determinada pelo design do bloco de switches que você cria. Agora, vamos dar uma olhada na conexão do GNS3 à Internet.

Conectando dispositivos GNS3 à Internet

Para conectar dispositivos GNS3 à Internet, você precisa usar um Ethernet adaptador no seu PC. Os adaptadores de rede sem fio não são suportados se você os usar diretamente, embora um possa funcionar se for criado uma bridge com um adaptador de loopback ou interface TAP (mas não conte com isso). Faça a conexão do GNS3 com a Ethernet da mesma maneira que você se conecta a um switch físico: adicione um Cloud node ao seu projeto e configure-o com uma interface NIO TAP ou NIO Ethernet.

Configurando o Windows

Nos sistemas Windows, crie uma ponte usando um adaptador de loopback e o adaptador Ethernet físico do seu PC. Em seguida, no GNS3, use um nó de nuvem configurado usando NIO Ethernet e selecione o adaptador de loopback. Como o adaptador de loopback está ligado ao adaptador Ethernet físico, você pode usar a nuvem para conectar-se a redes externas ao GNS3, incluindo a Internet. No Windows 8.x, instale um adaptador de loopback, mas não o adicione a uma ponte. Em vez disso, configure o ICS (Internet Connection Sharing) na sua interface física (Ethernet ou Wi-Fi). Para fazer isso, clique com o botão direito do mouse no botão **Start** e selecione **Network Connections**. Em seguida, clique com o botão direito do mouse na sua interface física e selecione **Properties**.

Selecione a guia **Sharing** e marque a opção **Allow other network users to connect through this computer's Internet connection**. Por fim, selecione seu adaptador de loopback no menu suspenso Conexão de rede doméstica e clique em **OK**.

Configurando sistemas baseados em Unix

No Ubuntu Linux, crie uma conexão Ethernet NIO usando o PC Interface Ethernet. No OS X e em alguns sistemas Linux, use um NIO TAP conexão configurada com /dev/tap0 e bridge da interface TAP à interface Ethernet do seu PC.

Criando uma rede simples

Crie um projeto adicionando um roteador e um Cloud node ao seu espaço de trabalho e adicionando um link do roteador à Cloud. Na Figura 7-20, a Cloud é configurada usando o adaptador de loopback do Windows, denominado *Local Area Connection 2*.

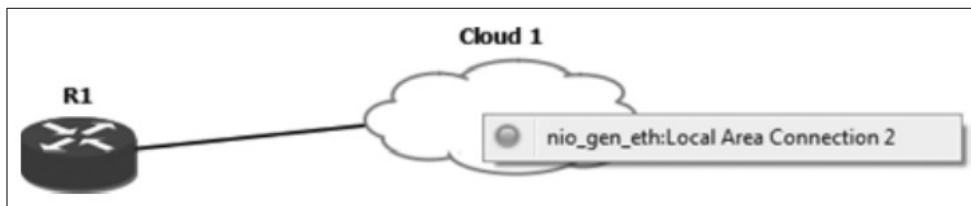


Figure 7-20: Connecting to a Cloud using a Windows loopback adapter

Para testar a conectividade com a Internet, conecte um cabo Ethernet do seu PC para um dispositivo de Internet, como um modem a cabo, e configure um endereço IP no seu roteador GNS3. Se você usa o DHCP para atribuir um endereço IP como eu fiz aqui, talvez seja necessário aguardar um momento para o roteador receber um endereço IP antes de poder testar a conectividade.

```
R1(config)# ip domain-lookup
R1(config)# ip name-server 8.8.8.8
R1(config)# interface f0/0
R1(config)# no shutdown
R1(config-if)# ip address dhcp
```

```
*Mar 1 00:01:08.875: %DHCP-6-ADDRESS_ASSIGN: Interface      FastEthernet0/0 assigned
DHCP address 192.168.1.101, mask 255.255.255.0, hostname R1
```

Após o seu roteador ter obtido um endereço IP, você poderá executar ping em um host na Internet. Tente fazer ping em [www.gns3.net!](http://www.gns3.net/) Você não está limitado a usar um roteador para se conectar à Internet; você também pode usar um dispositivo ASA, roteador Juniper ou qualquer outro dispositivo que suporte TCP / IP.

Nota

Se você tiver outros dispositivos atrás do roteador R1, precisará configurar o NAT no R1 antes que eles possam rotear para a Internet. Para obter mais informações, visite o site da Cisco (http://www.cisco.com/en/US/tech/tk361/technologies_tech_note09186a0080094e77.shtml#topic6).

Considerações finais

Neste capítulo, examinamos a configuração dos nodes do dispositivo GNS3 e a integração deles em seus projetos usando o Cisco IOS. Eles são simples de configurar e adequados para grandes projetos, pois reduzem bastante a carga no seu PC. Comparado aos dispositivos Dynamips, os nós do dispositivo GNS3 quase não usam recursos de PC.

Conectar um dispositivo GNS3 a um switch Cisco ativo é complicado. Se você optar por criar um trunk 802.1Q padrão para conectar-se a um switch ativo, poderá usar um roteador EtherSwitch ou um Ethernet switch node, mas o sistema operacional do seu PC e os drivers do adaptador Ethernet devem suportar a marcação 802.1Q. Sem as tags VLAN adequadas, o entroncamento não funcionará. Se você tiver um switch IOS extra, poderá criar um switch breakout, que é uma maneira muito confiável de integrar vários switches Cisco reais em seus projetos GNS3. Um switch breakout funciona de maneira mais confiável nos sistemas Linux, mas também pode ser configurada usando o Windows e o OS X. No próximo capítulo, veremos alguns recursos mais avançados, incluindo Cisco, ASA e IDS / IPS.

8

CISCO ASA, IDS/IPS, E IOS-XRV

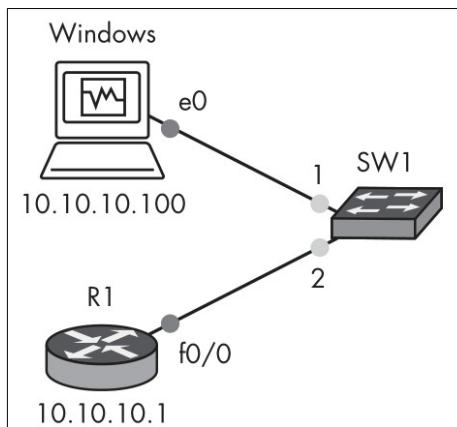
Você já viu algumas das maneiras pelas quais o GNS3 pode interagir com outros softwares e sistemas operacionais. Neste capítulo, você se aprofundará nos recursos avançados do GNS3 e explorará como pode expandir seus projetos interagindo com dispositivos virtuais e softwares adicionais do Quick Emulator (QEMU).

O conhecimento de tecnologias como ASAs da Cisco, sistemas de detecção de intrusão/sistemas de prevenção de intrusões (IDSs/IPSs) e IOS-XR amplia sua visão do Cisco e do GNS3 e pode ser útil na escolha de um caminho de certificação de rede. Além disso, é muito divertido jogar com produtos Cisco virtualizados que, de outra forma, são inacessíveis para a maioria das pessoas. Também é importante aprender a usar algumas das ferramentas baseadas em GUI da Cisco.

Começarei mostrando como instalar o software Cisco Configuration Professional (CCP), uma alternativa baseada na Web para configurar roteadores por meio da interface de linha de comando da Cisco. Em seguida, você aprenderá como configurar e executar um ASA. Discutirei o uso do software ASDM (Adaptive Security Device Manager) da Cisco, que é semelhante ao software CCP mencionado anteriormente, mas usado para configurar os ASAs. No final do capítulo, você aprenderá que a paciência não é apenas uma virtude, mas um pré-requisito ao configurar um Cisco IDS/IPS. Por fim, mostrarei como configurar e usar dispositivos Cisco IOS-Xrv no GNS3.

Cisco Configuration Professional

A maioria dos engenheiros usa comandos do IOS para configurar roteadores e switches, mas existem outras maneiras. O CCP é uma alternativa baseada na Web que usa “assistentes inteligentes” para simplificar a configuração do roteador e fornece ferramentas para ajudá-lo a monitorar e solucionar problemas de redes e VPNs. Em poucas palavras, o CCP permite que usuários menos experientes instalem seus equipamentos.



Configuração do Projeto

Para usar o CCP com GNS3, você cria um projeto simples usando um roteador e uma máquina virtual VirtualBox executando o Microsoft Windows, como na Figura 8-1. Embora existam outros métodos para fazer isso, escolhi demonstrar esse método porque ele deve funcionar em qualquer PC executando o GNS3 (Windows, Linux e OS X).

Faça logon no computador com Windows e desative o firewall para garantir que o CCP tenha comunicação irrestrita com o seu roteador. (Isso não é obrigatório, mas pode evitar dores de cabeça posteriormente.) Atribua ao convidado do Windows um endereço IP na mesma sub-rede que o seu roteador (neste exemplo, 10.10.10.100). Em seguida, crie uma configuração básica no seu roteador.

Figure 8-1: CCP topology with a router and Windows host

```
① R1(config)# ip http server  
R1(config)# ip http secure-server  
R1(config)# ip http authentication local  
② R1(config)# username admin privilege 15 secret cisco  
R1(config)# interface f0/0  
③ R1(config-if)# ip address 10.10.10.1 255.255.255.0  
R1(config-if)# no shutdown
```

Você precisa habilitar o servidor da web do roteador ①, crie um usuário com privilégios completos no modo EXEC ② e atribua um endereço IP à interface ③. Neste exemplo, o roteador recebe o endereço IP 10.10.10.1.

Nota

É necessário criar uma conta de administrador da Cisco com privilégios completos no modo EXEC (privilegio 15), para que mais tarde você tenha direitos suficientes para configurar o roteador usando o CCP.

Depois de configurar o roteador, teste a conectividade entre o convidado do Windows e o roteador usando um comando ping.

C:> ping 10.10.10.1

Se você conseguir executar o ping com êxito no roteador, é seguro continuar. Se você não puder executar ping no roteador, verifique seus endereços IP e interfaces.

Instalação do CCP

O CCP é um aplicativo baseado em Java que interage com um navegador da Web. Portanto, antes de começar, faça o download e instale o Java se você ainda não o possui (<http://www.java.com/>). Verifique se você possui a versão mais recente do Adobe Flash Player (<http://www.adobe.com/>). Você pode fazer o download do Cisco Configuration Professional no site da Cisco (<http://www.cisco.com/>). Para instalar o CCP, faça logon na sua máquina virtual Windows e inicie o programa de instalação; você deve ver o assistente de instalação do CCP. Clique em Avançar e siga as instruções para concluir a instalação.

Executando o CCP

Inicie o Cisco Configuration Professional clicando com o botão direito do mouse no ícone do programa e escolhendo Executar como Administrador. Quando o programa for aberto, você será solicitado a fornecer o endereço IP do roteador que deseja gerenciar. Você deve ver o CCP Device Manager, mostrado na Figura 8-2.

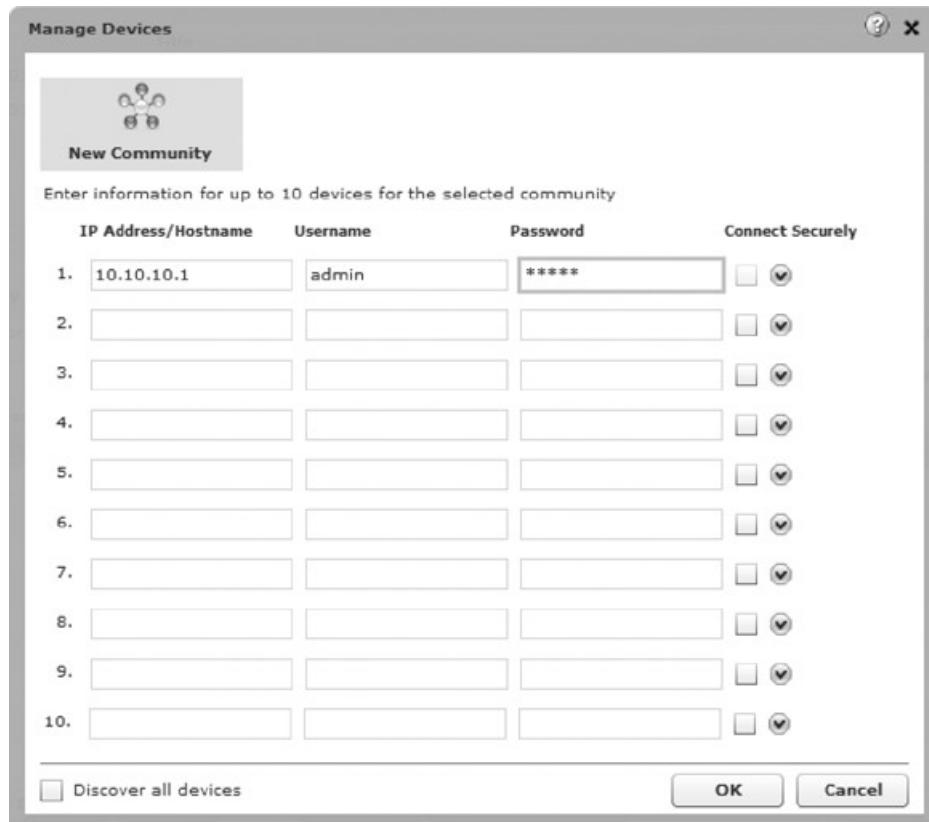


Figure 8-2: CCP Device Manager

Digite o endereço IP atribuído ao roteador (**10.10.10.1**), digite o nome de usuário e senha do administrador que você atribuiu anteriormente (**admin** e **cisco**) e, em seguida, clique em **OK**. Após o logon, você deverá ver a tela de gerenciamento do CCP, mostrada na Figura 8-3.

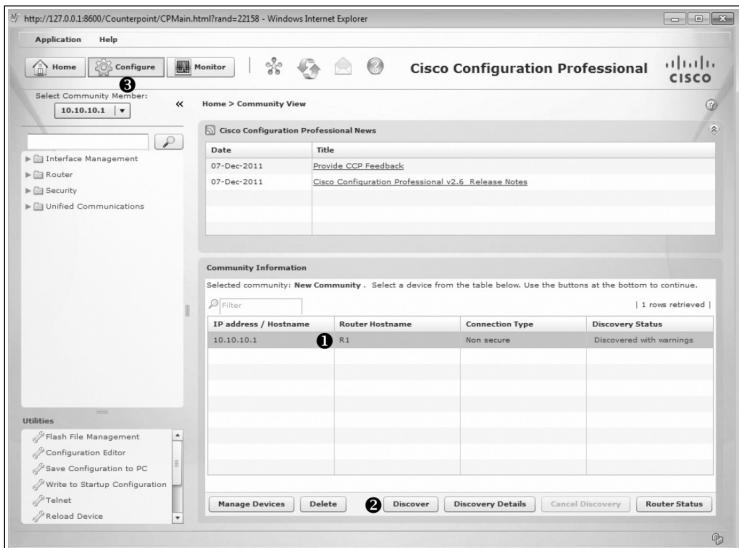


Figure 8-3: Cisco CCP management screen

Antes de gerenciar seu roteador, você deve selecioná-lo clicando primeiro no nome do host do roteador R1 ① e, em seguida, clicando em **Discover** ② para que o CCP possa descobrir seus recursos e capacidades. Após a descoberta, você pode configurar seu roteador clicando em **Configure** ③ na barra de ferramentas. A vantagem de usar o CCP é que ele o orienta no processo de atribuição de endereços IP, NAT, VPNs e outros recursos da Cisco sem que você precise conhecer nenhum comando do IOS. Esteja ciente de que os exames de certificação da Cisco concentram-se principalmente nos comandos do IOS, e não no CCP, para configurar dispositivos.

Firewall Cisco ASA

O ASA da Cisco é uma versão aprimorada do antigo firewall PIX. O GNS3 emula um Cisco ASA modelo 5520. Embora não seja um roteador, você pode se surpreender ao saber que o ASA suporta vários protocolos de roteamento, incluindo RIP, EIGRP e OSPF, permitindo que você os conecte facilmente em rede com outros dispositivos roteados GNS3.

Adquirindo uma imagem

Antes de poder usar uma máquina virtual ASA com GNS3, você precisa de um arquivo de imagem do sistema operacional ASA. A maneira mais rápida de obter uma imagem do sistema operacional ASA é copiá-la de um ASA que você já possui (ou seja, do CD de instalação do ASA ou diretamente de um dispositivo ASA). Copiar arquivos de um Cisco ASA funciona da mesma maneira que copiar arquivos de um roteador Cisco: você pode usar FTP ou TFTP. Neste exemplo, você usará um servidor TFTP. Existem muitos servidores TFTP gratuitos para escolher, então encontre um que você goste e instale-o no seu PC. Depois de ter um servidor TFTP em execução na sua rede, logue-se no seu ASA físico e copie seu arquivo de imagem ASA para o seu PC. Na listagem a seguir, meu arquivo de imagem ASA é nomeado *asa824-k8.bin* e meu servidor TFTP está sendo executado em um PC no endereço IP 192.168.1.100:

```
ciscoasa# copy flash:asa824-k8.bin tftp
Address or name of remote host []? 192.168.1.100
```

Depois de ter um arquivo de imagem ASA, é necessário fazer algumas modificações no arquivo antes de poder usá-lo com o GNS3.

Preparando a imagem ASA para GNS3

O Cisco ASA é realmente apenas um pequeno PC Linux, e os arquivos de imagem ASA como *asa824-k8.bin* contêm um sistema operacional Linux compacto projetado para rodar no hardware ASA. O arquivo de imagem inclui um kernel Linux e outro software de suporte para o aparelho. Para executar o software ASA usando o GNS3, é necessário descompactar o arquivo *.bin*, fazer algumas modificações e recompactá-lo da maneira adequada para o QEMU. Felizmente, existem muitas pessoas inteligentes nas comunidades Linux e Cisco que criaram software de descompactação de imagens que faz isso por você. Você pode fazer o download do Cisco Image Unpacker para Windows no site do GNS3 ou usar um script de shell do Linux como *repack.v4.sh*. Independentemente de qual descompactador escolher, você precisará encontrar um projetado para a sua versão do software ASA. Depois de executar o script, você deve ficar com dois arquivos: *asa-vmlinuz* (um kernel do Linux) e *asa-initrd.gz* (um arquivo de

disco RAM). Esses são os arquivos usados pelo QEMU e GNS3. Se você não deseja modificar seu próprio arquivo de imagem ASA, uma pesquisa rápida na Internet deve gerar muitos arquivos ASA prontos para uso. Essas imagens geralmente vêm em um arquivo *.zip* que contém os dois arquivos (*asa-vmlinu*x e *asa-initrd.gz*).

Configurando GNS3 para ASA

Antes de configurar um ASA no GNS3, verifique se QEMU está instalado e testado no seu PC. (Consulte as informações de instalação do QEMU para sistema operacional em particular no capítulo 6.) Em seguida, inicie o GNS3, selecione **Edit** ▶ **Preferences** no Linux e Windows ou **GNS3** ▶ **Preferences** no OS X e escolha **QEMU VMs** no painel à esquerda, como mostra a Figura 8-4.

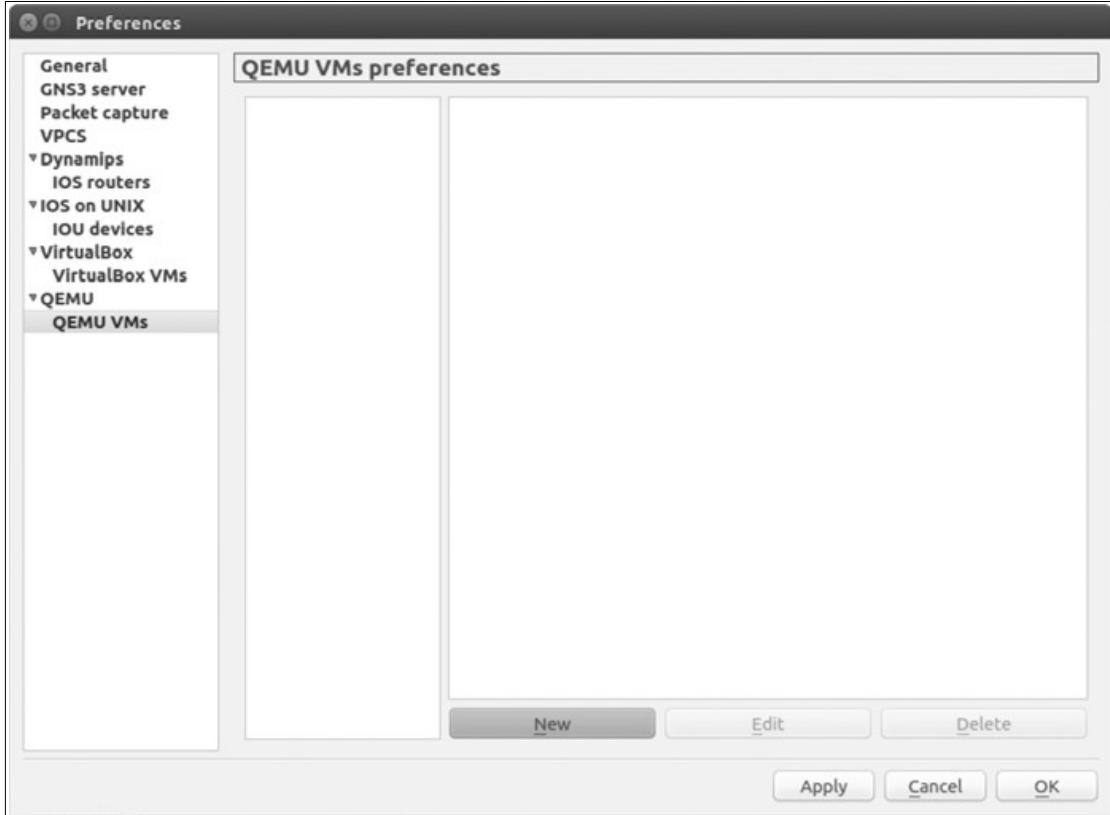


Figure 8-4: QEMU VMs preferences

Para criar um novo ASA no GNS3, clique em **New** para iniciar o assistente para Nova VM QEMU. Selecione **ASA 8.4 (2)** no menu suspenso **Type**, como mostrado na Figura 8-5.

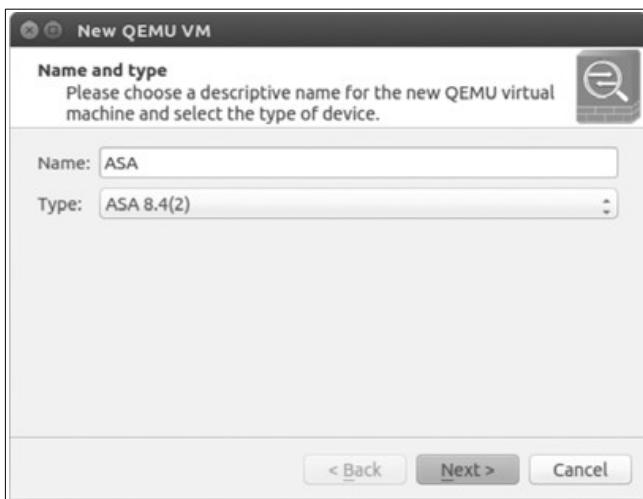


Figure 8-5: Creating a new QEMU virtual machine and setting Type to ASA 8.4(2)

Por padrão, seu dispositivo é nomeado automaticamente ASA, mas você pode renomeá-lo da maneira que preferir. Quando terminar de nomear seu ASA, clique em **Next** para continuar. O assistente deve localizar e escolher automaticamente o arquivo binário QEMU correto para o seu PC, como mostra a Figura 8-6.

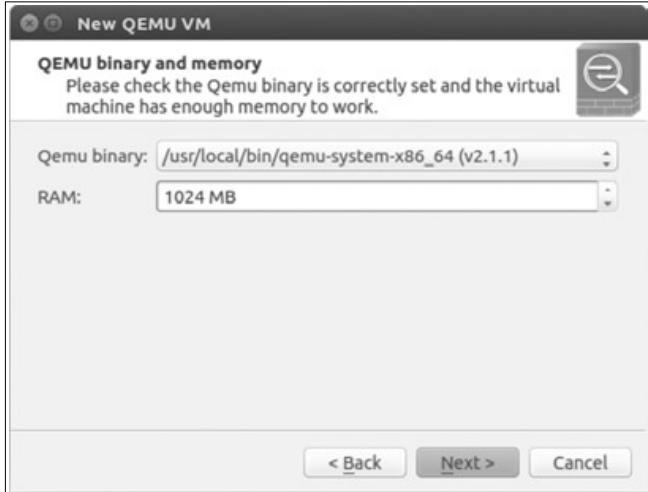


Figure 8-6: Selecting the ASA virtual machine's QEMU binary and memory

Se não encontrar um binário QEMU, verifique se o QEMU está instalado diretamente no seu PC e tente novamente. O valor padrão da RAM é 1024MB, mas esse é o valor mínimo necessário para executar a imagem ASA. Você pode aumentar o valor inserindo um novo valor no campo. Quando terminar, clique em Avançar para continuar o assistente. O último passo é procurar e selecionar o disco RAM inicial e a imagem do kernel, como mostra a Figura 8-7.

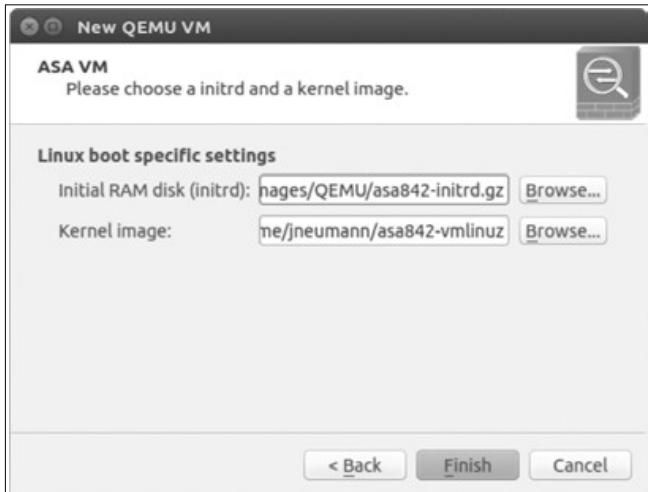


Figure 8-7: Linux boot-specific settings for an ASA virtual machine

Defina o disco RAM inicial (initrd) e a imagem do kernel como os arquivos corretos para seu computador; estes são geralmente denominados *asa842-initrd.gz* e *asa842-vmlinuz*, respectivamente. Quando terminar de escolher as duas imagens, clique em **Finish** para concluir a instalação. Após adicionar seu ASA com sucesso, o dispositivo ASA deve ser exibido na janela Preferências da VM QEMU, como mostra a Figura 8-8.

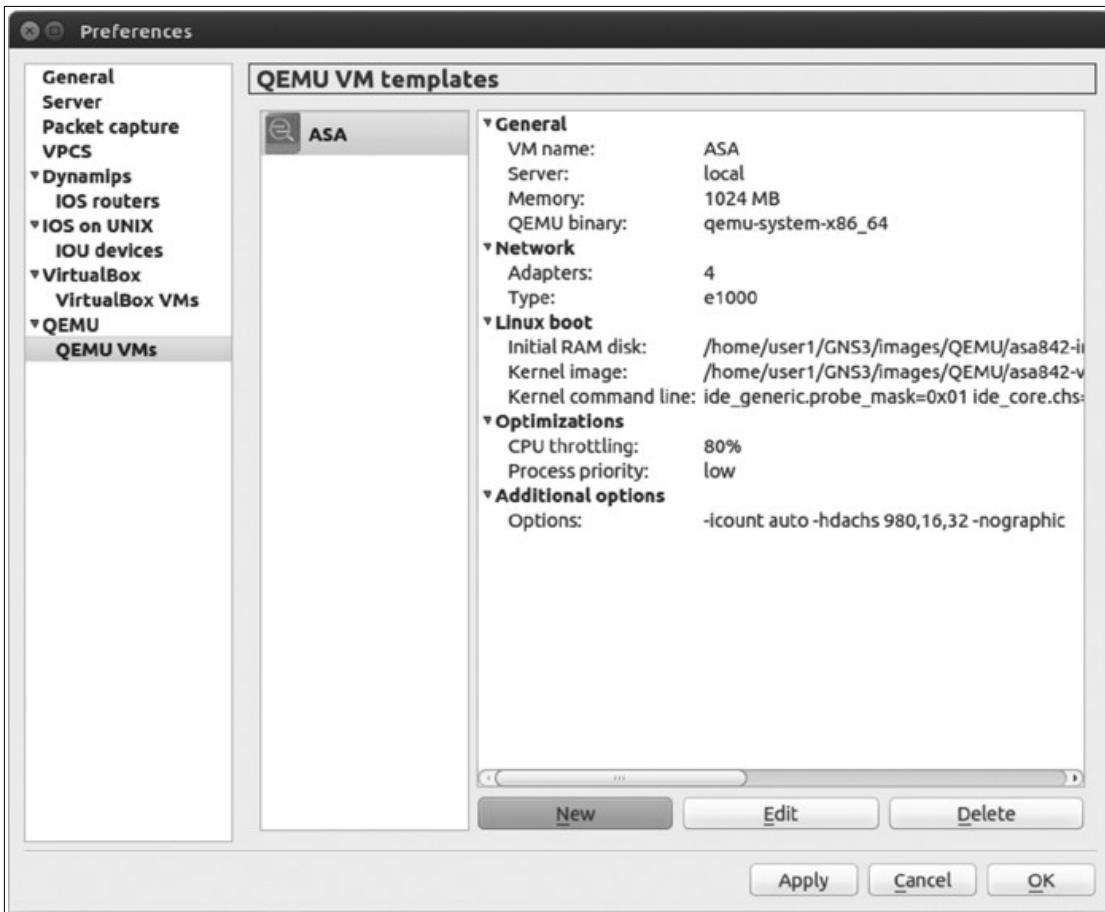


Figure 8-8: QEMU VMs preferences for an ASA virtual machine

As configurações atuais do seu ASA devem ser exibidas no painel à direita, e uma configuração que você deve observar é a otimização da CPU (localizada em Otimizações). Ao contrário dos dispositivos Dynamips, o ASA não tem uma opção de PC inativo para controlar o consumo da CPU. Isso significa que um ASA pode consumir toda a CPU, como um roteador Dynamips, quando nenhum valor de PC ocioso foi definido. Para evitar isso, o GNS3 usa outro aplicativo de código aberto (cpulimit) para ajustar a quantidade máxima de CPU que uma instância QEMU/ASA pode consumir. O valor padrão é 80%, o que funciona bem na maioria das situações. Você pode editar suas configurações ASA e aumentar ou diminuir o valor, mas tenha cuidado; usar muito pouco de sua CPU, diminuindo a porcentagem, pode resultar em desempenho ruim do ASA e travamentos frequentes do ASA. Uma porcentagem muito alta pode resultar em um desempenho geral mais lento do PC. Outra configuração a ser observada em Otimizações é a prioridade do processo. O valor padrão no GNS3 é baixo, mas pode ser definido como baixo, médio ou alto. A prioridade do processo determina quando a instância QEMU/ASA obtém o tempo da CPU.

Processos com alta prioridade obtêm acesso à CPU antes de processos com baixa prioridade. Em geral, alterar a prioridade deve ter pouco ou nenhum efeito em seu sistema, mas, para ser seguro, mantenha-o em nível baixo para impedir que seu ASA substitua potencialmente importantes processos do sistema. No Windows e no OS X, o programa cpulimit deveria ter sido instalado com o GNS3. No Ubuntu Linux, você precisa instalar o cpulimit usando o seguinte comando:

```
$ sudo apt-get install cpulimit
```

Agora que sua máquina virtual ASA não dominará seu sistema, vamos fazer logon em um ASA e executar uma configuração básica.

Testando um ASA no GNS3

Arraste um nó de firewall ASA da barra de ferramentas Dispositivos para o seu espaço de trabalho. Seu ASA deve estar localizado na seção Dispositivos de segurança da barra de ferramentas. Inicie o ASA e abra uma conexão de console GNS3. Enquanto ele carrega, você deve ver as mensagens de inicialização ASA padrão seguidas pelo prompt de comando ASA:

```
ciscoasa>
```

Algumas mensagens de erro antes do prompt são perfeitamente normais, mas se seu ASA falha ao iniciar ou você vê muitos erros, verifique suas configurações ou tente um arquivo de imagem ASA diferente.

Nota

Não é incomum um ASA no GNS3 travar ou paralisar durante o ciclo de inicialização, especialmente em hardware mais antigo. Se isso acontecer, pare e reinicie o ASA. Pode levar algumas tentativas antes de você obter uma inicialização bem-sucedida.

Para testar a conectividade de rede simples, crie um link do seu ASA para outro dispositivo GNS3 no seu espaço de trabalho. Em seguida, abra uma conexão de console ao ASA e configure uma interface com um endereço IP.

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# interface GigabitEthernet0
ciscoasa(config-if)# ip address 10.10.10.1 255.255.255.0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# no shutdown
```

Depois de configurar uma interface, use um comando ping para testar conectividade do seu ASA para outros dispositivos no seu projeto.

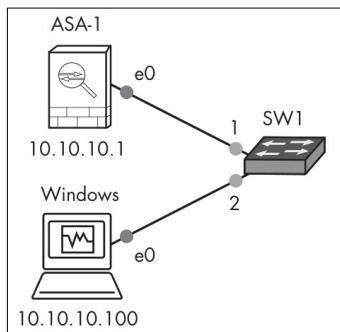
Atenção

Mesmo com a otimização da CPU ativada, os dispositivos ASA fazem uso intensivo o processador, portanto, você pode usá-los com moderação em seus projetos, especialmente se você tiver um PC de baixo custo.

Depois de verificar se o seu dispositivo ASA está funcionando corretamente, você está pronto para começar a adicioná-lo aos seus projetos. Isso pode ser útil para aprender como configurar o ASA ou se preparar para um exame de certificação Cisco.

Instalação do ASDM

O ASDM da Cisco é semelhante ao software CCP que foi abordado em "Cisco Configuration Professional" na página 124, então muitos detalhes são os mesmos. Como o CCP, o ASDM fornece uma interface da Web baseada em Java, aponte e clique. A principal diferença entre o CCP e o ASDM é que o ASDM foi projetado para configurar apenas o Cisco ASA, e não outros dispositivos Cisco.



Antes de instalar o software ASDM, crie um projeto como o da Figura 8-9. Você usará a máquina virtual do Windows para instalar e executar o aplicativo ASDM e, em seguida, iniciará o ASDM e o usará para uma olhada no ASA.

Há duas maneiras de adquirir o software ASDM: copie-o da memória flash de um ASA real ou encontre-o online. Depois de ter o software ASDM, ele precisa ser armazenado na unidade flash do seu ASA virtual; a partir daí, você o instalará no PC da máquina virtual Windows usando um navegador da web.

Figure 8-9: ASDM topology with an ASA firewall and Windows guest

Eu recomendo o Mozilla Firefox porque descobri que ele executa o ASDM melhor que o Internet Explorer. (Certifique-se de desativar os bloqueadores de pop-up e firewalls e instalar a versão mais recente do Java.) Você também precisará do software do servidor FTP ou TFTP para copiar o software ASDM da máquina virtual Windows GNS3 para o seu ASA. Depois de ter uma imagem ASDM, há algum trabalho de preparação a ser feito no Dispositivo ASA para que você possa copiar sobre a imagem ASDM. Digite estes comandos no ASA:

```
ciscoasa(config)# interface gigabitEthernet0
① ciscoasa(config-if)# ip address 10.10.10.1 255.255.255.0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# exit
② ciscoasa(config)# username admin password cisco privilege 15
③ ciscoasa(config)# http server enable
ciscoasa(config)# http 10.10.10.0 255.255.255.0 inside
```

Assim como quando você configura o CCP, comece atribuindo um endereço IP a um interface interna ①. Em seguida, crie uma conta de usuário local ②e habilite o Servidor HTTP ③. Depois que o ASA estiver configurado e você tiver o software ASDM no seu Servidor FTP ou TFTP, copie o software da sua máquina virtual Windows para a memória flash do ASA.

