


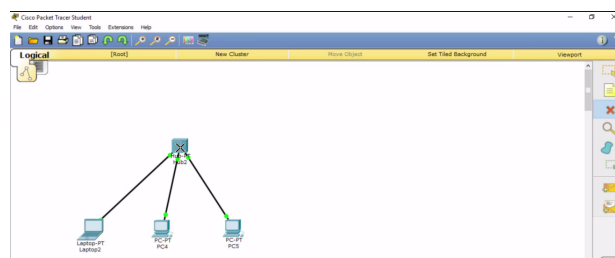
5 - Switches e seus avanços

Switches

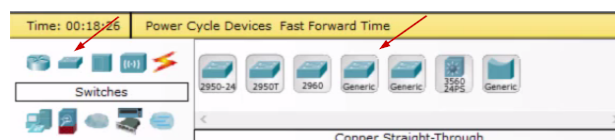
Vimos que os hubs apresentam uma certa limitação para identificar qual equipamento está em uma determinada porta, podendo ocasionar em lentidão e problemas de segurança como vimos nas análises do Wireshark.

Para evitarmos a limitação do hub, foram desenvolvidos outros equipamentos com o intuito de melhorar a performance. Um equipamento criado e que também interconecta os dispositivos finais recebe o nome de **Switch**. Nos aprofundaremos sobre o assunto.

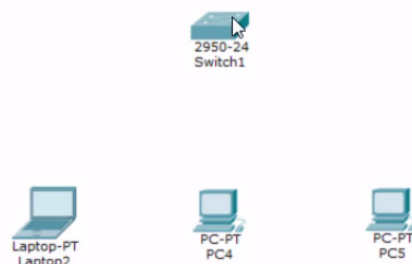
Vamos primeiro deletar o Hub que colocamos no projeto no Packet Tracer. Basta selecionar o ícone de  da coluna da direita e depois clicar sobre o Hub.



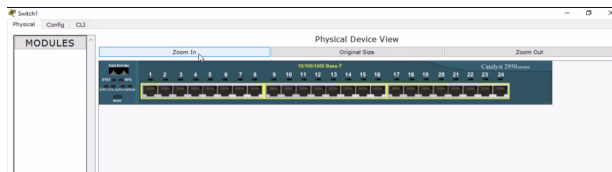
Deletamos o hub. Depois, clicaremos na tecla "Esc" para sairmos do modo "x". Em seguida, selecionaremos o Switch no menu do canto esquerdo.



Aparecerão diferentes opções de equipamentos. Como o software foi desenvolvido pela Cisco, a empresa utilizou seus próprios equipamentos. Selecionaremos um modelo:

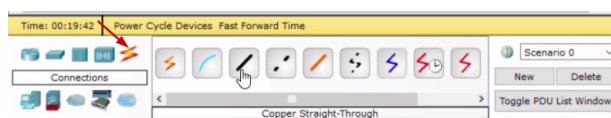


E depois, daremos um clique duplo no Switch. Então, irá aparecer a imagem com o layout do equipamento.

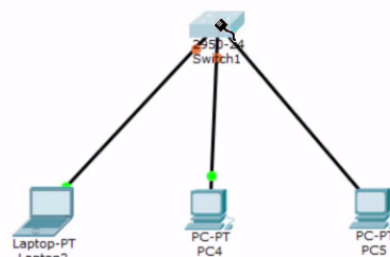


Dependendo do modelo e do fabricante, o modelo irá variar. Mas em essência, todos terão portas que nos permitem conectar os dispositivos finais dos computadores usados nas simulações.

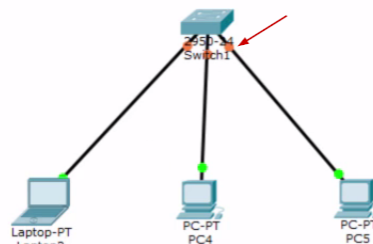
Veremos como conectar os computadores com o Switch. O hub e o switch terão o mesmo tipo de placa, que receberá o sinal nas portas das posições 1 e 2 e transmitirá nas posições 3 e 6. Sabemos que o laptop transmitirá na posição 1 e 2 e o Switch receberá na posição 1 e 2. Ocorre uma conexão natural e usaremos o cabo direto. Clicaremos no ícone do raio no menu da esquerda e selecionaremos o cabo direto.



