

Protegendo o Switch

Transcrição

Vimos o que um hacker pode fazer para comprometer o funcionamento do switch. Ele consegue, por meio do Kali Linux, mandar um grande número de endereços mac falsos com o objetivo de lotar a memória do equipamento. Uma vez que essa memória fica cheia, o switch não consegue mais diferenciar qual máquina está conectada em cada porta, e passa as informações para todas elas, atuando como um hub.

Fizemos isso com o Wireshark, que, ao ser aberto, nos mostra a atividade da rede Ethernet que estamos usando. Clicando sobre ela, veremos o relatório com os protocolos.

The top screenshot shows the Wireshark 'Capture' interface. The 'Capture' button is highlighted. Below it, the 'Capture filter' is empty. The 'Interface' list shows 'VirtualBox Host-Only Network' selected, and 'Ethernet' is highlighted. The bottom screenshot shows the 'Capturing from Ethernet' interface. The 'Capture' button is highlighted. Below it, the 'Capture filter' is empty. The 'Interface' list shows 'VirtualBox Host-Only Network' selected, and 'Ethernet' is highlighted. The packet list shows the following data:

No.	Time	Source	Destination	Protocol	Length	Info
5	3.012434	fe80::ffff:ffff:ffff:ffe	ff02::2	ICMPv6	103	Router Solicitation
6	3.199997	fe80::8000:f227:bec...	fe80::ffff:ffff:ffff:ffe	ICMPv6	151	Router Advertisement
7	3.276795	192.168.121.171	172.217.29.78	SSL	55	Continuation Data
8	3.393076	172.217.29.78	192.168.121.171	TCP	66	443 → 52291 [ACK] Seq=1 Ack=2 Win=361 Len=0 SLE=1 SRE=2
9	3.535234	192.168.121.171	172.217.29.78	SSL	55	Continuation Data
10	3.654212	172.217.29.78	192.168.121.171	TCP	66	443 → 52292 [ACK] Seq=1 Ack=2 Win=403 Len=0 SLE=1 SRE=2
11	3.848349	192.168.121.131	224.0.0.251	MDNS	703	Standard query response 0x0000 TXT TXT, cache flush PTR
12	3.848352	fe80::1c4f:8d13:ce0...	ff02::fb	MDNS	723	Standard query response 0x0000 TXT TXT, cache flush PTR
13	3.950111	192.168.121.131	224.0.0.251	MDNS	106	Standard query 0x0000 PTR _sleep-proxy_udp.local, "QU"
14	3.950112	fe80::1c4f:8d13:ce0...	ff02::fb	MDNS	126	Standard query 0x0000 PTR _sleep-proxy_udp.local, "QU"
15	3.993938	64.233.190.189	192.168.121.171	QUIC	83	Payload (Encrypted), Seq: 193
16	3.993938	64.233.190.189	192.168.121.171	QUIC	61	Payload (Encrypted), Seq: 194
17	3.995215	192.168.121.171	64.233.190.189	QUIC	81	Payload (Encrypted), CID: 15927585483535186082, Seq: 199
18	4.000938	192.168.121.171	64.233.190.189	QUIC	363	Payload (Encrypted), CID: 15927585483535186082, Seq: 200
19	4.210258	64.233.190.189	192.168.121.171	QUIC	76	Payload (Encrypted), Seq: 195

The bottom screenshot shows the 'Frame 1: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface 0'. The frame details are as follows:

- Ethernet II, Src: Micro-St_c1:aa:7f (d8:cb:8a:c1:aa:7f), Dst: Tp-LinkT_33:5e:32 (90:f6:52:33:5e:32)
- Internet Protocol Version 4, Src: 192.168.121.171, Dst: 54.172.82.211
- Transmission Control Protocol, Src Port: 50476 (50476), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 59
- Secure Sockets Layer

Suponhamos que a vítima queira acessar o site da Alura.



Enquanto ela tenta se logar, o hacker está fazendo a análise dos protocolos que trafegam na rede. O objetivo dele é ver a comunicação entre o usuário e o [site da Alura \(https://www.alura.com.br/\)](https://www.alura.com.br/). Para poder filtrar o tráfego, é preciso saber o endereço IP do site. Uma das formas de obter essa informação é com o `nslookup` no Prompt de Comando:

```
C:\Users\Alura>nslookup www.alura.com.br
```

Com esse comando, obteremos:

```
C:\Users\Alura>nslookup www.alura.com.br
```

```
Servidor: caelum121  
Address: 192.168.121.1
```

```
Não é resposta autoritativa:  
Nome: ghs.googlehosted.com  
Address: 64.233.186.121  
Aliases: www.alura.com.br
```

O endereço IP do site é 64.233.186.121 . Com essa informação, conseguimos filtrar o que realmente nos interessa no WireShark, com o `ip.addr==64.233.186.121` .

No.	Time	Source	Destination	Protocol	Length	Info
505	20.670409	192.168.121.171	64.233.186.121	TCP	66	52428 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
506	20.670470	192.168.121.171	64.233.186.121	TCP	66	52429 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
507	20.848113	64.233.186.121	192.168.121.171	TCP	66	80 → 52429 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK_PERM=1 WS=128
508	20.848113	64.233.186.121	192.168.121.171	TCP	66	80 → 52428 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK_PERM=1 WS=128
509	20.848198	192.168.121.171	64.233.186.121	TCP	54	52429 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
510	20.848222	192.168.121.171	64.233.186.121	TCP	54	52428 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
511	20.848640	192.168.121.171	64.233.186.121	HTTP	916	GET / HTTP/1.1
512	21.026779	64.233.186.121	192.168.121.171	TCP	60	80 → 52428 [ACK] Seq=1 Ack=863 Win=45568 Len=0
513	21.209648	64.233.186.121	192.168.121.171	HTTP	276	HTTP/1.1 302 Found
521	21.211431	192.168.121.171	64.233.186.121	TCP	66	52430 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
576	21.260006	192.168.121.171	64.233.186.121	TCP	54	52428 → 80 [ACK] Seq=863 Ack=223 Win=65792 Len=0
605	21.395226	64.233.186.121	192.168.121.171	TCP	66	443 → 52430 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1380 SACK_PERM=1 WS=128
606	21.395288	192.168.121.171	64.233.186.121	TCP	54	52430 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
607	21.395448	192.168.121.171	64.233.186.121	TLSv1.2	283	Client Hello
680	21.579830	64.233.186.121	192.168.121.171	TCP	60	443 → 52430 [ACK] Seq=1 Ack=230 Win=43904 Len=0

Agora estamos vendo toda a atividade com o site da Alura. Quando verificamos os tipos de protocolo listados, veremos o protocolo TLSv1.2. Os protocolos TLS são como uma evolução do SSL, fornecendo a criptografia da informação.

