GUIA PRÁTICO

de

REDES DE COMPUTADORES

Salomão Bento Nilo Pena

Lubango, 2018

GUIA PRÁTICO

de

REDES DE COMPUTADORES

Salomão Bento Nilo Pena

Críticas e sugestões

spena.live@sapo.pt

spenna.live@gmail.com

Lubango, 2018

Índice Geral

Índice de Figuras

Índice de tabelas

APRESENTAÇÃO

Prezado estudante de licenciatura, este é um documento denominado

"Guia Prático de Redes de Computadores".

É um documento que visa apresentar um conjunto de orientações didácticas relativas a disciplina de rede de computadores (RC) no curso de Informática no Instituto Superior de Ciências de Educação da Huíla (ISCED-HUÍLA), bem como as funcionalidades e os objectivos da disciplina como componente curricular.

Se você escolheu ser um profissional em educação coloque em mente que você nasceu para orientar, ensinar e formar pessoas e sua escolha não foi em vão, ela contribuirá necessariamente para uma das actividades humanas mais complexas (ensinar). Logo o rumo da educação depende da sua prática docente.

Este documento guiará e auxiliará os estudantes nos mais variados problemas encontrados ao logos das actividades académicas. A sua aplicabilidade é indispensável, visto que é um material de extrema importância e seu conteúdo foi elaborado especialmente para minimizar as dificuldades que os estudantes enfrentam ao longo das aulas e na convivência do dia-a-dia.

A disciplina de Redes de Computadores tem como objectivo...

(…) Proporcionar aos estudantes os conhecimentos sobre Redes de Computadores referentes a: protocolos, estrutura de cabos de uma rede, arquitectura, equipamentos, segurança e tipos de redes. Onde os estudantes aprendem a administrar redes de computadores cliente/ servidor.

O guia oferece recursos e conteúdos ricos que vão capacitar o auto estudo e a auto avaliação do estudante para garantir qualidade na formação, onde o objectivo principal é a qualificação técnica e satisfação do estudante como centro das aprendizagens.

AO LEITOR

Caro leitor, este compêndio que chamamos de "*guia prático de redes de computadores*" contém informações relevantes que poderão ajudar os estudantes, professores e leitores tecnólogos em geral a superar uma variedade de dificuldades que enfrentam no mundo das redes de computadores, ou seja no mundo do conectivismo. Apesar de que o guia foi elaborado maioritariamente para estudantes, isto não descarta a possibilidade de que não haja informação para outros leitores interessados em seu conteúdo. Não importa se você é estudante de redes, desde já o guia foi projectado para situar qualquer leitor que esteja motivado para aprender redes.

Com este guia você vai aprender passo a passo configurar topologias de redes, desde as mais simples até as mais complexas. Mas, antes precisa-se entender que os exercícios não devem ser deixados para depois. Repita-os até sentir-se capaz de resolver sem ajuda do guia ou outra. Estude com mais motivação e lembre-se, já tem um ponto a mais quem está motivado para aprender certo conteúdo.

O Guia prático de redes de computadores é um documento que pode ser usado como apoio há consultas na sala de aulas, no centro comercial, no ônibus e em qualquer outro lugar com o objectivo de aprendizagem e de partilha de conhecimentos. Se é professor deve usar o guia na sala de aulas para facilitar e orientar melhor seu trabalho docente educativo e também para deixar orientações aos estudantes. Os estudantes deverão usar o guia prático para resolver exercícios que o professor vai orientar.

O presente guia contém:

- ✓ Conteúdo para auxiliar a comunidade académica em geral
- ✓ Exercícios propostos
- ✓ Exercícios resolvidos
- ✓ Exemplos práticos entre outros aspectos

As orientações e todas outras informações presentes no guia não foram elaboradas só. Tiveram que ser censuradas e estruturadas de acordo com o conteúdo programático curricular da disciplina de R.C leccionada no ISCED da Huíla:

1. Introdução a redes (Equipamentos de Redes, Estrutura de cabos);
2. Arquitecturas de redes locais (Protocolos: Fundamentos);
3. Endereçamento em redes;
4. Encaminhamento de pacotes IP;
5. Redes locais;
6. Redes clientes servidor;
7. Segurança em redes e Desempenho;

De lembrar que os temas não foram seleccionados arbitrariamente nem ao critério do autor, os temas foram tirados do Plano Curricular do Curso de Informática anexado na Instituição de Ensino (ISCED-HUÍLA) para que não exista divergência de conteúdos programáticos. Sendo um guia prático é de inteira responsabilidade do leitor ir profundando o conteúdo teórico para enriquecer a prática.

Elaborou-se o guia maioritariamente para estudantes, lembre-se, logo, ao desenrolar do conteúdo utilizar-se-á frequentemente o termo (estudante). Mais como já nos referimos a pouco, isto não descarta a possibilidade de existir conteúdos para qualquer um de nós. Aliás, neste guia quando falamos de estudante não é necessariamente aquele que está a frequentar uma escola ou algo parecido. Estamos a tratar de estudante qualquer um que esteja estudando o guia cujo objectivo é estudar seu conteúdo e partilhar conhecimento.

OBJECTIVOS

Proporcionar um conjunto de orientações práticas simuladas utilizando o Cisco Packet Tracer 6.0.1, 7.0 e 7.1 de modo que até ao final do guia o estudante consiga:

- Aprender a configurar Redes de Computadores de uma forma teórico-prática e simulada.
- Projectar topologias de rede simuladas.
- Usar o Cisco Packet Tracer independente da versão para o desenvolvimento de experiências laboratoriais detalhadas.
- Usar interfaces gráficas e comandos da consola CLI (Command Line Interface) do referido Software para a configuração de redes simuladas.
- Estabelecer um melhor entendimento das ferramentas de Rede de Computadores e de simulação das mesmas no ambiente Cisco Packet Tracer.

INTRODUÇÃO

O presente guia visa dar um entendimento melhor das ferramentas de simulação de Redes de Computadores projectadas pelo simulador Virtual Cisco Packet Tracer, e deste modo poder estabelecer as funcionalidades básicas, gerais e avançadas.

No ambiente Cisco Packet Tracer é possível projectar Redes de Computadores, sem a necessidade de ter um outro dispositivo de Hardware ou Software adicional à máquina na qual está instalado. As configurações e funcionalidades do IOS que a Cisco prevê, somam um grande valor, porque o programa tem interfaces de Hardware genéricas e específicas desta companhia.

O referido software permite ao usuário saber o comportamento físico e real de uma rede ao mesmo tempo.

Neste guia, o estudante vai puder modelar topologias de redes variantes e seguir os passos sistematicamente para desencadear um desenvolvimento ininterrupto pessoal nas práticas de laboratório. É necessário que os estudantes ou os leitores em geral, resolvam exercícios para tirar deste guia o máximo proveito do que ele tem para oferecer.

É recomendável que os estudantes devem ter noções básicas sobre Rede de Computadores, Endereçamento IP, Protocolos de Rede, Encaminhamento de Pacotes, Modelo OSI, Modelo TCP/IP, Roteamento, entre outros aspectos. É também aconselhável que os utilizadores deste guia tenham um conhecimento prévio sobre a plataforma de simulação Packet Tracer independentemente da versão, de igual modo isto ajudará a entender melhor as práticas dentro e fora do ambiente estudantil. Por outra, se você ainda nunca teve contacto com um simulador de rede da Cisco, não

se preocupe, leia atentamente e siga as ilustrações, com certeza que o guia o ajudará sobre as configurações que desejar.

Este guia retracta aspectos bastante práticos e a teoria deixamos por conta do leitor buscar outras bibliografias para enriquecer seu aprendizado.

Aproveite o bastante!

Se você chegou ate aqui, com certeza está motivado para aprender.

O guia vai orientá-lo até ao final.

Boa caminhada e estaremos juntos ao longo do conteúdo.

1ª PARTE

APRESENTAÇÃO DO CISCO PACKET TRACER

1.1. Apresentação do cisco Packet Tracer

Antes de entrar em práticas de laboratório como tal, dar-se-á uma breve resenha daquilo que será o software a usar ao longo das mesmas.

O foco principal deste guia são as práticas de laboratório no ambiente gráfico de simulação de Rede da CISCO - **Cisco Packet Tracer**. Embora exista outras versões do referido software, optou-se pela versão 7.1, por questões de conveniência e por ser a mais recente.

1.1.1. O que é o cisco Packet Tracer?

O Packet Tracer é um software educacional gratuito de tecnologia de rede que oferece uma combinação sem igual de simulação realística e experiências de visualização através de equipamentos e configurações presente em situações reais. É um programa potente, desenvolvido pela Cisco Systems, Empresa Multinacional sediada na Califórnia – Estados Unidos de América, fundada em 1984 pelo casal Len Bosack e Sandy Lerner, ambos, ex-funcionários de computação da Universidade Standford University.

Não é de inteira responsabilidade do guia estudar o que é o cisco Packet Tracer, aqui, apenas trataremos de como desenvolver topologias de redes. Não obstante, para dar um melhor entendimento conheceremos primeiro o ambiente gráfico do Packet Tracer onde executaremos todas nossas práticas até ao final.

1.1.2. Como instalar o Cisco Packet Tracer?

Como todo executável da família Windows, o processo de instalação é bastante simples. O primeiro passo é fazer o Download (baixar) o software no site oficial da Cisco (www.cisco.com) e escolher a opção download de softwares o ainda fazê-lo directamente pelo link (https://software.cisco/download/navigator.html). Após descarregar faz-se a instalação. Como já dissemos o processo de instalação é bastante simples quando se usa o Windows.

Clique duplo sobre o executável (next, next e finsh) é só seguir as instruções de antes instalação, durante a instalação e pós instalação. Após instalação é criado um atalho  na área de trabalho (ambiente de trabalho). Clique duplo sobre o mesmo é apresentado a tela inicial do simulador de rede Cisco Packet Tracer – Figura 1.

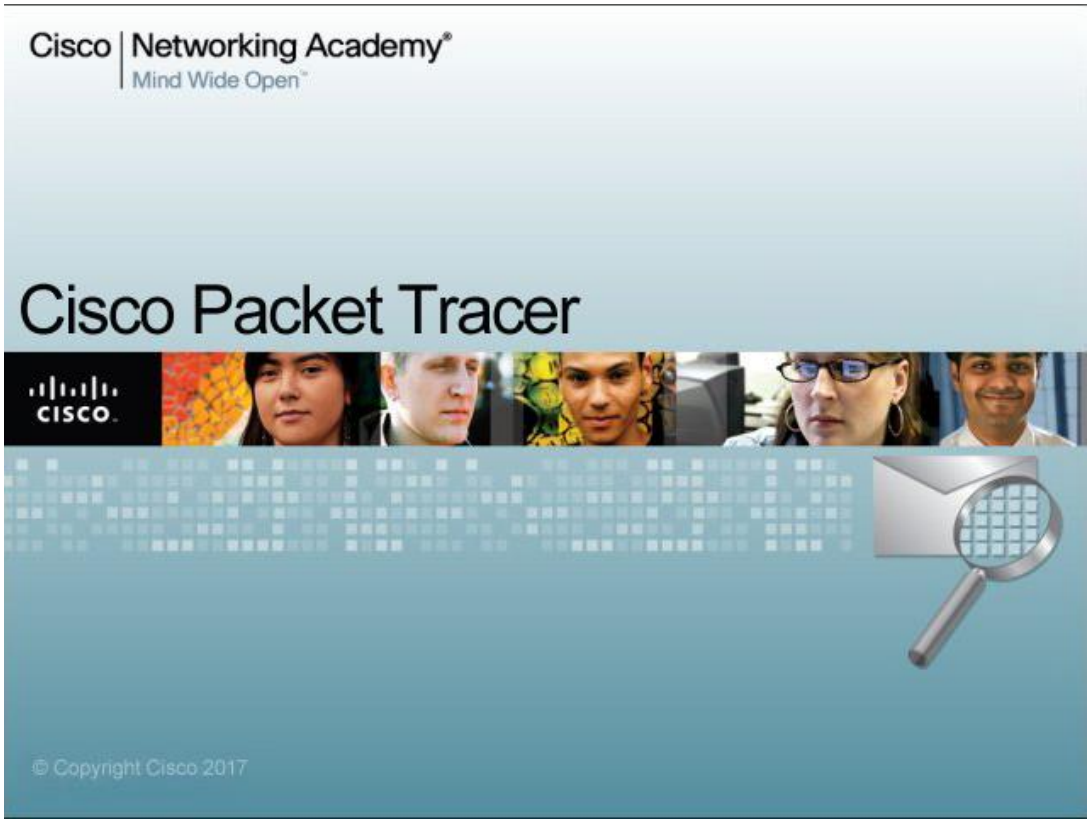


Fig. 1 - Tela de boas vindas do cisco Packet Tracer

1.1.3. Como usar o cisco Packet Tracer

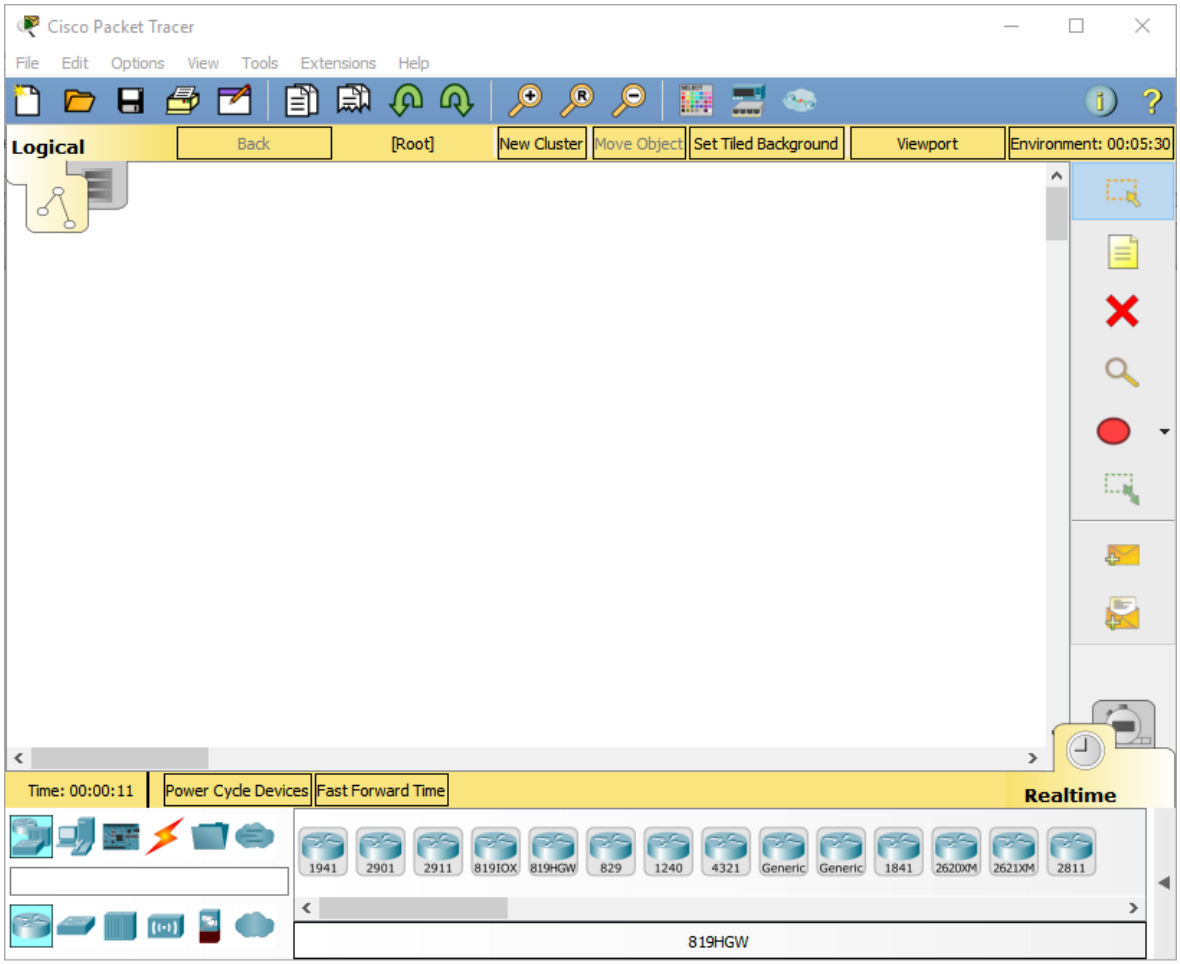


Fig. 2 - Área de trabalho

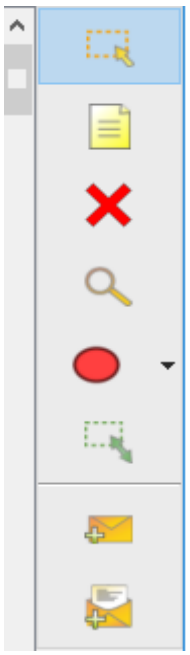
Para usar o Packet Tracer, precisamos primeiro conhecer e entender as partes que compõe a própria área de trabalho do Software.

O próprio software dispõe:

Menu principal, que integra (FILE, EDIT, OPTIONS, VIEW, TOOLS, EXTENSIONS e HELP), ainda no mesmo menu podemos encontrar as opções de acesso rápido como; **Novo** (NEW) para adicionar um cenário novo, de **Abrir** (OPEN) para abrir um cenário anteriormente feito, de **Guardar** (SAVE) para guardar seus cenários, de **Imprimir** (PRINT) para imprimir as suas topologias, um **Assistente de trabalho** (ACTIVITY WIZARD) e outros que aprenderemos com o tempo de práticas e com a necessidade dos mesmos.

No menu **FILE** (Ficheiro) encontramos as opções descritas no menu de acesso rápido. Não vamos entrar em tantos detalhes, pois aprenderemos mais sobre algumas opções a medida que vão surgindo as necessidades de uso. De um modo geral o que importa para nós são as informações relativas à construção de um cenário de rede.

1.1.4. Ferramentas para manipulação de dispositivos



- ✓ **Seleccionador** (**Select**) – permite seleccionar dispositivos e conexões;
- ✓ **Nota** (**Place Note**) – permite adicionar notas ou identificação;
- ✓ **Excluir** (**Delete**) – permite excluir dispositivos, conexões e notas exceptuando conexões sem fios;
- ✓ **Inspeccionador** (**Inspect**) – permite visualizar a tabela correspondente ao dispositivo seleccionado, entre elas podemos citar ***ARP, NAT, DNS Cache, MAC, IPv6;***
- ✓ **Desenhador** (**Draw**) – permite adicionar um desenho no cenário, permitindo delimitar uma área da topologia;
- ✓ **Redimensionar Forma** (**Resize Shape**) – permite redimensionar a forma desenhada no passo anterior.
- ✓ **PDU Simples** (**Simple UDP**) permite enviar pacotes do tipo ICMP entre dispositivos para testar conexões;
- ✓ **PDU Complexos** (**Complex UDP**) – permite enviar pacotes personalizados entre dispositivos conectados.

1.1.5. Dispositivos e conectores (equipamentos)

Para uma abordagem mais clara e sucinta dos conteúdos a serem abordados, mostraremos alguns dispositivos e conectores (equipamentos) de redes que vamos usar no ambiente cisco Packet Tracer mais que também são encontrados na vida real. As configurações que usaremos são válidas principalmente para equipamentos ciscos (mesmo na configuração

real) podem ser pouco aplicáveis em alguns equipamentos de redes de outras companhias. Ex.: a companhia Huawei, TP-LinK.

Ah! Se não são aplicadas então porquê estuda-los? Um bom profissional sabe. A necessidade faz com que adoptemos diferentes equipamentos de diferentes fabricantes em cada instalação de rede que nos forem solicitar.

Vamos aclarar bem as coisas. Os nomes dos equipamentos e procedimentos de configuração são válidos para todas as companhias ou fabricante de equipamentos de redes, o que praticamente muda são os nomes dos comandos a usar. Agora mostraremos as categorias dos equipamentos que usaremos ao longo das topologias. Como já foi frisado, alguns equipamentos serão conhecidos com o tempo e com a necessidade de uso.

1.1.5.1. Roteadores (Routers)

Roteadores (routers – do inglês) são equipamentos ou dispositivos de rede que encaminham pacotes de dados inter-redes, criando um conjunto de redes de sobreposição. Um roteador é conectado a duas ou mais linhas de dados de redes diferentes.

No cisco Packet Tracer os Roteadores são representados por figuras circulares em 3D. Ver fig. 3.

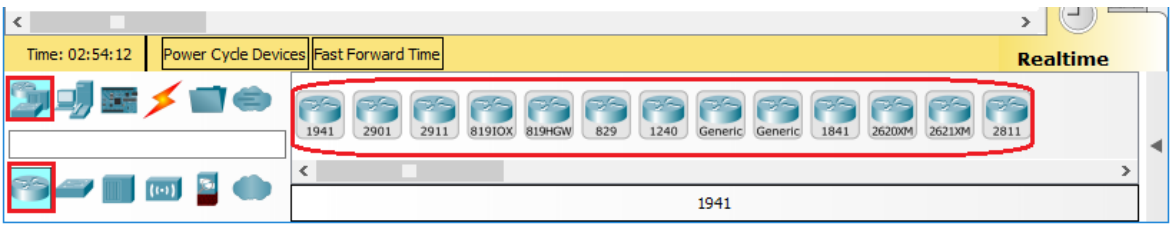


Fig. 3 – Roteadores (Routers)

1.1.5.2. Comutadores (Switches)

Um comutador ou switch como tecnicamente são chamados, é um equipamento de rede com capacidade eficaz de transmissão de dados. Na

sua maioria são equipamentos de camada 2 e foram desenvolvidos com o objectivo de oferecer qualidade na comunicação.

Na mesma categoria são enquadrados os seguintes equipamentos: Ponte ou **Bridge** em inglês e **Hubs**. Na verdade entre o Switch, Bridge e Hub a diferença é ínfima, quando se é novo no mundo de redes podemos confundir chamar todos eles de Hub, Switch ou Bridge.

Ah! Eu sou estagiário e novo no mundo das TI como saber na hora de comprar ou montar uma rede pessoal?

Bem, é simples. Se você é novo e não tem muito domínio dos equipamentos é melhor levar um profissional da área na hora de comprar seu material, caso não pode perguntar ao vendedor é claro que ele vai o informar. Por outra os equipamentos trazem consigo um folheto onde contenha toda a descrição. Na maioria das vezes essa descrição vem em inglês, daí que um profissional de TI deve saber pelo menos o básico do inglês. Outra diferença entre o hub, bridge e switch reside na quantidade de portas e na forma com são encaminhados os dados. O bridge possui apenas uma porta de entrada e outra de saída. Um switch é confundido com o hub quanto a topologia, a maior diferença reside no encaminhamento de pacotes. No ambiente cisco Packet Tracer são representados por figuras quadradas em 3D. Como apresenta a figura 4.

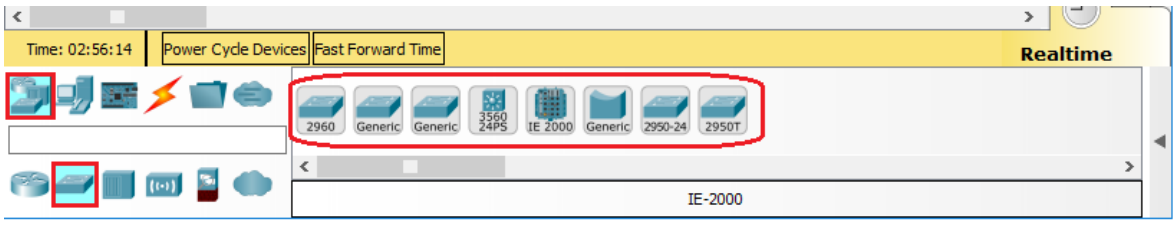


Fig. 4 – Switches

1.1.5.3. Outros dispositivos do simulador de rede cisco

O simulador cisco Packet Tracer traz uma vasta gama de dispositivos de rede descritos na figura 5, desde servidores, smartphones, tablets, (...) até solares. Os outros equipamentos serão conhecidos na prática em função das necessidades dos exercícios a resolver.

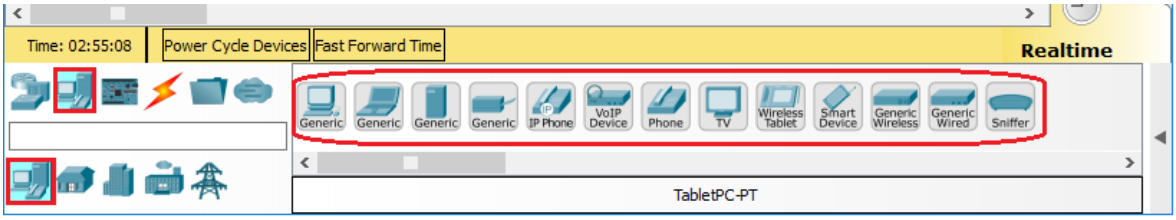


Fig. 5 - Outros dispositivos

1.1.5.4. Cabos de redes (Fios)

A figura 6 mostra os diferentes tipos de cabos de redes que serão usados nas práticas a serem desenvolvidas e que são também encontrados em qualquer loja onde vende equipamentos de rede. Os tipos de cabos representados na figura a seguir vão desde o **Console cable** até **USB cable**. Para informar que os cabos do Cisco Packet Tracer já trazem conectores como exemplo o Conector RJ45, RJ11 e outros.

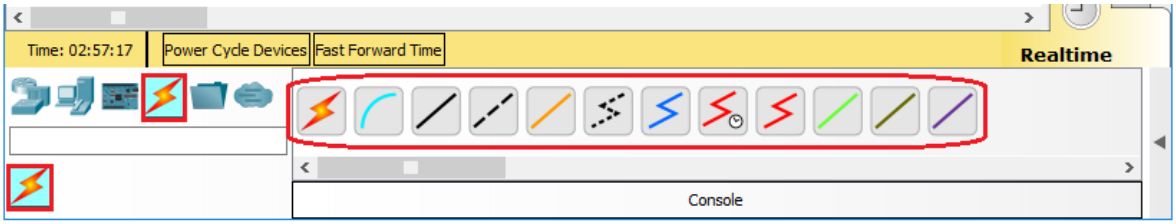


Fig. 6 – Cabos

1.1.6. Modo de simulação

O simulador Cisco Packet Tracer dispõe de dois modos de simulação, tais como: ***Real time*** e a ***Simulation***. Numa mesma topologia pode-se combinar os dois modos de simulação sem interferir na topologia a implementar. No modo real time o tráfego da informação é processado como se fosse real e não podemos ver os pacotes a serem encaminhados. E já no

modo simulation o tráfego da informação é vista a olho nu ou seja vê-se a forma como os pacotes circulam dentro da topologia.

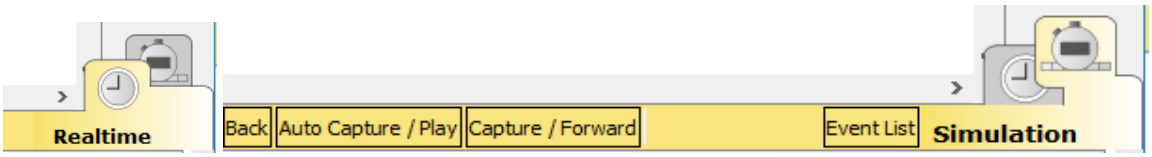


Fig. 7 - Modos de simulação (Real time e Simulation)

O modo de simulação ***Real time*** é representado por um relógio, enquanto modo ***Simulation*** é representado por um cronómetro. Para activar um ou outro modo devemos navegar com o cursor até a parte inferior a esquerda do simulador (direita para o usuário) e efectuar a devida activação.

1.1.7. Modo de visualização

Tal como vimos os modos de simulação, o mesmo acontece com os modos de visualização. O Cisco Packet Tracer dispõe também de dois modos de visualização: **o modo lógico e o físico**. No modo lógico é praticamente onde trabalhamos ou configuramos nossas topologias, adiciona-se os dispositivos e outros equipamentos de rede. No modo físico encontraremos as estruturas físicas dos equipamentos, a vista física da topologia, escritórios e mapas de cidades. Ambos modos localizam-se na parte superior no canto direito do simulador (esquerdo do usuário).

