

INTERCONEXÃO E PROTOCOLOS DE REDES

ANÁLISE DE TRÁFEGO E SIMULAÇÃO DE REDES

Autor: Me. Ramiro Sebastião Córdova Junior

Revisor: Luciana de Castro Lugli

INICIAR

introdução

Introdução

O dia a dia de profissionais que trabalham com redes de computadores é composto dos mais variados desafios. Em algumas situações, esses profissionais se deparam com a necessidade de realização de testes de soluções de rede sem prejudicar o funcionamento da mesma. Além disso, em muitas situações acontecem problemas de rede ou de aplicações que utilizam a comunicação em rede que necessitam de análises mais apurada para detecção do problema.

Diante deste contexto existem dois tipos de softwares (ou ferramentas) podem auxiliar os profissionais, os softwares de simulação e os softwares de análise de rede. Nesta unidade serão apresentados os principais conceitos de funcionamento destes dois tipos de software, além de apresentar exemplos de utilização destas ferramentas com o objetivo de oferecer um aporte às habilidades de gestores de redes. Os softwares apresentados são consolidados no mercado. Para a análise de tráfego, o software utilizado neste estudo é o Wireshark, e para simulação de redes é apresentado o software Packet Tracer, desenvolvido pela empresa Cisco.

Simulação e Análise de Tráfego em Redes

O desempenho de uma rede de computadores é um dos aspectos mais importantes a serem levados em consideração pelos projetistas e gerentes de redes. A análise de tráfego de rede juntamente com a simulação de funcionamento das aplicações em rede, são uma importante ferramenta para os profissionais da área. Neste tópico serão apresentados detalhes sobre como funciona um software de simulação de redes de computadores e também o funcionamento de um software analisador de tráfego de rede.

Simulação de Redes

As ferramentas de simulação são úteis para modelar e avaliar protocolos e tráfego de rede. Essas ferramentas são importantes, porque é complicado a realização de experiências para melhorias em redes que estão sendo utilizadas, principalmente no contexto corporativo.

A grande dificuldade encontrada com ferramentas de simulação a análise de tráfego são as suas interfaces. Muitas destas ferramentas não possuem interfaces

amigáveis, tornando difícil o entendimento e desencorajando os profissionais na sua utilização. Em relação aos simuladores de redes com interfaces mais simples se destacam o Packet Tracer e o GNS3 (MAKASIRANONDH et. al, 2010).

Neste material abordaremos o software Packet Tracer, que é uma ferramenta básica desenvolvida pela empresa CISCO Networks voltada para estudantes em busca das certificações oferecidas pela empresa. Com o Packet Tracer, é possível simular um ambiente de rede bem próximo da realidade utilizando equipamentos de rede da própria CISCO. A Figura 4.1 apresenta a interface inicial do Packet Tracer.

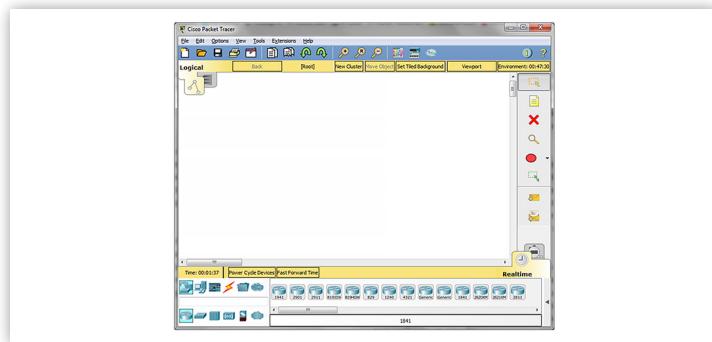


Figura 4.1: Interface do Cisco Packet Tracer

Fonte: Elaborada pelo Autor

Embora o Packet Tracer seja uma ferramenta interativa baseada em gráficos, também permite a utilização de uma interface de linha de comando baseada em texto. O Packet Tracer fornece um ambiente de rede virtual com detalhes substanciais do sistema operacional utilizado nos dispositivos de rede como switch e roteadores, por exemplo.

A ferramenta possui dois ambientes de trabalho, um lógico e outro físico. O ambiente de trabalho lógico permite a construção das topologias lógicas de rede utilizando os equipamentos de rede desenvolvidos pela CISCO. O ambiente de trabalho físico permite uma visualização gráfica da rede lógica e a representação dos dispositivos de rede em um ambiente real. A visão do ambiente físico permite representações geográficas de redes, incluindo cidades, prédios e racks de rede.

