Pontifícia Universidade Católica de Minas Gerais
Instituto de Ciências Exatas e Informática
Departamento de Ciência da Computação
Autor: Marco Antonio da Silva Barbosa
Colaborador: Lucas Porto Lopes

LABORATÓRIO DE REDES E SISTEMAS OPERACIONAIS

Objetivos: Conhecer simuladores de rede e verificar o funcionamento do simulador de redes Cisco Packet Tracer.

Switches de Rede

Os switches são equipamentos com a responsabilidade de tratar os frames que trafegam na rede, ou seja, atuam no mínimo até a camada 2 (camada de enlace de dados, onde o equipamento já é capaz de identificar início e fim dos quadros, controlar erros, e identificar origem e destino de Mac Address), sendo que muitos já atingem a camada 3 ou superiores. Desta forma permitindo que topologias estrelas sejam adotadas onde antes havia topologia em barramento com o cabo coaxial ou com hubs.

Seu principal objetivo é permitir a comutação entre as estações de trabalho e os servidores em uma rede local, mas com tecnologias como Metro-Ethernet já existem switches que interligam redes à longa distância. De qualquer forma sua principal utilização é ainda voltada para redes locais (LANs).

A manutenção de tabelas MACs (endereços físicos das placas de redes) dos dispositivos interligados em cada porta permite que este tipo de equipamento evite colisão tratando cada porta como ponto a ponto, direcionando os pacotes apenas para o destino específico, aumentando consideravelmente o desempenho quando comparado a redes que ainda utilizam hubs. Estas tabelas MACs são montadas dinamicamente à medida que as estações vão transmitindo dentro da rede.

Com a evolução dos hardwares estes switches são capazes de oferecer configurações físicas em modelos hierárquicos com o propósito de aumentar o desempenho e disponibilidade da rede, modelos em uma, duas ou até três camadas podem ser encontradas em ambientes de produção. A Figura 1 apresenta um modelo hierárquico em 3 camadas com uma de núcleo ou central (responsável em interligação do core da re-

de), outra de agregação (interliga os switchs de acesso) e a de acesso (interliga os dispositivos finais)

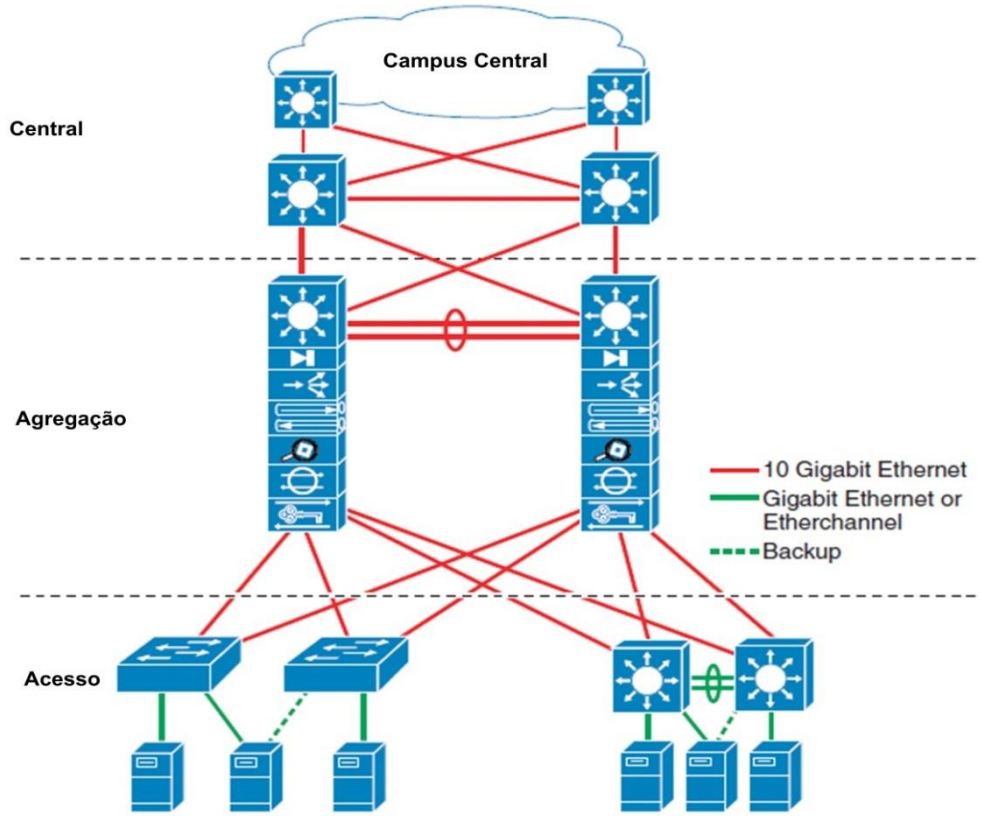

Figura 1. Modelo Hierárquico para configuração de Switches. Fonte: Cisco Networking

Além da topologia física os switches podem ser configurados para segregar o trafego entre os dispositivos, aplicando um conceito conhecido como VLAN (Virtual LAN): trata-se de um princípio que tem por objetivo segmentar o domínio de broadcast (reduz a carga nos segmentos) e isolar o trafego entre os dispositivos (aumenta segurança). Os principais objetivos com esta técnica são: aumentar segurança; reduzir custos; aumentar desempenho e melhorar gestão por parte da equipe de TI.

