INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Sistemas Operacionais de Rede
Prática 16: Camada de Aplicação e Protocolo DHCP.

Olá, meus Amores!! Tudo bem??? Na aula de hoje iremos compreender o papel da Camada de Aplicação no modelo TCP/IP, conhecer os principais protocolos da camada de aplicação (HTTP, DNS, FTP, DHCP, SMTP, etc.), entender o funcionamento detalhado do protocolo DHCP e realizar uma prática de configuração e análise de pacotes DHCP. Vamos lá!!! Preparados???

Camada de Aplicação

A camada de aplicação é a camada mais alta do modelo TCP/IP. Ela é responsável por:

- Permitir que os aplicativos interajam com a rede sem precisar se preocupar com os detalhes de implementação dos protocolos subjacentes. Ele estabelece padrões universais de comunicação por aplicação, facilitando o desenvolvimento de softwares.
- Ele fornece suporte para serviços, tais como: correio eletrônico, acesso e transferência de arquivos, acesso a recursos do sistema, navegação na Web e gerenciamento de redes.
- Facilita a interoperabilidade entre diferentes tipos de aplicativos e sistemas operacionais.

Em outras palavras, a camada de aplicação é responsável por fornecer serviços da rede aos aplicativos e usuário final. Além disso, ela determina como os dados devem ser organizados para que aplicações em computadores diferentes possam entender uns aos outros. Por exemplo, um navegador web derá entender o formato HTML/HTTP, enquanto um cliente de e-mail entenderá os protocolos SMTP/IMAP/POP3.

São exemplos de protocolos da camada de aplicação:

Aplicações	Protocolos
Protocolos de Suporte	DNS, DHCP, SNMP...
E-mail	STMP, IMAP, POP, ...
Web	HTTP, HTTPS, ...
Compartilhamento de arq.	FTP, TFTP, FTPS, ...
Mensagem instantânea	MSNMS, Yahoo!
Login remoto	SSH, VNC, RDP...
Texto	Telnet, ...
Telefonia via Internet	Skype protocol, RTP, ...

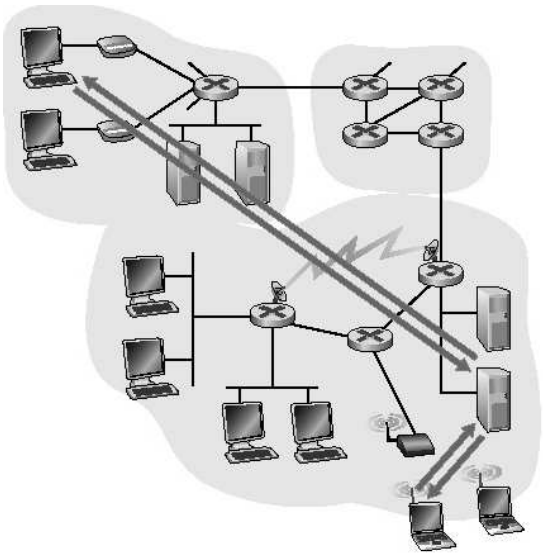
A camada de aplicação depende de portas e conexões fornecidas por TCP ou UDP para enviar e receber dados.

Arquitetura da Camada de Aplicação

O núcleo do desenvolvimento de aplicação de rede é escrever programas que rodem em sistemas finais diferentes e se comuniquem entre si. Existem atualmente duas arquitetura mais utilizadas em aplicações modernas de rede: Cliente-Servidor ou P2P.

Cliente-Servidor

Em uma arquitetura cliente-servidor há um equipamento sempre em funcionamento, denominado servidor, que atende a requisições de muitos outros equipamentos, denominados clientes. Um exemplo clássico é a aplicação Web na qual um servidor Web que está sempre em funcionamento atende a solicitações de navegadores dos clientes. Observe que, na arquitetura cliente-servidor, os clientes não se comunicam diretamente uns com os outros; por exemplo, na aplicação Web, dois navegadores não se comunicam de modo direto. Algumas das aplicações mais conhecidas que empregam a arquitetura cliente-servidor são Web, FTP, Telnet e e-mail.