Assim, se houver alguém mal-intencionado colhendo essas informações, via hub ou switch, a criptografia protegerá o usuário.

Vamos escolher um protocolo TCP e tentar reconstruir seu cabeçalho HTTP, da comunicação que ocorreu entre o usuário e o site. Clicaremos com o botão direito sobre o protocolo, e em Follow > TCP Stream.

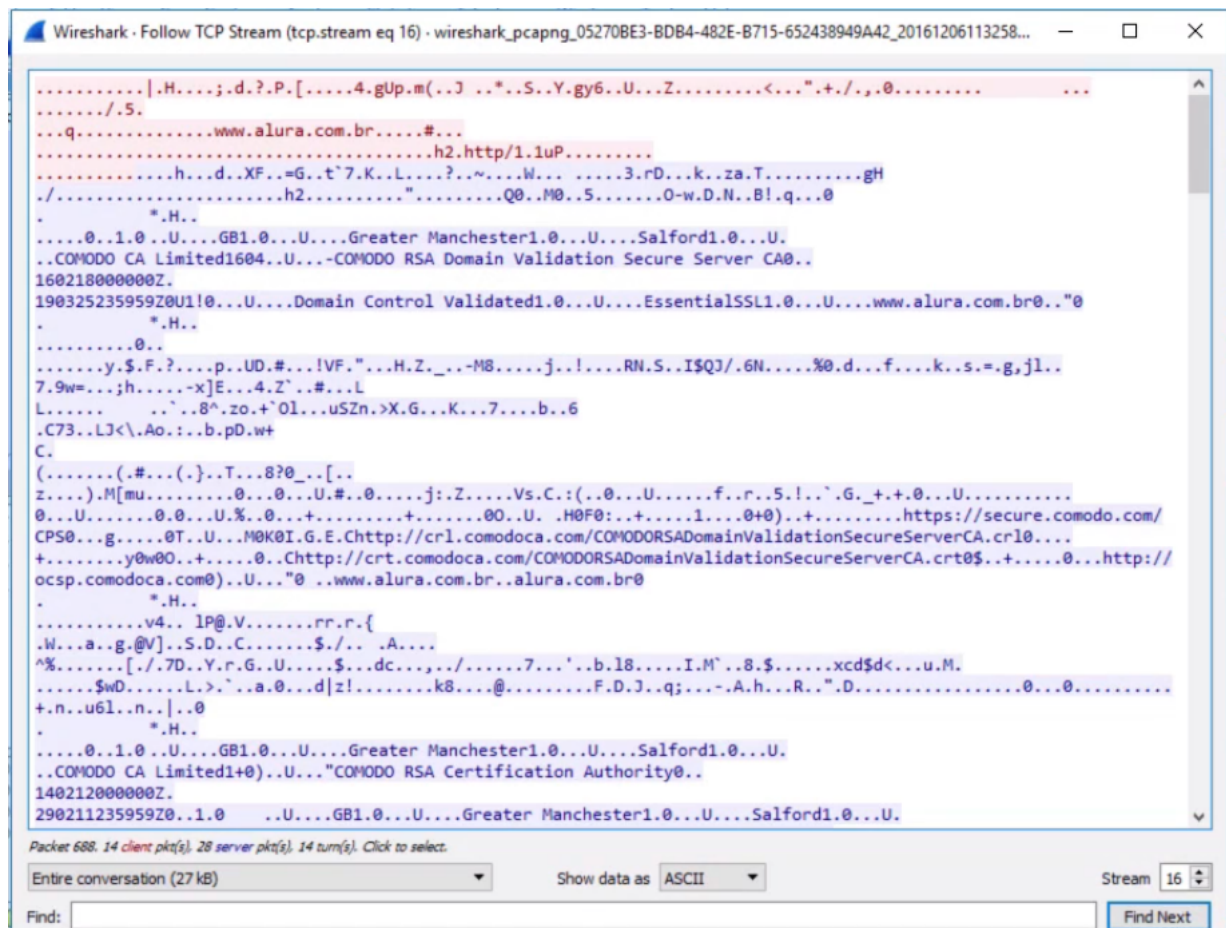
The screenshot shows the Wireshark interface with a packet list on the left and a packet details pane on the right. The packet list shows several TCP and TLSv1.2 packets. The packet details pane shows the selected packet (No. 1027) and its details: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. A right-click context menu is open over the selected packet, showing options like 'Follow', 'Copy', and 'Show Packet in New Window'. The 'Follow' option is selected, and a submenu is open showing 'TCP Stream', 'UDP Stream', and 'SSL Stream'.

No.	Time	Source	Destination	Protocol	Length	Info
808	22.397219	64.233.186.121	192.168.121.171	TCP	60	443 → 52430 [ACK] Seq=25459 Ack=1456 Win=46464 Len=0
825	22.557467	64.233.186.121	192.168.121.171	TCP	60	443 → 52430 [ACK] Seq=25459 Ack=1502 Win=46464 Len=0
1023	25.540127	192.168.121.171	64.233.186.121	TLSv1.2	155	Application Data
1024	25.724971	64.233.186.121	192.168.121.171	TCP	60	443 → 52430 [ACK] Seq=25459 Ack=1603 Win=46464 Len=0
1025	25.854591	64.233.186.121	192.168.121.171	TLSv1.2	215	Application Data
1026	25.854901	64.233.186.121	192.168.121.171	TLSv1.2	100	Application Data
1027	25.854971	192.168.121.171	64.233.186.121	TCP	54	52430 → 443 [ACK] Seq=1603 Ack=25666 Win=65792 Len=0
1028	25.855193	192.168.121.171	64.233.186.121	TLSv1.2	11	Application Data
1043	26.039231	64.233.186.121	192.168.121.171	TCP	60	443 → 52430 [ACK] Seq=25459 Ack=1603 Win=46464 Len=0
1362	65.848084	192.168.121.171	64.233.186.121	TCP	60	443 → 52430 [ACK] Seq=25459 Ack=1603 Win=46464 Len=0
1363	66.024767	64.233.186.121	192.168.121.171	TCP	60	443 → 52430 [ACK] Seq=25459 Ack=1603 Win=46464 Len=0
1364	66.210513	192.168.121.171	64.233.186.121	TCP	60	443 → 52430 [ACK] Seq=25459 Ack=1603 Win=46464 Len=0
1365	66.388123	64.233.186.121	192.168.121.171	TCP	60	443 → 52430 [ACK] Seq=25459 Ack=1603 Win=46464 Len=0
1385	71.039179	192.168.121.171	64.233.186.121	TCP	60	443 → 52430 [ACK] Seq=25459 Ack=1603 Win=46464 Len=0
1386	71.223005	64.233.186.121	192.168.121.171	TCP	60	443 → 52430 [ACK] Seq=25459 Ack=1603 Win=46464 Len=0