Clicaremos no laptop, selecionaremos a porta "FastEthernet0" e ligaremos até o Switch - que selecionaremos a porta "FastEthernet0/1". Repetiremos o processo com os demais computadores.

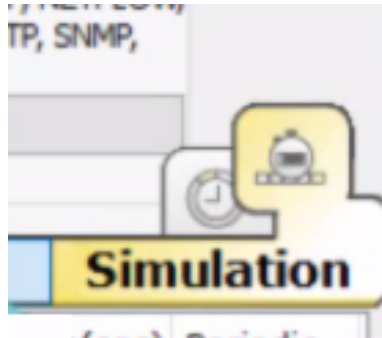


Mas diferente do Hub, que ficará sinalizado com luzes verdes, o Switch ficará com luzes da cor laranja.

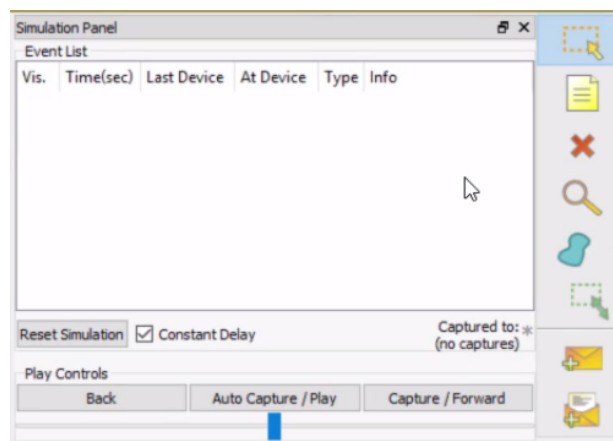


O Switch precisa de um período de tempo para habilitar a porta de comunicação. O processo demora alguns segundos e é retratado na simulação também. À medida que as portas vão sendo habilitadas, as luzes mudam de cor e ficam verdes.

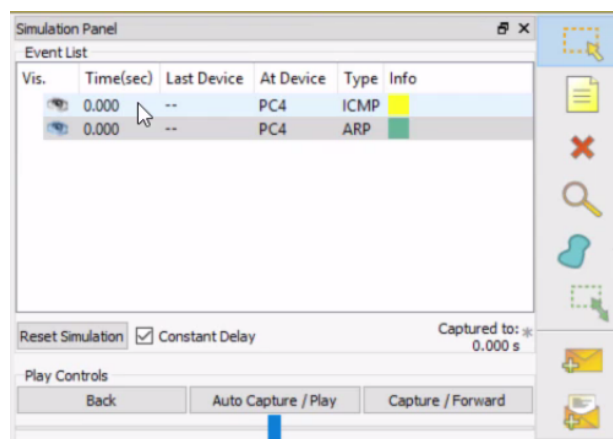
Em segund, testaremos a conectividade como foi feito anteriormente. Mas queremos quebrá-la em posições menores para que ela possa verificar como a comunicação acontece até chegar ao outro computador. Novamente, mudaremos a posição de "Realtime" para "Simulation" no canto inferior da direita.



E aparecerá a coluna que mostrará os protocolos da simulação.

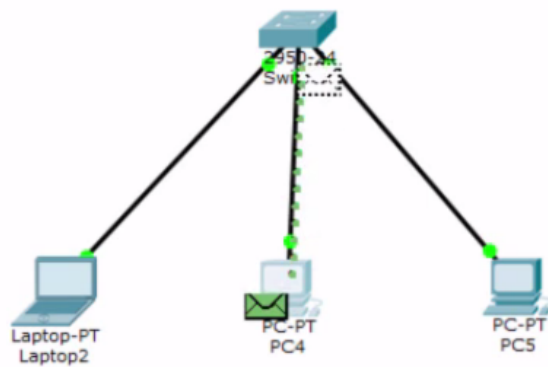


Agora temos o segundo computador que estou usando para a gravação do curso. Ao clicar no ícone dele, acessaremos o Command Prompt. Digitaremos na tela `ping 182.168.3.1`, usando o IP do laptop que queremos nos conectar. A partir disso, será mostrado no "Simulation Panel" os protocolos que vimos anteriormente no hub.

