



Roteiro Aula Prática

**REDES DE COMUNICAÇÃO
INDUSTRIAL**

ROTEIRO DE AULA PRÁTICA 1

NOME DA DISCIPLINA: REDES DE COMUNICAÇÃO INDUSTRIAL

Unidade: U2_MODELO DE REFERENCIA OSI

Aula: A3_CAMADAS DE REDE, TRANSPORTE E SEÇÃO

OBJETIVOS

Definição dos objetivos da aula prática:

Simular e analisar o fluxo de dados através das camadas do modelo OSI em uma rede local simples.

SOLUÇÃO DIGITAL:

Cisco Packet Tracer

O Cisco Packet Tracer é uma ferramenta de simulação versátil que pode ajudar a desenvolver e refinar habilidades essenciais em um ambiente digital interativo, inclusive:

- Praticar a criação de redes simples e complexas;
- Visualizar como funciona uma rede e, em seguida, criar e proteger a sua própria;
- Aprimorar as habilidades de rack, pilha e cabeamento no laboratório virtual;
- Integrar dispositivos de IoT, código Python e automação de rede.

O download do software está disponível no link a seguir. Para que consiga realizar o download você deve estar logado na página, acessando ou criando sua conta ao clicar no botão 'Login' no canto superior direito da página.

<https://www.netacad.com/resources/lab-downloads?courseLang=pt-BR>

A própria plataforma da Cisco disponibiliza um curso introdutório de uso do software, que está disponível no link indicado a seguir:

<https://www.netacad.com/courses/getting-started-cisco-packet-tracer?courseLang=pt-BR>

PROCEDIMENTOS PRÁTICOS E APLICAÇÕES

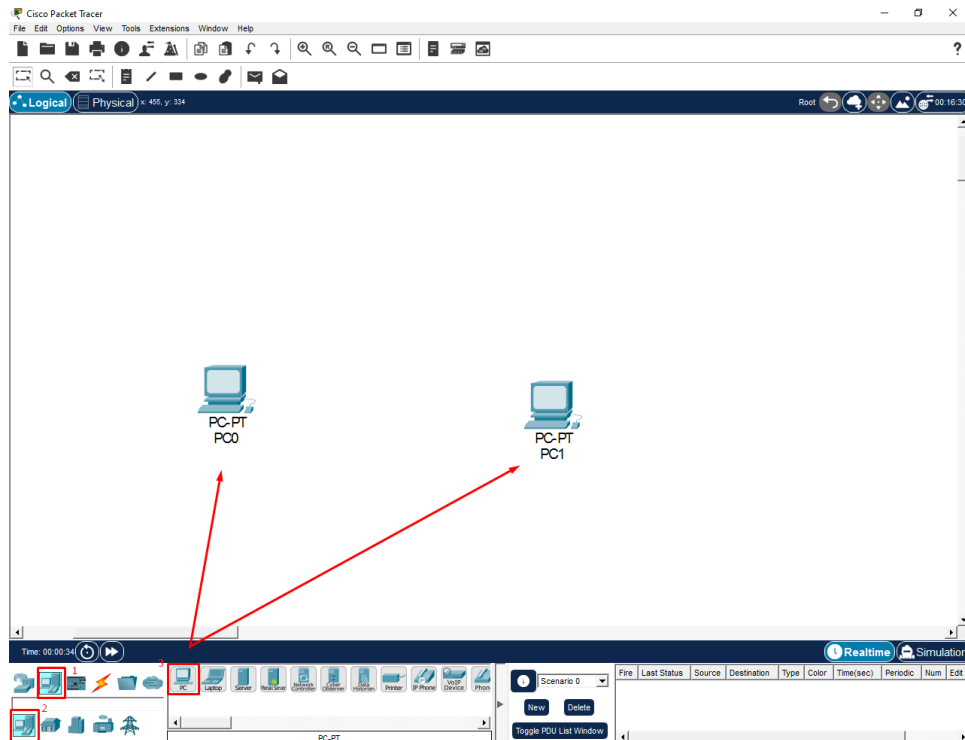
Procedimento/Atividade nº 1

Análise de Pacotes no Modelo OSI

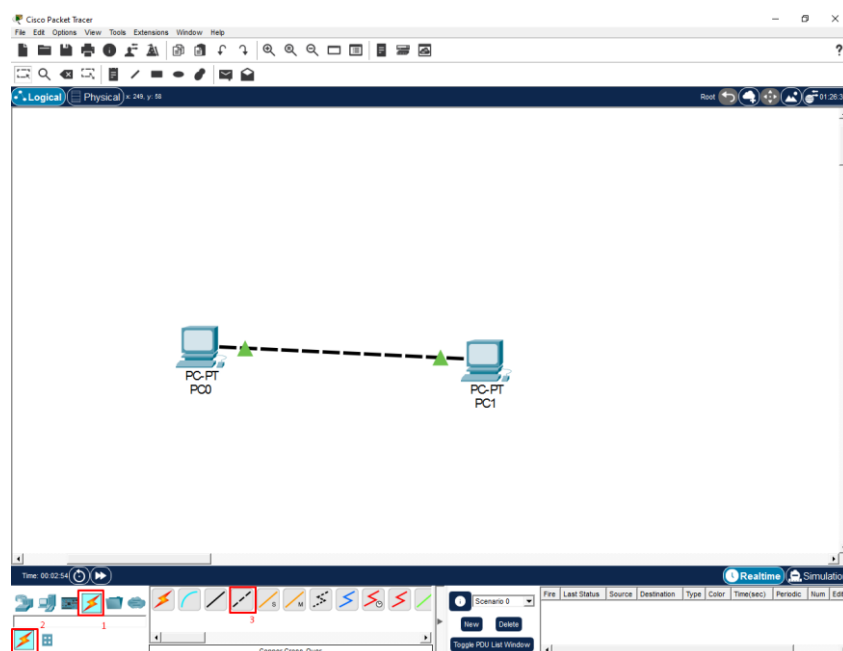
Atividade proposta: Construir uma rede local com dois computadores e observar o processo de encapsulamento de um pacote ICMP (Ping) ao viajar de um para o outro.