Frame 1027: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface
 Ethernet II, Src: Micro-St_c1:aa:7f (d8:cb:8a:c1:aa:7f), Dst: Tp-LinkT_33:
 Internet Protocol Version 4, Src: 192.168.121.171, Dst: 64.233.186.121
 Transmission Control Protocol, Src Port: 52430 (52430), Dst Port: 443 (443)

0000 90 f6 52 33 5e 32 d8 cb 8a c1 aa 7f 08 00 45 00 ..R3^2..E.
 0010 00 28 7a d8 40 00 80 06 4a 41 c0 a8 79 ab 40 e9 .(z.@... JA..y.@.
 0020 ba 79 cc ce 01 bb dc 49 e5 2e a6 77 14 9d 50 10 .y.....I ...w..P.
 0030 01 01 2e 06 00 00

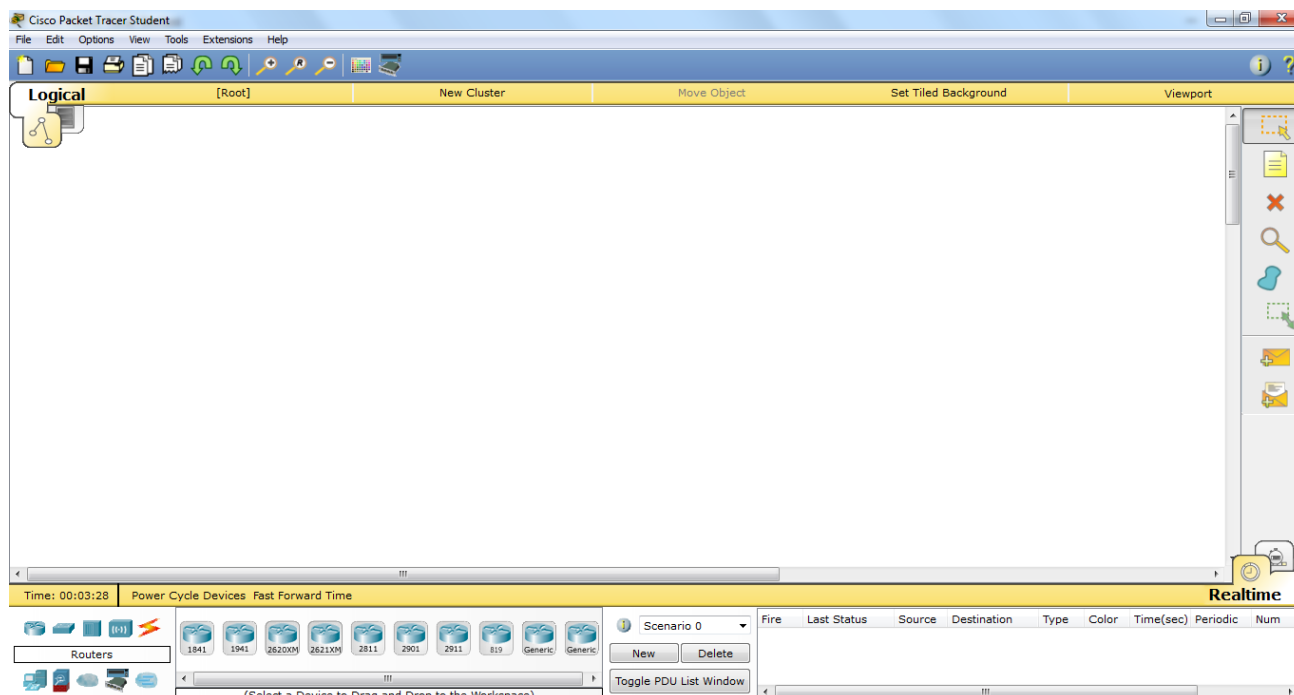
O programa abrirá a seguinte janela:



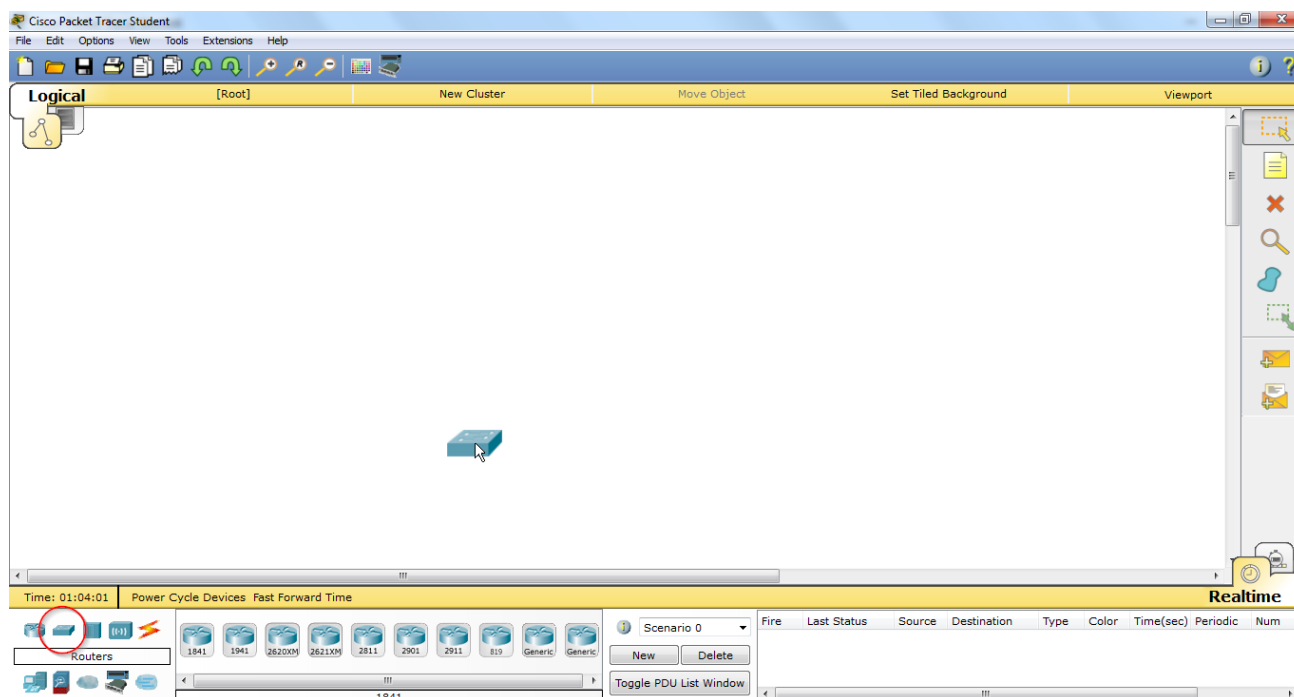
Temos nela uma série de informações com pontos, números e letras, mas nada muito inteligível. Como hackers, não tivemos muito sucesso. Sabemos então que O HTTPS é uma boa alternativa para proteger dados dos usuários. Mesmo assim, vamos aprender a proteger o switch, para evitar que um hacker possa comprometer seu funcionamento e tenha chance de obter informações que não deveria. Podemos fechar o WireShark, pois ele já cumpriu o seu papel.

No GNS3 não conseguimos fazer nenhuma configuração no switch. Por ser apenas uma simulação e não pertencer a nenhum fabricante, não conseguiremos fazer as alterações necessárias para conferir proteção ao switch. Por isso, vamos usar o programa Packet Tracer, que por ser uma simulação de equipamentos da Cisco, tem opções de configuração.

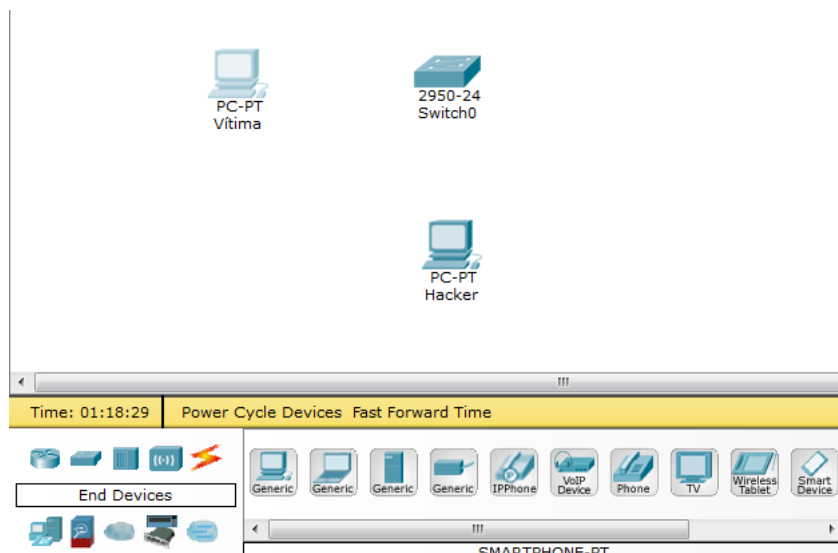
Para instalá-lo, basta baixar o [installer \(https://cursos.alura.com.br/course/seguranca-redes/task/22756\)](https://cursos.alura.com.br/course/seguranca-redes/task/22756). A instalação em si não tem nenhuma especificidade, basta segui-la até o final.



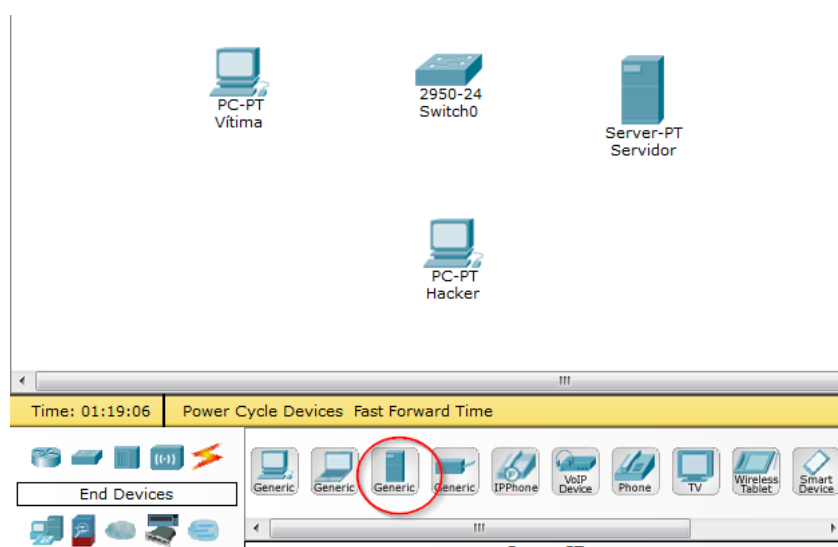
Dentre os equipamentos de rede no canto inferior esquerdo, escolheremos o switch. Basta clicar e arrastar.