A Figura 2 mostra um cenário onde dois switches são configurados com duas VLANs distintas de tal forma que os dispositivos da VLAN1 não se comunicam com os dispositivos da VLAN2 e para que o trafego passe de um switch para o outro uma interface em modo Trunk é configurado. O modo trunk altera o formato do pacote para identificar ao switch de destino a qual VLAN aquele pacote que está sendo entregue pertence, permitindo que uma única porta de cascata trafegue várias VLANs sem que haja mistura destes pacotes. Este conceito é conhecido como VTP (VLAN Trunk Protocol) ou ainda protocolo 802.1Q! (Lembre-se deste código, vc verá a configuração dele nos equipamentos!!!)

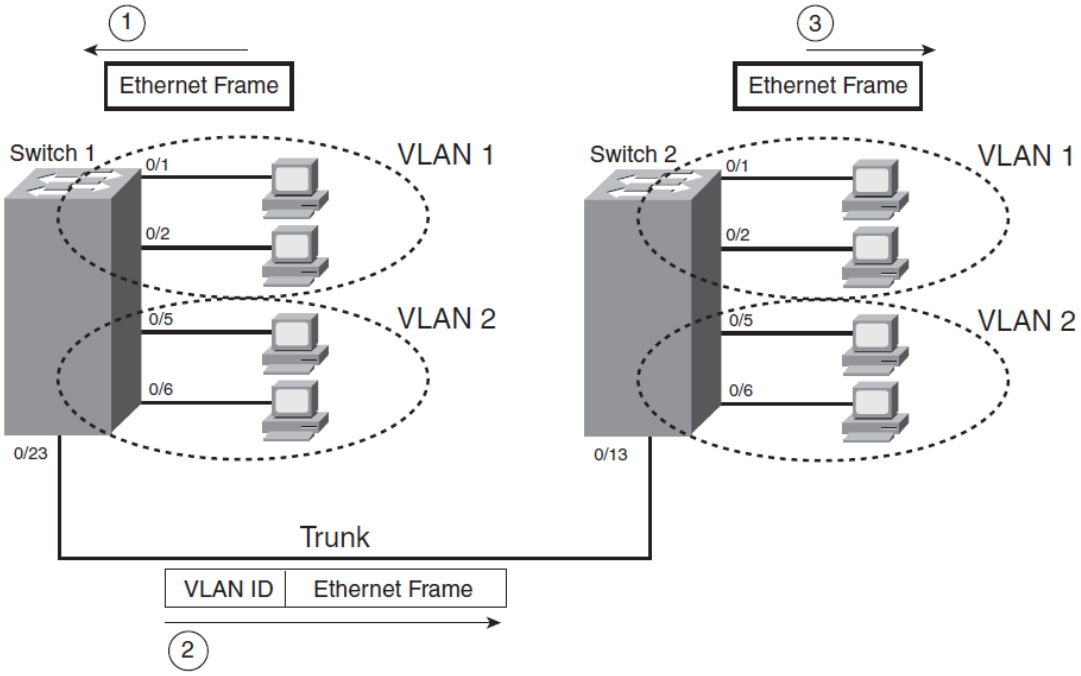

Figura 2. Cenário onde duas VLANs são configuradas com uma porta Trunk permitindo a comunicação entre os switches

Para permitir a comunicação entre as VLANs, um equipamento que suporte roteamento deve fazer a comunicação entre as VLANs, este papel pode ser assumido por switches que implementam camada três ou por roteadores. A Figura 3 exemplifica um caso onde um roteador assume o papel de rotear os pacotes entre VLANs distintas. Especial atenção ao lado esquerdo da imagem, onde é ilustrado a entrada de um quadro com a identificação da VLAN1 e a saída deste mesmo quadro, mas agora com a ID da VLAN2.

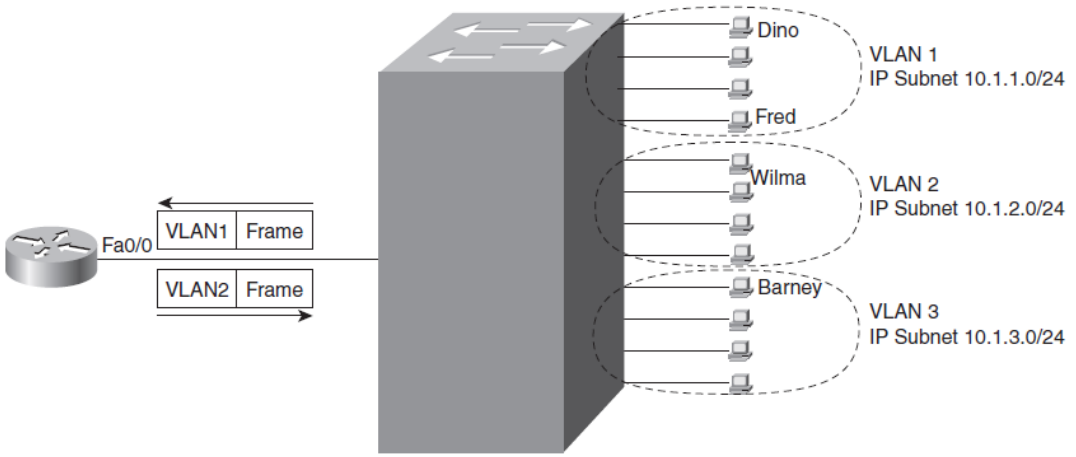

Figura 3. Intercomunicação entre VLANs com uso de roteadores

Por fim o protocolo Spanning Tree Protocol (STP), prevê redundância de ligação à rede permitindo que uma rede de comutação de camada 2 possa se recuperar de fa-

lhas, sem intervenção e em tempo hábil. Evitando o problema conhecido como tempestade de broadcast quando dois ou mais switches são interligados em loop. Existem hoje várias implementações (MSTP, RTSP, etc.) deste conceito com o objetivo de convergir mais rápido para um modelo ideal da rede. No exemplo da Figura 4 a interligação entre o switch 2 e 3 é desabilitada automaticamente pelo protocolo STP para evitar que o loop se forme e caso algum outro circuito deixe de funcionar ela pode assumir sua função para permitir a comunicação.