Procedimentos para a realização da atividade:

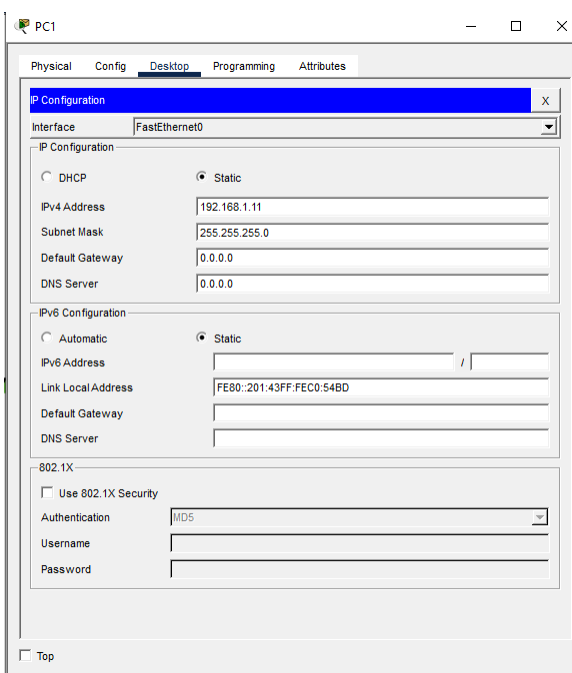
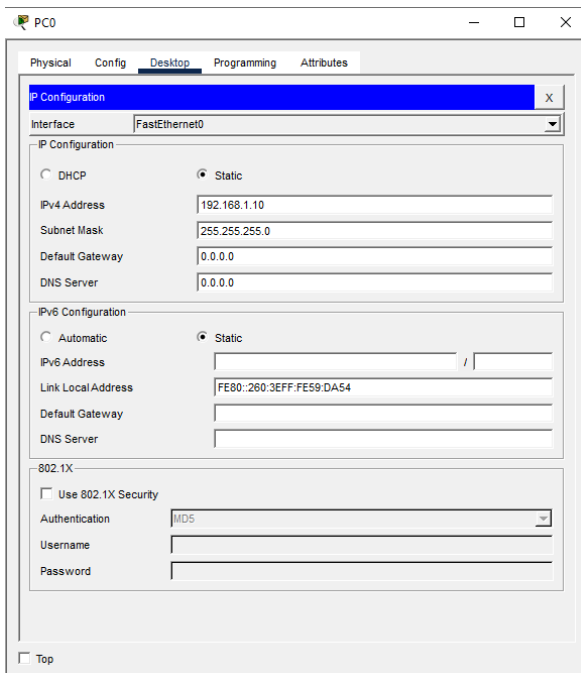
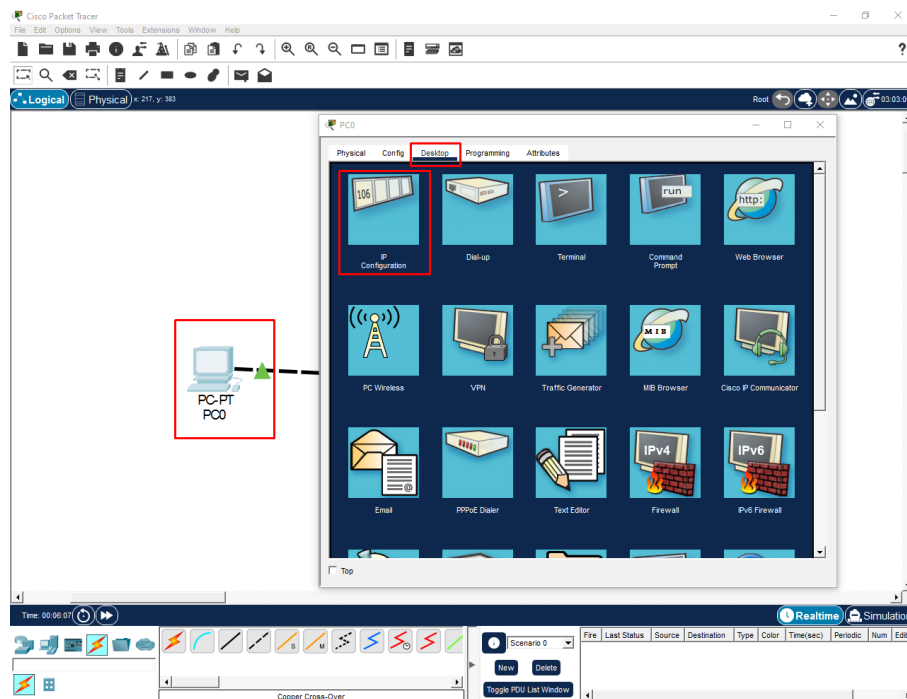
Abra o Cisco Packet Tracer. No painel de dispositivos (canto inferior esquerdo), selecione "End Devices" e arraste dois PCs (PC0 e PC1) para a área de trabalho.