```
ciscoasa# copy tftp flash
Source filename []? asdm-641.bin
Address or name of remote host []? 10.10.10.100
Destination filename [asdm-641.bin] <enter>
Accessing tftp://10.10.10.100/asdm-641.bin !!!!!!!!
```

Este exemplo copia um arquivo chamado asdm-641.bin da minha máquina virtual Windows GNS3 para o meu dispositivo ASA usando TFTP. Após copiar o arquivo ASDM, você precisa instalar o software na sua máquina virtual Windows. Inicie o seu navegador da web e abra uma conexão HTTP segura (HTTPS) com o endereço IP do seu ASA. Você deve receber uma tela semelhante à Figura 8-10.

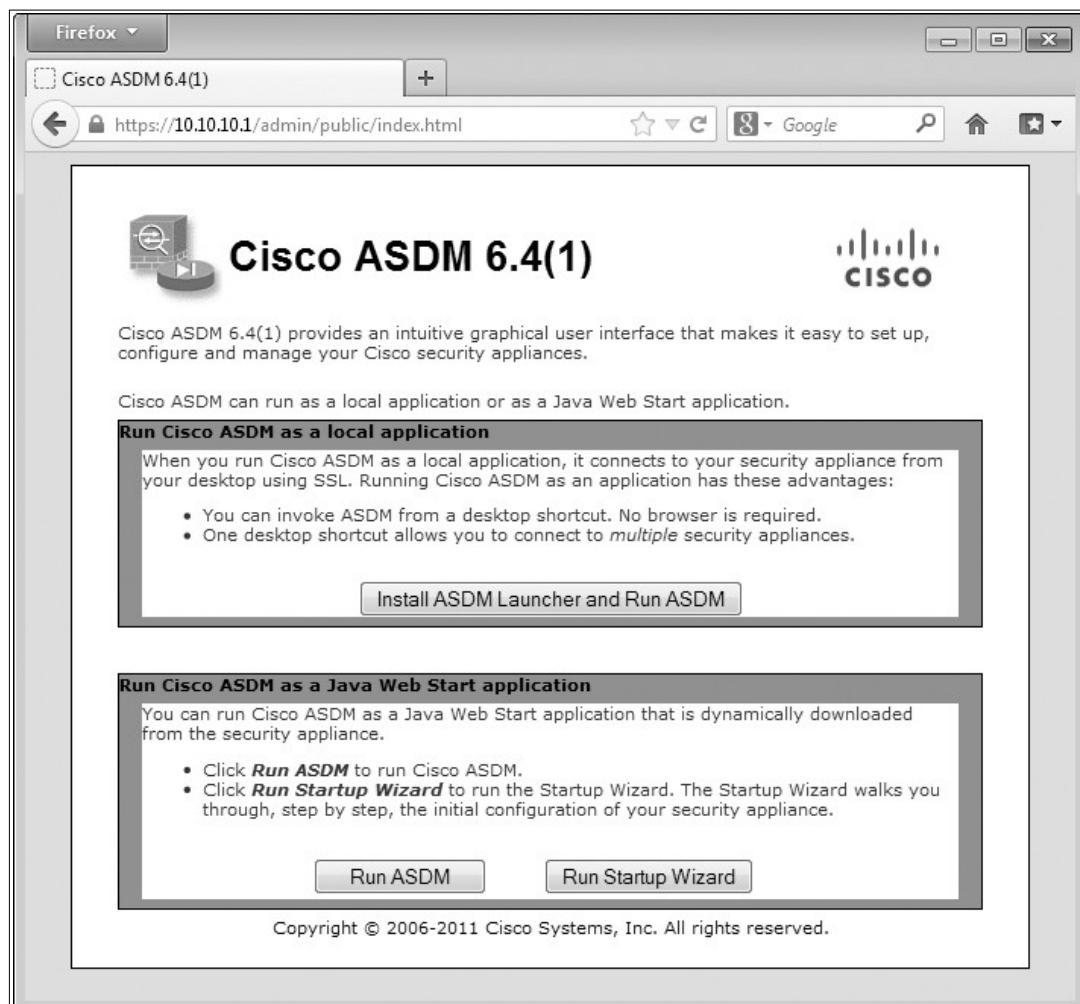


Figure 8-10: Cisco ASDM install screen

Como você usará a opção Java Web Start, clique em **Run ASDM**. Seu PC deve baixar o software Java e apresentar alguns avisos de segurança, nos quais você pode clicar com segurança até ver o Cisco ASDM-IDM Launcher, mostrado na Figura 8-11.



Figure 8-11: Windows ASDM-IDM Launcher

Digite seu nome de usuário e senha ASA (**admin** e **cisco**) e selecione OK para fazer logon no seu ASA. Após o logon bem-sucedido, você pode começar a configurar o sistema no Painel de Dispositivos ASDM, mostrado na Figura 8-12.

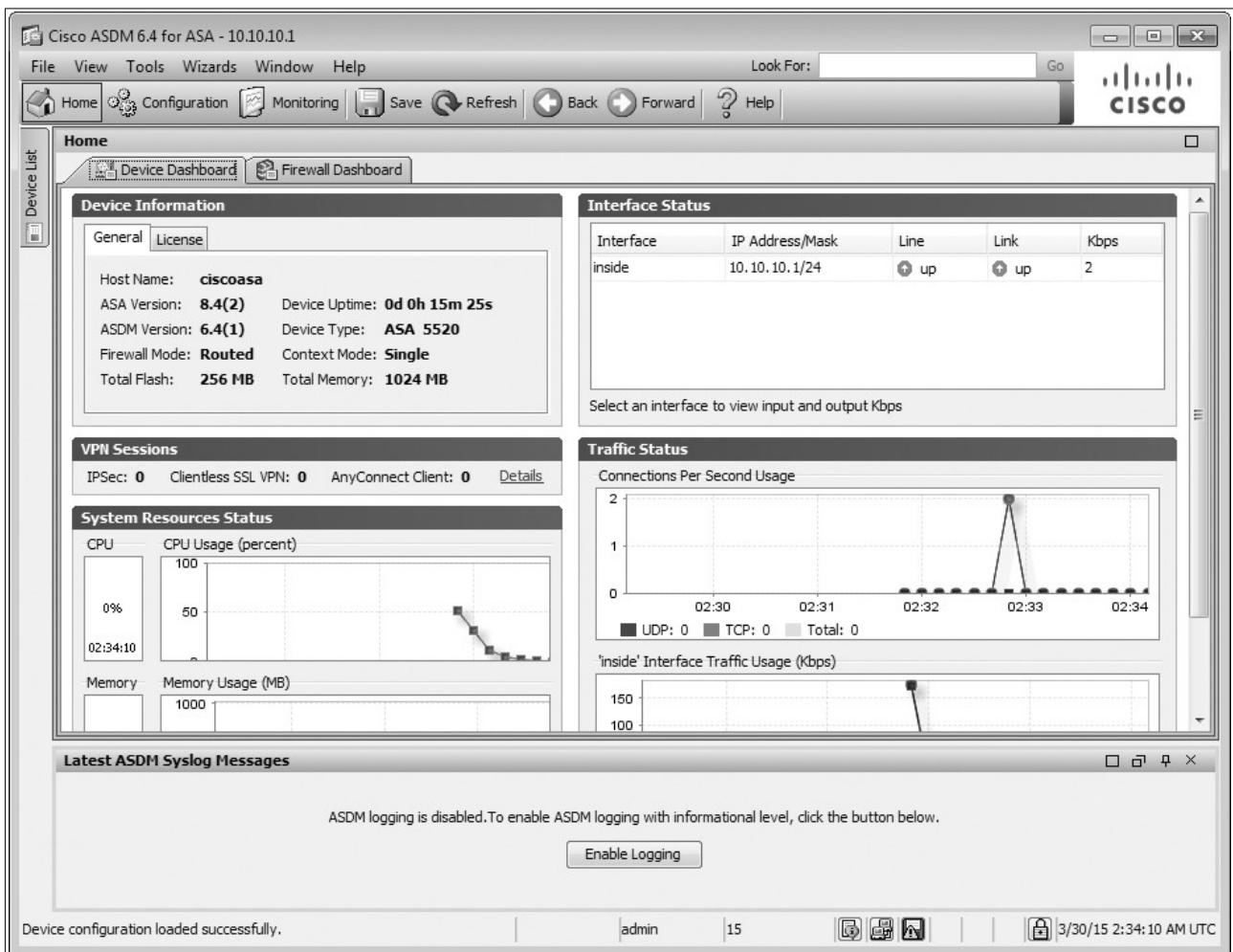


Figure 8-12: ASDM Device Dashboard

O Painel de dispositivos ASDM inclui vários assistentes que fornecem configurações guiadas para criar configurações comuns de rede e rede virtual privada (VPN). Ele também fornece muitas estatísticas em tempo real para ajudá-lo a monitorar o desempenho da sua rede. Embora não seja necessariamente útil no GNS3, essas informações podem ser inestimáveis para manter uma rede saudável na vida real.

Cisco IDS/IPS

O Cisco IDS/IPS identifica e evita atividades maliciosas em uma rede. No mundo real, um IDS / IPS pode ser um dispositivo Cisco independente ou um módulo que você conecta a um ASA ou roteador de serviço integrado. Criar uma máquina virtual IDS/IPS para GNS3 é uma verdadeira dor de cabeça em comparação com a maioria das tarefas; portanto, antes de começar, convém reservar algumas horas.

Adquirindo uma imagem IDS / IPS

Como o PIX e o ASA, o IDS / IPS é executado em software Linux especial. Se você possui um dispositivo físico IDS / IPS, um CD de atualização / recuperação contendo o software deve ter sido fornecido com o dispositivo. Para instalar o IDS / IPS usando uma máquina virtual QEMU, você precisa de um ISO imagem do CD. Você pode criar seu próprio arquivo de imagem ISO usando seu CD ou encontrar um na Internet. Neste exemplo, usei um arquivo de imagem do IOS chamado *IPS-K9-cd-1.1-a-6.0-6-E3.iso*. Outras versões do software podem funcionar bem, mas esta versão provou funcionar bem para criar um IDS/IPS compatível com GNS3.

Criando um sistema IDS/IPS pronto para QEMU

O software IDS/IPS é executado usando o QEMU, verifique se você o instalou no seu PC e testou-o com o GNS3 antes de começar. Em seguida, crie um diretório de construção para seu IDS/IPS e copie seu arquivo ISO para o diretório. É aqui que você cria a máquina virtual IDS/IPS. Para instalar o software IDS/IPS em uma máquina virtual QEMU, você precisa criar dois arquivos de imagem de disco rígido virtual QEMU. Abra uma janela do terminal e digite os seguintes comandos para criar as imagens:

```
$ qemu-img create ipsdisk1.img 512M  
$ qemu-img create ipsdisk2.img 4000M
```

NOTA

No Windows e no OS X, pode ser necessário definir o caminho do sistema para incluir o local da instalação do QEMU. Consulte “Instalando o QEMU no Windows e OS X” na página 63 para obter detalhes.

Agora que você criou os discos virtuais, digite o seguinte comando para inicializar sua máquina virtual a partir do arquivo de imagem ISO:

```
$ qemu-system-i386 -hda ipsdisk1.img -hdb ipsdisk2.img -m 1024 -cdrom IPS-K9 -cd-1.1-a-6.0-6-E3.iso -boot d
```

Nos sistemas Windows, substitua `qemu-system-i386` neste comando por `qemu-system-i386w`. Depois que o sistema inicializar, você verá uma tela semelhante à Figura 8-13.

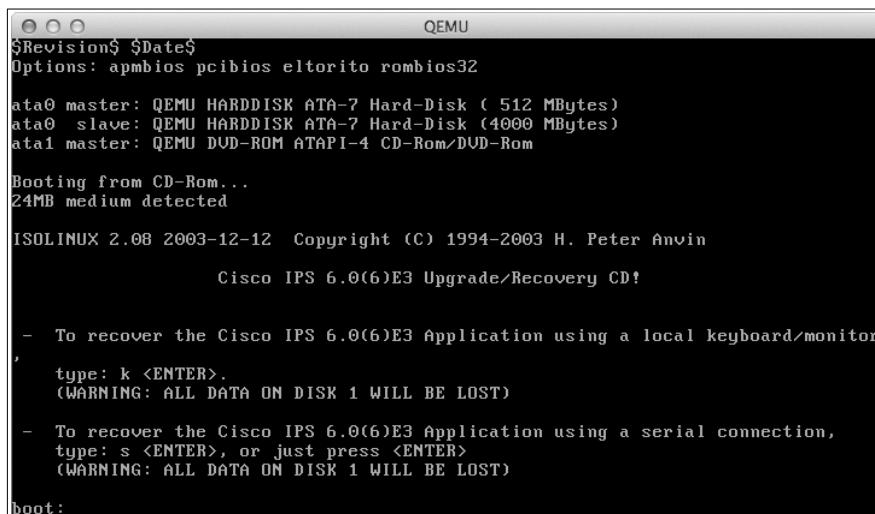
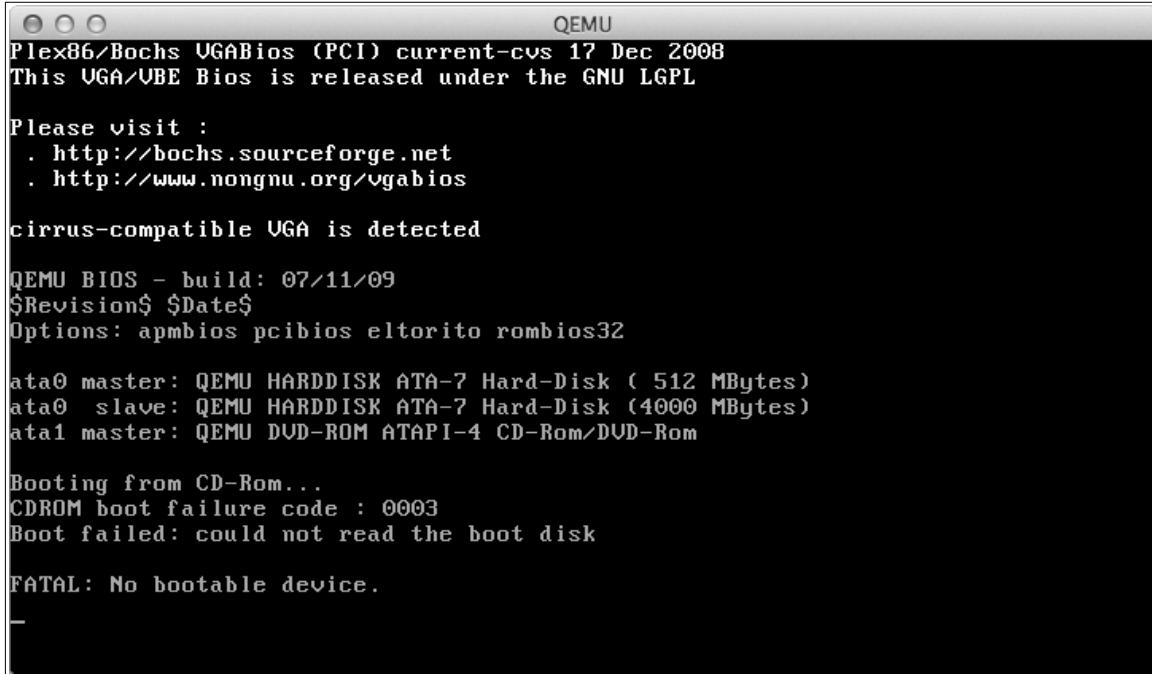


Figure 8-13: IDS/IPS installation screen

No prompt *boot:*, digite **k** para executar uma recuperação completa do sistema. Durante o processo de recuperação, sua máquina virtual QEMU inicializa o Linux a partir da imagem ISO, instala um carregador de inicialização GRUB e instala o software IDS/IPS. Quando a instalação terminar de copiar os arquivos, a máquina virtual será reiniciada automaticamente e terminará com uma mensagem de erro de inicialização "FATAL", como mostra a Figura 8-14.



The screenshot shows a terminal window titled "QEMU" with the following text output:

```
Plex86/Bochs VGABios (PCI) current-cvs 17 Dec 2008
This VGA/VBE Bios is released under the GNU LGPL

Please visit :
. http://bochs.sourceforge.net
. http://www.nongnu.org/vgabios

cirrus-compatible VGA is detected

QEMU BIOS - build: 07/11/09
$Revision$ $Date$
Options: apmbios pcibios eltorito rombios32

ata0 master: QEMU HARDDISK ATA-7 Hard-Disk ( 512 MBytes)
ata0 slave: QEMU HARDDISK ATA-7 Hard-Disk (4000 MBytes)
ata1 master: QEMU DVD-ROM ATAPI-4 CD-Rom/DVD-Rom

Booting from CD-Rom...
CDROM boot failure code : 0003
Boot failed: could not read the boot disk

FATAL: No bootable device.
```

Figure 8-14: FATAL: No bootable device

Não se preocupe, esse erro é perfeitamente normal e esperado. Saia do QEMU e digite o seguinte comando para inicializar o IDS/IPS novamente:

```
$ qemu-system-i386 -name IPS4215 -hda ipsdisk1.img -hdb ipsdisk2.img -m 1024 -smbios type=1,product=IDS-4215 -
net nic,vlan=1,model=e1000 -net nic,vlan=2,model=e1000
```

A máquina virtual IDS/IPS será inicializada em um menu de inicialização do Linux GRUB. No menu de inicialização, digite **e** para editar uma entrada. Use a tecla de seta para mover para baixo para destacar a entrada do *kernel* e digite **e** novamente para editar essa entrada. Use a tecla de seta para trás para localizar e alterar **init=/loadrc** para **init=1**. Pressione **ENTER** para aceitar a alteração e pressione **b** para inicializar no menu GRUB modificado. O sistema agora deve iniciar, ignorando a inicialização do IDS/IPS e trazê-lo para um console Linux. Na linha de comando do console, você usará o editor **vi** para modificar alguns arquivos de configuração do IDS/IPS.

NOTA

Você precisa usar o editor vi para modificar arquivos porque nenhum outro editor está instalado. Se você não conhece o vi, deve atualizá-lo antes de continuar. Basta procurar o man vi online ou digite man vi na linha de comando para visualizar a página do manual.

Depois de se familiarizar com os comandos de edição do **vi**, você estará pronto para continuar.

Como seqüestrar o hardware

Primeiro, você precisa enganar o software IDS / IPS para pensar que sua máquina virtual QEMU é um verdadeiro sensor de dispositivo Cisco IDS-4215. Para enganar o software, você deve modificar dois arquivos: *ids_functions* e *interface.conf*. A modificação desses arquivos é bastante entediante e o menor erro impedirá a criação de um dispositivo IDS/IPS em funcionamento. Comece digitando os seguintes comandos no prompt do shell:

```
-sh-2.05b# /loadrc  
-sh-2.05b# cd /etc/init.d  
-sh-2.05b# ./rc.init
```

Isso montará os sistemas de arquivos Linux usados pelo IDS / IPS e inicializará o sistema. Em seguida, use **vi** para abrir o arquivo *ids_functions*.

```
-sh-2.05b# vi ids_functions
```

Após abrir o arquivo, digite o comando **/845** para que o vi localize a seguinte entrada:

```
elif [[ `isCPU 845` -eq $TRUE && $NUM_OF_PROCS -eq 1 ]]; then  
    MODEL=$IDS4215  
    HTLBLOW=8  
    MEM_PAGES=${HTLBLOW}  
    DEFAULT_MGT_OS="fe0_0"  
    DEFAULT_MGT_CIDS="FastEthernet0/0"
```

Em seguida, edite a instrução **elif** e as instruções **DEFAULT_MGT** para que sejam lidas da seguinte maneira:

```
elif [[ 1 -eq 1 ]]; then  
    MODEL=$IDS4215  
    HTLBLOW=8  
    MEM_PAGES=${HTLBLOW}  
    DEFAULT_MGT_OS="ma0_0"  
    DEFAULT_MGTCIDS="Management0/0"
```

Quando você terminar de editar e tiver certeza de que fez as alterações corretas, salve o arquivo e saia do editor vi. Em seguida, você editará o arquivo interface.conf.

```
-sh-2.05b# cd /usr/cids/idsRoot/etc  
-sh-2.05b# vi interface.conf
```

Use a tecla de seta para ir para a seção que começa com ##### IDS-4215 #####, modifique cada uma das entradas da interface iniciando em **[models/IDS-4215/interfaces/1]** e terminando em **[models/IDS-4215/interfaces/6]**. Cada entrada deve ser exatamente igual às seis entradas a seguir:

```
[models/IDS-4215/interfaces/1]  
name-template=Management0/0  
port-number=0  
pci-path=3.0  
vendor-id=0x8086  
device-id=0x100e  
type=fe  
mgmt-capable=yes  
net-dev-only=yes  
tcp-reset-capable=yes
```

```
[models/IDS-4215/interfaces/2]  
name-template=FastEthernet0/0  
port-number=1  
pci-path=4.0
```

```

vendor-id=0x8086
device-id=0x100e
type=fe
sensing-capable=yes
tcp-reset-capable=yes

[models/IDS-4215/interfaces/3]
name-template=FastEthernet0/1
port-number=2
pci-path=5.0
vendor-id=0x8086
device-id=0x100e
type=fe
sensing-capable=yes
tcp-reset-capable=yes

[models/IDS-4215/interfaces/4]
name-template=FastEthernet0/2
port-number=3
pci-path=6.0
vendor-id=0x8086
device-id=0x100e
type=fe
sensing-capable=yes
tcp-reset-capable=yes

[models/IDS-4215/interfaces/5]
name-template=FastEthernet0/3
port-number=4
pci-path=7.0
vendor-id=0x8086
device-id=0x100e
type=fe
sensing-capable=yes
tcp-reset-capable=yes

[models/IDS-4215/interfaces/6]
name-template=FastEthernet0/4
port-number=5
pci-path=8.0
vendor-id=0x8086
device-id=0x100e
type=fe
sensing-capable=yes
tcp-reset-capable=yes

```

Depois de terminar de editar as interfaces, role pelas entradas e verifique se cada interface está configurada corretamente. Se você tem certeza de que tudo está correto, salve o arquivo e feche o vi. Reinicie a máquina virtual IDS/IPS usando o comando **reboot**.

```
-sh-2.05b# reboot
```

O sistema deve inicializar, configurar algumas coisas e reiniciar novamente automaticamente. Após a reinicialização automática, saia imediatamente do QEMU quando vir o gerenciador de inicialização do GRUB, mostrado na Figura 8-15. Se você não conseguir sair e reiniciar o QEMU sem usar as opções apropriadas, a instalação falhará e será necessário reiniciar. Após sair do QEMU, reinicie sua máquina virtual IDS/IPS com o seguintes opções de comando:

```
$ qemu-system-i386 -name IPS4215 -hda ipsdisk1.img -hdb ipsdisk2.img -m 1024 -smbios type=1,product=IDS-4215  
-net nic,vlan=1,model=e1000 -net nic,vlan=2,model=e1000
```

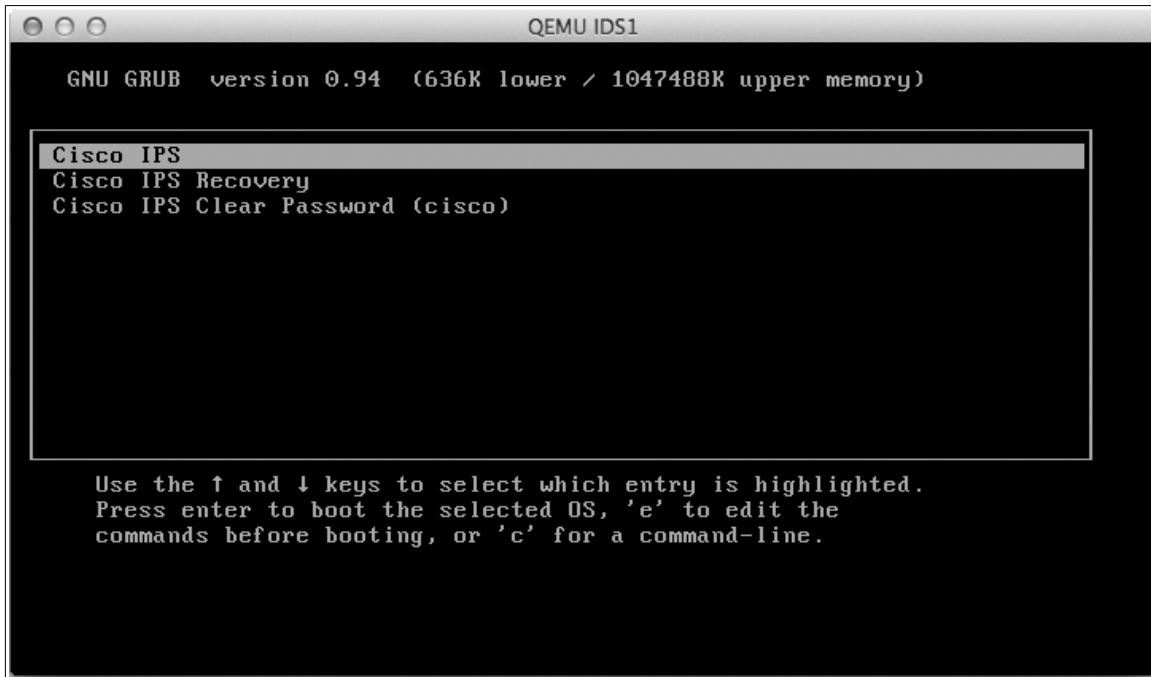


Figure 8-15: GRUB boot manager screen

Seu IDS/IPS agora deve inicializar no prompt de login mostrado na Figura 8-16.

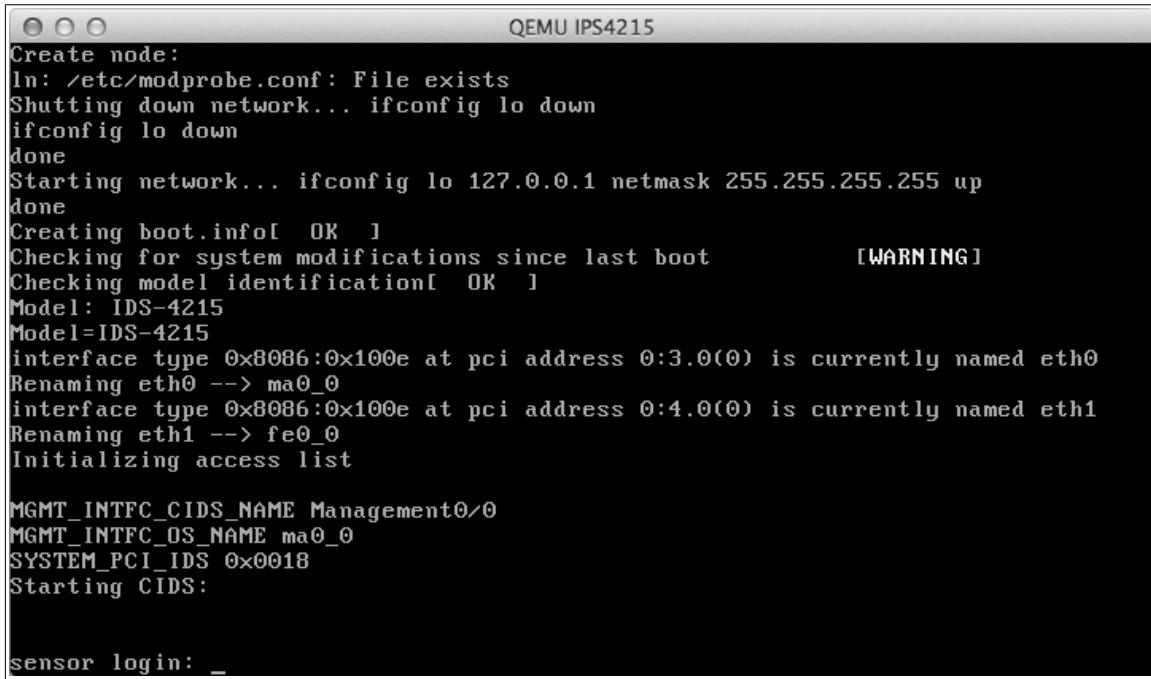


Figure 8-16: IDS/IPS login prompt

Você está quase pronto! Efetue logon no sistema digitando o nome de usuário padrão **cisco** e a senha **cisco**, e você deve ser instruído a redefinir a senha. Se alguma parte da configuração do IDS / IPS estiver incorreta, você poderá ver a mensagem “**UNSUPPORTED HARDWARE DETECTED**”, como na Figura 8-17. Nesse ponto, você pode continuar usando a máquina virtual IDS/IPS ou pode começar de novo. Eu recomendo que você comece novamente e crie um novo IDS/IPS até poder fazer logon sem erros. Se você continuar, o sistema IDS/IPS poderá produzir mais erros e não funcionar conforme o esperado.

```

Starting CIDS:

sensor login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wlc/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

*** ERROR: UNSUPPORTED HARDWARE DETECTED
This Cisco Systems IDS software version is not supported on this
hardware platform. Some capabilities will not be available.
For assistance, contact Cisco Systems Technical Assistance Center.
sensor# _
```

Figure 8-17: “UNSUPPORTED HARDWARE DETECTED” error

Quando você pode fazer logon sem erros, está pronto para continuar.

Testando IDS/IPS(ou paciência é uma virtude)

Na primeira vez que você efetua logon na máquina virtual IDS/IPS, você terá que esperar aproximadamente 20 minutos ou mais enquanto o sistema reconstrói suas tabelas de cache regex. Isso é normal mesmo para um dispositivo IDS / IPS real e você não deve interrompê-lo. Você pode verificar o progresso periodicamente usando o comando `iplog-status`.