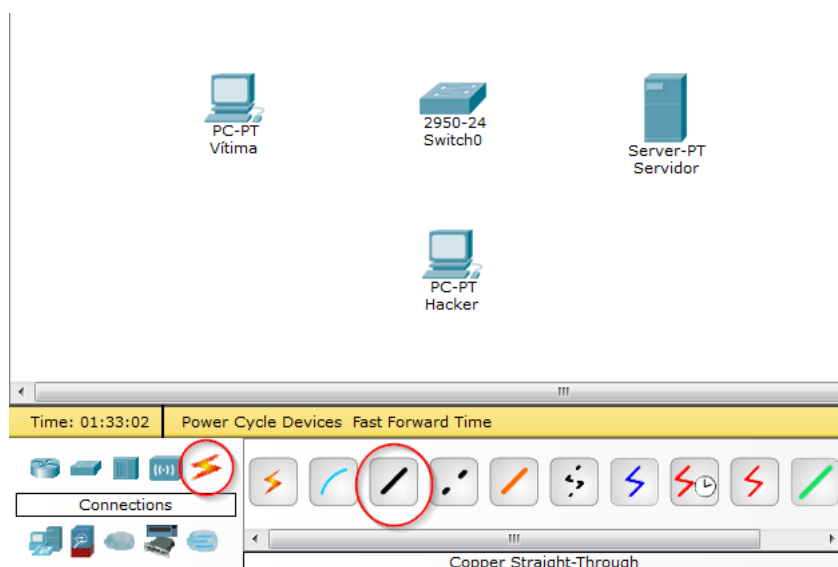
Depois, precisaremos de dois computadores: um para o hacker e um para a vítima. Depois de nomeá-los, ficará assim:



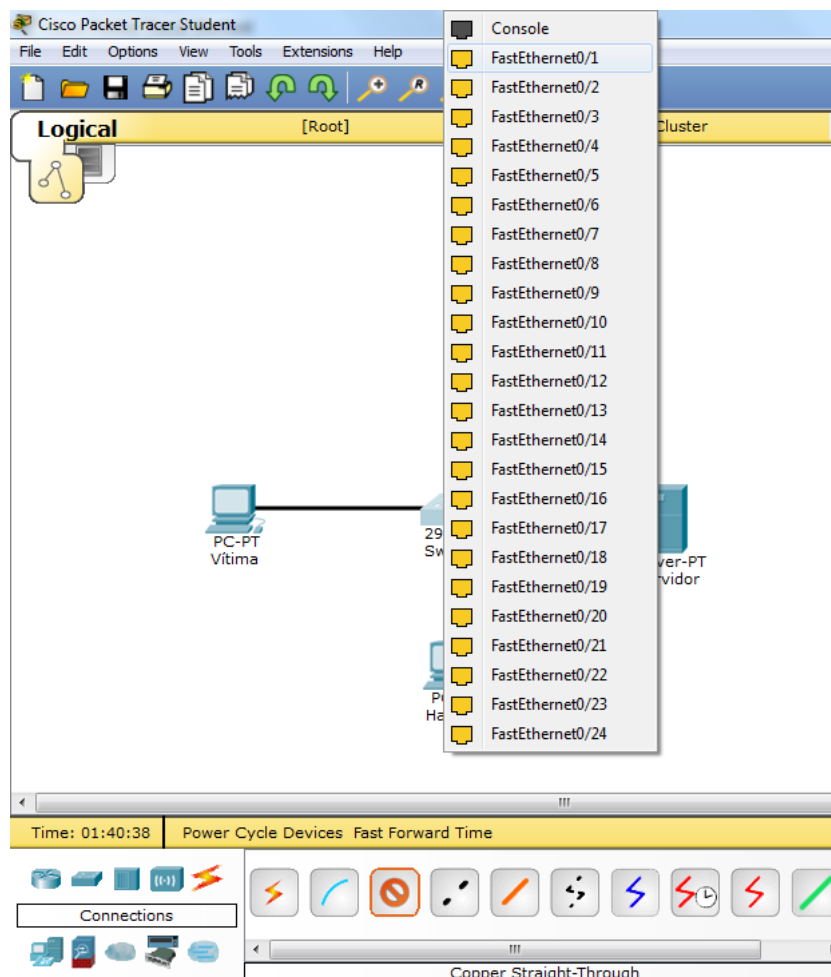
Há também um servidor. Ele ficará disponível também no menu inferior, mas no submenu à direita do anterior.



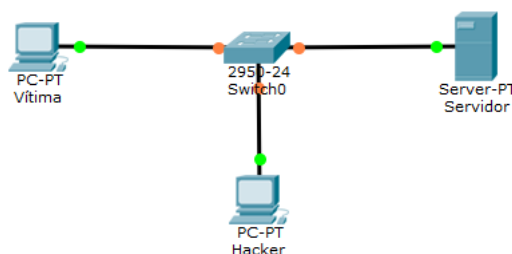
Precisamos conectar todos esses dispositivos. Como eles transmitem e recebem em portas diferentes, devemos fazer conexões diretas entre eles. Então, usaremos um cabo direto. Para isso, clicaremos no símbolo de raio, e a seguir na terceira opção de cabo no submenu, como assinalado a seguir.