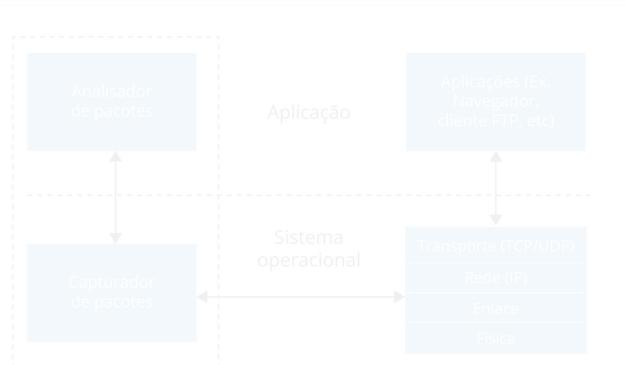
Existem dois modos de operação para representação visual de um comportamento da rede: tempo real e modo de simulação. O modo em tempo real permite a realização de práticas de configuração, pois os dispositivos da rede se comportam exatamente da mesma forma que os dispositivos reais da Cisco. No modo de simulação, eles podem ver, controlar e analisar intervalos de tempo e propagação de dados em uma rede e aprender como solucionar problemas de falhas de rede. Isso ajuda significativamente no entendimento dos conceitos fundamentais da operação da rede.

Análise de Tráfego em Redes

A análise de tráfego de rede pode ser definida como: "a inferência de informações da observação do fluxo de dados de tráfego de rede". Os analisadores de tráfego são executados sobre os dados à medida que são obtidos ou através de pequenos lotes geralmente chamados buffers, para permitir a análise dos dados com eficiência.

De modo geral, as ferramentas que analisam pacotes de rede são consideradas elementos passivos da rede que atuam na observação dos pacotes capturados (enviados e recebidos). Esse tipo de ferramenta não tem como característica a alteração do conteúdo destes pacotes, por isso são consideradas passivas. Como característica importante também pode-se citar que essas ferramentas permitem o armazenamento dos pacotes capturados.

As ferramentas que permitem a captura para análise de pacotes de rede geralmente possuem filtros que permitem selecionar o tráfego de interesse. Isso diminui a quantidade de pacotes capturados, possibilitando assim a análise do que é relevante. A figura 4.2 apresenta a estrutura de um software de análise de pacotes.



As aplicações comuns de serem utilizadas em rede, como navegadores e clientes de email utilizam os protocolos de rede que poderão ser analisados. O software analisador pode ser subdividido em dois módulos, o que realiza a análise e o que realiza a captura dos pacotes.

Para que seja possível a análise de pacotes é necessário que um software analisador de pacotes esteja instalado no computador e que seja executado um processo envolvendo comunicação em rede (ASRODIA, 2012). O software analisador irá realizar um monitoramento das atividades na camada de enlace, rede e transporte. O capturador de pacotes recebe uma cópia dos quadros e encaminha para o analisador, que faz a interpretação dos pacotes exibindo o seu conteúdo.

Saiba mais

Os softwares que realizam a captura e análise de pacotes em redes de computadores, além de serem utilizados na resolução de problemas de rede, podem ser utilizados de maneira maliciosa. É importante garantir que pessoas má intencionadas não estejam utilizando esse tipo de ferramenta para coleta de dados sigilosos.

Para saber mais detalhes sobre esse assunto acesse o artigo disponível no site da Avast.

Fonte: Elaborado pelo autor.

ACESSAR

Vamos Praticar

Um software que permite a análise de tráfego de rede é considerado um elemento passivo na rede, ou seja, não é capaz de alterar os pacotes que trafegam na rede. É comum dividir esse tipo de software em dois módulos com funções bem definidas. Quais os nomes desses dois módulos?

- a)** Pacotes e Frames
- b)** Empacotador e Analisador.
- c)** Analisador e capturador
- d)** Core e barramentos

- e) Analisador e testador
-

Análise de Tráfego com Wireshark

O software Wireshark é um analisador de pacotes de rede, que captura pacotes de rede e exibe esses dados de maneira detalhada. É possível dizer que um analisador de pacotes de rede é um dispositivo de medição usado para examinar o que está acontecendo dentro de um cabo de rede. É possível utilizar o Wireshark para verificar o tráfego de rede de um software suspeito, analisar o fluxo de tráfego na rede e também para solucionar problemas de rede.

Existe a possibilidade de capturar tráfego de diferentes tipos de meio físico, incluindo as redes sem fio. Os tipos de meio físico suportados dependem de vários aspectos, como o sistema operacional utilizado. O Wireshark é um software de código aberto que pode ser utilizado livremente em sem que seja necessário se preocupar com licenciamento (MOQADI & SILVA, 2011).

Para que seja possível realizar a análise de pacotes utilizando o Wireshark, é necessário possuir o software instalado. A Figura 4.3 apresenta a tela inicial do Wireshark. O download pode ser realizado na página do projeto wireshark. É importante salientar que muitas organizações não permitem a utilização do

Wireshark e ferramentas similares em suas redes. Portanto, não use essa ferramenta no trabalho sem a permissão adequada.