Nesta arquitetura, um dispositivo central provê serviços (servidor), outro chamado de clientes enviam requisições para o servidor que utiliza portas TCP/UDP bem-definidas (0-1023). O servidor responde as requisições com as informações solicitadas pelo cliente. Os clientes normalmente utilizam portas TCP/UDP dinâmicas (49152-65535).

Nesta abordagem temos como vantagens: controle centralizado, gerenciamento facilitado e segurança mais simples de implementar. Por outro lado, temos como desvantagem: dependência de servidor que se sair do ar a aplicação não funciona, ou se estiver sem recursos suficientes pode gerar lentidão nas respostas.

Em aplicações cliente-servidor, muitas vezes acontece de um único equipamento servidor ser incapaz de atender a todas as requisições de seus clientes. Por exemplo, um site popular de redes sociais (Instagram) pode ficar logo saturado se tiver apenas um servidor para atender a todas as solicitações. Por essa razão, eles utilizam datacenters.

Um datacenter é uma infraestrutura centralizada que abriga e gerencia componentes de processamento de dados e armazenamento. Os servidores são o coração de um datacenter. Eles executam aplicativos, processam dados e fornecem serviços para usuários finais ou outros sistemas. Um datacenter pode ter centenas de milhares de servidores. Google tem de 30 a 50 datacenters distribuídos no mundo inteiro, que em conjunto tratam de busca, YouTube, Gmail e outros serviços.

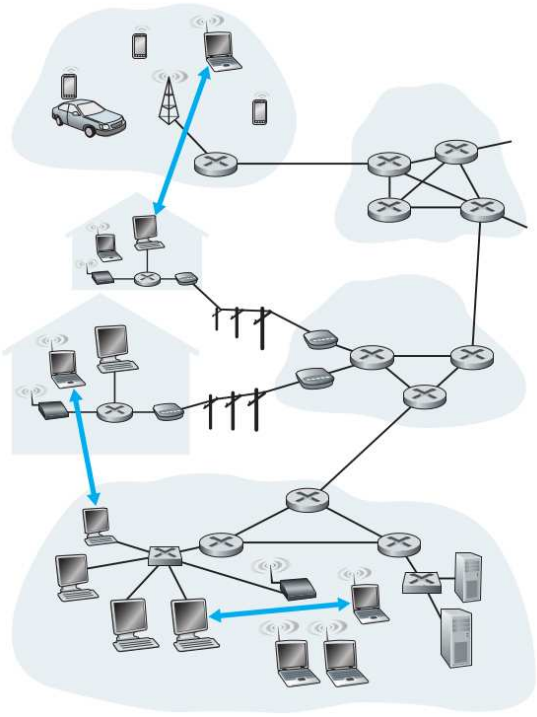
P2P

A aplicação utiliza a comunicação direta entre duplas de equipamentos conectados alternadamente, denominados pares. Como os pares se comunicam sem passar por nenhum servidor dedicado, a arquitetura é denominada par a par (peer-to-peer - P2P). Isso significa que cada peer pode solicitar dados, fornecer dados, armazenar partes das informações, compartilhar recursos e coordenar conexões com outros peers. Dessa forma, a rede P2P é naturalmente colaborativa, descentralizada e distribuída, permitindo grande escalabilidade e resiliência.

Muitas das aplicações de hoje mais populares e de intenso tráfego são baseadas nas arquiteturas P2P, incluindo compartilhamento de arquivos (por exemplo, BitTorrent), aceleração de download assistida por par (por exemplo, Xunlei), telefonia por Internet (por exemplo, Skype) e IPTV (por exemplo, KanKan e PPstream).

Quando um peer entra na rede, ele precisa descobrir outros peers. Isso pode acontecer via: lista armazenada localmente ou um servidor de entrada (modelo híbrido). Desta forma, os participantes ficam sabendo dos endereços ativos e das disponibilidade de dados.