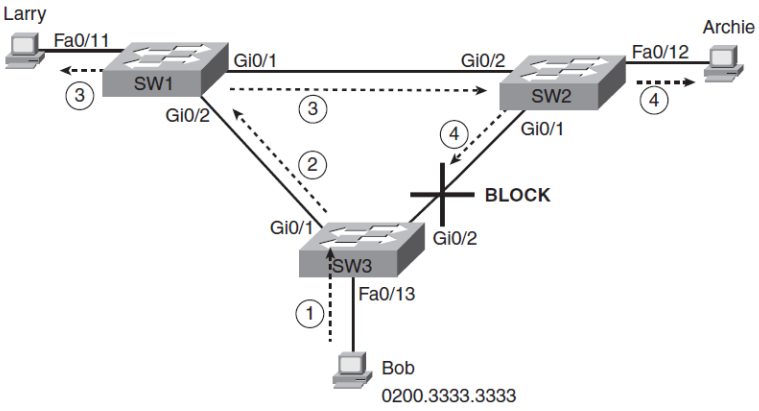

Figura 4. Estado das portas após o STP estabilizar

Na exposição do professor ele ainda deve falar da evolução das topologias de rede, o backplane dos switchs que podem ser blocking e no-blocking e por fim falar do tratamento dos quadros que pode adotar o modo store-and-forward e cut-through.

Simuladores de Rede

Um simulador de redes é um software que tem como objetivo apresentar uma interface em que o usuário pode criar uma rede, configurar os dispositivos dessa rede e testar o seu funcionamento, simulando um ambiente físico de roteadores, switches, modems e links de dados. É extremamente importante para testes e para o estudo e aprendizado de redes de computadores.

Entre os simuladores mais elaborados, tem-se:

- Packet Tracer da Cisco.
- GNS 3.0 (emulador)

- Routersim

A quantidade de comandos e funcionalidades de cada equipamento presente no simulador é que determina a sua qualidade, sendo o Packet Tracer e o GNS 3.0, os mais completos.

Nosso ambiente dispõe do RouterSim e Packet Tracer, este último será nosso ambiente nas próximas aulas e pode ser acessado pelo caminho: Windows, Todos os Programas, Cisco Packet Tracer, Cisco Packet Tracer. Com a conta criada na plataforma AVA da Cisco você pode fazer o download da última versão deste software. (www.netacad.com).

Em seu primeiro acesso, você deverá logar com a conta criada pelo professor no AVA (ambiente virtual de aprendizado) da Cisco, conforme Figura 5. Tendo problemas para logar com sua conta institucional, opte pelo logon de convidado no rodapé.

Figura 5. Login netacad.com Cisco

A tela principal possui diversas ferramentas para poder desenvolver e testar suas soluções para a rede, veja Figura 6.

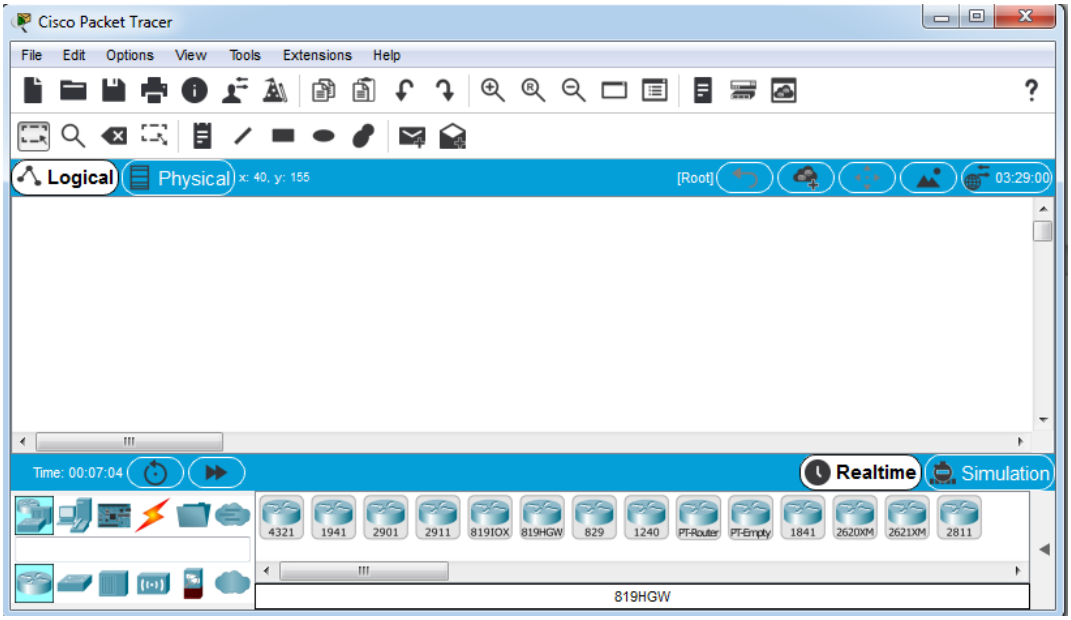

Figura 6. Tela principal do Cisco Packet Tracer

Nossa primeira simulação vai explorar conceitos **de switching como endereçamento IP, VLANs, trunk, roteamento entre VLANs e Spanning Tree**.