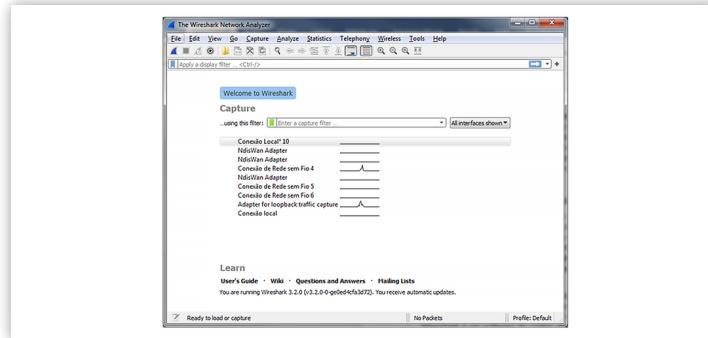


Figura 4.3: Tela inicial do Wireshark

Fonte: Elaborada pelo Autor

A lista apresentada na tela inicial apresenta as interfaces de rede disponíveis. Para iniciar a captura de pacotes basta dar um duplo clique na interface que se deseja capturar os pacotes. Os pacotes podem ser visualizados em tempo real, caso a interface esteja configurada em modo promíscuo, é possível visualizar os pacotes que trafegam na rede e não apenas os que forem endereçados para o adaptador de rede selecionado. A Figura 4.4 apresenta a tela do wireshark com pacotes capturados. Para encerrar a captura é necessário clicar no botão stop (canto superior esquerdo).

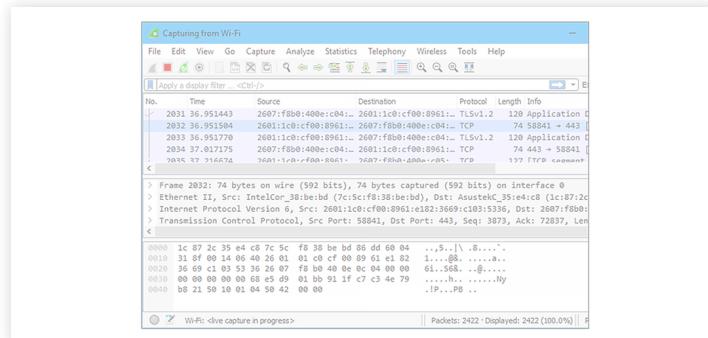


Figura 4.4: Captura de pacote no Wireshark

Fonte: Elaborada pelo Autor

Fonte: Elaborada pelo Autor
 O wireshark apresenta pacotes destacados a partir de uma variedade de cores diferentes. As cores ajudam a identificar mais facilmente os tipos de tráfego. Por padrão, roxo claro é tráfego TCP, azul claro é tráfego UDP e preto identifica pacotes com erros (que podem ter sido entregues fora de ordem). Para visualizar exatamente o que significam os códigos de cores, clique em View > Coloring Rules (Figura 4.5). Também é possível personalizar e modificar os padrões de cores.

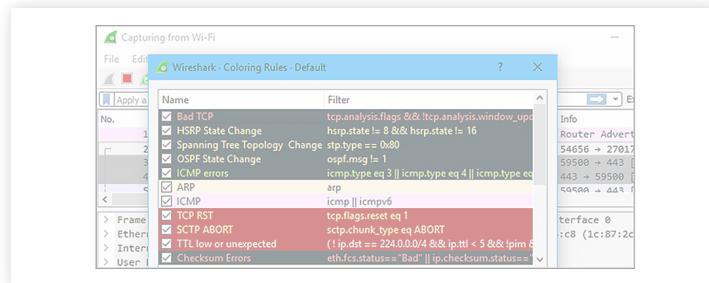


Figura 4.5: Tela com a legenda de cores no wireshark

Fonte: Elaborada pelo Autor

Para facilitar a captura e análise dos pacotes, o wireshark permite a utilização de filtros, ou seja, agiliza a captura de pacotes que realmente interessam. A maneira mais simples de aplicar um filtro é digitando na caixa de filtro na parte superior da janela e clicando em Aplicar (ou pressionando Enter). Por exemplo, digite "dns" e você verá apenas pacotes DNS, como mostra a Figura 4.6. Quando a digitação é iniciada o Wireshark ajuda a completar automaticamente o filtro a ser aplicado.

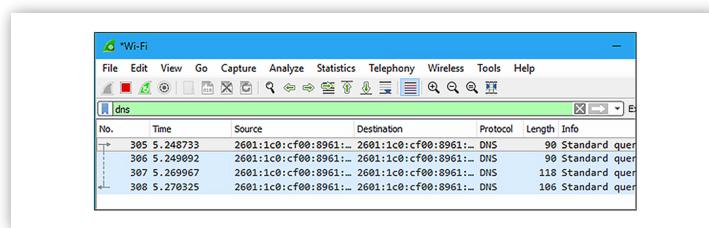


Figura 4.6: Filtro no Wireshark

Fonte: Elaborada pelo Autor

Também é possível utilizar alguns filtros padrões do próprio Wireshark. Para isto basta acessar Analyze > Display Filters. Também é possível criar filtros e salvar para utilizar posteriormente. Outra função interessante do software é o acompanhamento de fluxos TCP, ou seja, acompanhar a comunicação completa entre cliente e servidor. Para isto basta clicar com o botão direito no pacote desejado e escolher a opção Follow> TCP Stream.

Ao selecionar um pacote capturado, é possível observar as informações referentes ao mesmo na área central da tela. Nesta área são apresentadas as informações do pacote capturado, divididas por camada do modelo OSI. Na Figura 4.7 é possível visualizar as informações de um pacote capturado utilizando o protocolo HTTP.