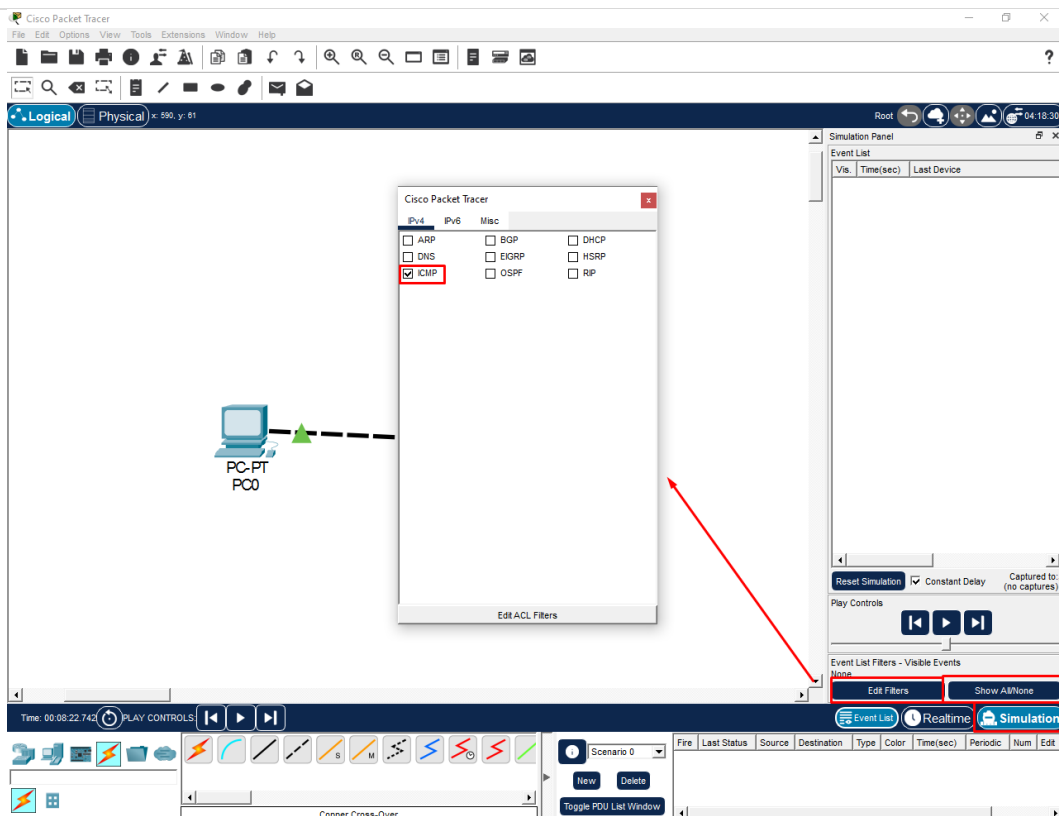
Selecione "Connections" (ícone de raio), escolha o cabo "Copper Cross-Over" (cabo cruzado) e conecte a porta FastEthernet0 do PC0 diretamente à porta FastEthernet0 do PC1.



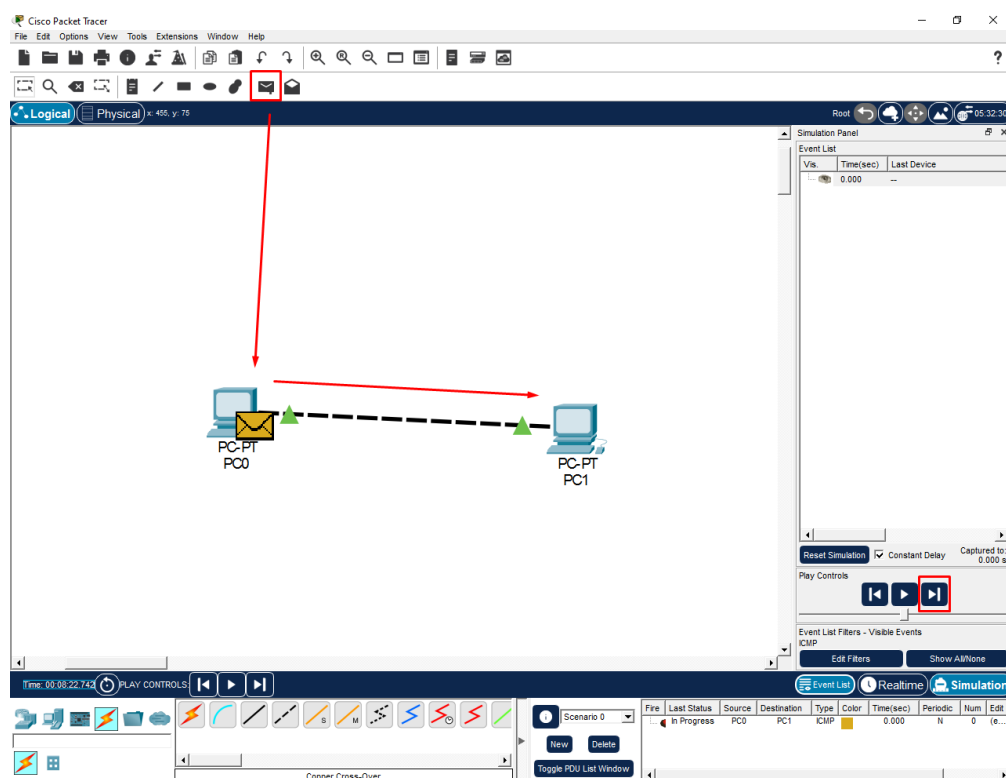
Clique no PC0, vá para a aba "Desktop" e depois em "IP Configuration". Configure o endereço IP como 192.168.1.10 e a máscara de sub-rede como 255.255.255.0. Clique no PC1, vá para a aba "Desktop" e depois em "IP Configuration". Configure o endereço IP como 192.168.1.11 e a máscara de sub-rede como 255.255.255.0.