Clique na opção de Switches e selecione o modelo 2950-24 depois clique na área de trabalho para colocar o dispositivo, ao todo serão dois. Em seguida coloque um do modelo 2960, com na Figura 7.

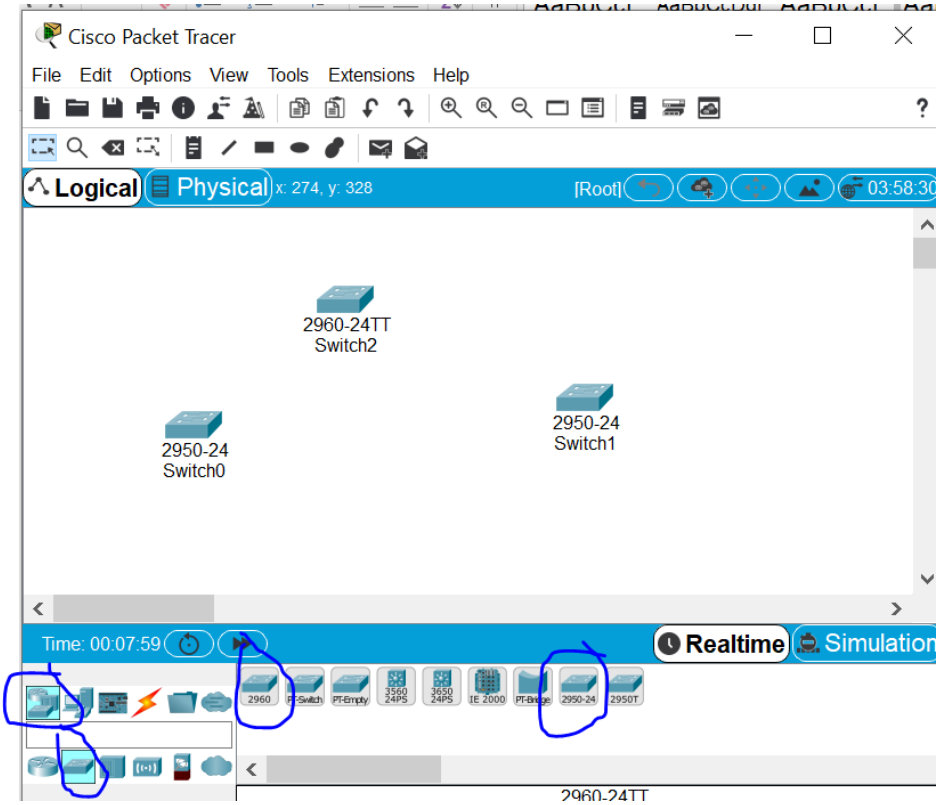

Figura 7. Selecionando Dispositivos de Rede.

Além disso, instancie 9 “end devices” do tipo PC, três para cada switch. Seu cenário ficará parecido com o da Figura 8.

Nosso objetivo com este cenário será produzir uma rede com 3 VLANs, com as faixas de ip 192.168.0.0/24, 192.168.1.0/24 e 192.168.2.0/24, nos três switches. Cada switch terá um host pendurado em cada VLAN.

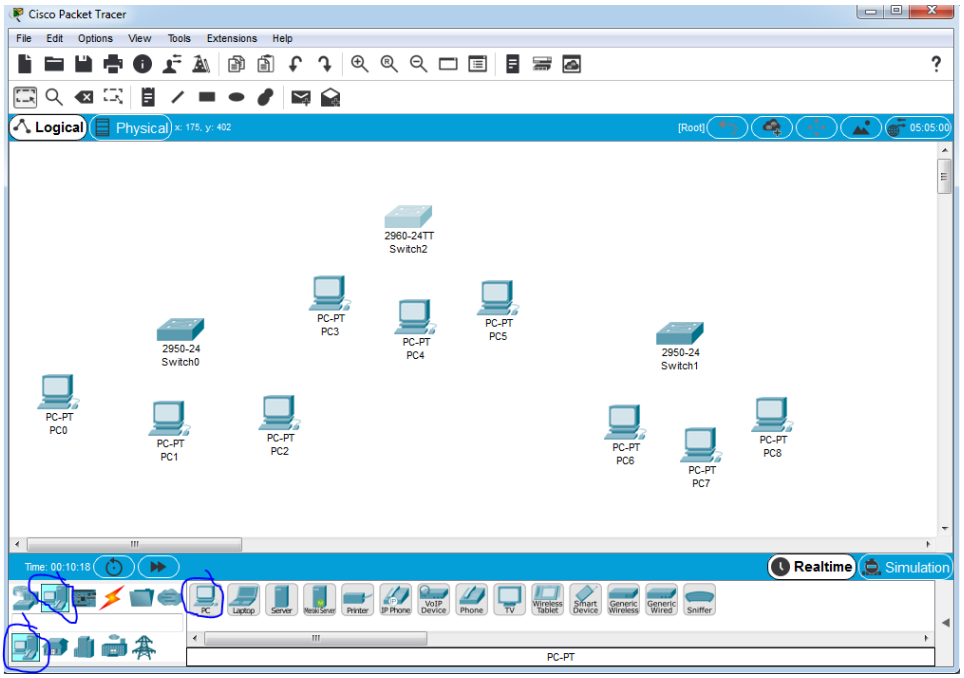

Figura 8: Topologia com os “end devices”.