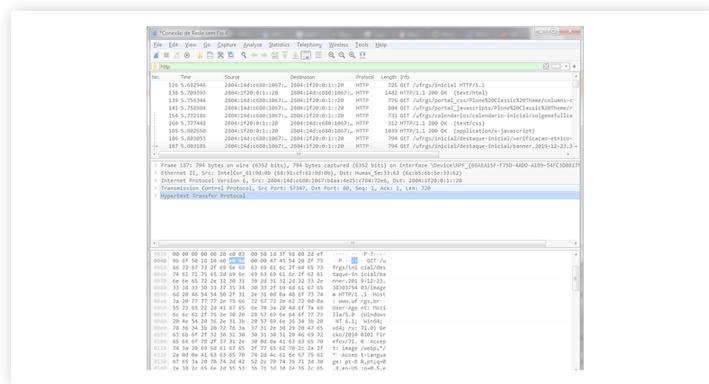


Figura 4.7: Informações de um pacote capturado com o Wireshark

Fonte: Elaborada pelo autor

Na linha 1 da descrição do pacote capturado são apresentadas (basta clicar) informações referentes a camada física, como o adaptador de rede utilizado. Na linha 2 são apresentadas informações referentes a camada de enlace, informando o endereço físico da origem e do destino. Na linha 3 podem ser visualizadas informações referentes a camada de rede, onde podem ser visualizados os endereços ip de origem e destino do pacote. Na linha 4 podem ser visualizadas informações referentes a camada de transporte, como porta de origem e porta de destino. Já na linha 5 é possível visualizar informações relacionadas a camada de aplicação, como a url solicitada.

reflita

Reflita

Analisando o potencial de uma ferramenta como o Wireshark, que permite visualizar o tráfego de rede, é possível perceber que pessoas que possuem o conhecimento técnico avançado podem capturar dados sigilosos de usuários da rede. A criptografia dos dados serve para que seja possível embaralhar as informações que trafegam em rede, porém o tráfego de rede aumenta. Este aumento varia conforme o nível de segurança desejado, ou seja, quanto maior for a segurança, maior será o aumento do tráfego. Como definir esse limite entre segurança e performance? Esse é um dos principais questionamentos para os profissionais que desenvolvem soluções em redes de computadores.

Fonte: Elaborado pelo autor

O Wireshark é uma das ferramentas mais populares para realização de captura e análise de tráfego de rede. Porém, existem outras ferramentas que permitem realizar as mesmas funções.

praticar

Vamos Praticar

Um analisador de tráfego de rede permite que sejam analisados os diferentes tipos de pacotes que trafegam na rede. Como a quantidade pode ser absurdamente grande de pacotes trafegando é interessante que seja possível a seleção dos pacotes conforme a

necessidade de análise. Qual o nome do recurso que garante essa possibilidade em um software analisador de pacotes?

- a)** Filtro
- b)** Protocolo
- c)** Botão de captura
- d)** Definição de cores
- e)** Regras de análise

Interconexão de Redes com Packet Tracer

O Cisco Packet Tracer é um programa de simulação de rede que possibilita experimentar e aprender os diferentes comportamentos possíveis em redes de computadores. É também uma parte vital da experiência de aprendizado da Networking Academy da empresa CISCO. O Packet Tracer permite simulação, visualização, autoria, avaliação e aprimora o ensino e o aprendizado de conceitos complexos de tecnologia (ČABARKAPA, 2015).

Configurando uma Rede

Para que seja possível criar e simular uma rede no Packet Tracer é necessário adicionar os dispositivos de rede no software, interconectá-los através de um meio físico e realizar a configuração de endereçamento ip dos equipamentos da rede. Vamos realizar estas etapas passo a passo.

Para fins de aprendizado vamos criar uma rede com 3 computadores e um laptop interconectados por um switch. Para isso devemos encontrar esses dispositivos na

parte inferior da tela do Packet Tracer. A Figura 4.11 mostra na tela do Packet Tracer onde encontrar esses itens.

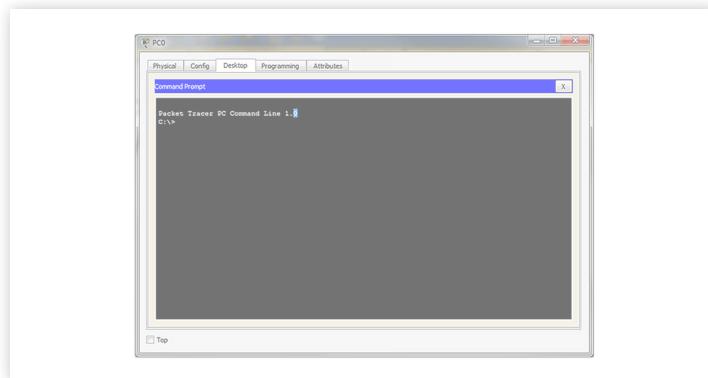
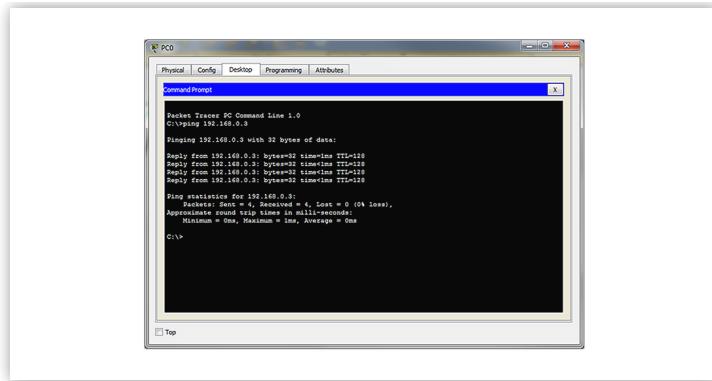