Com esta arquitetura, um arquivo pode ser baixado em partes de vários peers ao mesmo tempo (como no BitTorrent). Isso aumenta: velocidade, disponibilidade e redundância.



Temos como vantagens da arquitetura P2P: escalabilidade, tolerância a falhas pois não depende de um único ponto, baixo custo pois não exige infraestrutura central e velocidade elevada em downloads de arquivos em paralelos.

Por outro lado, temos como desvantagens: dificuldade de controle e administração, riscos de segurança (malware e arquivos modificados podem circular) e problemas legais (pirataria).

Protocolo DHCP

O DHCP (Protocolo de Configuração Dinâmica de *Hosts*) é um protocolo da camada de aplicação responsável pela configuração automática de endereços IP e outros parâmetros de rede para hosts. Sem este protocolo, todas as máquinas precisariam ser configuradas manualmente, o que seria inviável em redes grandes.

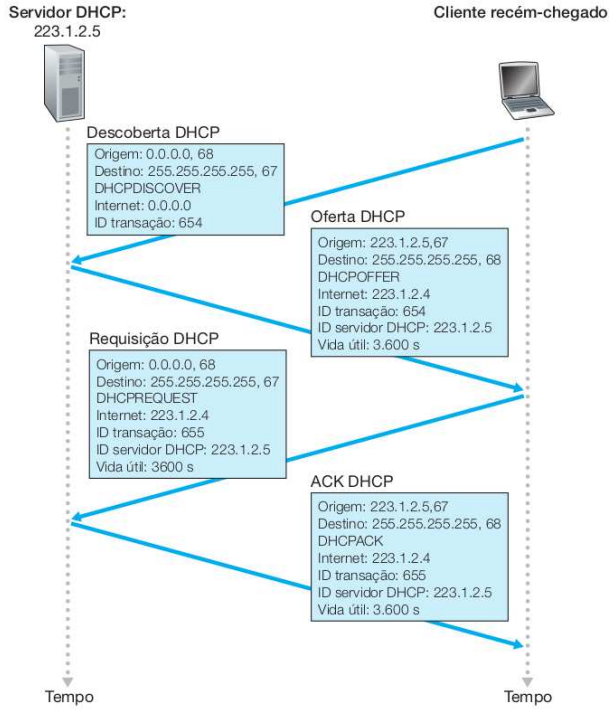
O DHCP utiliza a arquitetura cliente servidor. Cliente DHCP é o dispositivo que precisa obter informações de rede, por exemplos, computadores, celulares, notebooks, impressoras, câmeras IP etc. O servidor DHCP é o equipamento responsável por configurar automaticamente os clientes da rede com as informações da rede. O servidor pode estar em um roteador, máquina Linux/Windows ou smartphone IOS/Android.

De um modo geral, o trabalho de um servidor DHCP é fornecer informações de configuração da rede. As principais informações são:

- Endereço IP e *Netmask*;
- Servidor de Domínio (DNS);

- Endereço *Gateway* Padrão;
- Servidor de Impressão.
- Configurações complementares de rede (NTP, Voip);
- Tempo de Concessão;

Quando um dispositivo, chamado de cliente DHCP, conecta-se a uma rede configurada para usar DHCP, ele inicia um processo de comunicação para obter suas informações de rede com um processo de quatro etapas:



- Inicialmente o cliente envia uma mensagem de descoberta DHCP (dentro de um pacote UDP para a porta 67) com o endereço IP de destino de difusão 255.255.255.255 e um endereço IP de origem 0.0.0.0.
- Um servidor DHCP que recebe uma mensagem de descoberta DHCP responde ao cliente com uma mensagem de oferta DHCP, transmitida em broadcast (255.255.255.255). A mensagem de oferta do servidor contém o endereço IP proposto para o cliente, a máscara da rede e o tempo de concessão do endereço IP.
- O cliente escolherá dentre uma ou mais ofertas do servidor e responderá com uma mensagem de solicitação DHCP, repetindo os parâmetros de configuração.
- Por último, o servidor responde a mensagem de requisição DHCP com uma mensagem DHCP ACK, confirmando os parâmetros requisitados.