Vamos começar com a configuração dos hosts. Clique com o botão esquerdo sobre o PC0, deve ser apresentada uma tela conforme a Figura 9, selecione a aba de *Config*, onde vc já poderá colocar o IP do Default Gateway, depois clique na esquerda em Fast Ethernet 0 onde você colocará o ip e a máscara seguindo a distribuição da tabela 1.

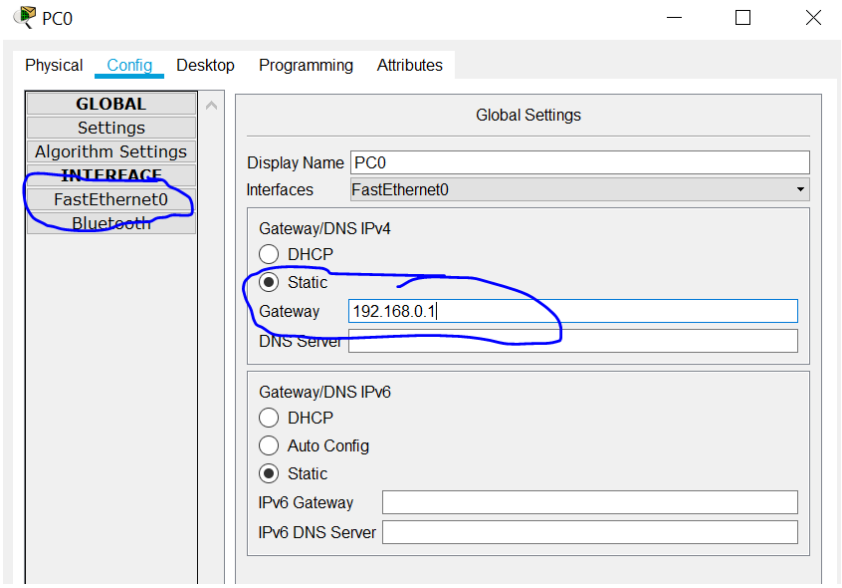

Figura 9. Tela do Config do PC0, com a informação do Gateway.

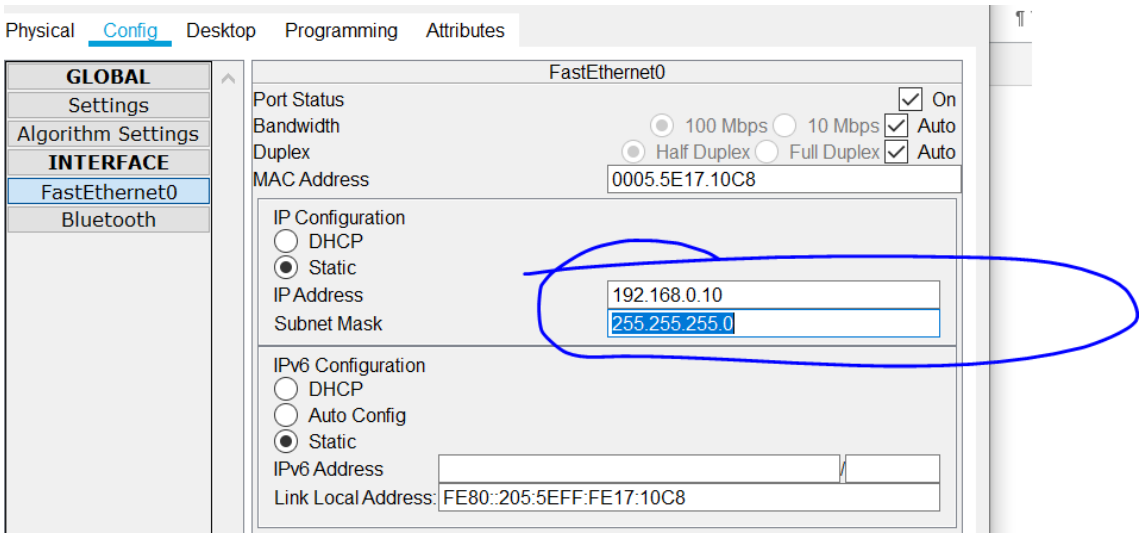

Figura 10. Configurações de IP da Rede no PC0.

Host	VLAN	Endereço	Máscara	Default Gate-way
Host PC0	1	192.168.0.10	255.255.255.0	192.168.0.1
Host PC1	2	192.168.1.10	255.255.255.0	192.168.1.1
Host PC2	3	192.168.2.10	255.255.255.0	192.168.2.1
Host PC3	1	192.168.0.11	255.255.255.0	192.168.0.1
Host PC4	2	192.168.1.11	255.255.255.0	192.168.1.1
Host PC5	3	192.168.2.11	255.255.255.0	192.168.2.1
Host PC6	1	192.168.0.12	255.255.255.0	192.168.0.1
Host PC7	2	192.168.1.12	255.255.255.0	192.168.1.1
Host PC8	3	192.168.2.12	255.255.255.0	192.168.2.1

Tabela 1: Distribuição de Endereços de IP dos Hosts

Na medida em que você for configurando cada estação, clique no ícone de Connections (no raio amarelo), depois na linha preta *Copper Straight-Through* como mostrado na Figura 11. Em seguida você deve selecionar o computador e clicar na porta de *Fas-*

tEthernet0, como na Figura Figura 12 e depois clique no switch e selecione a porta FastEthernet respectiva.

