TÉCNICAS DE SWITCHING

UNIDADE 2 - VLANS (IEEE 802.1Q)

Bruno de Souza Toledo

Introdução

As mudanças tecnológicas acontecem cotidianamente, tendo maior impacto nas empresas e nas redes de computadores comerciais, fazendo com que os administradores de rede façam constantes alterações em seus locais de trabalho. A realização dessas alterações nem sempre é fácil de realizar, pois, por exemplo, um par trançado do computador de um usuário poderá estar longe demais do *hub* correto.

Tendo em vista essa constante necessidade de alterações, para que os usuários pudessem ter suas solicitações atendidas com maior flexibilidade, os fornecedores de redes buscaram reverter o problema das atualizações, apresentando uma solução que substitui o cabeamento por *software*. Essa solução resultou na VLAN, ou LAN Virtual, regulamentada sob a norma IEEE 802.1Q e, atualmente, utilizada em muitas organizações.

Você sabe o que é VLAN ou LANs Virtuais? Considerando que você já possui um conhecimento básico em redes de computadores, conhecendo os principais tipos de redes e o enlaçamento de dados, iremos aqui estudar como fazer a aplicação de uma rede local virtual, VLAN.

Mas o que a LAN tem a ver com a VLAN? A LAN engloba todos os dispositivos de uma localidade, tais como: roteadores, servidores, impressoras. Uma LAN inclui, no mesmo domínio de *broadcast*, todos os dispositivos, de forma que quando um dispositivo envia um *frame* em *broadcast*, todos que estão conectados à rede irão recebê-lo. Já com o uso de VLANs, consegue-se separar os dispositivos em domínios de *broadcasts* distintos, que exigem, cada um deles, uma nova sub-rede. Com o uso de VLANs, um único *switch* pode ter diversos domínios de *broadcast*.

As LANs Virtuais são redes locais que agrupam um conjunto de computadores por meio de uma segmentação lógica. Ao configurar uma rede LAN Virtual, o responsável por ela tem que verificar quantas delas deverão ser criadas, quais computadores estão em cada rede e qual será o nome de cada uma. (TANENBAUM; WETHERALL, 2011).

Com o uso da VLAN diminui-se a quantidade de dispositivos no mesmo domínio de *broadcast*, que é quando um computador - ou até mesmo outro dispositivo conectado à rede - é capaz de fazer a comunicação com outro, sem ter a obrigação de utilizar um dispositivo de roteamento. Ela também diminui o uso de Unidade Central de Processamento (CPU) para envio dos *frames,* minimizando os riscos de segurança na medida que reduz o número de dispositivos que receberão os *frames*.

Nesta unidade, iniciaremos o aprendizado das VLANs, visando compreender quais são suas funções em uma rede, seus protocolos e suas configurações. Também veremos como configurar, com detalhes, as VLANs em *switches*, utilizando o simulador Cisco Packet Tracer.

2.1 Teoria, protocolos e configurações

Existem várias definições teóricas e conceituais para a VLAN, mas, de forma simples,

podemos dizer que uma VLAN é a divisão de um *switch* em partes que não estão se comunicando diretamente.

Nascimento e Tavares (2012), afirmam que uma VLAN é formada de dois ou mais dispositivos, compostos de *hardware*, interligados através de uma topologia física e lógica, que se comunicam entre si, formando uma rede, que nesse caso é desenvolvida para atender a determinados critérios, tais como: confiabilidade, desempenho e segurança.

Haffermann (2009, p. 2), também defende que para a obtenção do mesmo nível de "segmentação e segurança de uma rede local pode-se utilizar uma VLAN, pois esta proporciona uma segmentação lógica da rede através de comutadores (*bridges* ou *switches*) com esta função".

VOCÊ O CONHECE?

Walter David Sincoskie, engenheiro de computação americano, foi o inventor da VLAN. Ele também instalou a primeira rede local de *ethernet* no Bellcore, além de criar a tecnologia de voz sobre IP. Sincoskie se formou bacharel, mestre e doutor em Engenharia Elétrica pela Universidade de Delaware. Em 1984, em Bellcore, trabalhou como gerente no *Computer Communications Research,* criando o telefone via Internet, que resultou na VLAN que conhecemos.

A seguir falaremos mais sobre a VLAN, apresentando discussões sobre o seu uso e sua importância para as redes.

2.1.1 Por que VLANs em uma rede?

É comum uma VLAN em uma rede? Sim, atualmente é comum várias redes lógicas, constituídas por VLANs. Seu uso se justifica devido ao crescimento e complexidade das redes, que apresentam, por exemplo, o aumento dos grupos de usuários, os diferentes departamentos de uma empresa, bem como o aumento da quantidade de informações e velocidade na rede, que crescem a cada dia. (HAFFERMANN, 2009).

Observa-se, ainda, a maior necessidade de compartilhamento de equipamentos, tais como impressoras, câmeras, entre outros, por um mesmo meio de comunicação e,

assim, temos um alto tráfego na rede, que deverá ser bem gerenciada para evitar lentidão, travamentos ou falhas em seus serviços.

Imagine uma faculdade com diversos departamentos e que você foi contratado para construir toda a rede. Ela precisará de serviços e usuários diferentes trafegando por essa rede. Eles, por sua vez, serão ligados na mesma rede física, mas suas máquinas devem ficar separadas, mesmo que elas estejam conectadas no mesmo *switch* ou segmento de rede. Imagine a questão de segurança que envolve essa rede. Um aluno não poderá estar na mesma rede do serviço de recursos humanos, ou secretaria, por exemplo, certo?

Para exemplificar a rede dessa faculdade, podemos esboçar o seguinte cenário: 4 grupos de usuários com perfis distintos (recursos humanos, secretaria, direção e biblioteca). Os usuários desses 4 grupos encontram-se distribuídos no mesmo prédio, mas em andares diferentes, portanto, para esse rede foram configuradas VLANs para cada grupo. Essa comunicação entre os usuários, para acessarem os serviços diferentes de cada setor, só é possível se for configurado o encaminhamento no roteador, conforme a seguinte figura.