No canto inferior direito da tela, mude do modo "Realtime" para o modo "Simulation". Clique no botão "Edit Filters". Na aba "IPv4", certifique-se de que apenas o protocolo ICMP esteja selecionado. Feche a janela de filtros.



Na barra de ferramentas direita, clique no ícone de envelope fechado ("Add Simple PDU"). Clique primeiro no PC0 (origem) e depois no PC1 (destino). Um pacote ICMP (um envelope colorido) aparecerá sobre o PC0. Clique no botão "Capture / Forward" para fazer o pacote "viajar" do PC0 para o PC1. Clique novamente em "Capture / Forward". O PC1 gerará um pacote de resposta que viajará de volta para o PC0.



Agora, clique sobre os eventos que aparecem na lista do "Simulation Panel". Uma janela chamada "PDU Information" se abrirá. Explore a aba "OSI Model". Clique em cada camada (Layer 1, Layer 2, Layer 3) e leia a descrição do processo de encapsulamento. Explore a aba "Inbound PDU Details" e "Outbound PDU Details", conforme o pacote para ver os cabeçalhos do pacote sendo construído.

Avaliando os resultados:

Tire um print da tela mostrando a topologia da rede montada (dois PCs conectados) e a simulação realizada. E outros mostrando todos os pacotes que trafegaram na rede, obtidos ao se clicar sobre os eventos no "Simulation Panel". Adicionalmente, responda as perguntas a seguir:

1. Na janela "PDU Information" do último evento que aparece na lista do "Simulation Panel", na aba "OSI Model", qual é o endereço de destino (Dest. IP) na Camada 3?
2. Ainda na mesma janela, qual é o endereço de destino (Dest. MAC) na Camada 2?
3. Com base nas informações da aba "OSI Model", descreva com suas palavras o que a Camada 3 (a camada de Rede) adiciona ao pacote.
4. Explique por que, neste caso, não foi necessário um switch para a comunicação.

Checklist:

- ✓ Baixar e instalar o Cisco Packet Tracer.
- ✓ Adicionar 2 PCs à área de trabalho.
- ✓ Conectar os PCs com um cabo Cross-Over.
- ✓ Configurar os endereços IP dos PCs.
- ✓ Mudar para o modo de simulação.
- ✓ Filtrar para exibir apenas o protocolo ICMP.
- ✓ Criar uma PDU simples do PC0 para o PC1.
- ✓ Avançar a simulação e inspecionar a PDU.
- ✓ Responder às perguntas da avaliação.

RESULTADOS

Resultados do experimento:

Ao final dessa aula prática, você deverá enviar um arquivo em word contendo as informações obtidas no experimento, os cálculos realizados, em conjunto com um texto conclusivo a respeito das informações obtidas. O arquivo não pode exceder o tamanho de 2Mb.

- **Referências bibliográficas ABNT (quando houver).**

Resultados de Aprendizagem:

Ao finalizar esta atividade, você verá na prática como a teoria do Modelo OSI realmente funciona! Você vai aprender a analisar um pacote de dados e ver exatamente como ele é construído, camada por camada, antes de ser enviado pela rede. Você será capaz de apontar onde o endereço IP e o endereço MAC são adicionados e entenderá por que cada um deles é tão importante. Esta prática vai transformar um conceito teórico em algo visual e concreto, mostrando a base de toda comunicação em rede.

ROTEIRO DE AULA PRÁTICA 2

NOME DA DISCIPLINA: REDES DE COMUNICAÇÃO INDUSTRIAL

Unidade: U2_MODELO DE REFERÊNCIA OSI

Aula: A1_APLICAÇÃO SERVIÇOS E PROTOCOLO

OBJETIVOS

Definição dos objetivos da aula prática:

Configurar um servidor para distribuir endereços IP automaticamente em uma rede local utilizando o protocolo DHCP.

SOLUÇÃO DIGITAL:

Cisco Packet Tracer

O Cisco Packet Tracer é uma ferramenta de simulação versátil que pode ajudar a desenvolver e refinar habilidades essenciais em um ambiente digital interativo, inclusive:

- Praticar a criação de redes simples e complexas;
- Visualizar como funciona uma rede e, em seguida, criar e proteger a sua própria;
- Aprimorar as habilidades de rack, pilha e cabeamento no laboratório virtual;
- Integrar dispositivos de IoT, código Python e automação de rede.

O download do software está disponível no link a seguir. Para que consiga realizar o download você deve estar logado na página, acessando ou criando sua conta ao clicar no botão 'Login' no canto superior direito da página.