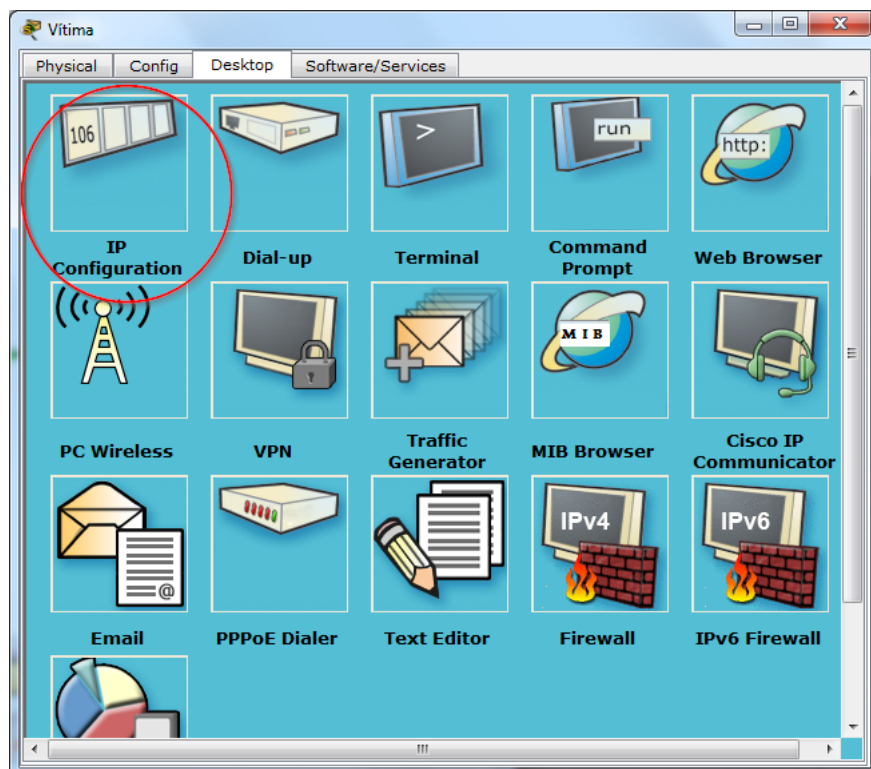
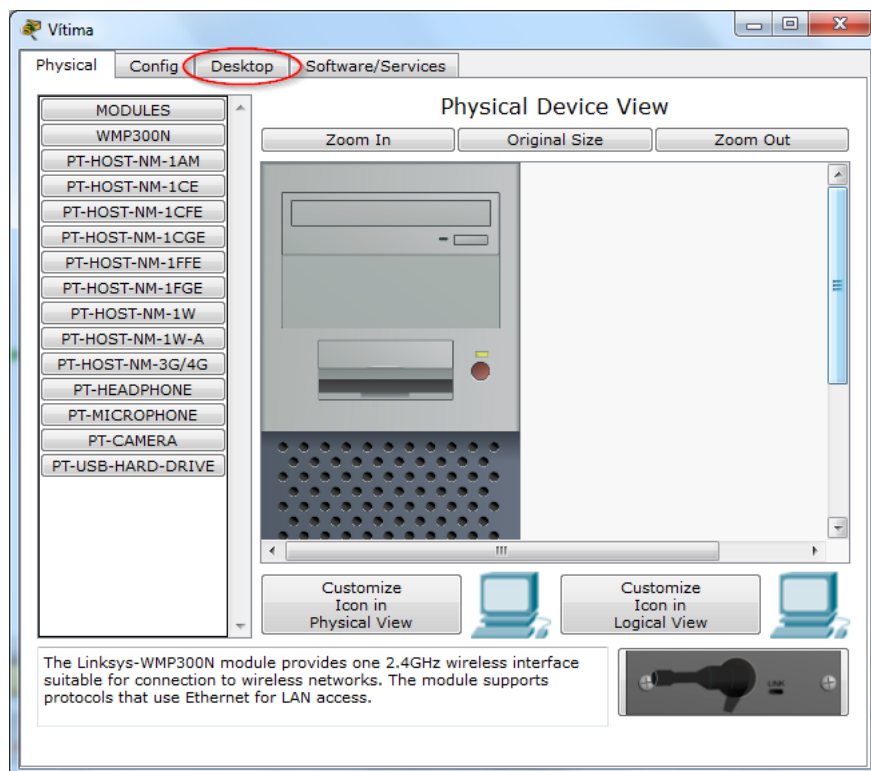
Conectaremos a máquina Vítima ao switch. Conectaremos na porta número 1 e seguiremos em ordem crescente.



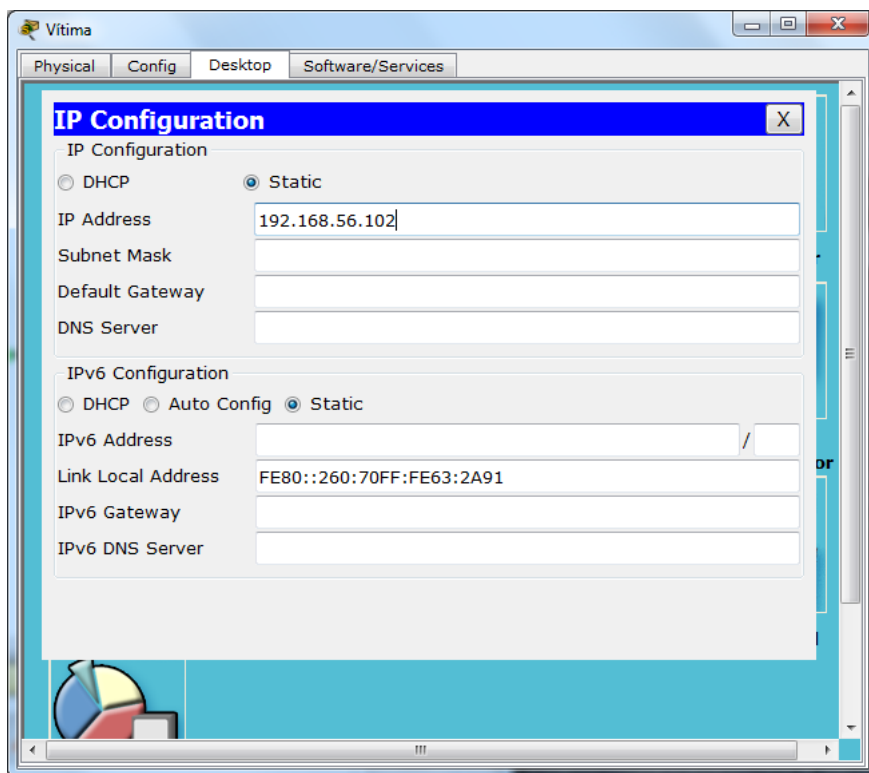
Faremos o mesmo para o Hacker e o Servidor .



Repare que as portas do switch ainda estão vermelhinhas. Isso significa que estão fechadas. Ele demora um pouquinho para inicializar essas portas, então vamos aproveitar esse tempo para atribuir os IPs às máquinas, como fizemos no GNS3. Clicaremos duas vezes sobre o Vítima , e dentro da janela que se abrirá sobre Desktop e depois IP Configuration .



Para que possamos inserir o IP, precisaremos selecionar a opção *Static*. Seguiremos os mesmos IPs que colocamos no GNS3, ou seja, este será 192.168.56.102.

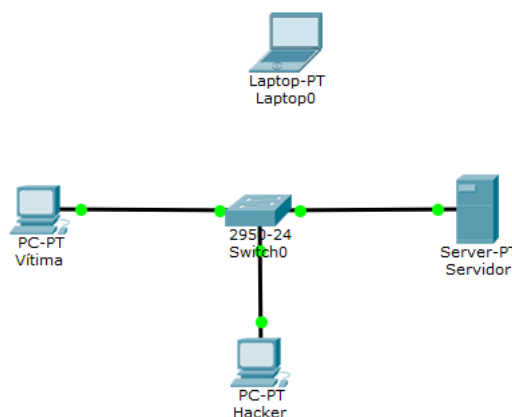


Depois de preencher o campo, basta fechar a janela. Repetiremos para o computador Hacker (192.168.56.101) e para o Servidor (192.168.56.103). Depois disso, nossas máquinas estarão configuradas. Mas como configurar o switch?