```
sensor# iplog-status
```

Se a mensagem de status exibir “*Error: getIpLogList : Analysis Engine is busy rebuilding regex tables. This may take a while.*”, que traduzindo é: “*Error: getIpLogList: O mecanismo de análise está ocupado reconstruindo tabelas regex. Isso pode demorar um pouco.*” O sistema ainda está funcionando e não deve ser interrompido. Após a conclusão da reconstrução, você deverá ver “*No IP logs available*”, que traduzido é “*Nenhum registro IP disponível*”. Quando a reconstrução estiver concluída, digite o comando `reset` para desligar e reinicie a máquina virtual. Infelizmente, não há uma maneira elegante de desligar o sistema. Para evitar corrupção de arquivo, feche o QEMU quando a reinicialização chegar ao menu de inicialização do GRUB.

Configurando o GNS3 para IDS/IPS

Adicionar um IDS/IPS ao GNS3 é semelhante a adicionar um ASA. Para adicionar um dispositivo IDS / IPS, inicie o GNS3, selecione **Edit>Preferences** no Linux e Windows ou **GNS3>Preferences** no OS X e selecione **QEMU VMs** na barra lateral, como mostra a Figura 8-18.

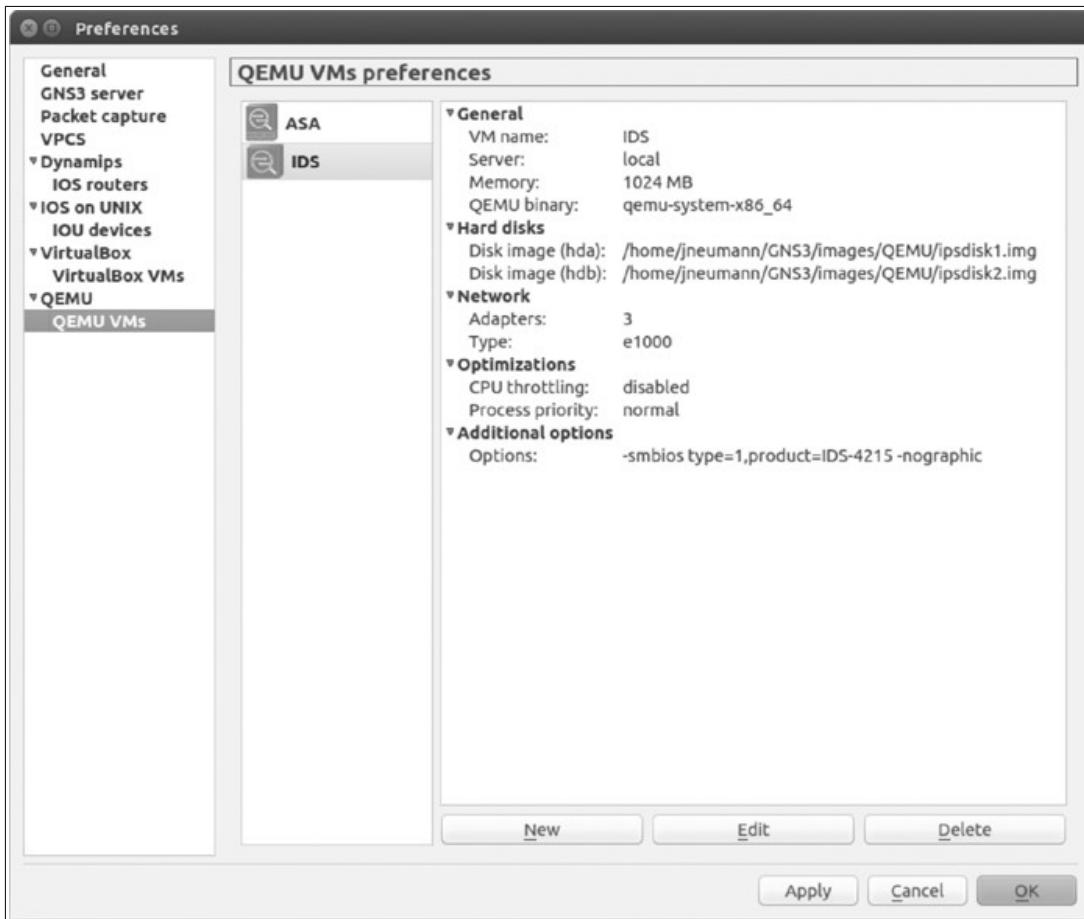


Figure 8-18: IDS Preferences

Para criar um novo IDS / IPS no GNS3, clique em **New** para iniciar o assistente para Nova VM QEMU. Selecione **IDS** no menu suspenso Tipo, como mostra a Figura 8-19.

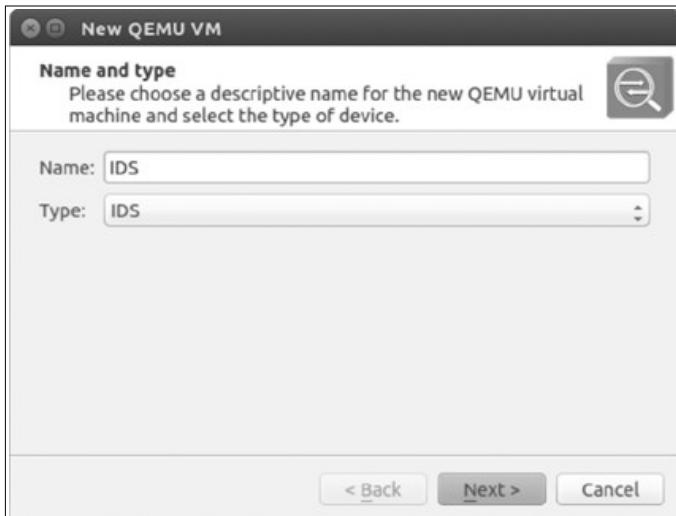


Figure 8-19: Selecting IDS in the New QEMU VM wizard

Por padrão, seu dispositivo é nomeado automaticamente IDS. Clique em **Next** para continuar. O GNS3 deve localizar e escolher automaticamente o arquivo binário QEMU correto para o seu PC, mostrado na Figura 8-20.

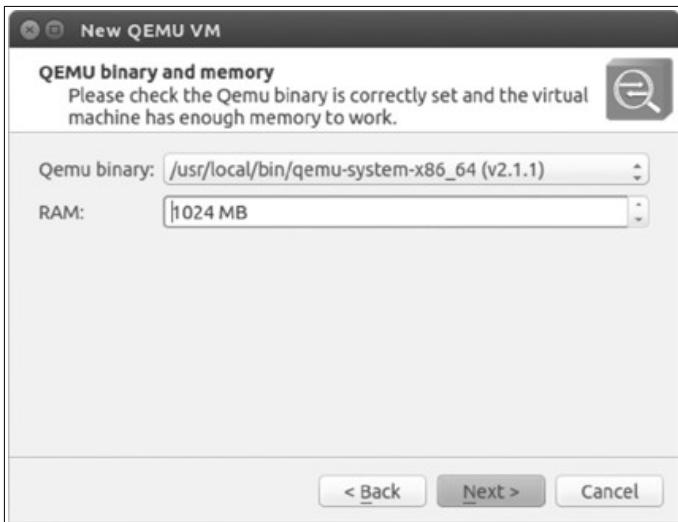


Figure 8-20: QEMU binary and memory screen

Defina o campo RAM para **1024 MB** ou mais, e clique em **Next** para continuar com a seleção Disk image (hda), mostrada na Figura 8-21.

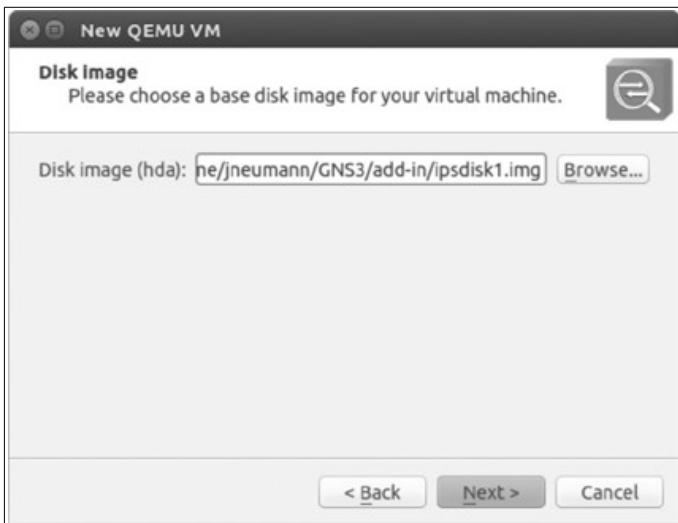


Figure 8-21: Chooseing a disk image

Procure e selecione o arquivo chamado *ipsdisk1.img* que foi criado quando você construiu seu sistema IDS pronto para QEMU. Clique em Avançar para continuar na tela de seleção Diskimage (hdb) e escolha *ipsdisk2.img*. Clique em **Finish** para concluir a instalação. Agora você está pronto para testar seu IDS.

Verificando IDS/IPS no GNS3

Para verificar se seu IDS / IPS está funcionando, arraste um nó IDS/IPS para sua área de trabalho e inicie o dispositivo. O GNS3 não pode abrir uma conexão de console com um dispositivo IDS/IPS até que seja totalmente inicializado. Isso significa que você não verá nenhuma mensagem IDS/IPS antes do prompt de login. Depois que o prompt de login aparecer, você poderá fazer login e configurar o IDS/IPS. Para impedir a corrupção do arquivo, use o comando *reset* sempre que desligar o dispositivo.

Depois de determinar que seu IDS / IPS está em boas condições de funcionamento, você deve fazer uma cópia de backup dos arquivos de imagem de disco QEMU. Se algo acontecer com o seu dispositivo IDS / IPS, uma cópia de backup dos arquivos poderá economizar horas de trabalho posteriormente.

Cisco IOS-XRv

A Cisco oferece uma versão do IOS-XR na forma de uma máquina virtual de 32 bits chamada IOS-XRv. O legal do IOS-XRv é que não é um emulador como IOU ou NX-OSv. Em vez disso, é uma versão "restrita" do IOS-XR que contém apenas um único processador de rota (RP). A taxa de transferência de rede é limitada a 2 Mbps, e há um usuário AAA codificado chamado cisco com a senha cisco, tornando impossível o uso em um ambiente de produção, a

menos que você queira uma rede lenta e insegura. Apesar dessas limitações, o sistema operacional inclui recursos de gerenciamento, roteamento e recursos de encaminhamento. O software foi projetado para ser executado usando o VMware ESXi ou QEMU, facilitando o uso com o GNS3. Se você possui uma conta Cisco CCO, poderá fazer o download do software na troca de arquivos da Cisco.

Configurando o GNS3 para IOS-XRv

Os arquivos Cisco IOS-XRv vêm em dois formatos de imagem; o primeiro é um OVA e o segundo é um arquivo do Virtual Machine Disk (VMDK). A imagem OVA (finalizada em *.ova*) é adequada para uso com o VMware ESXi; o arquivo VMDK (que termina em *.vmdk*) está pronto para ser usado com o QEMU e é o arquivo que você usará no GNS3. Neste exemplo, usarei um arquivo de imagem chamado *iosxrv-k9-demo-5.2.2.vmdk*. Adicionar um dispositivo IOS-XRv ao GNS3 é bastante direto. Você iniciará o assistente para Nova VM QEMU VM e seguirá as instruções; você editará o dispositivo, fazendo uma pequena alteração para aumentar o número de adaptadores. Para adicionar um dispositivo IOS-XRv, selecione **Edit>Preferences** no Linux e Windows ou **GNS3>Preferences** no OS X e selecione **QEMU VMs** no painel à esquerda. Clique em **New** para iniciar a configuração e abrir a caixa de diálogo na Figura 8-22.



Figure 8-22: New QEMU VM wizard

Defina Tipo como **Default** e insira um nome para o seu dispositivo; Entrei no **IOS-XRv**. Quando terminar, clique em **Next** para prosseguir com as configurações binárias e de memória do QEMU, mostradas na Figura 8-23.

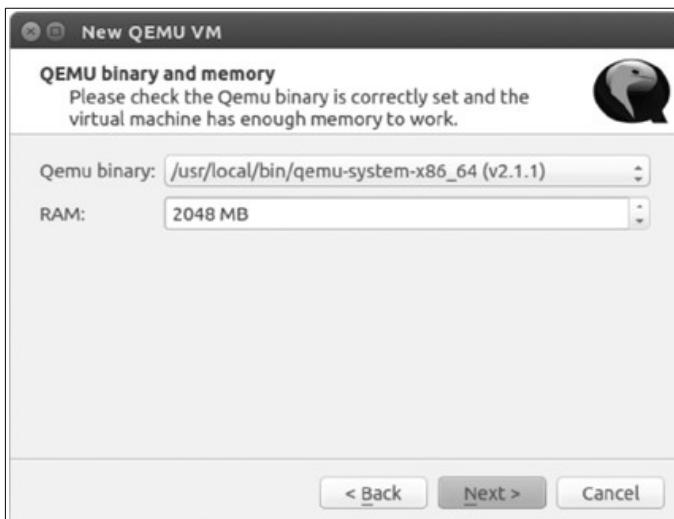


Figure 8-23: Configuring IOS-XRv for 64-bit systems

O IOS-XRv pode ser executado usando emulação de hardware QEMU de 32 ou 64 bits. Como estou executando um sistema operacional de 64 bits no meu PC, escolhi usar um binário QEMU de 64 bits, chamado *qemu-system-x86_64* (mostrado na Figura 8-23), e configurei a RAM como **2048 MB**, que é a quantidade recomendada. No entanto, se você executar um sistema operacional de 32 bits, como o Windows, precisará definir a RAM para menos de 2048 MB. Isso ocorre porque o programa QEMU de 32 bits não pode alocar tanta memória para a máquina virtual

IOS-XRv. Nesse caso, você deve inserir **1920 MB** e usar o menu suspenso para escolher o binário QEMU chamado *qemu-system-i386w.exe*, conforme mostrado na Figura 8-24.

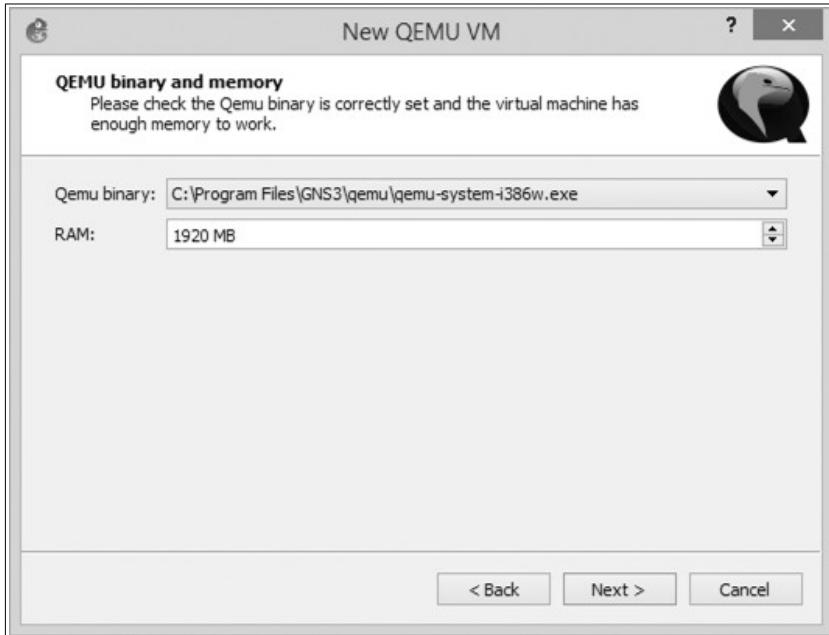


Figure 8-24: Configuring IOS-XRv for 32-bit Windows systems

Depois de configurar seu binário e RAM QEMU, clique em **Next** para prosseguir para a tela de seleção de imagem de disco na Figura 8-25.



Figure 8-25: Selecting a disk image

Clique no botão **Browse** para localizar e escolher seu arquivo de imagem IOS-XRv .vmdk. Eu selecionei uma imagem de disco chamada *iosxrv-k9-emo-5.2.2.vmdk*. Quando terminar de selecionar sua imagem, clique em **Finish** para fechar o assistente. Em seguida, selecione o seu dispositivo IOS-XRv recém-criado e clique em **Edit**. Selecione na guia **Network** e aumente o número de adaptadores para 4. Clique em **OK** para fechar a janela e clique em **Apply** e **OK** para confirmar a alteração. Você pode definir o número de adaptadores para o que melhor se adapte às suas necessidades, mas quatro devem ser adequados para a maioria dos projetos GNS3.

Criando um projeto IOS-XR simples

O Cisco IOS-XR é muito semelhante ao IOS, mas não é IOS. Nesta seção, você configurará um projeto simples usando um roteador Dynamips e um dispositivo IOS-XRv, mostrado na Figura 8-26.

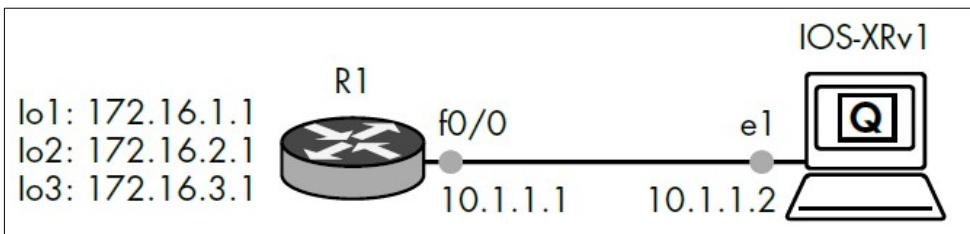


Figure 8-26: A simple IOS-XRv project

Você usará o EIGRP para anunciar três redes do roteador R1 para o Dispositivo IOS-XRv1. Por fim, você verificará as rotas usando alguns comandos do IOS-XR. Esta é apenas uma introdução básica ao IOS-XR. Se você realmente deseja aprender o IOS-XR, precisará aprofundar-se na documentação da Cisco.

Configurando o roteador

Comece configurando o roteador R1. Configure um endereço IP na interface Ethernet vinculada ao IOS-XRv1.

```
R1# configure terminal
R1(config)# interface f0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# no shutdown
```

Em seguida, configure os três endereços IP nas interfaces de loopback do roteador R1.

```
R1(config-if)# interface loopback1
R1(config-if)# ip address 172.16.1.1 255.255.255.0
R1(config-if)# interface loopback2
R1(config-if)# ip address 172.16.2.1 255.255.255.0
R1(config-if)# interface loopback3
R1(config-if)# ip address 172.16.3.1 255.255.255.0
R1(config-if)# exit
```

Esses endereços serão anunciados no seu dispositivo IOS-XRv1 usando o EIGRP. Por fim, configure o EIGRP e anuncie todas as redes.

```
R1(config)# router eigrp 10
R1(config-router)# no auto-summary
R1(config-router)# network 10.0.0.0
R1(config-router)# network 172.16.0.0
```

Depois de concluir a configuração do roteador R1, configure o dispositivo IOS-XR.

Configurando o dispositivo IOS-XR

Faça logon no IOS-XRv1 e crie uma configuração semelhante à que você criou no roteador R1. Você configurará um endereço IP e permitirá que o EIGRP permita que o IOS-XRv1 e o roteador R1 troquem informações de roteamento.

```
① RP/0/0/CPU0:ios#
RP/0/0/CPU0:ios# configure terminal
RP/0/0/CPU0:ios(config)# interface GigabitEthernet 0/0/0/0
② RP/0/0/CPU0:ios(config-if)# ipv4 address 10.1.1.2/24
RP/0/0/CPU0:ios(config-if)# no shutdown
RP/0/0/CPU0:ios(config)# router eigrp 10
```

```
③ RP/0/0/CPU0:ios(config-eigrp)# address-family ipv4  
④ RP/0/0/CPU0:ios(config-eigrp-af)# interface GigabitEthernet 0/0/0/0  
⑤ RP/0/0/CPU0:ios(config-eigrp-af)# commit
```

A primeira diferença notável entre IOS e IOS-RX é o prompt de comando. O prompt de comando do IOS-XRv1 ① indica que seu contexto é o primeiro processador de rota (RP/0/0/CPU0). Como esta é uma versão demo do IOS-XRv, é limitada a este processador de rota único.

Em seguida, quando um endereço IP estiver configurado em uma interface Ethernet, você precisa especificar a família do endereço IP que você está usando (IPv4 ou IPv6) e a máscara de sub-rede é representada na notação CIDR (/24) ②. Da mesma forma, você deve especificar IPv4 ou IPv6 ao configurar o processo de rota EIGRP ③. Por fim, você anuncia redes colocando uma interface configurada por IP no processo de rota EIGRP ④. Quando você acabar, certifique-se de confirmar suas alterações ⑤. Depois de configurar tudo, entre com o comando *show eigrp neighbours*, e você verá esta saída:

```
RP/0/0/CPU0:ios# show eigrp neighbours  
IPv4-EIGRP Neighbors for AS(10) VRF default  


| H | Address   | Interface  | Hold (sec) | Uptime (sec) | SRTT (ms) | RT0 (ms) | Q Cnt | Seq Num |
|---|-----------|------------|------------|--------------|-----------|----------|-------|---------|
| 0 | ①10.1.1.1 | ②Gi0/0/0/0 | 13         | 00:28:09     | 19        | 200      | 0     | 3       |


```

Em uma configuração correta, uma adjacência de vizinho EIGRP será formada com roteador R1 no endereço IP 10.1.1.1 ① da interface Gi0 / 0/0/0 ②. Agora, verifique se todas as redes 172.16.0.0 foram anunciadas do roteador R1 para o IOS-XRv1 usando o comando *show route*.

```
RP/0/0/CPU0:ios# show route  
--snip--  
C 10.1.1.0/24 is directly connected, 02:58:51, GigabitEthernet0/0/0/0  
L 10.1.1.2/32 is directly connected, 02:58:51, GigabitEthernet0/0/0/0  
D ①172.16.1.0/24 [90/2570240] via 10.1.1.1, 00:43:21, GigabitEthernet0/0/0/0  
D ①172.16.2.0/24 [90/2570240] via 10.1.1.1, 00:43:21, GigabitEthernet0/0/0/0  
D ①172.16.3.0/24 [90/2570240] via 10.1.1.1, 00:43:21, GigabitEthernet0/0/0/0
```

Todas as redes 172.16.0.0 foram adicionadas com sucesso à tabela de roteamento IOS-XR ①. Você pode testar a conectividade executando ping em um dos endereços.

```
RP/0/0/CPU0:ios# ping 172.16.1.1  
Thu Oct 16 03:20:27.508 UTC  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:  
!!!!!  
① Success rate is 100 percent (5/5), round-trip min/avg/max = 9/19/49 ms
```

Aqui, o ping teve 100% de sucesso ①. Agora, salve a configuração.

```
RP/0/0/CPU0:ios# copy running-config nvram:  
Thu Oct 16 03:22:39.679 UTC  
Destination file name (control-c to abort): [/running-config]? <enter>  
Building configuration.  
24 lines built in 1 second  
[OK]
```

A essa altura, deve estar óbvio que o IOS-XR é um pouco diferente do IOS tradicional, mas também é semelhante. O IOS-XRv é uma plataforma confiável, e é muito divertido brincar com o GNS3. Talvez um dia a Cisco

portará uma versão do IOS-XR de seus roteadores de classe de operadora para seus roteadores comerciais menores. Nesse caso, praticar com o IOS-XR no GNS3 ajudará a prepará-lo para isso.

Pensamentos finais

Usando o GNS3, você pode rapidamente se tornar proficiente na configuração e instalação de firewalls ASA. Tendo trabalhado com equipamentos da Cisco por mais de uma década, aprendi que os ASAs são sólidos e funcionam muito bem para pequenas instalações de rede. Compreender como configurar o ASA é uma obrigação para qualquer pessoa envolvida em redes de pequenas empresas. Eles são um dos poucos produtos Cisco não corporativos com preços razoáveis, recursos avançados e fáceis de instalar.

Usando o ASDM, você pode configurar rapidamente um ASA para permitir usuários remotos para se conectarem às suas redes corporativas por meio de uma VPN IPSec. Vários clientes VPN de plataforma cruzada são compatíveis com o Cisco ASAs e roteadores; O OS X possui um cliente Cisco VPN integrado. No Windows, você deve instalar o software Cisco VPN Client ou Cisco AnyConnect. No Linux, você pode usar a Conexão de rede virtual privada (VPNC), o que funciona muito bem. Uso o VPNC diariamente com o Linux para acessar VPNs em todo o país. No próximo capítulo, você examinará o Cisco IOU e aprenderá como integrar dispositivos IOU em projetos GNS3. É um novo avanço empolgante que amplia o futuro do GNS3.

9 CISCO IOS ON UNIX E NX-Osv

Neste capítulo, discutirei estratégias para instalar e integrar dispositivos Cisco IOU com o GNS3. Você também aprenderá como instalar e executar o sistema operacional de switch de última geração da Cisco (NX-OS) usando o VirtualBox e o NX-Osv.

IOU da Cisco

Cisco IOU é uma das coisas mais legais que aconteceu com a comunidade educacional da Cisco há muito tempo. O IOU funciona de maneira semelhante ao Dynamips, mas usa muito menos recursos. Como o Dynamips, o IOU permite adicionar roteadores e switches aos seus projetos GNS3. Ao contrário do Dynamips, as imagens IOU simulam os recursos de um trem da tecnologia IOS em vez do componente de hardware de um modelo específico da Cisco. Cada arquivo de imagem IOU é um aplicativo binário independente que executa uma instância de um dispositivo. Existem imagens projetadas para roteamento, comutação, voz sobre IP (VoIP) e Pagent (para gerar tráfego IP). A IOU não requer que um hipervisor emule o hardware da Cisco, geralmente tornando os dispositivos IOU com menos memória e muita CPU do que os dispositivos Dynamips. A vantagem óbvia aqui é que você pode criar topologias maiores em um PC configurado modestamente. Em 2010, a Cisco integrou a IOU na Cisco Learning Network para forneça laboratórios virtuais on-line para os alunos do CCNA e do CCNP. Os laboratórios são baratos e bem desenhados. Se você está interessado no Cisco Learning Labs, consulte o Cisco Learning Center (<http://learningnetwork.cisco.com/>). Como o nome indica, o IOS no Unix é executado apenas em sistemas baseados em Unix. Às vezes referido como IOS no Linux (IOL), foi desenvolvido no Solaris Unix e Linux.

O que significa IOU para GNS3

Depois que a Cisco anunciou que estava se afastando do hardware padrão do setor em favor do hardware ISR (Integrated Service Router), a comunidade GNS3 se perguntou se o fim do Dynamips e do GNS3 havia chegado. Sem acesso às especificações técnicas para o novo hardware proprietário, seria impossível criar um novo hipervisor necessário para executar o software IOS mais recente. Eventualmente, os dispositivos antigos da Dynamips parariam de receber atualizações do IOS e se tornariam obsoletos. Na verdade, a Cisco mantém o IOS atualizado para os roteadores da série 7200 que o GNS3 usa, mas todos os outros roteadores GNS3 ficam congelados na versão de IOS 12.4 (15) T, que impõe limites ao aprendizado de tecnologias modernas, como VoIP. É por isso que IOU é emocionante. Ele dá vida nova ao GNS3, permitindo que você integre tecnologias IOS atualizadas nos seus projetos GNS3 - e isso é muito legal!

Switching, Switching, e mais Switching!

Um dos melhores motivos para integrar a IOU ao GNS3 é que você pode usar muitos dos recursos avançados de comutação da Cisco, que estão ausentes no módulo NM-16ESW no Dynamips (consulte o Apêndice C). Esses recursos permitem que o GNS3 melhore seu jogo e se torne uma ferramenta de treinamento abrangente para certificações mais avançadas como o CCIE.

Com o IOU, você não precisa mais comprar Switches físicos e criar um breakout switch ou usar pequenos truques engraçados como a bridging ISL para acessar Switches reais. Usando um roteador GNS3 EtherSwitch, agora é possível criar um link de tronco 802.1Q regular dos Switches Dynamips para um bloco de Switches IOU em execução no seu PC. Os switches IOU são estáveis, executam rápido e, ao contrário dos switches físicos, são completamente portáteis, o que significa que eles podem viajar com você em um laptop como parte de seus projetos GNS3.

Imagens do IOU

As imagens IOU são projetadas com base nos recursos do IOS, e seus nomes de arquivos geralmente revelam quais recursos eles incluem, assim como os nomes de arquivos de imagem do IOS. Por exemplo, vamos detalhar o nome do arquivo de um switch IOU chamado *I86BI_LINUXL2-UPK9-M-15.0*.

I86BI Indica que esta é uma imagem binária de 32 bits da Intel.

LINUX Indica que é executado no Linux.

L2 Indica que é um Switch L2/L3.

UPK9 Indica que a imagem contém recursos criptográficos avançados como 3DES/AES.

M Indica que é um IOS da linha principal.

15.0 Especifica a versão do IOS em que a imagem se baseia.

Usando essas informações, você poderá examinar praticamente qualquer nome do arquivo IOU para determinar rapidamente quais recursos ele inclui.

O que você deve saber antes de instalar o IOU

Por padrão, uma instalação padrão do GNS3 não permite executar dispositivos IOU. Os dispositivos IOU são arquivos binários do Linux, portanto, eles podem ser executados usando apenas um sistema operacional Linux. Normalmente, as imagens são arquivos binários de 32 bits, mas com os arquivos de biblioteca adequados, você pode executá-los facilmente nos sistemas Linux de 64 bits. Se você estiver executando o GNS3 no Windows ou no OS X, precisará instalar um programa de virtualização como o VirtualBox e executar seus dispositivos IOU usando uma máquina virtual Linux. Felizmente, o GNS3 fornece uma máquina virtual IOU que você pode baixar no site do GNS3. A máquina virtual GNS3 IOU está pronta para executar imagens IOU, fornece uma maneira fácil de carregar suas imagens e não exige que você saiba como usar os comandos do Linux.

A vantagem de executar o GNS3 no Linux é que instalar e configurar O IOU é mais direto e tudo deve funcionar perfeitamente sem configuração extra. A desvantagem é que você precisa saber um pouco sobre o Linux, mas, na minha opinião, esse é um pequeno preço a pagar. Quando você executa o GNS3 no Windows ou no OS X, é necessário configurá-lo para se comunicar com a máquina virtual do Linux por TCP / IP, o que pode ser complicado de gerenciar. Se os endereços IP da sua estação de trabalho ou da máquina virtual de IOU mudarem (o que geralmente acontece), você precisará reconfigurar o GNS3 para usar os novos endereços IP. Além disso, ao atualizar o GNS3, é necessário atualizar o software do servidor GNS3 que é executado na máquina virtual IOU. Os números da versão devem ser idênticos ou o IOU não será executado. Essas etapas são desnecessárias quando você executa o GNS3 e o IOU no Linux.

Configurando o IOU em um PC Linux

Existem algumas vantagens distintas na execução do GNS3 e IOU em um PC Linux. A maior delas é que você não precisa usar uma máquina virtual de IOU, porque no Linux os arquivos de imagem de IOU são executados nativamente. Isso significa que você não precisa abrir mão de recursos preciosos, como ciclos de CPU e memória, que seriam utilizados pela máquina virtual IOU. Outra vantagem é que você pode usar o Wireshark para capturar e monitorar pacotes entre dois dispositivos IOU, o que não é possível ao usar a máquina virtual IOU. Isso ocorre porque o arquivo de captura .pcap, criado quando você inicia uma captura do Wireshark, é salvo na máquina virtual IOU e não localmente; portanto, o Wireshark não pode acessar o arquivo. Se você estiver executando o GNS3 no Linux, siga as instruções nesta seção para obter o IOU em funcionamento. Caso contrário, pule para a seção “Usando a máquina virtual GNS3 IOU no Windows e no OS X” na página 160.

Instalando IOU

Quando você executa uma imagem IOU, a imagem procura o arquivo *libcrypto.so.4* e não será executada sem ele. Embora um arquivo da biblioteca *libcrypto* já possa estar instalado no seu sistema, você deve instalar a *libssl1.0.0* porque esta versão está provado ser estável com imagens IOU. Em seguida, crie um link simbólico (link simbólico) de *libcrypto.so.1.0.0* para *libcrypto.so.4*; um link simbólico é o equivalente do Linux a um atalho do Windows. Se você estiver usando uma versão de 32 bits do Ubuntu, instale a *libcrypto* usando os seguintes comandos:

```
$ sudo apt-get install libssl1.0.0
$ sudo ln -s /lib/i386-linux-gnu/libcrypto.so.1.0.0 /lib/libcrypto.so.4
```

Ao executar um sistema Ubuntu de 64 bits, você precisará instalar o pacote *libssl* de 32 bits antes que você possa configurar o *libcrypto* e executar um Imagem IOU de 32 bits. Se você possui um sistema Ubuntu de 32 bits, pode desconsiderar os próximos comandos.

```
$ sudo apt-get install libssl1.0.0:i386
$ sudo ln -s /lib/i386-linux-gnu/libcrypto.so.1.0.0 /lib/i386-linux-gnu/libcrypto.so.4
```

Se você não está executando o Ubuntu, pode ser necessário fazer uma pequena pesquisa para configurar a *libcrypto* no seu sistema, porque nem todos os sistemas Linux usam os mesmos arquivos e versões de biblioteca ou armazenam os arquivos nos mesmos diretórios do Ubuntu. A chave é que o arquivo *libcrypto* deve ser vinculado a *libcrypto.so.4*. Depois de configurar o *libcrypto.so.4*, copie um ou mais arquivos de imagem IOU para o seu sistema Ubuntu. Você precisa tornar os arquivos IOU executáveis antes que eles sejam executados; aqui está como:

```
$ sudo chmod 555 I86BI_LINUXL2-UPK9-M-15.0.bin
```

Em seguida, instale as dependências para o aplicativo GNS3 *iouyap*. Este programa é responsável por configurar a comunicação entre IOU e outros dispositivos GNS3, como roteadores Dynamips. Comece instalando o *bison* e o *flex*, dois pacotes necessários antes da compilação do *iouyap*.

```
$ sudo apt-get install bison
$ sudo apt-get install flex
```

Agora, instale e compile o programa *iniparser* usando os seguintes comandos:

```
$ sudo apt-get install git
$ git clone http://github.com/ndevilla/iniparser.git
$ cd iniparser
$ make
$ sudo cp libiniparser.* /usr/lib/
$ sudo cp src/iniparser.h /usr/local/include
$ sudo cp src/dictionary.h /usr/local/include
```

Um arquivo ZIP contendo *iouyap* deveria ter sido incluído no seu GNS3 para download do Linux. Descompacte *iouyap-<x>.zip*, substituindo <x> pela versão que você possui e compile o programa usando os seguintes comandos:

```
$ cd iouyap-x
$ sudo make
$ sudo make install
```

Se necessário, copie o aplicativo compilado para o diretório /usr/local/bin.

```
$ sudo copy iouyap /usr/local/bin
```

Agora que todos os aplicativos estão instalados, você precisa fazer algumas configurações.

Criando um arquivo de licença

Antes de executar o IOU, você deve criar um arquivo de licença que contenha o nome do host do seu PC e uma chave de licença válida. A chave de licença é gerada a partir do seu nome de host do Linux, portanto, verifique se você está satisfeito com o nome de host do seu PC. Se você alterar seu nome de host, precisará inserir uma nova chave de licença. Depois de obter uma chave de licença, use um editor de texto para criar o arquivo de licença. Normalmente nomeio meu arquivo como *.iourc*, mas qualquer nome serve. A seguir, é apresentado um exemplo de um arquivo de licença para um PC chamado Ubuntu, usando a chave de licença 1234567812345678. O nome do host faz distinção entre maiúsculas e minúsculas, portanto, tenha cuidado ao inseri-lo no arquivo de licença.