<https://www.netacad.com/resources/lab-downloads?courseLang=pt-BR>

A própria plataforma da Cisco disponibiliza um curso introdutório de uso do software, que está disponível no link indicado a seguir:

<https://www.netacad.com/courses/getting-started-cisco-packet-tracer?courseLang=pt-BR>

PROCEDIMENTOS PRÁTICOS E APLICAÇÕES

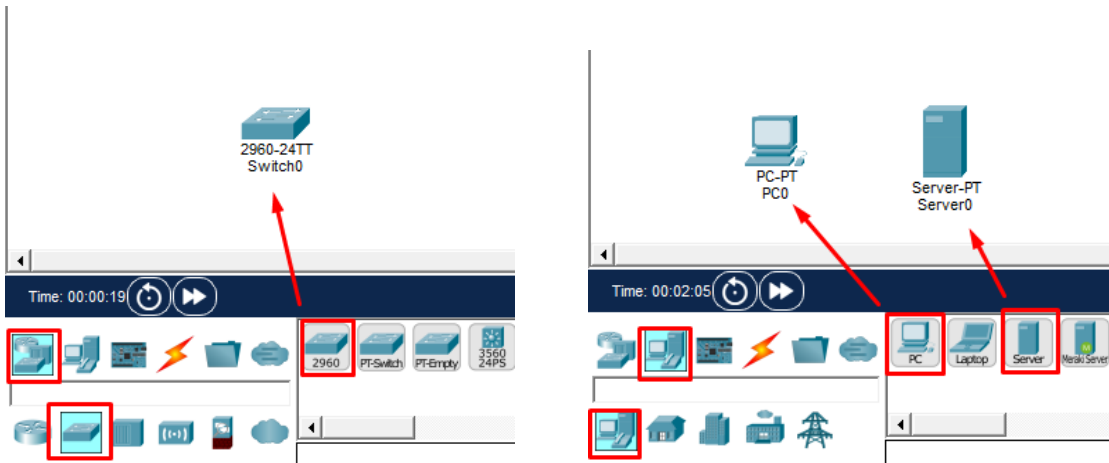
Procedimento/Atividade nº 1

Automação de Endereçamento IP com Servidor DHCP.

Atividade proposta: construir uma rede local onde um servidor centraliza e distribui automaticamente as configurações de IP (endereço, máscara, gateway e DNS) para os computadores clientes.

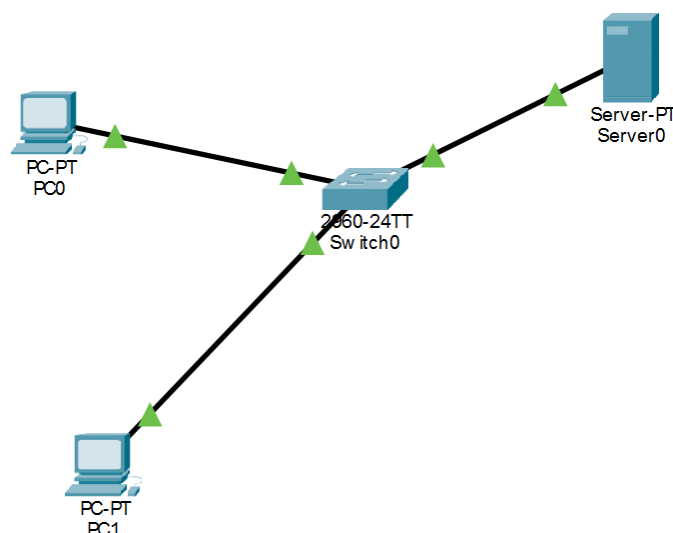
Procedimentos para a realização da atividade:

Abra o Cisco Packet Tracer. No painel de dispositivos, adicione um Server (Servidor), um Switch (modelo 2960) e dois PCs (PC0 e PC1) à área de trabalho.

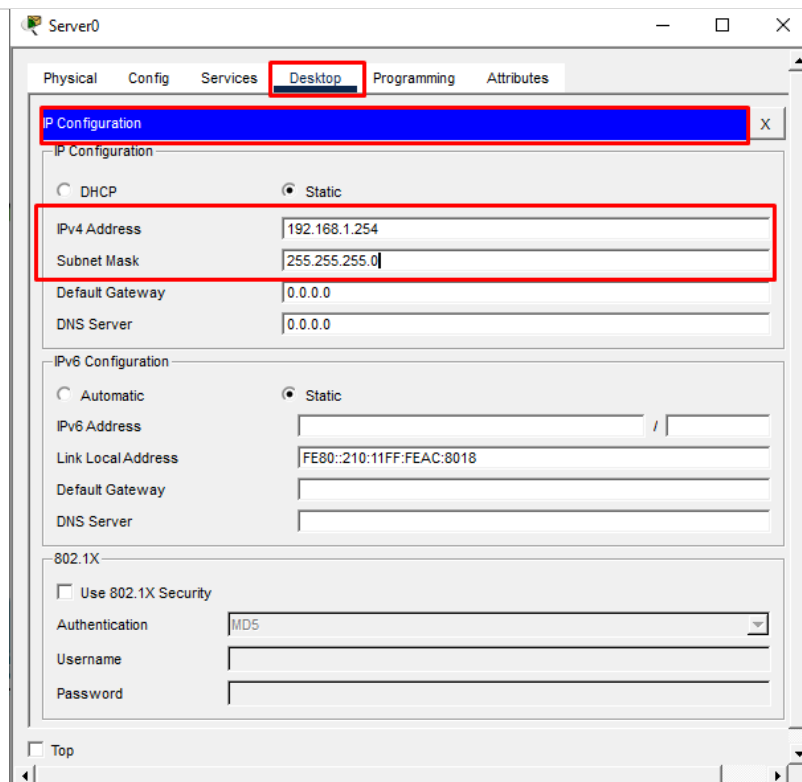


Use cabos "Copper Straight-Through" para conectar todos os dispositivos ao switch. Realize as seguintes ligações:

- Servidor -> Porta FastEthernet0/1
- PC0 -> Porta FastEthernet0/2
- PC1 -> Porta FastEthernet0/3