E agora o cliente está conectado na rede e poderá trocar mensagens.

Configurações TCP/IP no Windows

O TCP/IP é um conjunto de protocolos padrão criado para permitir as comunicações em redes empresariais e na Internet. Os elementos básicos de configuração do TCP/IP são:

- Endereço IP: é uma *string* de identificação única de 32 *bits* (no IPv4);
- Máscara de Subrede (ou simplesmente *netmask*): é um endreço de 32 *bits*. Através da máscara é possível determinar o endereço da rede, endereço dos demais equipamentos na rede e o endereço de *broadcast*.
- *Gateway*: é o endereço IP de *host* ou roteador na rede. Este equipamento vai habilitar o tráfico de informações para redes externas, tais como Internet.
- Endereço de Servidores de Nomes (DNS): representam os endereços IP do servidor que convertem os nomes dos *hosts* da rede para seus respectivos endereços IP.

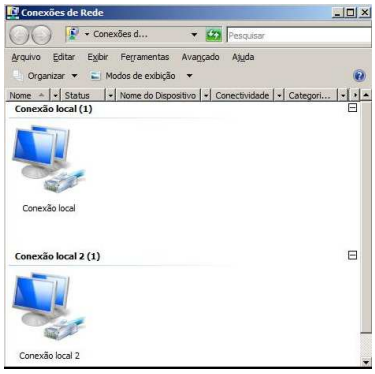
Gerenciador de Conexões

Para gerenciar as propriedades do TCP/IP o Windows possui o Gerenciador de Conexões. Ele permite que os administradores criem conexões com uma interface do usuário, usem protocolos de autenticação específicos, verifiquem a existência de programas necessários, verifiquem configurações do Registro ou executem qualquer combinação dessas tarefas.

O Gerenciador de Conexões é formado pelo Central de Rede e Compartilhamento e a pasta Conexões de Rede. O Central de Rede e Compartilhamento fornece informações de *status* em tempo real sobre a rede. Através dela é possível verificar se o computador está conectado à rede ou à Internet, o tipo de conexão, tipo de acesso a outros computadores na rede e alterar as configurações de rede.

Para abrir Central de Rede e Compartilhamento clique em “Iniciar”, “Painel de Controle”, “Rede e Internet” e “Central de Rede e Compartilhamento”.

Para abrir a pasta Conexões de Rede clique em "Alterar as configurações do adaptador" na barra lateral da Central de Rede e Compartilhamento. A pasta Conexões de Rede mostra todas as conexões de rede. Nesta interface é possível selecionar uma conexão e exibir informações de *status*, como duração da conexão, velocidade e quantidade de dados transmitidos e recebidos; e você pode usar qualquer ferramenta de diagnóstico disponível para uma determinada conexão.



Configurando uma Conexão Automaticamente

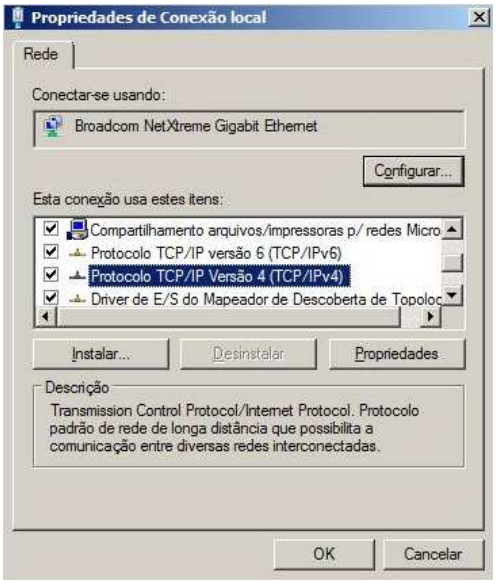
Existem duas possibilidades de configuração de um adaptador de rede. São elas: automaticamente (utilizando o protocolo DHCP) e manualmente. Para configurar os parâmetros automaticamente utilize os seguintes passos:

1. Clique em "Iniciar", "Painel de Controle" e "Central de Rede e Compartilhamento".

2. Abra a pasta Conexões de rede. Para isso, clique em "Alterar as configurações do adaptador" na barra lateral da Central de Rede e Compartilhamento.