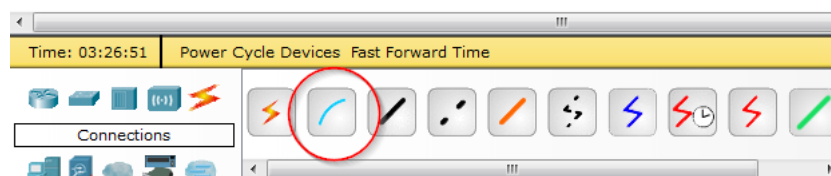
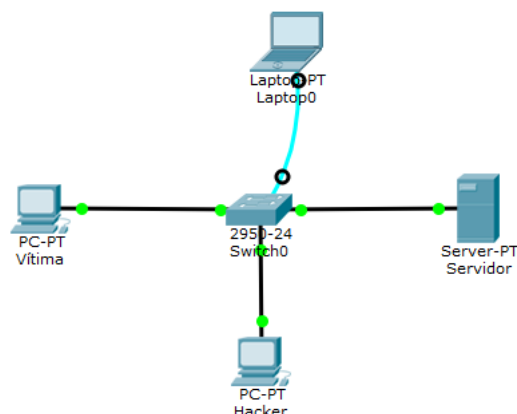
Para fazer a configuração dos aparelhos da Cisco, precisaremos de um cabo especial, o Rollover Cable. É um cabo azul com uma porta RJ45, que conectamos na porta de console do equipamento, e uma porta serial que é conectada ao computador.



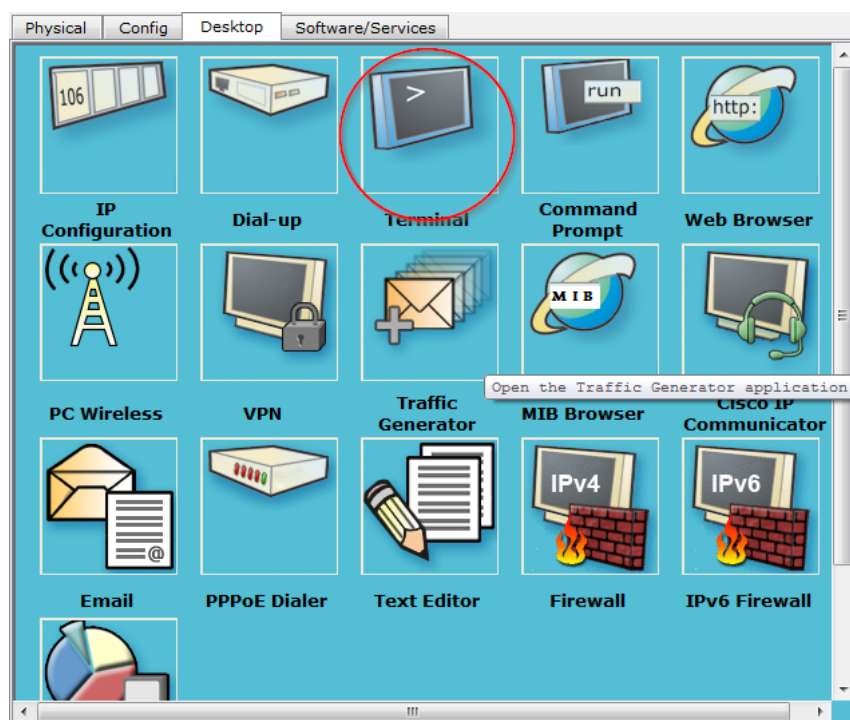
Por um programa terminal, podemos acessar as configurações para alterá-las, assim como fazemos com um roteador. Fazendo como na vida real, levaremos um computador para fazer essa configurações.

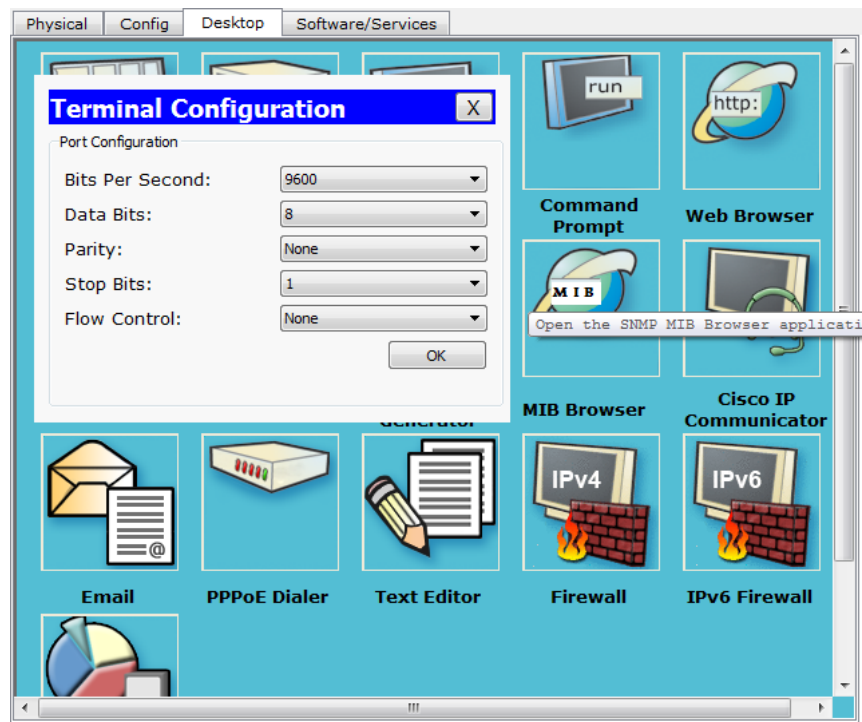


A seguir, iremos conectá-lo com um cabo Rollover, o segundo dentre as opções de cabo. Depois, ele será conectado na porta de console do switch e na porta serial do notebook, a RS 232 .