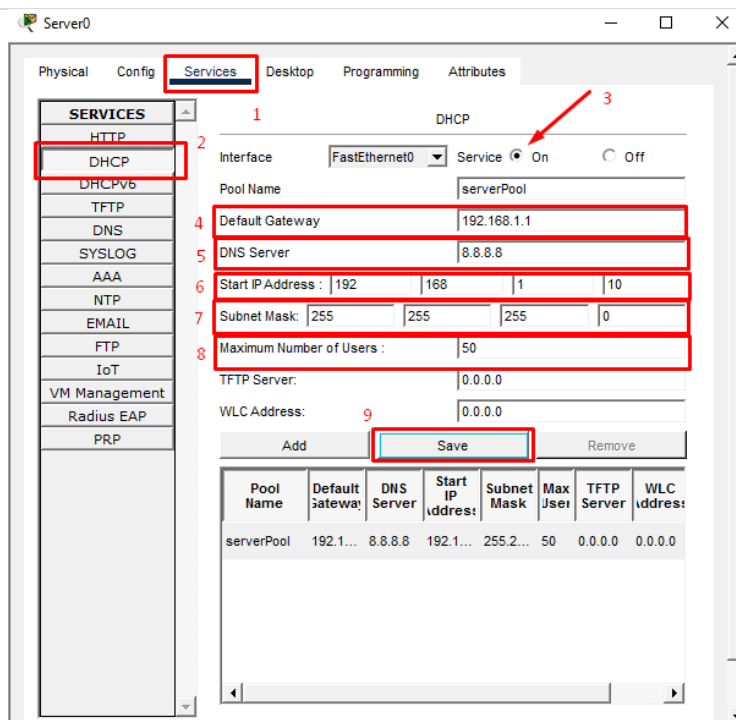
Para realizar a configuração do servidor, clique sobre ele e vá para a aba "Desktop" -> "IP Configuration". Configure um endereço IP estático para o servidor. Use: IP Address: 192.168.1.254; Subnet Mask: 255.255.255.0.



Para ativar e configurar o serviço DHCP, ainda na janela do Servidor, vá para a aba "Services". No menu à esquerda, clique em DHCP. Marque a opção "Service" como On para ligar o serviço. Preencha os campos para criar o "pool" de endereços (a faixa de IPs que será distribuída):

- Pool Name: pode deixar serverPool.
- Default Gateway: 192.168.1.1 (endereço de um roteador, que não vamos usar, mas é bom praticar).
- DNS Server: 8.8.8.8 (um DNS público, para fins de prática).
- Start IP Address: 192.168.1.10 (o primeiro IP que será distribuído).
- Subnet Mask: 255.255.255.0.
- Maximum Number of Users: 50.

Clique no botão 'Save' para salvar a configuração do pool.



Agora, é necessário realizar a configuração dos PCs para serem Clientes DHCP. Para isso, clique no PC0. Vá para a aba "Desktop" -> "IP Configuration". Marque a opção DHCP. Aguarde alguns segundos. Você verá a mensagem "DHCP request successful." e os campos de IP, Máscara, Gateway e DNS serão preenchidos automaticamente. O PC0 deve receber o IP 192.168.1.10. Repita o processo para o PC1. Clique nele, vá em "Desktop" -> "IP Configuration" e marque DHCP. Ele deverá receber o próximo endereço disponível, 192.168.1.11.

Para testar a conectividade, no PC0, abra o "Command Prompt" no "Desktop". Digite o comando `ipconfig /all`. Verifique se as informações recebidas (IP, Gateway, Servidor DHCP) estão corretas. Tente pingar o PC1 usando o endereço IP que ele recebeu: `'ping 192.168.1.11'`. O ping deve funcionar.

Avaliando os resultados:

Apresente em seu relatório as seguintes capturas de tela:

- Mostrando a configuração do serviço DHCP na aba "Services" do seu servidor.
- Tela de "IP Configuration" do PC0 e do PC1, mostrando os dados que ele recebeu automaticamente via DHCP.
- Comandos `'ipconfig /all'` e `'ping'` enviados para o teste de comunicação da rede.

Adicionalmente, responda as questões a seguir:

1. Qual endereço IP o PC1 recebeu?

2. No procedimento, por que o servidor precisa de um endereço IP estático (fixo) em vez de usar DHCP também?
3. Se você adicionasse um terceiro PC (PC2) à rede e o configurasse como cliente DHCP, qual endereço IP você esperaria que ele recebesse? Por quê?

Checklist:

- ✓ Clicar no link do experimento MEDIDAS DE MASSA E VOLUME DE LÍQUIDOS;
- ✓ Garantir a Segurança e Preparação do Experimento;
- ✓ Utilizar a pisseta e o béquer;

RESULTADOS**Resultados do experimento:**

Ao final dessa aula prática, você deverá enviar um arquivo em word contendo as informações obtidas no experimento, os cálculos realizados, em conjunto com um texto conclusivo a respeito das informações obtidas. O arquivo não pode exceder o tamanho de 2Mb.

- **Referências bibliográficas ABNT (quando houver).**

Resultados de Aprendizagem:

Nesta atividade, você vai dar um passo importante para se tornar um administrador de redes! Você aprenderá a configurar um servidor DHCP, o serviço que funciona como o "gerente de endereços" de uma rede. Você entenderá a diferença entre um IP estático (fixo, para o servidor) e um IP dinâmico (automático, para os clientes). Ao final, você será capaz de automatizar toda a configuração de rede de múltiplos computadores, uma habilidade essencial que economiza um tempo enorme e evita erros em redes de qualquer tamanho, desde um escritório até um complexo industrial.