```
[license]
Ubuntu = 1234567812345678
```

Se você não tiver certeza do nome do seu host Linux, poderá usar o comando hostname do seu terminal para exibir o nome.

Configurando o GNS3

Em seguida, defina o caminho para o aplicativo iouyap e seu arquivo de licença IOU nas preferências do IOS on UNIX. O aplicativo iouyap é usado para conectar o Dynamips e outros dispositivos GNS3 com dispositivos IOU, para que todos os seus dispositivos possam ser conectados em rede sem problemas. Selecione **Edit>Preferences** e, em seguida, selecione **IOS on UNIX** no menu esquerdo, como mostra a Figura 9-1.



Figure 9-1: IOS on UNIX preferences, General settings tab

Na guia Configurações gerais, defina o caminho e o nome do seu arquivo de licença no caminho para IOURC. Refere-se ao arquivo de licença IOU que você criou anteriormente. Além disso, defina o caminho do arquivo para o seu arquivo iouyap em Caminho para iouyap, geralmente `/usr/local/bin/iouyap`. Em seguida, vá para a guia Configurações do servidor, mostrada na Figura 9-2.

Marque a caixa de seleção **Always use the local server (Linux only)** (**Sempre usar o servidor local (somente Linux)**) para que O IOU usa o PC local para integração GNS3 e IOU. Em seguida, vá para a guia Configurações avançadas, mostrada na Figura 9-3.

Cada dispositivo IOU recebe um número de porta de console exclusivo dentro do intervalo definido. Não altere esses valores, a menos que o intervalo entre em conflito com outros aplicativos baseados em IP em execução no seu PC; o mesmo vale para o intervalo de portas de encapsulamento UDP. As portas UDP são usadas para configurar a comunicação de rede entre IOU e outros dispositivos GNS3.



Figure 9-2: IOS on UNIX preferences, Server settings tab



Figure 9-3: IOS on UNIX preferences, Advanced settings tab

Por fim, expanda **IOS on UNIX** no menu esquerdo da janela Preferences para exibir a seção IOU devices, mostrada na Figura 9-4. A partir daqui, você pode adicionar um ou mais arquivos de imagem IOU ao GNS3.

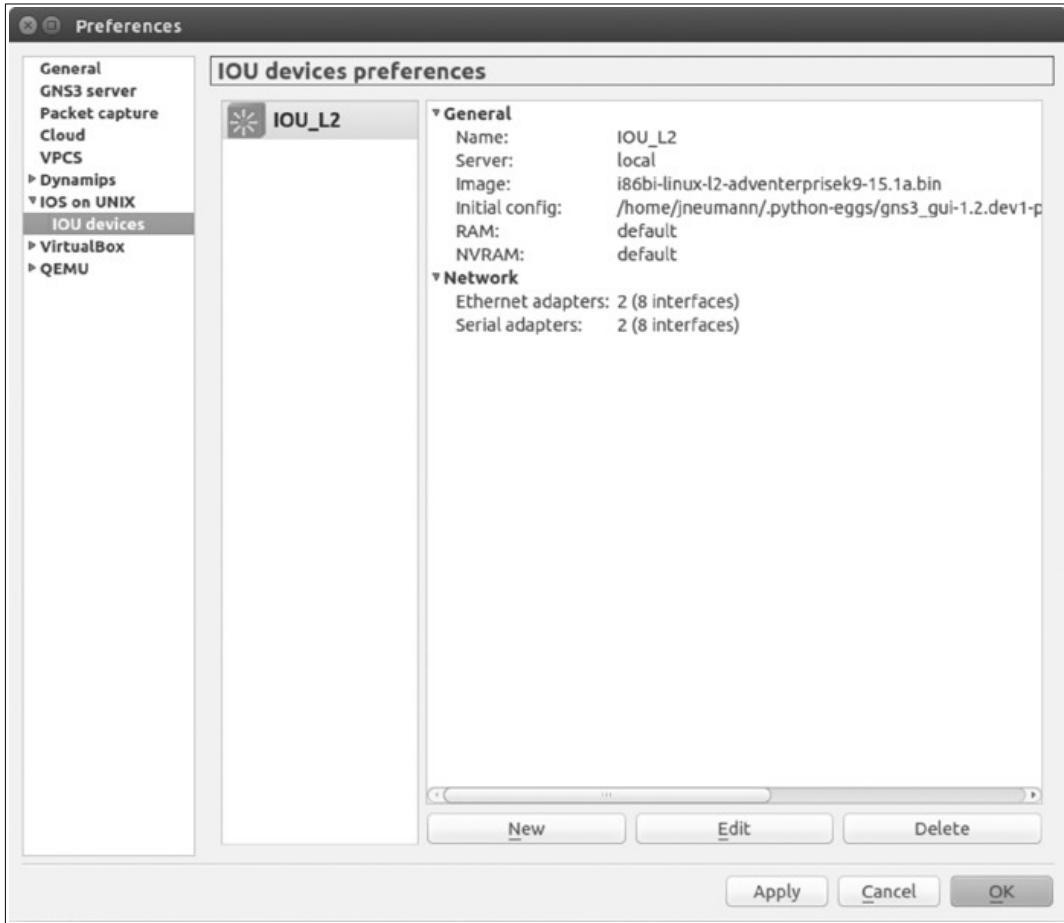


Figure 9-4: Adding IOU images to GNS3

Para adicionar um arquivo de imagem IOU ao GNS3, clique no botão **New** para iniciar o Assistente de novo dispositivo IOU, mostrado na Figura 9-5.



Figure 9-5: New IOU device wizard

Digite um nome para o seu novo dispositivo (IOU_L2 neste exemplo); depois clique no botão **Browse** para localizar e selecionar seu arquivo de imagem IOU. Quando terminar, clique em **Finish** para concluir o assistente. Uma vez adicionado, seu arquivo de imagem IOU deve ser copiado para o diretório de usuário do GNS3 em **/GNS3/images/IOU**. Para configurar um dispositivo IOU, arraste um ícone de dispositivo IOU da barra de ferramentas de dispositivos para o seu espaço de trabalho. Clique com o botão direito do mouse no dispositivo e escolha **Configure** para abrir o configurador do Node (mostrado na Figura 9-6).

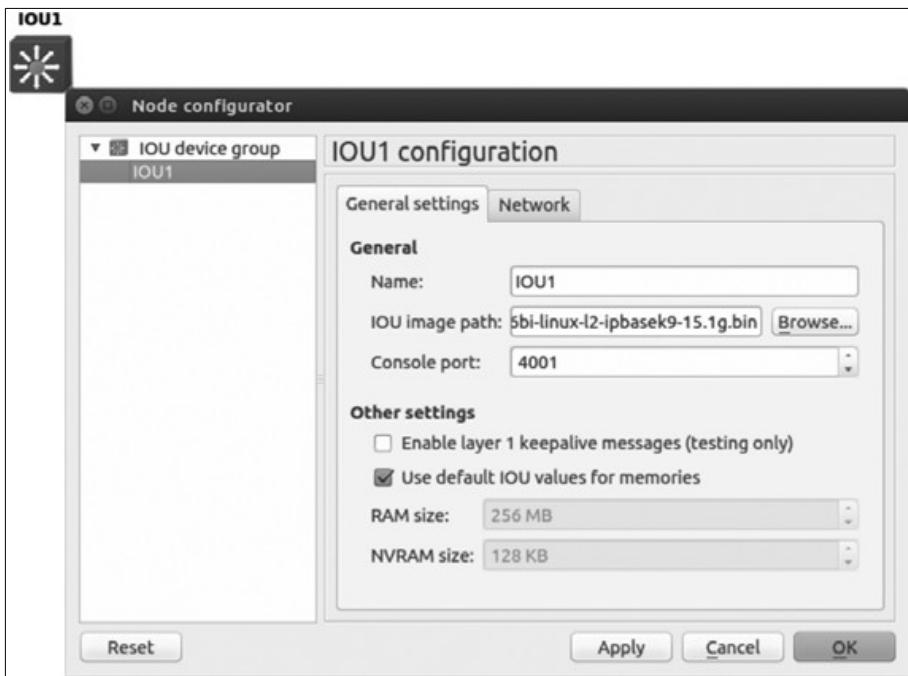


Figure 9-6: IOU Node configurator

As opções na guia Configurações gerais permitem renomear seu dispositivo e alterar o arquivo de imagem IOU, o número da porta do console e os valores padrão de RAM e NVRAM. Você pode alterar o número de adaptadores Ethernet e serial instalados, ajustando os valores na guia Rede. O padrão é dois de cada adaptador, mas eles fornecem quatro interfaces cada, oferecendo um total de oito interfaces Ethernet e oito interfaces seriais. Isso deve ser suficiente para a maioria dos projetos, mas você pode ajustar facilmente a quantidade para atender às suas necessidades. O número total combinado de adaptadores (Ethernet e serial) não pode exceder 16, para um total de 64 interfaces por dispositivo IOU. Um dispositivo IOU pode ser vinculado a qualquer outro dispositivo GNS3, assim como você faria com um roteador ou comutador Dynamips padrão. Você pode até vinculá-los a dispositivos, o que significa que os links podem ser formados entre os dispositivos depois que eles são iniciados.

Para exportar uma configuração de IOU, digite **copy running-config unix: initial -config.cfg** no console IOU e clique com o botão direito do mouse no dispositivo IOU no seu espaço de trabalho e selecione **Export config**. Você será solicitado a fornecer um nome de arquivo e um local onde o arquivo será salvo. Você pode importar uma configuração selecionando **Import config**. Se você deseja executar o IOU no Windows ou no OS X, leia a próxima seção. Caso contrário, você pode pular para “NX-OSv” na página 168.

Como mencionei em “Coisas para saber antes de instalar o IOU” na página 153, Os sistemas Windows e OS X podem executar IOU apenas usando uma máquina virtual Linux. Se você ainda não o fez, faça o download e instale o VirtualBox (<https://www.virtualbox.org/>). A aceitação das configurações de instalação padrão deve fornecer tudo o que você precisa para executar uma máquina virtual IOU. Depois de instalar o VirtualBox, visite o site do GNS3 (<http://www.gns3.com/>) e baixe o arquivo OVA chamado *GNS3 IOU VM.ova*. Esta é uma máquina virtual Linux que foi pré-configurada com todas as ferramentas necessárias para executar a IOU, mas não inclui nenhum arquivo de imagem da IOU. Em vez disso, ele fornece um utilitário baseado na Web que permite carregar facilmente seus arquivos de imagem no dispositivo, mas você precisará importá-lo para o VirtualBox antes de poder usá-lo.

Importando a máquina virtual GNS3 IOU para o VirtualBox Comece iniciando o aplicativo VirtualBox. Após o carregamento do aplicativo, selecione **File>Import Appliance**. Você deve receber a caixa de diálogo Importar dispositivo virtual, mostrada na Figura 9-7.

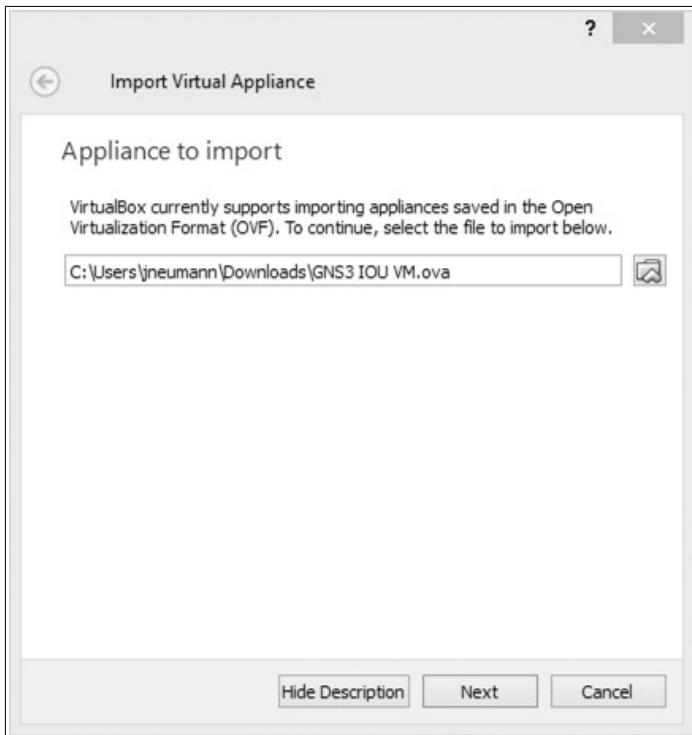


Figure 9-7: Select the virtual appliance.

Use o ícone de navegação para localizar e selecionar o arquivo *GNS3 IOU VM.ova*. Na Figura 9-7, minha máquina virtual está localizada no meu diretório *Downloads*, *C:\Users\jneumann\Downloads*. Depois de selecionar o arquivo, clique em **Next** e verifique as configurações do dispositivo. Eles devem se parecer com a Figura 9-8.

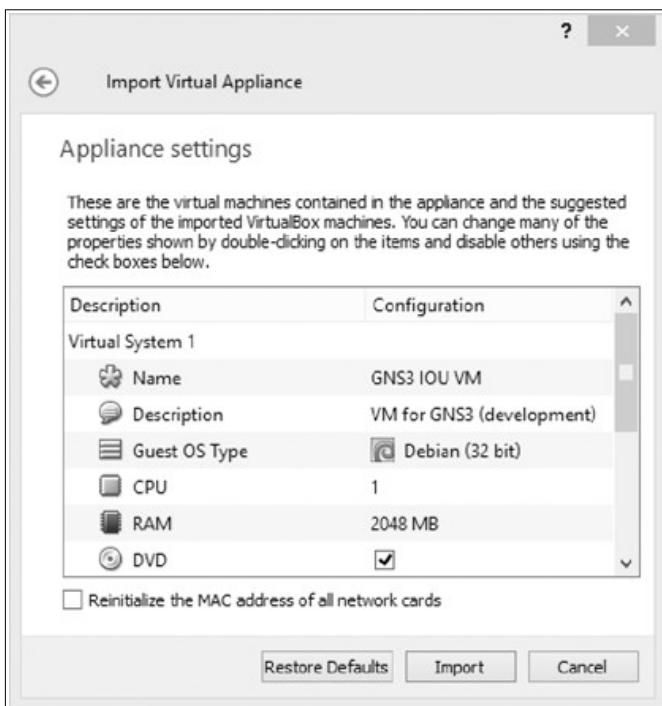


Figure 9-8: Virtual Appliance settings

Você deve poder aceitar as configurações sugeridas do dispositivo. Observe que a configuração padrão da RAM é 2048MB. Descobri que a RAM pode ser reduzida para 1024 MB se você estiver usando apenas alguns dispositivos de IOU em seus projetos. Isso reduz a quantidade total de memória usada no seu PC e pode ajudar o GNS3 a ter um desempenho melhor se você estiver sem recursos. Se não tiver certeza, aceite os padrões e clique em **Import** para concluir a importação. Você sempre pode modificar as configurações posteriormente. Após importar a máquina virtual, clique em **Settings** e, em seguida, clique em **Network** para acessar o painel Rede, mostrado na Figura 9-9.

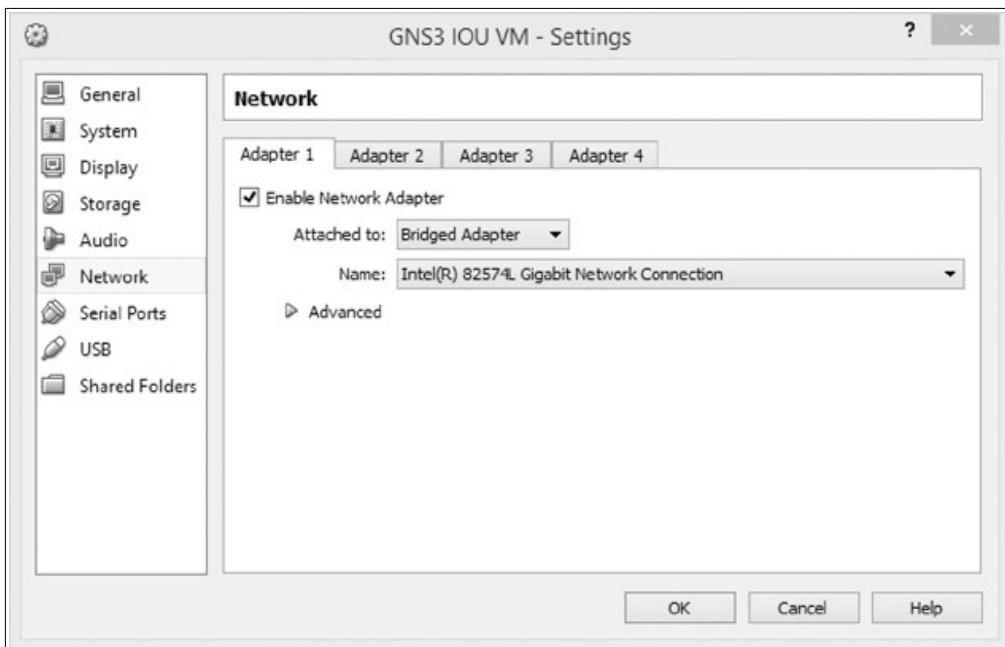


Figure 9-9: Bridge the network adapter to your PC.

Na guia Adaptador 1, selecione a opção **Enable Network Adapter**. Em seguida, escolha **Bridged Adapter** ao lado do campo Anexado a. Quando terminar, clique em **OK**. Isso conecta o adaptador Ethernet da sua máquina virtual ao seu PC e permite que ele acesse a Internet para que você possa instalar pacotes adicionais, se necessário.

Upload de arquivos de imagem IOU

Agora que você importou a máquina virtual GNS3 IOU, poderá executar a máquina virtual e fazer upload de seus arquivos de imagem IOU. Para ligar a máquina virtual, selecione **GNS3 IOU VM**, como na Figura 9-10, e clique em **Start**.

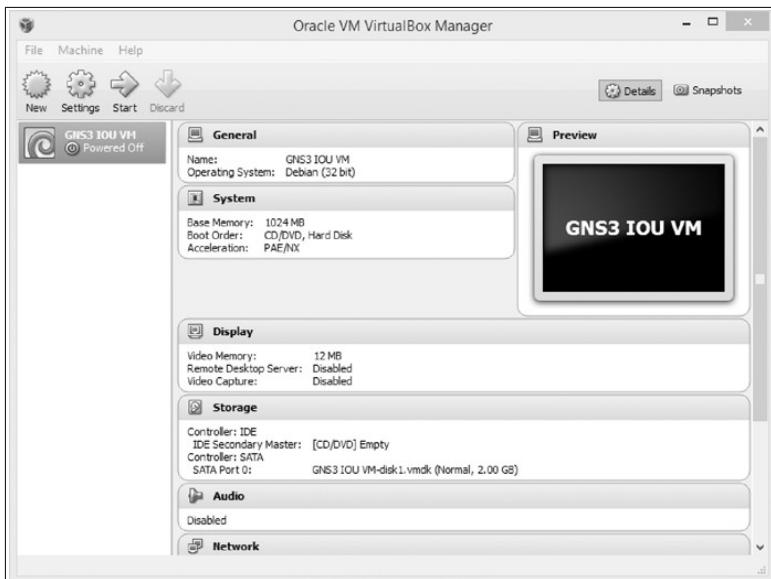


Figure 9-10: Select and start your GNS3 IOU virtual machine.

É normal que a máquina virtual leve um ou dois minutos para iniciar porque está inicializando um sistema operacional Linux totalmente funcional. Depois que a máquina virtual estiver em funcionamento, uma mensagem do console semelhante à seguinte deve ser exibida na tela:

Welcome to GNS3 IOU appliance

Use 172.16.231.204 to configure a remote server in GNS3 Preferences

Use your browser with <http://172.16.231.204:8000/upload> to upload IOS images

gns3-iouvm login:

Observe que a tela instrui você a usar o navegador da Web do seu PC para fazer o upload de arquivos de imagem IOU para o dispositivo. Para que isso funcione, seu PC e a máquina virtual GNS3 IOU devem ter um endereço IP atribuído a partir da sua rede local. Neste exemplo, o endereço IP da minha máquina virtual é 172.16.231.204.

NOTA

Às vezes, a máquina virtual IOU pode não exibir o endereço IP. Nesse caso, faça logon na máquina virtual usando o nome de usuário root e a senha cisco. Em seguida, digite ifconfig eth0 para exibir o endereço IP da interface Ethernet da sua máquina virtual.

Para fazer upload de um arquivo de imagem IOU, abra o navegador da web e navegue até o endereço IP, usando a porta 8000 conforme as instruções. Depois de inserir o URL (<http://172.16.231.204:8000/upload> neste exemplo), você deve receber uma página da web como a da Figura 9-11.



Figure 9-11: Select and upload your IOU image files

Use o botão **Browse...** para selecionar um arquivo de imagem IOU do seu PC. Depois de selecionado, clique em fazer **upload** para concluir o processo. Repita esta etapa para cada imagem que você deseja usar com o GNS3 e seu arquivo de licença IOU. As imagens são armazenadas na máquina virtual IOU em `/home/gns3/GNS3/images` e o caminho é exibido na página da Web para referência posterior. Você precisará dessas informações ao configurar suas imagens de IOU no GNS3. Portanto, é uma boa ideia destacar e copiar o caminho completo e o nome do arquivo agora. Dessa forma, você não precisará digitar mais tarde.

Configurando o GNS3 para IOU

Agora que o IOU está pronto, você apenas precisa preparar o GNS3. Primeiro, crie um arquivo de licença de texto sem formatação no seu PC usando o nome do host `gns3-iouvm`, como no exemplo a seguir. Substitua 1234567812345678 pelo seu número de licença.

```
[license]
gns3-iouvm = 1234567812345678
```

Um nome comum que é frequentemente usado para o arquivo de licença IOU é `.iourc`, mas você pode usar qualquer nome que faça sentido para você (por exemplo, você pode chamá-lo de `iou-license.txt`) e o arquivo de licença pode ser armazenado em qualquer lugar do sistema.

Depois de criar o arquivo de licença, você estará pronto para configurar as preferências do GNS3 para IOU. Inicie o GNS3, selecione **Edit>Preferences** no Windows ou **GNS3>Preferences** no OS X e selecione **GNS3 server**, conforme mostrado na Figura 9-12.

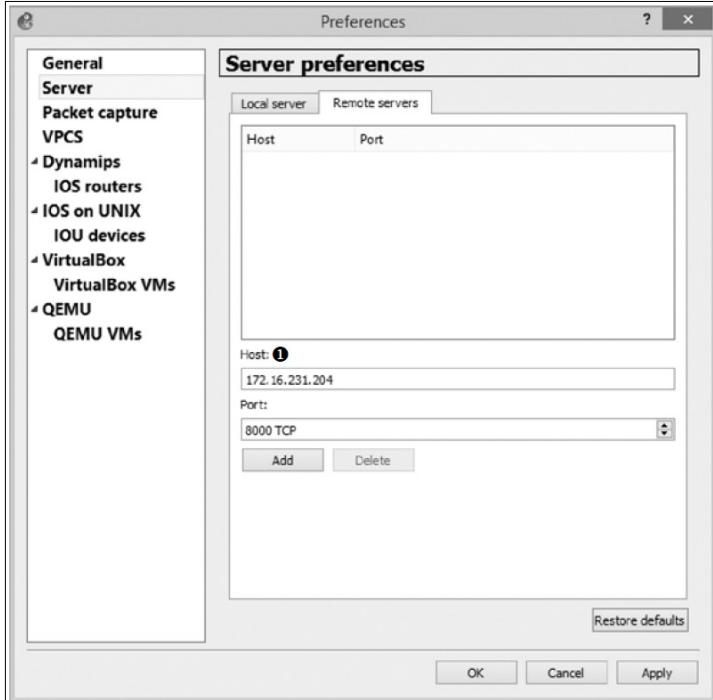


Figure 9-12: GNS3 server preferences, Remote servers tab

Selecione a guia Servidores remotos. Em Host ① digite o endereço IP da sua máquina virtual GNS3 IOU, clique em **Add** e, em seguida, clique em **Apply**. Neste exemplo, o endereço IP da minha máquina virtual GNS3 IOU é 172.16.231.204. Em seguida, informe ao GNS3 onde encontrar o arquivo de licença IOU. Clique em **IOS on UNIX** no painel à esquerda e selecione a guia Configurações gerais, mostrada na Figura 9-13. Clique no botão **Browse...** à direita do campo Caminho para IOURC para localize seu arquivo de licença. Selecione o arquivo e clique em **Add** e **Apply**. Neste exemplo, o caminho para o meu arquivo de licença é *C:\Users\jneumann\GNS3\iourc_license.txt*.

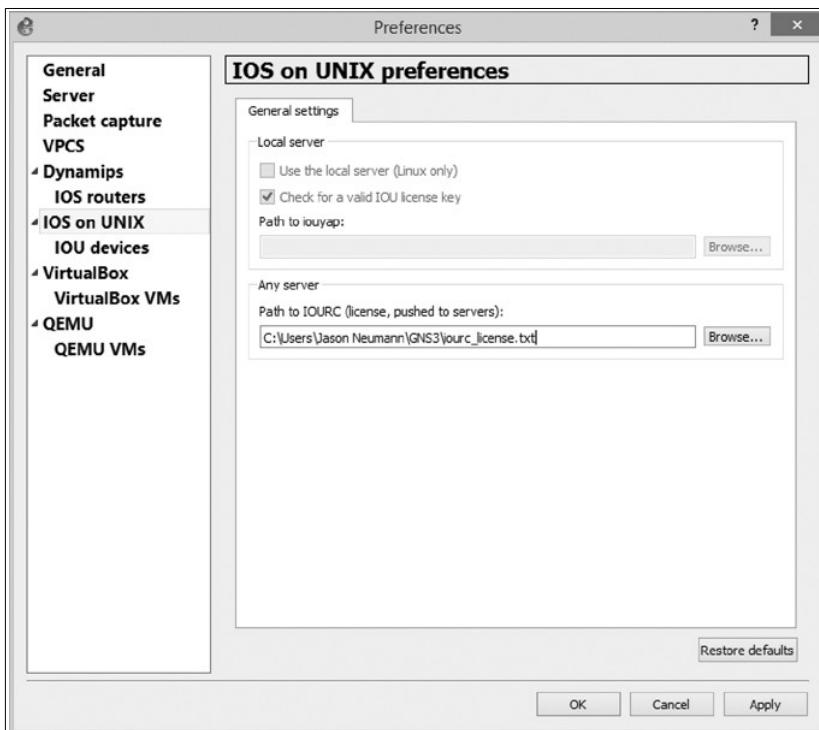


Figure 9-13: IOS on UNIX preferences, General settings tab

Em seguida, expanda **IOS on UNIX** no painel à esquerda para exibir dispositivos IOU, como mostra a Figura 9-14. A etapa final da configuração é adicionar o caminho a um arquivo de imagem IOU. Selecione **IOS devices** e clique em **New** para iniciar o assistente. Em Tipo de servidor, verifique se há uma seleção ao lado de **Remote** e clique em **Next**. Uma mensagem sobre a escolha de um caminho para sua imagem deve aparecer; clique em **OK** e você verá a janela **New IOU device**, mostrada na Figura 9-15. Digite um nome para o seu dispositivo IOU (*IOU_L2*, por exemplo) e depois digite o caminho da imagem IOU. Como as imagens IOU estão instaladas na máquina virtual Linux, você deverá inserir o "nome do caminho do Linux" no seu arquivo de imagem. Esse caminho é `/home/gns3/GNS3/images/<image_name>`. Neste exemplo, digitei `/home/gns3/GNS3/images/i86bi-linux-l2-adventerprisek9-15.1a.bin`. Você pode encontrar essas informações na página da IOU usada para carregar seus arquivos de imagem (consulte a Figura 9-11). Cuidado para inserir o caminho e o nome do arquivo corretamente; caso contrário, o IOU não funcionará. Eu recomendo copiar e colar as informações diretamente da página da Web da máquina virtual IOU para evitar qualquer confusão.

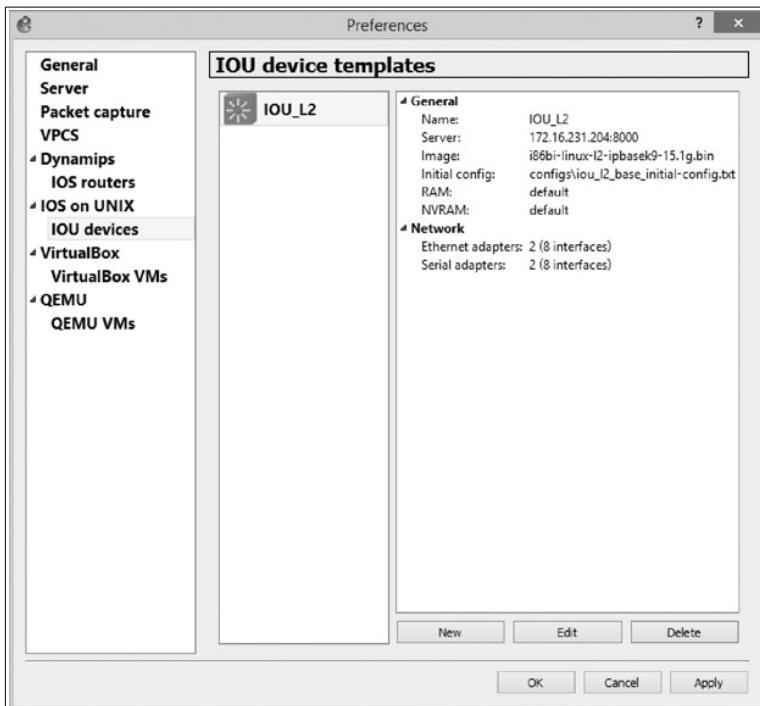


Figure 9-14: IOU devices preferences

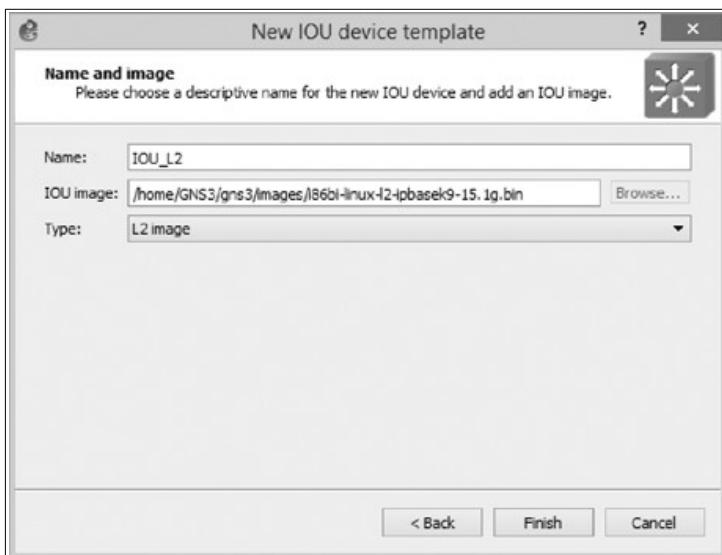


Figure 9-15: New IOU device window

Quando terminar, clique em **Finish** para fechar o assistente e clique em **Apply** e **OK** para concluir a configuração. Depois de adicionar uma imagem de IOU, você está pronto para começar a usar dispositivos de IOU em seus projetos.

Se você atualizar o GNS3 para uma nova versão, também precisará atualizar o servidor na sua máquina virtual GNS3 IOU para a mesma versão ou não funcionará. Para atualizar o servidor, efetue logon na máquina virtual GNS3 IOU e digite os seguintes comandos, substituindo *version* pela sua versão do GNS3:

```
Login: root
Password: cisco
# pip3 install gns3-server==version
```

IOU em ação

Agora vamos criar um projeto simples, isso permite que um switch IOU roteie o tráfego TCP / IP entre duas VLANs. Comece criando o projeto mostrado na Figura 9-16.

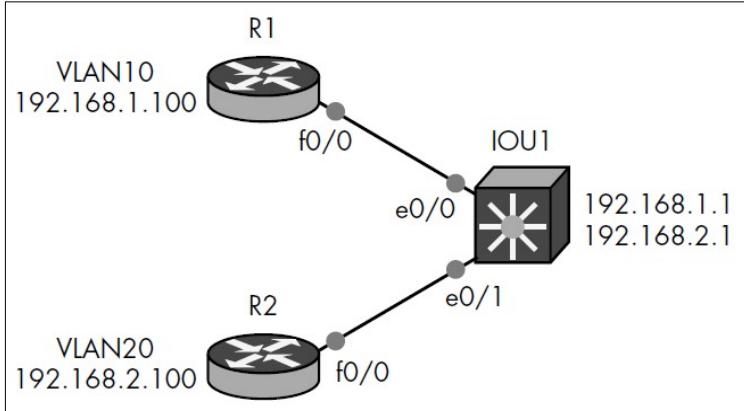


Figure 9-16: VLAN routing using an IOU switch

Neste projeto, você configurará um switch IOU L2 com duas VLANs (VLAN 10 e VLAN 20). Em seguida, você atribuirá o roteador R1 à VLAN 10 e roteador R2 para VLAN 20. Neste laboratório, o switch IOU encaminhará pacotes entre as duas VLANs para que R1 e R2 possam efetuar ping um ao outro. Comece configurando a opção IOU1 da seguinte maneira:

```
IOU1# configure terminal
① IOU1(config)# ip routing
② IOU1(config)# vlan 10
IOU1(config-vlan)# vlan 20
③ IOU1(config-vlan)# interface vlan 10
④ IOU1(config-if)# ip address 192.168.1.1 255.255.255.0
⑤ IOU1(config-if)# no shutdown
IOU1(config-if)# interface vlan 20
IOU1(config-if)# ip address 192.168.2.1 255.255.255.0
IOU1(config-if)# no shutdown
⑥ IOU1(config)# interface Ethernet 0/0
⑦ IOU1(config-if)# switchport mode access
⑧ IOU1(config-if)# switchport access vlan 10
IOU1(config-if)# no shutdown
IOU1(config-if)# interface Ethernet 0/1
IOU1(config-if)# switchport mode access
IOU1(config-if)# switchport access vlan 20
IOU1(config-if)# no shutdown
```

Habilite o roteamento IP ① e crie as duas VLANs (10 e 20) usando o comando *vlan* ②. Em seguida, crie uma interface virtual comutada (SVI) ③ para cada VLAN e atribua a cada SVI um endereço IP ④. Use o comando *no shutdown* ⑤ para abrir a interface. Agora vá sob as interfaces físicas ⑥ que estão conectadas ao R1 e ao R2, faça-as acessar as portas ⑦ e atribua-as à VLAN apropriada ⑧. Em seguida, configure um endereço IP no roteador R1.