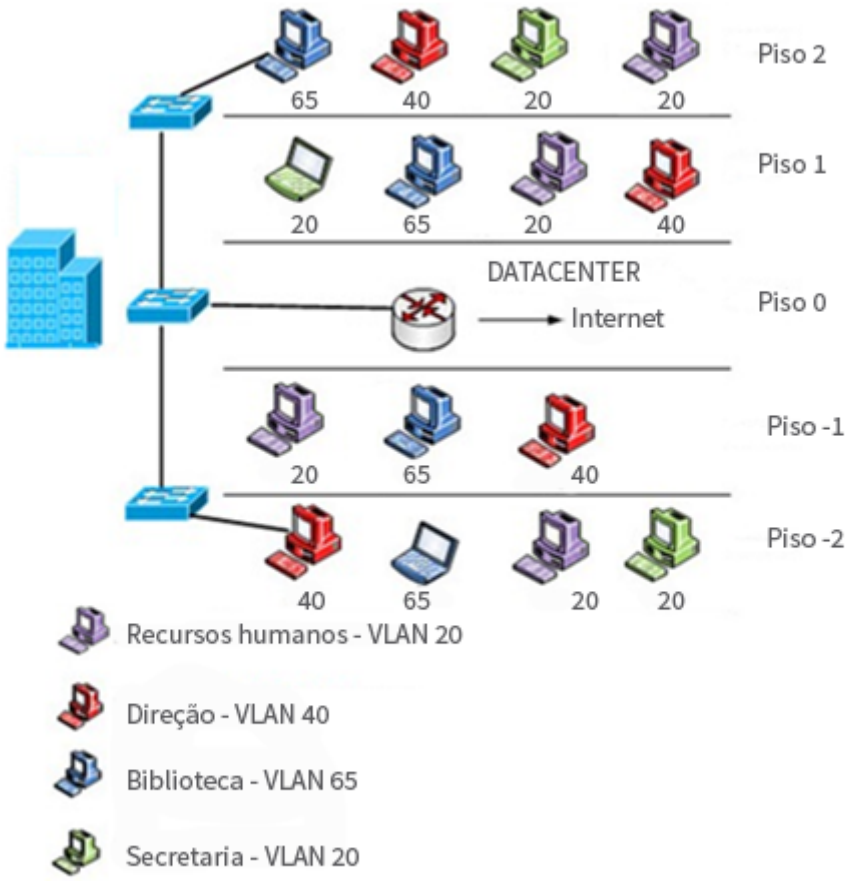


Figura 1 - Configuração do encaminhamento no roteador.
Fonte: Elaborado pelo autor, 2019, baseado em CISCO, 2006.

VLANs em uma rede física têm a sua composição definida pelos critérios de organização, segmentação e segurança. Esses três critérios podem ser descritos conforme descrição abaixo. Clique e confira!

Organização	Distintos setores ou serviços podem ter a sua própria VLAN, que poderá ser configurada nos *switches* existentes, e, assim, usuários do mesmo setor podem, por exemplo, ficar em locais físicos diferentes.
Segmentação	É permitido separar a rede física em redes lógicas menores, para administrar melhor a utilização e o tráfego. A segmentação surgiu para restringir a dissipação de *broadcasts* em uma rede local, ou seja, irá segmentar a rede e bloquear *broadcast* de equipamentos.

Segurança	Critério que define se os usuários de uma rede podem ou não ter acesso a determinadas informações de um setor.

VAMOS PRATICAR?

Considere a seguinte situação-problema: você foi contrat
ser o administrador da rede de uma faculdade e im
tecnologia VoIP. Por conta disso, o diretor da faculdade o
para fazer o novo mapeamento da faculdade, especifi
possibilidades da implantação VoIP, levando em consideraçã
funciona de duas formas: ligações feitas de computa
computador e ligações feitas de computador para telefon
celular.

Considerando a situação-problema apresentada, você
apresentar um esboço de um projeto com as ações necessá
a execução desse trabalho, tais como: 1) fazer a segmen
redes de dados e voz em redes distintas, tendo em vista o
melhorias que ela trará para a rede da faculdade; 2) apres
cenário com perfis distintos de uso da rede, bem
equipamentos necessários para criar e administrar
descrevendo quais são os seus critérios de uso. Não es
compartilhar a sua atividade no fórum da seção “Compartilh

Agora que você já descobriu as vantagens da VLAN em uma rede, veremos, no próximo item, que há diferentes tipos de VLANs, conceituando cada um deles.

2.1.2 Tipos de VLANs

As VLANs são classificadas de quatro maneiras: baseadas em Portas, endereço MAC, em Tipo de protocolo e Camadas Superiores. De acordo com Chapell e Farkas (2003), cada um desses tipos pode ser explicado do seguinte modo:

- VLAN baseada em Portas: para cada VLAN há um conjunto de portas integrantes. Pode-se dizer que a desvantagem é que

nesse tipo de rede quando uma estação tem o seu local alterado, passando a utilizar uma porta diferente daquela associada anteriormente, o administrador da rede deverá efetuar uma reconfiguração do comutador;

- VLAN baseada em Endereço MAC: o mapeamento ocorre entre o endereço MAC e a porta VLAN correspondente. Porém, sem precisar reconfigurar o comutador, o que é uma vantagem, pois, após alterar o lugar da estação, o MAC que está associado à interface de rede do computador continua ligado na sua VLAN. A desvantagem é que o agrupamento deve ser feito já no início e se houver muitos computadores conectados a situação se torna complexa;
- VLAN baseada em Tipo de protocolo: é a segmentação de VLANs que utiliza como critério o tipo de protocolo que irá fazer a comunicação. Então, o IP de sub-rede é utilizado para unir as VLANs. Uma vantagem é que as estações podem alterar de localidade sem precisar reconfigurar a rede, porém, gasta-se mais tempo para o envio e recebimento da informação;
- VLAN baseada em Camadas Superiores: são segmentadas por aplicação ou serviço. Um exemplo: a disponibilização de um servidor Protocolo de Transferência de Hipertexto (HTTP) para uma VLAN específica, e um serviço de Protocolo de Transferência de Arquivos (FTP) em outra VLAN.

2.1.3 Conexões de Dispositivos VLANs

Baseado em um *switch* Cisco para a criação de VLAN, existem alguns tipos de portas, como: as portas de acesso (ligações de acesso) e as portas *trunk* (ligações partilhadas). Uma porta de acesso (*acess port*) associa uma porta do *switch* a uma única VLAN (sem considerar um *voice* LAN).
Clique nas setas para aprender mais sobre essas conexões.
Assim, uma porta *trunk* transporta todo o tráfego de mais de uma VLAN no mesmo circuito. Temos dois tipos de porta *trunk*:

- *Trunk* ISL (*Inter-Switch Link*), com a qual o tráfego deve ser convertido em um *frame Inter-Switch Link* (ISL), caso contrário é excluído. Apesar de ser um padrão criado pela Cisco, nem todos

Se uma porta de acesso receber um *frame* e apontar com um ID de uma VLAN distinta da configurada, ela será excluída e o MAC original não aparecerá na tabela MAC. Caso contrário, o *frame* é encaminhado. Esse tipo de porta é usado para ligar computadores, impressoras, entre outros. As portas do *switch* são configuradas na VLAN 1, por padrão ou *default* (ou pelo usuário).

Já uma porta *trunk* é utilizada para interligação de *switches* aos roteadores, e permite o tráfego de várias VLANs. Configurando uma porta como *trunk*, todo o tráfego de todas as VLANs criadas no *switch* pode passar por ela, a não ser que o administrador da rede restrinja o número de VLANs (CISCO, 2010).

os switches Cisco suportam ISL;

- *Trunk* 802.1Q, que aceita tráfego com e sem *tag*. Caso um *frame* aceite a *tag* encaminha-se para a VLAN. Caso contrário, ele será encaminhado para a VLAN padrão.