Figura 4.11: Tela do prompt de comando

Fonte: Elaborada pelo autor

Esse prompt de comando permite a execução de comandos disponíveis em alguns sistemas operacionais, entre eles o comando PING. Este comando permite a realização de um teste de conectividade entre o host onde será executado o comando e um host de destino. Um conjunto de pacotes é enviado ao host de destino e o comando retorna algumas estatísticas referentes a esse processo, permitindo observar se a conectividade entre os hosts está ok.

No nosso exemplo podemos testar se existe conectividade entre o PC0 e o PC2. Para isto, basta digitar no prompt o comando ping 192.168.0.3 e pressionar a tecla ENTER. A Figura 4.12 apresenta o resultado do comando.



*Figura 4.12: Comando ping no prompt de comando
Fonte: Elaborada pelo autor*

É possível visualizar no retorno do comando que foram enviados 4 pacotes, todos os pacotes foram recebidos no destino e nenhum pacote foi perdido. Esse é o retorno que indica o sucesso no teste de conectividade entre o PC0 e o PC2 na nossa rede simulada.

A outra opção de teste de conectividade entre hosts na nossa rede simulada pode ser realizada via interface gráfica do Packet Tracer. Para realizarmos o mesmo teste de conectividade podemos acionar a ferramenta de envio de pacotes, que fica na barra de ferramentas a direita da tela e possui como símbolo um envelope amarelo com o sinal de adição (+). Para enviar pacotes do PC0 para o PC3, basta clicar na ferramenta e depois dar um clique no PC0 e um clique no PC3. No canto inferior direito é possível verificar o resultado do comando. A Figura 4.13 mostra como visualizar o resultado do teste.

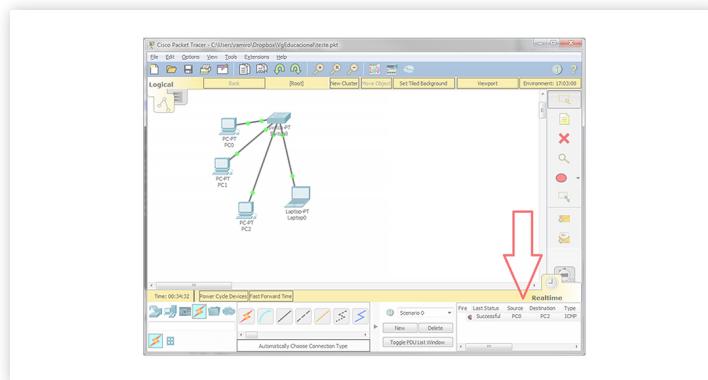


Figura 4.13: Teste de conectividade por interface gráfica

Fonte: Elaborada pelo autor

Notem que o protocolo utilizado é o ICMP, o mesmo protocolo utilizado pelo comando PING. A indicação “Successfull” significa que o pacote saiu da origem e chegou no destino, ou seja, a conectividade entre o PC0 e o PC2 está ok. Esses dois procedimentos de testes podem ser realizados entre os demais hosts da rede simulada para que seja possível verificar se existe conectividade entre todos os hosts.

praticar

Vamos Praticar

O packet Tracer permite que seja desenhada uma topologia de rede e também que sejam realizados testes do ponto de vista lógico. Estes testes garantem que o ambiente de rede que está sendo simulado irá funcionar caso as configurações sejam aplicadas corretamente. Como é possível realizar a configuração de endereçamento IP nos hosts do packet Tracer?

- a) Deve-se acessar o menu configure network e inserir as configurações

- b)** Deve-se acessar a opção Ip configuration de cada host e inserir as configurações
 - c)** Deve-se acessar a opção Desktop de cada host e inserir as configurações
 - d)** Deve-se importar de um arquivo de texto as configurações para dentro do packet Tracer
 - e)** Deve-se exportar de um arquivo .xls as configurações para dentro do Packet Tracer
-

Protocolos da Camada de Aplicação

Para que seja possível acompanhar os serviços referente aos protocolos de aplicação comuns em redes de computadores como DHCP, HTTP e DNS, vamos criar uma nova rede e realizar as conexões físicas no simulador. Esta rede pode inicialmente possuir 3 computadores interconectados através de um switch. A Figura 4.14 mostra como deve ficar a rede simulada.