```
R1(config)# interface f0/0
R1(config-if)# ip address 192.168.1.100 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Depois de atribuir o endereço IP a F0/0 em R1, defina o endereço de gateway padrão como 192.168.1.1 para que o roteador use IOU1 como gateway. Por fim, configure o R2 de maneira semelhante.

```
R2(config)# interface f0/0
R2(config-if)# ip address 192.168.2.100 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

Depois de configurar o projeto, você pode testar o roteamento de VLAN usando o comando ping. O roteador R1 deve poder executar ping no roteador R2 por meio do switch IOU1, conforme a seguir:

```
R1# ping 192.168.2.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/24/32 ms
```

É o suficiente para colocar os dispositivos IOU em funcionamento com o GNS3. Agora vamos dar uma olhada no mais novo sistema operacional da Cisco, o NX-OS.

NX-OSv

O Cisco NX-OS é executado em uma classe de comutadores do datacenter conhecida como Nexus. Embora parecido com o IOS, o NX-OS não é o IOS e usa um conjunto diferente de comandos de configuração. O NX-OSv, às vezes chamado de Titanium, é uma máquina virtual Linux que executa um simulador do NX-OS usando software de virtualização, como o VirtualBox. O NX-OSv não é uma simulação completa do sistema operacional e está faltando muitas funcionalidades. Ele fornece recursos e comandos suficientes para lhe dar uma ideia de como o NX-OS funciona e pode ser conectado em rede a dispositivos GNS3. Depois de adquirir uma imagem do NX-OSv, faça uma cópia e mantenha-a em um local seguro, caso sua cópia de trabalho seja corrompida de alguma forma. Crie um diretório para o NX-OSv no seu diretório GNS3 e copie o arquivo de imagem do NX-OSv. Você deve ter um arquivo chamado *N7K.vmdk*. Seu nome do arquivo pode ser diferente dependendo da sua versão do NX-OSv. Com seu arquivo de imagem no lugar, é hora de instalar o NX-OSv no VirtualBox.

Importando o NX-OSv para o VirtualBox

O NX-OSv geralmente vem pronto para ser executado na forma de um único arquivo de disco rígido da máquina virtual (arquivo .vmdk), e você pode executá-lo usando VMware, VirtualBox ou QEMU. O VirtualBox é gratuito e executa o NX-OSv de maneira confiável, mesmo em PCs com processadores mais antigos, como o Core 2 Duo, então abordarei o VirtualBox aqui. A configuração consiste em importar o arquivo de imagem do disco rígido para uma máquina virtual Linux personalizada e ajustar algumas configurações. Se você não possui o VirtualBox instalado no seu PC, faça o download e instale-o agora. Inicie o VirtualBox e clique em Novo para criar uma nova máquina virtual. Você deve receber o assistente Criar máquina virtual, mostrado na Figura 9-17.



Figure 9-17: Create Virtual Machine wizard, Name and operating system window

Digite um nome para o dispositivo, defina Tipo como **Linux** e Versão como **Other Linux (64-bit)** e, em seguida, clique em **Next** para continuar. Você deve receber a janela Tamanho da memória, mostrada na Figura 9-18. Para ajustar o tamanho da memória, use o controle deslizante ou digite a quantidade no campo fornecido. O NX-OSv funciona melhor com 2048 MB de RAM. Quando terminar, clique em **Next** para definir as configurações do disco rígido, mostradas na Figura 9-19.

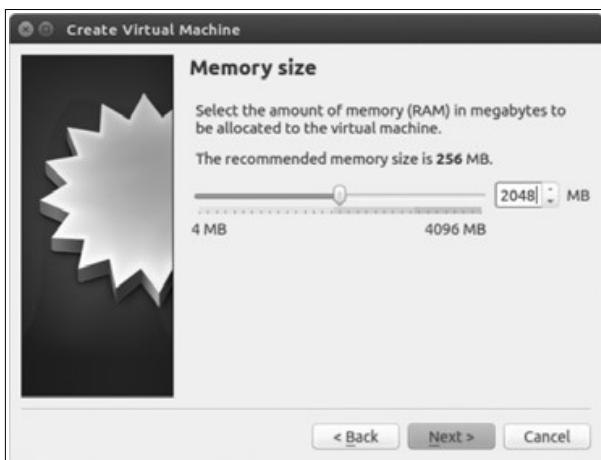


Figure 9-18: Create Virtual Machine wizard, Memory size window



Figure 9-19: Create Virtual Machine wizard, Hard drive window

Para conectar o disco rígido virtual do NX-OS à sua máquina virtual, selecione **Use an existing virtual hard drive file** e clique no ícone de navegação para localizar o arquivo **.vmdk** do NX-OSv. Selecione o arquivo e clique em **Create** para concluir a criação da máquina virtual.

Configurando o GNS3 para NX-OSv

Inicie o GNS3 e adicione a máquina virtual NX-OSv à sua biblioteca de máquinas virtuais. Selecione **Edit>Preferences** e expanda **VirtualBox** para mostre as máquinas virtuais do VirtualBox, como mostra a Figura 9-20. Daqui você pode adicionar máquinas virtuais do VirtualBox ao GNS3, que é o último passo antes de poder usar o NX-OSv.

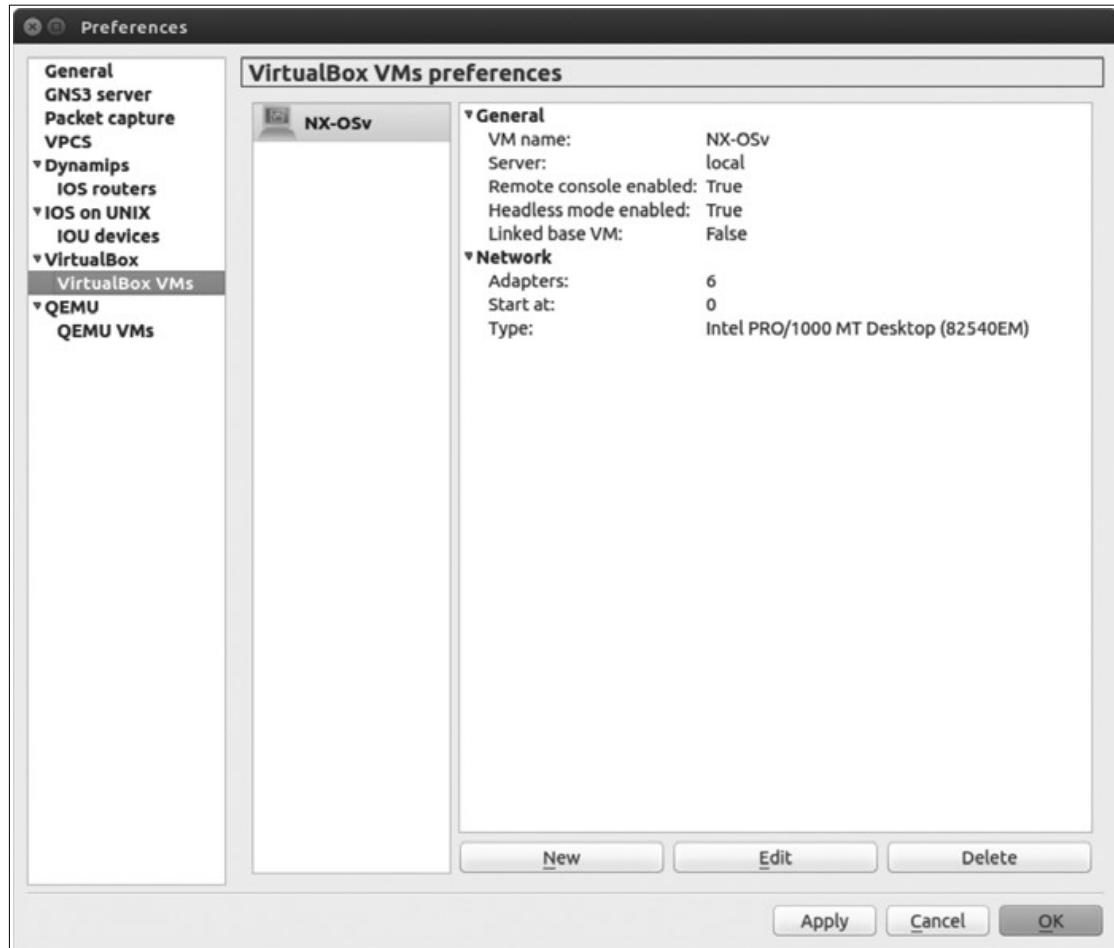


Figure 9-20: Adding the NX-OSv VirtualBox virtual machine to GNS3

Clique em **New** para iniciar o assistente do VirtualBox, selecione sua máquina virtual NX-OSv no menu suspenso nome da máquina virtual e clique em **Finish**. Agora clique em **Edit** e navegue até a guia Configurações gerais. Selecione as caixas **Enable remote console** e **Start VM in headless mode** e clique em **Apply**. Na guia Rede, altere o número de interfaces de 1 para 6 e clique em **Apply** para fechar a janela. Em seguida, clique em Aplicar e **OK** para concluir a instalação. Para usar uma máquina virtual NX-OSv em seus projetos, arraste sua máquina virtual NX-OSv da barra de ferramentas Dispositivos finais para o seu espaço de trabalho.

NX-OSv em ação

Agora que você adicionou o dispositivo NX-OSv ao GNS3, vamos usá-lo em um projeto. Crie uma topologia que inclua um dispositivo NX-OSv e um roteador IOS, como mostra a Figura 9-21. Este projeto publicitará todas as redes 172.16.0.0 de R1 a NX-OSv usando o Cisco EIGRP.

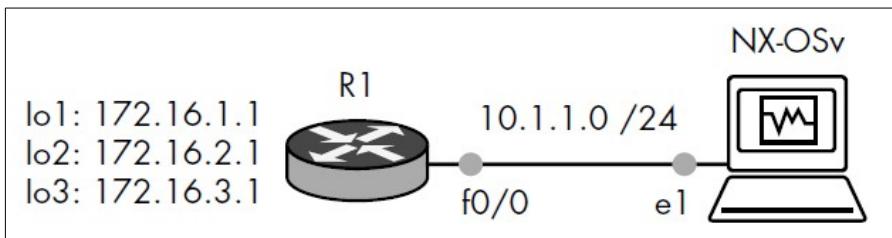


Figure 9-21: Simple topology using NX-OSv

Depois de criar o projeto, inicie todos os seus dispositivos e abra uma conexão de console ao NX-OSv. O NX-OS em execução em um PC leva muito tempo para inicializar e geralmente fica parado por um minuto na mensagem *SCSI disk detected*, exibida na Figura 9-22. Isso é normal, então seja paciente enquanto ele inicializa.

Figure 9-22: Booting NX-OSv

Se você não vir as mensagens de inicialização, pode ter configurado incorretamente alguma coisa. Volte e verifique todas as suas configurações no VirtualBox e GNS3. Se você continuar tendo problemas, pode haver algo errado com seu arquivo de imagem *N7K.vmdk*. Depois que o sistema iniciar, você receberá um prompt de login, como o mostrado aqui:

User Access verification

O login e a senha padrão devem ser *admin* e *admin*. Use essas credenciais para fazer logon no NX-OSv. Este é um bom momento para inserir alguns comandos. Eu começaria com *show run*, *show version* e *show interface brief*, mas você pode tentar qualquer comando do IOS que esteja familiarizado. Alguns serão os mesmos no NX-OS; outros não. Você pode usar o ponto de interrogação (?) para exibir uma lista completa. Agora que você deu uma olhada no NX-OSv, você pode configurar seu projeto. Primeiro, você configura o roteador R1. Abra um console no roteador R1 e digite os seguintes comandos para configurar todos os endereços IP do projeto:

```
R1# configure terminal  
R1(config)# interface f0/0  
R1(config-if)# no shutdown  
R1(config-if)# ip address 10.1.1.1 255.255.255.0  
R1(config-if)# interface loopback1  
R1(config-if)# ip address 172.16.1.1 255.255.255.0  
R1(config-if)# interface loopback2  
R1(config-if)# ip address 172.16.2.1 255.255.255.0  
R1(config-if)# interface loopback3  
R1(config-if)# ip address 172.16.3.1 255.255.255.0
```

Em seguida, ative o EIGRP e anuncie todas as redes IP.

```
R1(config-if)# router eigrp 10  
R1(config-router)# no auto-summary  
R1(config-router)# network 10.0.0.0
```

```
R1(config-router)# network 172.16.0.0
```

Agora faça logon no NX-OSv e configure um endereço IP da mesma sub-rede que a interface f0/0 de R1.

```
vNX-OS-01# configure terminal  
vNX-OS-01(config)# interface ethernet 2/1  
vNX-OS-01(config-if)# ip address 10.1.1.2/24  
vNX-OS-01(config-if)# no shutdown
```

A primeira coisa que você deve notar é que o NX-OS aceita apenas endereços IP usando a notação CIDR; portanto, aqui, a máscara de sub-rede é inserida como /24 e não 255.255.255.0, como comumente usada no IOS. Agora use o comando *ping* para testar a conectividade do NX-OSv ao roteador R1 e sair para o modo de configuração.

```
vNX-OS-01(config-if)# do ping 10.1.1.1  
PING 192.168.1.1 (10.1.1.1): 56 data bytes  
64 bytes from 10.1.1.1: icmp_seq=0 ttl=254 time=19.494 ms  
64 bytes from 10.1.1.1: icmp_seq=1 ttl=254 time=7.849 ms  
64 bytes from 10.1.1.1: icmp_seq=2 ttl=254 time=7.511 ms  
64 bytes from 10.1.1.1: icmp_seq=3 ttl=254 time=20.637 ms  
64 bytes from 10.1.1.1: icmp_seq=4 ttl=254 time=8.524 ms  
--- 10.1.1.1 ping statistics ---  
5 packets transmitted, 5 packets received, 0.00% packet loss  
round-trip min/avg/max = 7.511/12.803/20.637 ms  
vNX-OS-01(config-if)# exit
```

Agora vamos configurar o NX-OSv para que ele possa trocar rotas anunciadas pelo EIGRP com o roteador R1. Observe que o NX-OS permite executar o EIGRP apenas por um período de cortesia de 120 dias, a menos que você tenha uma licença de recurso. Digite o comando *license grace-period* para iniciar o período de cortesia.

```
vNX-OS-01(config)# license grace-period  
vNX-OS-01(config)# feature eigrp  
vNX-OS-01(config)# router eigrp 10  
vNX-OS-01(config)# network 10.0.0.0/8  
vNX-OS-01(config)# exit
```

Você pode verificar se as rotas do R1 estão sendo anunciadas para o NX-OSv usando o comando *show ip route*.

```
vNX-OS-01# show ip route  
IP Route Table for VRF "default"  
'*' denotes best ucast next-hop  
'***' denotes best mcast next-hop  
'[x/y]' denotes [preference/metric]  
'%<string>' in via output denotes VRF <string>  
  
10.1.1.0/24, ubest/mbest: 1/0, attached  
    *via 10.1.1.2, Eth2/1, [0/0], 00:49:54, direct  
10.1.1.2/32, ubest/mbest: 1/0, attached  
    *via 10.1.1.2, Eth2/1, [0/0], 00:49:54, local  
172.16.1.0/24, ubest/mbest: 1/0  
    *via 10.1.1.1, Eth2/1, [90/130816], 00:32:04, eigrp-10, internal  
172.16.2.0/24, ubest/mbest: 1/0  
    *via 10.1.1.1, Eth2/1, [90/130816], 00:32:04, eigrp-10, internal  
172.16.3.0/24, ubest/mbest: 1/0  
    *via 10.1.1.1, Eth2/1, [90/130816], 00:32:04, eigrp-10, internal
```

Nas linhas anteriores, observe que a saída deste comando é diferente do IOS, mas todas as informações pertinentes estão lá. Neste exemplo, todas as rotas 172.16.0.0 foram anunciadas de R1 para NX-OSv via EIGRP, portanto, você deve poder executar ping em qualquer um desses endereços. Tente isso agora.

```
NX-OSv-01# ping 172.16.2.1
PING 172.16.2.1 (172.16.2.1): 56 data bytes
64 bytes from 172.16.2.1: icmp_seq=0 ttl=254 time=20 ms
64 bytes from 172.16.2.1: icmp_seq=1 ttl=254 time=10 ms
64 bytes from 172.16.2.1: icmp_seq=2 ttl=254 time=20 ms
64 bytes from 172.16.2.1: icmp_seq=3 ttl=254 time=10 ms
64 bytes from 172.16.2.1: icmp_seq=4 ttl=254 time=20 ms

--- 172.16.2.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 10/16/20 ms
```

Por fim, salve sua configuração. O comando em si é o mesmo que IOS, mas fornece saída diferente.

```
vNX-OS-01# copy running-config startup-config
[########################################] 100%
Copy complete.
VNX-OS-01#
```

Agora que você criou um projeto simples, pode começar a experimentar o NX-OSv por conta própria. Lembre-se de que algumas funções definitivamente estarão ausentes. Na minha versão, por exemplo, nenhuma das funcionalidades do switch L2 funciona, apenas o roteamento da camada 3. Outro item a ter em conta é a conclusão da guia; funciona apenas em alguns comandos, portanto, não presuma que um comando não funcione apenas porque o NX-OSv não fornece o preenchimento de guias na linha de comando. Apesar dessas limitações, ainda acho divertido adicionar dispositivos NX-OS aos meus projetos, e tenho certeza que você também. Para saber mais sobre o Cisco Nexus e o NX-OS, visite <http://www.cisco.com/en/US/products/ps9402/index.html>.

Pensamentos finais

Neste capítulo, você explorou o IOS no Unix e aprendeu como aproveitar o IOU para adicionar recursos de comutação quase completos ao GNS3 sem usar switches físicos. Embora não seja necessário para as certificações no nível CCNA, a alternância de IOU é altamente útil para as certificações CCNP e CCIE. Em seguida, você instalou o NX-OSv, uma máquina virtual que simula um servidor Cisco Switch Nexus executando o NX-OS. O NX-OSv pode ser conectado em rede a dispositivos GNS3 usando protocolos como OSPF e EIGRP, e é divertido brincar com ele, mas falta muito da funcionalidade que você encontraria usando um comutador Nexus real. No próximo capítulo, mostrarei algumas coisas divertidas que você pode fazer com o GNS3, como criar um servidor de acesso simulado para gerenciar seus roteadores.

10 Coisas legais para fazer em um dia chuvoso

Agora que você viu os recursos mais usados do GNS3, vamos explorar alguns truques divertidos que você pode fazer com seus projetos do GNS3. Primeiro, você criará um servidor de acesso Cisco simulado que funciona como seu equivalente real da Cisco. A seguir, mostrarei como mover seus projetos GNS3 de um sistema operacional para outro e como copiar as configurações do roteador virtual GNS3 do GNS3 para os roteadores Cisco reais. Por fim, você compartilhará o carregamento de recursos de um projeto usando vários PCs, cria alguns laboratórios nerds e simula alguns cenários reais de rede.

Gerenciando dispositivos de um Servidor Accesso

Um servidor de acesso permite gerenciar todos os dispositivos de rede a partir de um console central, para que você possa simultaneamente fazer logon em vários consoles de dispositivos e alternar facilmente entre eles. É uma maneira eficiente de gerenciar dispositivos em grandes redes Cisco e, com apenas um pouco de esforço, você pode criar um servidor de acesso virtual Cisco totalmente funcional (às vezes chamado de terminal ou servidor de comunicação) para gerenciar seus dispositivos GNS3. Acho que usar um servidor de acesso virtual é uma maneira rápida de gerenciar e configurar dispositivos no GNS3 e também para aprender os comandos e as teclas de um servidor de acesso real. Um servidor de acesso virtual GNS3 possui dois componentes. O primeiro é um nó da nuvem configurado com uma interface virtual; você usará um driver de adaptador de loopback no Windows e um adaptador TAP no Linux. O segundo é um roteador Cisco Dynamips que atua como o console de gerenciamento. A configuração do próprio servidor de acesso virtual varia um pouco, dependendo do seu sistema operacional. Abrangerei o Windows e o Ubuntu Linux, mas os conceitos se aplicam a outros sistemas operacionais Linux. Infelizmente, o OS X não é suportado no momento da escrita.

Instalando a interface virtual

Se você usa Windows ou Linux, será necessário instalar um adaptador de rede virtual e atribuir um endereço IP a ele. No Windows, você instala um driver de adaptador de loopback e, em sistemas baseados em Unix, como o Linux, instala um driver TAP. Se você é um usuário Linux, pode pular para “Configurando um Adaptador TAP no Linux” na página 179.

Configurando um adaptador de loopback no Windows

Se você ainda não o fez, instale o driver do Microsoft Loopback Adapter. (Consulte “Utilizando um adaptador de loopback no Windows” na página 106.) Depois de instalar o adaptador, atribua-lhe um endereço IP. O endereço IP e a máscara de sub-rede escolhidos devem ser exclusivos de qualquer adaptador de rede já configurado no seu PC e de qualquer endereço IP que você planeja usar na topologia de rede GNS3. Para configurar o adaptador, abra o **Control Panel** do Windows e selecione **Network and Sharing Center**. Em seguida, selecione **Change Adapter Settings** para exibir uma lista de adaptadores disponíveis, conforme mostrado na Figura 10-1.

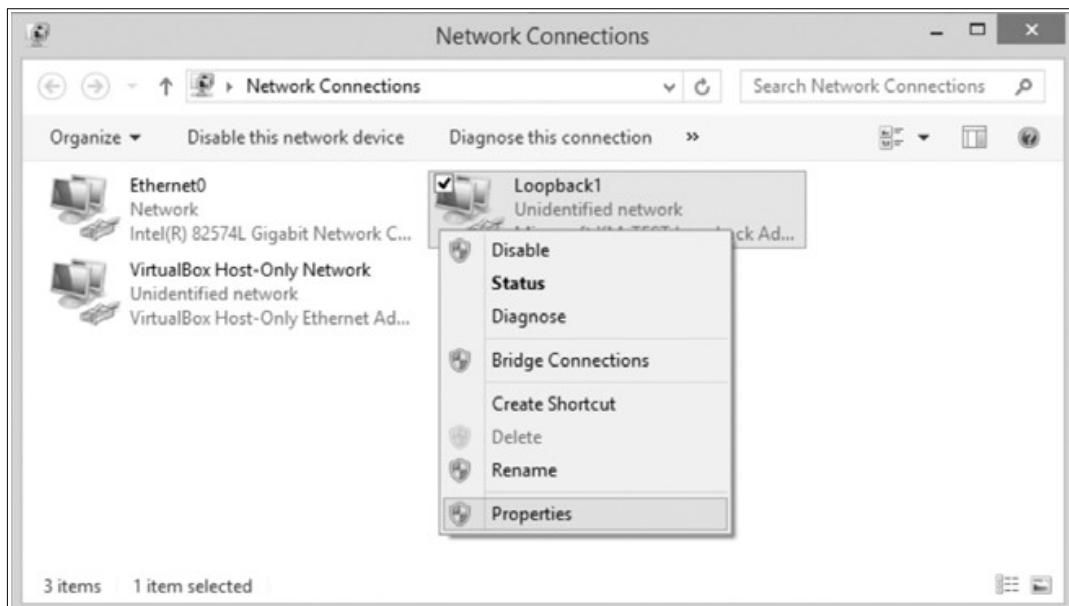


Figure 10-1: Selecting Properties to configure the Microsoft Loopback Adapter driver

Clique com o botão direito do mouse no driver Microsoft Loopback Adapter e selecione **Properties**. Na janela Propriedades, selecione **Internet Protocol Version 4 (TCP/IPv4)** e clique no botão **Properties**, para exibir as configurações de endereço IP, mostradas na Figura 10-2.

Selecione **Use the following IP address** e insira um IP exclusivo endereço e máscara de sub-rede. Escolhi 9.9.9.9 e 255.255.255.0, mas qualquer endereço e máscara funcionará, desde que sejam exclusivos de qualquer endereço atribuído a qualquer adaptador Ethernet no seu PC, e de qualquer endereço que você planeja usar na sua topologia de rede GNS3. Não é necessário incluir um endereço de gateway padrão nem fornecer servidores DNS, pois eles não serão usados pelo servidor de acesso. Quando terminar, clique em **OK** para concluir a configuração. Agora

feche todas as janelas abertas e inicie o GNS3. Se você é um usuário Linux, continue lendo; caso contrário, você pode pular para “Preparando o servidor GNS3” na página 180.



Figure 10-2: Configuring your Loopback Adapter driver with an IP address

Configurando um Adaptador TAP no Linux

No Ubuntu Linux, você usará um adaptador TAP virtual para o servidor de acesso. Abra um terminal e digite o seguinte comando para instalar os drivers:

```
$ sudo apt-get install uml-utilities
```

Para ativar o tap0, digite o seguinte comando, substituindo *jneumann* pelo seu nome de usuário do Linux:

```
$ sudo tunctl -u jneumann -t tap0
```

Em seguida, atribua um endereço IP exclusivo à interface tap0. O endereço IP e a máscara de sub-rede escolhidos devem ser exclusivos de qualquer adaptador de rede configurado no seu PC e de qualquer endereço IP que você planeja usar na topologia de rede GNS3.

```
$ sudo ifconfig tap0 9.9.9.9 netmask 255.255.255.0 up
```

Para garantir que a interface tap0 mantenha seu endereço IP e esteja disponível após uma reinicialização, você precisará alterar as configurações de rede do Linux.

Abra o arquivo de interfaces em /etc/networks/ em um editor de texto como pico ou vi. Você precisará de privilégios de administrador para fazer alterações no arquivo, faça logon como root ou execute o editor com o comando sudo, como nas interfaces sudo pico. Em seguida, acrescente o seguinte ao final do arquivo:

```
auto tap0
iface tap0 inet static
    pre-up tunctl -t tap0
    up ifconfig tap0 up
    down ifconfig tap0 down
    address 9.9.9.9
```

netmask 255.255.255.0

Com esses comandos no lugar, salve o arquivo de interfaces, feche-o e reinicie. Quando o Ubuntu reiniciar, o driver TAP deve carregar automaticamente e a interface tap0 deve estar pronta para uso.

ATENÇÃO

Tenha cuidado ao editar o arquivo /etc/networks/interfaces. Um erro de digitação aqui pode impedir que o Ubuntu seja inicializado corretamente.

Digite o comando *ifconfig* para verificar as configurações tap0:

```
$ ifconfig
--snip--
① tap0      Link encap:Ethernet HWaddr 16:81:25:c1:cc:8c
②           inet addr:9.9.9.9 Bcast:9.9.9.255 Mask:255.255.255.0
                  UP BROADCAST MULTICAST MTU:1500 Metric:1
                  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:500
                  RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```

A saída do *ifconfig* deve mostrar que o adaptador tap0 está ativado ① e configurado com um endereço IP ②. Depois de instalar e configurar um adaptador virtual, será necessário configurar o servidor GNS3.

Preparando o servidor GNS3

No Windows, execute o GNS3 como administrador. Comece ligando o servidor GNS3 ao endereço IP da sua interface virtual; caso contrário, seu servidor de acesso não funcionará. Clique em **Edit>Preferences** e escolha o **GNS3 server** na coluna esquerda. Selecione o menu suspenso **Host binding** e, em seguida, selecione o endereço IP atribuído à interface virtual, como mostra a Figura 10-3. Na Figura 10-3, o endereço IP é 9.9.9.9 ①. Clique em **Apply** e em **OK**, e o servidor GNS3 deve reiniciar com a nova ligação de host.

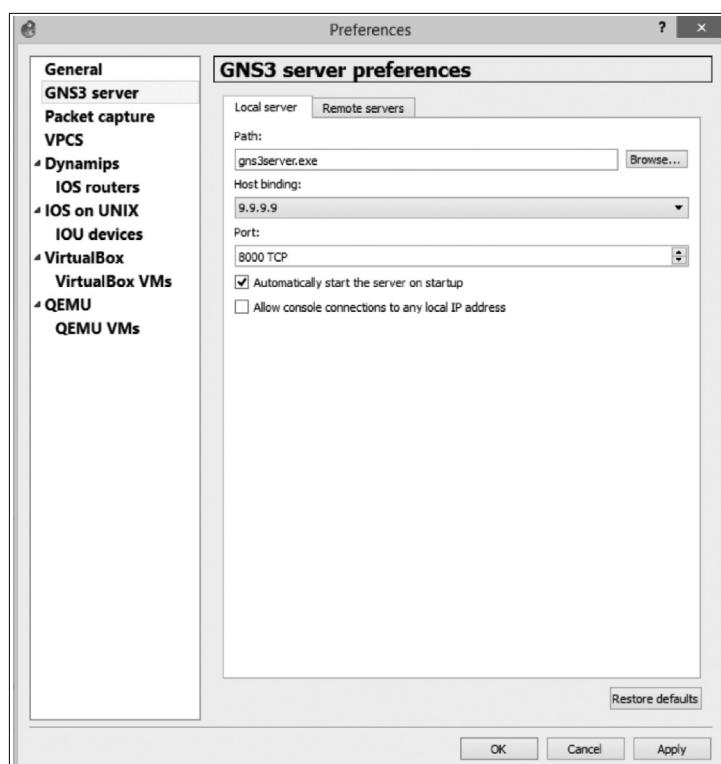


Figure 10-3: Changing the GNS3 server host binding

Criando um servidor de acesso virtual no GNS3

Com o servidor GNS3 vinculado ao endereço IP do adaptador virtual, você pode criar o servidor de acesso virtual. O servidor de acesso é criado usando dois dispositivos: um Cloud node e um roteador Dynamips IOS.

Configurando o Cloud node

Inicie um projeto adicionando um Cloud node ao seu espaço de trabalho. Clique com o botão direito do mouse no Cloud node e selecione **Configure**. Se você estiver executando o Windows, selecione a guia **NIO Ethernet** (mostrada na Figura 10-4). Clique no menu suspenso em Generic Ethernet NIO e selecione o driver do Microsoft Loopback Adapter (**Loopback1** neste exemplo); depois clique em **Add**, **Apply** e **OK** para concluir a configuração. Se você estiver executando o GNS3 no Ubuntu Linux, configure o Cloud node usando **tap0**. Em vez da NIO Ethernet, selecione a guia **NIO TAP** e digite **tap0** no campo da interface TAP, como na Figura 10-5.

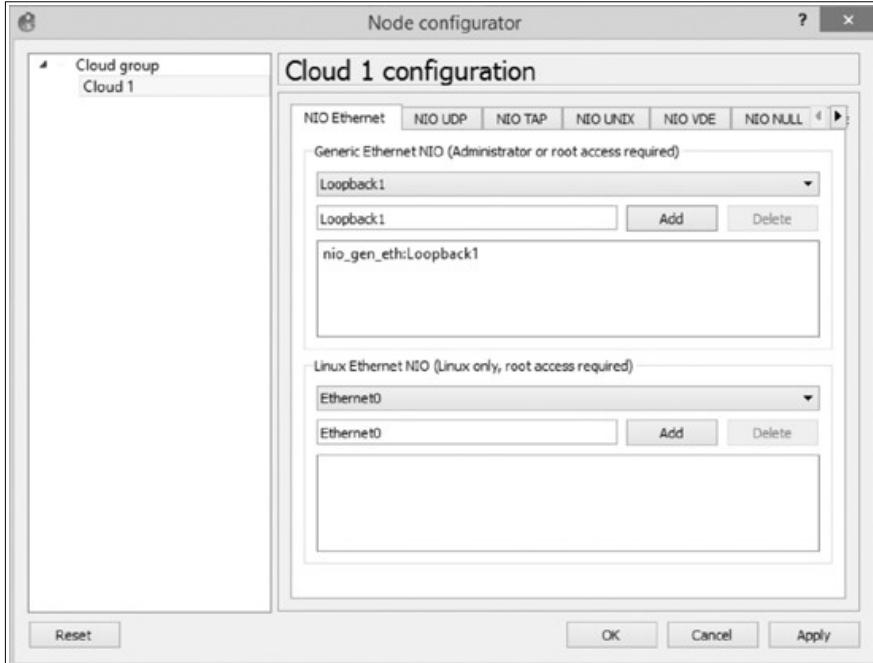


Figure 10-4: Configuring the Cloud node with a Loopback Adapter driver in Windows

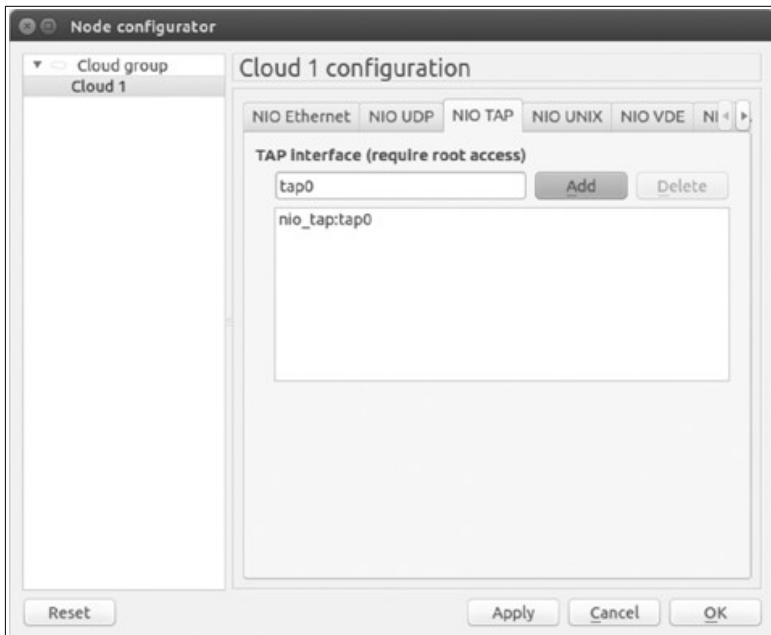


Figure 10-5: Configuring NIO TAP with tap0 on Ubuntu Linux

Quando terminar, clique em **Add**, **Apply**, e **OK** para concluir a configuração do Cloud node.

Configurando o roteador do servidor de acesso

Após configurar o Cloud node, adicione um roteador Dynamips à sua área de trabalho e crie um link do roteador para o nó da Nuvem. Juntos, esses dois dispositivos compreendem o servidor de acesso virtual, mostrado na Figura 10-6. Eles não serão vinculados a nenhum outro dispositivo no seu projeto GNS3.

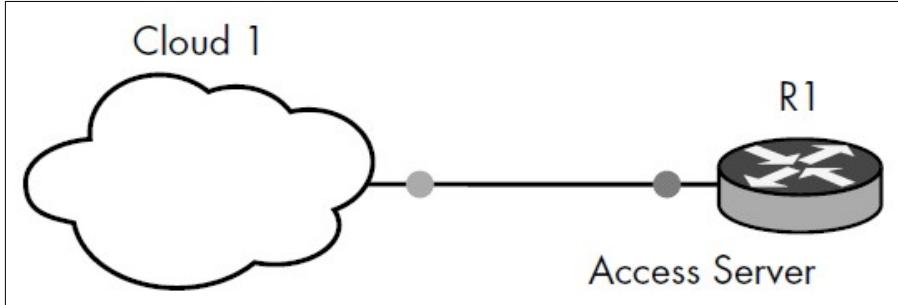


Figure 10-6: Virtual access server

Depois de vincular os componentes do servidor de acesso virtual, adicione mais roteadores para sua área de trabalho para criar uma rede simples de três roteadores, como mostra a Figura 10-7. Essa é a topologia de rede que será gerenciada usando o servidor de acesso virtual.

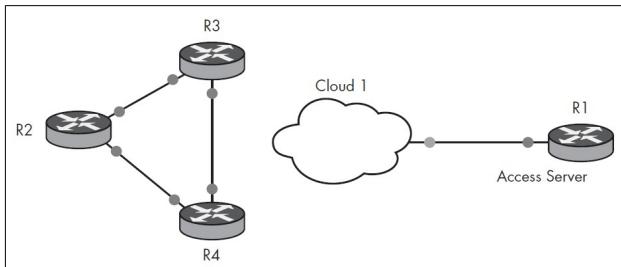


Figure 10-7: Network configured with a virtual Cisco access server

A Figura 10-7 mostra que você criou um servidor de acesso virtual usando roteador R1 e um Cloud node (Cloud1), e você criou uma topologia de rede composta por três roteadores, denominados R2, R3 e R4. Agora que você criou o servidor de acesso e uma topologia de rede GNS3, você pode configurar o roteador do servidor de acesso. Atribua ao roteador R1 um endereço IP da mesma rede que o adaptador virtual do seu PC e teste a conectividade de R1 à interface do adaptador virtual. Por exemplo, se você atribuiu ao adaptador virtual o endereço IP 9.9.9.9 255.255.255.0 como eu, você pode atribuir ao roteador do servidor de acesso R1 qualquer endereço IP nesse intervalo de rede. Eu uso o endereço IP 9.9.9.8 e a máscara de sub-rede 255.255.255.0. Para configurar o endereço na interface f0/0, abra uma conexão de console ao roteador R1 e digite os seguintes comandos:

```
R1>enable
R1#configure terminal
R1(config)#interface f0/0
R1(config-if)#ip address 9.9.9.8 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
R1#ping 9.9.9.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9.9.9.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Nesta configuração, a interface do roteador R1 f0/0 está vinculada à Cloud node e configurado com o endereço IP 9.9.9.8 255.255.255.0. Teste a conexão entre o R1 e a interface virtual usando um comando *ping*. Se o teste de ping for bem-sucedido, você estará pronto para seguir em frente. Se o teste de ping não tiver êxito, verifique se todas as suas

interfaces estão ativadas e se a interface virtual (loopback ou TAP) está configurada com o endereço IP e a máscara de sub-rede adequados.

Configurando uma tabela de nome de host IP da Cisco

Depois de configurar um endereço IP no servidor de acesso virtual (R1), você estará pronto para configurar uma tabela de nome de host IP usando as informações coletadas dos dispositivos que o servidor de acesso gerenciará. Neste projeto, os dispositivos são roteadores R2, R3 e R4. Usando os comandos do Cisco IOS, você cria uma tabela de nome de host IP usando o endereço IP da interface virtual (9.9.9.9) e os números de porta do console que o GNS3 atribuiu aos roteadores usados na topologia de rede. Uma tabela de nome de host IP da Cisco funciona como um arquivo de hosts Unix, exceto que você também inclui números de porta na tabela. Você criará uma entrada para cada dispositivo na topologia que deseja gerenciar. Comece localizando os números de porta do console dos roteadores que o servidor de acesso gerenciará. Neste projeto, você está interessado apenas nos números de porta do console dos roteadores R2, R3 e R4. Você pode encontrar rapidamente o número da porta do console de qualquer dispositivo passando o mouse sobre o dispositivo, conforme mostrado em Figura 10-8.

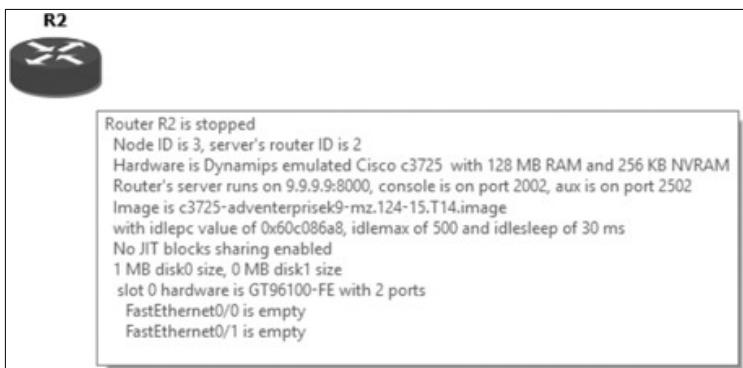


Figure 10-8: Displaying device information

O console do roteador R2 está na porta 2002. Como os números de porta do console são atribuídos seqüencialmente à medida que os dispositivos são adicionados a um projeto, os roteadores R2, R3 e R4 devem ter sido atribuídos aos números de porta do console 2002, 2003 e 2004, respectivamente. Se não tiver certeza, passe o mouse sobre o ícone de cada dispositivo para verificar as informações.

NOTA

Se você adicionar vários roteadores ao mesmo tempo, em vez de um de cada vez, os números da porta do console poderão não ser atribuídos em ordem sequencial.

Para criar a tabela de nome de host IP, abra um console no roteador R1 (o servidor de acesso) e digite os seguintes comandos:

```
R1#configure terminal
R1(config)#ip host R2 2002 9.9.9.9
R1(config)#ip host R3 2003 9.9.9.9
R1(config)#ip host R4 2004 9.9.9.9
R1(config)#exit
R1#
```

Observe que os números de porta do host correspondem aos números de porta do console exclusivos dos três roteadores que você deseja gerenciar, mas o endereço IP é sempre o mesmo; é o endereço IP atribuído ao adaptador virtual (9.9.9.9). Isso ocorre porque quando o servidor de acesso virtual abre um console para um dos roteadores de laboratório, o GNS3 cria uma sessão de telnet do servidor de acesso para os roteadores usando o endereço IP do adaptador virtual. A partir daí, ele se conecta ao número da porta do console individual que você atribuiu. Por exemplo, quando o servidor de acesso abre uma conexão de console ao roteador R2, o GNS3 faz telnet para o endereço IP 9.9.9.9 usando o número da porta 2002. Isso é semelhante à maneira como um servidor de acesso Cisco real funciona. Agora, verifique quais hosts estão configurados no seu servidor de acesso virtual com o comando show hosts.