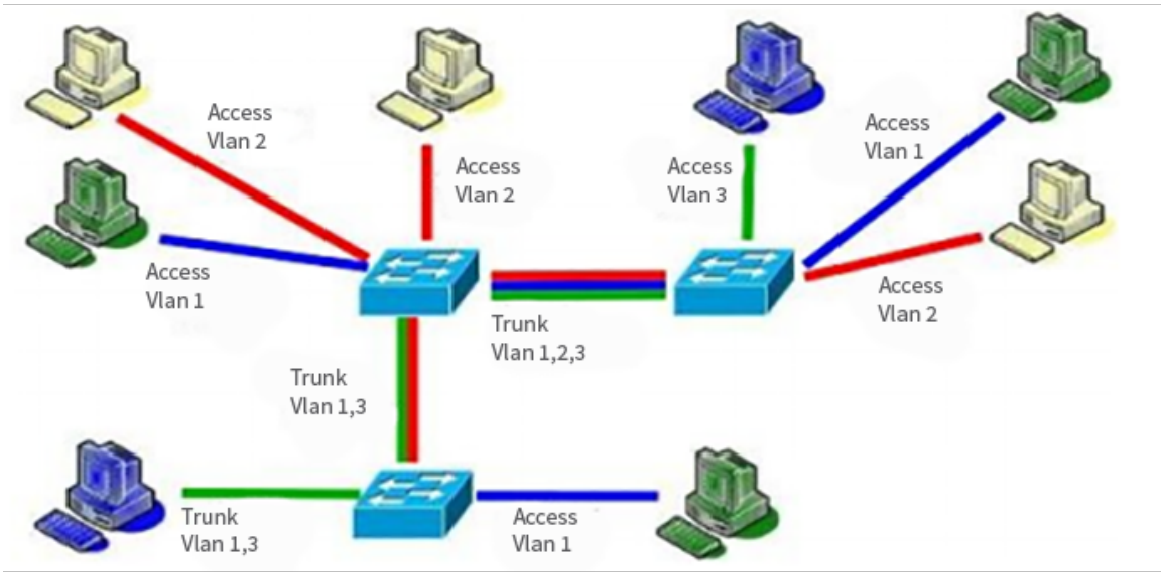


Figura 2 - Disposição dos enlaces Trunking e Access.
Fonte: HAFFERMANN, 2009, p. 10.

A figura apresenta a ligação entre os dois *switches* (chamaremos o esquerdo de A, e o direito de B), pelas portas *trunk* no mesmo *link*, devido à necessidade de passar o tráfego da VLAN 100 e 200.

VOCÊ SABIA?

A Cisco criou a plataforma *Networking Academy Program*, que é um programa baseado no uso de ferramentas *e-learning*, para ofertar aos seus clientes (estudantes) conhecimentos e habilidades em tecnologia Internet. A plataforma oferece serviços como laboratórios práticos, minicursos com provas para verificar o seu conhecimento, instruções para certificação, entre outros. Trata-se de um programa que já está presente em vários países e conta com milhares de profissionais qualificados, de acordo com a empresa. Segundo a Cisco (2019), "além da qualificação, o programa tem por objetivo prover ao aluno um certificado de qualidade, com reconhecimento internacional". Para ter informações detalhadas sobre a plataforma, acesse: <https://www.cisco.com/c/dam/global/pt_br/assets/docs/Datasheet_CCNP.pdf> (https://www.cisco.com/c/dam/global/pt_br/assets/docs/Datasheet_CCNP.pdf>).

Você quer conhecer melhor as vantagens das LANs Virtuais? Na próxima seção veremos as diversas vantagens de sua utilização.

2.1.4 Vantagens das VLANs

As VLANs possuem diversas vantagens, entre as quais podemos destacar as seguintes:

- a melhoria de desempenho, pois, diminui o *broadcast* da rede;
- é ágil para conexão e movimentação nas estações em distintas redes físicas;
- insubmissão da topologia física, pois cria topologias virtuais, assegurando que a topologia física não seja modificada;
- segmentação lógica da rede, em que as VLANs permitem a junção das estações, como, por exemplo, os computadores de um determinado departamento de uma empresa ficam juntos, compartilhando de um mesmo meio;
- redução de custo e facilidade de gerenciamento, pois sabe-se

que a maior parte dos custos de uma empresa com a rede são de alterações, deslocamentos, compra de novos equipamentos. Desse modo, se antes, quando um usuário era modificado fisicamente em uma LAN, era preciso modificações de cabeamento, endereçamento e reconfigurações, mas isso não ocorre com as VLANs, que oferece soluções mais simples;

- segurança, pois distintas partes da rede têm os tráfegos separados, impedindo que os dados fiquem expostos na rede durante sua transmissão. Podemos citar também o exemplo de usabilidade, quando um determinado setor de uma empresa não pode ter a informação visível a todos, permitindo o acesso apenas para pessoas autorizadas. Na seção 1.1.6, estudaremos mais sobre segurança, considerado um dos aspectos mais importantes para as redes.

2.1.5 Configurar Portas VLANs no Switch Cisco

As VLANs possuem três formas distintas de configurações para a conexão dos dispositivos: manual; automática e semiautomática. Cada uma delas possui características diferentes, sendo:

- manual ou estática: nesse processo as configurações iniciais e todas as alterações subsequentes são de responsabilidade do administrador da rede. Essa rede, após implantada, fica dependente de um responsável para a sua manutenção, devido sua complexidade. Diferente das VLANs que não dependem de reconfigurações constantes;
- automática ou dinâmica: os dispositivos são conectados e/ou desconectados automaticamente das redes, seguindo as configurações do administrador para essas restrições. Esse tipo de configuração é feito através de critérios estabelecidos pelo administrador, sendo utilizado em qualquer tamanho de rede, principalmente nas grandes redes, pela facilidade de administração;
- semiautomática ou semiestática: é uma mescla das duas configurações anteriores que, por ser condicionada de forma

semiautomática, permite que as configurações iniciais sejam definidas manualmente, enquanto as configurações posteriores podem ser realizadas dinamicamente, ou, ainda, pode-se iniciar as configurações de forma automática e, posteriormente, realizá-la de forma manual.

2.1.6 Roteamento entre VLANs

As VLANs são indicadas para a segmentação de redes. Porém, em muitos casos elas têm a necessidade de se comunicar e, para isso, utiliza-se o roteamento. O roteamento poderá ser feito de três formas diferentes, sendo elas:

- roteamento através de múltiplos enlaces: um enlace de cada VLAN conecta-se às portas do roteador. Serve para redes de pequeno porte. Esse tipo de roteamento é usado no padrão IEEE 802.1Q, em suporte a *frames* e quando os *links* são configurados no modo enlace. Ele é inviável para estruturas maiores, pois elas necessitam de roteadores de maior capacidade de processamento e de número de portas para a interconexão das VLANs;
- roteamento através de enlace único com Trunking: a tecnologia de Trunk é usada para unir, de forma completa ou parcial, todas as VLANs em uma mesma conexão física do *switch* ao roteador. Esse tipo de roteamento precisa ter suporte a VLANs, ou seja, precisa ser configurado no modo Trunk. Nesse roteamento são produzidas interfaces virtuais com as configurações de rede para cada VLAN. Quando a comunicação for de VLAN distintas, os *frames* passam pelo enlace até o roteador e retorna no mesmo caminho, porém já pertencente a VLAN de destino. É uma solução mais simples, segura e rápida, além de ser de menor custo, pois não há a necessidade de novos computadores e nem equipamentos de rede, não sendo necessário modificar a estrutura física de rede;
- roteamento por comutador com processador de rotas

> interno: caracteriza-se pelo uso de comutadores da terceira camada OSI (Transporte), que são os *switches* de camada três. A principal vantagem é a de unir todas as funções de comutação e roteamento em um único aparelho, ganhando no quesito espaço físico, além de velocidade de transmissão dos dados pelo fato de utilizar um único aparelho, uma vantagem é, por exemplo, a velocidade de um enlace em par trançado. Podem ser criadas interfaces de rede virtuais, chamadas de Switch Virtual Interface (SVI's) que são associadas a cada VLAN da rede, e encaminham os *frames* para a interconexão entre as diferentes VLANs. Essa seria a sua vantagem, o que a faz ser considerada a melhor das três opções. A desvantagem principal seria o custo desse tipo de equipamento de comutação de camada três, sendo indicada apenas para estruturas grandes. (KUROSE; ROSS, 2014, p. 358).