ROTEIRO DE AULA PRÁTICA 3

NOME DA DISCIPLINA: REDES DE COMUNICAÇÃO INDUSTRIAL

Unidade: U4_REDES_INDUSTRIAIS_ETHERNET_E_INTERNET

Aula: A3_PROJETO DE REDES INDUSTRIAIS E INTERCONEXÃO DE REDE

OBJETIVOS

Definição dos objetivos da aula prática:

Projetar e simular uma rede industrial segmentada utilizando VLANs para separar o tráfego de automação do tráfego corporativo.

SOLUÇÃO DIGITAL:

Cisco Packet Tracer

O Cisco Packet Tracer é uma ferramenta de simulação versátil que pode ajudar a desenvolver e refinar habilidades essenciais em um ambiente digital interativo, inclusive:

- Praticar a criação de redes simples e complexas;
- Visualizar como funciona uma rede e, em seguida, criar e proteger a sua própria;
- Aprimorar as habilidades de rack, pilha e cabeamento no laboratório virtual;
- Integrar dispositivos de IoT, código Python e automação de rede.

O download do software está disponível no link a seguir. Para que consiga realizar o download você deve estar logado na página, acessando ou criando sua conta ao clicar no botão 'Login' no canto superior direito da página.

<https://www.netacad.com/resources/lab-downloads?courseLang=pt-BR>

A própria plataforma da Cisco disponibiliza um curso introdutório de uso do software, que está disponível no link indicado a seguir:

<https://www.netacad.com/courses/getting-started-cisco-packet-tracer?courseLang=pt-BR>

PROCEDIMENTOS PRÁTICOS E APLICAÇÕES

Procedimento/Atividade nº 1

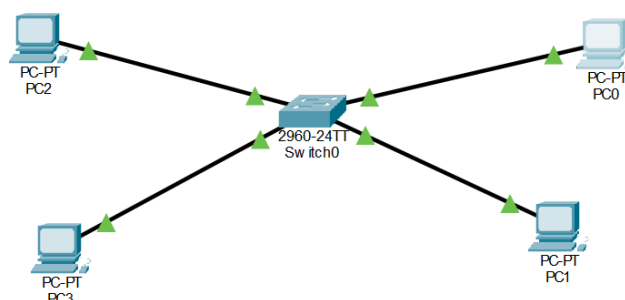
Isolamento de Redes com VLANs em um Switch

Atividade proposta: criar duas redes virtuais (VLANs) em um único switch e verificar que os dispositivos em VLANs diferentes não conseguem se comunicar diretamente.

Procedimentos para a realização da atividade:

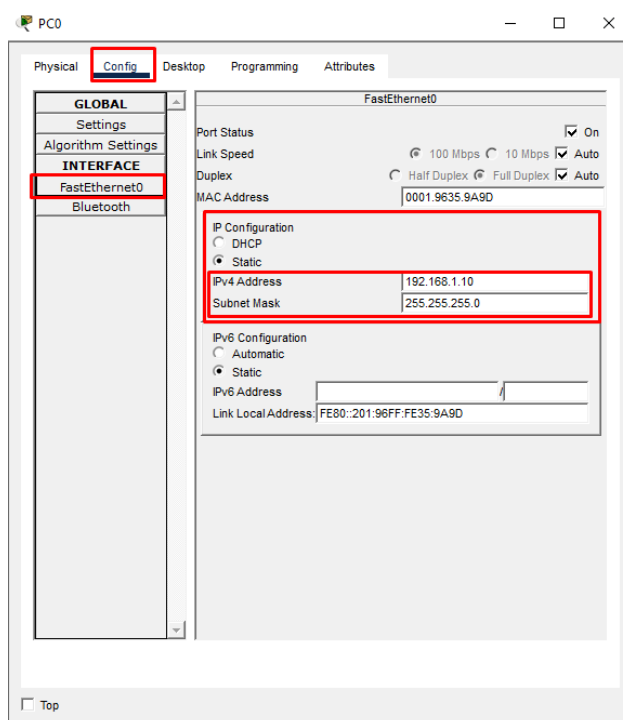
Abra o Cisco Packet Tracer. Adicione um switch (modelo 2960) e quatro PCs (PC0, PC1, PC2, PC3). Use cabos "Copper Straight-Through" para conectar os PCs ao switch:

- PC0 -> Porta FastEthernet0/1
- PC1 -> Porta FastEthernet0/2
- PC2 -> Porta FastEthernet0/11
- PC3 -> Porta FastEthernet0/12