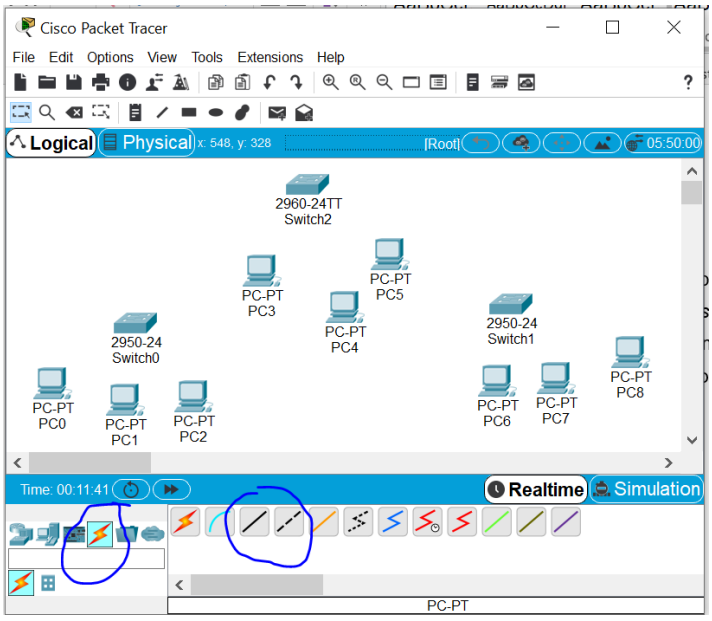

Figura 11. Selecionando Conexões

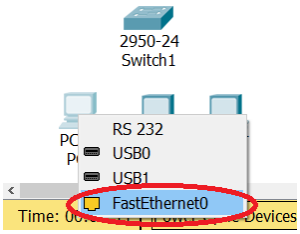

Figura 12: Conexões de um computador

Você pode reparar que vai aparecer uma bolinha ou triângulo verde, mais próximo do host e um laranja próxima do switch conforme a Figura 13, elas vão ficar piscando por um tempo até que a bolinha laranja fique verde, Figura 14Figura . Isso acontece porque o switch precisa de um tempo para poder habilitar a porta de comunicação. Esse processo pode ser observado usando o modo de simulação.

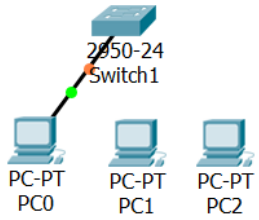

Figura 13: Switch sem conexão com o host

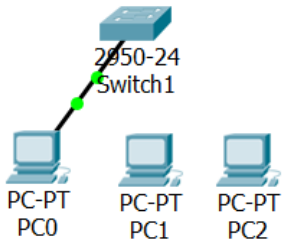

Figura 14: Switch com conexão estabelecida

Faça o mesmo para todos os hosts. Finalmente, ligue a porta *FastEthernet0/24* do Switch1 (2950-24) à porta *GigabitEthernet0/1* do switch0 (2960-24), e a porta GigabitEthernet0/2 no Switch2 em sua porta *FastEthernet0/24,* porém você deve usar o cabo preto tracejado *Copper Cross Over*, o outro cabo funcionaria também. A sua topologia agora deve estar semelhante à Figura 5.

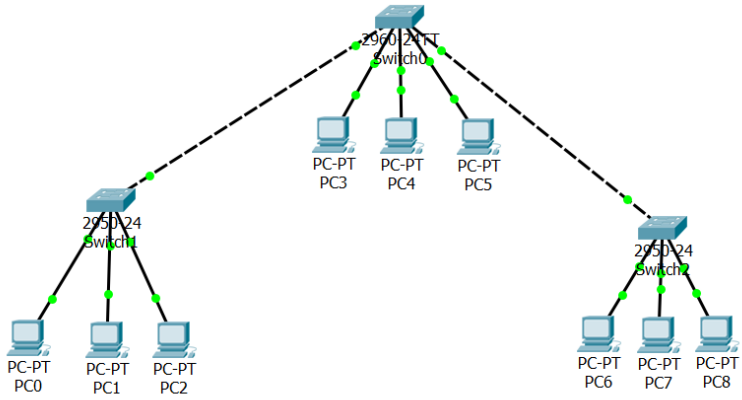

Figura 15: Topologia com ligações de rede e configuração ip dos hosts

Clicando em um computador, na aba Desktop você pode acessar o seu *Command Prompt* para realizar alguns testes de conexão (Figura). Use o comando ping 192.168.0.11 e verifique se existe resposta e teste as demais conexões. Você pode usar o **modo de simulação** para visualizar a comunicação que acontece entre os aparelhos, para isso basta ativar o modo no ícone do canto inferior direito conforme a Fi-

gura 17 e usar os controles para visualizar os pacotes sendo enviados pela rede (Figura 18).