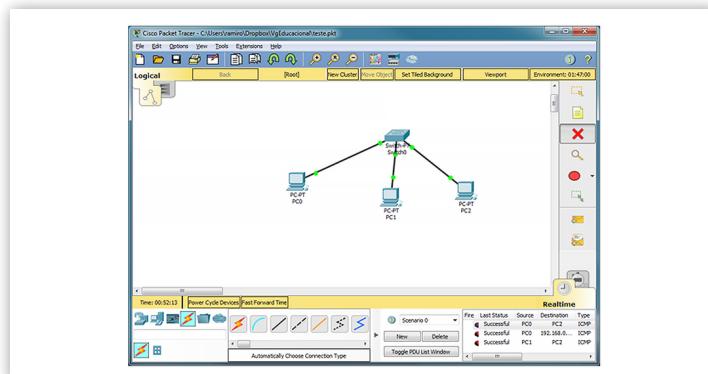


Figura 4.14: Rede de exemplo
Fonte: Elaborada pelo autor

A partir do momento que temos a rede, iremos adicionando os servidores conforme o protocolo a ser testado. A seguir iremos realizar o passo a passo das configurações e testes.

Servidor DHCP

O servidor DHCP tem como objetivo prover as configurações de endereçamento IP aos hosts de rede que estiverem configurados para utilizar o protocolo DHCP. Para que possamos testar o protocolo vamos inserir na nossa rede simulada um servidor e definir seu nome como sendo SRVDHCP. A Figura 4.15 mostra como ficará a rede simulada.

Após adicionar o SRVDHCP é necessário realizar a configuração de endereçamento ip do mesmo. Podemos configurar esse servidor com o endereço ip 192.168.0.254. Para que seja possível configurar o serviço DHCP nesse servidor, é necessário acessar a opção Services e selecionar o serviço DHCP. Inicialmente é necessário habilitar o serviço, isto pode ser feito marcando a opção On. As outras configurações importantes para que o serviço funcione são:

- Start Ip Address: esta opção permite definir qual será o primeiro endereço ip a ser endereçado. Os demais hosts receberão ip na sequência;

- Subnet Mask: é a máscara de sub rede utilizada pelo servidor, este campo é preenchido automaticamente pelo Packet Tracer, mas é importante verificar se está correto;
- Maximum Number of Users: define o número máximo de ips que serão concedidos pelo servidor DHCP;

Com essas opções já é possível iniciar o serviço com configurações básicas. Como a nossa rede simulada não possui gateway e nem um servidor DNS, essas opções ficarão sem alteração. Porém, é comum em redes que o serviço DHCP também entregue essas configurações aos clientes. A Figura 4.16 apresenta a tela de configuração do nosso servidor DHCP. Após inserir as configurações é importante clicar em save (salvar).

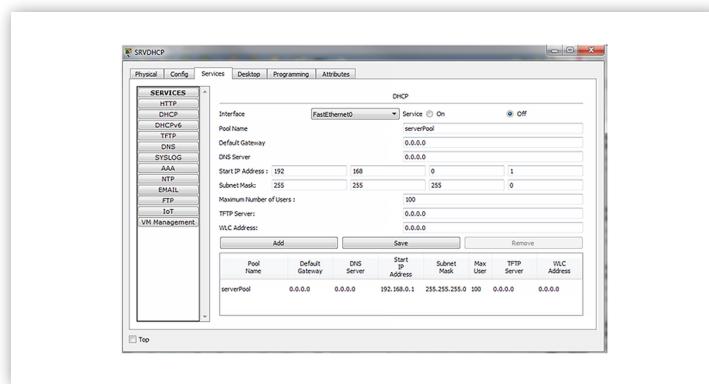


Figura 4.16: Rede de exemplo com o servidor DHCP

Fonte: Elaborada pelo autor

Agora é necessário que todos os computadores da rede simulada estejam configurados para receberem ip por DHCP. Para isto é necessário acessar em cada um dos computadores as configurações de ip e marcar a opção DHCP. Para realizar um teste, podemos acessar o prompt de comando do PC1, por exemplo, e executar o comando ipconfig. Este comando apresenta as configurações ip do host. A Figura 4.17 apresenta a tela após a execução do comando.

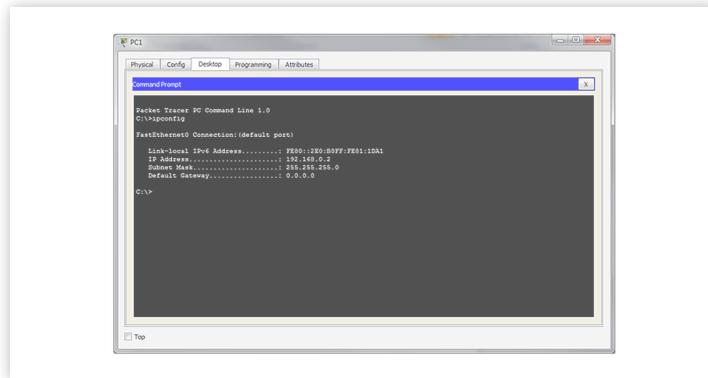


Figura 4.17: Resultado do comando ipconfig

Fonte: Elaborada pelo autor

É possível verificar que o PC1 recebeu o endereço ip 192.168.0.2, o que significa que o serviço está funcionando e o protocolo DHCP está em funcionamento na nossa rede simulada. Este teste pode ser repetido em todos os hosts da rede simulada para verificar se todos receberam ip corretamente.