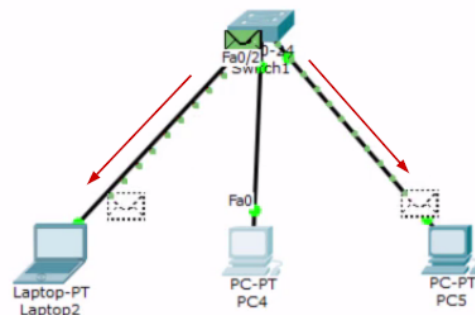


O protocolo ICMP está dentro do ping e o ARP, que não sabe onde está localizado o IP e perguntará para todos na rede.

Vamos seguir a animação.



Observe que a informação do ARP para tentar descobrir onde está o laptop foi passada para o Switch, que também não sabe qual computador está conectado. Ele irá enviar as requisições para os outros computadores, com exceção da máquina de onde foi originada a informação.



A informações foi enviada para os dois computadores. Mas o terceiro não recebeu a requisição, porque o IP termina com o número 3.

Então, a informação será descartada. O laptop receberá a informação do Switch e depois, irá devolvê-la par ao mesmo. Até aqui, o processo é o mesmo de quando utilizamos o Hub.

No entanto, nesta etapa, o hub continuaria enviando a informação para os dois computadores, porque ele não conseguia identificar onde os computadores estavam conectados. Mas o Switch irá retornar a informação dos dois computadores apenas para máquina que enviou inicialmente a requisição. Esse é o grande diferencial, o Switch aprende onde os computadores estão conectados. Como ele faz isso?

Falamos anteriormente que com os protocolos ARP não sabemos onde estão conectados os equipamentos. Quando o dispositivo que é procurado receber a requisição, ele retornará um número de série que está na placa de rede, chamado endereço de mac. Vamos pesquisar no Terminal qual é o número da placa do computador utilizado na gravação. Faremos isto digitando:

```
c:\Users\Alura>ipconfig /all
```

Vamos pesquisar qual é a rede Wi-fi que está sendo usada:

```

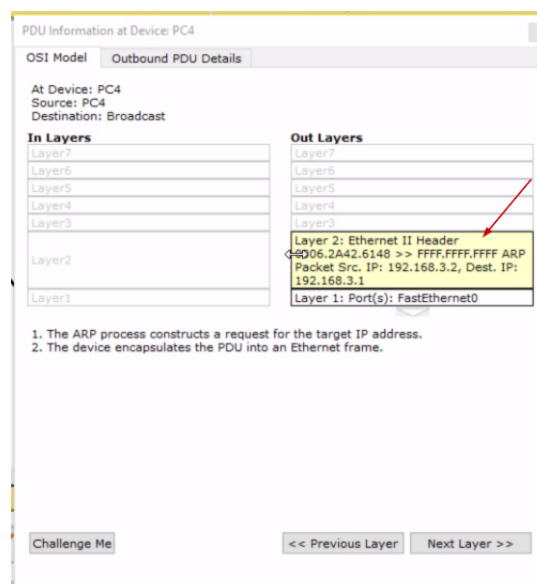
Adaptador de Rede sem Fio Wi-Fi 2:
Sufixo DNS específico de conexão. . . . . : home
Descrição . . . . . : Broadcom 802.11ac Network Adapter #2
Endereço Físico . . . . . : 88-E6-50-16-34-76
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
Endereço IPv4. . . . . : 192.168.1.33(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : quarta-feira, 14 de setembro de 2016 09:44:10
Concessão Expira. . . . . : quarta-feira, 14 de setembro de 2016 21:47:31
Gateway Padrão. . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
Servidores DNS. . . . . : 192.168.1.1
NetBIOS em Tcpip. . . . . : Habilitado

```

Ele indicou o número de série da minha placa de rede: **80-E6-50-16-34-76**. Este é um número único que vem direto do fabricante. Quando fazemos a requisição do ARP e perguntamos quem tem um número específico de IP, na verdade estamos perguntando qual é o endereço mac da máquina com o endereço IP.