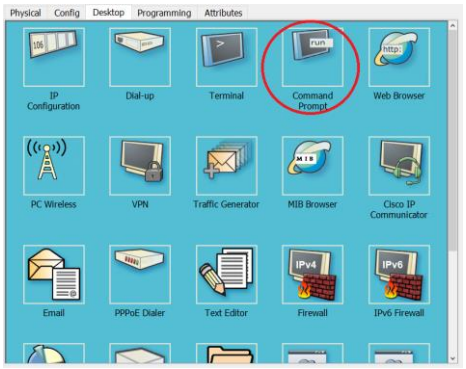

Figura 16: Tela de comandos para desktop do host

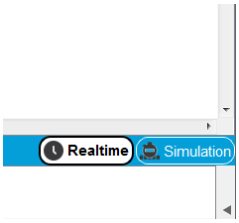

Figura 17: Modo de tempo real e simulação

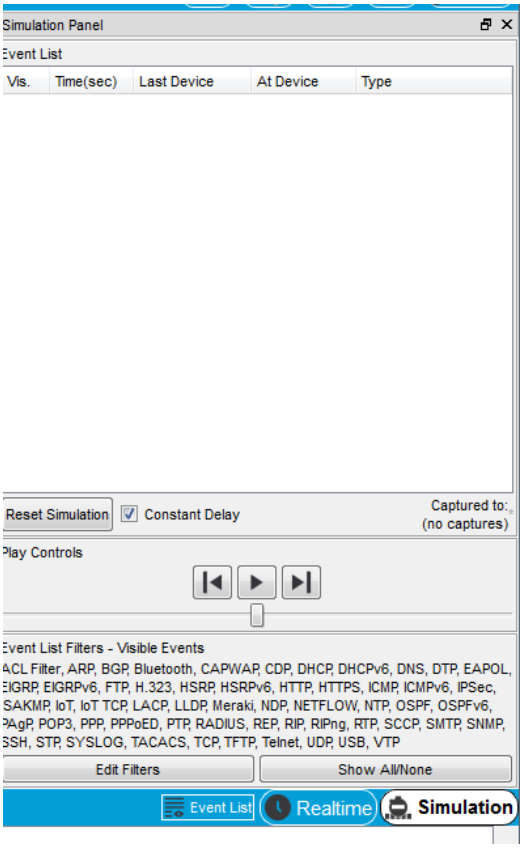

Figura 9. Tela de Simulação.

O problema que temos neste momento é que todas as estações estão em um mesmo “grupo de broadcast”, isto implica que um usuário mais esperto poderia trocar seu IP para ver as estações de outro grupo de IP e mais grave que isto, alguns switchs permitiriam a comunicação entre as estações mesmo com os IPs em blocos diferentes (não é o caso desses switches que estamos usando). Ou ainda, se você da estação 192.168.0.10 tentar pingar a 192.168.1.10 não vai funcionar, porque estes switches não permitem, mas se vc trocar o ip de 192.168.0 10 para 192.168.1.20 vai conseguir.

A partir de agora começaremos a fazer a configuração nos switches das VLANs para impedir que máquinas em VLANs distintas se comuniquem.

Existem várias formas de fazer a configuração de VLANs ela pode ser por porta, por Ip das estações ou por autenticação junto com o protocolo 802.1x que aproveita o usuário que foi autenticado no Windows. Ou seja, uma vez que o usuário foi autenticado, o Windows conversa com o Switch que interage com o servidor Radius na rede, instalado em um AD ou LDAP para identificar a qual VLAN aquele usuário pertence.

No nosso laboratório vamos para o mais simples, fazer a configuração por porta. As portas 1 de cada switch permanecerão na Vlan1 que também tem a função de administração dos switches, ou seja, se vc quiser fazer um telnet para configurar o switch a estação deve estar em uma porta da VLAN 1, por este motivo configuraremos os switchs na faixa de ip 192.168.0.0/24.

As outras VLANs serão a 2 e 3 que vamos chamar de adm e acad respectivamente. Para começar a configuração dê um clique no switch 2950 mais à esquerda que lhe será apresentando uma tela com as configurações físicas dele, mude para a aba *CLI*. Os passos a serem seguidos são os seguintes, a figura 19 mostra estes comandos:

1. Entraremos em modo privilegiado
2. Entraremos em modo de configuração Global (comando “configure terminal”)
3. Atribuiremos um nome ao Switch 2950-A (comando “hostname 2950-A”)
4. Atribuiremos o endereço ip 192.168.0.254 com a máscara 255.255.255.0 para a VLAN 1
5. Setaremos o default gateway como 192.168.0.1
6. Salvaremos as configurações na NVRAM

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname 2950-A
2950-A(config)# interface vlan 1
2950-A(config-if)#ip address 192.168.0.254 255.255.255.0
2950-A(config-if)#exit
2950-A(config)#ip default-gateway 192.168.0.1
2950-A(config)#end
2950-A# wr mem
```

Figura 19. Prompt de CLI do Switch A.

Você pode usar a tecla tab para auto completar os comandos, similar ao terminal Linux, e usar a tecla “?” para que a linha de comando te informe as opções para completar o comando, caso o resultado seja <cr>, significa que o comando está completo.

Vamos agora criar as VLANs 2 e 3, atribuir nome a todas as VLANs e indicar quais portas estarão em quais VLANs (Figura 20). Entre novamente no switch com o duplo clique:

1. Entraremos em modo privilegiado e veremos as configurações do seu switch.
2. Entraremos em modo de configuração Global
3. Atribuiremos nome a cada uma das VLANs
4. Entraremos nas interfaces f0/2 e f0/3 para configuramos as portas no modo de acesso, ou seja, onde são ligados os “end devices” e em seguida informamos em qual VLAN aquela porta pertence.
5. Salvaremos as configurações na NVRAM

```
Switch>enable
2950-A#show vlan
2950-A# config terminal
2950-A (config)# vlan 2
2950-A (config if)# name adm
2950-A (config if)# exit
2950-A (config)# vlan 3
2950-A (config if)# name acad
2950-A (config if)# exit
2950-A (config)# interface fastEthernet 0/2
2950-A (config if)# switchport mode access
2950-A (config if)# switchport access vlan 2
2950-A (config if)# exit
2950-A (config)# interface fastEthernet 0/3
2950-A (config if)# switchport mode access
2950-A (config if)# switchport access vlan 3
2950-A (config if)# end
2950-A# show vlan
```

Figura 20. Configurando interfaces do switch.

Agora falta a configuração da interface fastEthernet0/24 como Trunk (Figura 21).