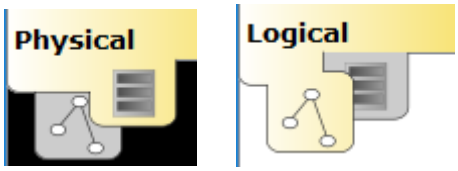


Fig. 8 - Modo de visualização de rede

1.1.8. Como adicionar dispositivos na área de trabalho?

Para adicionar um dispositivo na área de trabalho basta fazer um clique sobre o mesmo, o cursor mudará de forma, tomará a forma do símbolo (+) ou seja adicionar e em seguida clicar na área em branco, isto é na área onde deseja o inserir. Quando deseja inserir mais de um equipamen-

to do mesmo tipo, pressione a tecla **CTRL** do teclado do seu computador antes de seleccionar o dispositivo pretendido. Seleccione o dispositivo pretendido (com a tecla CTRL pressionada) Depois de adicionar quantos queira pressione a tecla **ESC**. Ver a Figura 9.

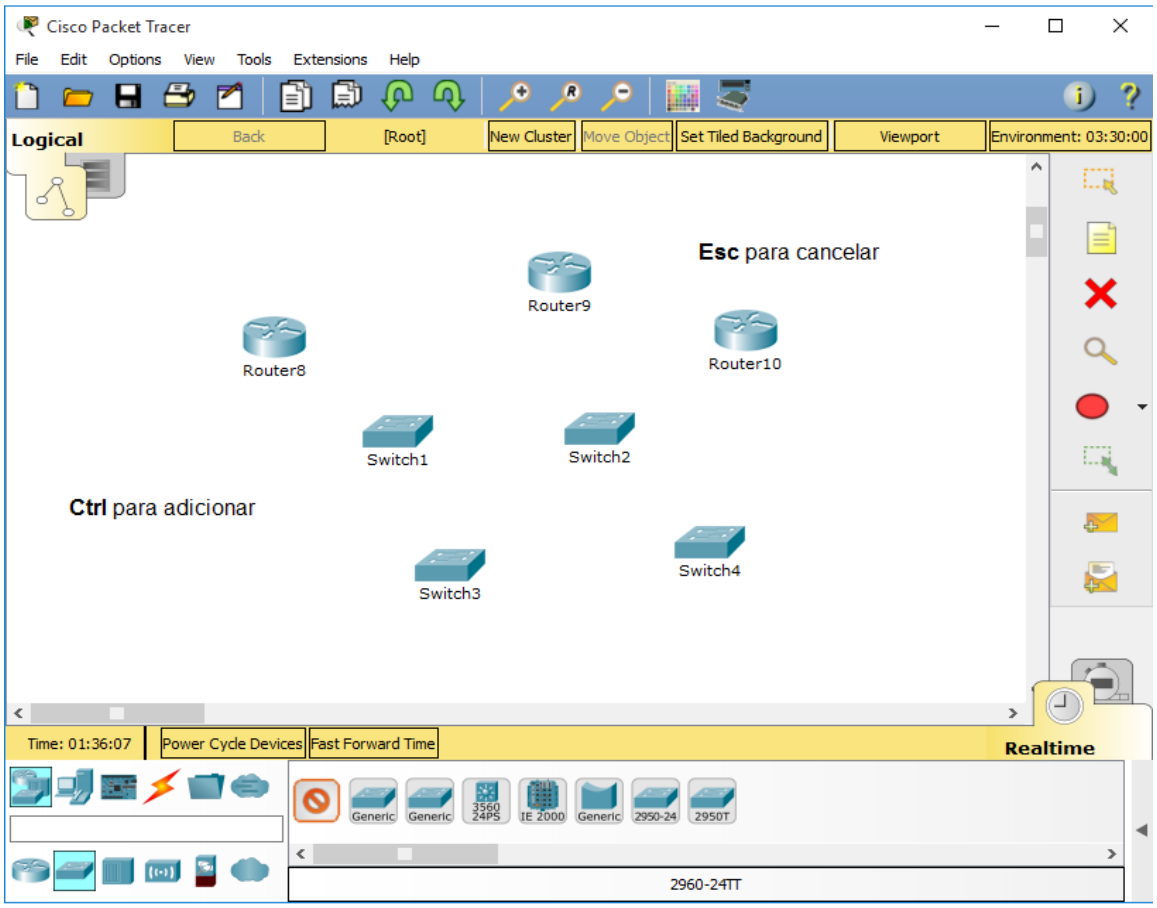


Fig. 9 - Adicionando dispositivos usando tecla Ctrl

1.1.9. Configuração de equipamentos

Nota. *Não é objectivo do guia ensinar como usar o Packet Tracer.*

Nosso objectivo é ensinar a projectar redes simuladas no laboratório virtual Cisco Packet Tracer. O estudante, assim como qualquer outro leitor interessado, deve ir explorando o software a medida que vai se acostumando com o mesmo e conhecer novas funcionalidades desta potente ferramenta. Também é de vital importância que a medida que se vai ilustrando o estudante deve colher informações relevantes que poderão o aju-

dar a resolver os exercícios propostos, principalmente os comandos a serem usados na linha de comandos.

Também deixa-se claro que não usaremos configurações gráficas demasiadas, isto é, os dispositivos da vida real são configurados a partir da linha de comandos e não na forma visual.

Se você chegou até aqui, só nos resta parabenizá-lo, já tem meio caminho andado. Agora é preciso redobrar esforços e vontade para seguir em frente. Se você deseja ser um profissional em Rede de Computadores, então trate de aproveitar o máximo possível da informação que o guia tem para lhe oferecer e lembre-se, a sabedoria é algo que se treina bastante, apesar de que alguns herdam factores genéticos que os possibilitam a aprendizagem.

Agora vamos entrar na 2ª parte do nosso guia intitulada "práticas de laboratório" onde aprenderemos como motar topologias de rede com o simulador Cisco Packet Tracer. Estude bastante e faça e refaça os exercícios, prática bastante, e lembre-se sabedoria treina-se não é algo natural.

Dica…

Qual é forma de aprender rápido os conteúdos?

É simples, depende de você…

Não existe uma fórmula comum para aprender conteúdos…

… Na verdade qualquer um pode aprender rápido os conteúdos, depende do programa que usa.

"Sucesso é conseguir o que você quer.
Felicidade é querer o que você conseguiu". Lair Ribeiro.

Parabéns!!!!!

2ª PARTE

PRÁTICAS DE LABORATÓRIO

2.1. LABORATÓRIO 1

2.1.1. Configurando de dois computadores

Topologia

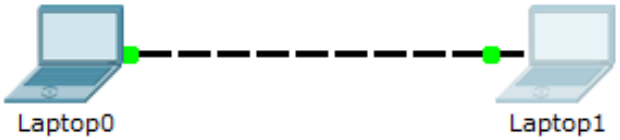


Fig. 10 - Testando conexão com ping

Competências

De um modo introdutório, objectiva-se que até finalizando a prática o estudante saiba

- Configurar topologias de redes até 10 computadores mínimos
- Definir o que é IP
- Definir máscara de rede e gateway
- Testar uma conexão usando comando ping
- Distinguir cabo Cross-Over dos demais

Fundamentos

A topologia acima simula uma rede local de apenas dois (2) computadores. Na verdade é uma rede doméstica. Sobre a teoria que aprendeu até ao momento, siga atenciosamente os passos até terminar a prática.

1º Passo – direccionado o cursor do rato para o menu ferramentas, a adicione dois computadores (Laptops). Ver Fig. 5, e desenha a topologia em causa;

2º Passo – Fazer a conexão com o cabo Cross-Over (**Copper Cross-Over**) em cada uma das interfaces de rede de cada computador (o cabo cross-over é representado por linha descontínua [- -] ver figura 6). Feito isso, siga atentamente os passos seguintes:

- Abrir o Laptop0 e dando um clique (clique esquerdo do rato) → ***Desktop → IP Configuration;***

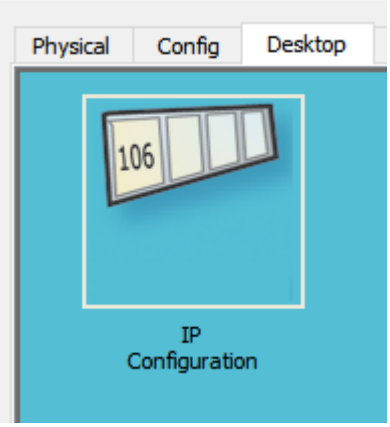


Fig. 11 - Configuração do Laptop0

Clicando no botão ***IP Configuration*** adicione os endereços conforme a figura a seguir.

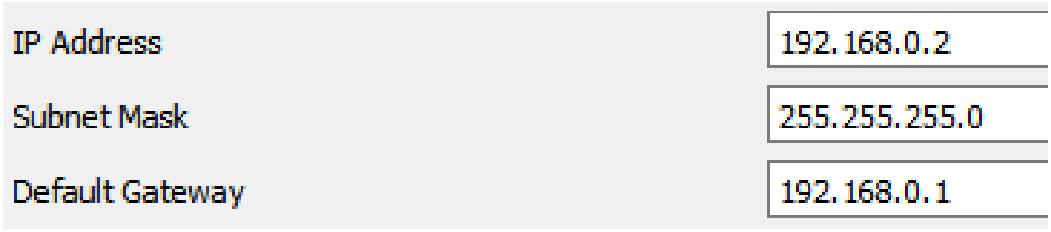


Fig. 12 – Adicionando IP no Laptop0

Terminado, feche a janela e faça o mesmo no Laptop 1 ou outro independentemente da numeração que estiver no seu ambiente de desenvolvimento.

No campo – ***IP Address*** adicione o endereço seguinte: **192.168.0.3**, ***Subnet Mask*** e ***Default Gataway*** preencha conforme a figura 12 ilustra.

Feche a janela em questão, em seguida clique sobre o botão **Command Prompt**. Na janela que abrirá digite ***Ping*** "**Endereço IP do computador a testar**", para testar a conexão entre as máquinas ou seja (***Ping 192.168.0.2***) e pressione a tecla ***Enter***. Veja o exemplo a seguir.

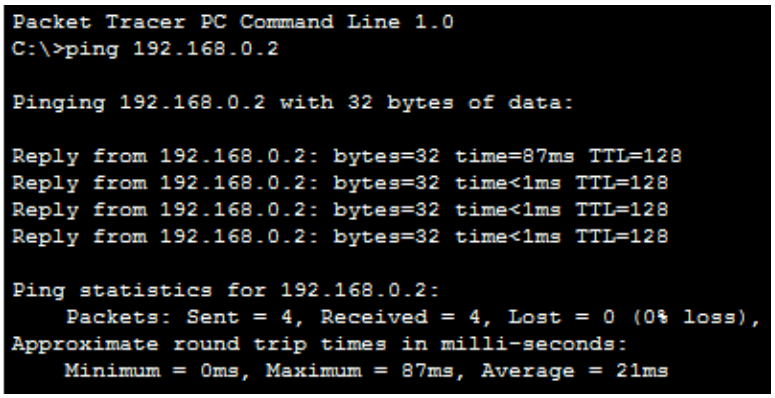


Fig. 13 - Testando Conexão usando PING

COMENTÁRIOS

PC> Ping 192.168.0.2

Disparando 192.168.0.2 com 32 Bytes de dados

Resposta de 192.168.0.2: bytes=32 tempo=0ms TTL=128

Resposta de 192.168.0.2: bytes=32 tempo=0ms TTL=128

Resposta de 192.168.0.2: bytes=32 tempo=0ms TTL=128

Resposta de 192.168.0.2: bytes=32 tempo=0ms TTL=128

Estatística do ping para 192.168.0.2:

Pacotes: Enviados=4, Recebidos=4 Perdidos=0 (0% de perda)

Aproximar um número redondo de vezes em milissegundos:

Mínimo=0ms, Máximo=0ms, Média=0ms

No entanto, falamos, falamos e explicamos, mais você acabou ficando perdido no meio de tantos termos técnicos sem perceber nada. Não é mesmo?

É isso aí, as vezes as coisas rodam um pouco na cabeça e ficamos perdidos, mais não se preocupe, tudo virá ao normal. Acostume-se e não siga *traduzindo* do *inglês* para *português* todos termos que te vão aparecendo. Algumas traduções são danadas. No mundo de TI o que conta é a vaidade tecnológica, os termos devem ser pronunciados em sua língua original.

É bem verdade, eu percebi que você não intendeu o que é um *IP Address*, *Subnet Mask* e *Default Gateway* pior ainda *Copper Cross-Over.*

IP Address? *Um endereço de IP ou simplesmente IP Address do inglês é um número lógico separado por pontos que identifica cada computador na rede. Ou seja é um indentificador logico. Enquanto um computador estiver ligado numa rede ele será identificado por um IP.*

Subnet Mask? *Uma Subnet mask ou simplesmete* ***máscara de rede*** *em português é um número lógico com 32 bits tal igual ao IP de rede e cuja função é identificar quais bits pertencem a rede e quais pertencem aos hosts.*

Default Gateway? *Um Gataway é um IP único que representa a porta de saída para encaminhar pacotes a outros computadores (estando ou não a mesma rede), normalmente é o primeiro da rede.*

Agora que já sabes ficou simples não é mesmo? Em resumo estes foram os passos necessários para colocar dois computadores a conversarem entre si. Cada prática é uma prática, tenta aprender ao máximo em cada prática que for fazendo. Em caso de não perceber a prática anterior não avance pela seguinte. Repita e pratique até aprender e só depois avance pela seguinte. Aprendeu-se como configurar topologias simples e testar uma conexão usando o comando *ping*, definimos o que é um IP, Máscara de rede e Gateway. Utilizamos também um cabo cross-over para interligar os computadores. Um cabo cross-over é aquele cujas extremidades usam padrão Ethernet diferente, isto é, se numa das extremidades está configurada o padrão ***Ethernet A*** noutra é a ***B***.

Resolva a ficha de exercícios a seguir:

2.1.1. Auto avaliação

A ficha de exercício em causa tem por objectivo consolidar o aprendizado anterior e colocar em disposição um desafio ao estudante para saber se este aprendeu ou não.

Topologia:

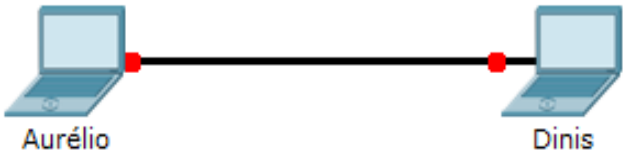


Fig. 14 - Exercício 1

Fundamentação

Aurélio e Dinis são irmãos. Têm uma empresa de emissão de cartões de visitas e cartões PVC. Tendo a necessidade de implementar uma LAN que pudesse facilitar a comunicação e transferências de arquivos entre as duas máquinas, convidaram um técnico que fez a instalação a rede. Bem, a instalação foi bem-sucedida, os IPs foram bem introduzidos. Mas observou-se um problema, a máquina de Aurélio não consegue receber dados vindo de Dinis. Você como amigo e estudante de rede foi convidado para dar solução ao problema.

Máquina de Aurélio:

IP: *192.168.11. 100*

Máscara: *255.255.255.0*

Gateway: *192.168.11.1*

Máquina de Dinis:

IP: *192.168.11. 101*

Máscara: *255.255.255.0*

Gateway: *192.168.11.1*

Com base aos conhecimentos adquiridos resolva:

a) Desenhe a referida topologia;
b) Digite os endereços;
c) Teste a configuração e solucione o problema.
d) Qual foi o erro cometido pelo técnico?
e) Quais competência adquiriu com a resolução deste problema?
f) O que é um Cabo directo e o que é um cabo Cross-over?
g) O que é um endereço de rede?
h) O que é uma máscara de rede?
i) O que é o padrão Ethernet?

2.2. LABORATÓRIO 2

2.2.1. Envio de pacotes por difusão

Topologia

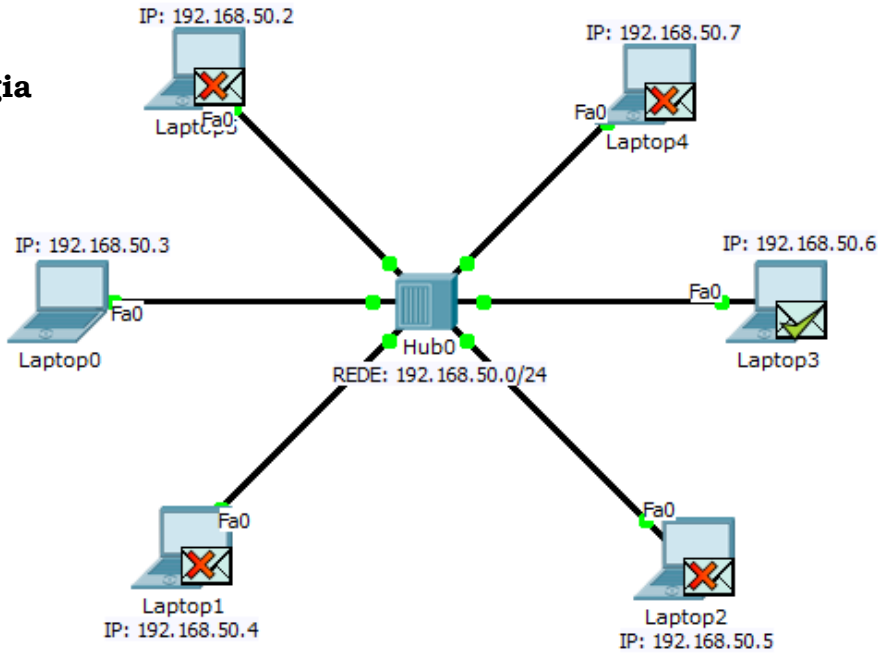


Fig. 15 - Topologia estrela usando HUB

Competências

Queremos que até ao final do laboratório o aprendiz saiba:

- Distinguir topologia em estrela com hub
- Endereçar pacotes por difusão
- Definir hub

Fundamentação

Eis uma topologia estrela com HUB onde é apresentado o teste de envio de pacotes. As redes em estrela são as mais comuns hoje em dia, utilizam cabo par trançado (entrelaçado) e um hub como ponto central (pode ser um Switch). O hub sendo um equipamento repetidor de sinal de rede se encarrega em redistribuir os **dados**[1] para todas as estações a ele

[1] *É a menor unidade de transmissão numa rede. No modelo OSI os dados provenientes da camada de aplicação são enviados para baixo na camada de transporte, onde são transformados em pacotes…*

conectado. Em uma rede por difusão o sinal é difundido por todas as portas do *hub* mas só o dispositivo com o MAC de destino abre o pacote ou seja somente o destinatário tem autoria de o abrir.

Na topologia acima referida vemos que todos os equipamentos encontram-se um sinal (X) no pacote enviado (excepto os Laptops 0 e 3), isto é, porque não são dispositivos a quem se destina o pacote.

- ✓ Usando as competências do laboratório 2.1 configure a topologia em causa;
- ✓ Configure os campos ***IP Address*** de cada computador, adicionando o endereço IP correspondente a cada computador, usando para o mesmo efeito no campo ***Gateway*** o seguinte endereço: ***192.168.50.1***.
- ✓ Finalizando a configuração teste sua conectividade.

Portanto, esta não é uma prática como tal. No fundo é mais uma revisão para ajudá-lo a familiarizar-se com a ferramenta.

Antes de entrar na prática seguinte elabore exercícios similares e aperfeiçoe mais. Estude teoria sobre Configuração de protocolos **DHCP** e **DNS**.

2.3. LABORATÓRIO 3

2.3.1.Configuração do DHCP e DNS

Topologia

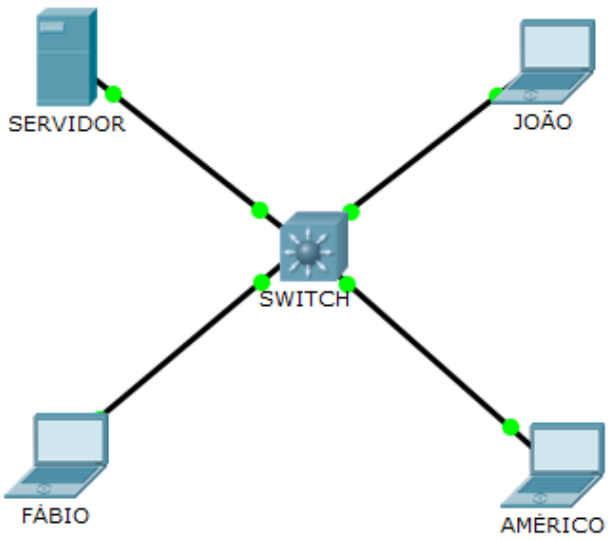


Fig. 16 - Configuração do protocolo DHCP e DNS

Competências

Queremos que até ao final do laboratório o estudante saiba:

- Mapear uma rede cliente servidor;
- Configurar o protocolo DHCP;
- Configurar o protocolo DNS;

2.3.1.1. O que é? E configurar o protocolo DHCP?

DHCP – *Dynamic Host Configuration Protocol*: é um ***protocolo*** [2] usado para atribuir automática e dinamicamente os endereços lógicos (Endereços IPs) às máquinas. É um protocolo baseado na arquitectura Cliente – Servidor para a atribuição dinâmica de endereços em uma rede *TCP/IP*.

Fundamentação

Dado o endereço de rede **192.168.0.0/24**, simule o comportamento da rede da topologia na fig. 16 usando os seguintes equipamentos:

- 1 Servidor
- 1 Switch Multilayer 3560 -24ps ou outro modelo com 24 portas.
- 3 Computadores

Depois de modelar a topologia sega os passos seguintes:

1º Passo – Abrir o Servidor (dando um clique sobre o mesmo)

2º Passo – Aba (separador) ***Desktop → IP Configuration***

3º Passo – Clique no botão (***static***), preencha os campos IP Address, Subnet Mask, Default Gateway e DNS Server conforme a figura 17. Praticamente os campos mencionados não são novidades, já são familiares com excepção ao campo DNS Server.

[2] *Conjunto de convenções ou regras estabelecidas para permitir comunicação entre duas ou mais entidades de diferentes sistemas.*

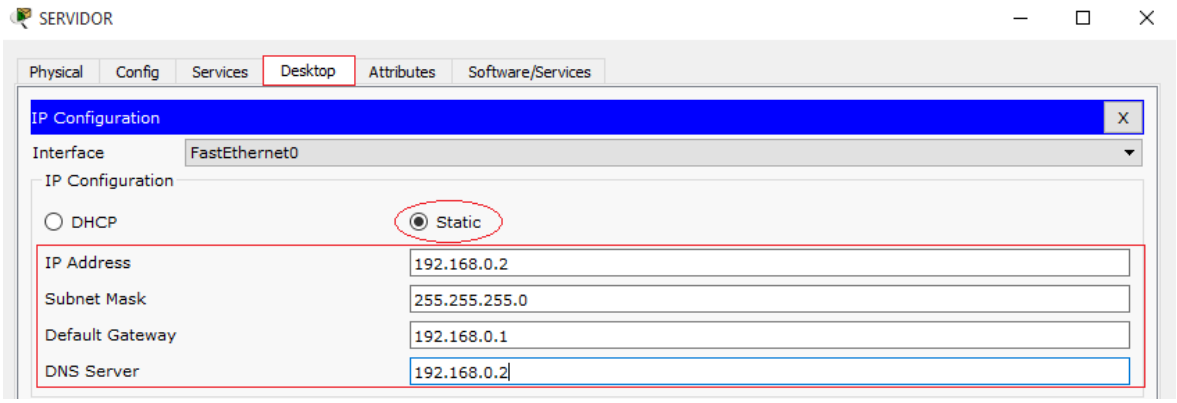


Fig. 17 - Atribuir IP estáticos ao servidor

4º Passo – Feche a aba ***IP Configuration*** e vá em Serviços (**Services**) ou **Config** em caso de versões anteriores. Configure o protocolo ***DHCP*** veja a figura a seguir e finalize clicando em **Save**.

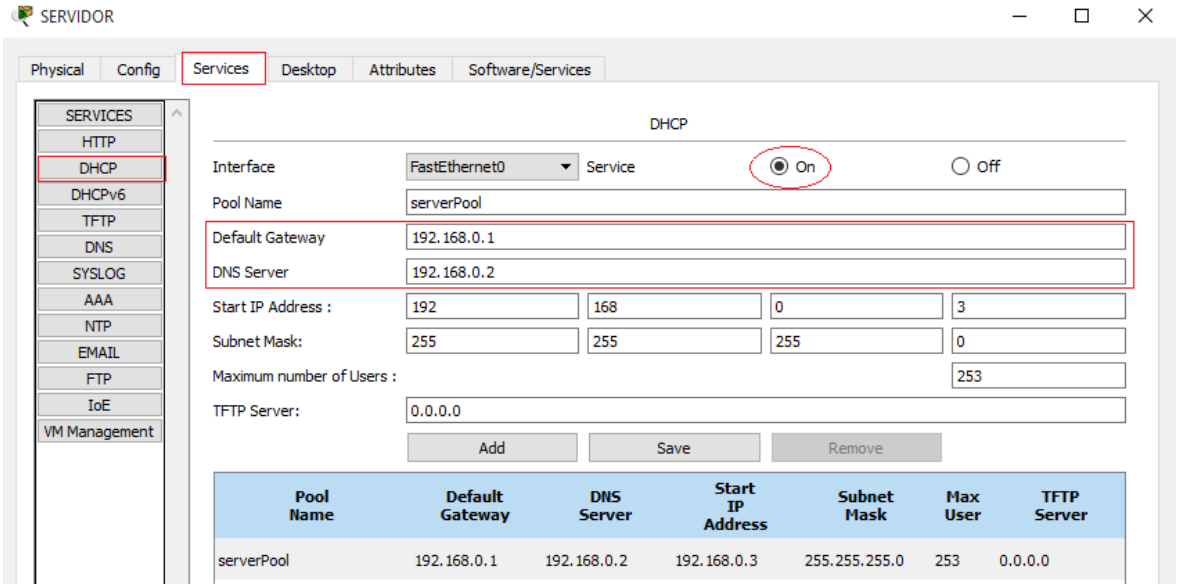


Fig. 18 - Configurando DHCP

Para que haja comunicação é indispensável que as máquinas recebam IPs. Para tal, é necessário algumas configurações que veremos nos passos seguintes.

Vamos juntos! Feche a janela do ***servidor*** em que te encontras, vá a cada máquina e faça conforme os passos seguintes:

1º Passo – Clique sobre a máquina que pretende atribuir endereço via ***DHCP*** → Janela principal → ***Desktop → IP Configuration → DHCP*** e aguarde 5 segundos. O Servidor enviará o IP solicitado pela máquina. Veja a figura a seguir:

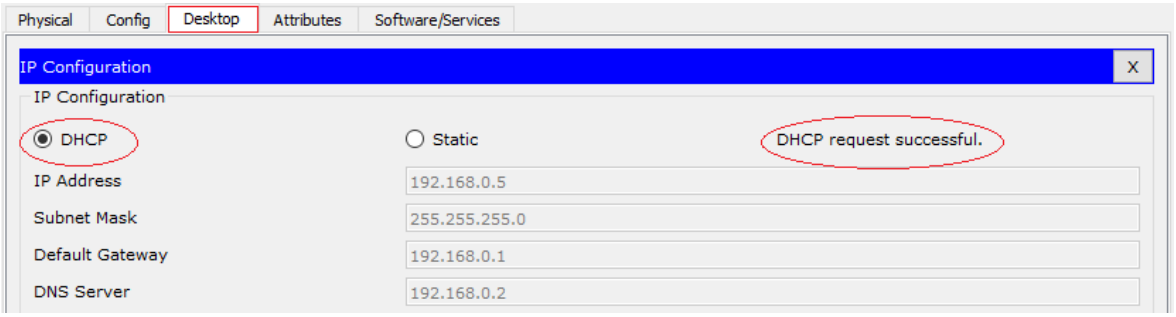


Fig. 19 - Requisitando IPs via DHCP

... Agora faça o mesmo com todas as máquinas restante. Lembre-se, nesta prática o autor faz menção de 3 computadores, poderia ser 10, 20, ou mais. No caso de haver 10 ou mais computadores, o procedimento é o mesmo para todos os computadores (...).

Feito isso, as máquinas clientes receberão endereços e prontos para estabelecer comunicação com as demais máquinas. Teste sua conexão usando ping.

2.3.1.2. Configuração do protocolo DNS

DNS – *Domain Name System*: (Tradução de nomes de domínio) é um mecanismo de tradução de nomes em endereços IPs e vice-versa (Camada de Internet do modelo TCP/IP). Em geral é mais difícil ter que fixar o endereço IP que um simples nome. Praticamente o DNS funciona como uma banco de dados. Graças o DNS, senão teríamos que decorar os IPs de cada URL ou domínio que quiséssemos acessar.