Para entender, vamos fazer um comparação com outra situação do mundo real. No Brasil, podemos ter vários tipos de documento: RG, CPF e Passaporte. Mas o passaporte pode ser utilizado em outros países, por ser internacionalmente válido. Já o RG é mais local. O endereço mac funciona mais localmente e só funciona em uma rede pequena. Já IP é uma identificação da máquina globalmente. O endereço mac está uma camada abaixo do endereço IP, mas para chegar na camada de cima precisamos da de baixo. Funciona de forma semelhante a uma pirâmide em que precisamos passar por cada camada para chegar ao topo.

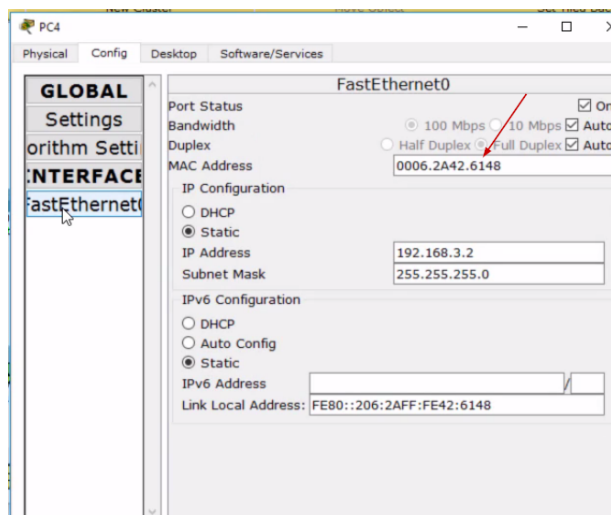
Vamos abrir o protocolo ARP e ver qual tipo de informação ele está passando:



O meu computador envia requisição para todos os outros, representado pelo **FFFF.FFFF.FFFF**, quem tem o IP **192.168.3.1**.

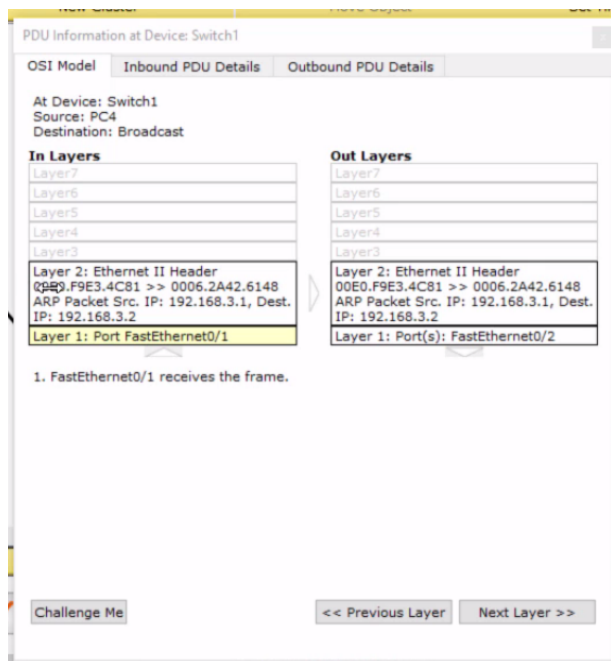
No entanto, o Switch é um equipamento mais inteligente e consegue lembrar qual o mac está gravado em cada porta e conseguirá lembrar de quem ele recebeu a requisição.

Vamos analisar a aba "Config" e clicar na parte de "FastEthernet0", que é a placa do meu computador:



Vemos o endereço mac marcado. Este número aparecia no protocolo ARP.

Continuaremos analisando o protocolo ARP, dessa vez pesquisaremos o protocolo referente ao laptop.