```
R1>show hosts
Default domain is not set
Name/address lookup uses static mappings

Codes: UN - unknown, EX - expired, OK - OK,
       ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined
```

Host ^①	Port ^②	Flags	Age	Type	Address(es) ^③
R2	2002	(perm, OK)	0	IP	9.9.9.9
R3	2003	(perm, OK)	0	IP	9.9.9.9
R4	2004	(perm, OK)	1	IP	9.9.9.9

Este comando exibe o nome do host ^①, número da porta ^②, e endereço IP ^③ para cada host configurado no servidor de acesso.

Limitações do servidor virtual

Existem limitações quanto a quais dispositivos podem ser gerenciados pelo servidor de acesso virtual. Como o servidor GNS3 está vinculado a um adaptador virtual e é executado “localmente” no seu PC, o servidor de acesso virtual pode gerenciar apenas dispositivos locais. Em um PC com Windows, você não pode gerenciar máquinas virtuais do VirtualBox, incluindo IOU, embora possa gerenciar dispositivos QEMU, como o Junos. No Ubuntu Linux, você pode gerenciar todos os dispositivos, incluindo Dynamips, IOU, QEMU e VirtualBox, desde que estejam executando localmente no seu PC Linux.

Para saber mais sobre como configurar e usar um servidor de acesso Cisco real, visite o site da Cisco (<http://www.cisco.com/>) e pesquise *configuring a comm server*. Por enquanto, você deve saber tudo o que precisa para experimentar seu servidor de acesso virtual.

Vendo o servidor de acesso virtual em ação

Depois de configurar totalmente o servidor de acesso e iniciar os roteadores do projeto, você poderá gerenciar esses roteadores usando o servidor de acesso. Você pode abrir uma conexão de console com vários roteadores e alternar facilmente entre eles.

Abrindo consoles

Comece abrindo uma conexão de console para R1. Clique com o botão direito do mouse no roteador R1 e escolha **Console**. Em seguida, digite o nome do host que você deseja gerenciar e pressione *ENTER*. Os nomes de host fazem distinção entre maiúsculas e minúsculas, portanto, digite corretamente o nome.

```
R1>R2
Translating "R2"
Trying R2 (9.9.9.9①, 2002②)... Open
Connected to Dynamips VM "R2" (ID 1, type c3600) - Console port
Press ENTER to get the prompt.
R2>③
```

Neste exemplo, abro uma sessão com o roteador R2 inserindo R2 na linha de comando do servidor de acesso. A saída mostra que uma sessão é estabelecida usando o endereço IP 9.9.9.9 ^① e o número da porta 2002 ^②, e o prompt ^③ foi alterado para o roteador que está sendo gerenciado (R2 neste exemplo). Após a abertura da sessão, você pode configurar o roteador como se tivesse aberto um console diretamente do GNS3.

Quando você terminar de configurar o roteador, retorne ao console do servidor de acesso; basta pressionar SHIFT-CTRL-6 e, em seguida, pressione a tecla X. (A Cisco chama essa combinação de ações de *escape sequence*.) Após retornar ao console do servidor de acesso, digite o nome de outro roteador no seu projeto para abrir um console nele. Tente entrar no **R3** agora e configure o roteador como desejar. Quando terminar, use a sequência de escape

novamente para retornar ao servidor de acesso. Mesmo que você esteja atualmente conectado ao console do servidor de acesso, as sessões nos outros dois roteadores permanecem abertas. Para exibir uma lista de sessões abertas e seus números de conexão correspondentes, digite o comando *show sessions*.

R1>show sessions

Conn	Host	Address	Byte	Idle	Conn	Name
	1 R2	9.9.9.9	0	0		R2
①*	2 R3	9.9.9.9	0	0		R3

Você deve ver duas conexões ativas (1 e 2). O asterisco ① próximo a Conn 2 indica que o roteador R3 foi a última sessão usada. Para retornar à última sessão, pressione enter. Para retornar a uma sessão diferente, digite um número de conexão e pressione *ENTER*; por exemplo, você deve digitar 1 para retornar ao roteador R2.

Fechando consoles

Quando você estiver pronto para se desconectar de uma conexão aberta, insira o comando *disconnect* seguido pelo número da conexão; depois pressione enter para confirmar o fechamento da sessão.

R1>disconnect 2

Closing connection to R3 [confirm]

R1>

Neste exemplo, desconectei do roteador R3 (conexão 2). Após desconectar uma sessão, você precisará digitar o nome do host novamente para se reconectar ao dispositivo.

Definindo tempos limite de conexão

Convém ajustar a configuração de tempo limite (por meio do parâmetro *exec-timeout* do console) nos roteadores e no servidor de acesso para garantir que você não seja desconectado automaticamente durante os períodos de inatividade, como quando você não está configurando ativamente um roteador. O valor padrão é dez minutos, mas pode ser definido como mais alto, mais baixo ou alterado para infinito. Os comandos a seguir configuram o tempo limite do console para zero minutos e zero segundos (infinito):

R1>enable

R1#configure terminal

R1(config)#line console 0

R1(config-line)#exec-timeout 0 0

A configuração de inicialização padrão do GNS3 já deveria ter feito isso por você, mas saiba que, do ponto de vista da segurança, nunca permitir que o roteador atinja o tempo limite é uma má ideia nos ambientes de produção. No entanto, é altamente conveniente em ambientes de laboratório como o GNS3.

Implantando configurações em hardware real

Um dos benefícios do GNS3 é que ele permite criar e testar configurações de rede que podem ser usadas posteriormente em equipamentos reais. Você simplesmente exporta uma configuração de roteador no GNS3 e carrega-a em um roteador Cisco IOS real.

Exportando configurações GNS3 para roteadores Cisco

Depois de testar completamente uma configuração de roteador no GNS3, você está pronto para exportá-la e carregá-la em um roteador Cisco real. Você pode exportar todos os roteadores em seu projeto ou exportar a configuração de um dispositivo individual.

Antes de exportar uma configuração do roteador GNS3 IOS, efetue login no roteador e salve o arquivo *running-config* no arquivo *startup-config*. O arquivo de configuração salvo *startup-config* é a configuração que será exportada pelo GNS3.

```
R1#copy running-config startup-config
```

Se você tiver dispositivos de IOU em seu projeto, precisará fazer cópias dos arquivos *running-config* também. Basta fazer login no dispositivo e digite o seguinte comando para criar um arquivo de texto da configuração IOU:

```
IOU#copy running-config unix:initial-config.cfg
```

Depois de salvar um arquivo de configuração em execução, você pode exportar todas as configurações do dispositivo ao mesmo tempo, selecionando **File>Import/Export device configs**. O GNS3 deve então mostrar o diálogo na Figura 10-9.

Selecione **Export configs to a directory** no menu suspenso, clique em **OK**, navegue até o local em que deseja salvar seus arquivos de configuração e clique em **Open** para salvar as configurações. Os arquivos de configuração exportados receberão o nome dos dispositivos em sua área de trabalho, como *R1_startup-config.cfg* e *IOU1_initial-config.cfg*. Para cada dispositivo IOS, você também verá um arquivo de configuração privado usado apenas pelo GNS3 e que contém chaves criptográficas SSH. Você não precisa fazer o upload para o seu roteador Cisco real. Esse método de exportação é um procedimento do tipo tudo ou nada que exporta todas as configurações do dispositivo no seu projeto. Para exportar a configuração de um único dispositivo, salve a configuração, clique com o botão direito do mouse no dispositivo em seu projeto e selecione **Export config**. O arquivo salvo será nomeado usando o nome do dispositivo.



Figure 10-9: Import/export tool for configuration files

Importando configurações do roteador Cisco para o GNS3

Agora, vamos ver como importar uma configuração de roteador Cisco em produção para GNS3. Comece fazendo logon no seu roteador Cisco real e salvando sua configuração no seu PC, usando FTP ou TFTP. Use um editor de texto para limpar qualquer discrepância no nome da interface. Em seguida, acrescente o nome do arquivo exportado com *.cfg* para garantir que o GNS3 possa reconhecer o arquivo. Se você ainda não o fez, salve seu projeto GNS3 e pare o roteador GNS3 que é o destino da importação. Por fim, clique com o botão direito do mouse no roteador GNS3 e escolha **Import config**. Navegue até o diretório em que você salvou o arquivo *.cfg* e selecione o arquivo para importá-lo para o roteador. Quando você reinicia o roteador GNS3, ele deve carregar e executar a configuração do IOS que você copiou do roteador Cisco em produção.

Nota

Ao mover as configurações para frente e para trás entre roteadores reais e o GNS3, talvez seja necessário executar alguma limpeza na configuração do IOS. Por exemplo, seu roteador GNS3 pode ter uma interface chamada FastEthernet 0/0, enquanto o roteador Cisco real possui uma interface chamada FastEthernet 0. Nesse caso, use um editor de texto e modifique o arquivo antes de importá-lo para o GNS3.

Copiando projetos GNS3 entre plataformas

Algum dia, você pode querer que seus projetos sejam executados em um PC que usa um sistema operacional diferente do seu PC existente. Se seus projetos GNS3 incluírem apenas roteadores e comutadores Dynamips IOS, você poderá copiá-los entre plataformas diferentes, como Windows e Linux, com o mínimo de esforço. Mas se eles são compostos por outros tipos de dispositivos, como IOU, QEMU ou VirtualBox, o processo pode ser complicado. De qualquer forma, mover um projeto entre plataformas é principalmente uma questão de copiar um ou mais projetos da sua antiga pasta de projetos do GNS3 para a pasta de projetos em um novo PC.

Projetos somente IOS

Se o seu projeto consistir apenas em roteadores Dynamips, quase nenhuma configuração adicional será necessária, desde que o computador de destino tenha arquivos de imagem compatíveis. Se o PC de destino estiver configurado com arquivos de imagem IOS diferentes ou as imagens estiverem armazenadas em um diretório diferente, o GNS3 deverá solicitar que você substitua o arquivo de imagem original por um que já esteja configurado no computador de destino, como mostra a Figura 10-10.

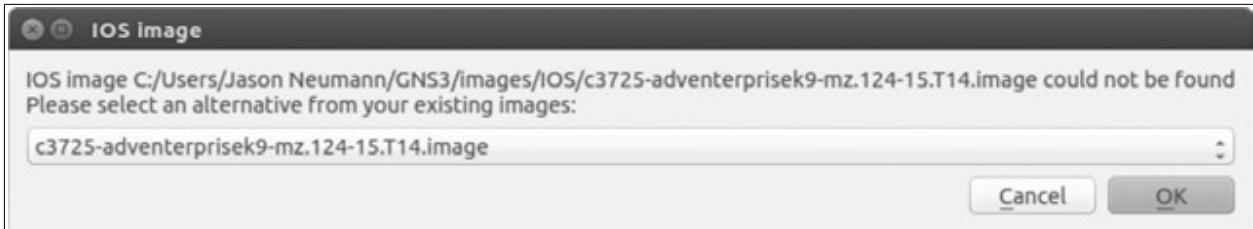


Figure 10-10: Substituting an IOS image file

Neste exemplo, você está movendo um projeto de um PC com Windows para um host Linux. Embora o arquivo *c3725-adventerprisek9-mz-124-15.T14.image* esteja configurado no host Linux na Figura 10-10, o GNS3 não conseguiu localizá-lo porque o Windows armazena arquivos de imagem do IOS usando um caminho diferente do Linux. Nesse caso, o GNS3 deve exibir uma lista de imagens IOS configuradas e permitem que você escolha um. Use o menu suspenso para selecionar uma imagem e clique em **OK**. Após selecionar a imagem, o GNS3 deve atualizar as informações do caminho no arquivo do projeto no PC de destino. Para tornar a alteração permanente, você precisa salvar seu projeto. Todas as configurações originais do IOS devem permanecer intactas e seu projeto deve ser executado conforme o esperado. Caso contrário, comece novamente e tente usar um arquivo de imagem diferente.

Projetos com dispositivos IOU

A cópia de projetos que contêm dispositivos IOU pode ser um pouco mais trabalhosa. O método mais fácil é recriar os dispositivos de IOU no projeto no PC de destino e fazer o upload da configuração original de IOU. Antes de copiar o projeto para uma nova plataforma, siga estas etapas:

1. Efetue logon em cada dispositivo IOU no projeto e copie a configuração em execução no arquivo *unix: initial-config.cfg*. Clique com o botão direito do mouse em um dispositivo IOU e escolha **Export config** para salvar a configuração. Certifique-se de copiar o arquivo de configuração exportado para o novo sistema ao copiar seu projeto.
2. Abra o projeto no PC de destino e resolva os problemas de substituição do arquivo de imagem do IOS (consulte a Figura 10-10).
3. No PC de destino, exclua o dispositivo IOU do seu projeto, adicione um novo um e vincule o dispositivo IOU a outros dispositivos do projeto usando as mesmas interfaces que o projeto original.

Para importar a configuração, siga estas etapas:

1. Clique com o botão direito do mouse no dispositivo IOU no PC de destino e clique em **Import config**.
2. Navegue até o diretório em que a configuração IOU está salva e selecione o arquivo. Faça isso para cada dispositivo IOU no seu projeto.
3. Quando terminar, inicie todos os dispositivos em seu novo projeto e verifique se tudo funciona conforme o esperado. Faça logon em cada dispositivo IOU e examine sua configuração. Se tudo parecer bom, salve seu projeto atualizado.

Por fim, vejamos a transferência de projetos que usam o VirtualBox.

Projetos com dispositivos VirtualBox

Se você estiver usando um dispositivo VirtualBox em seu projeto original, você precisará exportá-lo para um arquivo OVA. Inicie o VirtualBox e escolha **File>Export Appliance** para salvar o arquivo do dispositivo. Com o OVA preparado, siga estas etapas:

1. Copie o arquivo OVA para o novo PC, inicie o VirtualBox e escolha **File>Export Appliance** para importar o arquivo.
2. Inicie o GNS3 e adicione a máquina virtual VirtualBox em Preferências, conforme discutido em “*Importing Appliances*” na página 51.
3. Adicione o dispositivo ao seu projeto GNS3 e vincule-o a outros dispositivos, selecionando as mesmas interfaces que foram usadas no projeto original.

Quando você iniciar seu projeto no novo PC, seus dispositivos VirtualBox deverão ter a mesma configuração que tinham no PC antigo.

Explorando o console GNS3

O console de gerenciamento GNS3 fornece uma interface de linha de comando que você pode usar para controlar os dispositivos do projeto. Com base no console Dynagen original que foi escrito para o Dynamips, o console de gerenciamento foi adaptado e atualizado para o GNS3. Não abordarei todos os aspectos do console aqui, mas mostrarei algumas coisas mais úteis que você pode fazer com ele. Por padrão, o console de gerenciamento deve estar visível quando você inicia o GNS3. Caso contrário, selecione **View>Docks>Console** para exibir a janela do console.

No prompt de gerenciamento (=>), digite *help* ou um ponto de interrogação (?) para ver uma lista de comandos. Como você pode ver na lista a seguir, você pode executar tarefas familiares na CLI, como iniciar e parar dispositivos:

```
=> ?
```

Documented commands (type help <topic>):

```
=====
```

```
console  debug  help   reload  show   start  stop   suspend  version
```

Para exibir os detalhes e a sintaxe de um comando específico, digite *help* seguido de um nome de comando, conforme mostrado aqui:

```
=> help show
      Show detail information about every device in current lab:
      show device
```



```
      Show detail information about a device:
      show device <device_name>
```



```
      Show the whole topology:
      show run
```



```
      Show topology info of a device:
      show run <device_name>
```

O comando *show* oferece muitas opções diferentes para exibir informações sobre seus hypervisores, dispositivos e configurações. Por exemplo, o comando *show run* exibe todo o conteúdo do seu arquivo de configuração do projeto. Dois comandos úteis para testar redes são *suspend* e *start*. Juntos, eles podem ser usados para simular uma falha e recuperação do roteador.

Outro comando útil é o comando *debug*. Ele pode fornecer informações úteis quando um projeto não está sendo executado corretamente.

Criando projetos usando vários PCs

Você pode executar dispositivos usando vários PCs, permitindo distribuir a carga de recursos entre vários computadores. O compartilhamento de recursos permite que você use um PC para projetar seus projetos enquanto executa os dispositivos em um ou mais outros PCs. Isso significa que você pode criar e gerenciar seu projeto GNS3 usando uma estação de trabalho de ponta (como um laptop antigo) enquanto executa os dispositivos em um servidor de ponta. Se você usa vários servidores, pode criar um *uberlab* GNS3! Nesta seção, mostrarei como compartilhar recursos em uma configuração básica client/server e estratégias de cobertura para a criação de um *uberlab*. Desative os firewalls em todos os PCs antes de começar a configurar o compartilhamento de carga client/server (ou multiserver) e vamos começar.

Uma configuração Client/Server do Dynamips

Nesse cenário, você opera o GNS3 em um computador, enquanto outro servidor GNS3 é executado em outro PC. Se você estiver executando o GNS3 no OS X ou Windows, isso pode parecer familiar, porque é assim que a máquina virtual IOU funciona. A máquina virtual IOU é executada em um computador virtual e não em um PC separado, mas, caso contrário, o conceito é o mesmo.

Preparando suas estações de trabalho

Neste exemplo, usarei o Windows para o PC cliente e o Ubuntu Linux para o PC servidor. Comece instalando o GNS3 nas duas estações de trabalho. Uma estação de trabalho será o cliente, onde você configura e gerencia seus projetos, e a outra é o servidor. O servidor executará apenas roteadores Dynamips e deverá ter o melhor hardware, pois fará a maior parte do trabalho. Quanto mais poder de processamento e memória o servidor tiver, melhor será o desempenho dos seus dispositivos.

Inicie o GNS3 em cada computador e configure um arquivo de imagem do IOS. Isso permite executar roteadores Dynamips locais e remotos ao mesmo tempo e conectá-los em rede usando o GNS3 no PC cliente. Ao configurar o GNS3 no PC do servidor, certifique-se de registrar o caminho e o nome do arquivo do seu arquivo de imagem do IOS. No meu servidor Ubuntu, o caminho do arquivo de imagem é */home/jneumann/GNS3/images/IOS/c3725-adventerprisek9-mz.124-15.T14.image*. Você precisa dessas informações para configurar o roteador Dynamips remoto no PC cliente.

Em seguida, encontre o endereço IP de cada um dos seus PCs GNS3. Neste exemplo, meu PC cliente está configurado com o endereço IP 172.16.231.202 e meu PC servidor está configurado com o endereço IP 172.16.231.205. Após configurar o GNS3 e gravar as informações de IP e caminho da imagem, você estará pronto para começar.

Executando gns3server

Você deve executar o programa *gns3server* a partir do diretório de instalação. Faça logon no PC do servidor remoto e abra uma janela de terminal no Linux e OS X ou um prompt de comando se você estiver executando o Windows. No Windows, acesse o diretório *C:\ Arquivos de Programas\GNS3* e, no OS X, acesse o diretório */Applications/GNS3.app/Contents/Resources/Server/Contents/MacOS*. Ao iniciar o programa do servidor, você deve especificar o endereço IP do PC do servidor e o número da porta na qual o servidor escutará; digite o comando *gns3server --host server-ip --port port-number*. Se você não souber o endereço IP do seu PC servidor, pode ser preguiçoso e usar 0.0.0.0 e o *gns3server* escutará em todas as interfaces configuradas. No exemplo a seguir, inicie o programa *gns3server* no Ubuntu Linux no diretório */usr/local/bin/*.