Exemplo: Torna mais fácil fixar o www.isced.ed.ao que o endereço de rede 172.13.0.0.

Como configurar o DNS no Cisco Packet Tracer?

A configuração do DNS no Cisco Packet Tracer é bem simples.

Vamos configurar o DNS no cenário anteriormente configurado.

Siga as instruções a baixo:

Voltando para o **Servidor**, na aba **Services** (ou **Config** para versões anteriores) clique no botão **DNS** ver figura a seguir.

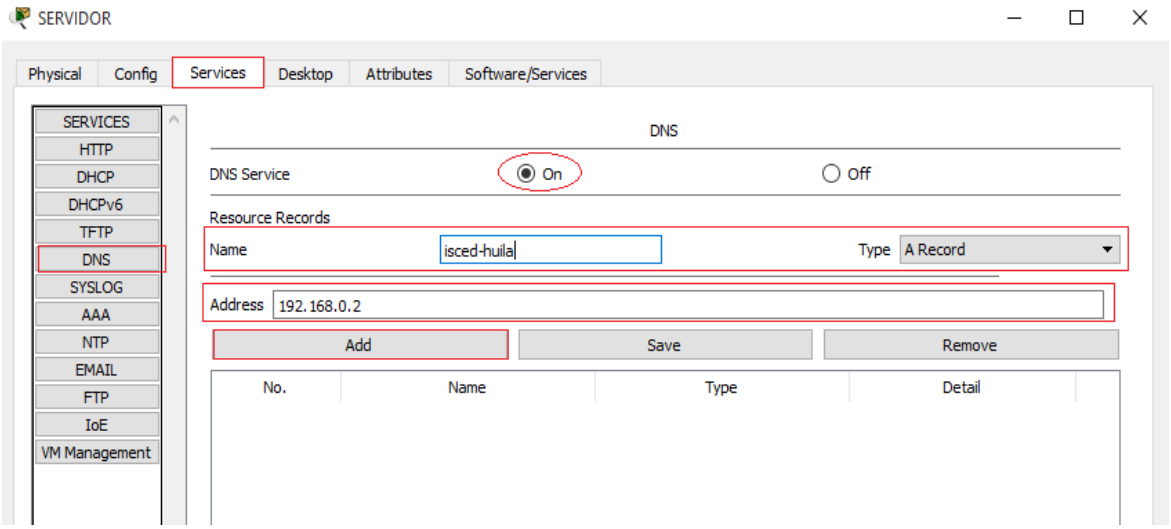


Fig. 20 - Configurando o protocolo DNS

1º Passo – Dê um clique no botão ***DNS*** e preencha os campos, tal como se apresenta na figura 20.

2º Passo – preencha o nome a ser traduzido (no com Name), no campo Address (Endereço IP) preencha o IP do servidor e clique em Add (Adicionar), lembrando que neste caso o endereço do servidor é 192.168.0.2.

Volte a adicionar os nomes possíveis conforme o exemplo da figura 21.

N.I:

Um único endereço pode traduzir vários nomes.

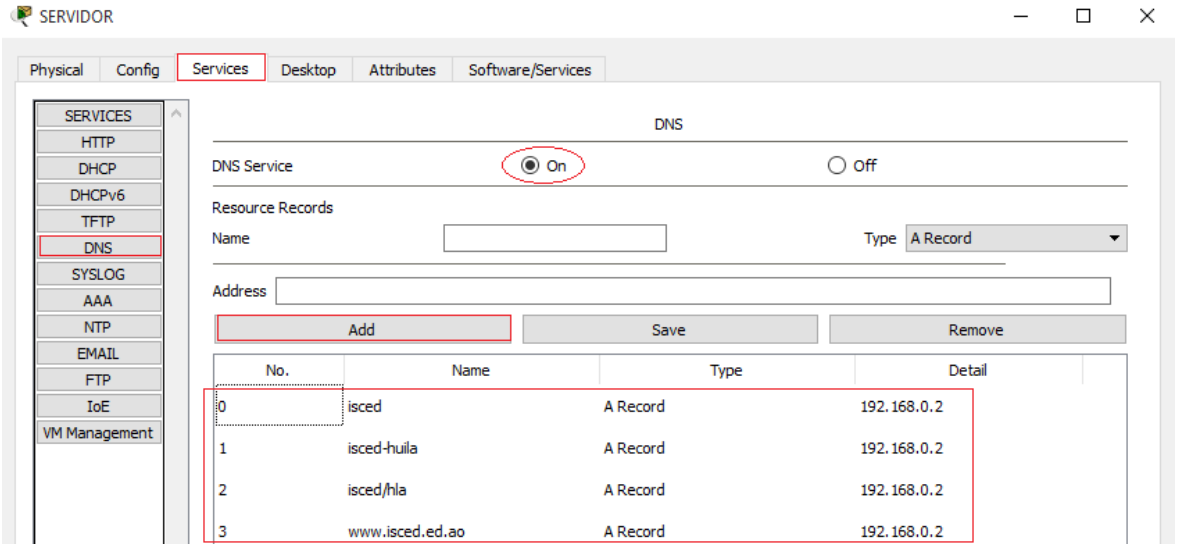


Fig. 21 - Tradução de nomes

– Fechando a janela do servidor e, voltando a um computador cliente para far-se-á os testes.
– Abra um computador cliente e clique em Web Browser. Siga a figura a baixo.

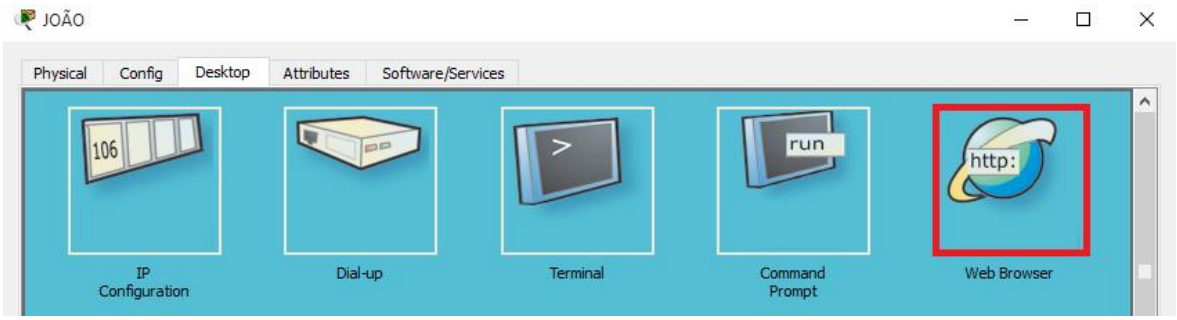


Fig. 22 - Testando DNS via http

– Digite um dos nomes anteriormente cadastrados (Fig. 21) no campo URL. Ver a Fig. 23. Se a configuração for bem-sucedida aparecerá a página da Cisco com notas de boas vindas.

No nosso exemplo a página já se encontra personalizada. Caso domine um pouco de HTML então vá as propriedades da página e personalize-a

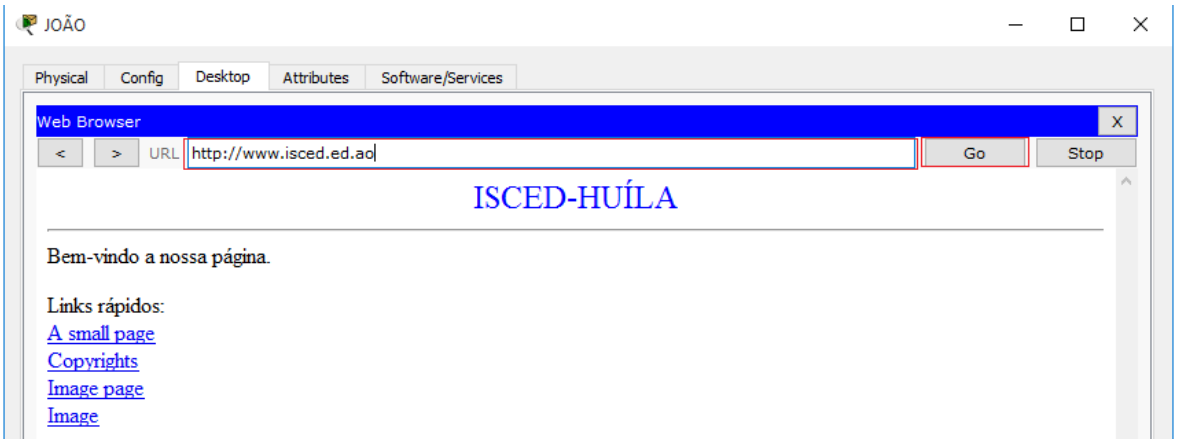


Fig. 23 - Procolo http

Resumo

Como resumo aprendemos como mapear redes cliente servidor e aprendemos a configurar protocolos DHCP e DNS, distribuímos IPs aos computadores, depois de configurar o DNS testamos com o protocolo http.

2.3.1.3. Auto avaliação

a) Em poucas palavras explica o que aprendeu com este laboratório?
b) Explique detalhadamente para que serve o DHCP;
c) Para que serve o protocolo DNS?
d) O que é o protocolo http e para que serve?
e) O que é um servidor?
f) Define switch e suas funcionalidades.
g) Observe detalhadamente a topologia e explique que tipo de cabo foi usado na topologia em causa?
h) Configure os protocolos DHCP e DNS na topologia com os seguintes equipamentos: 1 servidor, 6 computadores e 1 switch.
i) Mapeie uma rede cliente servidor que implemente 3 Switches 10 computadores, 1 servidor e configure os protocolo DHCP.

2.4. LABORATÓRIO 4

2.4.1.Configuração o serviço Webmail

Competências

- Relacionar os conteúdos aprendidos na aula teórica à prática;
- Resolver outros problemas relacionados a configuração de um serviço Webmail tando simulado quanto prático;
- Criar um domínio de rede de computador;
- Configurar um serviço Webmail de forma autónoma;
- Adicionar usuários ao domínio.

Fundamentos

Para configuração do serviço Webmail primeiro precisamos criar o domínio de rede.

Ah! O que é um domínio de rede?

É um nome que basicamente serve para identificar/localizar conjunto de computadores e/ou dispositivos interconectados na rede. É um nome concebido praticamente para memorização fácil dos endereços de computadores/dispositivos na internet.

Um segundo passo é a criação dos usuários (user) com suas devidas senhas (password).

Prática

Usando a topologia do laboratório 3 configure seguindo os passos seguintes:

- Abra o **servidor**, aba **Services** (ou **Config** para versões anteriores)
- Clique no botão ***Email*** *(Correio Electrónico)*

- Ligue o Protocolo (***SMTP*** – Simple Mail Tranfer Protocol). Deixe também o Protocolo (***POP3*** – Post Office Protocol Version 3) ligado.
- Adicione um ***Domínio*** (Domain) ao seu critério, lembrando que para o nosso exemplo usamos o ***isced.ed.ao*** e clique no botão (***Set***).
- Adicione a identificação do usuário e sua senha nos campos (***user e password***), finalmente clique sobre o botão cujo símbolo é (**+**) e volte a adicionar outros usuários sejam quantos quiser, o procedimento é sempre o mesmo, usuário, senha e clique em (**+**). Por norma os nomes dos usuários a serem cadastrados no domínio devem ser escritos da seguinte forma: {**primeiro nome [ponto (.)] último nome**}.

Ex: aurelio.pena

Ver a figura 24.

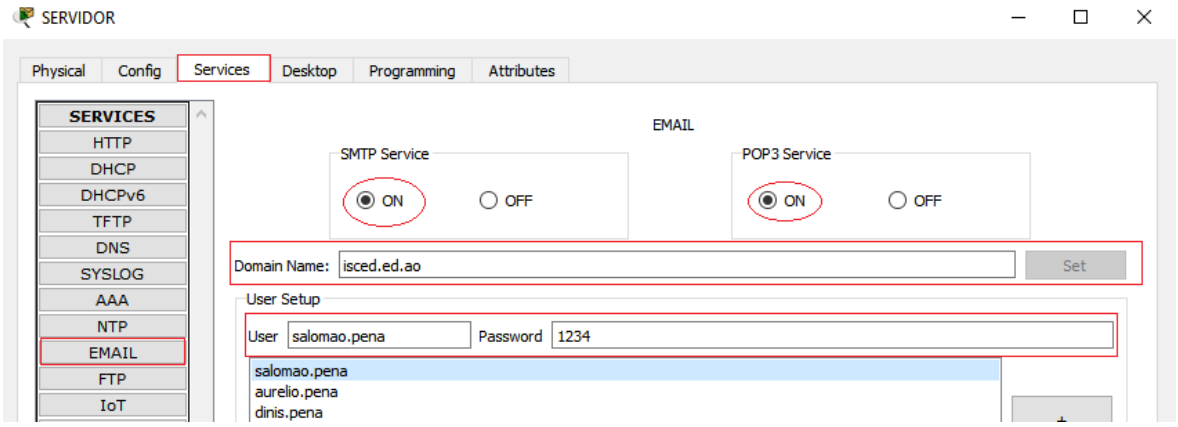


Fig. 24 - Configurando Domínio e adicionando usuários

N.I: *Como norma, o nome do Domínio (Domain) não pode ser escrito com letras maiúsculas, acentos ou outros caracteres especiais. Evite o uso abusivo de pontos (.) na separação entre palavras.*

Depois de adicionar os usuários pretendidos, ***feche a janela***. Abra uma máquina cliente (Computador) qualquer e siga os seguintes passos:

- Aba ***Desktop*** *do computador,* ***Email*** e preencha os campos da janela em causa.

- **Informações do usuário:** Nome e endereço de email.

– **Informações do servidor:** Caixa de entrada e caixa de saída.
– **Informações de Logon:** Nome do usuário e senha. Fig. 25.

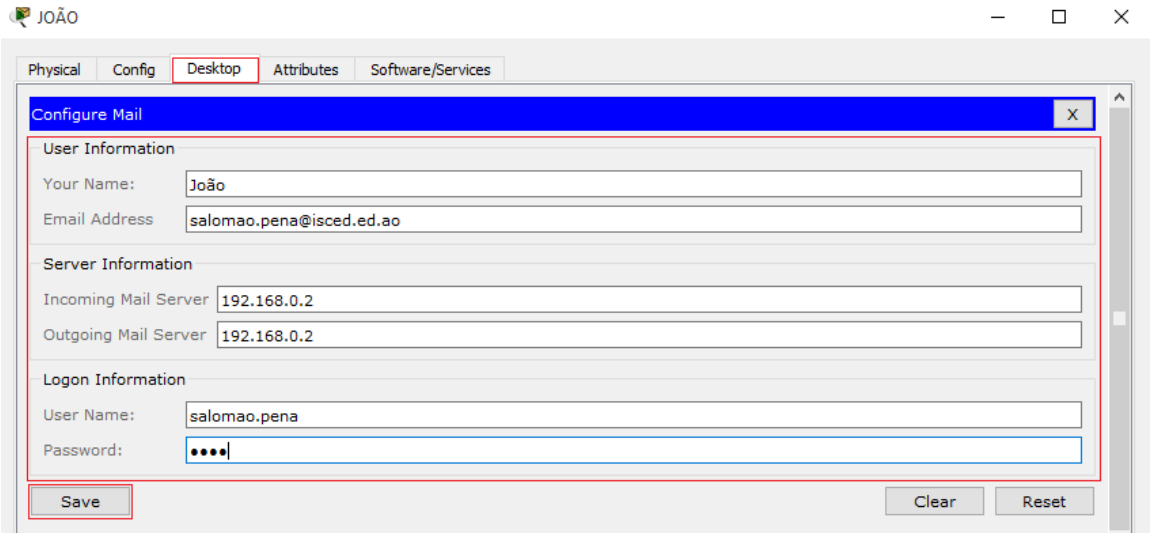


Fig. 25 - Configuração do serviço webmail na máquina de João

N.I: *Nas informações de **Logon** o nome do usuário deve coincidir com o nome de usuário cadastrado no domínio. Se não o fazer, não haverá troca de emails entre usuários. Lembre-se que no cisco Packet Tracer cada usuário ocupa um único computador, nesse caso cada usuário contido no domínio vai ocupar um computador. Na máquina de João cadastramos Salomão, e nas duas restantes cadastraremos os dois nomes restantes Dinis e Aurélio.*

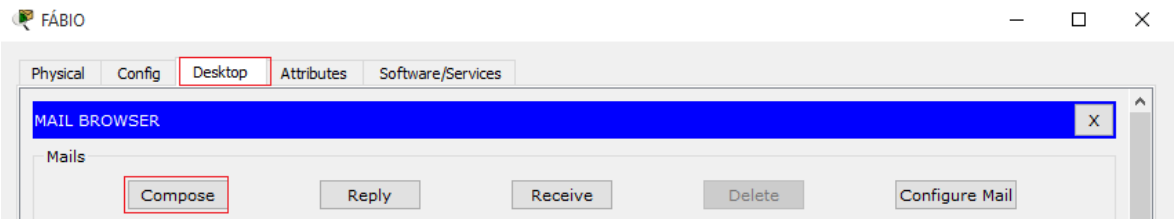


Fig. 26 - Compor email

Depois de ter configurado o email no computador de Fábio e clicar no botão **Salvar** (SAVE), ver Fig. 25, aparecerá uma janela similar a figura 26 e clique em **Compose** para compor (escrever) o email. Na janela a seguir digite o seu texto e finalize clicando e **Send** (enviar), ver fig. 27.

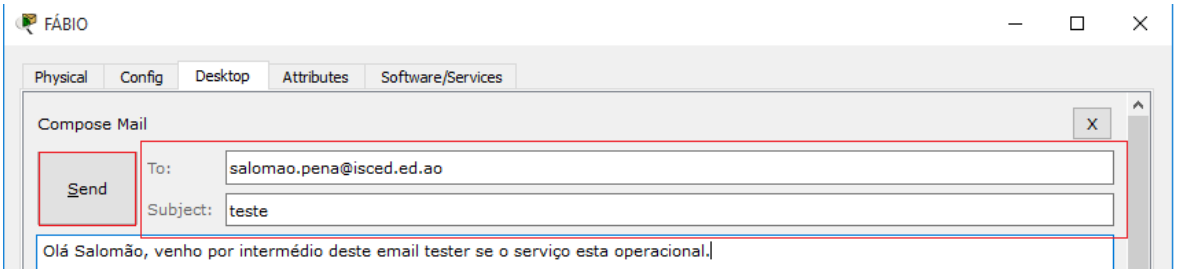


Fig. 27 - Enviar email

O Cisco Packet Tracer também tem a caixa de entrada. Para ver um email recebido clicamos em ***receive*** (recebidos).

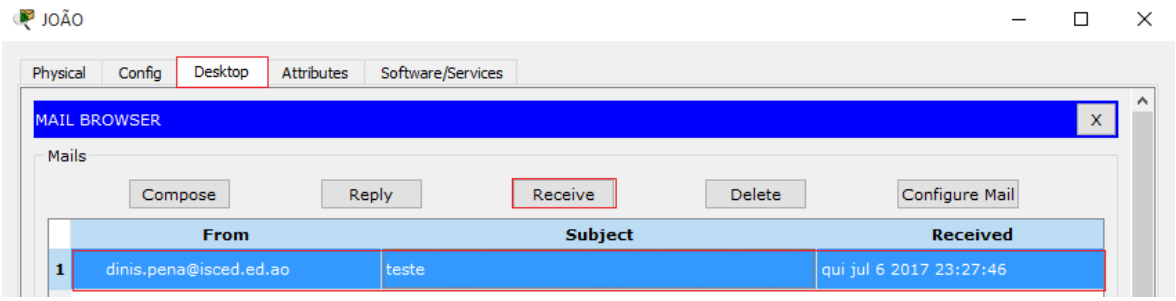


Fig. 28 - Ler email

Depois de fazer a litura clique no botão **Reply** (Responder), aparece uma tela fig. 29. Na verdade é bem semelhante a fig. 27.

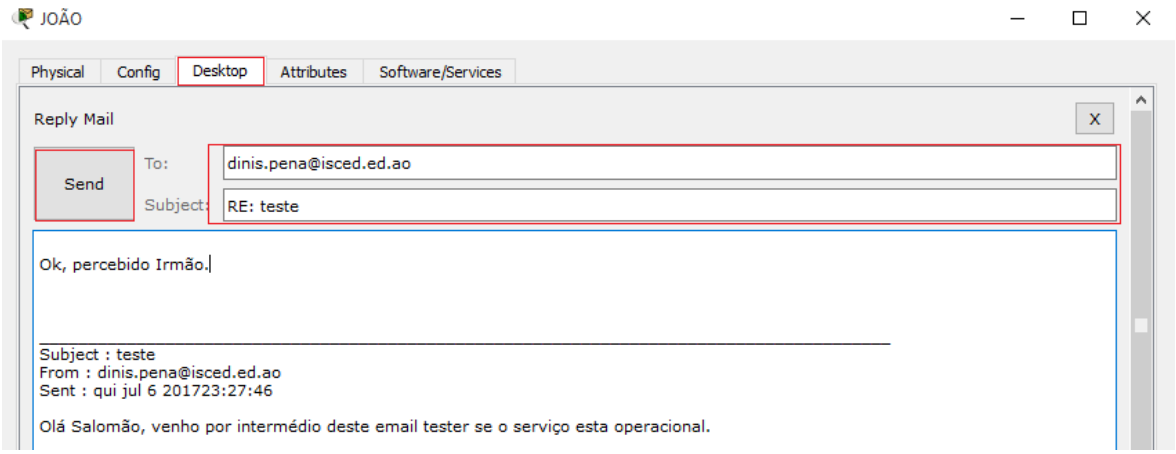


Fig. 29 - Responder email

Portanto, foram os passos a seguir para configuração do serviço webmail no Laboratório Virtual Cisco Packet Tracer. Treine bastante e resolva os exercícios propostos.

Dica de um amigo!

Lembre-se, para se ter domínio é preciso treinar bastante. Os melhores vencedores treinam todos os dias para alcançar o que desejam.

2.4.2. Auto avaliação

a) Faça um breve resumo do que aprendeu.
b) O que o comoveu neste laboratório?
c) O que de interessante achou?
d) Que curiosidade despertou em ti o laboratório em questão?
e) Para que serve um domínio?
f) Para que serve o protocolo SMTP?
g) Qual é a função do protocolo POP3?
h) Qual é a diferença entre o protocolo SMTP e o IMAP?
i) Diferencie o protocolo IMAP do POP3?
j) Identifique quais os componentes principais do sistema Webmail?
k) O que significa dizer que o SMTP é um protocolo de envio de informações (push protocol)?
l) A Empresa **Informaticom.com** sediada na província da Huíla especialmente no Lubango, bairro Comercial, é dona de vários empreendimentos e faz comércio de produtos informáticos. Emprega mais de 40 funcionários nas suas instalações e por vezes os problemas são inúmeros em relação a comunicação entre funcionários de departamentos diferentes, agendas de trabalhos, reuniões entre outros aspectos comunicativos.

Com base ao problema encontrado, a empresa solicitou-te auxílio para a implementação de um serviço Webmail. Prontamente, você aceitou e colaborou: Usando o Packet Tracer implemente o serviço Webmail na topologia a baixo e todos outros serviços capazes de garantir a comunicação viável entre funcionários da empresa. Lembrando que a topologia pode ser alterada em função da necessidade.

Topologia

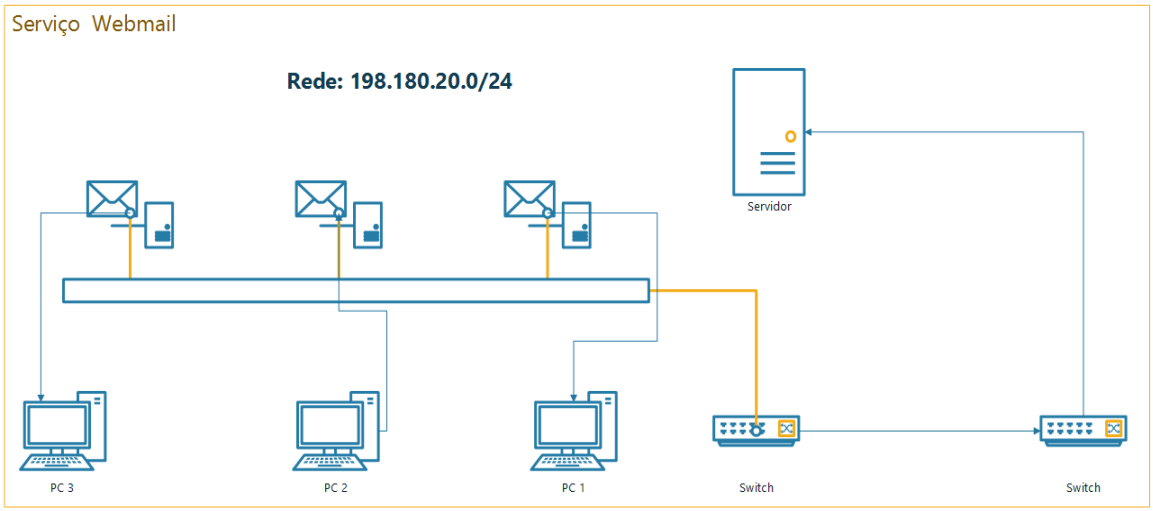


Fig. 30 - Exercício sobre o serviço mail

Equipamentos a usar

- Um servidor;
- Dois Switches;
- Três ou mais computadores;

m) Mapeie topologia estrela cliente servidor com 20 Workstations usando 3 Switches e configure também o protocolo DHCP. Implemente-a usando o IP 192.168.1.50.0, implica dizer que a máscara é natural ou seja é 255.255.255.0.

n) Faça uma breve abordagem dos serviços implementados e até agora e recrie as topologias.

o) Estude teorias sobre o protocolo OSI.

p) Estude bastante sobre o Protocolo TCP/IP

2.5. LABORATÓRIO 5

2.5.1. Domínio de colisão e broadcast

Topologia

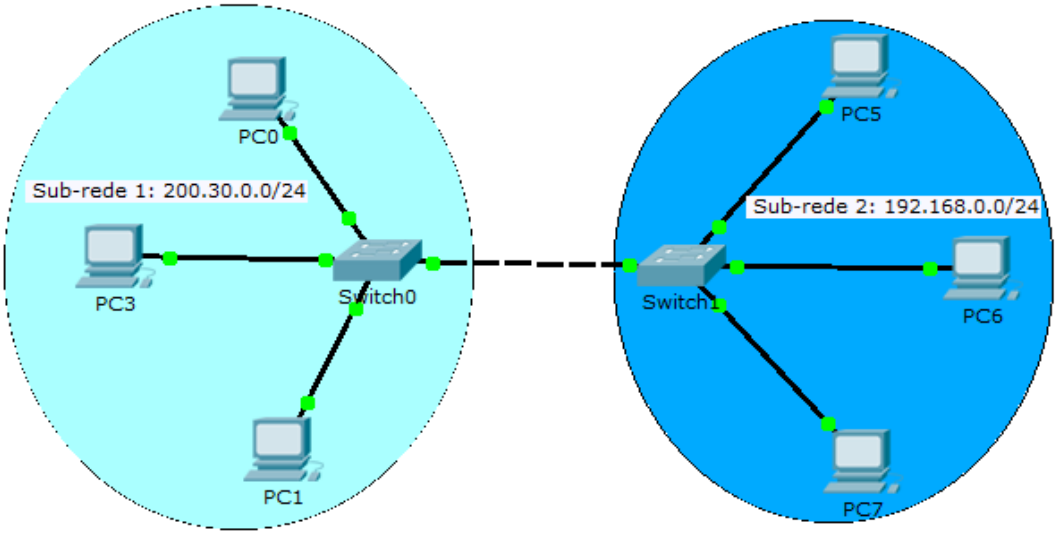


Fig. 31 - Domínio de colisões

Competências

Queremos de um modo geral que até ao final do laboratório o caro leitor adquira as seguintes habilidades:

- Perceber quais os factores influenciam na segurança e desempenho de uma rede;
- Entender como os pacotes trafegam na rede;
- Saber o que é um domínio de colisão;
- Diferencias domínio de broadcast do domínio de colisão;

Fundamentos

Para esta topologia o nosso foco assenta-se em abordar de forma precisa e concisa o que é domínio de colisões e porque ocorre. Domínio de colisões é um segmento físico de uma rede, onde possíveis pacotes colidem nos canais de comunicação, dado que interfere bastante na comunicação.