O protocolo diz que para o endereço MAC que fez a procura, com o final 6148 está o endereço MAC 4C81. Logo, quando o retorno do ARP voltar para o Switch, o aparelho irá perceber que a sua porta está conectada com o endereço mac 00E0.F9E3.4C81. Outro endereço será colocado na memória. Mas a informação será retornada para a máquina com o endereço mac 0006.2A42.6148, no caso, o segundo computador. O Switch já conhece quem é e sabe onde está conectado. Ele não achará mais necessário passar a informação para o terceiro computador. Esta é a grande mudança proporcionada pelo Switch: ele memoriza o endereço mac e a partir dele, identificar com qual máquina ele quer se comunicar. Isto significa uma melhoria significativa tanto na questão do tráfego como na segurança, porque a informação não corre o risco de ser recebida pelo usuário malicioso. Pelo menos, ficou mais difícil que isto aconteça. Mas existem algumas questões que podem ser exploradas pelos usuários maliciosos. O Switch guardará a informação da localização de quem está conectado no endereço de memória. Mas se esta estiver lotada, os hackers poderão se aproveitar do fato para comprometer o Switch. Por isso, eles podem lotar

a memória do Switch com diversos endereços falsos, e o aparelho já não poderá mais decifrar o endereço de cada computador e voltará a passar as informações para todas as máquinas, atuando da mesma forma que um hub. Essa ação é relativamente fácil de ser feita. O Switch traz grandes melhorias, mas também apresenta fragilidades que podem ser exploradas por hackers.

Algo que podemos fazer como prevenção desse tipo de ação maliciosa, é o que chamamos de **segurança da porta**, em que é determinado o número de endereços mac que cada porta poderá aceitar. Por exemplo, podemos definir que a porta que está conectada com o laptop só poderá aceitar o endereço mac do mesmo e de outra máquina. Ou seja, podemos configurá-la para aceitar dois endereços mac. Caso um usuário malicioso tente se conectar com esta porta e começa a enviar vários endereços mac falsos, a porta será desabilitada. E assim, o hacker não será bem-sucedido.

O que é o protocolo ARP?

O ARP é o protocolo utilizado para fazer o mapeamento entre o endereço IP e o endereço MAC de um dispositivo. Isso é necessário porque o MAC encontra-se um nível abaixo do IP e eu preciso dele para poder transmitir as informações.

Em redes de computadores, temos protocolos que possuem hierarquias diferentes. Para poder chegar até o IP que está na camada 3, eu preciso passar pelo MAC que está na camada 2, pense como se fosse escalar uma pirâmide, não dá pra chegar ao topo sem passar pelo meio dela!

Qual equipamento veio para substituir os hubs?

Switches

Qual é a principal diferença entre os Hubs e os Switches?

O Hub não consegue aprender onde um equipamento está localizado, o Switch sim

Os hubs não conseguem aprender o endereço MAC das máquinas, já os Switches possuem essa função.

Como o Switch aprende onde um equipamento está localizado?

Os dispositivos ao se comunicarem passam pelo Switch e ao passar pelo Switch ele grava em sua memória quem está conectado em qual porta.

Qual é uma forma de ataque usada para conseguir informações passadas no Switch destinadas a outro usuário?

Métodos usados por usuários maliciosos seria de inserir vários endereços MAC falsos para “lotar” a memória do Switch, uma vez que a memória esteja cheia, o Switch não vai conseguir definir quem está onde e ele passa a atuar como um Hub.

Como podemos nos prevenir contra esse ataque?

Podemos configurar a porta do Switch para aceitar um número máximo de endereços MAC, ao ultrapassar esse limite a porta é desligada e o ataque não teria sucesso.

Mãos à obra: Switches

- Clique em cima do Hub e remova ele de nosso projeto pressionando o botão DELETE. No canto inferior esquerdo selecione a opção Swicthes e arraste para a área de trabalho. Posteriormente clique no ícone “Connections” e selecione a opção de cabo direto (3ª opção da esquerda para a direita).

- Clique no computador e posteriormente no Switch, a conexão poderá ser feita em qualquer porta. Depois disso no canto inferior direito troque o modo de operação de “RealTime” para “Simulation”.
- Clique em um dos computadores -> Aba Desktop -> Command prompt -> digite: ping (#ip de um dos outros dois computadores#) pressione ENTER
- Clique na aba inferior no botão “Capture/Forward” e analise que o retorno da informação volta somente para o computador que fez a requisição, isso porque o Switch consegue aprender o endereço MAC das máquinas que estão conectadas.