Como se pode perceber, pela explicação detalhada sobre os três diferentes modos de roteamento, será preciso avaliar as vantagens e desvantagens de cada um deles, para que se possa decidir qual é a melhor opção para cada caso.

2.1.7 Segurança

A segurança é sem dúvida uma das vantagens da VLAN para segmentação de redes, pois ela separa de forma lógica o tráfego de uma rede virtual composta por servidores, por exemplo, da rede virtual dos usuários. A utilização de soluções paralelas pode reforçar ainda mais a segurança de uma rede composta por VLANs.

> Um aspecto necessário e muito sensível quando se trata de VLANs é o roteamento de tráfego entre as diferentes redes virtuais. Em qualquer implementação de VLAN faz-se necessário interligar as redes com roteadores, e é desejável que haja garantias de que nenhuma delas seja acessada por membros de outras VLANs, exceto quando necessário e autorizado. O uso de roteadores com o auxílio de ferramentas de filtragem de pacotes (*firewall*) são muito eficientes na função de alcançar este nível de segurança. O método de roteamento com *Switch* de camada 3 é o mais vantajoso em termos de segurança, ainda mais se este dispuser de firewall interno reunindo assim, em um só aparelho, as funções de comutação, roteamento e filtragem de pacotes tornando-o muito mais rápido se comparado ao uso conjunto de um roteador com um switch comum (camada 2). No entanto o custo de aquisição deste tipo de *switch* ainda é muito elevado e nem todas organizações têm condições de

> equipar suas redes com esta solução (HAFFERMANN, 2009, p. 18).

Nesse caso, utiliza-se o método de roteamento de enlace único com Trunking, em que um comutador e suporte da VLAN conecta as redes virtuais a um roteador através de um enlace com Trunk.

Também devemos observar qual é o tipo de configuração das VLANs pois, se ela for feita de forma manual, existe o risco de conexão em uma rede virtual que não seja a correta, por erro do administrador da rede. Isso pode comprometer a restrição ao uso das informações de uma empresa, por exemplo.

Alguns autores indicam outros métodos, tal como o automático ou semiautomático.

> Um método mais adequado de configuração de VLANs seria o automático ou semiautomático. Tanto no modo automático, como no semiautomático, a inserção de um dispositivo é toda baseada em regras previamente configuradas, sendo que no modo semiautomático parte desta configuração inicial ou posterior pode ser feita manualmente, e onde quer que o equipamento seja conectado, este sempre pertencerá a mesma VLAN, a menos que haja alguma alteração nas regras ou configurações pelo administrador da rede. Assim não há riscos de segurança por mudanças inadvertidas de cabeamento ou dispositivos como no método de configuração manual. Estes modos, no entanto, exigem um maior conhecimento dos administradores de rede para realizar todas as configurações necessárias de modo a não permitir a entrada de dispositivos não conhecidos em uma VLAN restrita. (HAFFERMANN, 2009, p. 19).

Desse modo, salientamos que os demais métodos, apresentados até aqui, são indicados apenas em redes pequenas, pois não exige muito tempo e planejamento para configurar e implantar.

VOCÊ QUER VER?

Uma ótima indicação de filme com o tema de segurança é o filme "A senha: Swordfish" (2001), dirigido por Dominic Sena. Nele é apresentado o complexo submundo do chamado ciberespaço, com ênfase para aspectos dos sistemas de segurança mais avançados, como os *firewalls* e senhas. O foco do filme é mostrar os segredos ocultos da rede, sobretudo informações pessoais, como segredos e informações financeiras. O protagonista é um perigoso espião, contratado pela CIA, que vê nele a melhor opção para convencer um *hacker*, que saiu recentemente da prisão, a ajudar no roubo de seis bilhões de dólares. Vale muito a pena ver esse filme para entender mais sobre segurança. Recomendamos! Para ver o filme completo, acesse: <https://www.youtube.com/watch?v=563cAQEPc84 (https://www.youtube.com/watch?v=563cAQEPc84)>.

Na próxima seção, iremos entender o que é um simulador de rede, qual deles é melhor para utilizar, além de configurar VLANs por este simulador.

2.2 Prática de configuração de VLANs em simulador

O que são simuladores de redes? De forma simples, pode-se dizer que são *softwares* ou ferramentas que simulam equipamentos de redes reais de diversos fabricantes. O mais conhecido é o Packet Tracer da Cisco, que detalharemos na próxima seção.
Este *software* (ou programa) é gratuito e muito utilizado no mundo acadêmico, pois permite simular diversos equipamentos.
Clique nas setas abaixo e conheça mais sobre a prática.

Mas, qual a importância dos simuladores de redes no mundo acadêmico? Atualmente temos diversos equipamentos de redes de vários segmentos e utilidades, porém, fica inviável estudá-los, pelo alto custo e por não serem tão fáceis de encontrar. Então, utilizamos simuladores de redes, pois facilita o aprendizado nas faculdades, escolas técnicas e centros de formação e treinamentos de cursos específicos na área de redes. Para você, aluno, que está cursando essa disciplina, esse simulador poderá ajudá-lo a estudar mais

sobre as redes em sua casa. Com ele você poderá simular, errar e corrigir até acertar, pois o foco é a sua aprendizagem.

Para os administradores de rede esse programa é muito importante, pois, por exemplo, pode ser utilizado para um novo projeto de redes, ou até mesmo para alterações em uma rede já criada. A sua utilização por grande parte de profissionais de redes se justifica porque ele permite os testes sem afetar a rede atual, uma vez que é apenas uma simulação, evitando, assim, qualquer problema com as configurações nos equipamentos da empresa.

Apresentamos aqui o Packet Tracer, pois é o mais recomendado, mas certamente existem outros simuladores e, por isso, não podemos afirmar qual deles é o melhor, pois cada um possui uma especificação e finalidade distintas para os diversos níveis de configuração. Por exemplo, tem simuladores proprietários que tem a finalidade de testar equipamentos de redes específicos de uma marca, ou seja, usar apenas com aquele equipamento na sua rede. Já os simuladores abertos não proprietários simulam todos os tipos de equipamentos de redes.

Os comandos do Packet Tracer podem ser copiados e salvos posteriormente em editores de textos para sua reutilização em equipamentos reais. Ou seja, pode-se testar as configurações e salvá-las, para posterior uso em equipamentos reais.