Um *Hub* é um domínio de colisão. É um, barramento lógico com um canal de comunicação que é compartilhado por todas as portas, ver laboratório 2. No *Switch*, o caso é particular, ele possui um canal exclusivo

para cada porta. O número de domínio de colisão de um *Switch* é igual ao número de portas dele. O *Hub* e o *Switch* possuem apenas um domínio de broadcast cada, e o roteador tem um domínio de broadcast em cada porta.

Domínio de ***broadcast*** é um segmento lógico de uma rede onde um dispositivo qualquer nela conectada é capaz de comunicar-se com outro sem a necessidade de utilizar um dispositivo de roteamento (Roteadores).

Dada a topologia acima, monte-a usando os seguintes equipamentos:

- 2 Switches;
- 6 Computadores;
- Configure manualmente a rede 1 usando o IP (200.30.0.0/24);
- Configure manualmente a rede 2 usando o IP (192.168.0.0/24);
- Não esquecer que os Gateways devem ser os primeiros IPs;
- Active o modo de simulação (**simulation time**);
- Apos ter feito isso teste a conexão com o comando ping seguindo os seguintes passos →Clique (esquerdo do rato) sobre o PC da rede 2 →**Desktop** →**Comand prompt,** digite **ping –t 192.168.0.3** em seguida clique em **Auto Capture/Play**;
- Observe o comportamento da rede.

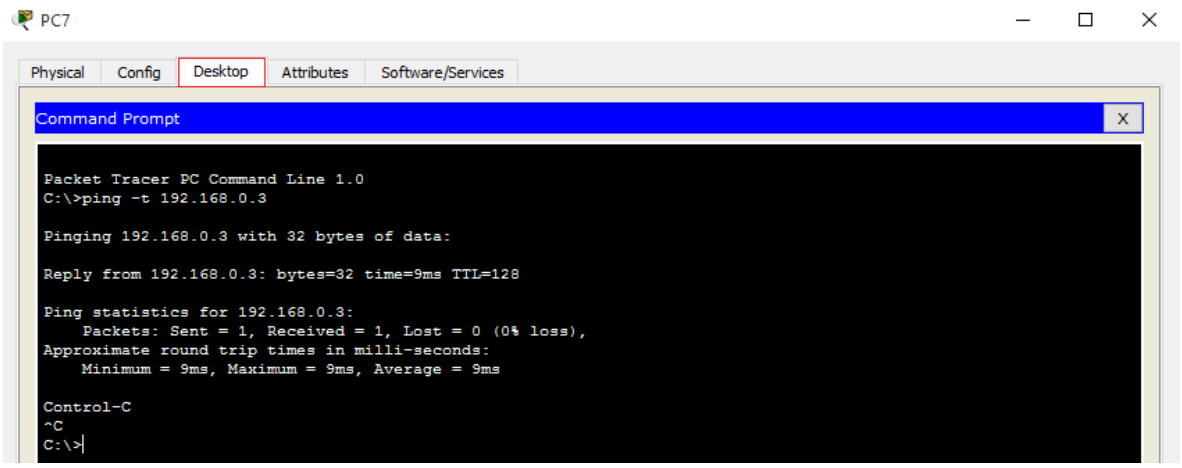


Fig. 32 - Usando loop de Ping com uma máquina

O **ping – t** é um comando que realiza loop (repetição) de um pacote na rede e para terminar clique a tecla **CTRL + C.** Feito isso clique no botão **Delete** do cenário.

Se a configuração for bem-feita o teste será bem-sucedido.

Problema: *Imagine que vários usuários em simultâneo tentassem trocar pacotes entre redes.*

O que aconteceria? Vamos ver o resultado.

– Em uma máquina qualquer da rede 2, digite **ping – t 200.30.0.2** e pressione a tecla (**Enter**), seguida do clique em **Auto Capture/Play**. Notar-se-á que haver circulação do pacote na rede até se perdendo e se voltar em **Comand prompt** será emitido uma mensagem "**Request Timed Out**" ou seja **tempo excedido**, isto porque os pacotes estão se perdendo na rede provocado por colisões.

A figura a 33 demonstra exactamente o ocorrido. Observe que a estatística do ***ping*** realizado, demonstra que foram enviados 2 pacotes, recebidos 0 e perdidos 2, nenhum deles chegou a rede de destino.

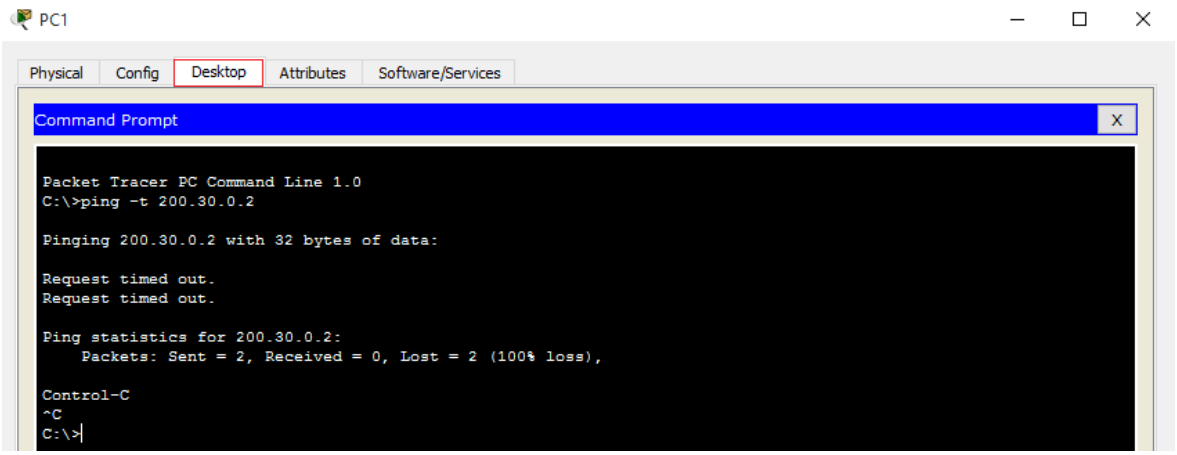


Fig. 33 - Usando loop de Ping com duas máquias

Como solucionar o problema?

Para um mesmo problema existem várias soluções. Mais para este problema existem três soluções: a primeira seria aplicar um *roteador* que sirva de *ponte* para interligar as duas redes A segunda e criar *interfaces VLAN* e uma outra solução seria criar *VLAN* (conteúdo a tratar mais a diante).

Por questões didácticas e de escolha, vamos resolver o problema usando a primeira solução. Figura 34.

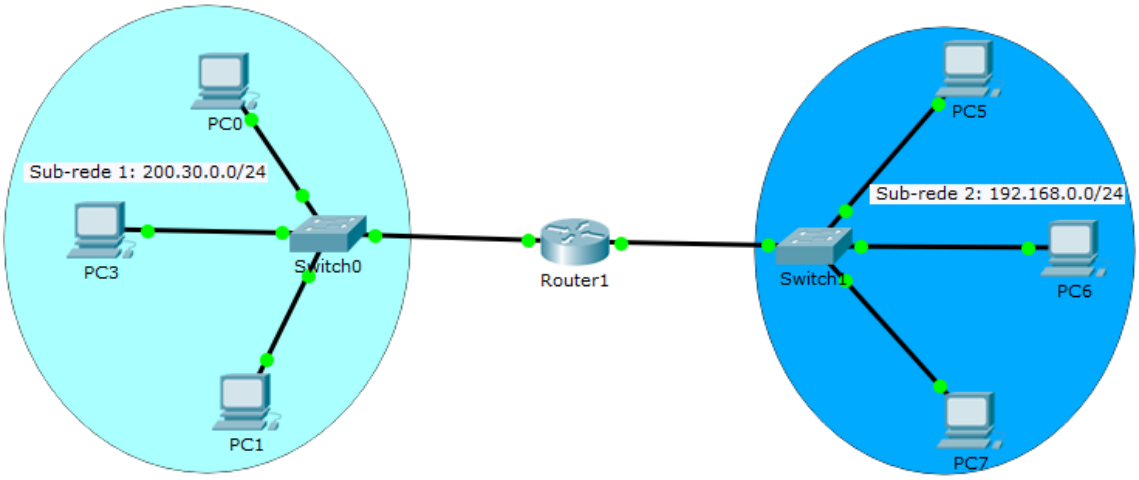


Fig. 34 - Como resolver o problema de colisões?

Com base aos conhecimentos adquiridos implemente um roteador (**Router 2911**) ver fig. 2 e 3. Interligue uma interface do roteador a cada uma das interfaces de cada **switch**.

- Dando um clique sobre o *roteador* inserido, configure a topologia em questão seguindo a figura 35.
- Configure a interface **Gigabit Ethernet0/0** que interliga o *roteador* ao *switch* da rede 1 (200.30.0.0/24). Adicione no campo **IP Address** o **gateway** (200.30.0.1) da rede 1 e clique no botão ***ON.***
- Clique no botão **Gigabit Ethernet0/1** que interliga ao *switch* da rede 2 (192.168.0.0/24) e adicione no campo **IP Address o gateway** (192.168.0.1) da rede 2 e clique também no botão ***ON.***

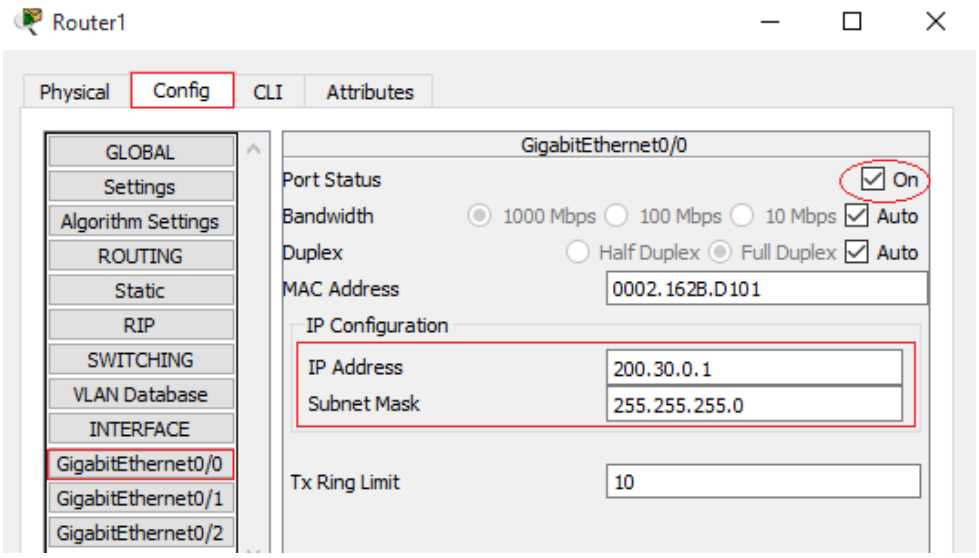


Fig. 35 - Adicionado IP na interface GE0/0

Finalmente, tente trocar informação entre a sub-rede 1 e a 2 e vice-versa. Se a configuração for bem-feita notar-se-á que a comunicação entre as duas sub-redes será bem-sucedida.

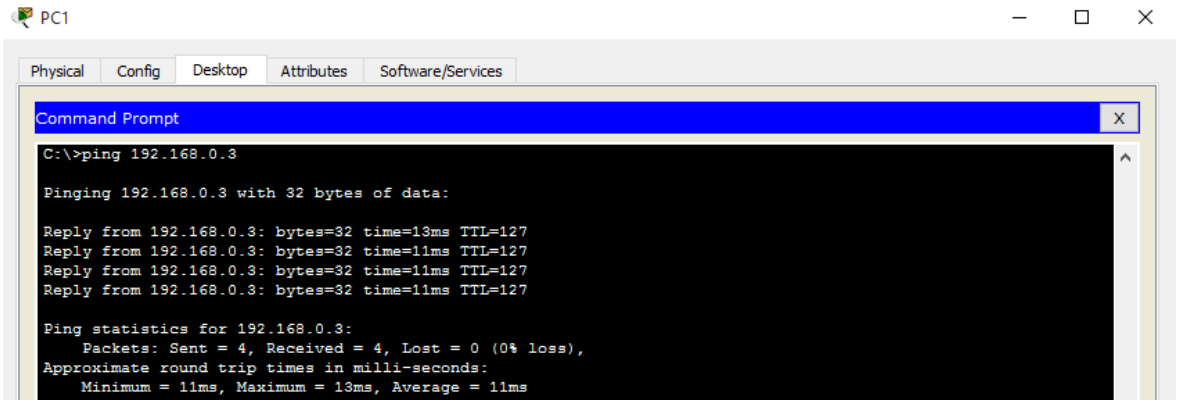


Fig. 36 – Teste de conexão após implementar o roteador

2.5.2. Auto avaliação

a) Em uma breve descrição faça um resumo de apenas 10 linhas do que aprendeu?

b) Quais os factores que influências no desempenho de um rede?

c) O que é um roteador?

d) O que é um loop?

e) Observe a figura 31 e 34 e descreva a diferença existente, quanto ao tipo de cabo e equipamentos.

f) Em quais casos se usa o cabo cross over?
g) O que é o um domínio de broadcast?
h) O que é um domínio de colisão?
i) Porquê que o Hub e Switch não separam domínio de colisões?
j) A chuva, tempestades e nuvens também são elementos que interferem na comunicação. Comente!
k) O comando *ping –t* é usado para evitar ciclos? Confirme a veracidade da afirmação!
l) No Cisco Packet Tracer a combinação (CTRL + C) é usada para colar arquivos da área de transferência. Comente!
m) Com ajuda de um colega, amigo ou mesmo a internet, procure as outras formas de resolver colisões de pacotes na rede.

2.6. COMANDOS BÁSICOS DO CISCO PACKET TRACER

Para a configurar um equipamento de rede em ambiente real, não é feito de forma gráfica. A configuração dos equipamentos é feita na *linha de comandos, nos browsers*, ou outro meio. Logo, não fugiremos dessa regra básica. Contudo organizou-se alguns comandos básicos introdutórios que usaremos ao longo dos projectos realizados no laboratório Virtual Cisco Packet Tracer. Lembre-se que da prática 1 a 5 os equipamentos foram configurados de forma gráfica, de agora em diante tudo será na linha de comandos CLI (*Comand Line Interface*). Cabe ao leitor buscar mais comandos para auxílio de determinados laboratórios. Eis os comandos:

ENABLE (EN) – *Comando para entrar no modo privilegiado*

CONFIGURE TERMINAL (CONF TE) – *Comando para entrar no modo de configuração*

HOSTNAME – *Comando para atribuir nome aos dispositivos (ROUTERS e SWITCHS)*

EXIT – *Comando para Sair de um modo para outro*

DO WR – *Comando para guardar as configurações*

WRITE – *Comando para guardar as configurações no modo privilegiado*

NO SHUTDOWN – *Comando para ligar a porta (interface de rede)*

SHUTDOWN – *Comando para desligar a porta (interface de rede)*

SHOW IP ROUTE – *Mostra as configurações de IPs atribuídos*

IP ADDRESS [Endereço] – *Comando para atribuir IP em uma determinada interface de rede (porta)*

ENABLE PASSWORD CISCO – *Comando para habilitar a senha*

ENABLE SECRET – *Comando para habilitar palavra secreta ou simplesmente senha*

BANNER MOTOD – *(@BOM DIA ROUTER@) Comando para adicionar palavra de boas vindas. A palavra deve ser limitada pelos caracteres (@)*

SERVICE PASSWORD-ENCRYPTION – *Comando para encriptar a senha*

LINE CONSOLE 0 – *Comando para entrar na linha de configuração da porta consola*

PASSIVE-INTERFACE – *Impede que o roteador receba pacotes RIP*
CLOCKRATE – *Comando para configuração da taxa de transmissão*
INTERFACE LOOPBACK [número**] –** *Configuração da interface loopback*.

Estes são alguns nomes daquilo que é o básico dos comandos a serem usados no laboratório Cisco Packet Tracer. Tente aprende-los e partir para as práticas seguintes. Não necessita partir a cabeça para memoriza-los todos, o importante é saber o que se deseja fazer e lembrar no mínimo duas (2) letras do comando desejado. Exemplo: ao invés de escrever **Enabled**, escreva somente (**En**). Também pode-se escrever a inicial do comando desejado é pressionar na tecla **TAB** (Tabulação) para completar o mesmo.

Dica...

Treine bastante, para tornar-se o melhor naquilo que quer aprender. Os mais sucedidos na vida treinam todos dias.

A partir de agora a configuração dos equipamentos será na linha de comandos. Será um processo mais complexo, tente pedir auxílio aos colegas (caso seja estudante) e forme grupo de 3 ou 4 estudantes para facilitar a resolução dos problemas.

2.7. LABORATÓRIO 6

2.7.1. Sub-redes

O uso de sub-redes é um mecanismo que permite minimizar o problema do crescimento das tabelas de roteamento na internet introduzido pele RTF 950/1985 e o uso eficiente dos IPs. Uma sub-rede é nada mais que uma divisão logica de um endereço de rede.

Praticamente cada sub-rede possui um indentificador especifico dentro da rede principal – ***SubnetID*** obtido através da divisão dos bits do campo – ***HostID***. A união dos dois campos NetID e SubnetID é chamando de prefixo de rede extsndido (*Extend – Network Prefix*).

2.7.2. Vantagens do uso das sub-redes

- Uso de um único IP Address para várias redes físicas
- Permite misturar tecnologias como *Ethernet* e *Token Ring.*
- *Possibilita a distribuição melhor do tráfego de dados*

Formato de um endereço de rede

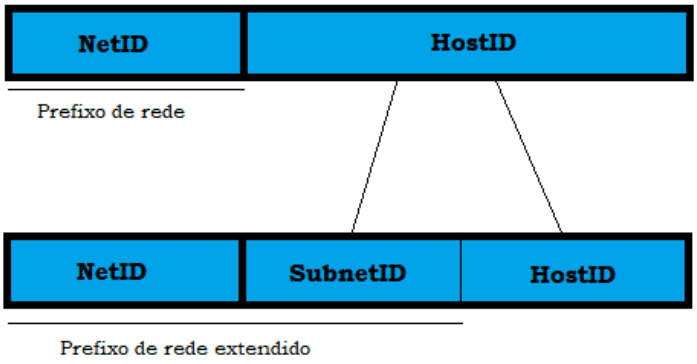


Fig. 37 - Representação do formato de endereço de rede

Em um ambiente de sub-redes como saber qual a fronteira entre *SubnetID* e *HostID*? Quais bits do endereço IP serão usados para definir sub-redes?

Como forma mais simples e solução viável é a utilização da máscara de rede (*Subnet Mask*). A máscara de rede é um número com 32 bits usado para identificar um *extend network prefix* (*NetID* + *SubnetID*) de um

HostID em um *IP address*. A máscara de rede é, também usada para determinar se um *IP address* está localizado dentro de uma rede local ou remota. Os bits a 1 (um) da máscara representam a rede (*NetID*) e os bits a zero (0) representam as máquinas (*Hosts/HotID*).

Nota: *Cada Host de uma rede TCP/IP requer uma máscara de sub-rede, isto significa que mesmo que tivéssemos apenas um segmento único de rede.*

A máscara pode ser ***Default (****Padrão****)*** quando o endereço não está dividido em sub-redes. ***Personalizada*** quando é dividida em sub-redes. Exemplos de máscaras ***Default*** em função da classe:

- Classe A: 255.0.0.0
- Classe B: 255.255.0.0
- Classe C: 255.255.255.0

Uma máscara de redes são interpretados em binários logo ficaria:

- Classe A: 11111111.00000000.00000000.00000000
- Classe B: 11111111.11111111.00000000.00000000
- Classe C: 11111111.11111111.11111111.00000000

Em função disto a cada bit a 1 (um) acrescido em um das máscaras estaríamos a calcular sub-redes. Exemplos:

Dado o endereço 192.168.20.0 da classe com máscara *default* ficaria da seguinte forma:

11111111.11111111.11111111.00000000=255.255.255.0

11111111.11111111.11111111.11000000=255.255.255.192

Logo teríamos os endereços seguintes: 192.168.20.0, 192.168.20.64, 192.168.20.128 e 192.168.20.192. Viu é simples e muito prático. Com a máscara .192 temos 4 *IP Address.*

2.7.3. Mapear sub-redes

Topologia

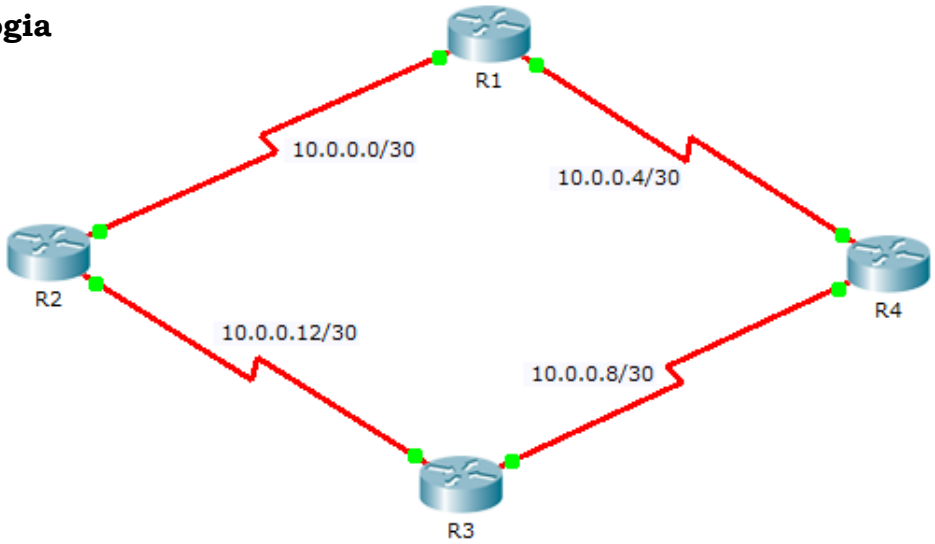


Fig. 38 – Topologia sobre sub-redes

Competências

- Criar sub-redes de modo a permitir a utilização eficiente dos endereços atribuídos;
- Saber optimizar os endereços disponíveis em cada sub-rede;
- Aprender a mapear e segmentar sub-redes;
- Configurar sub-redes nos roteadores a partir da linha de comandos (CLI);

Fundamentos

Para calcular sub-redes e os respectivos *host* o primeiro é saber o que queremos se é sub-redes ou *hosts*. No cálculo de sub-redes um dos requisitos principais é o cálculo da variação. A variação no cálculo de sub-redes em classe C é dada pela fórmula: ***Variação*** = 2^8 - *valor de bits a 1 (um) da máscara no último Byte.* Tando sub-redes quanto *hosts* o cálculo da variação é o mesmo.

As fórmulas principais que vão garantir a quantidade de sub-rede ou *hosts* que se precisam são:

*[**2** nº de bits a **1** >= Nº de sub-redes pretendidas (dois elevado ao nº de bits a **1** tem que ser maior ou igual a quantidade de sub-redes pretendidas)]* para calcular os *hosts* é: [**2** nº de bits a **0** – **2** >= Nº de hosts pretendidos (dois elevado a bits a **0** tem que ser maior ou igual a nº de hosts pretendidos)]

Do endereço de rede da Classe A 10.0.0.0/8 ou seja de com máscara 255.0.0.0 vamos mapear a rede da topologia ilustrada na figura 38.

1º Passo – dividir o endereço dado em 4 sub-redes de 2 hosts.

Sub-rede	IP /Interface	Máscara
10.0.0.0	10.0.0.1 – Se1/0	255.255.255.252
	10.0.0.2 – Se0/0	255.255.255.252
10.0.0.4	10.0.0.5 – Se0/0	255.255.255.252
	10.0.0.6 – Se1/0	255.255.255.252
10.0.0.8	10.0.0.9 – Se1/0	255.255.255.252
	10.0.0.10 – Se0/0	255.255.255.252
10.0.0.12	10.0.0.13 – Se0/0	255.255.255.252
	10.0.0.14 – Se1/0	255.255.255.252

Tabela 1 - Calculo de Sub-redes

2º Passo – montar a devida topologia.

- Adicionar 4 roteadores genéricos vazios (**Generic-PT-Empty**);
- Abra um roteador, aba **Phisycal**;
- Desligar o roteador clicando no botão 
- Adicionar 2 portas seriais (**PT-ROUTER-NM-1S**) para cada roteador, fig.39.
- Renomear os roteadores: aba **Config → Display Name, [**nome do roteador**]**.

Nota: Este nome é visível apenas para o utilizador final.

Faça o mesmo com os restantes, e, interligue-os conforme apresenta a topologia em causa, usando *cabo serial* (Serial cable) ver fig. 6, é representado por uma cor vermelho alaranjada. Finalmente configure:

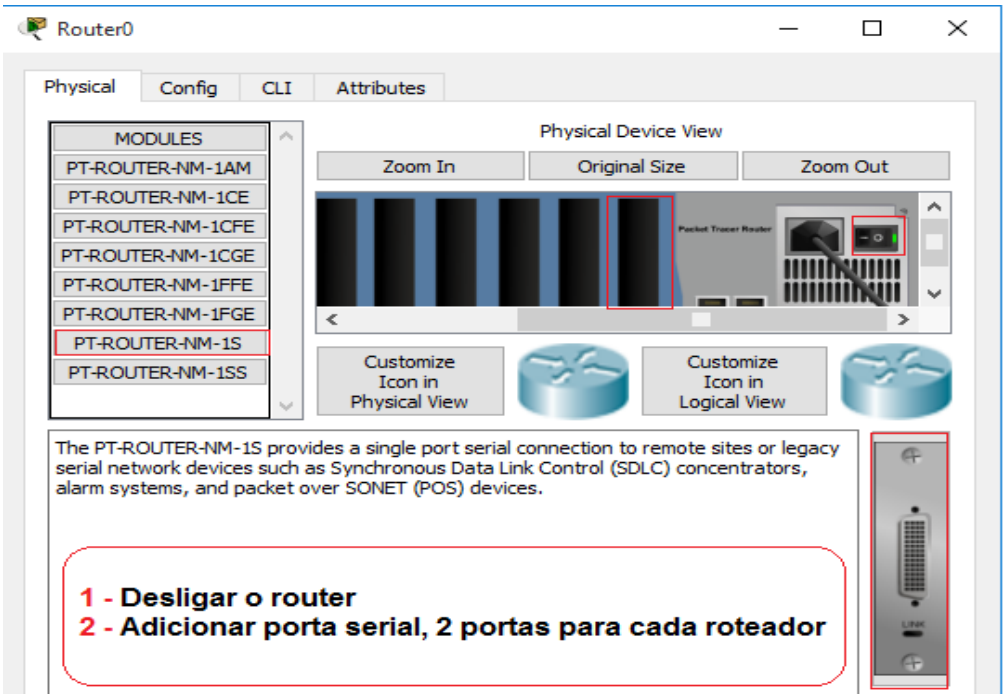


Fig. 39 - Adicionar portas (interface de rede) no roteador

Configuração do R1

Abra o roteador R1, aba CLI e configure:

Continue with configuration dialog? [yes / no]: no //Entrar na consola

Router> enable //Comando para entrar no modo privilegiado

Router# configure terminal //Entra no modo de configuração

Router (config)#hostname R1// Renomeia o equipamento

R1 (config)#interface serial 0/0**//Configuração da Interface seria 0/0**

R1 (config-if)#ip address 10.0.0.5 255.255.255.252

R1 (config-if)#no shutdown //Comando para ligar a interface

R1 (config-if)#do wr//Comando para guardar os dados

R1 (config-if)#exit//Comando para sair de um submodo para outro

R1 (config)#interface serial 1/0**//Configuração da Interface seria 1/0**

R1 (config-if)#ip address 10.0.0.1 255.255.255.252

R1 (config-if)#no shutdown

R1 (config-if)#do wr

R1 (config-if)#exit

Configuração do R2

Continue with configuration dialog? [yes/no]: no

Router>enable

Router#configure terminal

Router (config)#hostname R2

R2 (config)#interface serial 1/0//C**onfiguração da Interface seria 1/0**

R2 (config-if)#no shutdown

R2 (config-if)#ip address 10.0.0.14 255.255.255.252

R2 (config-if)#do wr

R2 (config-if)#exit

R2 (config)#interface serial 0/0**//Configuração da Interface seria 0/0**

R2 (config-if)#ip address 10.0.0.2 255.255.255.252

R2 (config-if)#do wr

R2 (config-if)#no shutdown

Configuração do R3

Continue with configuration dialog? [yes/no]: no

Router>enable

Router#configure terminal

Router(config)#hostname R3

R3 (config)#interface serial 1/0**//Configuração da Interface seria 1/0**

R3 (config-if)#no shutdown

R3 (config-if)#ip address 10.0.0.10 255.255.255.252

R3 (config-if)#do wr

R3 (config-if)# exit

R3 (config)#interface serial 0/0**//Configuração da Interface seria 0/0**

R3 (config-if)#ip address 10.0.0.13 255.255.255.252

R3 (config-if)#no shutdown

R3 (config-if)# do wr

Configuração do R4

Continue with configuration dialog? [yes/no]: no
Router>enable
Router#configure terminal
Router(config)#hostname R4
R4 (config)#interface serial 0/0**//Configuração da Interface seria 0/0**
R4 (config-if)#no shutdown
R4 (config-if)#ip address 10.0.0.6 255.255.255.252
R4 (config-if)# do wr
R4 (config-if)#exit
R4 (config)#interface serial 1/0**//Configuração da Interface seria 1/0**
R4 (config-if)#ip address 10.0.0.9 255.255.255.252
R4 (config-if)# do wr
R4 (config-if)#end//Sair do modo de configuração pra global

Resumo

Neste laboratório viu-se como criar e calcular sub-redes, abordou-se que a criação de sub-redes contribui bastante na utilização eficiente dos endereços de rede. Também definimos o que são sub-redes e apredemos que as mesmas devem possuir um identificador, abordamos também sobre as vantagens das mesmas. Depois montamos a topologia de rede e aprendeu-se a configurar roteador usando comandos básicos do cisco Packet tracer. Portanto é importante que o leitor trate de memorizar certos comandos, porque desde agora em diante precisar-se-ão o bastante.