```
$ gns3server --host 172.16.231.205 --port 8000
2015-06-06 18:32:45 INFO main.py:145 GNS3 server version x.x
2015-06-06 18:32:45 INFO main.py:147 Copyright (c) 2007-2015 GNS3 Technologies
Inc.
2015-06-06 18:32:45 INFO main.py:150 Config file /home/jneumann/.config/GNS3/
gns3_server.conf loaded
2015-06-06 18:32:45 INFO main.py:163 Running with Python 3.4.2 and has PID 3436
2015-06-06 18:32:45 INFO main.py:72 Current locale is en_US.UTF-8
2015-06-06 18:32:45 WARNING project.py:397 Purge old temporary project f3b11fb8
-82ed-42c1-b66a-226198ce6189
```

2015-06-06 18:32:45 INFO server.py:214 ① Starting server on 172.16.231.205:8000

Depois de iniciar o servidor, você verá resultados semelhantes, e se tudo correr bem, o servidor iniciará em 172.16.231.205:8000 ①, mostrado na última linha da saída. Isso indica que o programa do servidor está escutando no endereço IP 172.16.231.205 usando o número da porta 8000.

Nota

Se você deseja que o servidor GNS3 escute em algum outro número de porta, por exemplo, 8001, digite gns3server --host 172.16.231.205 --port 8001. Para ver uma lista completa das opções do servidor, digite gns3server --help na linha de comando.

Configurando o Cliente

Isso é tudo o que há para configurar o servidor, para que você possa voltar sua atenção para o cliente GNS3, um PC com Windows neste exemplo. No GNS3, selecione **Edit>Preferences** e selecione **GNS3 Server**, conforme mostrado na Figura 10-11.

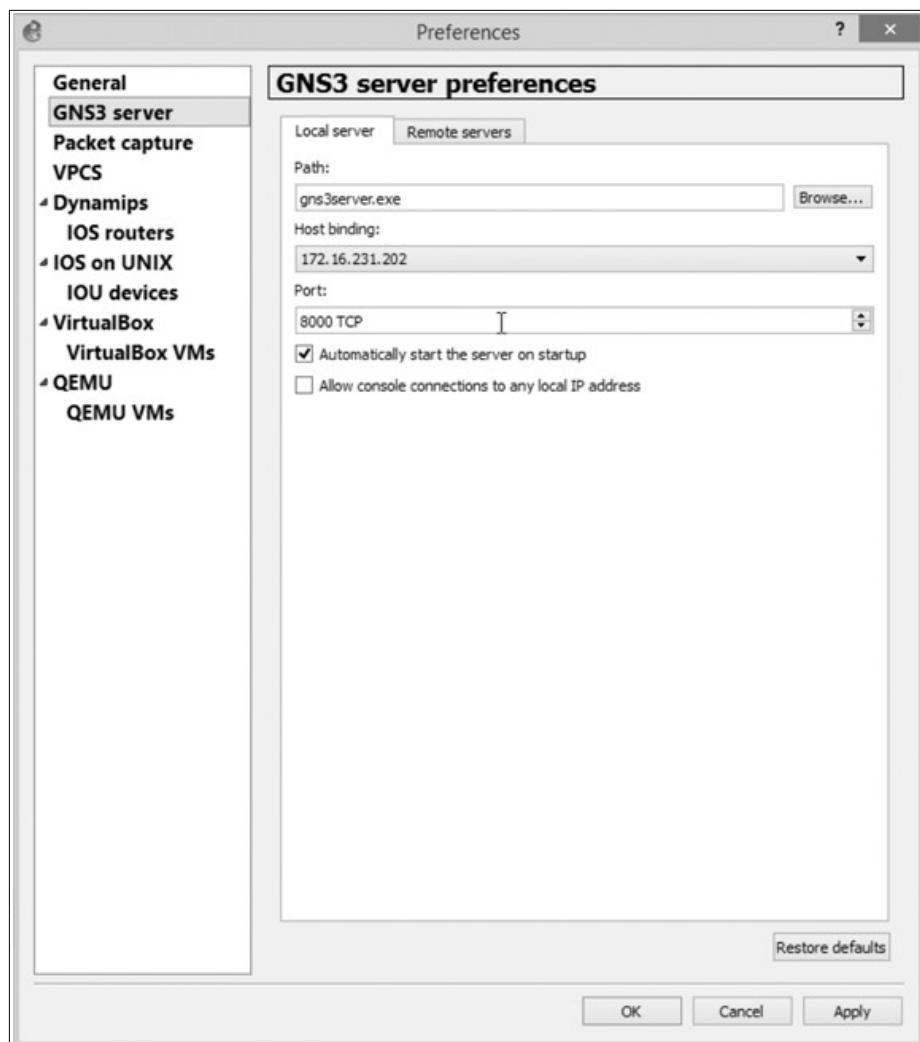


Figure 10-11: Setting the host binding to the IP address of the Ethernet adapter

Clique no menu suspenso **Host binding** e selecione o endereço IP de sua interface Ethernet. Neste PC, o endereço é 172.16.231.202. Clique em **Apply** para concluir a configuração. Em seguida, adicione o endereço IP do servidor remoto GNS3 à lista de servidores remotos no cliente. Clique na guia **Remote Servers**, como mostra a Figura 10-12.

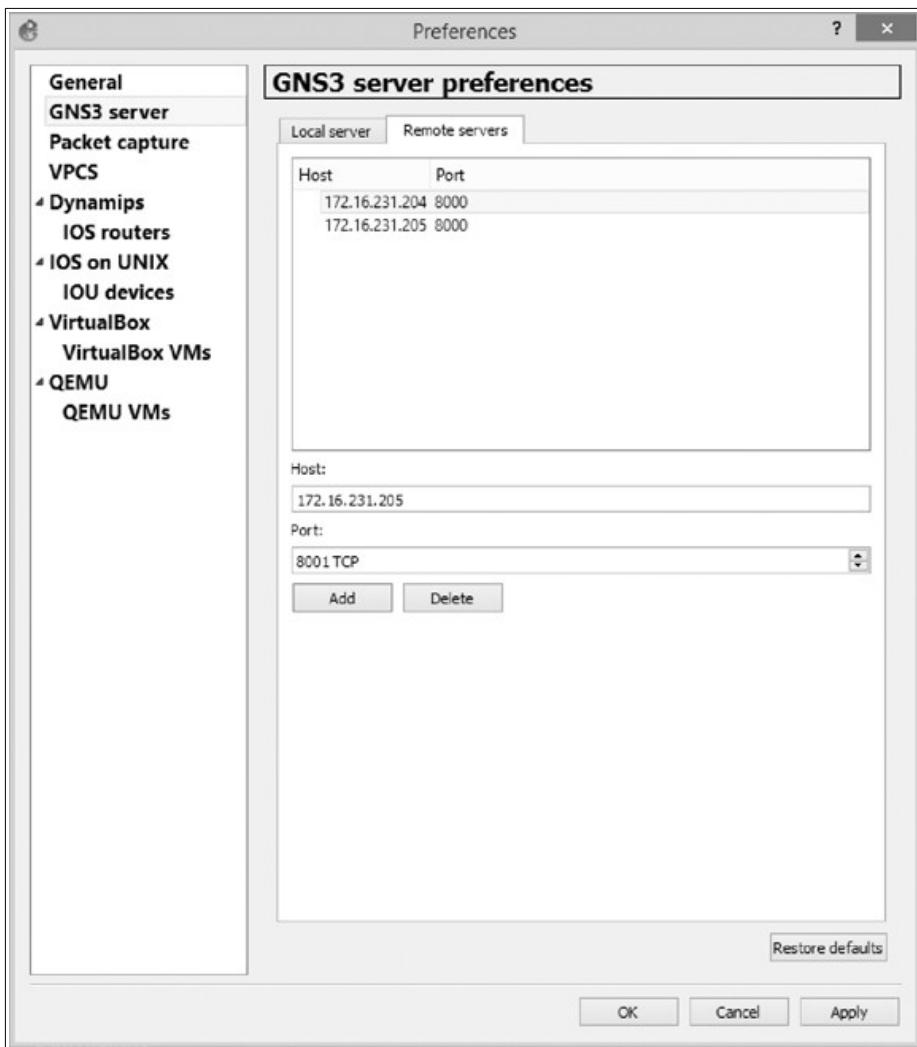


Figure 10-12: Configuring the remote server IP on the client host

No campo Host, digite o endereço IP do servidor GNS3 remoto. Neste exemplo, esse endereço IP é 172.16.231.205. O número da porta padrão deve ser 8000, mas você pode alterá-lo se tiver escolhido outro número de porta no PC remoto. Após adicionar o servidor remoto, clique em **Apply** para salvar as configurações. Em seguida, selecione **Dynamips** no menu lateral e clique na guia **General settings**, conforme mostrado na Figura 10-13. Desmarque a configuração **Use the local server** e clique em **Apply**. Isso garante que você tem a opção de selecionar um servidor remoto ao configurar um roteador Dynamips. Em seguida, clique em **IOS routers**, como mostra a Figura 10-14.

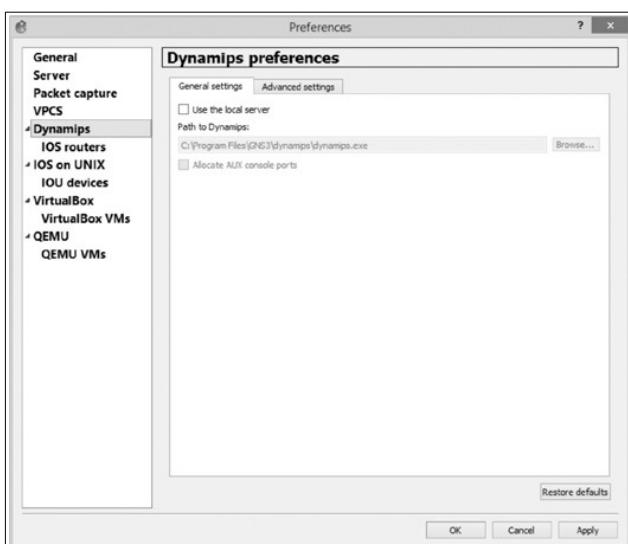


Figure 10-13: Dynamips server settings

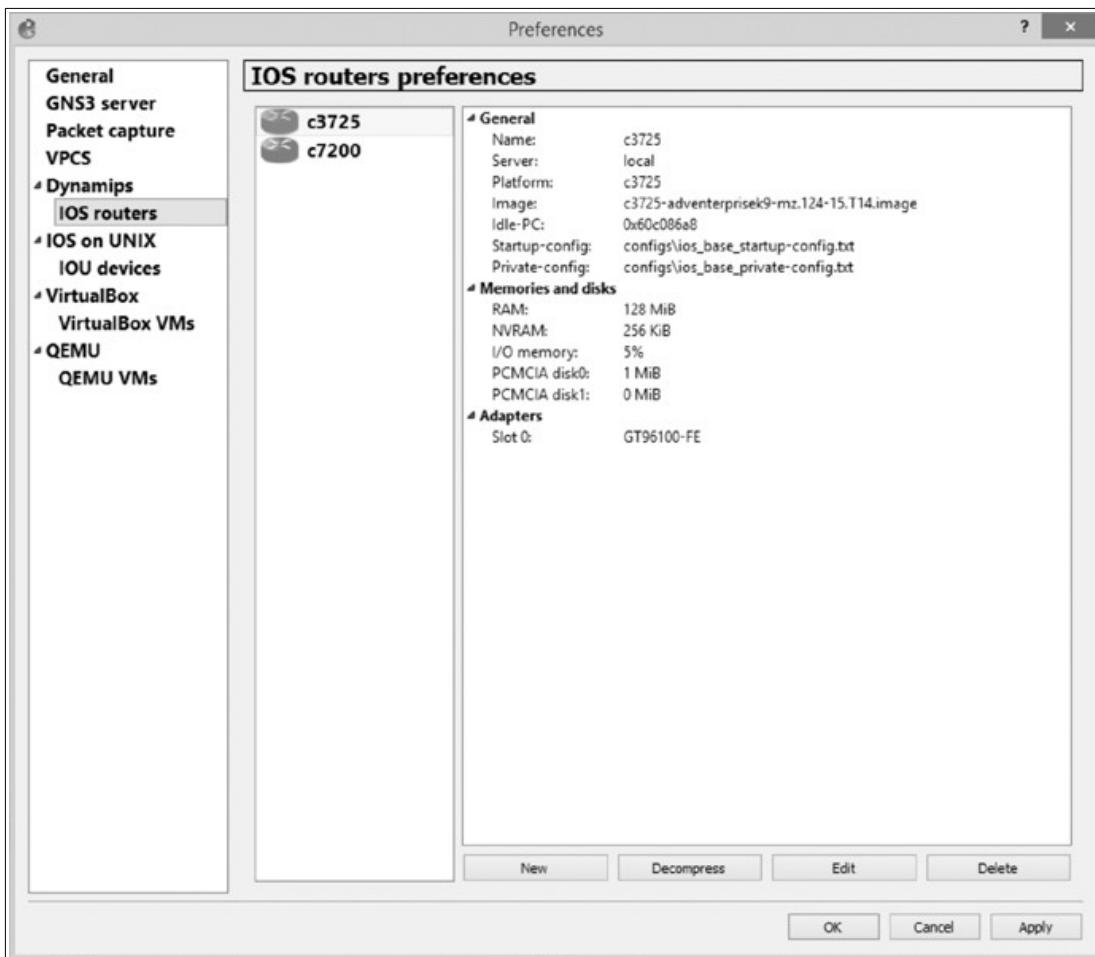


Figure 10-14: Configuring a remote Dynamips router

Clique em **New** para adicionar um roteador IOS remoto ao PC cliente, conforme mostrado em Figura 10-15.

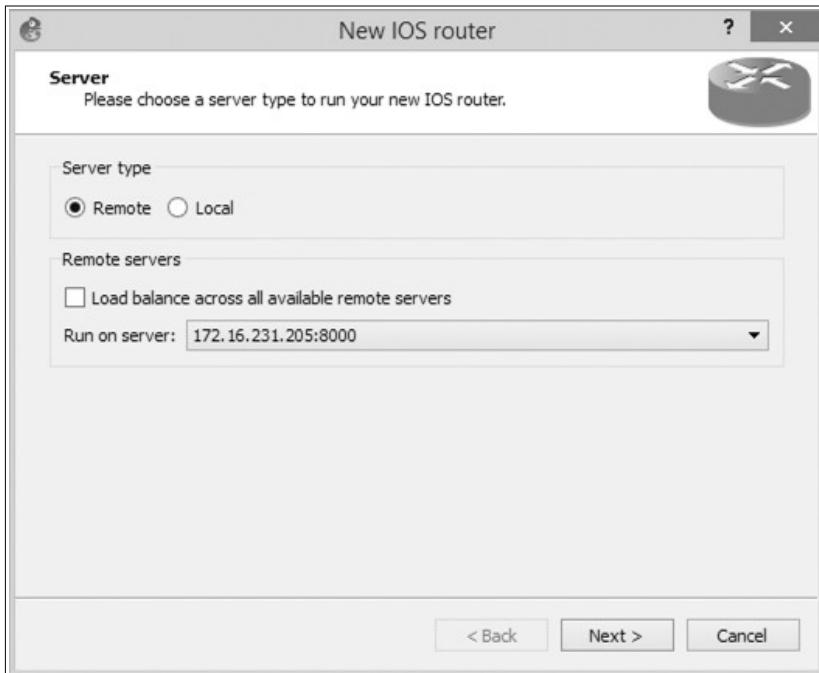


Figure 10-15: Selecting the Remote server type

Em **Tipo de servidor**, selecione **Remote** e desmarque **Load balance across all available remote servers**. Clique no menu suspenso **Run on Server**, selecione o endereço IP do servidor remoto na lista e clique em **Next** para continuar. Digite o caminho e o nome da imagem do IOS que você gravou no servidor remoto, como mostra a Figura 10-16.

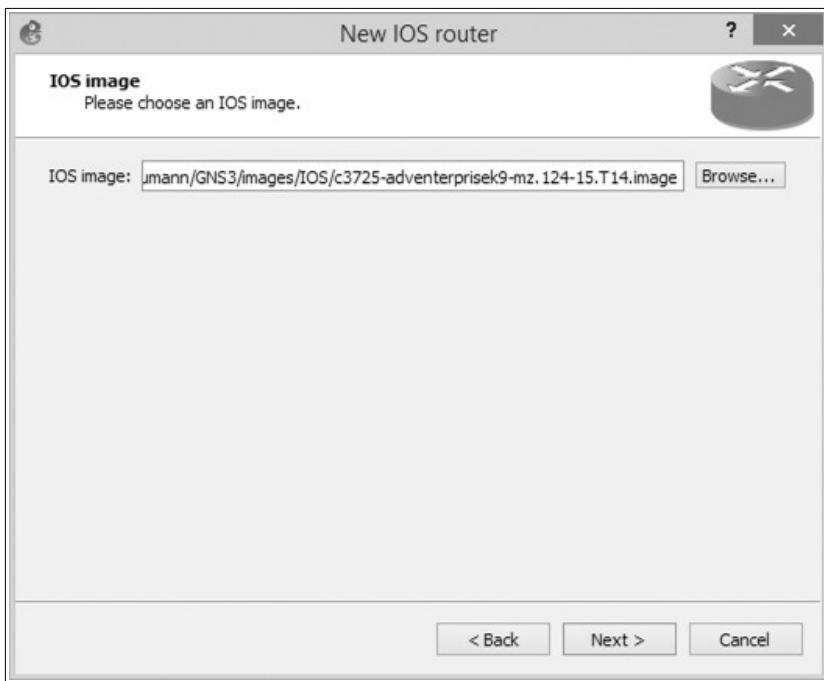


Figure 10-16: Entering the remote IOS image path

Depois de inserir o caminho e o nome do arquivo, clique em **Next** para continuar. Digite um nome no campo Nome do seu roteador, como mostra a Figura 10-17.



Figure 10-17: Naming your router

Chamei meu roteador de *c3725_on_Ubuntu* para poder identificá-lo facilmente na barra de ferramentas Dispositivos e sei pelo nome que ele está configurado para ser executado em um servidor remoto. Nesse ponto, você pode clicar nas opções restantes como se estivesse configurando um roteador Dynamips local. Certifique-se de inserir um valor de PC ocioso quando solicitado, ou calcule um se você ainda não o fez. Lembre-se de que os valores do PC ocioso são calculados por imagem, para que o mesmo valor possa ser usado em qualquer PC que esteja usando o mesmo arquivo de imagem do IOS. Quando você terminar de adicionar o roteador, ele deverá ser exibido na seção Roteadores da barra de ferramentas Dispositivos, conforme mostrado na Figura 10-18. Este exemplo possui dois roteadores c3725; um é um roteador local instalado no PC com Windows e o outro está instalado no servidor Ubuntu remoto. Ao criar um projeto, você pode usar os dois roteadores no mesmo projeto, reduzindo pela metade o consumo de CPU e memória no PC cliente. Agora que você sabe como configurar o GNS3 usando vários PCs, pode aproveitar a capacidade de criar grandes projetos GNS3.

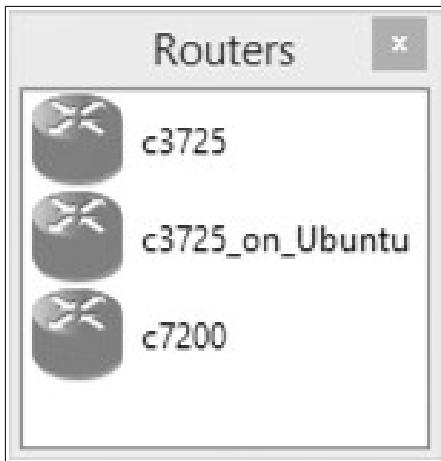


Figure 10-18: Routers section of the Devices toolbar

Executando QEMU em um servidor remoto

Além de executar roteadores IOU e IOS em um servidor remoto, você também pode executar o QEMU em um servidor remoto. Apenas certifique-se de instalar o QEMU no PC do servidor antes de começar. O processo de configuração de um dispositivo QEMU remoto no PC cliente é quase o mesmo que qualquer outro dispositivo remoto. No entanto, durante o New QEMU VM wizard, você precisará selecionar o arquivo binário QEMU para a máquina virtual, mostrado na Figura 10-19.

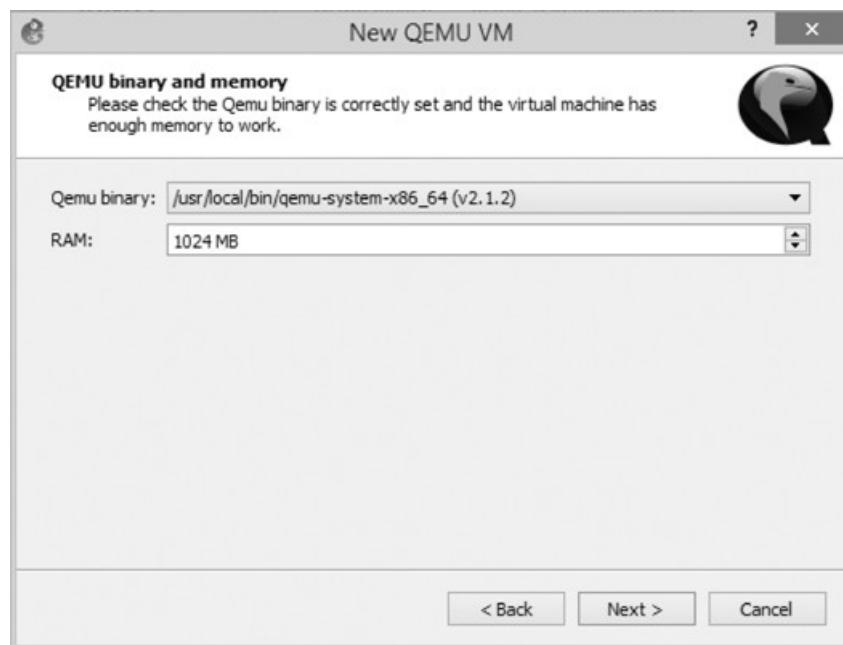


Figure 10-19: Configuring the QEMU binary

O GNS3 deve consultar o servidor remoto em busca de uma lista de arquivos binários QEMU instalados, e a máquina virtual que você cria deve ser executada no servidor remoto usando o arquivo binário selecionado. Use o menu suspenso para selecionar um arquivo binário para sua máquina virtual, geralmente qemu-system-i386 ou qemu-system-x86_64. Ajuste o tamanho da RAM e clique em Next. Configure as opções restantes como se a máquina virtual fosse um dispositivo local.

Criando um Uberlab GNS3

O GNS3 tem tudo a ver com escalabilidade, e você pode usá-lo para criar projetos realmente grandes com dezenas de switches e roteadores. Uma das melhores maneiras de criar um uberlab é usar vários servidores GNS3. Mas e se você tiver um computador muito rápido e alguns outros que também não funcionam? Nesse caso, convém executar mais dispositivos em uma máquina que na outra. Por exemplo, você pode executar a maioria dos seus roteadores no servidor high-end e executar menos dispositivos nas máquinas menos poderosas.

Um überlab não precisa se limitar a computadores executando em sua rede local. Se você estiver usando o GNS3 em uma rede corporativa com vários sites conectados por uma VPN, poderá usar o modelo de client/server para executar uma variedade de hypervisores de toda a cidade ou mesmo do país! Tudo o que você precisa fazer é iniciar o aplicativo *gns3server* em um computador remoto (pela VPN) e configurar seu cliente local usando o endereço IP do PC remoto. A única diferença entre isso e uma configuração regular de client/server é que os pacotes serão enviados pela VPN ao servidor remoto.

Laboratórios Nerd para diversão e lucro

Você explorou as ferramentas necessárias para configurar todos os tipos de projetos em GNS3, mas o que você deve fazer com esse novo conhecimento? Você pode estudar para obter certificações ou apenas se divertir! Nesta seção, discuto os dois. Muitos desses projetos são destinados a usuários avançados, mas sinta-se à vontade para modificá-los para criar projetos e desafios mais adequados ao seu nível de habilidade.

Preparando-se para os exames da Cisco

O GNS3 é uma ferramenta incrível para educação e certificação, e tem tudo o que você precisa para obter a certificação Juniper ou Cisco, desde o nível de entrada JNCIA ou CCNA até a jóia da coroa das certificações Cisco, o CCIE. Para exames de nível básico, como CCNA ou CCNP, comece pesquisando on-line para encontrar todos os tipos de exemplos de rede. Você pode até usar os vídeos CBT Nuggets ou Bryant Advantage com o GNS3. Seus vídeos são uma boa maneira de começar, e o GNS3 é uma ótima ferramenta para experimentar os conceitos que eles introduzem. Se você está estudando para o CCIE, convém usar algo como as pastas de trabalho do INE (<http://www.ine.com/>). Eles provaram ser líderes na preparação do laboratório do CCIE.

Protegendo suas redes

Hoje em dia, quase todo mundo armazena informações confidenciais em algum tipo de servidor de rede, portanto, ter uma infraestrutura de rede segura não é apenas uma boa idéia, é uma maneira de evitar perdas financeiras substanciais, processos indesejados e envolvimentos com erros e omissões de sua empresa Operadora de seguros (errors and omissions E&O). Nesta seção, descrevo alguns desafios relacionados à segurança que podem ser divertido e educativo e evita o roubo ou perda de dados.

O desafio "Hack My Rack"

Organize uma competição de segurança com seus amigos! Cada desafiante cria um projeto GNS3 em seu PC e aplica o máximo de segurança possível a seus dispositivos. O desafio é que cada usuário descubra a segurança dos outros usuários.

Depois que cada usuário cria sua própria rede em seu PC, eles têm permissão para instalar uma máquina virtual do VirtualBox no PC de seus amigos com todas as ferramentas de quebra de sistema que desejam usar. Quando os desafiantes terminam de criar suas redes, eles trocam de computador e iniciam o relógio. Agora começa a Batalha real! Use sua máquina virtual VirtualBox para invadir a rede GNS3 de outro desafiante.

Criando VPNs da Cisco

Crie uma VPN site-a-site da Cisco ou VPN multisite usando roteadores Cisco e dispositivos ASA. Tente configurar um roteador Cisco com hospedagem múltipla com failover de VPN. Nesse cenário, seus roteadores de borda WAN podem ter duas ou mais interfaces configuradas com o BGP para simular links WAN a um provedor de serviços de Internet. Um dia você pode querer um de sua preferência ou um cliente pode precisar de um. Aprender a fazê-lo no GNS3 é melhor do que descobrir durante a prestação de suporte ao seu cliente!

Praticando cenários do mundo real

As seguintes idéias de projeto foram projetadas para que você pense sobre a vida fora da caixa de areia do GNS3. Como administrador ou engenheiro de rede, você precisará entender o inter-funcionamento de redes com hospedagem múltipla, o design de blocos de Switches e a integração multiservidor, apenas para citar alguns. Projetar, executar e solucionar esses tipos de redes no GNS3 é uma excelente preparação para o mundo real.

Projeto de bloco de switch Cisco

Entender Switching é uma parte importante do gerenciamento de redes. Embora o roteador GNS3 EtherSwitch e a IOU tenham funcionalidade restrita, eles são úteis para configurar e testar blocos de switches redundantes com

protocolos como HSRP, VRRP e GLBP. Tente criar um bloco de switches de modelo de campus da Cisco totalmente redundante com acesso à Internet.

Redes com hospedagem múltipla

Embora muitas pequenas empresas se conectem à Internet usando um único endereço IP estático, empresas maiores precisam de mais IPs estáticos e links BGP para manter sua presença na Internet. Usando alguns roteadores GNS3 e BGP, você pode simular uma rede com hospedagem múltipla conectada a vários provedores de serviços da Internet. Adicione roteadores adicionais ao seu falso provedor de serviços de Internet para simular sites como <http://www.google.com/> ou <http://www.gns3.com/>. Em seguida, efetue ping nos sites falsos da sua rede com hospedagem múltipla.

Integração de múltiplos fornecedores

Crie um projeto usando Cisco, Juniper, Arista, Linux ou qualquer outro dispositivo roteável que você possa imaginar. Configure os dispositivos usando padrões abertos, como RIP, OSPF, BGP ou outros padrões abertos suportados por todos os fornecedores ou use a redistribuição de rotas para converter rotas de um dispositivo de fornecedor para outro. A idéia é aprender o máximo possível sobre a integração de vários fornecedores.

Use tudo, incluindo a "pia da cozinha"

Este projeto envolve tudo! É simples: crie o maior e mais incrível projeto que você pode imaginar. Use o maior número possível de PCs remotos e execute tudo o que o GNS3 tem a oferecer: roteadores, switches, ASAs, IDSs/IPSS da Cisco, Juniper, Firefly, Vyatta, Arista e qualquer outra coisa que você possa imaginar. Aplique todos os protocolos de roteamento e comutação e teste a conectividade de ponta a ponta usando *ping* ou *traceroute*. Certifique-se de configurar pelo menos um switch ATM, uma nuvem Frame Relay e uma VPN ou duas.

Quantos roteadores são necessários para apagar uma lâmpada?

Aqui está uma maneira divertida de obter direitos de se gabar. Desafie um amigo para ver cujo PC pode executar mais roteadores no GNS3. Com o valor ideal de PC ocioso, você pode executar mais de 100 antes de o Dynamips travar ou o GNS3 começar a ficar lento demais para usar. Um truque é executar o GNS3 no Linux porque o Dynamips parece ter uma escala melhor no Linux do que no Windows ou no OS X.

Routers Gone Rogue

Esse desafio de “mosca na sopa” é outra maneira de se divertir com um amigo. Cada desafiante constrói uma rede complexa usando quantos roteadores quiserem. Quanto mais melhor! As redes são então configuradas e exaustivamente testadas. Quando os dois desafiantes ficam satisfeitos por suas redes estarem funcionando corretamente, eles trocam de computador e interrompem as redes um do outro alterando algumas definições de configuração (soltando uma mosca na sopa). Uma interrupção pode ser tão simples quanto desligar uma interface ou tão complexa quanto filtrar rotas BGP. Tudo depende das habilidades dos indivíduos e da complexidade de suas redes. Depois que as redes são interrompidas, os concorrentes trocam os computadores novamente e cada um tenta ser o primeiro a analisar e reparar sua rede original.

Pensamentos finais

Um servidor de acesso virtual da Cisco exige algum trabalho para configurar, mas, uma vez configurado, é uma maneira fácil de gerenciar seus dispositivos. Se você possui um projeto pequeno que usa apenas alguns roteadores, pode não ser necessário. Mas se você precisar gerenciar algumas dezenas de dispositivos, ele rapidamente se tornará uma ferramenta inestimável. O GNS3 é executado em vários sistemas operacionais de PC, mas você não está preso ao que está usando no momento. Mover projetos entre sistemas é bastante simples, portanto, não tenha medo de tentar algo novo. O GNS3 foi projetado usando Linux e portado para Windows e OS X, por isso é excelente no Linux e geralmente usa menos recursos do que em execução no Windows.

Se você não possui o hardware de PC mais recente, pode equilibrar a carga de hipervisores em vários PCs e criar grandes projetos que executam melhor do que em um único PC. Essa também é uma ótima maneira de redirecionar os PCs抗igos que você possui em sua casa ou escritório. Mas a coisa mais importante a lembrar sobre o GNS3 é que é divertido usar porque você cria redes que, de outra forma, podem estar fora de seu alcance. Portanto, seja criativo e divirta-se!

A

Socorro! Eu cai e eu não consigo me levantar

O GNS3 é um programa complexo e, como qualquer coisa complexa, ocasionalmente se comporta de maneiras inesperadas. Eu já incluí dicas de solução de problemas ao longo do livro, portanto, neste apêndice, não fornecerei muitas informações de correção. Em vez disso, fornecerei estratégias básicas para resolver problemas e abordarei alguns problemas comuns e possíveis soluções.

Identificando o problema

Os problemas do GNS3 se enquadram amplamente em duas categorias.

Problemas repentinos Problemas que ocorrem com um projeto que estava funcionando anteriormente.

Problemas de recursos Problemas que ocorrem ao implementar um novo recurso.

Problemas súbitos aparecem do nada. Seu projeto pode estar funcionando bem há semanas e, de repente, ele não abre, ou quando abre, os dispositivos se recusam a iniciar. Os problemas de recursos geralmente ocorrem ao criar um novo projeto ou implementar um novo recurso em um projeto existente. Os dois tipos de problemas podem ser frustrantes e, se você usar o GNS3 por um período de tempo, provavelmente encontrará pelo menos um deles.

Problemas repentinos

Quando um projeto está funcionando bem e de repente desenvolve um problema, geralmente indica que algo mudou. Algo pode ter mudado no seu PC, no GNS3 ou no próprio projeto. Por parte do GNS3, pode ser que você tenha alterado inadvertidamente uma configuração ou feito alterações em um aplicativo auxiliar, como Dynamips, QEMU ou VirtualBox. Também pode significar que você atualizou para uma versão problemática do GNS3. Sempre que uma nova versão do GNS3 é lançada, é sempre bom testá-la usando um PC ou máquina virtual sobressalente antes de atualizar seu ambiente de produção. Esta seção fornece dicas para ajudar a corrigir alguns problemas repentinos.

Parando falhas de Dynamips

Um programa Dynamips instável pode resultar na perda de conexões com os dispositivos. Nesse caso, você poderá ver uma mensagem de erro do console GNS3 indicando que o Dynamips parou de funcionar, conforme mostrado na Figura A-1.

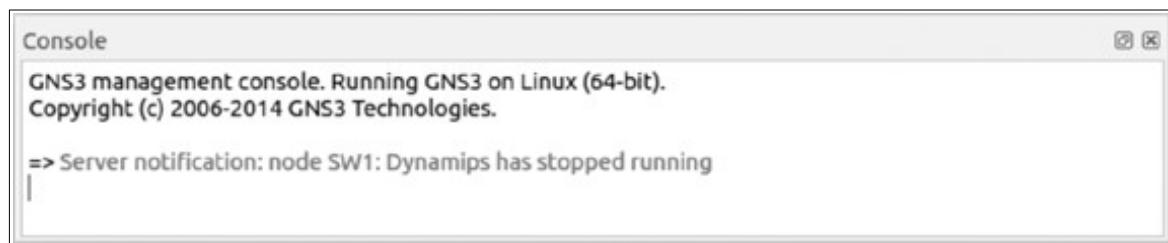


Figure A-1: Communication failure with Dynamips

Esta mensagem pode indicar que você está executando um software em seu PC que conflita com o Dynamips, que possui uma versão instável do Dynamips ou que não possui recursos livres suficientes para o PC, como ciclos de memória ou CPU. Tente fechar todos os aplicativos não essenciais, reiniciar o PC, desativar todos os softwares antivírus/antispam e desativar o firewall. Se o Dynamips continuar travando, talvez seja necessário reinstalar ou restaurar o Dynamips ou GNS3 a partir de um backup.

Quando as imagens IOS falham ao carregar

A memória do roteador é um problema comum que pode fazer com que os roteadores Dynamips se comportem mal. Quando um roteador se recusa a iniciar, verifique os requisitos de RAM da Cisco para a versão exata da imagem do IOS que você está usando - você pode ter atribuído muita memória ou insuficiente. Para verificar os requisitos, visite

o site do Cisco Feature Navigator; navegue para <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. A partir daqui, você pode usar o recurso Pesquisar por software para inserir os detalhes do seu IOS, e o navegador fornecerá os requisitos. Se a configuração de RAM de um roteador IOS estiver muito baixa, o roteador poderá falhar ao iniciar ou travar ao iniciar, e a janela do console GNS3 pode exibir uma mensagem de erro, como a mostrada na Figura A-2.



Figure A-2: Failed to load Cisco IOS image error message

Nesse caso, você deve reconfigurar o roteador e atribuir-lhe mais memória. Clique com o botão direito do mouse no roteador e selecione **Configure** para exibir o **GNS3 Node Configurator**. Escolha o nome do seu roteador no painel à esquerda e clique na guia **Memories and disks** para exibir a configuração de RAM. Se você aumentar a memória e o roteador ainda se recusar a iniciar, você pode ter um arquivo de imagem do IOS corrompido e deve tentar outro. Quando você tem um arquivo de imagem do IOS corrompido, ele pode não exibir nenhuma mensagem de erro na janela do console do GNS3. Em vez disso, o console do roteador pode não responder ou exibir informações que podem fornecer uma pista sobre o problema, como na Figura A-3.

A screenshot of a terminal window titled "R1". The window displays a series of error messages indicating multiple TLB (Store) exceptions. The text in the terminal is as follows:

```
PC = 0x8024ed44, Cause = 0x0000000c, Status Reg = 0x34400002 *** TLB (Store) Exception *** PC = 0x8024ed44, Cause = 0x0000000c, Status Reg = 0x34400002 *** TLB (Store) Exception *** PC = 0x8024ed44, Cause = 0x0000000c, Status Reg = 0x34400002 *** TLB (Store) Exception *** PC = 0x8024ed44, Cause = 0x0000000c, Status Reg = 0x34400002 *** TLB (Store) Exception *** PC = 0x8024ed44, Cause = 0x0000000c, Status Reg = 0x34400002 *** TLB (Store) Exception *** PC = 0x8024ed44, Cause = 0x0000000c, Status Reg = 0x34400002 *** TLB (Store) Exception *** PC = 0x8024ed44, Cause = 0x0000000c, Status Reg = 0x34400002 *** TLB (Store) Exception ***
```

Figure A-3: IOS image fails to load

A saída do console mostra que o IOS está lançando erros de exceção a uma taxa alarmante. Isso pode indicar que o arquivo de imagem do IOS está corrompido ou que foi configurado incorretamente no GNS3. Verifique e corrija as configurações de imagem usando o Cisco Feature Navigator ou substitua o arquivo de imagem, se necessário.

Resolvendo erros de memória IOS

Adicionar muita memória a um roteador Dynamips pode impedir que um roteador de inicializar corretamente. Por exemplo, a RAM máxima manipulada por um c7200 com NPE-400 é de 512 MB. Se você adicionar mais, digamos 1024 MB, poderá ver uma mensagem de erro na janela do console GNS3 ou a seguinte mensagem exibida no console do roteador:

!!! WARNING - VM is not running, will be unresponsive (status=1) !!!

A mensagem do console do roteador, **!!! WARNING - VM is not running, will be unresponsive (status=1) !!!** (**!!!! AVISO - A VM não está sendo executada, não responde (status = 1) !!!**), é uma indicação clara de que este roteador travou na inicialização. Nesse caso, pare o dispositivo e verifique sua configuração. O problema indicado aqui é que o dispositivo recebeu muita memória. Para corrigir o problema, reduza a quantidade de memória atribuída ao dispositivo ou substitua o arquivo de imagem do IOS por uma versão diferente. Mesmo quando um roteador parece funcionar corretamente, você pode encontrar erros ao configurar o IOS. Aqui está uma situação interessante em que um roteador é inicializado com êxito, mesmo com pouca memória, mas exibindo mensagens de erro durante a configuração:

```
R1(config-if)#ip nat inside
%NBAR ERROR: parsing stopped
%NBAR Error : Activation failed due to insufficient dynamic memory
%NBAR Error: Stile could not add protocol node
%NAT: Error activating CNBAR on the interface Vlan1
R1(config-if)#
*Mar 1 00:00:57.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0,
changed state to up
*Mar 1 00:00:57.251: %SYS-2-MALLOCFAIL: Memory allocation of 10260 bytes
failed from 0x62915CD4, alignment 0
Pool: Processor Free: 18968 Cause: Memory fragmentation
Alternate Pool: None Free: 0 Cause: No Alternate pool
-Process= "Exec", ipl= 0, pid= 195, -Traceback= 0x6148BFF8 0x60016604
0x6001C564 0x6001CBBC 0x636756E4 0x62915CDC 0x628F468C 0x628F88C4 0x628F5968
0x628F87A0 0x628F5968 0x628F8344 0x628F5968 0x628F5B2C 0x62928FBC 0x62933A20
R1(config-if)#
*Mar 1 00:00:57.275: %NBAR-2-NOMEMORY: No memory available for StILE lmalloc,
-Traceback= 0x6148BFF8 0x62915CF8 0x628F468C 0x628F88C4 0x628F5968 0x628F87A0
0x628F5968 0x628F8344 0x628F5968 0x628F5B2C 0x62928FBC 0x62933A20 0x62920BD0
0x6293DF70 0x6293E2F0 0x61C77C70
R1(config-if)#

```

Neste exemplo, o roteador R1 estava funcionando bem até que eu tentei configurar a conversão de endereços de rede. Como este roteador está com pouca memória, o Cisco IOS exibe imediatamente as mensagens de erro de alocação de memória. Atribuir mais memória ao roteador no GNS3 deve corrigir o problema.

Resolvendo erros de NIO

Os erros de NIO ocorrem com mais freqüência quando você tenta vincular um dispositivo GNS3 a um adaptador Ethernet físico no seu PC usando o Cloud node. Se você estiver com problemas para vincular dispositivos entre si ou com um Cloud node ou se receber uma mensagem de erro de NIO como a mostrada na Figura A-4, pode ter um problema de permissão.

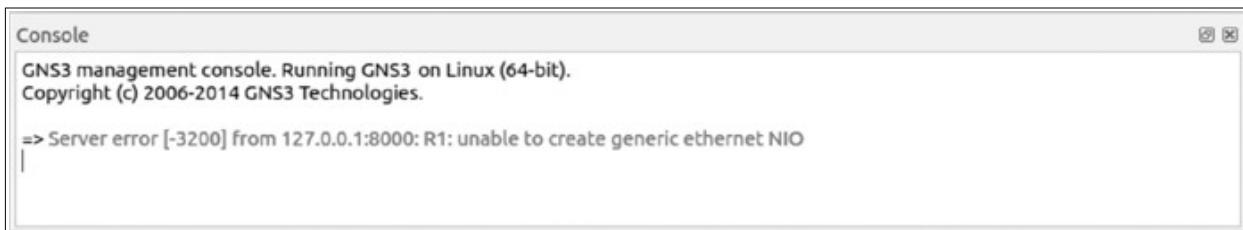


Figure A-4: Unable to create generic Ethernet NIO error message

Nesse caso, pode ser necessário atribuir a si mesmo privilégios elevados. E se você está executando o GNS3 no Windows, inicie o GNS3 usando a conta de administrador: clique com o botão direito do mouse no ícone GNS3 e selecione **Run as Administrator**. Se você estiver usando o OS X, pode ser necessário atribuir permissões de propriedade aos arquivos de dispositivo */dev/tap* ou */dev/bpf*, como no exemplo a seguir:

```
$ sudo chown $(id -un):$(id -gn) /dev/bpf*
$ sudo chown $(id -un):$(id -gn) /dev/tap*
```

Esses comandos atribuirão o ID do usuário atualmente conectado aos arquivos do dispositivo, permitindo que sua conta de usuário use os arquivos enquanto executa o GNS3. Você precisará definir essas permissões sempre que reiniciar o Mac, pois o OS X redefine todas as permissões de arquivo do dispositivo na inicialização. Para um alto grau de segurança, use o comando *setcap* para elevar os recursos do arquivo dynamips. No Ubuntu, pode ser necessário instalar o libcap2 antes de inserir o comando *setcap*.

```
$ sudo apt-get install libcap2
$ sudo setcap cap_net_raw,cap_net_admin+eip /usr/local/bin/dynamips
```

Considerações sobre segurança do Linux

Se você estiver executando o Linux, pode ser necessário executar o Dynamips com permissões elevadas. Para isso, existem dois métodos para escolher, dependendo da sua distribuição Linux. Você pode usar os comandos *chown* e *chmod* do Linux ou o comando *setcap*. Ambos os métodos devem resolver um problema de permissão, mas o método *chmod/chown* é menos seguro porque fornece ao aplicativo Dynamips a capacidade de executar com permissões completas no nível da root. Se um código malicioso entrar no Dynamips, toda a segurança do Linux poderá ser comprometida. O comando *setcap* do Linux permite atribuir recursos semelhantes de root de um arquivo, sem realmente fornecer permissões no nível de root do arquivo. Isso fornece à Dynamips as permissões de que ele precisa, sem comprometer a segurança do Linux mediante a assinatura excessiva de permissões de nível root. Portanto, é o método preferido para corrigir erros de GNS3 NIO. Infelizmente, o *setcap* não está disponível em todas as plataformas Linux, mas é suportado no Ubuntu e na maioria dos sistemas baseados em Debian.

Se você não conseguir usar o comando *setcap*, use os comandos *chown* e *chmod* para elevar o Dynamips com privilégios no nível de root.