Servidor HTTP

Os servidores que hospedam uma ou mais páginas WEB utilizam o protocolo HTTP para controlar as requisições de acesso as páginas. Podemos na nossa rede simulada adicionar mais um servidor e nomeá-lo como SRVHTTP. Este servidor irá hospedar uma página WEB que deve ser acessada pelos hosts da rede.

Esse serviço é bem simples de ser configurado e testado. No servidor adicionado (SRVHTTP) na nossa rede simulada, vamos configurar o endereço ip 192.168.0.253. Uma vez que o endereço ip está correto e o servidor está conectado no switch podemos ativar o serviço HTTP. Para isso, no SRVHTTP devemos acessar a opção Services e escolher o serviço HTTP (lado esquerdo).

Será apresentada uma tela onde é possível marcar a opção On (ativar) tanto o protocolo HTTP como o protocolo HTTPS. Abaixo é apresentada uma lista de arquivos com código HTML de exemplo para servir como página inicial do servidor HTTP. Podemos excluir todos exceto o que possui o nome "index.html", este será o arquivo com o código HTML referente a página inicial do servidor HTTP da rede

simulada. A Figura 4.18 apresenta como deve ficar a tela de configuração do serviço HTTP.

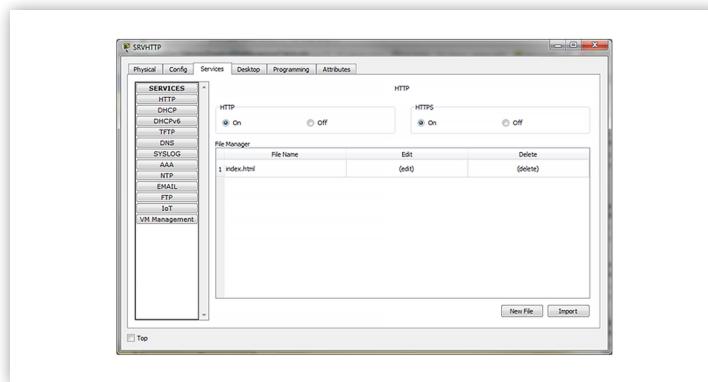
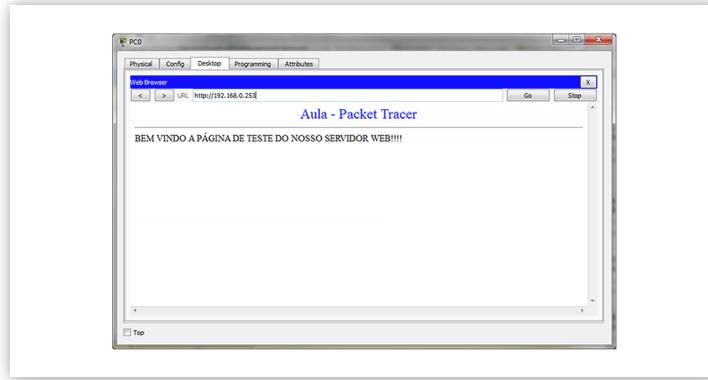


Figura 4.18: Configuração do serviço HTTP

Fonte: Elaborada pelo autor

É possível editar o código HTML referente a página Inicial, para isto é necessário clicar no arquivo index.html que o código será aberto. No caso do nosso exemplo foram feitas algumas customizações, mas o padrão é uma página referente ao próprio Packet Tracer.

Após a ativação do serviço e definição da página inicial, para realizar um teste iremos abrir o navegador web do PC0. Para isto é necessário acessar a opção Desktop > Web Browser. Na linha referente a url devemos informar o endereço ip do SRVHTTP, que é 192.168.0.253. No navegador deverá abrir a página inicial definida anteriormente. A Figura 4.19 apresenta a página web.



*Figura 4.19: Página de teste
Fonte: Elaborada pelo autor*

Este mesmo teste pode ser realizado em todos os hosts da rede. Para que seja possível acessar a página através de um nome, é necessário a configuração do protocolo DNS.

Servidor DNS

O servidor DNS permite converter os endereços ips em nomes. É um serviço bastante utilizado em redes, pois não torna necessário que sejam decorados os endereços ips dos hosts a serem acessados. Na nossa rede simulada vamos inserir mais um servidor que será chamado de SRVDNS.

No SRVDNS vamos configurar o endereço ip 192.168.0.252. Após a configuração de ip é necessário realizar a configuração do serviço DNS, para isto devemos acessar a opção Services e escolher o serviço DNS (lado esquerdo). Na tela referente ao serviço devemos informar o nome e abaixo o endereço ip referente ao nome. Por exemplo, vamos definir o nome www.testederede.com associado ao endereço ip 192.168.0.253 (ip do servidor HTTP). Além disso, podemos associar os nomes dos hosts aos endereços deles para que os mesmos possam ser identificados na rede pelo nome e não apenas pelo endereço ip. A Figura 4.20 mostra como ficará a tela de configuração do serviço DNS no SRVDNS.