CASO

Cisco e AMD se unem para dar suporte à tecnologia AMD MxGPU: a primeira solução de GPU virtual por *hardware* do mundo! Assim, as duas empresas anunciam as atuais demandas de virtualização de gráficos corporativos, unificando a plataforma de servidor UCS Série C da Cisco (a mais famosa que existe) com as placas de vídeo AMD, que dão suporte à tecnologia MxGPU (GPU Multiusuário). Apesar de ser uma união que traz benefícios, a junção também aponta para uma preocupação em dominar o mercado e, desse modo, ao risco de monopólio desse tipo de tecnologia. Essa nova tecnologia veio para permitir o aumento da velocidade de resposta de aplicativos e *desktops* virtuais, que permite ao responsável da área de tecnologia de uma empresa, por exemplo, oferecer estações de trabalho mais potentes e gráficos reais a partir do *datacenter* a qualquer usuário na sua rede, ou seja, um ambiente projetado para ter servidores e outros componentes como equipamentos de rede tais como *switches*, roteadores, entre outros. Esse modelo visa atender os clientes da Cisco no quesito segurança, desempenho e velocidade de GPU, trazendo vantagens como, melhorar a produtividade e mobilidade dos seus usuários, segurança IP, entre outras.

Agora que vimos a utilização da configuração de VLANs em simulador, e como utilizar suas funções, veremos um pouco mais sobre o simulador Packet Tracer, aprendendo como utilizá-lo.

2.2.1 Packet Tracer

O Packet Tracer é um simulador de rede desenvolvido pela maior empresa de equipamentos para redes do mundo, conhecida por Cisco System. Ele é muito utilizado principalmente para os iniciantes que estão na área de tecnologia. Ele já possui ferramentas e equipamentos prontos para serem configurados e, com isso, com poucos cliques pode ser executado sem nenhum problema.
Para fazer o *download* do Packet Tracer, você deverá ir no site da Lab Cisco, no *link* <http://labcisco.blogspot.com/p/laboratorios.html (http://labcisco.blogspot.com/p/laboratorios.html)>, ou, se preferir, poderá fazer o *download* direto do site da Cisco NETACAD (*Cisco Network Academy*), no *link* :<https://www.netacad.com (https://www.netacad.com)>.

VOCÊ QUER LER?

A NETACAD fornece diversos cursos na área de redes. Não só isso, mas cursos nas áreas de segurança, internet das coisas, negócios e muitos mais. Para aumentar o seu conhecimento na área de tecnologia, acesse o site <https://www.netacad.com/pt-br (https://www.netacad.com/pt-br)> e clique no *menu* "cursos". Você poderá ler e conhecer sobre as diversas atividades ofertadas, escolhendo aquela que mais combina com você.

De forma geral, o Packet Tracer, ou Cisco Packet Tracer, é um *software* gratuito que tem a função de colaborar na criação de uma rede na prática (criar, configurar e simular o funcionamento de uma rede), permitindo:

- criar e simular ambientes de redes LANs e WANs;
- realizar simulações tal como roteamento entre LANs;
- criar VLANs;
- criar Redes Locais; entre outros.

É importante observar a sua limitação em relação, por exemplo em tentar criar redes utilizando tecnologia de servidores ou com outros equipamentos que não sejam comercializados pela empresa CISCO.

Para utilizá-lo de forma gratuita é necessário realizar um cadastro no site, de acordo com o seguinte passo:

- primeiro acesse o *link* direto do curso de Packet Tracer: <https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer>;
- clique em "inscreva-se hoje";
- em seguida aparecerá a página, conforme a figura:

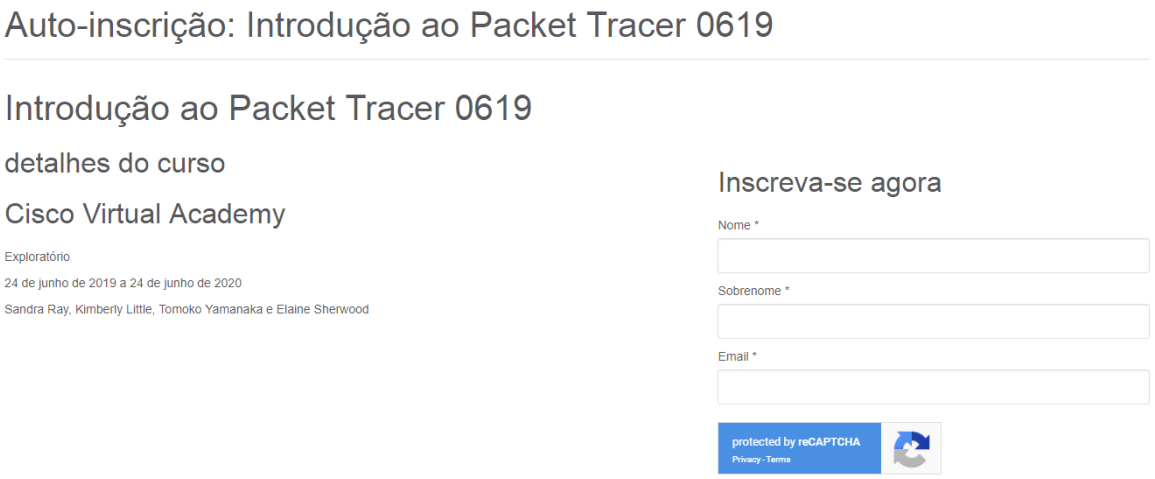


Figura 3 - Inscrição no Curso de Packet Tracer.
Fonte: NETACAD, 2019.

- após o preenchimento do cadastro inicial, você irá receber um e-mail da empresa, para ativação da conta;
- ativando a conta via e-mail, irá aparecer uma página para completar o seu cadastro. Preencha os dados e clique em "Registro". Uma observação, é no campo Empresa, caso não apareça a sua você poderá digitar que será aceito pelo site;
- com o cadastro pronto, você será redirecionado para o site da NETACAD, mas se isso não acontecer, utilize o *link*: <https://www.netacad.com/>;
- em seguida, clique em "entrar", digite o e-mail e a senha criados por você no cadastro;
- aparecerá uma nova página com uma mensagem *"We're excited to have you join us. Before you get started, we need to know a few things about you"* (Estamos felizes em ter você se juntar a nós. Antes de começar, precisamos saber algumas coisas sobre você);
- aparecerá alguns dados já preenchidos por você no cadastro anterior e novos campos para serem preenchidos, tais como: *What is your practical experience in IT or networking?* (Qual a sua experiência em prática em TI ou em rede?); *Gender* (Gênero);

Country (País); *State* (Estado); *Do you have a Disability?* (Você tem alguma deficiência?); *Birth Date* (Data de Aniversário). Todos os campos são de preenchimento obrigatório;

- Em seguida, clique em “criar conta”;
- Por fim, aparecerá a página inicial para o *download*;
- Vá para o *menu* “*Resources*” (Recursos), conforme a figura:

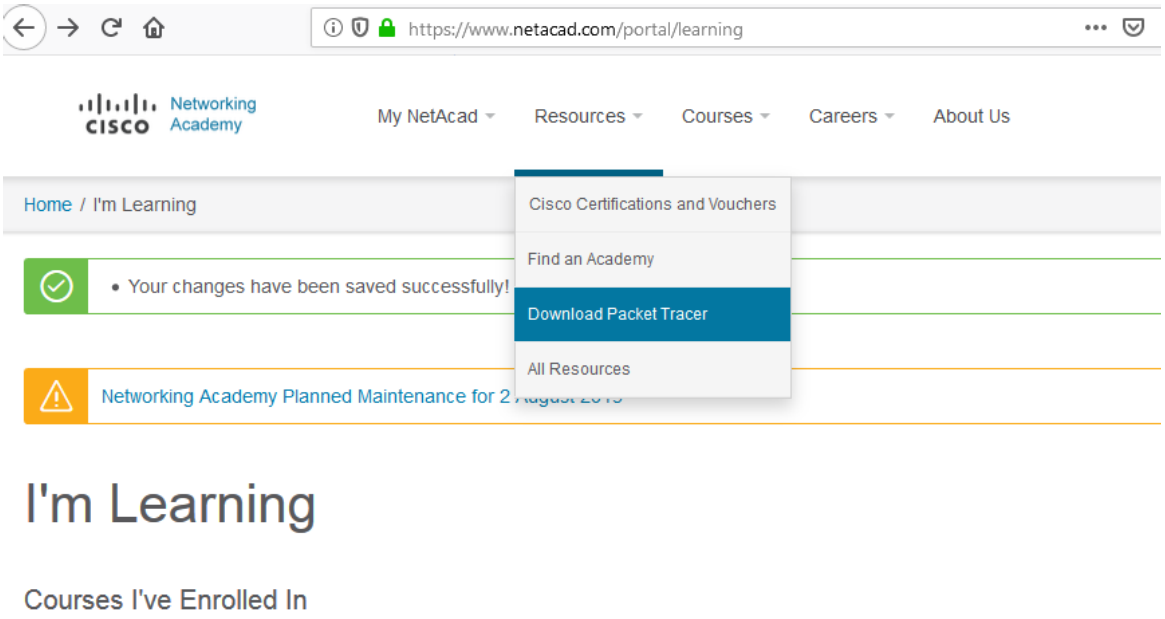


Figura 4 - Página para download do Packet Tracer.
Fonte: NETACAD, 2019.

Na página do *download,* teremos a opção de Windows Desktop, Version 7.2.1, English 64 Bit e 32 Bit; Linux Desktop, Version 7.2.1 English, 64 Bit; macOS, Version 7.2.1 English ou Mobile - iOS Version 3.0 English. Escolha conforme o Sistema Operacional do seu dispositivo (*Notebook* ou Computador Pessoal).
Após o *download,* instale o *software*. Ao abrir, basta clicar em “avançar” em todas as solicitações que ocorrerem. Bem simples!

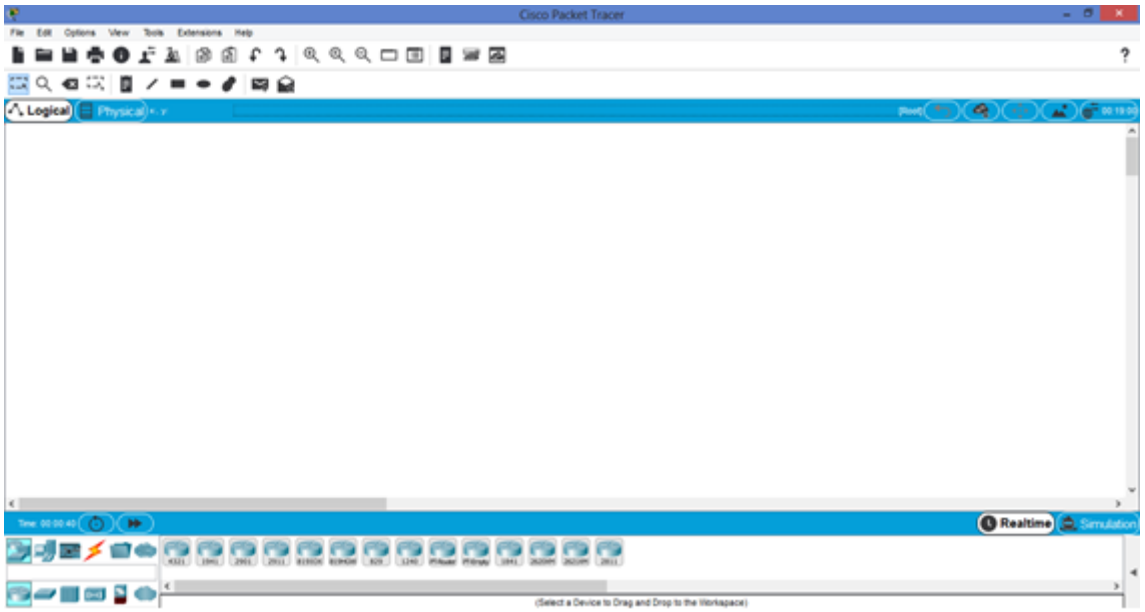


Figura 5 - Packet Tracer, tela do simulador pronto para uso.
Fonte: NETACAD, 2019.

Caso queira fazer o curso, no site acima indicado, clique em *Networking Academy Planned Maintenance*.

Você já deve ter percebido que o curso é oferecido em língua inglesa, portanto, se você tem dificuldade com esse idioma, poderá usar o google tradutor ou plugin para tradução automática das páginas, lembrando que o navegador Google Chrome já vem com esse plugin instalado.

VAMOS PRATICAR?

Sabemos agora que o Packet Tracer é um *software* ed
gratuito, que tem o objetivo de simular uma rede de comp
certo? Ele simula equipamentos e configurações pres
situações do nosso dia a dia ou das empresas. Como você
na imagem anterior, o programa apresenta uma interfac
simples. Viu também o passo a passo para se obter o *so*
forma gratuita.

Então, chegou a hora de praticar! O que você deve fazer
seguir o passo a passo das instruções anteriores, até conse
o *download* e instalar o Packet Tracer no seu comput
seguida, deverá criar uma rede simples (LAN) com a con
que desejar, utilizando as barras superiores (barras de bot
geral), barra de dispositivo, barra de ajustes e barra de te
se familiarizar melhor com a ferramenta. O objetivo dessa
é que você pratique os conhecimentos teóricos de redes
aqui. Não esqueça de compartilhar sua atividade no fórum
"Compartilhe".

Agora que você já praticou seus conhecimentos no simulador da Cisco, vamos, a seguir, utilizar o Packet Tracer para a configuração de VLANs.

2.2.2 Configuração de VLANs com Packet Tracer

Para começar, utilizaremos como base a Figura da seção 1.1.3. Vamos também definir o seguinte endereçamento: **VLAN 100**: 192.168.100.0/24 e **VLAN 200**: 192.168.200.0/24. Seguindo as instruções do manual da Cisco (2019), vamos criar as VLANs no *switch* A e depois associar a porta Fa0/2 e Fa0/3 à VLAN 100 e a Fa0/4 à VLAN 200. Vamos, ainda, atribuir o nome "Alunos" à VLAN 100 e "Docentes" à VLAN 200.
Para tal, entramos no **SwitchA** e realizamos algumas configurações.
Primeiro, insira um *switch* no Packet Tracer. Ele fica na parte inferior do *software*. Clique e arraste para o centro da tela do *software*, conforme a Figura.