2.7.4. Auto avaliação

a) Explique porquê criar sub-redes?
b) Define uma sub-rede.
c) Liste outras vantagens do uso de sub-redes.
d) De um modo geral diga o que achou de interessante?
e) Quais bits do endereço IP serão usados para definir sub-redes?
f) Qual é o comando cisco a usar para configurar IPs nas interfaces de rede?

g) A máscara de rede é, também usada para determinar se um *IP address* está localizado dentro de uma rede local ou remota. Comente!

h) Com é chamada a união dos campos *NetID* e *SubnetID*?

i) Além do comando (**do wr**) usado para guardar as configurações, existem outros. Investigue e liste-os.

j) O que significa dizer que cada *host* de uma sub-rede deve possuir uma máscara?

k) Quando é que a máscara é default e quando que é customizada?

l) Configure uma estrutura de rede que compõe 3 roteadores de sua preferência e configure-os usando os conhecimentos apreendidos na faixa de IP 200.28.20.0.

m) **No shutdown** é um comando de configurações usado para_____.

n) Apresenta uma topologia interligada e configurada com 6 roteadores usando o IP 192.168.37.0. efectue e apresente todos os calculas realizados.

2.8. LABORATÓRIO 7

2.8.1. VLSM

Topologia

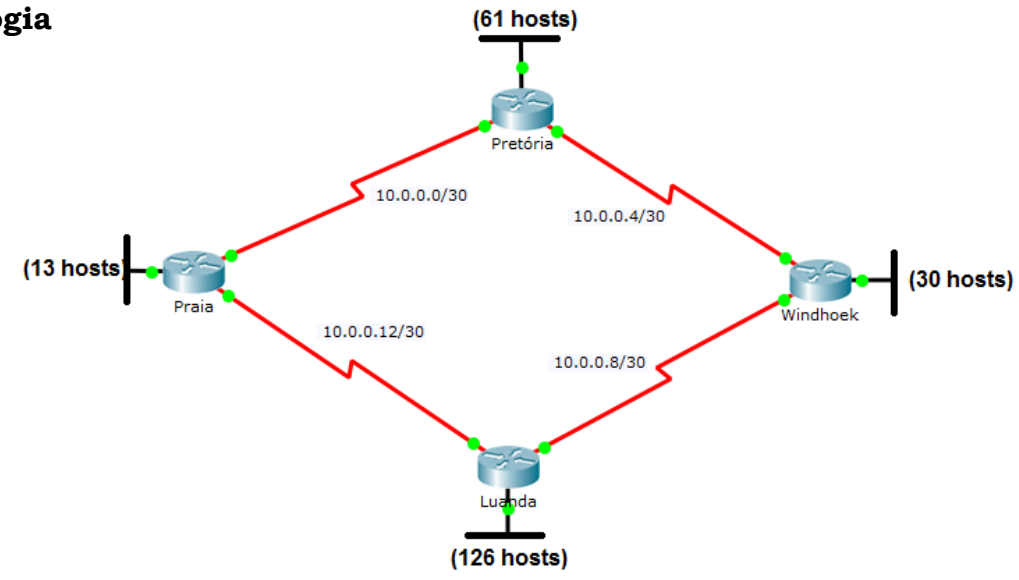


Fig. 40 Topologia sobre VLSM

Competencias

Objectiva-se que, até ao final do laboratório o leitor consiga:

- Projectar sub-redes *VLSM*, de modo a associar uma máscara para cada sub-rede em função do número de endereços necessários.
- Determinar a quantidade de sub-redes necessárias para satisfazer os *hosts* pretendidos.

Fundamentação

VLSM (*Variable Length Subnet Mask*) – Máscara de sub-redes com tamanho variável, é uma técnica que permite que mais de uma máscara seja definida para um determinado IP, (Modelo Classless). A criação do VLSM é bastante vantajosa, pois permite a utilização eficiente do endereço atribuído à uma organização.

Para calcular sub-redes VLSM e os respectivos hosts, primeiro devemos alocar as que tiverem maior requisito dentro da faixa de endereços, isto é os requisitos devem ser listados do maior ao menor, ou seja calcula-se a sub-rede com maior número de hosts, depois a segunda até terminar todas.

O cálculo de VLSM obdece os mesmos princípios de cálculos de subredes. As formulas são as mesmas com excepção de algumas regras listadas no segundo paragrafo sobre fundamentos de VLSM.

Dado o endereço de classe C 200.11.0.0/24, renomeie (nome de exibição e nome do host) os roteadores da prática do laboratório 6 de modo que:

- R1 – Pretória
- R2 – Praia
- R3 – Luanda
- R4 – Windhoek

NOTA

Como já vimos, vale lembrar que para calcular sub-redes VLSM e os respectivos hosts, devemos alocar primeiro as sub-redes que tiverem maior número de dispositivos. Agrupe as sub-redes segundo a quantidade de dispositivos começando pela sub-rede que tiver maior quantidade de dispositivos.

Para este laboratório, **Pretória** exige uma média de 61 hosts. Para satisfazer a exigência precisa-se uma quantidade de 6 bits, já que $2^6 - 2 = 62$ endereços válidos, resultando num desperdício mínimo de 1 host. A cidade de **Praia** exige 13 hosts, use 4 bits, **Luanda** 126 hosts, neste caso use 7 bits e no final **Windhoek** exigem 30 host, precisa-se de 5 bits.

1º Passo – Dividir o endereço dado (200.11.0.0/24) em 4 sub-redes.

Luanda: $2^7 - 2 = 126$

Endereço	**Sub-redes**	**Sub-rede em uso**
200.11.0.0/24	**200.11.0.0/25**	200.11.0.0/25 **(126 hosts) End. de rede**
	200.11.0.128/25	200.11.0.127/25 **End. de (Broadcast)**

Tabela 2 – Cidade de Luanda (Angola)

Pretória: $2^6 - 2 = 62$

Endereço	**Sub-redes**	**Sub-rede em uso**
200.11.0.128/25	**200.11.0.128/26**	200.11.0.128/26 **(62 hosts) End. de rede**
	200.11.0.192/26	200.11.0.191/26 **End. de (Broadcast)**

Tabela 3 – Cidade de Pretória (África do Sul)

Windhoek: $2^5 - 2 = 30$

Endereço	**Sub-redes**	**Sub-rede em uso**
200.11.0.192/26	**200.11.0.192/27**	200.11.0.192/27 **(30 hosts) End. de rede**
	200.11.0.224/27	200.11.0.223/27 **End. de (Broadcast)**

Tabela 4 – Cidade de Windhoek (Namíbia)

Praia: $2^4 - 2 = 14$

Endereço	Sub-redes	Sub-rede em uso
200.11.0.224/27	**200.11.0.224/28**	200.11.0.224/28 **(14 hosts) End. de rede**
	200.11.0.240/28	200.11.0.239 **End. de (Broad-cast)**

Tabela 5 – Cidade de Praia (Cabo-Verde)

2.8.2. Como o Hostname (nome do equipamento)?

Para renomear um equipamento no cisco Packet Tracer, é muito simples. Os comandos usados para nomear, são os mesmos usados para renomear. Ver exemplo a seguir.

Exemplo:

R1> enable

R1 #configure terminal

R1 (config)#hostname **Pretoria**

Pretoria (config)#

...Renomeie os roteadores em falta. Neste caso são o R2, R3 e R4. Terminado, siga as orientações que a seguir.

- Adicionar uma (1) porta *Gigabit Ethernet* (**PT-ROUTER-NM-1CGE**) a cada um dos roteadores (em caso de dúvida reveja a prática anterior);
- Adicionar um *switch 2960-24TT* a cada um dos roteadores;
- Interligar os *switches* aos roteadores (nas portas Gigabit Ethernet);
- Conectar no mínimo 3 computadores a cada *switch* local e um *servidor*;
- Configurar as sub-redes locais, lembrando que o primeiro IP da rede será o **gateway** (porta de saída);
- Adicionar o IP de cada sub-rede local ao roteador correspondente (exemplo: Luanda ***(****config-if)# IP Address* ***[Gateway da sub-rede local, Máscara de sub-rede])*** ou seja estando no roteador de Luanda configure: **Luanda (Config-if)# IP Address 200.11.0.1 255.255.255.128.**
- Termine as configurações dos restantes roteadores lembrando que cada sub-rede local comporta um Gateway que deve ser introduzido na interface que liga **roteador** – **switch** e vice-versa.

– Terminado teste a comunicação entre os equipamentos locais.

Nota: Esta configuração não garante que haja comunicação com todos equipamentos da topologia. Somente para equipamentos locais.

Resumo

Resumindo, VLSM é uma técnica Classless que permite atribuir mais de uma máscara para o mesmo endereço de rede. Neste laboratório viu-se como renomear os equipamentos, como adicionar portas *Gigabit Ethernet* aos rotadores de modo a permita-nos agregar mais equipamentos. Também adicionou-se os *switches* e fez-se a interligação com os roteadores locais, configurou-se e finamente testou-se. Com base aos conhecimentos adquiridos resolva os exercícios que se seguiem.

2.8.3. Auto avaliação

O endereço alocado 200.11.0.0/24 dividiu-se em 4 sub-redes:

a) Quantos *hosts* suportam cada sub-rede?
b) Qual é a primeira regra a ser feita ao calcular sub-redes VLSM?
c) Quantos bits foram emprestados na rede em cada sub-rede VLSM?
d) Qual é o último endereço válido para Luanda?
e) Quantos endereços válidos têm a sub-rede 200.11.0.240/28?
f) Qual é o endereço de broadcast da mesma?
g) A inequação $2^{\text{bits em 0}} - 2 = 2^{\text{número positivo qualquer}}$ representa que cálculo?
h) Qual a velocidade de transmissão máxima de um cabo *Gigabit Ethernet*?
i) Dando a mesma rede, desenvolva um esquema de rede usando VLSM de modo que Luanda tenha 30 hosts, Pretória = 12, Praia = 40 e Windhoek = 27.
j) **Problema:** A empresa Fenix Innovation tem cinco (5) departamentos. Havendo necessidade de criar uma rede com sub-redes VLSM para separação de fluxo de dados convidou-te como administrador de rede. Prontamente você aceitou. Do endereço de rede

192.198.11.0/24 para LANs e 1.0.0.0/8 para Links WAN calcule: ***DF*** (Departamento de Finanças 4 hosts), ***DRH*** (Departamento de Recursos Humanos 12 hosts), ***DDSD*** (Departamento de desenvolvimento de softwares e design 48 hosts), ***DV*** (Departamento de Vendas 14 hosts) e ***DRE*** (Departamento das Relações Exteriores 29 hosts).

- Qual é a quantidade de hosts encontradas nos links WANs?
- Qual é a nova máscara para o endereço 1.0.0.0/8 que encontrou?
- Quantas sub-redes foram encontradas para o endereço 1.0.0.0/8
- Quais os endereços de redes e broadcast das sub-redes achadas?
- Quantas sub-redes VLSM achou para o endereço 192.198.11.0?
- Qual é a quantidade de hosts de cada sub-rede?
- Quais os endereços de rede achados?
- Quais as máscaras para cada sub-redes?
- Quais os endereços de broadcast de cada sub-rede?
- Mapeie e mostre a topologia da empresa.

2.9. LABORATÓRIO 8

2.9.1.Configuração do NAT (Network Address Translation)

Topologia

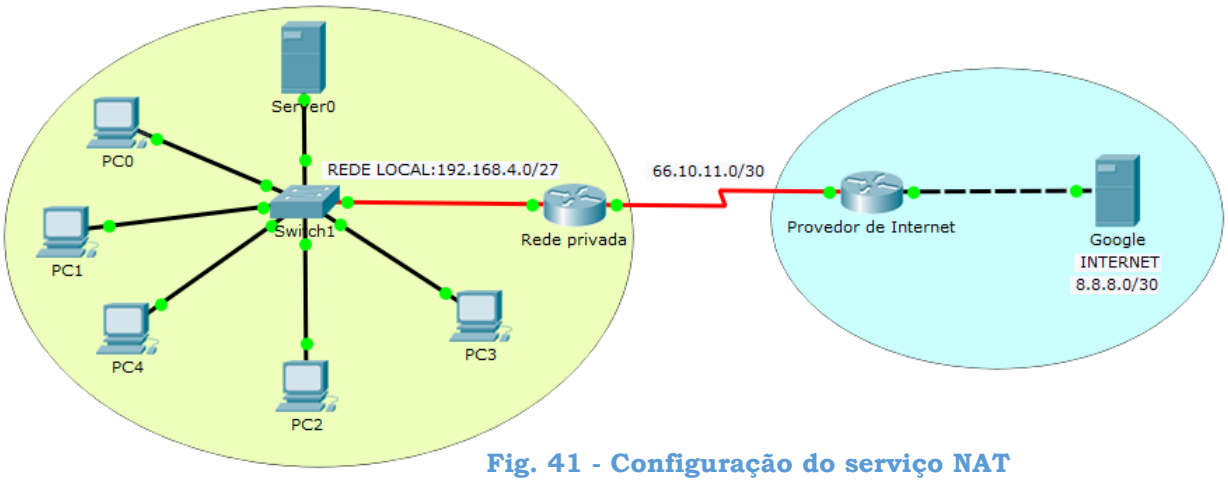


Fig. 41 - Configuração do serviço NAT

Competências

Até ao final do laboratório o leitor será capaz de:

- Configurar o serviço NAT para realizar a tradução dos endereços IPv4 privados de origem de uma rede interna para endereços públicos roteáveis na Internet;
- Redireccionar endereços e portas para que um dado serviço em execução na rede interna privada possa ser acessível através da Internet pública.

Fundamentos

O serviço NAT foi criado com apenas um objectivo primordial; economizar endereços IPv4, uma vez que toda uma rede com **endereços privados da RFC 1918** (**Request for Comment**) pode ter acesso à Internet através de apenas um (ou poucos) endereço (s) público (s).

Dados os endereços 192.168.4.0/27, 66.10.11.0/30 e 10.0.0.0/8, mostrar-se-á como configurar o NAT de modo a fazer o redireccionamento de endereços e de portas, dando privilégio a execução de serviços contidos na Web em execução na rede privada 192.168.4.0/27 sejam acessados pelos usuários em qualquer parte do mundo.

Usando o simulador de rede cisco Packet Tracer, monte a topologia acima referida adicionando:

- Cinco (5) computadores (PC0 a PC4);
- Dois (2) servidores, 1 (um) para rede local (intranet) e 1 (um) para rede pública (internet);
- Adicionar um (1) *switch* genérico vazio (**Switch-PT-Empty**), adicionar 6 portas *FastEthernet* (**PT-SWITCH-NM-1CF**) e uma Gigabit Ethernet de *fibra óptica* (**PT-SWITCH-NM-1FGE**) no mesmo;
- Adicionar um roteador genérico vazio (**Router-PT-Empty**) para rede privada (local), adicionando ao mesmo uma porta Gigabit Ethernet de *fibra óptica* (**PT-SWITCH-NM-1FGE**) e uma serial (**PT-ROUTER-NM-1S**);

- Adicionar um roteador genérico vazio (**Router-PT-Empty**) de provedor de internet e sobre o mesmo adicionar também uma porta serial (**PT-ROUTER-NM-1S**) e uma *Gigabit Ethernet* (**PT-SWITCH-NM-1CGE**);
- Remover a porta *Fast Ethenet* do servidor do Google (internet) e adicionar uma porta *Gigabit Ethernet* e montar de acordo a figura 41.

Configuração do servidor da rede privada

Configure o serviço DHCP ao servidor de modo que as máquinas recebam IPs automaticamente:

Servidor: 192.168.4.2

Gateway: 192.168.4.1

Teste a conexão local.

Configuração do default gateway no Switch

O Default Gateway não nada mais que o Gateway da rede local. É o mesmo que nos permitirá que haja comunicação entre a rede local e a pública. Siga os seguintes comandos:

Switch>enable
Switch#configure terminal
Switch(config)#ip default-gateway 192.168.4.1 **//Adicionando o Gateway**

Configuração da interface gigabitEthernet9/0 que interliga o roteador ao Switch local

Router>enable
Router# configure terminal
Router# hostname NAT
NAT (config)#interface gigabitEthernet 9/0
NAT (config-if)#ip address 192.168.4.1 255.255.255.224
NAT (config-if)#no shutdown
NAT (config-if)#do wr
NAT (confi-if)#exit

Configuração da interface serial0/0 que interliga o rotador local ao provedor de internet

NAT (config)# interface serial 0/0
NAT (config-if)# ip address 66.10.11.1 255.255.255.252
NAT (config-if)# no shutdown
NAT (config-if)# do wr
NAT (confi-if)# exit

Configuração da interface serial0/0 que interliga o provedor de internet ao rotador local

Router> enable
Router #configure terminal
Router (config)# hostname Internet
Internet (config)# interface serial 0/0
Internet (config-if)# ip address 66.10.11.2 255.255.255.252
Internet (config-if)# no shutdown
Internet (config-if)# do wr
Internet (confi-if)# exit

Configuração da interface Gigabit Ethernet que interliga o provedor de internet ao Servidor do Google

Internet (config)# interface gigabitEthernet 1/0
Internet (config-if)# ip address 8.8.8.1 255.255.255.252
Internet (config-if)# no shutdown
Internet (config-if)# do wr
Internet (config-if)# exit

Configurar o servidor da rede pública (internet)

Nesta etapa vamos configurar o servidor da rede pública que vai comunicar-se com as demais redes privadas. Configure o servidor da rede pública com os seguintes endereços:
Servidor: 8.8.8.2

Gateway: 8.8.8.1

Habilitar o NAT no roteador que interliga a rede privada à rede pública

NAT (config)# interface gigabitEthernet 9/0
NAT (config-if)# ip nat inside**//Porta de entrada**
NAT(config-if)# exit
NAT (config)# interface serial 0/0
NAT (config-if)# ip nat outside **//Porta de saída**
NAT(config-if)#exit

2.9.2. Lista de acesso ao roteador Local

NAT (config)# access-list 1 permit 192.168.4.0 224.255.255.255
NAT (config)# ip nat inside source static tcp 192.168.4.1 ?
<1-65535> Local UDP/TCP port **//Porta local**
NAT (config)# ip nat inside source static tcp 192.168.4.1 80 ?
A.B.C.D Inside global IP address
NAT (config)# ip nat inside source static tcp 192.168.4.1 80 66.10.11.1 ?
<1-65535> Global UDP/TCP port **//Porta de rede pública**
NAT (config)# ip nat inside source static tcp 192.168.4.1 80 66.10.11.1 8080 ?
<cr>

NAT(config)#ip nat inside source static tcp 192.168.4.1 80 66.10.11.1 8080

A linha realçada com azul faz o redireccionamento de endereços. Repare que para fazer isto, informamos o mapeamento entre o endereço **inside** e o outro **outside** e também informou-se ao roteador que todos os pacotes destinados ao seu endereço público na porta 8080 (66.10.11.2:8080) devem ser encaminhados para o endereço privado do servidor na porta padrão (192.168.4.1:80).

Configuração de rotas estáticas

NAT (config)# ip route 8.8.8.0 255.255.255.252 66.10.11.2
Internet (config)# ip route 192.168.4.0 255.255.255.224 66.10.11.1

Para configurar rotas estáticas no laboratório cisco Packet Tracer é muito simples basta escrever o comando: **IP ROUTE** *[IP da rede que se pretende alcançar* | *Máscara* | *Próximo salto]* (conteúdo a abordar noutras práticas de laboratório).

Em resumo é praticamente isto. Muito simples e prático no dia-a-dia.

2.9.3. Auto avaliação

a) Faça um breve resumo de tudo que aprendeu.
b) Para que serve o NAT?
c) Explique detalhadamente o mapeamento inside e outside.
d) Explique como é feita o redireccionamento dos pacotes públicos na porta 8080 para os privados na porta 80.
e) Para que serve o protocolo TCP?
f) Para serve a porta 8080?

2.10. ENCAMINHAMENTO DE PACOTES

Encaminhamento (português de Portugal) ou Roteamento (português do Brasil), (***Routing do Inlgês***) é o processo utilizado pelo roteador para encaminhar um pacote para uma determinada rede de destino.

2.10.1. LABORATÓRIO 9

2.10.1.1. Encaminhamento estático

Método que consiste em adicionar manualmente rotas na tabela de encaminhamento do router (roteador). O encaminhamento estático é normalmente adequado para redes de pequena dimensão, onde o cenário de rede não é complexo e raramente sofre alterações.

Topologia

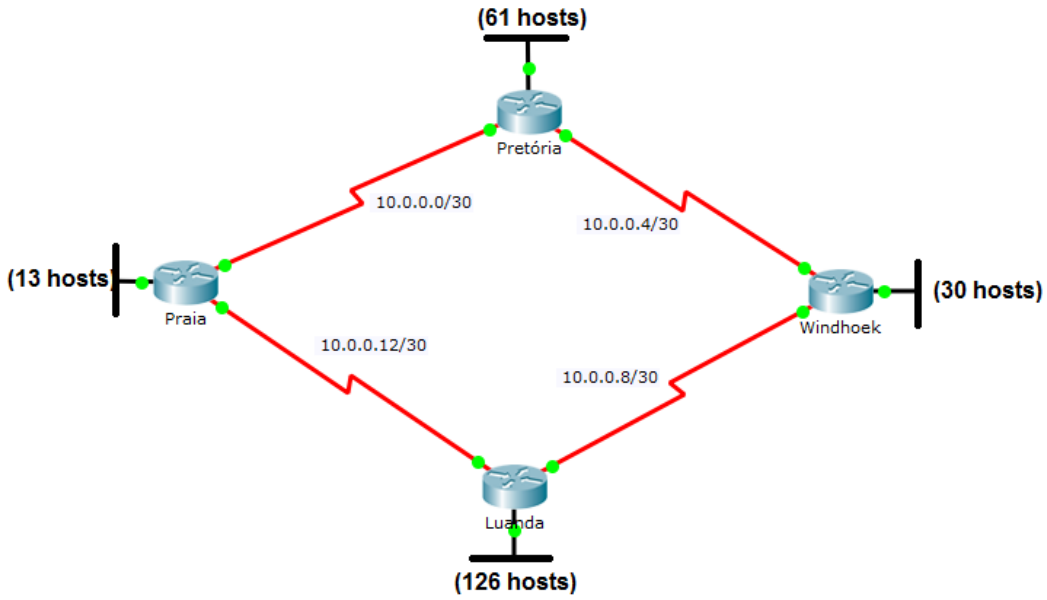


Fig. 42 - Encaminhamento estático

Competências

- Saber construir tabelas de encaminhamento estático;
- Estabelecer a confiança entre routers (distancia administrativa)

Fundamentos

Para esta prática buscaremos a topologia usada no laboratório 8. Se ainda não se lembra ou por algum motivo a perdeu, trate de repeti-lo e seguir com a prática em questão.

A sintaxe para adicionar uma rota estáticas obedece os seguintes critérios:

#IP Route [IP da rede remota] [Máscara] [Endereço do próximo router ou interface de saída] [Distancia administrativa]. E outros elementos opcionais.

— **Rede remota**: endereço de rede que se pretende alcançar;
— **Máscara:** máscara de rede associada ao endereço IP da rede remota;

— **Endereço do próximo router:** endereço IP da interface do próximo roteador, directamente ligado ao roteador de origem;
— **Interface de saída:** pode ser usada em substituição ao endereço do próximo roteador;
— **Distancia Administrativa** é um valor que os roteadores usam para seleccionar o melhor caminho quando há duas ou mais rotas para o mesmo destino.

Usando a topologia da prática de laboratório 8, aprenderemos como adicionar rotas estáticas na tabela de roteamento a fim de estabelecer comunicação a todas as sub-redes da topologia.

Sabendo que o IP da sub-rede local que liga e **Luanda é 200.11.0.0/25**, **Pretória é 200.11.0.128/26**, **Windhoek é 200.11.0.192/27** e **Praia é 200.11.0.224/28** seguiremos a diante com as configurações seguintes:

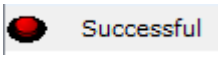
Entrando nas configurações do roteador de **Luanda** → aba (separador) **CLI** e configure a rota estática para endereçar pacotes a sub-rede local de **Windhoek**. Supondo que o caro leitor esteja em modo de configuração, digite os comandos a baixo:

```
Luanda (config) # ip route 200.11.0.192 255.255.255.192 10.0.0.9
Luanda (config) # do wr
```

Note que 200.11.0.192 é o IP da rede local de Windhoek associado a ele, a sua máscara e o IP 10.0.0.9 é o IP associado a interface do próximo router.

Nota: Está configuração não garante-nos que haja comunicação entre as duas sub-redes locais, para tal, é preciso irmos no roteador de **Windhoek** e fazer a mesma configuração os comandos são os mesmo (IP ROUTE) altera apenas os IPs. Clique sobre o router de **Windhoek** → Aba **CLI** → Entre no modo de configuração do router e digite os comandos a seguir:

```
Windhoek (config)# ip route 200.11.0.0 255.255.255.128 10.0.0.10
Windhoek (config)# do wr
```

Nesta fase vamos tentar trocar informações entre as duas sub-redes. Coloque em modo de simulação (**Simulation**) e veja qual será o comportamento da rede. É claro se a configuração for bem-feita o caro praticante receberá uma mensagem de sucesso. 

Distancia administrativa, tal como vimos que é um valor usado pelos router para quantificar a confiança entre os mesmo e garantir qual a melhor rota para o router encaminhar pacotes. Lembre-se que quanto menor o número maior será a confiança ou seja são inversamente proporcional. Para adicionar o valor a distância administrativa, é muito simples os comandos são os mesmos a usar com excepção do parâmetro a passar. Os valores numéricos a serem fornecidos na distância administrativa variam entre 0 a 255.

Veja o exemplo, no caso de haver duas ou mais rotas para **Windhoek** o caso mais prático seria:

```
Luanda (config) # ip route 200.11.0.192 255.255.255.192 10.0.0.9 1
Luanda (config) # do wr
```

Com certeza adicionamos 1 porque será a via principal. Para as demais rotas o parâmetro fornecido deve ser de 2 em diante. Lembre-se que se tivéssemos uma rota cujo valor fosse 255, podemos crer que a nenhum momento o router iria escolher esta rota.

2.10.1.2. Rota por defeito

É uma rota estática usada para encaminhar pacotes a redes desconhecidas com um único ponto de saída. Para configurar **rotas por defeito**, primeiro temos que definir um roteador principal que conheça todas as redes remotas da topologia. Exemplo prático, se tivéssemos que definir como roteador principal o roteador de **luanda**, neste teríamos que infor-

mar as 5 redes remotas via encaminhamento estático e nos demais roteadores configuraríamos o rotas por defeito para evitar loop na rede.