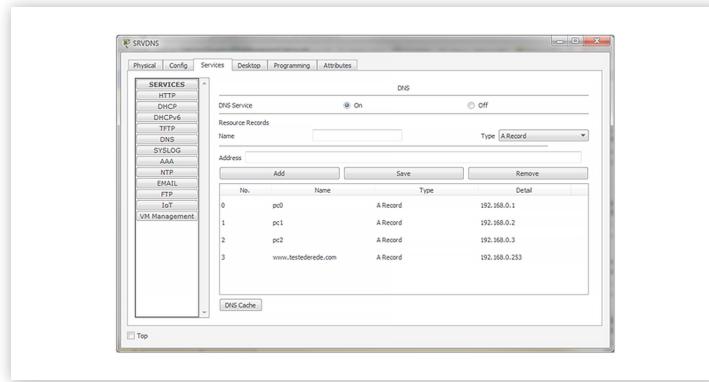


Figura 4.20: Tela de configuração do serviço DNS

Fonte: Elaborada pelo autor

Após a realização da configuração do serviço, é necessário informar ao servidor DHCP que existe um servidor DNS na rede. Assim, a configuração de DNS também será enviada via protocolo DHCP. Para isso é necessário acessar o serviço DHCP no SRVDHCP e no campo Dns Server colocar o endereço 192.168.0.252.

Feito isto, para realizarmos um teste é necessário abrir o navegador WEB em qualquer host da rede e na url informar o endereço www.testederede.com, que está associado ao endereço ip do servidor HTTP. A página inicial deverá aparecer para confirmar que o serviço DNS está ok. Outra possibilidade de teste é acessar o prompt de comando de algum host e realizar um ping pelo nome do host (PC0 ou PC1 ou PC2).

praticar
Vamos Praticar

A configuração dos serviços correspondentes aos protocolos mais comuns da camada de aplicação pode ser realizada através da interface gráfica do packet tracer, o que facilita

bastante o aprendizado e agiliza a realização das simulações através do software. Qual o protocolo que deve ser implementado para garantir a entrega de endereços ip aos hosts da rede?

- a)** DNS
- b)** DHCP
- c)** HTTP
- d)** HTTPS
- e)** ICMP

Indicações Material Complementar



LIVRO

Criando Redes Locais com o Cisco Packet Tracer 5

Pablo Luis Fazanaro

Editora: Clube de Autores

ISBN: 978-8591552818

Comentário: Neste livro é apresentado passo a passo os procedimentos de configuração de cenários de redes simuladas no packet tracer. São apresentados exemplos práticos desde cenários mais simples até cenários mais complexos.

WEB

Wireshark: entendendo e analisando protocolos de rede

Tipo: Canal do YouTube

Ano: 2018

Comentário: Este vídeo mostra como funciona na prática a ferramenta Wireshark para captura e análise de tráfego de pacotes de rede.

ACESSAR

conclusão

Conclusão

Os profissionais que atuam na gestão ou desenvolvimento de soluções para redes de computadores, constantemente necessitam realizar testes de possíveis novas soluções. Esses testes quando realizados no ambiente real podem causar alguns transtornos que podem variar desde lentidão na rede até mesmo a indisponibilidade de serviços. Diante deste contexto, fica clara a necessidade de um ambiente específico para testes e os softwares de simulação exercem um papel fundamental, permitindo que os profissionais possam testar as soluções sem afetar o ambiente real.

Além da simulação de redes, esta unidade abordou a análise de tráfego de rede. Analisar o tráfego de rede pode ajudar os profissionais da área de redes a solucionar problemas cuja solução não é tão simples de ser identificada. Os softwares analisadores permitem que o tráfego seja filtrado para realização de análises mais apuradas dos pacotes.

Tanto a simulação de soluções quanto a análise de pacotes de rede podem ser consideradas habilidades importantes para um profissional que trabalha com redes de computadores. Sendo assim, ter o conhecimento básico de ferramentas que permitam realizar essas atividades é essencial.

referências

Referências Bibliográficas

ASRODIA, Pallavi; PATEL, Hemlata. Network traffic analysis using packet sniffer. **International journal of engineering research and applications**, v. 2, n. 3, p. 854-856, 2012.

ČABARKAPA, D. Application of Cisco Packet Tracer 6.2 in teaching of advanced computer networks. **Information Technology and Development of Education ITRO 2015**, p. 153, 2015.

MAKASIRANONDH, Woratat; MAJ, S. Paul; VEAL, David. Pedagogical evaluation of simulation tools usage in Network Technology Education. **Engineering and Technology**, v. 8, p. 321-326, 2010.

MOQADI, Kanan Ali Abdulla; SILVA, V. C. O. Uso de ferramentas de gerencia de rede para analise de desempenho de uma rede local. **Universidade Luterana do Brasil**, 2011.