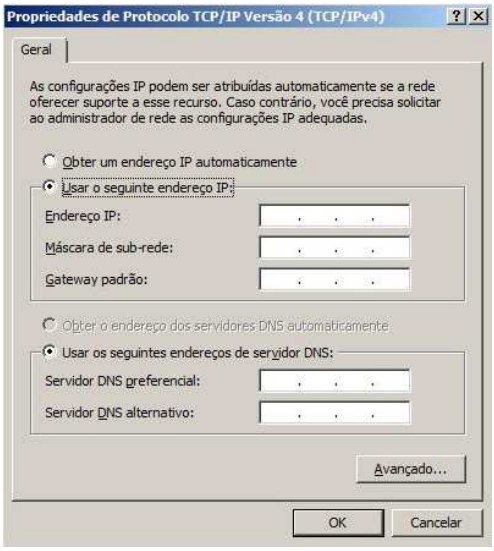
3. Clique com o botão direito do *mouse* sobre a Conexão Local, ao aparecer o menu clique em "Propriedades".

4. Na guia "Geral", em "Esta conexão usa estes itens:", clique em Protocolo TCP/IP Versão 4 (TCP/IPv4) e, em seguida, clique em "Propriedades".



5. Na janela de Propriedades de Protocolo TCP/IP, marque: Configuração automática (DHCP), "Obter um endereço IP automaticamente" e "Obter o endereço dos servidores DNS automaticamente".

6. Clique em "OK".



ipconfig

O comando `ipconfig` é uma ferramenta de linha de comando do Windows. Ele exibe todos os valores de configuração de rede TCP/IP e atualiza as configurações do protocolo de configuração dinâmica de *hosts* (DHCP) e do sistema de nomes de domínios (DNS).

Quando usado sem parâmetros, o `ipconfig` exibe endereços IPv6 ou o endereço IPv4, a máscara da sub-rede e o *gateway* padrão para todos os adaptadores.

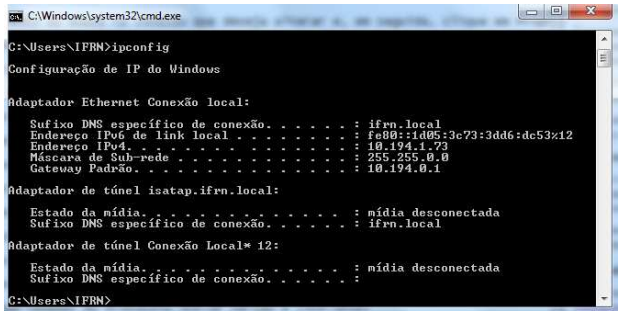
O mesmo também pode ser utilizado com os seguintes parâmetros:

***/all*:** Exibe todas as informações de configuração da interfaces de redes instaladas;

***/release*:** Libera o endereço ip do adaptador especificado;

***/renew*:** Renova o endereço ip para o adaptador especificado;

Note que as opções */Release* e */Renew* apenas podem ser utilizadas se o sistema estiver configurado com DHCP.



Exercício

Iremos realizar uma atividade com Wireshark para analisarmos as mensagens e o funcionamento do protocolo DHCP e utilizaremos o Packet Tracer para configurar um servidor DHCP.