Sintaxe principal:

#IP ROUTE [0.0.0.0 | 0.0.0.0] [IP do próximo router] ou seja, supondo que estamos enviando pacotes de **Luanda** para **Windhoek** e vice-versa seria o seguinte:

```
Luanda (config) # ip route 0.0.0.0 0.0.0.0 10.0.0.9
Luanda (config) # do wr
```

Em suma é isso, bem simples na prática e muito útil na vida real. Desta feita, vimos como adicionar tabelas de encaminhamento estático e manipular a confiança entre roteadores. No entanto deixar-mos-emos que o caro praticante termine a prática sozinho buscando conhecimentos apreendidos nos exemplos ilustrados e deixar a topologia toda operacional. Teste a comunicação, em que estando num ponto qualquer da topologia consiga-se comunicar com qualquer uma das redes locais.

2.10.1.3. Auto avaliação

a) Detalhe encaminhamento de pacotes IP.
b) O que é o encaminhamento estático?
c) Em que nível do modelo OSI ocorre o encaminhamento de pacotes IP?
d) Quais equipamentos de rede realizam o encaminhamento de pacotes IP?
e) Quando o roteador recebe um pacote, na prática ele executa duas funções principais: quais?
f) Em que consiste o encaminhamento por estático e por defeito?
g) Para que serve a distância administrativa?´
h) Quais comandos a usar para a configuração de uma rota estática?
i) Monte uma topologia usando 3 roteadores e adicione rotas estáticas por defeito para garantir a operacionalização das mesmas. Use os seguintes endereções IPs 20.20.20.0/30 para links WAN e

195.168.30.0/24 subdividido em três sub-redes locais. Uma deve ter 40 hosts, a outra 20, e a última 59.

2.10.2. Encaminhamento dinâmico

O encaminhamento dinâmico é um mecanismo que consiste em preencher as tabelas de encaminhamento dos Routers usando um protocolo[3] de encaminhamento. Neste último o administrador da rede não intervém directamente no preenchimento das tabelas de encaminhamento do roteador. O encaminhamento dinâmico é ao contrário do encaminhamento estático. É adequando para redes grandes, complexas e que sofrem alterações constantes. A utilização de protocolos de encaminhamento, muitas das vezes resulta em sobrecargas no router e também obriga que o administrador tenha conhecimentos básicos sobre protocolos de encaminhamento a configurar.

Os protocolos de encaminhamento mais conhecidos são: **RIP** (Routing Information Protocol) na versão 1 e 2, **IGRP** (Interior Gateway Routing Protocol), **EIGRP** (Enhenced Interior Gateway Routing Protocol), **OSPF** (Open Shortest Path First), **IS-IS** (Intermediate System-to-Intermediate System), **BGP** (Border Gateway Protocol) e outros. Os protocolos de encaminhamento estão divididos internos (**IGP** – Interior Gateway Protocol) e externos (**EGP** – External Gateway Protocol).

2.10.2.1. Características dos protocolos de encaminhamento

Os protocolos **RIP** versão 1 e 2 e **IGRP** são baseados na distância (hop count). O **EIGRP** é um protocolo híbrido e o **OSPF** é um protocolo baseado na topologia (Link State).

[3] Um protocolo de rede de computadores é nada mais e nada menos que um conjunto de padrões e conversões estabelecidas para permitir a troca de informações entre duas ou mais entidades.

Não estudaremos todos protocolos mencionados, neste guia nos limitaremos apenas nos protocolos **RIPv2**, **EIGRP** e **OSPF**. Cabe ao caro leitor ir em busca do conhecimento e estudar outros restantes.

Nota: Para configurar um protocolo de encaminhamento em um router não é necessário que o administrador da rede saiba todas as redes que compõem a topologia. Basta configurar as redes directamente ligadas ao router em causa.

2.10.2.2. LABORATÓRIO 10

2.10.2.2.1. Protocolo RIPv2

Topologia

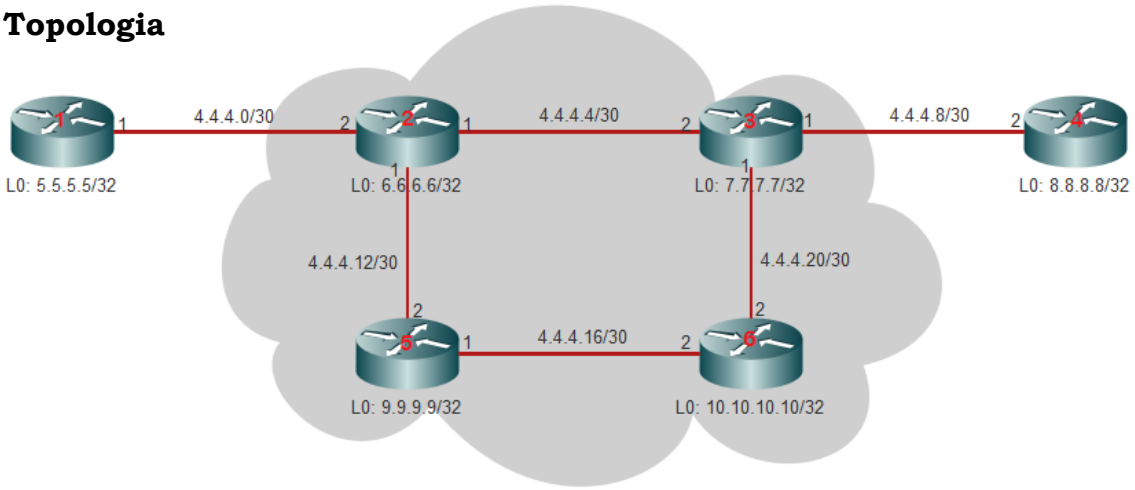


Fig. 43 - Usando protocolo RIPv2

Competências

De forma geral, queremos que até ao final da prática o estudante adquira conhecimentos sólidos para resolver problemas práticos:

- Configurar de interfaces loopback;
- Configurar protocolo de encaminhamento RIPv2;
- Endereçar pacotes através do protocolo RIPv2;
- Entender a importância dos protocolos de encaminhamento;

Fundamentos

O RIP é um protocolo de roteamento classificado como vector de distância possui actualmente duas versões, é Classfull com o limite de 15 saltos. O RIP envia pacotes de actualização de rotas em 30 em 30 segundos. Se uma rota ficar inactiva até 90 segundos considera esta rota como não válida e elimina-a da sua tabela de encaminhamento.

Sintaxe de configuração do protocolo RIPv2

#Router RIP ↵ *//Comando para configurar o protocol RIP*
#Version 2 ↵ *// Comando para configurar a versão 2*
#No auto-summary ↵ *//Comado para suporte de VLSM*
#Network [IP da rede directamente ligada ao router] ↵

Prática

Com auxílio do Software de simulação de rede **Cisco Packet Tracer**, mapeie a topologia a cima usando cabos de **Fibra Óptica** (Gigabit Ethernet). Use routers genéricos (Generic Empty) para o mapeamento da referida topologia.

- Faça o endereçamento IP nas devidas Interfaces de rede;
- Adicione os IP's ímpares nas interfaces identificadas com o nº 1 na topologia acima;
- Vamos endereçar primeiro os IPs às interfaces dos routers e mais tarde configuraremos o protocolo RIPv2. Confere as configurações:

R1

--- System Configuration Dialog ---
Continue with configuration dialog? [yes / no]: no
Router> enable
Router #configure terminal
Router (config)#hostname R1
R1(config) #interface loopback 0
R1(config-if)#ip address 5.5.5.5 255.255.255.255

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)# interface gigabitEthernet 0/0

R1(config-if) #ip address 4.4.4.1 255.255.255.252

R1(config-if)#no shutdown

R1(config-if)#do wr

R2

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Router>enable

Router #configure terminal

Router (config) #hostname R2

R2(config)#interface loopback 0 *//Interface loopback*

R2(config-if)#ip address 6.6.6.6 255.255.255.255

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#interface gigabitEthernet 0/0 *//interface Gigabit Ethernet 0/0*

R2(config-if)#ip address 4.4.4.2 255.255.255.252

R2(config-if)#no shutdown

R2(config)#exit

R2(config)#interface gigabitEthernet 2/0 *//Interface Gigabit Ethernet 2/0*

R2(config-if)#ip address 4.4.4.13 255.255.255.252

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#interface gigabitEthernet 1/0 *//Interface Gigabit Ethernet* 1/0

R2(config-if)#ip address 4.4.4.5 255.255.255.252

R2(config-if)#no shutdown

R2(config)#exit

R2 #copy startup-config running-config *//Comando para guardar*

(...) Termine o endereçamento de IPs nos restantes roteadores. Note que a configuração é mesmíssima em todos os aspectos, o que muda é simplesmente os números das interfaces e os referidos IPs.

(...). Voltando agora faremos o encaminhamento dinâmico usando o protocolo RIPv2.

Configurando o protocolo RIPv2 nos roteadores.

Como já nos referimos, para configurar um protocolo de encaminhamento no router, não tem segredos. O importante é anunciar todas redes directamente a ele ligadas.

Exemplo: para configurar o protocolo **RIPv2** no router (**R1**) veja que basta adicionar a rede **5.5.5.5/32** (Interface loopback 0) e a rede **4.4.4.0/30** que interliga os routers (**R1** e **R2**).

Como ficaria o no router (**R2**)?

Será que anunciaríamos as redes (6.6.6.6/32, 4.4.4.4/30, 4.4.4.12/30) e a 4.4.4.0/30 como já está anunciada no router **R1** não precisa? Errado! As redes directamente ligadas para o router (**R2**) envolvem: 6.6.6.6/32, 4.4.4.0/30, 4.4.4.4/30, 4.4.4.12/30. Agora veja a seguir.

R1

Estando no modo de configuração digite os comandos a seguir

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 5.5.5.5
R1(config-router)#network 4.4.4.0
R1(config-router)#do wr
```

R2

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 4.4.4.0
R2(config-router)#network 6.6.6.6
R2(config-router)#network 4.4.4.4
R2(config-router)#network 4.4.4.12
R2(config-router)#do wr
```

R3

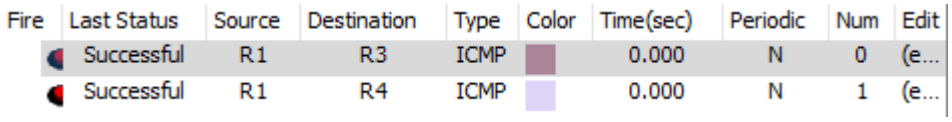
```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#no auto-summary
R3(config-router)#network 4.4.4.4
R3(config-router)#network 7.7.7.7
R3(config-router)#network 4.4.4.20
R3(config-router)#do wr
```

R4

```
R4(config)#router rip
R4(config-router)#version 2
R4(config-router)#no auto-summary
R4(config-router)#network 8.8.8.8
R4(config-router)#network 4.4.4.8
R4(config-router)#do wr
```

(...) Termine as configurações de encaminhamento nos outros dois routers.

Viu... bem simples. Agora testando o envio de pacotes entre os routers (**R3** e **R4**) veja que o envio foi realizado com sucesso. Ver a figura a seguir.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	R1	R3	ICMP		0.000	N	0	(e...
	Successful	R1	R4	ICMP		0.000	N	1	(e...

Fig. 44 - Teste de envio

Para ver as configurações feitas basta que digite o comando:

#show ip route *//mostra a tabela de roteamento (Router)*
#show running-config *//mostra as configurações feitas no equipamento*

Finalizando é isto aí. Bem simples na prática e muito útil na vida real. Lembre-se pratique sempre que poderes e tire pelo menos 30 minutos por dia para exercitar redes, só assim tornar-se-á um verdadeiro herói. Grandes mestres treinam todos os dias, é esta particularidade que os faz ser mestre.

2.10.2.2.2. Auto avaliação

a) Com base a prática que acabou de realizar a que conclusão chegou?
b) Qual foi a grande diferença que notou em relação ao roteamento (encaminhamento) estático?
c) Quais comandos novos aprendeu com essa prática?
d) Um cliente da empresa *Vina nova* solicitou-te para segmentar a rede 200.10.20.0 em 4 sub-redes duas com 28 hosts uma com 60 e última com 12. E também provavelmente deu um link WAN da faixa 1.1.1.0/30. Calcule as sub-redes faça o endereçamento IP das referidas interfaces e finalize configurando o protocolo RIPv2.

2.10.2.3. LABORATÓRIO 11

2.10.2.3.1. Protocolo EIGRP

Topologia

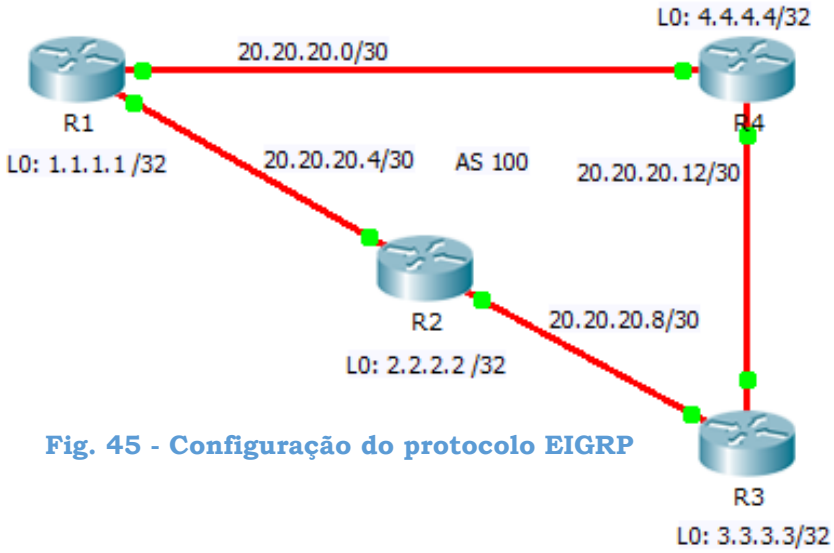


Fig. 45 - Configuração do protocolo EIGRP

Competências

Pretende-se até ao final da prática em causa o leitor possua um conhecimento sólido nas vertentes seguintes:

- Configurar rotas dinâmicas usado o protocolo EIGRP;
- Saber o que são ASs (Sistemas Autónomos ou Autonomous Systems);
- Diferenciar protocolos RIP e EIGRP;
- Discernir as vantagens e desvantagens do protocolo RIP em detrimento do EIGRP;

Fundamentos

Batalhas na vida nunca terminam. Portanto o objectivo primordial desta prática é configurar o protocolo EIGRP.

O EIGRP é um protocolo de roteamento híbrido ou vector de distancia avançando, pois ele traz as características dos protocolos vectores distancia e link state lançando em 1992 pela Cisco System. Na verdade é uma versão do IGRP aprimorada. Acredita-se que a mesma tecnologia vec-

tor distância existente no IGRP também é usada no EIGRP. O EIGRP era proprietário da Cisco, sendo a sua aplicação restringia-se apenas em equipamentos Cisco. No entanto a "**Cisco Live London 2013**" anunciou que o EIGRP seria liberado para o IETF como "**RFC International**". Suporta VLSM (Classless), distância administrativa de 90, suporta até 255 saltos, sumarização automática, suporta autenticação, tem um excelente tempo de convergência e suporta IPv6.

Como Funciona?

O EIGRP tem quatro componentes básicos:

- Descoberta/recuperação de vizinhos;
- Protocolo de transporte confiável;
- Máquina de estado finito DUAL;
- Módulos dependente de protocolo

A descoberta/recuperação de vizinhos é o processo utilizado pelos roteadores para conhecer dinamicamente outros roteadores nas redes às quais estão directamente conectados.

Requisitos e comandos de configuração do EIGRP

Para configuração do EIGRP começa-se com a definição de um AS (Autonomous System – Sistema Autónomo). Este número varia de 1 a 65535 e deve ser o mesmo em todos os roteadores do mesmo domínio de roteamento EIGRP.

Antes de configurar o EIGRP, precisa-se definir interfaces loopbacks que sirvam como "router-id" do EIGRP, veja os comandos abaixo:

```
#Interface loopback 0 ip address 1.1.1.1 255.255.255.255
```

Sintaxe de configuração:

```
#router eigrp [ numero do AS]
#no auto-summary
#network [Rede directamente ligada] [Máscara-curinga ou invertida]
```

Esses são os comandos principais dentro daquilo que é a configuração do EIGRP, portanto existem outros mais avançados. Em caso de dúvida use o ponto de interrogação a medida que configura (? = Help).

Supondo que a topologia já esteja bem endereçada e configurada todas as interfaces loopback, veja a configuração do protocolo EIGRP nos roteadores baixo:

Prática

R1*//Configurando Router 1*

R1(config)#router eigrp 100 *//número do AS*
R1(config-router)#no auto-summary
R1(config-router)#network 1.1.1.1 0.0.0.0 *//IP da rede mais a máscara invertida.*
R1(config-router)#network 20.20.20.0 0.0.0.3
R1(config-router)#network 20.20.20.4 0.0.0.3
R1(config-router)# do wr
R1(config-router)# exit

R2 *//Configurando Router 2*

R2(config)#router eigrp 100
R2(config-router)#no auto-summary
R2(config-router)#network 2.2.2.2 0.0.0.0
R2(config-router)#network 20.20.20.4 0.0.0.3
R2(config-router)#network 20.20.20.8 0.0.0.3
R2(config-router)#do wr
R2(config-router)#exit

R3*//Configurando Router 3*

R3(config)#router eigrp 100
R3(config-router)#no auto-summary
R3(config-router)#network 3.3.3.3 0.0.0.0

R3(config-router)#network 20.20.20.8 0.0.0.3
R3(config-router)#network 20.20.20.12 0.0.0.3
R3(config-router)#do wr
R3(config-router)#exit

R4//*Configurando Router 4*

R4(config)#router eigrp 100
R4(config-router)#no auto-summary
R4(config-router)#network 4.4.4.4 0.0.0.0
R4(config-router)#network 20.20.20.0 0.0.0.3
R4(config-router)#network 20.20.20.12 0.0.0.3
R4(config-router)#do wr
R4(config-router)#exit

Portando foi tão simples, e muito prático no quotidiano. Nesta prática aprendemos o que é o protocolo EIGRP, como funciona e como configurar.

2.10.2.3.2. Auto avaliação

Resolva os exercícios a baixo:

a) O que é o protocolo EIGRP?
b) Como funciona o protocolo EIGRP e quais comandos são usados para a configuração do mesmo?
c) Confirme a veracidade das afirmações:

- ✓ O protocolo EIGRP tem uma distância administrativa de 90;
- ✓ O protocolo EIGRP não suporta VLSM;
- ✓ O EIGRP suporta até 500 saltos;
- ✓ O protocolo EIGRP não é um protocolo de transporte fiável;
- ✓ O EIGRP é proprietário da Cisco;
- ✓ A sigla “AS” vem do inglês e significa Sistema Autónomo;
- ✓ Uma rota com 5 saltos no protocolo EIGRP, com certeza será a melhor rota da topologia;

✓ O comando usado para verificar o trajecto de um pacote é o Traceroute;

✓ O Running-config é um comando usado para ver rotas remotas;

d) Diferencie o protocolo EIGRP do RIP.

2.10.2.4. LABORATÓRIO 12

2.10.2.4.1. Protocolo OSPF

Topologia

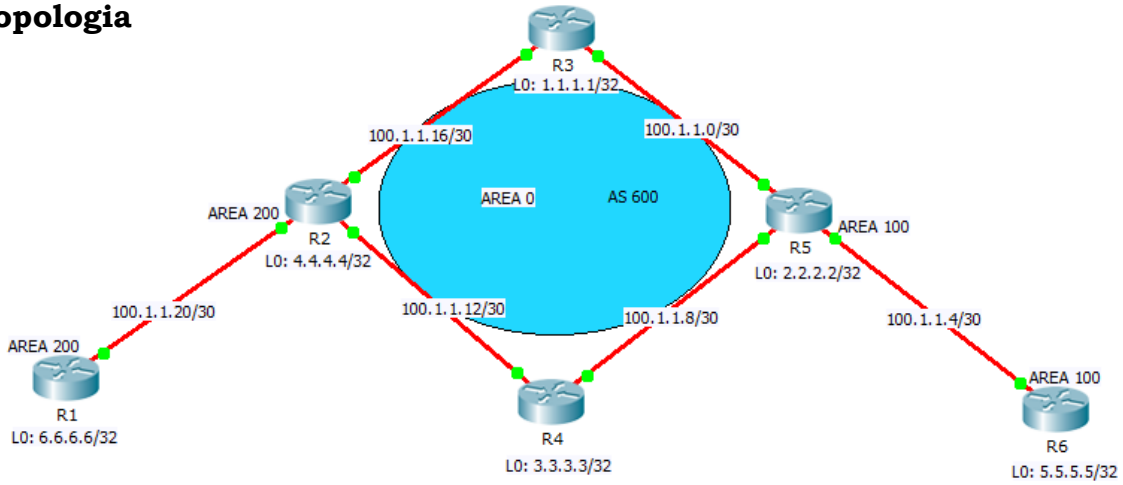


Fig. 46 - Protocolo OSPF

Competências

- Saber configurar o protocolo OSPF nos roteadores;
- Saber discernir a diferença existente entre o protocolo EIGRP e OSPF;
- Diferenciar o OSPF do EIGRP

Fundamentos

Bem-vindo de volta! Nas duas últimas práticas se bem me lembro falamos sobre encaminhamento dinâmico, falamos dos protocolos RIPv2 e EIGRP. Vimos quais as características que diferem um do outro. Como o prometido é devido e prometemos estudar somente os três protocolos principais de encaminhamento hoje vamos falar do último protocolo, isto é o OSPF.

O OSPF (Open Shortest Path First) é um protocolo de roteamento baseado na topologia (link-state) desenvolvido pela IETF (Internet Engeneering Task Force) como substituto para o RIP, caracteriza-se por ser um protocolo intra-domínio ou interno (Interior Gateway Protocol) ou seja é um protocolo aberto.

Operações de fluxo

— Releções de vizinhaças e adjacencias com outros roteadores;
— Determinação de rotas;
— Troca de informação de encaminhamento.

Características

— Criação de redes hierárquicas;
— Divisão de uma rede em áreas;
— Suporte a VLSM;
— Suporte a múltiplas métricas;
— Balanceamento de carga;
— Sem limites de saltos;

Sintaxe de configuração:

Para configurar o protocolo de encaminhamento OSPF, usa-se os seguintes comandos:

#router OSPF [número do processo] *//Activa o protocolo OSPF. O número do Processo varia entre 1 a 65535*
#network [endereço de rede][máscara de rede invertida] Area [número da área].
Exemplo:

#router ospf 100
#network 1.1.1.0 0.0.0.3 area 0
Outros comandos:

#show ip ospf
#show ip protocols
#show ip ospf interface
#show ip route
#show ip ospf database
#show ip ospf neigbors

2.10.2.4.2. Classificação dos roteadores quanto a hierarquia

- **Routers de área principal** – Quanto a hierarquia assumem sempre a existência da área 0 (área principal/backbone);
- **Routers internos** – São aqueles que têm todas as interfaces na mesma área;
- **Routers de fronteiras de área** – São ligados a mais do que uma área (os chamandos ABR – Area Border Router);
- **Routers de fronteira de sistema autónomos** – São aqueles que interligam sistemas autónomos.

Caro leitor se chegou até aqui é lógico que está a nos acompanhar desde o princípio. Segue com máxima atenção e juntos vamos configurar o protocolo OSPF. Na topologia acima já fizemos o endereçamento IP nas interfaces e também já configuramos as interfaces loopbacks. Não seu caso antes de partir para a configuração do protocolo OSPF trate de fazer o devido endereçamento e siga os comandos a baixo.

Note que não precisa fazer igual, aliás, será pouco provável ser igual porque o número das interfaces no teu caso podem ser diferentes, uma ou outra pode coincidir, então trate de compreender o que está feito para fazer algo funcional.

Prática

R1

R1(config)#router ospf 600 *//número do processo//Process ID*
R1(config-router)#network 6.6.6.6 0.0.0.0 area 200
R1(config-router)#network 100.1.1.20 0.0.0.3 area 200

```
R1(config-router)#do wr
R1(config-router)#exit
```

R2

```
R2(config)#router ospf 600
R2(config-router)#network 4.4.4.4 0.0.0.0 area 0
R2(config-router)#network 100.1.1.20 0.0.0.3 area 200
R2(config-router)#network 100.1.1.16 0.0.0.3 area 0
R2(config-router)#network 100.1.1.12 0.0.0.3 area 0
R2(config-router)#do wr
R2(config-router)#exit
```

R3

```
R3(config)#router ospf 600
R3(config-router)#network 1.1.1.1 0.0.0.0 area 0
R3(config-router)#network 100.1.1.16 0.0.0.3 area 0
R3(config-router)#network 100.1.1.0 0.0.0.3 area 0
R3(config-router)#do wr
R3(config-router)#exit
```

R4

```
R4(config)#router ospf 600
R4(config-router)#network 3.3.3.3 0.0.0.0 area 0
R4(config-router)#network 100.1.1.12 0.0.0.3 area 0
R4(config-router)#network 100.1.1.8 0.0.0.3 area 0
R4(config-router)#do wr
R4(config-router)#exit
```

... Continue a configuração dos roteadores R5 e R6.

Dizem por aí que, tudo que é bom dura pouco. No entanto esses foram os passos que devemos prosseguir para a configuração do protocolo

OSPF. Falando de protocolos de encaminhamento chegamos ao fim daquilo que é mais uma jornada. Foi simples e muito útil na vida prática. Agora só nos resta parabenizá-lo e deixar que faça o resto para aperfeiçoar ou seja aprofundar seus conhecimentos em rede.

2.10.2.4.3. Auto avaliação

a) Em poucas palavras descreve a que conclusão chegou?
b) Quais as operações de fluxos do OSPF?
c) Quais são as características do protocolo OSPF?
d) Explique o funcionamento do OSPF.
e) Qual é a ocorrência de saltos no protocolo OSPF?
f) Diferencie o OSPF do EIGRP.
g) Diferencie o OSPF do RIPv2.
h) Classifique os routers quanto a hierarquia.
i) Qual é a sintaxe de configuração do OSPF?

2.11. VLANs

2.11.1. LABORATÓRIO 13

2.11.1.1. Configuração de VLANs

Topologia

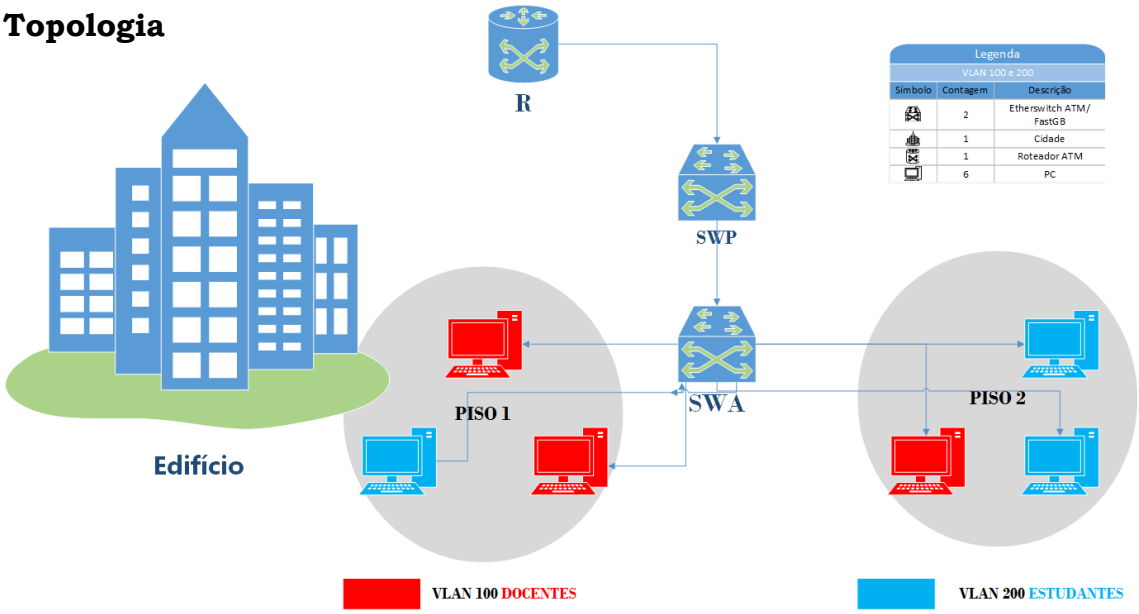


Fig. 47 - Topologia sobre VLAN

Competências

- Saber configurar redes LANs Vitruais (VLANs);
- Saber criar e separar vários domínios de broadcast com um mesmo switch;

Fundamentos

A complexidade e o crescimento das redes informáticas nos dias actuais, é muito comum redes físicas serem construídas por várias redes lógicas, as quais são chamadas de VLANs. Uma VLAN é nada mais que uma separação de rede física em várias redes lógicas de acordo com critérios estabelecidos (ex. separação de trafego por grupo de usuários de departamentos). Agora imagine que uma universidade lhe contacte para montar uma rede. Considerando que sejam implementados os seguintes serviços: controlo de pessoal, gestão de alunos, gestão de serviços acadé-

micos e etc. veja que não faz sentido todos esses serviços fazer parte da mesma rede física. Logo é importante que as máquinas estejam em redes separadas.