```
2950-A# configure terminal
2950-A (config)# interface fastEthernet 0/24
2950-A (config if)# switchport mode trunk
2950-A (config if)# end
2950-A# wr mem
```

Figura 21. Configurando Cascata no modo TRUNK

Repita todo o processo para o outro switch 2950 alterando apenas o IP da VLAN 1 para 192.168.0.253 e o nome do switch para 2950-B. Repita o processo também no switch 2960, colocando nele o ip 192.168.0.252 e prestando atenção para o fato de que duas as portas que ficarão no modo trunk são a GigaEthernet0/1 e GigaEthernet0/2.

Faça testes de pings. As estações 192.168.1.* vão se pingar entre elas, mas não entre as outras 192.168.0.* e 192.168.2.*, E AGORA MESMO QUE VC MUDE O IP DO PC0 PARA 192.168.1.20 ele não se comunicará com a outra VLAN. Os switchs só poderão ser pingados dos hosts das faixas 192.168.0.*

Vamos agora colocar um elemento de rede que fará o roteamento entre as três sub-redes. Insira um Roteador 1841 na sua topologia e ligue-o a porta 24 do switch 2960.

Coloque esta porta em modo trunk e configure a interface do roteador com IP nas três faixas de rede 192.168.0.1/1.1/2.1.

Por padrão, os roteadores Cisco veem com as portas desativadas, para podermos configurar as portas vamos usar o modo de CLI, ao iniciar ele pergunta se desejamos fazer as configurações automáticas, no caso **NÃO**. Todas as configurações do roteador e switch serão descritas abaixo:

No switch 2960 (Figura 22):

```
2960> enable
2960# configure terminal
2960 (config)# interface FastEthernet 0/24
2960 (config if)# switchport mode trunk
2960 (config if)# end
2960# wr mem
```

Figura 22. Modo TRUNK para porta que liga o Roteador.

No roteador (Figura 23):

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Router> enable
Router# configure terminal
// vamos configurar ip para vlan 1 na interface repare que além de escrever fastEthernet 0/0 colocamos um .1 para indicar que é para VLAN 1!
Router (config)# interface fastEthernet 0/0.1
// indicamos que está sendo usado o 8021q com a vlan 1
Router (config if)# encapsulation dot1q 1
Router (config if)# ip addr 192.168.0.1 255.255.255.0
Router (config if)# exit
Router (config)# interface fastEthernet 0/0.2
Router (config if)# encapsulation dot1q 2
Router (config if)# ip addr 192.168.1.1 255.255.255.0
Router (config if)# exit
Router (config)# interface fastEthernet 0/0.3
Router (config if)# encapsulation dot1q 3
Router (config if)# ip addr 192.168.2.1 255.255.255.0
Router (config if)# exit
// vamos subir a interface
Router (config)# interface f0/0
// retiramos a interface de modo down
Router (config if)# no shutdown
Router (config if)# end
Router # wr mem
```

Figura 23. Configurações Roteador.

Sua topologia final deve ter ficado conforme a Figura 24.

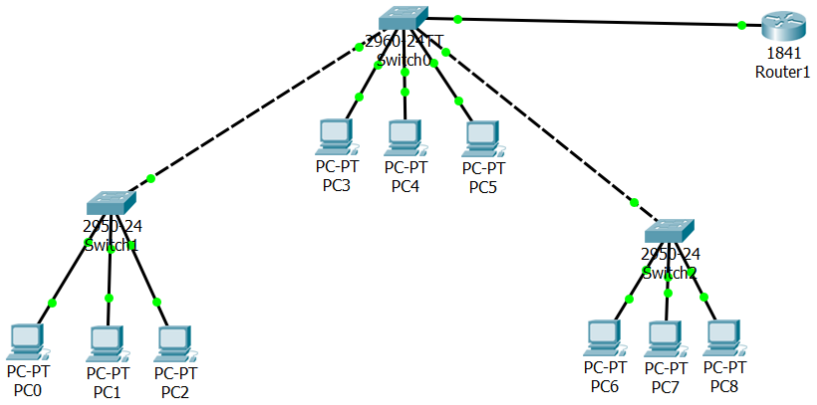

Figura 24: Topologia final da configuração de switch

Agora todas as VLANs se pingarão com o auxílio do Roteador. Se você chegou até aqui tente agora usar o modo de simulação, clicando à direita no canto inferior, dando um ping do pc0 192.168.0.10 para o 192.168.1.11. Use o PLAY para ver o pacote caminhando.

Habilite a visualização do ARP para ver o broadcast viajando na rede.

Feche loop entre os switches e veja as interfaces sendo desabilitadas automaticamente.

Faça mais alguma coisa pra não ficar no ZAP ZAP!!!!!