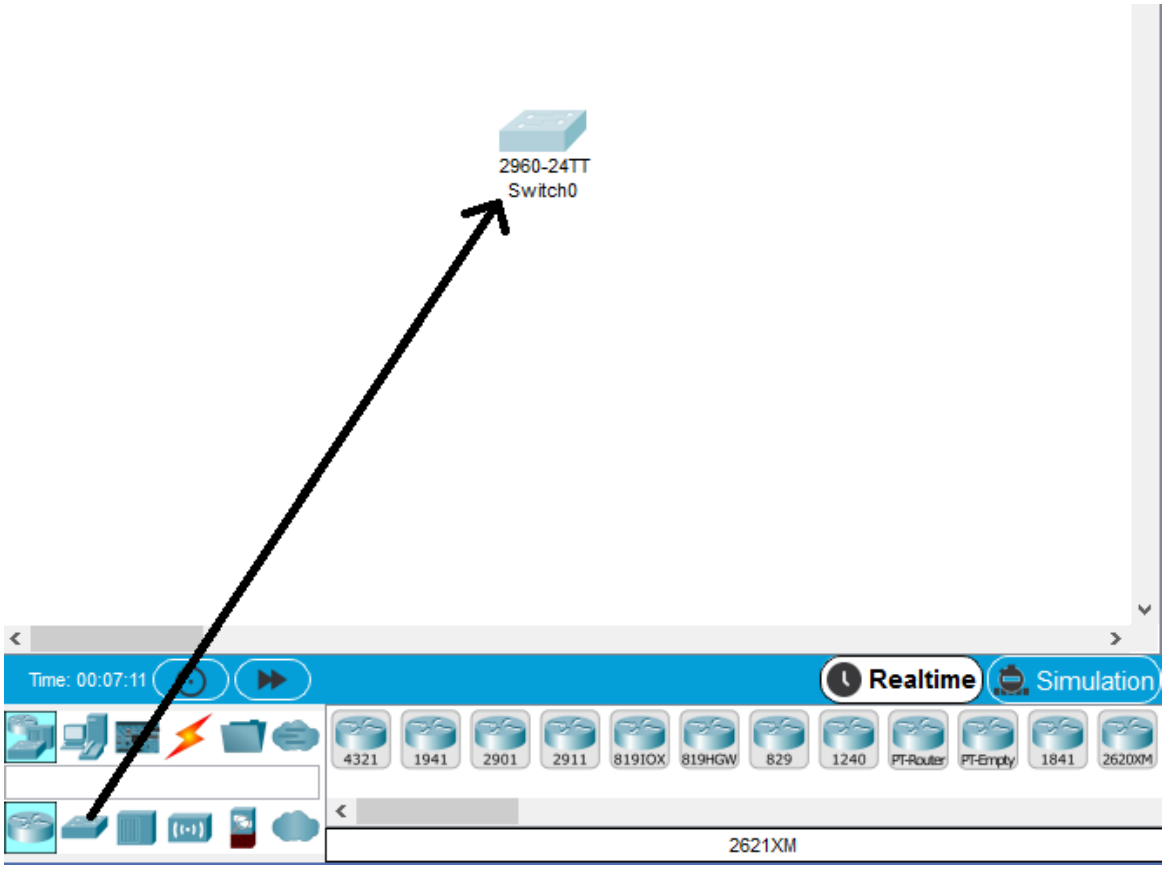


Figura 6 - Inserindo Switch no Packet Tracer.
Fonte: NETACAD, 2019.

Agora, clique duas vezes (duplo clique) na figura do *switch* que inseriu e vá na opção CLI (Tela de Comandos). No final da tela de comandos, após "*Press RETURN to get started*!" dê *ENTER*.

Para acessar o modo de comando administrador (modo privilegiado), e ter acesso a todas as configurações do *software*, digitamos o comando *enable*. Perceba que apareceu o caracter #. As instruções de comandos, apresentadas a seguir, serão digitadas também no CLI:

SwitchA**> enable**
SwitchA# configure terminal
SwitchA**(**config**)** *#vlan 100*
SwitchA**(**config-vlan**)** *#name alunos*
SwitchA**(**config-vlan**)** *#vlan 200*
SwitchA**(**config-vlan**)** *#name docentes*
SwitchA**(**config-vlan**)** *#exit*

SwitchA**(**config**)** *#interface fastEthernet 0/2*
SwitchA**(**config-if**)** *#switchport mode access*
SwitchA**(**config-if**)** *#switchport access vlan 100*

SwitchA**(**config-if**)***#interface fastEthernet 0/3*
SwitchA**(**config-if**)***#switchport mode access*
SwitchA**(**config-if**)***#switchport access vlan 100*

SwitchA**(**config-if**)***#interface fastEthernet 0/4*
SwitchA**(**config-if**)***#switchport mode access*
SwitchA**(**config-if**)***#switchport access vlan 200*
Devem realizar uma configuração semelhante para o **SwitchB**
SwitchB**> enable**
SwitchB# configure terminal
SwitchB**(**config**)***#vlan 100*
SwitchB**(**config-vlan**)***#name alunos*
SwitchB**(**config-vlan**)***#vlan 200*
SwitchB**(**config-vlan**)***#name docentes*
SwitchB**(**config-vlan**)***#exit*

SwitchB**(**config**)***#interface fastEthernet 0/2*
SwitchB**(**config-if**)***#switchport mode access*
SwitchB**(**config-if**)***#switchport access vlan 100*

SwitchB**(**config-if**)***#interface fastEthernet 0/3*
SwitchB**(**config-if**)***#switchport mode access*
SwitchB**(**config-if**)***#switchport access vlan 200*

SwitchB**(**config-if**)***#interface fastEthernet 0/4*
SwitchB**(**config-if**)***#switchport mode access*
SwitchB**(**config-if**)***#switchport access vlan 200*
Por fim, vamos configurar as portas trunk. Para tal, vamos ao **SwitchA**, e definimos a porta fastEthernet 0/1 como Trunk.
SwitchA**(**config-if**)***#interface fastEthernet 0/1*
SwitchA**(**config-if**)***#switchport mode trunk*
Devem realizar uma configuração semelhante para o **SwitchB**
SwitchB**(**config-if**)***#interface fastEthernet 0/1*
SwitchB**(**config-if**)***#switchport mode trunk*
Caso você pretenda ver as VLANS por porta, execute o comando **show vlan.**
Para os testes iremos verificar a comunicação entre as máquinas da mesma VLAN, ligadas a *switches* distintos. Para isso, vamos tentar pingar do PC0 para o PC3 (que pertencem à VLAN 100). Em seguida vamos pingar do PC2 para PC5 (que pertencem à VLAN 200). A comunicação entre PC0 e PC3, é feita conforme a figura.