Mensagens DHCP com o Wireshark

Para Analisarmos o protocolo DHCP, iremos capturar as mensagens DHCP trocadas como resultado da execução de alguns comandos. Forme duplas e realize as seguintes etapas são:

1. Configure a sua placa de rede para obter o endereço IP do DHCP.

2. Abra o *prompt* de comandos do windows e digite: `ipconfig /release`. Este comando libera o endereço IP atual, então o seu computador passa a ter o endereço 0.0.0.0;

3. Abra o Wireshark e começe a captura da suas interface Ethernet;

4. Agora retorne ao *prompt* de comandos e digite: `ipconfig /renew`. Este comando fará com que o seu computador solicite informações da rede, incluindo um novo endereço IP. Observe as mensagens enviadas. Uma outra forma de forçar uma renovação de endereço IP seria através da desativação e ativação da placa de rede.

5. Pare a captura do Wireshark. Para visualizar somente as mensagens DHCP utilize o filtro "**bootp**" no campo filter.

Responda as demais questões colocando as respostas num arquivo de texto, e depois anexe o mesmo no Google Sala de Aula. São elas:

6. As mensagens DHCP obtidas são enviadas por UDP ou TCP? Quais foram as portas?

7. Qual é o endereço do servidor DHCP?

8. Qual é o endereço IP que o servidor DHCP oferece?

9. Apresente as informações da rede que estão presentes na mensagem DHCP offer. Qual é o valor da máscara, gateway e servidor DNS da rede?

10. Qual foi o tempo de concessão seu endereço IP obteve em sua experiência? Pesquise qual é o objetivo deste tempo?

Configuração DHCP com o Packet Tracer

Neste exemplo vamos utilizar o protocolo DHCP no Cisco Packet Tracer. Em outras palavras, veremos como configurar um servidor DHCP com o roteador Packet Tracer. Para isso:

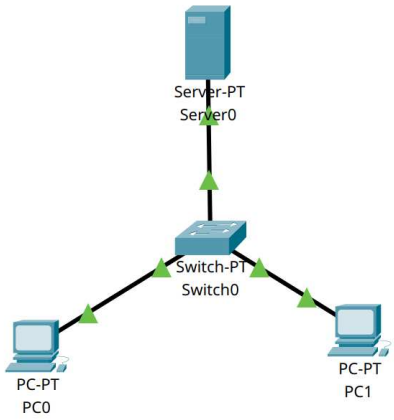
01. Inicie o simulador Packet Tracer em seu computador.

02. No menu na Barra de Dispositivos (canto inferior esquerdo), selecione os dispositivos necessários:

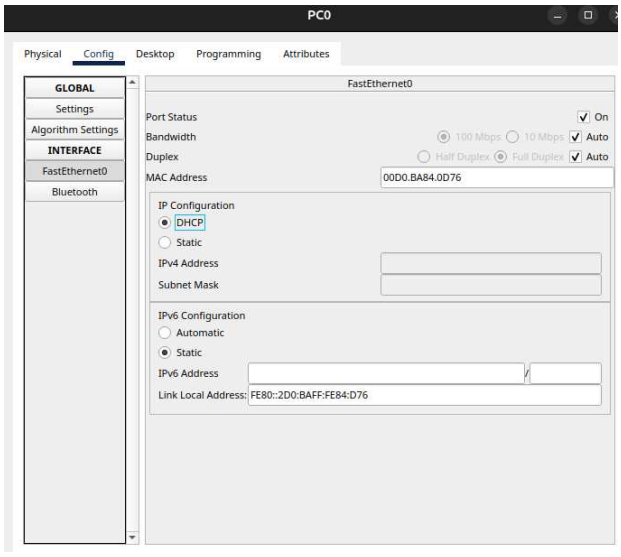
- Switch: Vá para "Network Devices"  e no subgrupos selecione "Switch". Clique em Switch-PT arraste um ele para a área de trabalho.
- Computadores: Vá para "End Devices"  e arraste 2 "PC-PT" para a área de trabalho.
- Servidor: Vá em "End Devices"  e arraste 1 "Server-PT" para a área de trabalho.

03. Agora iremos conectar estes dois PCs e o Switch através de um cabo UTP. Para isso, clique no símbolo de um raio avermelhado  e depois novamente no raio avermelhado  , desta forma será selecionado o cabo automaticamente.