```
$ sudo chown root /usr/local/bin/dynamips
$ sudo chmod 4755 /usr/local/bin/dynamips
```

Se você não conseguir conectar um dispositivo IOU a um adaptador físico ou um adaptador TAP virtual no Linux, tente aplicar os comandos *setcap* ao aplicativo iouyap. Isso funciona porque o iouyap é o software GNS3 que une dispositivos IOU a outros dispositivos GNS3, bem como interfaces virtuais e físicas. Aqui, você oferece a você os mesmos recursos elevados que você acabou de fornecer ao Dynamips:

```
$ sudo setcap cap_net_raw,cap_net_admin+eip /usr/local/bin/iouyap
```

Outro possível problema de NIO é o método escolhido para conectar o GNS3 ao seu adaptador Ethernet físico. Isto é especialmente verdade em PCs com Windows. Se você estiver usando o Windows 7, ao tentar conectar o GNS3 à Internet, crie uma Bridge usando seu adaptador Ethernet físico e um adaptador de loopback (descrito em “Conexão de dispositivos GNS3 à Internet” na página 120). Se você estiver executando o Windows 8, poderá obter melhores resultados se conectar o Cloud node diretamente ao seu adaptador Ethernet físico ou usar o compartilhamento de conexão com a Internet.

Corrigindo problemas do console

Os problemas do console podem impedir que um console se abra, faça com que ele abra e feche imediatamente, ou com uma ação lenta ou sem resposta ao configurar um dispositivo. Existem várias razões pelas quais uma conexão de console pode se comportar mal. Na maioria das vezes, o problema ocorre devido a configurações

incorretas no GNS3, como configurações do dispositivo QEMU ou configurações do VirtualBox, mas também pode ser um problema com uma imagem do dispositivo, como um arquivo de imagem IOU ou ASA corrompido.

Quando um console não abre, verifique primeiro a preferência do aplicativo de console GNS3. Abra **Preferências**, selecione **General** no painel à esquerda, clique na guia **Console Applications** e verifique se o tipo de terminal listado em Comandos pré-configurados corresponde ao programa de terminal do seu sistema operacional. Caso contrário, use o menu suspenso para selecionar seu terminal; depois clique em **Set**, **Apply** e **OK** para salvar a configuração.

Se você se desconectar imediatamente após abrir um console, seu firewall pode estar bloqueando a conexão de rede do aplicativo do console com o dispositivo GNS3. Se o dispositivo for um dispositivo QEMU, o problema geralmente está relacionado à própria máquina virtual QEMU ou à sua configuração. Primeiro, verifique se você atribuiu a quantidade correta de memória à máquina virtual QEMU. Você pode visitar os fóruns do GNS3 Jungle ou um site de um fornecedor de terceiros para verificar os requisitos do dispositivo. Se a alocação de memória estiver correta e o problema persistir, verifique as propriedades do dispositivo da máquina virtual QEMU. Vá para **Preferências** e selecione **QEMU VMs** no painel à esquerda. Selecione seu dispositivo QEMU na lista, clique em **Edit** e clique na guia **Advanced settings**. Verifique se as opções em Configurações adicionais estão corretas. Caso contrário, corrija a entrada e tente novamente.

Da mesma forma, você pode solucionar problemas de suas máquinas virtuais do VirtualBox examinando as configurações da máquina virtual. Vá para **Preferências** e selecione **VirtualBox VMs** no painel à esquerda. Selecione seu dispositivo VirtualBox na lista, clique em **Edit** e clique na guia **General settings**. Verifique se as opções **Enable Remote Console** e **Start VM in Headless Mode** estão configuradas corretamente para sua máquina virtual VirtualBox.

Se o console estiver lento quando você iniciar um roteador Dynamips, o roteador pode não ter sido atribuído a um valor ideal de PC ocioso(*Idle-PC value*). Um valor de PC ocioso mal escolhido pode ser tão devastador em sua CPU quanto não ter nenhum valor definido. Para verificar ou definir seu valor de PC inativo, clique com o botão direito do mouse no roteador, selecione **Configure** para abrir o Configurador de nodes e verifique seu valor de PC inativo na guia **Advanced**. Se o roteador recebeu um valor de PC ocioso e o dispositivo está consumindo muita CPU, pode ser necessário recalcular o valor. (Consulte “Configurando um valor manual do PC ocioso” na página 26.)

Seu console também pode ficar lento se você alterou alguma das configurações avançadas de otimização do Dynamips, como Idlemax ou Idlesleep. Idlemax e Idlesleep são usados em conjunto com o valor Idle-PC; Idlemax determina quantas vezes dormir durante a execução de loops ociosos no código do roteador, e o valor Idlesleep determina quanto tempo dorme. Tente redefini-los para seus valores padrão clicando no botão **Reset**, como mostra a Figura A-5.

A equipe de desenvolvimento do GNS3 determinou que os valores padrão Idlemax e Idlesleep são ideais para a maioria dos usuários, mas você pode conseguir um desempenho um pouco melhor da CPU alterando-os conforme descrito em “Conservando recursos” na página 214.

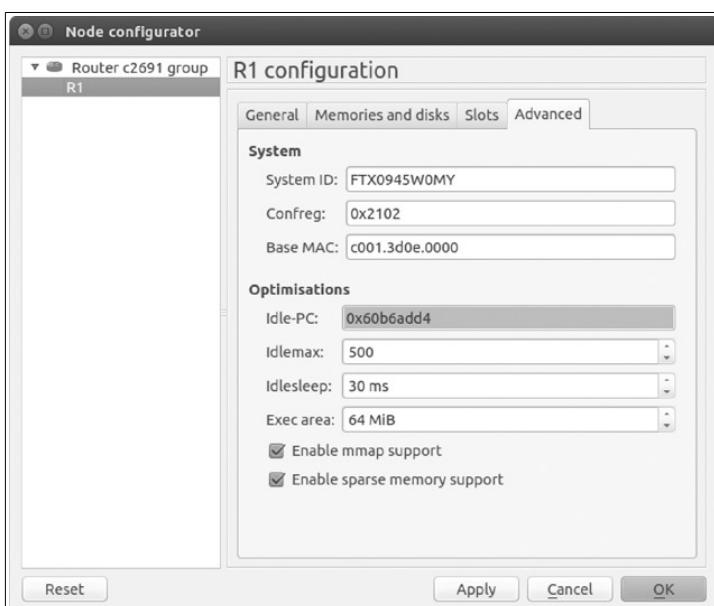


Figure A-5: Advanced router configuration

Se o console lento for um dispositivo de IOU e você estiver usando a máquina virtual de IOU (necessária para Windows e OS X), tente atribuir mais memória à máquina virtual de IOU no VirtualBox.

Problemas de recursos

Os problemas de recursos ocorrem quando você tenta implementar um recurso do GNS3 que você não usou antes e geralmente resultam de algum tipo de erro do usuário. O GNS3 possui muitos recursos e opções, e os projetos podem se complicar rapidamente, principalmente quando você executa o GNS3 usando vários PCs ou quando adiciona máquinas virtuais QEMU e VirtualBox aos seus projetos. Os problemas de recursos também podem estar na configuração de seus dispositivos.

Problemas de configuração

Se você estiver enfrentando um problema de roteamento de rede em um projeto, pode ser que tenha cometido um erro ao configurar o sistema operacional de rede do seu dispositivo; afinal, o GNS3 é uma ferramenta de aprendizado e você cometerá erros ao longo do caminho. Ao configurar recursos usando sistemas operacionais como Arista, IOS e Junos OS, é fácil cometer um erro que pode interromper sua rede. Verifique as configurações do seu dispositivo e verifique se você não atribuiu a máscara de sub-rede errada a um endereço IP ou se esqueceu de criar uma interface. Uma maneira de evitar esse tipo de problema é configurar os dispositivos do projeto GNS3 da mesma maneira que você faria em uma rede real. Comece com alguns dispositivos, configure e teste-os e continue adicionando e testando dispositivos até criar um projeto totalmente funcional.

Usando imagens IOS não suportadas

Em resumo, não tente usar imagens não suportadas. O Dynamips suporta um número limitado de roteadores Cisco (consulte o Apêndice B para obter uma lista completa). Se você vir um erro de imagem não suportado, como mostra a Figura A-6, ao tentar instalar um arquivo de imagem, é porque o arquivo de imagem não é suportado pelo GNS3.

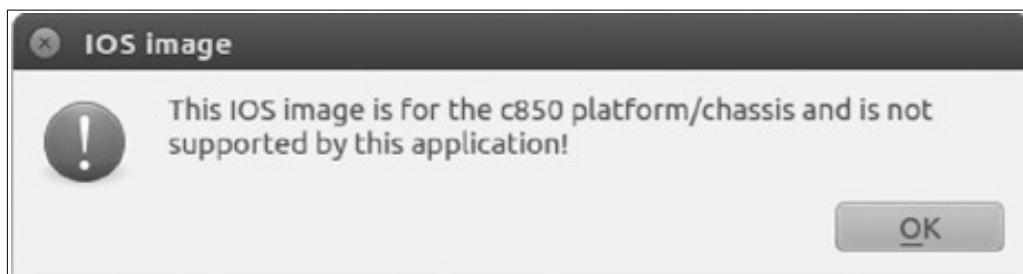


Figure A-6: Unsupported IOS image error

Na Figura A-6, tentei usar um arquivo de imagem de uma plataforma de roteador Cisco c850 não suportada pelo GNS3. A única opção quando você vê essa mensagem de erro é descartar o arquivo e substituí-lo por um que seja suportado pelo GNS3.

A opção nuclear

Se você continuar tendo problemas com o GNS3 depois de tentar as ações discutidas até o momento, poderá usar a opção nuclear como último recurso e limpar o arquivo de configurações do GNS3. Depois de destruir o arquivo, você perderá todas as configurações do GNS3 e precisará reconfigurar o GNS3 como se fosse um sistema recém-instalado.

NOTA

Nenhum dos seus projetos salvos deve ser afetado pela limpeza do arquivo de configurações do GNS3, nem os dispositivos VirtualBox ou QEMU nesses projetos.

Antes de começar, faça backup do seu arquivo de configuração existente. Isso lhe dará a opção de retornar às configurações antigas, se necessário. Vá para **Preferences** e escolha a preferência **General**; em seguida, na nova janela, selecione a guia **General**, como mostra a Figura A-7.

O arquivo de configurações do GNS3 é exibido no arquivo de configuração ①. Para fazer backup do arquivo, clique no botão **Export** ③. Escolha um nome e um local para salvar o arquivo. Observe a localização do arquivo

original (*neste exemplo, é /home/jneumann/.config/GNS3/gns3_gui.conf*) e, quando a exportação estiver concluída, feche o GNS3 e exclua ou renomeie esse arquivo original. Agora, quando você reabrir o GNS3, todas as preferências serão limpas como se você o tivesse instalado pela primeira vez. Se você decidir que limpar o arquivo foi um erro, você pode usar **Import** ② para restabelecer o arquivo de configurações original do GNS3.

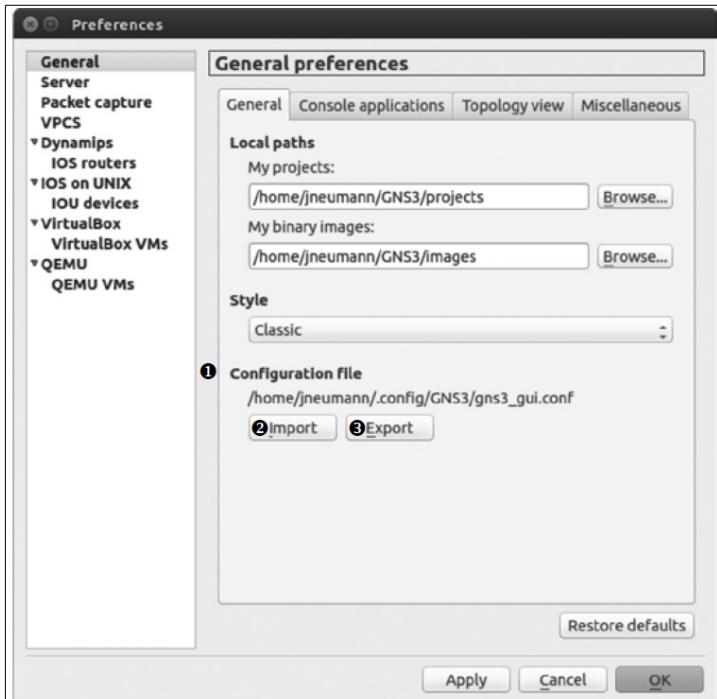


Figure A-7: Exporting and clearing the GNS3 configuration file

NOTA

Em raras ocasiões, o arquivo de configurações do GNS3 pode ser corrompido. Mantenha um backup atual do seu arquivo de configurações do GNS3 o tempo todo, para poder reverter para uma versão funcional, se necessário.

Hardware Sobrecarregado

Quando o GNS3 está lento e os dispositivos estão travando, pode ser uma pista de que você está sobrecarregando o processador do seu PC com muitos dispositivos; isso certamente diminuirá a resposta do console e pode causar falha no Dynamips. Se for esse o caso, considere reduzir o seu projeto, atualizar o seu PC ou usar vários PCs com o GNS3. Uma ótima maneira de criar grandes projetos sem sobrecarregar sua CPU é carregar seus hypervisores em vários PCs, conforme descrito em “Criando projetos usando vários PCs” na página 191.

Resolvendo conflitos de número de porta

Em algum momento, outro software no seu computador provavelmente entrará em conflito com o GNS3. Isso geralmente acontece quando o software está usando um número de porta que o GNS3 precisa. Se o número da porta usado for o mesmo que o aplicativo do servidor GNS3, o GNS3 será carregado, mas o servidor deverá selecionar outro número de porta. Quando isso acontecer, investigue o problema usando o comando *netstat*, que deve estar incluído nos sistemas baseados no Windows e no Unix, como Linux e OS X.

```
$ netstat -an|more
```

Active Internet connections (servers and established)					
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.1.1:53	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8000	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:39191	127.0.0.1:8000①	TIME_WAIT
tcp6	0	0	::1:631	::*	LISTEN
tcp6	1	0	::1:53974	::1:631	CLOSE_WAIT
udp	0	0	0.0.0.0:59759	0.0.0.0:*	
udp	0	0	0.0.0.0:39309	0.0.0.0:*	
udp	0	0	127.0.1.1:53	0.0.0.0:*	
udp	0	0	0.0.0.0:68	0.0.0.0:*	
udp	0	0	0.0.0.0:631	0.0.0.0:*	
udp	0	0	0.0.0.0:5353	0.0.0.0:*	
udp6	0	0	::::57463	::*	
udp6	0	0	::::45876	::*	
udp6	0	0	::::5353	::*	

O número da porta TCP 8000 ① é o número da porta padrão reservado para o Programa do servidor GNS3, mas a saída *netstat* mostra que outro aplicativo está usando essa porta. Para resolver esse problema, localize o aplicativo incorreto e feche-o ou altere o número da porta padrão usado pelo GNS3. Para alterar o número da porta, vá para **Preferences>Servers>Local Server Port** e defina o número da porta como algo diferente de 8000, como 8001.

Pesquisando defeitos um ASA

Quando você instala um ASA no GNS3, certifique-se de selecionar **ASA 8.4 (2)** no menu suspenso **Type** durante o assistente de instalação. O assistente GNS3 deve preencher automaticamente os campos obrigatórios com as informações corretas. Se o seu ASA estiver configurado corretamente, mas travar ou funcionar mal, o ASA pode estar causando um alto uso da CPU, o que, por sua vez, causa um prejuízo no desempenho geral do seu PC. Você pode reduzir bastante o uso da CPU ajustando a porcentagem limite da CPU para o seu ASA. Vá para **Preferences**, selecione seu ASA, clique em **Edit** e ative **CPU throttling**. Tenha cuidado, porém, porque limitar demais o uso da CPU do ASA também pode fazer com que um ASA deixe de responder. Para obter os melhores resultados, tente ajustar a configuração até encontrar um ponto ideal que reduz o uso da CPU sem afetar negativamente o desempenho.

Conservando Recursos

No geral, o GNS3 faz um bom trabalho ao lidar com projetos de quase qualquer tamanho, desde que você tenha os recursos de hardware adequados, mas quanto maior o seu projeto, maior a probabilidade de encontrar problemas. A melhor maneira de evitar esses problemas é adotar uma abordagem minimalista ao criar um projeto e evitar adicionar complexidade desnecessária aos seus projetos.

Selecione os dispositivos cuidadosamente

No GNS3, sempre escolha dispositivos que usem a menor quantidade de RAM e consumo de CPU. Por exemplo, evite usar um roteador c7200, que requer 512 MB de RAM, se você puder usar um roteador c3700 que use apenas 128 MB. Ao usar dispositivos Dynamips, use o mesmo modelo de dispositivo para todos os roteadores no seu projeto; O GNS3 pode compartilhar recursos entre eles. O uso de vários modelos de roteadores diferentes pode levar ao consumo de recursos e ao baixo desempenho. Você também pode usar dispositivos emulados, como o Ethernet Switch node em vez de um roteador EtherSwitch, para economizar memória e processador.

Otimizar valores de Idle-PC(PC ocioso)

Para reduzir o uso de recursos do sistema, ajuste os valores do PC ocioso. Seus valores atuais podem ser bons quando você estiver executando um pequeno número de dispositivos IOS, mas projetos maiores se beneficiarão de valores mais otimizados. Para encontrar os melhores valores para você, primeiro coloque seu computador em uma estado inativo: reinicie-o e feche todos os programas, incluindo software antivírus. Se você estiver usando o Windows, feche o máximo de aplicativos da bandeja do sistema. Quando estiver pronto, adicione um roteador à sua área de trabalho, inicie-o, clique com o botão direito do mouse no roteador e escolha PC inativo para começar a calcular os

valores do PC inativo. Durante o processo, monitore cuidadosamente sua CPU após aplicar cada novo valor e registre todos os valores. Procure o que utiliza menos recursos e, quando o encontrar, aplique-o ao dispositivo.

Fazendo backup de seus projetos

É importante fazer backup dos seus projetos GNS3, principalmente porque eles se tornam mais complexos e levam mais tempo para serem criados. Ninguém gosta de perder o trabalho que passou horas criando! Você pode fazer backup de toda a pasta GNS3, fazer backup da pasta de projetos ou fazer backup de pastas de projeto individuais. O backup regular de toda a pasta GNS3 é a melhor maneira de garantir que você sempre tenha uma cópia atual de todos os projetos e imagens, mas isso pode consumir muito tempo e exigir uma quantidade razoável de espaço em disco.

Se você tiver pouco tempo ou recursos, faça pelo menos o backup de projetos individuais da pasta de projetos. Verifique se você ainda possui uma cópia de backup de toda a pasta GNS3 e atualize o backup completo do GNS3, copiando projetos individuais para o backup, conforme necessário. A desvantagem dessa abordagem é que ela depende de você se lembrar de copiar projetos novos ou atualizados toda vez que atualiza seu backup, e você pode esquecer de fazer o backup de um projeto importante. Sei por experiência própria que descobrir que você acabou de perder todo o trabalho que você coloca em um projeto complexo pode ser uma revelação preocupante.

Sugiro uma estratégia de backup completa, bem como fazer backup de projetos individuais conforme você os cria. Você pode criar grandes projetos em fases e testar cada componente ao longo do caminho e, depois de ter um grupo de componentes funcionando corretamente, faça o backup do projeto. Em seguida, repita esse procedimento até que o projeto esteja totalmente configurado e sua rede esteja funcional. O emprego de capturas instantâneas do GNS3 durante a criação de projetos complexos também pode ser útil: se você cometer um erro, volte ao estado de funcionamento restaurando uma captura instantânea (consulte “Usando a barra de ferramentas GNS3” na página 34). Mas, independentemente da estratégia de backup escolhida, a maneira mais simples de armazenar os arquivos do projeto de backup é copiando toda a pasta do projeto em um grande pen drive ou disco rígido externo.

Bem vindo a selva

Quando um problema é grande demais para você descobrir por conta própria, não tenha medo de pedir ajuda. O site do GNS3 (<http://www.gns3.com/>) fornece uma infinidade de informações e abriga um fórum dedicado, chamado GNS3 Jungle. Aqui você pode relatar problemas, fazer perguntas e ajudar outros usuários com suas perguntas. Para acessar o GNS3 Jungle, accesse o site GNS3 e selecione **Community**. Antes de postar uma pergunta, pesquise no site para ver se sua pergunta já foi feita e respondida. O GNS3 Jungle possui uma base de membros extremamente ativa; portanto, as perguntas geralmente recebem respostas rápidas. Se você postar uma pergunta e ela não receber uma resposta tão rapidamente quanto gostaria, não a repasse ou responda à sua própria postagem para aumentar a lista. Postar a mesma pergunta várias vezes confundirá apenas as pessoas que tentam ajudar. Geralmente, quando uma pergunta fica sem resposta, é porque ninguém que atualmente está vendo o fórum tem a resposta. Seja paciente e alguém deve responder no devido tempo.

Ao fazer uma pergunta, Eu recomendo fornecer as seguintes informações:

- versão GNS3
- Nome e versão do seu sistema operacional
- Específicos da plataforma (32 ou 64 bits, processador e RAM)
- Uma descrição clara do problema
- Uma captura de tela das mensagens de erro (se aplicável)
- Uma captura de tela das configurações de preferência (se aplicável)
- Topologia (se aplicável)
- Configurações do dispositivo (se aplicável)

Informação detalhada ajuda seus colegas usuários do GNS3 a determinar seu problema e a devolver uma solução mais rapidamente.

Pensamentos finais

Embora o GNS3 geralmente funcione bem, problemas surgem de tempos em tempos. Neste apêndice, você examinou alguns problemas comuns e estratégias básicas de solução de problemas para corrigir esses problemas. Você aprendeu que firewalls, software antivírus, e, ocasionalmente, um aplicativo baseado em TCP / IP pode causar estragos no GNS3. Em caso de dúvida, desative o firewall, desative o software antivírus e feche os programas desnecessários antes de iniciar o GNS3. Você também aprendeu que muitas vezes a maneira mais rápida de consertar um projeto com defeito é restaurar o projeto de um backup. Você sempre deve manter uma cópia de backup atual de toda a pasta GNS3 e do arquivo de configurações do GNS3. Restaurar dados de um backup é a maneira mais segura de começar a funcionar após um desastre.

B

Hardware Cisco Compatível com GNS3

Este apêndice lista o hardware da Cisco suportado pelo Dynamips e GNS3. O Dynamips emula apenas roteadores Cisco que usam a arquitetura MIPS e não suporta todos os modelos da Cisco. Após a lista de roteadores suportados, você encontrará uma lista de arquivos de imagem IOS recomendados que o GNS3 pode aplicar automaticamente os valores corretos de Idle-PC sem executar um cálculo de PC ocioso.

Cisco Hardware suportado

No GNS3, você pode emular os roteadores Cisco de cinco séries diferentes (1700, 2600, 3600, 3700 e 7200), com graus variados de suporte a recursos.

Table B-1: 1700 Series Routers

Model	Slots	WIC	Card Support
1720, 1721, 1750, and 1751	One (none available) CISCO1710-MB-1FE-1E in Slot 1 provides one Fast Ethernet: F0	None	None
1760	One (none available) C1700-MB-1ETH in Slot 1 provides one Fast Ethernet port: F0	Two	WIC-1T (1 serial port) WIC-2T (2 serial ports) WIC-1ENET (1 Ethernet port)

Table B-2: 2600 Series Routers

Model	NM Slots	WIC	Card Support
2610	One (one available) CISCO2600-MB-1E in Slot 1 provides one Ethernet port: F0/0	Two	NM-1FE-TX (1 Fast Ethernet port) NM-1E (1 Ethernet port) NM-4E (4 Ethernet ports) NM-16ESW (16 port switch) WIC-1T (1 serial port) WIC-2T (2 serial ports)
2611	Two (one available) CISCO2600-MB-2E in Slot 1 provides two Ethernet ports: F0/0 and F0/1	Two	NM-1FE-TX (1 Fast Ethernet port) NM-1E (1 Ethernet port) NM-4E (4 Ethernet ports) NM-16ESW (16 port switch) WIC-1T (1 serial port) WIC-2T (2 serial ports)

Table B-2: 2600 Series Routers

Model	NM Slots	WIC	Card Support
2620	Two (one available) CISCO2600-MB-1FE in Slot 1 provides one Fast Ethernet port: F0/0	Two	NM-1FE-TX (1 Fast Ethernet port) NM-1E (1 Ethernet port) NM-4E (4 Ethernet ports) NM-16ESW (16 port switch) WIC-1T (1 serial port) WIC-2T (2 serial ports)
2621	Two (one available) CISCO2600-MB-2FE in Slot 1 provides two Fast Ethernet ports: F0/0 and F0/1	Two	NM-1FE-TX (1 Fast Ethernet port) NM-1E (1 Ethernet port) NM-4E (4 Ethernet ports) NM-16ESW (16 port switch) WIC-1T (1 serial port) WIC-2T (2 serial ports)
2610XM	Two (one available) CISCO2600-MB-1FE in Slot 1 provides one Fast Ethernet port: F0/0	Two	NM-1FE-TX (1 Fast Ethernet port) NM-1E (1 Ethernet port) NM-4E (4 Ethernet ports) NM-16ESW (16 port switch) WIC-1T (1 serial port) WIC-2T (2 serial ports)
2611XM	Two (one available) CISCO2600-MB-2FE in Slot 1 provides two Fast Ethernet ports: F0/0 and F0/1	Two	NM-1FE-TX (1 Fast Ethernet port) NM-1E (1 Ethernet port) NM-4E (4 Ethernet ports) NM-16ESW (16 port switch) WIC-1T (1 serial port) WIC-2T (2 serial ports)
Model	NM Slots	WIC	Card Support
2620XM	Two (one available) CISCO2600-MB-1FE in Slot 1 provides one Fast Ethernet port: F0/0	Two	NM-1FE-TX (1 Fast Ethernet port) NM-1E (1 Ethernet port) NM-4E (4 Ethernet ports) NM-16ESW (16 port switch) WIC-1T (1 serial port) WIC-2T (2 serial ports)
2621XM	Two (one available) CISCO2600-MB-2FE in Slot 1 provides two Fast Ethernet ports: F0/0 and F0/1	Two	NM-1FE-TX (1 Fast Ethernet port) NM-1E (1 Ethernet port) NM-4E (4 Ethernet ports) NM-16ESW (16 port switch) WIC-1T (1 serial port) WIC-2T (2 serial ports)
2650XM	Two (one available) CISCO2600-MB-1FE in Slot 1 provides one Fast Ethernet port: F0/0	Two	NM-1FE-TX (1 Fast Ethernet port) NM-1E (1 Ethernet port) NM-4E (4 Ethernet ports) NM-16ESW (16 port switch) WIC-1T (1 serial port) WIC-2T (2 serial ports)
2651XM	Two (one available) GT96100-FE in Slot 1 provides one Fast Ethernet port: F0/0	Three	NM-1FE-TX (1 Fast Ethernet port) NM-1E (1 Ethernet port) NM-4E (4 Ethernet ports) NM-16ESW (16 port switch) WIC-1T (1 serial port) WIC-2T (2 serial ports)

Table B-2: 2600 Series Routers

Model	NM Slots	WIC	Card Support
2691	Two (one available) CISCO2600-MB-2FE in Slot 1 provides two Fast Ethernet ports: F0/0 and F0/1	Two	NM-1FE-TX (1 Fast Ethernet port) NM-1E (1 Ethernet port) NM-4E (4 Ethernet ports) NM-16ESW (16 port switch) WIC-1T (1 serial port) WIC-2T (2 serial ports)

Table B-3: 3600 Series Routers

Model	NM Slots	WIC	Card Support
3620	Two (one available) CISCO2600-MB-2FE in Slot 1 provides two Fast Ethernet ports: F0/0 and F0/1	None	NM-1FE-TX (1 Fast Ethernet port) NM-1E (1 Ethernet port) NM-4E (4 Ethernet ports) NM-16ESW (16 port switch) NM-4T (4 serial ports)
3640	Four	None	NM-1FE-TX (1 Fast Ethernet port) NM-1E (1 Ethernet port) NM-4E (4 Ethernet ports) NM-16ESW (16 port switch) NM-4T (4 serial ports)
3640	Four	None	NM-1FE-TX (1 Fast Ethernet port) NM-1E (1 Ethernet port) NM-4E (4 Ethernet ports) NM-16ESW (16 port switch) NM-4T (4 serial ports)

Table B-4: 3700 Series Routers

Model	NM Slots	WIC	Card Support
3725	Three (two available) GT96100-FE in Slot 1 provides one Fast Ethernet port: F0/0	Three	NM-1FE-TX (1 Fast Ethernet port) NM-4T (4 serial ports) NM-16ESW (16 port switch) WIC-1T (1 serial port) WIC-2T (2 serial ports)
3745	Three (two available) GT96100-FE in Slot 1 provides one Fast Ethernet port: F0/0	Three	NM-1FE-TX (1 Fast Ethernet port) NM-4T (4 serial ports) NM-16ESW (16 port switch) WIC-1T (1 serial port) WIC-2T (2 serial ports)

Table B-5: 7200 Series Routers

Model	Slots	Chassis	NPE	Card Support
7206	Six	STD VXR	NPE-100 NPE-150 NPE-175 NPE-200 NPE-225 NPE-300 NPE-400 NPE-G2	C7200-IO-FE (1 Fast Ethernet port) C7200-IO-2FE (2 Fast Ethernet ports) C7200-IO-GE-E (1 Gigabit Ethernet port) PA-FE-TX (1 Fast Ethernet port) PA-2FE-TX (2 Fast Ethernet ports) PA-4E (4 Ethernet ports) PA-8E (8 Ethernet ports) PA-4T+ (4 serial ports) PA-8T (8 serial ports) PA-A1 (1 ATM port) PA-POS-OC3 (1 POS port) PA-GE (1 Gigabit Ethernet port)

Compatibilidade IOS

Os roteadores a seguir não estão mais recebendo atualizações do IOS da Cisco. Os nomes de arquivos do IOS listados aqui são as versões recomendadas para o GNS3, embora as versões mais antigas funcionem bem.

Table B-6: c1700 Series Routers

Version	Filename	MD5 Checksum	Minimum RAM
12.4.25d Mainline	c1700-adventuresek9 -mz.124-25d.bin	3ed8d56a8757771105 a56070e4147716	128MB
12.4.15T14 Technology Train	c1700-adventuresek9 -mz.124-15.T14.bin	351190de8764263e85 a2b50718f394fd	160MB

Table B-7: c2600 Series Routers

Version	Filename	MD5 Checksum	Minimum RAM
12.4.25d Mainline	c2600-adventuresek9 -mz.124-25d.bin	8ec1f6fe57dfb3c3 cf3568c0e475853	128MB
12.4.15T14 Technology Train	c2600-adventuresek9 -mz.124-15.T14.bin	12b8548b23e2ec593 652ae9310ac797f	256MB

Table B-8: c2691 Series Routers

Version	Filename	MD5 Checksum	Minimum RAM
12.4.25d Mainline	c2691-adventuresek9 -mz.124-25d.bin	a8e1f5821d874565 95488d6221ce42e5	192MB
12.4.15T14 Technology Train	c2691-adventuresek9 -mz.124-15.T14.bin	91388104d7276ad 09204e36d2dfcf52d	256MB

Table B-9: c3620 Series Routers

Version	Filename	MD5 Checksum	Minimum RAM
12.2.26c	c3620-a3jk8s-mz.122 -26c.bin	dd34b958ad362ef54 ba48b187f4c97b4	64MB

Table B-10: c3640 Series Routers

Version	Filename	MD5 Checksum	Minimum RAM
12.4.25d Mainline	c3640-a3js-mz.124-25d .bin	db9f63ca1b46d18f b835496bffe608a	128MB

Table B-11: c3660 Series Routers

Version	Filename	MD5 Checksum	Minimum RAM
12.4.25d Mainline	c3660-a3jk9s-mz.124 -25d.bin	4ac7e947f13c189d 746149dc74992890	192MB
12.4.15T14 Technology Train	c3660-a3jk9s-mz .124-15.T14.bin	39950b7a563aa08 e94a168260409f1e6	256MB

Table B-12: c3725 Series Routers

Version	Filename	MD5 Checksum	Minimum RAM
12.4.25d Mainline	c3725-adventurese9 -mz.124-25d.bin	ac3d313d3caff5be eee244b81d2c024c	128MB
12.4.15T14 Technology Train	c3725-adventurese9 -mz.124-15.T14.bin	42baf17af10d9a147 1bf542f0bfd07c7	256MB

Table B-13: c3745 Series Routers

Version	Filename	MD5 Checksum	Minimum RAM
12.4.25d Mainline	c3745-adventurese9 -mz.124-25d.bin	563797308a3036337 c3dee9b4ab54649	256MB
12.4.15T14 Technology Train	c3745-adventurese9 -mz.124-15.T14.bin	a696619869a972ec3a 27742d38031b6a	256MB

O roteador Cisco c7200 series continua recebendo atualizações do IOS da Cisco e suporta a versão 15.x do IOS.

Table B-14: c7200 Series Routers

Version	Filename	MD5 Checksum	Minimum RAM
12.4.25g Mainline	c7200-a3jk9s-mz.124 -25g.bin	3a78cb61831b3ef1 530f7402f5986556	256MB
12.4.24T4 Technology Train	c7200-adventurese9 -mz.124-24.T5	3c4148f62acf56602 ce3b371eba60c9	256MB
IOS 15.2.4	c7200-adventurese9 -mz.152-4.M7.bin		512MB

C

Limitações de NM-16ESW e IOU L2

O módulo GNS3 Dynamips NM-16ESW opera de forma idêntica ao seu equivalente real da Cisco. Como esse módulo físico, o módulo Dynamips não oferece suporte a todos os recursos de um switch Cisco Catalyst, o que significa que a única maneira garantida de obter a funcionalidade completa do switch Catalyst é integrar um ou mais switches reais em seus projetos GNS3. Listo os recursos não suportados neste apêndice, bem como os recursos que as imagens IOU L2 podem não suportar. Se você deseja usar um recurso específico do switch Catalyst, verifique essas listas primeiro para ver se você precisa usar um Switch físico.

Recursos NM-16ESW não suportados

O módulo de Switch NM-16ESW não suporta os seguintes recursos:

- Access Switch Device Manager (SDM) Template
- ACL – Improved Merging Algorithm
- ARP Optimization
- BGP Increased Support of Numbered as-path Access Lists to 500
- BGP Restart Neighbor Session After max-prefix Limit Reached

- BGP Route-Map Continue Support for Outbound Policy
- Clear Counters Per Port
- DHCP Snooping
- DHCP Snooping Counters
- Diagnostics Options on Bootup
- ErrDisable Reactivation Per Port
- ErrDisable Timeout
- EtherChannel
- EtherChannel – Flexible PAgP
- EtherChannel Guard
- Fallback Bridging
- Flex Link Bi-directional Fast Convergence
- Flex Link VLAN Load-Balancing
- Flex Links Interface Preemption
- GOLD – Generic Online Diagnostics
- IEEE 802.1ab, Link Layer Discovery Protocol
- IEEE 802.1s – Multiple Spanning Tree (MST) Standard Compliance
- IEEE 802.1s VLAN Multiple Spanning Trees
- IEEE 802.1t
- IEEE 802.1W Spanning Tree Rapid Reconfiguration
- IEEE 802.1x Auth Fail Open
- IEEE 802.1x Auth Fail VLAN
- IEEE 802.1x VLAN Assignment
- IEEE 802.1x Wake on LAN Support
- IEEE 802.1x Authenticator
- IEEE 802.1x Multi-Domain Authentication
- IEEE 802.1x with Port Security
- IEEE 802.1x RADIUS Accounting
- IEEE 802.3ad Link Aggregation (LACP)
- IEEE 802.3af Power over Ethernet
- IGMP Fast Leave

- IGMP Version 1
- IGRP
- IP Phone Detection Enhancements
- IP Phone Enhancement – PHY Loop Detection
- IPSG (IP Source Guard)
- Jumbo Frames
- L2PT – Layer 2 Protocol Tunneling
- MAC Authentication Bypass
- MLD Snooping
- Multicast EtherChannel Load Balancing
- NAC – L2 IEEE 802.1x
- NAC – L2 IP
- NAC – L2 IP with Auth Fail Open
- Packet-Based Storm Control
- Per Port Per VLAN Policing
- Port Security
- Port Security on Private VLAN Ports
- Private VLANs
- QoS Policy Propagation via Border Gateway Protocol (QPPB)
- Rapid-Per-VLAN-Spanning Tree (Rapid-PVST)
- Reduced MAC Address Usage
- Remote SPAN (RSPAN)
- Smart Port
- Spanning Tree Protocol (STP) – Loop Guard
- Spanning Tree Protocol (STP) – PortFast BPDU Filtering
- Spanning Tree Protocol (STP) – PortFast Support for Trunks
- Spanning Tree Protocol (STP) – Root Guard
- Spanning Tree Protocol (STP) – Uplink Load Balancing
- SRR (Shaped Round Robin)
- Standby Supervisor Port Usage
- STP Syslog Messages
- Switching Database Manager (SDM)

- Trunk Failover
- Trusted Boundary (extended trust for CDP devices)
- Unicast MAC Filtering
- UniDirectional Link Detection (UDLD)
- VLAN Access Control List (VACL)
- VLAN Aware Port Security
- Weighted Tail Drop (WTD)

TRADUÇÃO INICIADA POR GLAILSON-GRADUANDO EM REDES, EM NOVEMBRO DE 2019. REVISADO E CONCLUÍDO EM 27 DE JANEIRO DE 2020 ÀS 18:01.

Z2xhaWxzbg25AcHJvdG9ubWFpbC5jb20=

*Agradeço a Deus por essa conquista.
Agradeço à minha esposa Vasti,
mulher sempre presente e amorosa.
Agradeço aos meus Professores
Hedwio Carvalho, Rejane Cunha e
Emmanoela Lopes.*