A separação de uma rede física em redes lógicas resume-se em:

- ✓ Organização;
- ✓ Segurança;
- ✓ Segmentação;
- ✓ Flexibilidade;
- ✓ Escalabilidade;
- ✓ Redução de custos.

2.11.1.2. Classificação de VLANs

Estáticas – são configuradas estaticamente pelo administrador da rede que vai atribuindo portas do Switch a cada uma das VLANs.

Dinâmicas – são definidas por um Software e geridas por um banco de dados.

Prática

Monte a topologia acima, segundo par e passo as seguintes etapas:

Dado o IP de rede Classe C, determine duas VLANs, uma para os Estudantes e outra para Professores/Docentes.

REDE	**VLAN 100**	**VLAN 200**
192.168.30.0	192.168.30.0	192.168.30.128
Mácara	255.255.255.128	255.255.255.128
Gateway	192.168.30.1	192.168.30.129
DNS server	192.168.30.2	192.168.30.130

Tabela 6 – Descrição de VLANs e seus devidos IPs

Configuração do Switch de Acesso (*SWA*)

Switch>enable

Switch#configure terminal

Switch(config)#hostname SWA

SWA (config)#vlan 100

SWA (config-vlan)#name Docentes

SWA (config-vlan)#vlan 200

SWA (config-vlan)#name Estudantes

SWA (config-vlan)#exit

SWA (config)# interface range fastEthernet0/1-10 *//Faixa de interfaces FE(1-10)*

SWA (config-if-range)#switchport mode access *//Definir como modo de acesso*

SWA (config-if-range)#switchport access vlan 100 *//Potas de acesso VLAN 100*

SWA (config-if-range)#exit

SWA (config)# interface range fastEthernet0/11-20

SWA (config-if-range)#switchport mode access

SWA (config-if-range)#switchport access vlan 200

SWA (config-if-range)#exit

SWA (config)#interface GigabitEthernet0/1*//Interface que liga* ***SWA*** *e* ***SWP***

SWA (config-if)#switchport mode trunk *//Definir o modo Trunk (Tronco)*

SWA (config-if)#switchport trunk allowed vlan all *//adicionar todas as VLAN no modo Trunk*

SWA (config-if)#switchport trunk allowed vlan except 1

Configuração do Switch Principal (*SWP*)

Switch>enable

Switch#configure terminal

Switch(config)#hostname SWP

SWP (config)#

SWP (config)#vlan 100
SWP (config-vlan)#name Docentes
SWP (config-vlan)#vlan 200
SWP (config-vlan)#name Estudantes
SWP (config-vlan)#exit

SWP (config)#interface GigabitEthernet0/1*//Interface que liga **SWP** e **R***
SWP (config-if)#switchport mode trunk *//Definir o modo Trunk (Tronco)*
SWP (config-if)#switchport trunk allowed vlan all *//adicionar todas as VLAN no modo Trunk*
SWP (config-if)#switchport trunk allowed vlan except 1

Configuração do Roteador (*R*)

Roteador
Router >enable
Router #configure terminal
R(config)#hostname R
R(config)#interface gigabitEthernet 0/0
R(config-if)#no shutdown
R(config)#interface gigabitEthernet 0/0.100 *// subinterfaces de VLAN 100*
R(config-subif)# encapsulation dot1Q 100*//Definir o encapsulamento*
R(config-subif)#ip address 192.168.30.1 255.255.255.128
R(config-subif)#exit
R(config)#interface gigabitEthernet 0/0.200 *// subinterfaces de VLAN 200*
R(config-subif)# encapsulation dot1Q 200 *//Definir o encapsulamento*
R(config-subif)#ip address 192.168.30.129 255.255.255.128
R(config-subif)#exit

R(config)# ip dhcp pool **Docentes** *//Definir a poll de IPs no roteador*
R(dhcp-config)#network 192.168.30.0 255.255.255.128
R(dhcp-config)#default-router 192.168.30.1
R(dhcp-config)#dns-server 192.168.30.2

R(config)#ip dhcp pool **Estudantes**

R(dhcp-config)#network 192.168.30.128 255.255.255.128

R(dhcp-config)#default-router 192.168.30.129

R(dhcp-config)#dns-server 192.168.30.130

2.11.1.3. Auto avaliação

a) Faça um breve resumo do laboratório.

b) O que achou da prática?

c) A que conclusão chegou?

d) Como ocorre o processo de separação de redes físicas em lógicas?

e) Classifique as VLANs quanto a configuração.

f) Quais as vantagens de utilização de VLANs em uma organização?

g) Crie e configure as VLANs da topologia com os seguintes departamentos: 10-Finanças 12 PCs, 20-Recuros Humanos 3 PCs, 30-Apoio ao Pessoal 80 PCs, 40- Secretaria

h) Com base aos conhecimentos adquiridos sobre VLANs resolva a topologia a baixo:

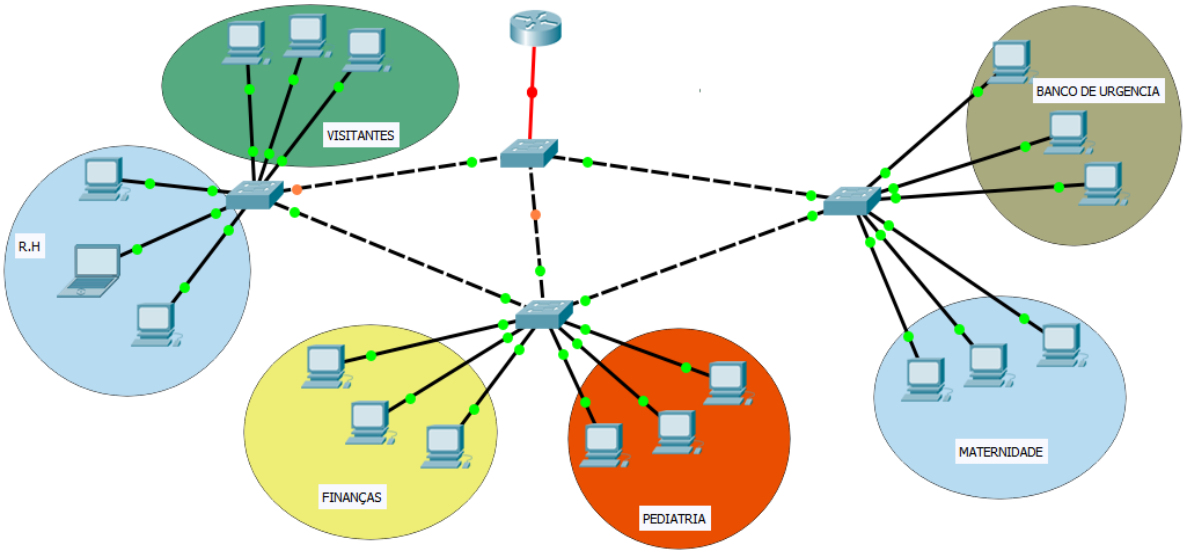


Fig. 48 - Topologia de exercício de VLAN

2.12. LABORATÓRIO 15

2.12.1. Configuração de Links Aggregation com switch

Topologia

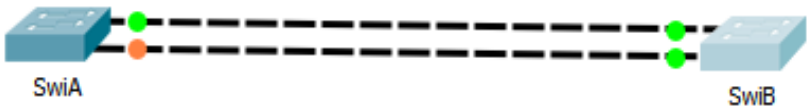


Fig. 49 - Link aggregation com switch

Competências

Em busca de soluções de problemas, queremos que até ao final do laboratório em questão o estudante ou seja, o caro leitor consiga:

- Configurar topologia de rede usando o protocolo LACP/PAgP
- Resolver problemas comuns baseados em Link Aggregation (L.A)

Fundamentos

Link Aggregation é uma nova especificação do IEEE, permite agregar várias portas físicas para formar uma (porta) lógica. Quando se usa Links Aggregation em uma determinada rede, existe uma probabilidade enorme de aumentar a largura de banda, balanceamento de tráfego e outros tantos benefícios.

A agregação (Agrupamento) de diversas interfaces Ethernet (portas físicas) para a utilização de uma única porta lógica com o intuito de prover redundância e aumento de largura de banda é uma actividade muito comum em redes de médio e grande porte.

Este laboratório traz consigo a configuração básica do Ethernet Channel em pilhas nos Switches Ciscos. Em função da velocidade o Ethernet Channel pode ser chamado de Fast Ethernet Channel e Gigabit Ethernet Channel. Para a configuração dos Ethernet Channels ou Port Channel existem dois protocolos principais: O Link Aggregation Control

Protocol (**LACP**) do IEEE e o Port Aggregation Protocol (**PAgP**). Este último é proprietário da Cisco sendo ele usado em Switches ou routers ciscos.

Existem algumas formas de estabelecer a agregação de portas, como por exemplo:

- **Manual:** sem a certificação do meio por protocolos auxiliares;
- **PAgP:** Protocolo disponível em equipamentos Cisco;
- **LACP:** Protocolo padrão IEEE, disponível quase em todos *Switches* gerenciáveis.

Prática

Para configurar o link aggregation nos Switches da cisco é simples. Com base a topologia acima configure o switch da esquerda usando os comandos a baixo:

Switch A

Switch>enable

Switch#configure terminal

Switch(config)#hostname SwiA

SwiA(config)#interface range gigabitEthernet 0/1-2

SwiA(config-if-range)#channel-group 1 mode on

SwiA(config-if-range)#switchport mode trunk *// trunks ou access mode*

SwiA(config-if-range)#exit

SwiA(config)#interface port-channel 1

SwiA(config-if)#exit

SwiA# show etherchannel*//Para mostrar as configuração*

Switch B

Switch>enable

Switch#configure terminal

Switch(config)#hostname SwiA

SwiB(config)#interface range gigabitEthernet 0/1-2

SwiB(config-if-range)#channel-group 1 mode on

SwiB(config-if-range)#switchport mode trunk

SwiB(config-if-range)#exit
SwiB(config)#interface port-channel 1
SwiB(config-if)#exit
SwiB# show etherchannel//*Para mostrar as configuração*

Os comandos **[interface range gigabitEthernet 0/1-2]** permitem a configuração de mais de uma porta em simultâneo. Temos interfaces giga-bits interligando os dois Switches, logo a configuração é a mesma tanto para a interface 1 quanto a 2. No entanto estes são os passos que devemos seguir na configuração do *port-channel* ou link aggegation, tanto nas portas *trunks* assim com de *acesso*. O número de portas vária em função das necessidades o que importa é a forma como se configura. A configuração é a mesma independentemente do número de portas.

2.12.2. Auto avaliação

a) Com base ao conhecimento adquirido faça um breve resumo.
b) O que é um link aggregation?
c) Para que serve os links aggregations?
d) Quais as formas de estabelecer agregação de portas?
e) Define LACP-
f) Como é classificado o *ethernet channel* quanto a velocidade?
g) Mapeie uma topologia VLAN que implemente agregação de portas?
h) Com base aos conhecimentos adquiridos resolva:

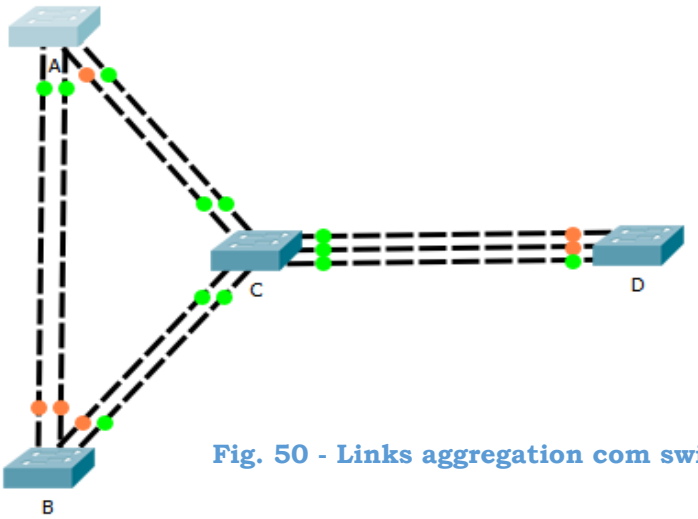


Fig. 50 - Links aggregation com switch, exercicio

2.13. LABORATÓRIO 16

2.13.1. Links aggregation com roteadores

Topologia

Fig. 51 - Link aggregation com routers

Competências

- Saber configurar links aggregation com roteadores
- Configurar topologia de rede usando o protocolo LACP/PAgP nos roteadores

Fundamentos

Para esta prática de laboratório não há muita ladainha a contar, afinal, tudo que se precisa de links aggregation já foi dito na prática de laboratório com switches. Lembre-se, quando se pretende agregar portas *Links Aggregation* podemos usar apenas um protocolo de cadas vez (***Link Aggregation Control Protocol - LACP***) ou (***Port Aggregation Protocol - PAgP***). O PAgP é proprietário da Cisco e o segundo é standard do IEEE permitindo que comutadores de diferentes fabricantes possam formar agregações.

Os protocolos acima mencionados possuem cada um entre eles diferentes modos de funcionamentos: *ON, AUTO, DESIRABLE, PASSIVE e ACTIVE*. Estes modos possuem suas descrições que não vamos aqui frisar.

Prática

Para configuração do *Link Aggregation* ou *Port Channel* nos roteadores da cisco existem alguns requisitos um pouco diferentes dos switches. E, isto torna a configuração mais delicada e atenciosa.

Eis a configuração

Roteador A

Router>enable
Router#configure terminal
Router#hostname A
A (config)#interface port-channel 1
A (config-if)#ip address 192.168.1.1 255.255.255.0
A (config-if)#exit
A (config)#interface range gigabitEthernet 0/0-2*//configurações de portas*
A (config-if-range)#no ip address
A (config-if-range)#channel-group 1
A (config-if-range)# no shutdown
A #show interfaces port-channel 1 *//mostra as configurações*

Roteador A

Router>enable
Router#configure terminal
Router#hostname B
B (config)#interface port-channel 1
B (config-if)#ip address 192.168.1.2 255.255.255.0
B (config-if)#exit
B (config)#interface range gigabitEthernet 0/0-2
B (config-if-range)#no ip address
B (config-if-range)#channel-group 1
B (config-if-range)# no shutdown
B #show interfaces port-channel 1

No entanto estas foram as configurações do port-channel ou link aggregation com roteadores. Muito simples e útil na vida prática.

2.13.2. Auto avaliação

a) Diferencie o *link aggregation* com switches do *link aggregation* com roteador.
b) Será possível configurar o *LACP* e *PAgP* em simultâneo? Porquê?
c) Quais são os modos de funcionamentos do *link aggregation*?
d) Para você o que significa standard?
e) Desenhe uma topologia com cinco (5) roteadores e implemente o link aggregation.

2.14. LABORATÓRIO 17

2.14.1. Configurações de VPNs

Topologia

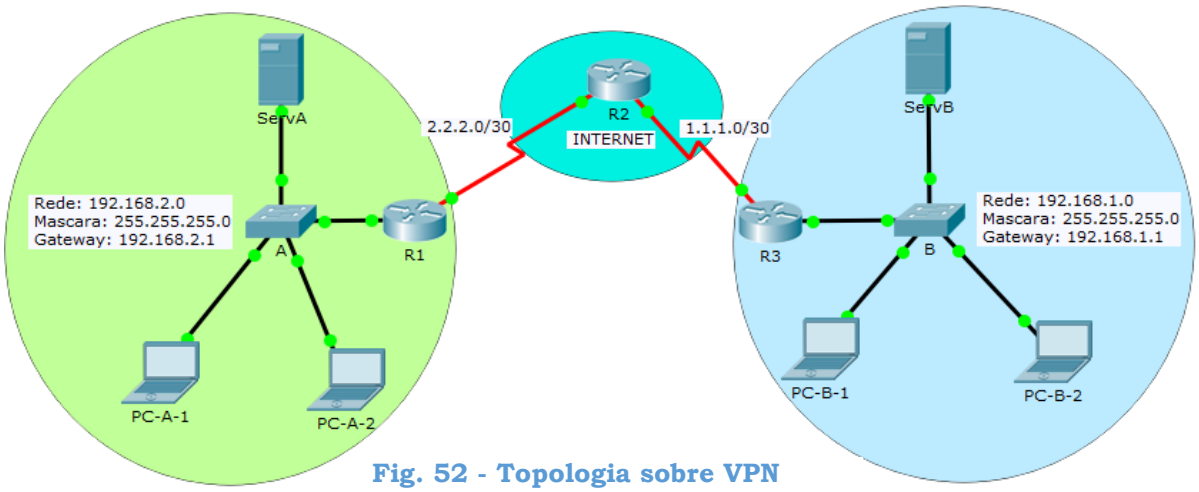


Fig. 52 - Topologia sobre VPN

Competências

Queremos que até ao final este laboratório o caro leitor adquira as seguintes competências:

- Projectar VPN no Packet Tracer;
- Saber configurar o IPSec;
- Saber habilitar o nível de segurança com IPSec;
- Saber habilitar as propriedades do ISAKMP;

– Saber configurar as assinaturas de criptografia nas interfaces de saídas em ambiente Cisco Packet tracer.

Fundamentos

As Redes Virtuais Privadas ou simplesmente VPN (sigla inglesa) são construída sobre uma estrutura de rede pública, a internet. Nas VPNs a comunicação é cifrada de forma a manter confidencialidade dos dados ponto a ponto.

Na verdade quando um cliente estabelece uma ligação VPN, é criado um canal de comunicação seguro, usando técnicas de criptografia e autenticação permitindo a troca confiável de dados sobre redes públicas.

Suite IPSec (IP Security Protocol) é uma pilha de protocolos que permitem a constituição de tuneis seguros sobre redes. Tudo que passa através da rede, é cifrado pelo gateway e IPSec, e decifrado pelo outro extremo da comunicação.

IPSec o que é afinal?

É um protocolo aberto criado pela IETF, que inicialmente foi criado para operar sobre o protocolo IPv6 e que mais tarde foi adaptado para operar no protocolo IPv4. O IPSec pode ser usado de duas formas distintas: em modo de *transporte* e em modo *túnel* e opera sobre três protocolos:

- AH (Autentication Header)
- ESP (Encapsulating Security Payload)
- IKE (Internet Key Exchange).

Vantagens

- Troca de dados de forma mais segura entre terminais ligados a ela;
- Garante que os dados não sejam interceptados por intrusos;
- Oculta a localização geográfica real do internauta.

Prática

Monte a topologia a cima, ver fig.52:

a) Use 3 roteadores 1941, 2 Switches, 2 Servidores e 4 PCs.

Supondo que já tem os IPs das interfaces endereçados, as redes privadas (**A** e **B**) configuradas, segue as etapas seguintes:

Nota: não esquece de fazer roteamento (Estático ou dinâmico)

1ª Etapa: Activar o módulo Securityk9

Para completar esta actividade, devemos primeiros activar a licença de segurança da tecnologia cisco:

a) Estando no modo global digite o comando **show version** para saber se a licença de segurança do módulo **securityk9** está activa, Fig.53.

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
data          None          None          None

Configuration register is 0x2102
```

Fig. 53 - Verificar a licença de segurança do Módulo Security K9

b) O passo seguinte é activar a licença do módulo de segurança (**Security k9**) no **R1**, aceitar (ACCEPT [yes/no]) a licença digitando (**yes**) e reiniciar o roteador. Seguindo os comandos a baixo:

R1(config)#**license boot module c1900 technology-package securityk9**
R1(config)#**end**
R1#copy **running-config startup-config**
R1#**reload**

c) Repetir o processo feito na línea (a), digitando (novamente) o comando **show version**. Ver Fig. 52.

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None

Configuration register is 0x2102
```

Fig. 54 - Activação da licença do Módulo Security K9

Para configurar o **R3** repete-se os mesmos passos das líneas (a - c) realizados no **R1**.

2ª Etapa: Configurar o IPSec no Roteador (R1)

a) Neste passo testa-se a conexão entre o roteador **R1** e um dos computadores da rede **B**.

b) No passo seguinte configurar-se a lista de acesso (Access-list - 110) no **R1** veja como fica:

R1 (config)#access-list 110 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

c) Nesta fase vamos configurar o **ISAKMAP** e suas políticas de criptografia no **R1**, e também configuraremos a chave de criptografia do **ISAKMAP**. Veja o exemplo seguinte:

R1(config)#**crypto isakmp policy 200**
R1(config-isakmp)#**encryption aes 256**
R1(config-isakmp)#**authentication pre-share**
R1(config-isakmp)#**group 2**
R1(config-isakmp)#**exit**

R1(config)#**crypto isakmp key cisco address 1.1.1.2** *//Saída do R3*

d) Configuração do IPSec. Veja como fica no exemplo a seguir:

R1(config)#**crypto ipsec transform-set VPN-CONJUNTO esp-3des esp-sha-hmac**
R1(config)#**crypto map VPN-MAP 200 ipsec-isakmp**
R1(config-crypto-map)#**description Conexao para o Roteador (R3)**
R1(config-crypto-map)#**set peer 1.1.1.2** *//Saida do R3*
R1(config-crypto-map)#**set transform-set VPN-CONJUNTO**
R1(config-crypto-map)#**match address 110** *//Lista de acesso*
R1(config-crypto-map)#**exit**

e) Neste passo vamos e criptografar a interface de saída do **R1** veja a seguir:

R1(config)#**interface serial 0/1/0**
R1(config-if)#**crypto map VPN-MAP**
R1(config-if)#**exit**

3ª Etapa: Configuração do IPSec no Roteador (R3) para permitir conexões via VPN com o R1

a) Configuração da lista de acesso no **R3** (Access-list-110)

R3(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

b) Nesta fase vamos configurar o **ISAKMAP** e suas políticas de criptografia no **R1**, e também configuraremos a chave de criptografia do **ISAKMAP**. Veja o exemplo seguinte:

R3(config)#**crypto isakmp policy 200**
R3(config-isakmp)#**encryption aes 256**
R3(config-isakmp)#**authentication pre-share**
R3(config-isakmp)#**group 2**
R3(config-isakmp)#**exit**

R3(config)#**crypto isakmp key cisco address 2.2.2.1** ***//Saida do R1***

c) Configuração do IPSec. Veja como fica no exemplo a seguir:

R3(config)#**crypto ipsec transform-set VPN-CONJUNTO esp-3des esp-sha-hmac**
R3(config)#**crypto map VPN-MAP 200 ipsec-isakmp**
R3(config-crypto-map)#**set peer 2.2.2.1**
R3(config-crypto-map)#**set transform-set VPN-CONJUNTO**
R3(config-crypto-map)#**match address 110**
R3(config-crypto-map)#**exit**

d) Neste passo vamos e criptografar a interface de saída do **R1**, veja a seguir:

R3(config)#**interface serial 0/1/0**
R3(config-if)#**crypto map VPN-MAP**

4ª Etapa: Verificar a VPN com IPSec

Neste passo utiliza-se o comando **show crypto ipsec sa**. Observe o que acontece com os pacotes.

Finalizando, agradecemos pela sua paciência e estamos convictos que o caro leitor gostou da prática. Foi um momento muito interessante, agora resolva os exercícios que se seguem.

2.14.2. Auto avaliação

a) Com está prática a que conclusão chegou e o que de interessante achou?
b) Que papel desempenha as VPN na transferência de dados?
c) Enumere os passos a seguir para a activação do módulo de segurança Securityk9.
d) Explique o que acontece quando um cliente estabelece uma ligação VPN?
e) O IPSec pode ser usado de duas formas: enumere-as.

f) Mapeie uma topologia ao seu critério usando os conhecimentos adquiridos na prática de laboratório em questão.

2.15. LABORATÓRIO 18

2.15.1. Configuração do VoIP

Topologia

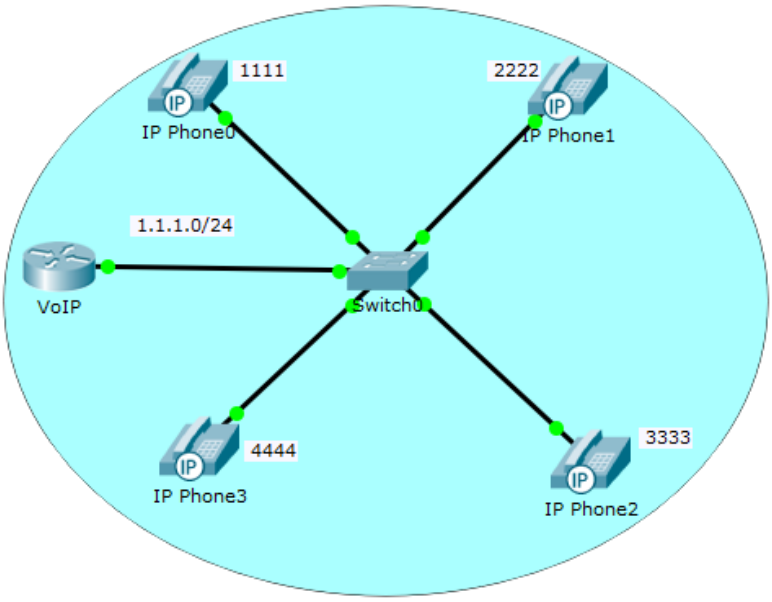


Fig. 55 - Topologia sobre VoIP

Competências

Anseia-se com esta prática de laboratório, que o leitor saiba:

– Configurar serviços de telefonia VoIP no cisco Packet Tracer;

Fundamentos

VoIP é um termo inglês **Voice over Internet Protocol**. Traduzindo significa Voz sobre IP e corresponde sobretudo, a possibilidade de efectuar chamadas de voz ou vídeo através da internet. O VoIP é uma tecnologia que consiste na conversão de sinais analógicos em digitais que posteriormente são enviados através da internet.

Vantagem

- Redução de custos com ligações telefónicas;

Limitações

- Dependência total da internet;
- A qualidade da chamada depende da qualidade do sinal

Prática

a) Monte a topologia acima e faça as devidas ligações. Ao ligar o cabo do switch para o telefone, escolha (switch) e não PC.

Nota: no simulador cisco os telefones encontram-se desligados. Para liga-los temos de conectar o cabo da fonte eléctrica ao telefone. Clique sobre o cabo sem soltar arraste até conectá-lo ao telefone. Veja Fig.56.