Os equipamentos interligados ficará da seguinte forma:

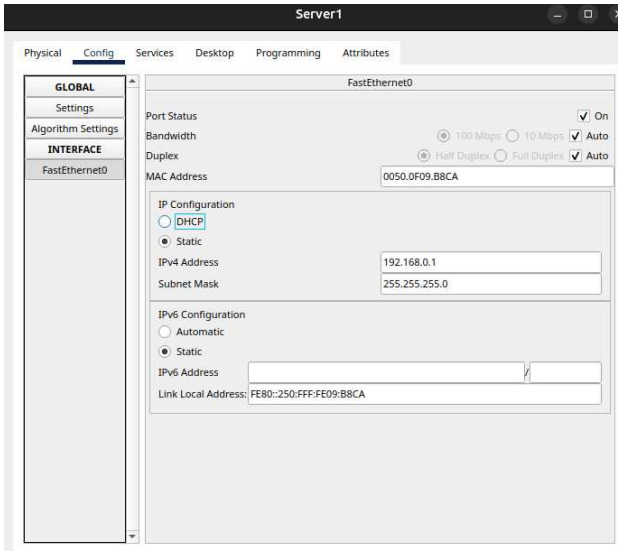


04. Agora vamos configurar a rede nas máquinas. Clique duas vezes em cada PC para abrir a janela de configuração. Vá para a aba "Desktop" e selecione "IP Configuration" e selecione a opção "DHCP".

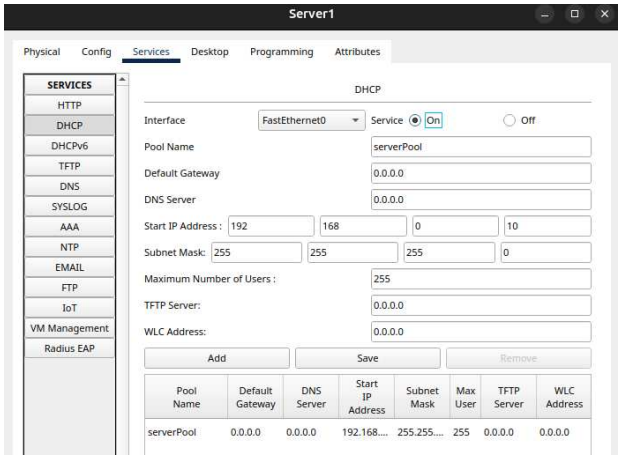


05. No servidor, clique duas vezes para abrir a janela de configuração. Vá para a aba "Config", "Interface" e "FastEthernet". Em IP Configuration selecione "Static" e insira em:

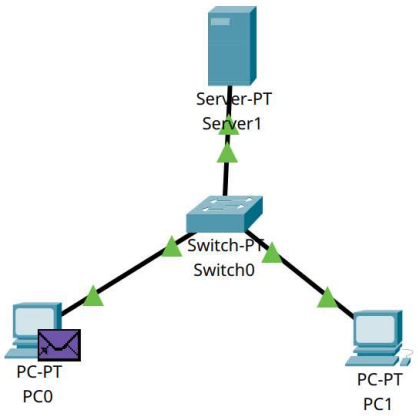
- IPv4 Address: 192.168.0.1;
- Subnet Mask: 255.255.255.0.



06. Ainda no servidor, na aba, "Services", "DHCP", "Service" selecione "On". Em "Start IP Address" coloque 192.168.0.10 e clique em "Save".



Espere uns 30 segundos para os computadores conseguirem obter as informações do servidor DHCP e se configurar. Depois realize o teste de conectividade com o "Add Simple PDU"  no canto superior da tela.



Exercício

11. Em dupla realize as configurações do servidor DHCP e das máquinas clientes. Depois encaminhe pacotes de PC1 para PC2 e verifique que há conectividade entre os equipamentos. Grave um vídeo (da tela do computador ou celular) com o respectivo testes. Depois, anexe um arquivo com os resultados dos exercícios anteriores e o vídeo no Google Sala de Aula e informe os componentes do grupo nos comentários da postagem.