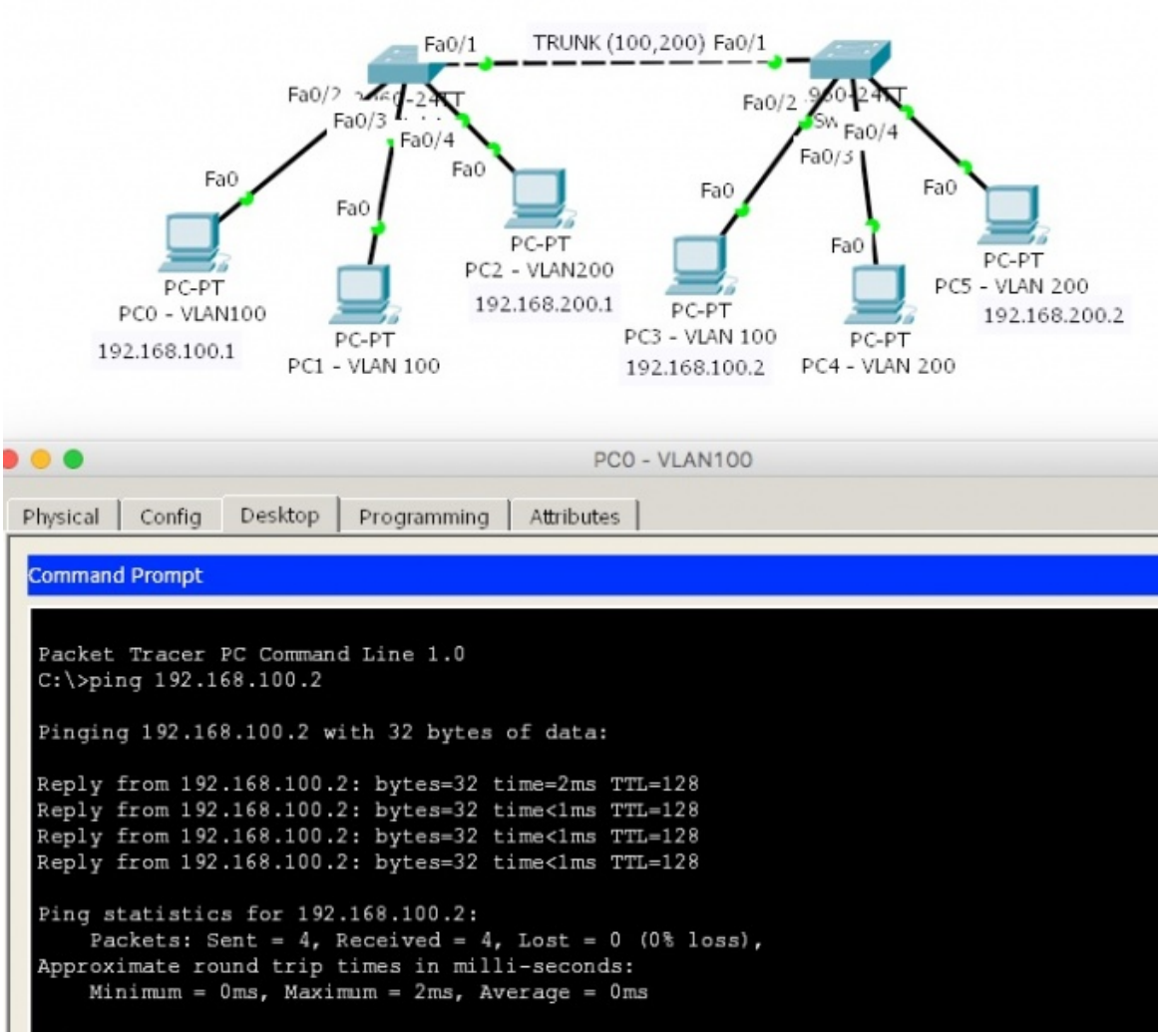


Figura 7 - Comunicação entre PC0 e PC3.
Fonte: NETACAD, 2019.

Como é possível perceber pela imagem, também é possível a comunicação entre PC2 e PC5.

Com essa simulação feita, certamente você já sabe dar os primeiros passos no uso do Packet Tracer e entender a sua relevância para o aprendizado, assim como a importância das VLANs para as redes.

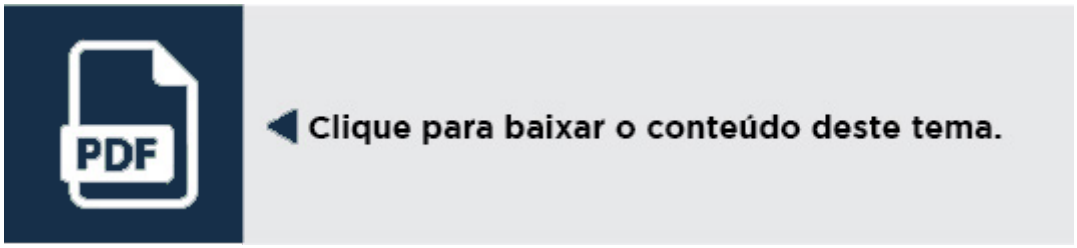
Síntese

Tivemos como principal objetivo desse estudo, aprofundar os seus conhecimentos sobre as VLANs e demonstrar a importância dos simuladores de redes. Demonstramos, ao longo da unidade, que a VLAN deve ser feita de acordo com a necessidade da empresa. Ressalta-se que algumas configurações são feitas de forma manual, e são úteis para

pequenas empresas, ao passo que as configurações automáticas são mais adequadas para as grandes empresas. Também demonstramos como utilizar um simulador aplicando a VLAN.

Nesta unidade, você teve a oportunidade de:

- a contenção dos pacotes de difusão;
- o aumento da rede e o seu melhor desempenho;
- o aumento da segurança e a redução de custos;
- a facilidade de manutenção;
- e maior facilidade de gerenciamento.



Bibliografia

A SENHA. Direção: Dominic Sena. USA. Suspense. 99 min. 2001. Disponível em: <https://www.youtube.com/watch?v=563cAQEPc84 (https://www.youtube.com/watch?v=563cAQEPc84)>. Acesso em: 31/07/2019.

CHAPELL, L. FARKAS, D. **Diagnosticando Redes Cisco**. São Paulo: Pearson Education do Brasil, 2003.

CISCO. **Sistema operacional inter-redes Cisco (Cisco IOS).** 2006. Disponível em: <https://www.cisco.com/c/pt_br/support/docs/ios-nx-os-software/ios-software-releases-110/13178-15.html (https://www.cisco.com/c/pt_br/support/docs/ios-nx-os-software/ios-software-releases-110/13178-15.html)>. Acesso em: 31/07/2019.

_____. **Programa Cisco Networking Academy.** 2019. Disponível em: <https://www.cisco.com/c/dam/global/pt_br/assets/docs/Datasheet_CCNP.pdf (https://www.cisco.com/c/dam/global/pt_br/assets/docs/Datasheet_CCNP.pdf)>. Acesso em: 31/07/2019.

_____. **Configuring Access and Trunk Interfaces**. 2010. Disponível em: <http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/AccessTrunk.pdf (http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/AccessTrunk.pdf)>. Acesso em: 31/07/2019.

HAFFERMAN, Leonardo. **Segmentação de Redes com VLAN.** 2009. Disponível em: <https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Leonardo%20Haffermann%20-%20Artigo.pdf (https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Leonardo%20Haffermann%20-%20Artigo.pdf)>. Acesso em: 31/07/2019.

KUROSE, J. F. ROSS, K. W. **Redes de Computadores e a Internet:** uma Abordagem Top-Down. 6. ed. São Paulo: Pearson. 2014.

LABCISCO. 2019. Laboratório Cisco. Disponível em: <http://labcisco.blogspot.com/p/laboratorios.html (http://labcisco.blogspot.com/p/laboratorios.html)>. Acesso em: 31/07/2019.

NASCIMENTO, M. B.; TAVARES, A. C. **Roteadores e Switch.** Guia De Certificação Para Certificação Ccna. 2. ed. São Paulo: Ciência Moderna, 2012.
NETACAD. Cisco Network Academy. 2019. Disponível em: <https://www.netacad.com (https://www.netacad.com)>. Acesso em: 31/07/2019.
TANENBAUM, A. S.; WETHERALL, D. **Redes de Computadores**. 5 ed. São Paulo: Pearson, 2011.