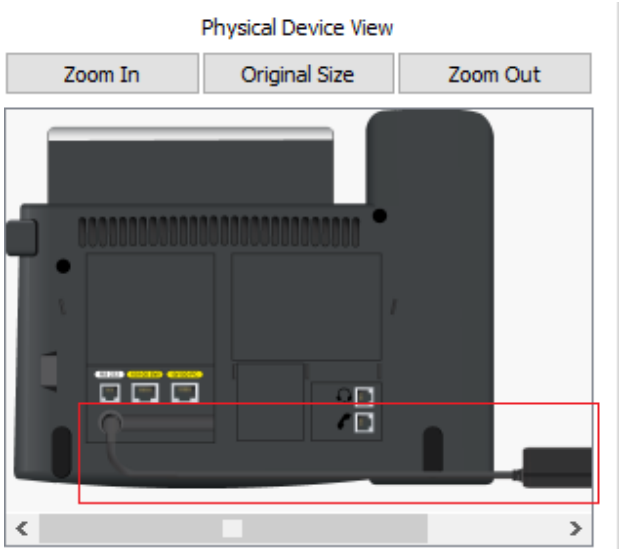


Fig. 56 - Adicionar cabo de alimentação ao Telefone

b) Dando um clique sobre o telefone → Aba GUI, aparece o Interface gráfica do telefone tal como na vida real. Fig. 57

Fig. 57 - Interface gráfica do telefone

Configuração do Switch

Switch>enable

Switch#configure terminal

Switch(config)#interface range fastEthernet 0/1-10

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport voice vlan 1

Switch(config-if-range)#exit

Switch(config)#do wr

Configuração do roteador 2811

Router>enable

Router#configure terminal

Router#(config)#hostname VoIP

VoIP(config)#interface fastEthernet 0/0

VoIP(config-if)#ip address 1.1.1.1 255.255.255.0

VoIP(config-if)#no shutdown

VoIP(config-if)#exit

VoIP(config)#ip dhcp pool VoIP *//Configuração do DHCP pool*

VoIP(dhcp-config)#network 1.1.1.0 255.255.255.0

VoIP(dhcp-config)#default-router 1.1.1.1 *//Adicionar o Gateway*

VoIP(dhcp-config)#option 150 ip 1.1.1.1 *//Coloque no lugar do DNS Server a Opção 150 que é o mesmo Gateway*
VoIP(dhcp-config)#exit

VoIP(config)# telephony-service *//Habilita o serviço VoIP na rede*
VoIP(config-telephony)#max-dn 40 *//Máximo de linhas telefónicas*
VoIP(config-telephony)#max-ephones 40 *//Máximo de dispositivos telefónicos*
VoIP(config-telephony)#ip source-address 1.1.1.1 port 2000
VoIP(config-telephony)# auto assign 1 to 40
VoIP(config-telephony)# exit

VoIP(config)#ephone-dn 1 *//Configurar o telefone 1*
VoIP(config-ephone-dn)#number 1111
VoIP(config-ephone-dn)#exit

VoIP(config)#ephone-dn 2 *//Configurar o telefone 2*
VoIP(config-ephone-dn)#number 2222
VoIP(config-ephone-dn)#exit

VoIP(config)#ephone-dn 3 *//Configurar o telefone 3*
VoIP(config-ephone-dn)#number 3333
VoIP(config-ephone-dn)#exit

VoIP(config)#ephone-dn 4 *//Configurar o telefone 4*
VoIP(config-ephone-dn)#number 4444
VoIP(config-ephone-dn)#exit

Fácil né? É, muito fácil e prático também.

2.15.2. Auto avaliação

a) A que conclusão o caro leitor chegou?
b) O Que de importante colheu neste laboratório?
c) O que significa a sigla VoIP?
d) Enumnere as vantagens desta tecnologia.
e) Enumere suas limitações.
f) O que é VOIP?
g) Monte uma topologia que implemente o serviço que acabou de aprender.
h) A empresa SoftNet é nova no mercado angolano e, está precisando um administrador de rede para a implementação de uma rede com os seguintes serviços: Uma VLAN com 20 usuários normais, uma VLAN com 10 utilizadores para o departamento de Finanças, uma VLAN com 5 utilizadores para o departamento de R.H, uma VLAN com 7 telefones para o sercretaria e recepção e 2 telefones para o gabinete do director geral e o adjunto. Protamente você colaborou e aceitou. Desenhe a topologia e implemente os serviços pretendidos.

2.16. LABORATÓRIO 19

2.16.1. Serviço de TV no Cisco Packet Tracer

Topologia

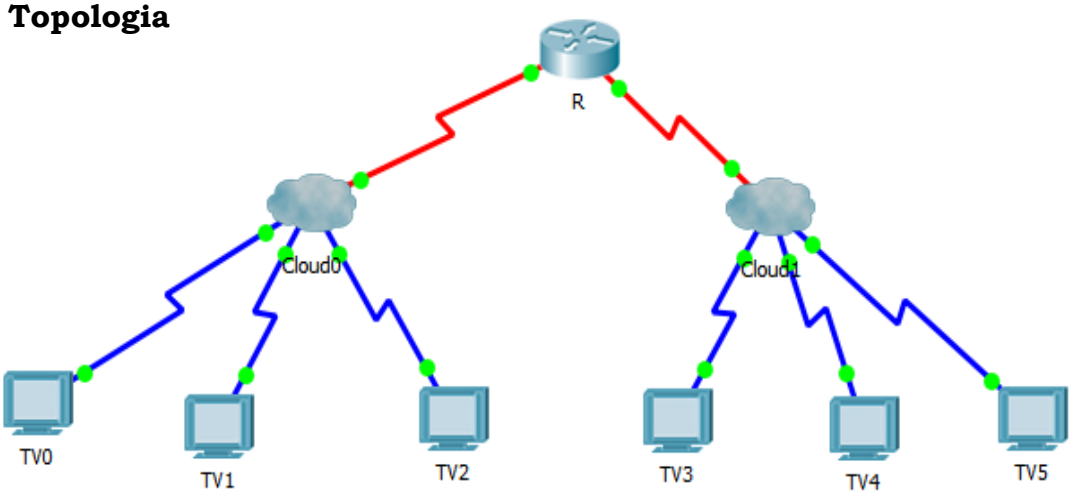


Fig. 58 - Serviço de TV no Cisco Packet Tracer

Competências

Pretende-se que até ao final da prática de laboratório o leitor consiga:

- Configurar serviço de TV no ambiente Cisco Packet Tracer
- Configurar serviço de salas vídeos conferências

Fundamentos

Este laboratório mostra como é feita a configurar e manusear serviços de TV no ambiente virtual Cisco Packet Tracer. Na verdade este não é um laboratório como tal, é, apenas um fundamento prático para quem deseja aprender mais.

Este laboratório tem por foco, não só, mostrar como é feita a implementação de serviços de TV no Cisco Packet Tracer, como também, ilustrar como é feita a configuração (simulação) de serviços de sala de vídeos conferências.

Prática

Com o Cisco Packet Tracer aberto, siga as instruções abaixo com base a topologia acima, ver figura 58.

a) Adicionar um roteador 2811,2 Generic Cloud-PT e 6 TVs (TV-PT)

Configurações

– Dando um clique sobre o Cloud, aparece a figura a baixo, aba ***Physical*** adicionar duas (2) portas ***PT-CLOUD-NM-1CX*** no Cloud, sem esquecer de desligar primeiro equipamento. Repita o mesmo procedimento no outro Cloud. Ver fig. 59

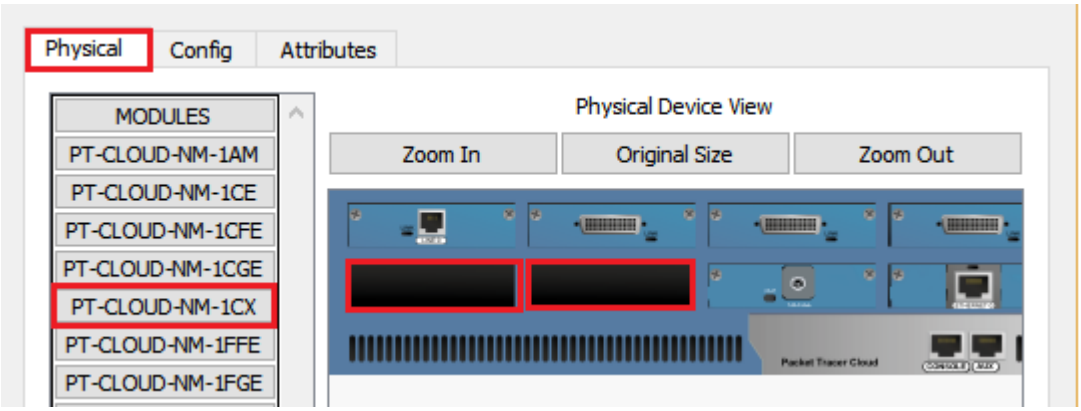


Fig. 59 - Adicionar portas coaxiais no Cloud-PT

– Neste ponto vamos adicionar portas seriais ao roteador 2811. Abrindo o roteador, aba Physical e adiciona-se a porta ***NM-4A/S***

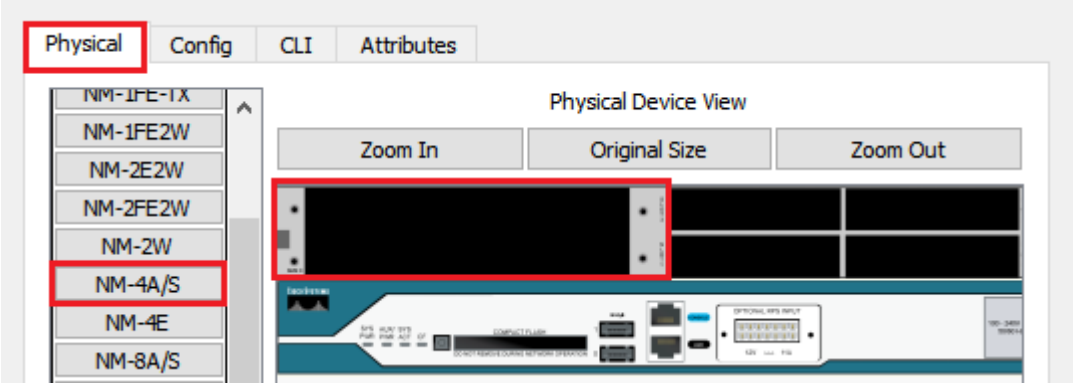


Fig. 60 - Adicionar porta serial ao roteador 2811

– Interligar o roteador com dois (2) cabos seriais e as TVs com o Coaxial. Ver fig.58
– Configure as interfaces do roteador seguindo os comandos a baixo:

Router>enable
Router#configure terminal
Router(config)#interface Serial1/0//*Interface Serial 0/1*
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.35.1 255.255.255.0
Router(config)#interface Serial1/1//*Interface Serial 1/1*
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.36.1 255.255.255.0

– Neste passo vamos ao ***Cloud*** → *Aba Config* ***TV Settings*** e clique no botão [**...**] para buscar imagens no directório em que se encontram. Clique na imagem e clique em [**+**] para adicionar. Adicione quantas quiser ver fig. 61. Faça o mesmo no outro Coud.

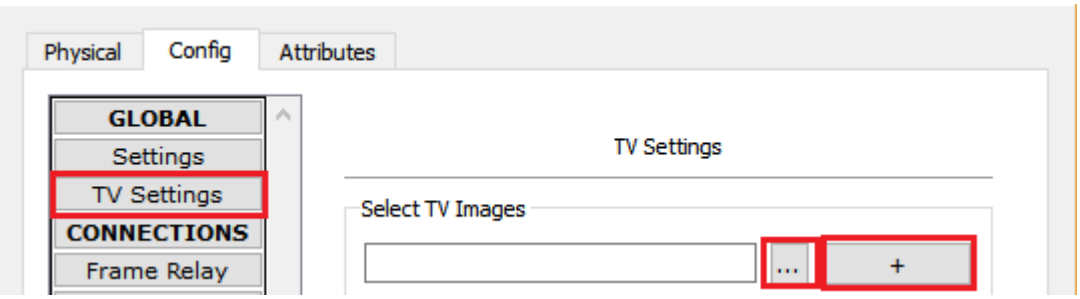


Fig. 61 - Adicionar imagens no Cloud

– Para visualizar as imagens, basta clicar na TV clicar em ***ON***, aparecerá uma figura similar a imagem a seguir.

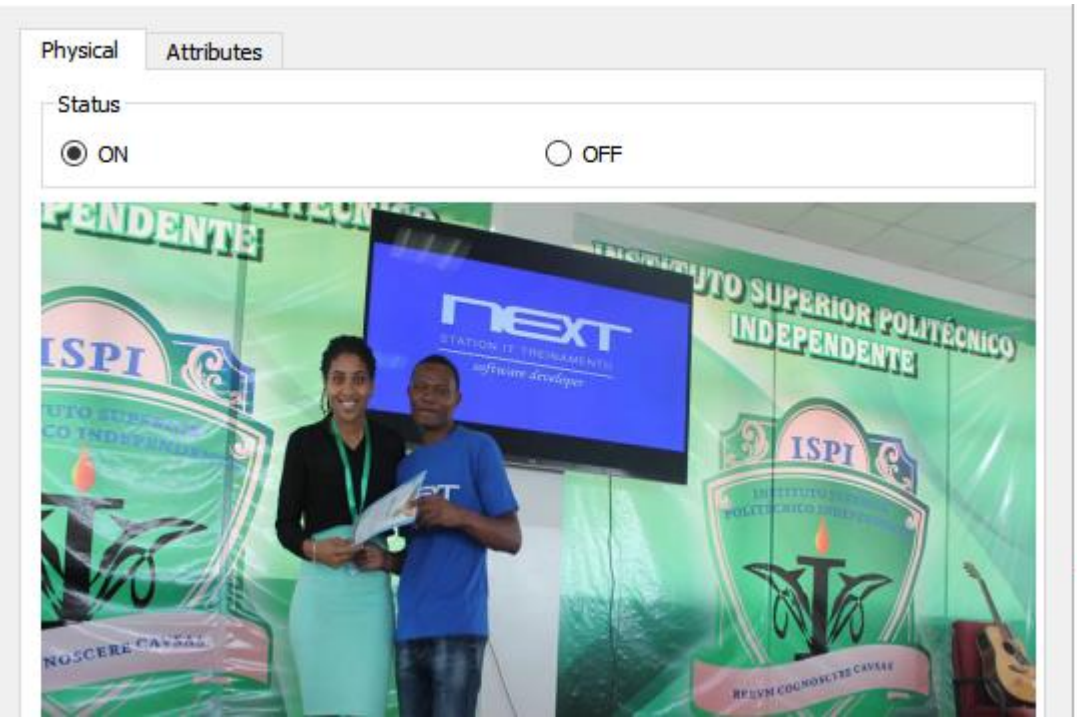


Fig. 62 - Visualização de imagens na TV

Resumindo, foi mais um laboratório introdutório sobre serviço de televisão e internet. Parabéns por chegar até aqui. Se desejar aprofundar seus conhecimentos não pare por aqui.

2.17. CONCLUSÃO

Sem mais palavra, resta-nos agradecer e parabenizá-lo pela paciência e o belo esforço de estar connosco em todos os laboratórios. Pontanto o agradecemos a você, por acompanhar-nos nesta grande jornada de práticas de laboratório no ambiente Cisco Packet Tracer desde o primeiro laboratório até ao último. Acredita-se que se você seguiu do primeiro ao último aproveitou e ganhou muito conhecimento.

Este Guia constitui uma grande ferramenta daquilo que é o foco do mesmo, uma vez que trata de ser um Guia de Práticas de Laboratório para auxiliar os estudantes do 3º ano do Curso de I.E no ISCED/HLA na Disciplina de Rede de Computadores e não só. É válido para qualquer leitor que espera aprender a tão desejada ferramenta que nos liga ao mundo do conectivismo.

Se deseja aperfeiçoar suas práticas e aprofundar seus conhecimentos, não pare por aqui, busque e corra atrás do conhecimento. Aprender é uma tarefa diária e um investimento árduo, então é necessário que busquemos aprendizagem todos os dias da vida.

Esperamos que gostem do guia e estaremos abertos para sugestões e críticas.

Boa sorte!

2.18. LISTA DE EXERCÍCIOS PROPOSTOS

2.18.1. Problemas

1. Problema:

No congresso internacional de TI que ocorreu em Angola, concretamente na província da Huíla, abordou-se vários temas e um deles foi a criação de uma rede local que pudesse unir a UMN e ISCED/HLA, ambas Instituições sediadas na mesma província.

O Administrador de rede forneceu a faixa de IP 190.35.0.0/17 e o projecto foi aceite. Segmente a rede de modo que permita ter:

a) Três (3) sub-redes para dispositivos móveis dos estudantes. Cada sub-rede deve suportar no mínimo 715 dispositivos;
b) Uma (1) sub-rede com 38 câmeras de vigilância para laboratórios de Informática;
c) Uma (1) sub-rede para 4094 Computadores;
d) Uma (1) sub-rede para 356 servidores;
e) Qual é a faixa de IPs válidos em cada sub-rede?
f) Qual é a nova máscara que achou em cada sub-rede?
g) Quais o endereços de broadcast de cada sub-rede?
h) Totalizando quantas sub-redes foram criadas?

2. Problema:

Tio António deseja subdividir a faixa de IPs (172.59.0.0/16) da sua empresa. Segundo ele, o modelo "**Classless**" ajuda bastante a diminuir o desperdício de endereços IPs. A empresa de a Tecno Corporation, tem 16 filiais. Cada filial tem entre 800 a 950 dispositivos conectados na rede. Tio António ficou em dúvida como realizar este cálculo, diante disso solicitou sua ajuda. Realize os cálculos e explique ao tio António todo procedimento que você realizou para encontrar as sub-redes.

a) Qual é número de bits emprestado?
b) Liste os endereços de rede de cada sub-rede;
c) Liste os endereços de broadcast de cada sub-rede;
d) Liste o total de sub-redes que achou_____;
e) Número de host válidos_____;
f) Qual será a nova máscara para satisfazer os requisitos?
g) Qual é a faixa de endereços destinados a numeração de hosts da 10ª sub-rede?

3. Problema

Do IP dados da Classe B 172.58.0.0/16 apresente os resultados convincentes para 10 sub-redes

a) Quantas sub-redes achou?
b) Qual é a nova mascara?
c) Total de sub-redes .
d) Total de endereços válidos por cada sub-rede.
e) Total de bits emprestados.
f) Endereços de broadcast de cada sub-rede.

4. Problema

O Sr. João António está participando na conferência Internacional de telecomunicações a ser realizado na província do Huambo. Ele, inicialmente deseja criar uma seção no campus da região sul. Na concepção dele, todas as universidades devem estar interligadas. Outros aspectos a serem considerados:

a) Cada universidade tem uma rede local, sendo UMN com os endereços 192.168.1.0/26; ISCED-HUILA: 172.16.1.0/25; ISPI: 10.10.0.0/24; CC: 10.20.0.0/26;
b) O primeiro IP de cada rede local deve ser alocado para o roteador;
c) Cada rede local deve ser representada por três computadores;

d) Todos os computadores – de todas as redes – devem se comunicar;
e) A interligação entre as redes deverá utilizar as faixas de rede mostradas na topologia;

5. Problema

O ISPI recebeu uma nova faixa de endereços IPv4. Salomão, recebeu a missão de descobrir quantos IPs estão disponíveis para a nova faixa, infelizmente o administrador da rede só disse para ele a máscara de sub-rede. Portanto, ajude-o a descobrir quantos IPs estão disponíveis em uma rede que use a máscara 255.255.252.0.

6. Problema

Jorge deseja subdividir a faixa de IPs (10.2.0.0/16) da sua empresa. Bem, segundo ele, o modelo "Classless" ajuda a diminuir o desperdício de endereços IPs. A empresa dele, a Jo Corporation, tem 16 filiais. Cada filial tem entre 800 e 950 dispositivos conectados na rede. Jorge ficou em dúvida em como realizar esse cálculo, diante disso, solicitou a sua ajuda. Realize os cálculos e explique a Jorge todo o procedimento que você realizou para encontrar as sub-redes.

7. Problema

A empresa Fenix Innovation está querendo interligar suas filiais. Ela deseja que haja comunicação entre as filiais, a ideia inicial é de uma topologia full-mesh (todos os roteadores interconectados). O professor Tomás Selombo é o administrador de redes de lá e lhe chamou para implementar tais mudanças na rede. A proposta dele é utilizar a faixa 10.4.0.0/16 para as interligações.

No total são 5 filiais: Lubango (rede local: 172.16.0.0/21), Humpata (rede local: 172.16.8.0/21), Chioco (rede local: 172.16.16.0/21), Arco-íris

(rede local: 172.16.24.0/21) e Chibia (rede local: 172.16.32.0/21). Monte no simulador Cisco Packet Tracer a topologia explicada obedecendo aos seguintes critérios:

a) Configure o endereçamento entre as filiais visando dirimir todo e qualquer desperdício de endereços IP;
b) Configure a velocidade dos links utilizados para interligação das filiais para 8,5Mb/s
c) Configure a velocidade dos links utilizados para rede local com a velocidade de 2048Kb/s
d) Configure o roteamento estático
e) Todas as redes locais devem ser representadas por um computador
f) Por fim, teste a comunicação entre todos os computadores por meio do ping e do tracerat
g) Refaça o roteamento, agora utilizando o protocolo RIP – na versão que você julgar mais adequada.

8. Problema

O Ministério das Telecomunicações e Tecnologias da Informação está reestruturando a rede de todos os campus universitários. Agora, cada campus terá uma rede corporativa e uma rede académica – ambas serão disponibilizadas por meio de uma rede sem fio. Monte uma simulação no Cisco Packet Tracer obedecendo aos seguintes critérios:

a) Configure 4 roteadores, cada um sendo um campus (o nome dos campus fica a seu critério);
b) Cada campus deverá ter dois Access Points configurados – um para rede corporativa (SSID WMTTI-Corporativo) e um para académica (WMTTI-Aberta);
c) Cada rede sem fio deve ter dois clientes configurados;
d) A comunicação entre os campus deve ser concentrada em um único roteador (Campus central);

e) Cada campus deverá ter duas sub-redes, a académica comportando 2000 mil hosts e a corporativa suportando 1230 hosts;
f) O endereçamento da rede académica deve estar dentro da faixa 200.143.0.0/16;
g) O endereçamento da rede corporativa deve estar dentro da faixa 177.20.128.0/19;
h) A faixa de rede para interligação é 10.4.0.0/16
i) O roteamento deve utilizar o protocolo OSPF.

9. Problema

Partindo do endereço lógico da classe 200.23.56.0. Calcule o melhor ajuste VSLM para 5 LANs de acordo com número se hosts de cada uma e também para os 4 links WANs que interligam as 5 LANs. LAN A com 25 hosts, LAN B com 35 hosts, LAN C com 9 hosts, LAN D com 61 hosts e a LAN 5 hosts.

a) Apresente a referida topologia usando 4 roteadores e torne-a operacional
b) Apresente todos os cálculos possíveis
c) Quais faixa de IPs destinadas a numeração de hosts para cada LAN?
d) Qual é a faixa destinada a numeração de hosts para os links WANs?

10. Problema

Resolva a topologia com base a quantidade de hosts exigida por cada sub-rede. Os números situados dentro dos círculos representam a quantidade de hosts para os links WANs.

Dado o IP da classe C 192.168.1.0 resolva a topologia:

Topologia

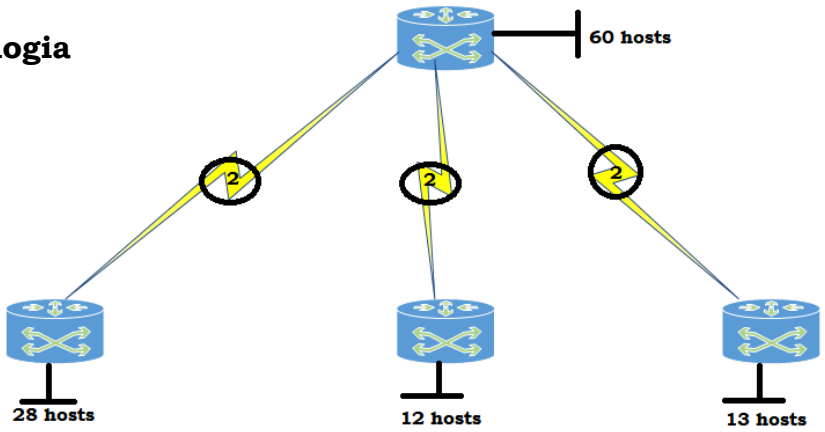


Fig. 63 - Topologia de rede relativo ao 10° problema

11. Problema

Um administrador de rede precisa implementar uma rede usando o IP 192.168.50.0, de tal forma, ter uma (1) sub-rede para 14 hosts, uma (1) sub-rede para 15 hosts, uma (1) sub-rede para 30 hosts, uma (1) sub-rede para 120 hosts e quatro (4) sub-redes com dois (2) hosts disponíveis para endereçar as portas dos roteadores. Você foi convidado para dar suporte ao administrador. Por isso especifique:

a) Os IPs de rede de cada sub-rede.
b) Os IPs de broadcast de cada sub-rede.
c) A faixa destinada a numeração de hosts de cada sub-rede.

2.18.2. Exercícios

1. Dado o endereço de rede 167.99.34.66 e a máscara 255.255.255.192. Quais são os endereços IPs que podem ser usados nesta rede?
2. Do IP 194.5.118.3 e da máscara 255.255.255.0. Quais são as sub-redes?
3. Quais endereços de redes podem ser usados na rede 140.1.1.1 com a máscara 255.255.255.0?
4. Quais das seguintes sub-redes são válidas na rede 180.1.0.0 quando se utiliza a máscara 255.255.255.0?

a) 180.1.2.0
b) 180.1.4.0
c) 180.1.8.0
d) 180.1.16.0
e) 180.1.32.0
f) 180.1.40.0

5. Considerando as afirmações abaixo, indique as afirmações verdadeiras e justifique as falsas:

I. ( ) Quando um computador da na rede A necessita se comunicar com um computador da rede B, ele envia uma mensagem ARP Request em Broadcast solicitando o endereço físico (MAC) do destinatário da rede B.

II. ( ) Os pacotes enviada pelos computadores da rede A para a B, poderão seguir um trajecto de acordo com o nível de congestionamento dos enlaces da rede.

III. ( ) A camada física, representa um conjunto de bits 0 e 1 em formato eléctricos ou ópticos.

IV. ( ) o HTTP é um protocolo que permite que as aplicações desenvolvidas por fabricantes diferentes se comuniquem pela rede.

V. ( ) A camada física define os endereços do tipo MAC.

VI. ( ) A camada de rede define os endereços lógicos.

VII. ( ) Os switches Ethernets possuem internamente uma tabela que relaciona os endereços MAC dos computadores as portas aos quais estão conectados.

VIII. ( ) Os Hubs são dispositivos de camada 1 e, operam sempre em broadcast.

IX. ( ) O CSMA/CD é uma protocolo de controlo de comunicação de dados utilizado em uma rede por difusão para que todos Workstations possam receber todas as mensagem.

X. Se existirem duas LANs para serem interligados utilizar-se-ia um hub.

6. Os dispositivos de rede que baseiam seu roteamento em endereços de tabelas são:
   a) Gateways e Switches ( )
   b) Switches e pontes ( )
   c) Repetidores e Switches ( )
   d) Roteadores e pontes ( )
   e) Roteadores e hubs ( )

7. Em relação aos roteadores e switches, assinale as opções incorrectas
   a) Os switches tradicionais (de camada 2) transportam o quadro inteiro de acordo com o seu MAC. Já nos roteadores o pacote é extraído do quadro e o endereço contido no pacote é usado com o objectivo de definir para onde é enviado o quadro.
   b) Os roteadores são dispositivos de propósitos especial, dedicado a tarefa de interconexão de redes, sendo apropriados para conectar duas LANs, WANs ou mais. Porém, não é possível conectar uma LAN a uma WAN, pois para esse tipo de conexão é preciso utilizar um Gateway
   c) Para realizar um roteamento entre máquinas em redes distintas, é importante possuir um endereço lógico de cada computador, outrossim, cada roteador é designado apenas com um IP público.
   d) Os switches (de camada 3) realizam a conversão semântica da mensagem, sendo possível a troca de pacotes entre redes com conexão TCP e outra com SNA.
8. Assinale o equipamento que representa dispositivos de camada 2 do modelo OSI:
   a) Switches
   b) Roteadores
   c) Hubs
   d) Gateway
   e) Patch-panels
9. Em uma rede de computadores, um gateway é usado para:

a) Converter nomes de sites em endereços IPs
b) Permitir a conexão entre dois computadores com arquitecturas de redes diferentes
c) Criar uma conexão segura entre dois computadores
d) Verificar o conteúdo dos pacotes e identificar vírus de computadores
e) Aumentar o sinal de transmissão de redes sem fio.

10. É um dispositivo utilizado em redes de computadores para reencaminhar módulos (frames) entre os diversos nós. Além disso, segmenta a rede internamente, sendo que a cada porta corresponde um domínio de colisão diferente, o que significa que não haverá colisões entre pacotes de segmentos diferentes. Qual é o equipamento?

11. Assinale as afirmações correctas. As redes Ethernet que utilizam Switches no lugar de hubs como ponto de conexão central para as máquinas conectadas a elas possuem as seguintes vantagens:
a) Homogeneidade dos enlaces, garantido que todas as portas tenham a mesma velocidade.
b) Capacidade de processar pacotes até ao nível de rede simplificando a administração.
c) Eliminação de colisões permitindo que a vazão total roteada seja proporcional ao número de portas.
d) Filtragem de pacotes com base no endereço IP do remetente, aumentando a segurança da rede.