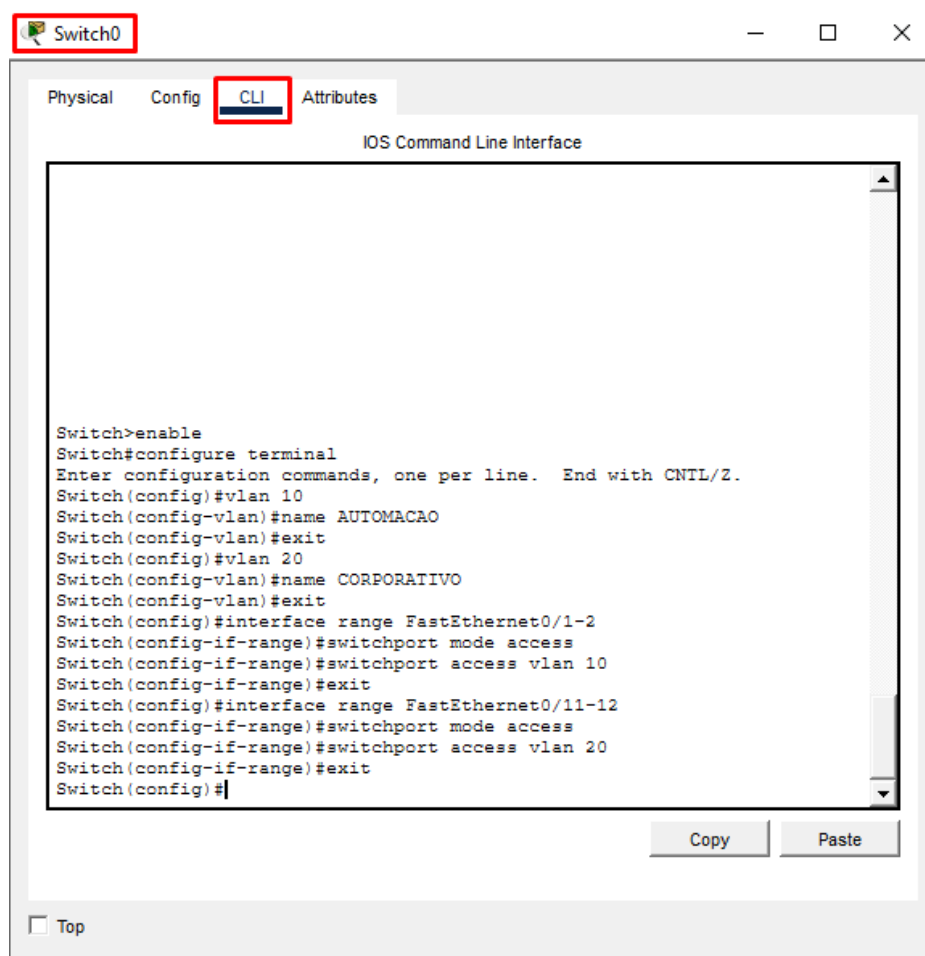


Realize a configuração dos PCs, em que todos estão na mesma sub-rede IP de propósito, para provar que a VLAN isola o tráfego mesmo assim:

- PC0: IP 192.168.1.10, Máscara 255.255.255.0.
- PC1: IP 192.168.1.11, Máscara 255.255.255.0.
- PC2: IP 192.168.1.20, Máscara 255.255.255.0.
- PC3: IP 192.168.1.21, Máscara 255.255.255.0.



Realize a configuração do Switch (VLANs). Ao clicar no switch, vá para a aba "CLI" e pressione Enter. Para entrar no modo de configuração digite 'enable', depois 'configure terminal'. Para criar a VLAN de Automação digite os seguintes comandos na sequência: 'vlan 10', 'name AUTOMACAO' e 'exit'. Crie a VLAN Corporativa: 'vlan 20', 'name CORPORATIVO' e 'exit'. Atribua as portas dos PCs de Automação (PC0, PC1) à VLAN 10 digitando os comandos: 'interface range FastEthernet0/1-2', 'switchport mode access', 'switchport access vlan 10' e 'exit'. Atribua as portas dos PCs Corporativos (PC2, PC3) à VLAN 20 com seguinte sequência de comandos: 'interface range FastEthernet0/11-12', 'switchport mode access', 'switchport access vlan 20' e 'exit'.



Para testar a conectividade, acesse o PC0, abra o "Desktop" -> "Command Prompt". Tente pingar o PC1 com o comando 'ping 192.168.1.11'. O ping deve ter sucesso, pois estão na mesma VLAN. Agora, tente pingar o PC2 com 'ping 192.168.1.20'. O ping deve falhar, pois estão em VLANs diferentes. Para confirmar, vá para o PC2 e tente pingar o PC3 ('ping 192.168.1.21'). O ping deve ter sucesso.

Avaliando os resultados:

Apresente capturas de tela da montagem e configuração realizada no simulador e dos comandos ping realizados nos PCs. Adicionalmente, responda as perguntas a seguir:

1. Qual comando você usaria na CLI do switch para verificar se as portas foram corretamente atribuídas às VLANs "AUTOMACAO" e "CORPORATIVO"?
2. O ping do PC0 para o PC1 funcionou? Por quê?
3. O ping do PC0 para o PC2 funcionou? Por quê?
4. Qual é a principal vantagem de usar esta configuração em um ambiente industrial real?

Checklist:

- ✓ Adicionar 1 switch e 4 PCs.
- ✓ Conectar os PCs ao switch.
- ✓ Configurar os endereços IP de todos os PCs.
- ✓ Acessar a CLI do switch.
- ✓ Criar as VLANs 10 e 20.
- ✓ Atribuir as portas às suas respectivas VLANs.
- ✓ Realizar os testes de ping para verificar a comunicação e o isolamento.
- ✓ Responder às perguntas da avaliação.

RESULTADOS

Resultados do experimento:

Ao final dessa aula prática, você deverá enviar um arquivo em word contendo as informações obtidas no experimento, os cálculos realizados, em conjunto com um texto conclusivo a respeito das informações obtidas. O arquivo não pode exceder o tamanho de 2Mb.

- **Referências bibliográficas ABNT (quando houver).**

Resultados de Aprendizagem:

Nesta atividade, você vai aprender uma das técnicas mais importantes para a segurança de redes industriais: a segmentação com VLANs. Você será capaz de pegar um único switch e dividi-lo em várias redes virtuais completamente isoladas, como se fossem switches diferentes. Ao final, você vai comprovar com seus próprios testes que um computador da rede "corporativa" não consegue se comunicar com um computador da rede de "automação". Dominar essa habilidade é fundamental para proteger os sistemas críticos de uma fábrica contra falhas e ataques, uma competência muito valorizada no mercado.