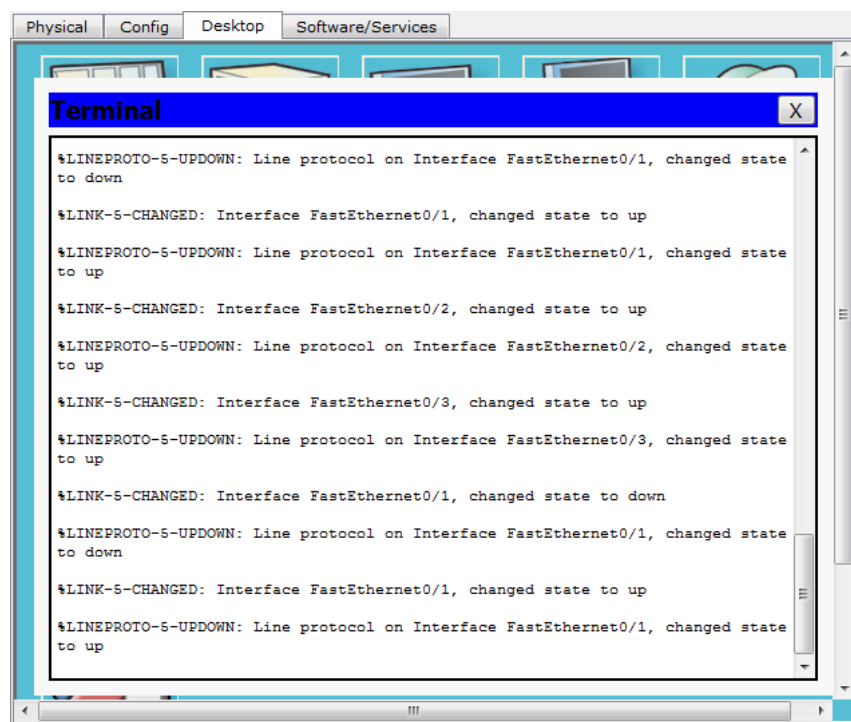


A seguir, clicaremos duas vezes sobre o notebook, e então em Desktop e em Terminal .

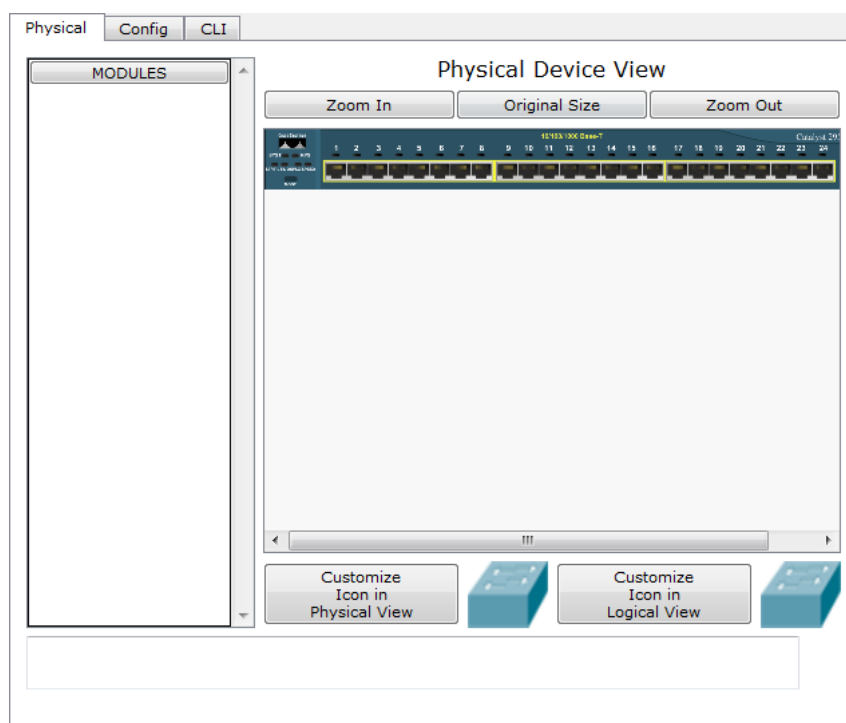




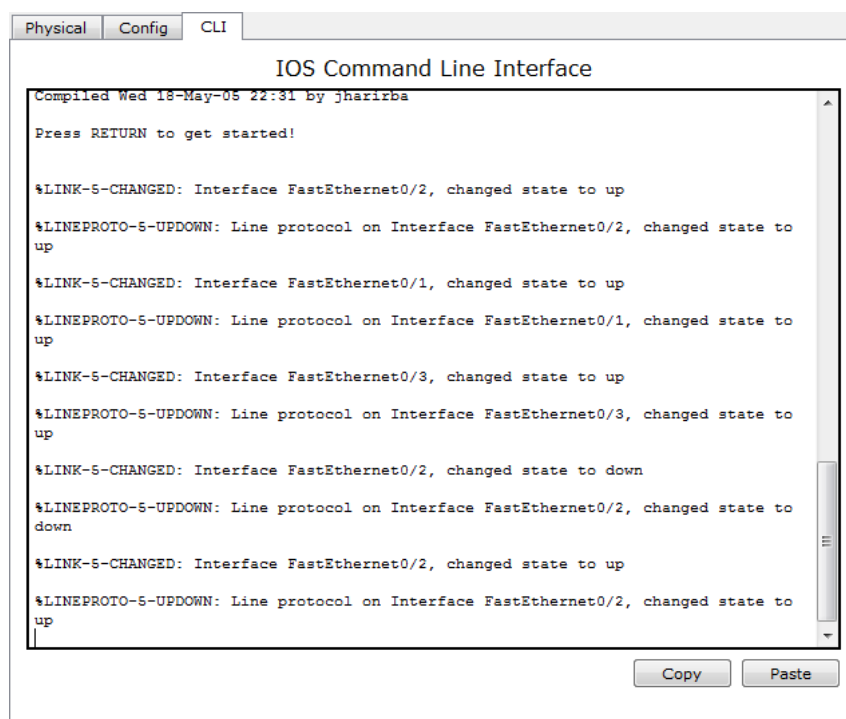
Basta aceitar as configurações e o terminal será aberto.



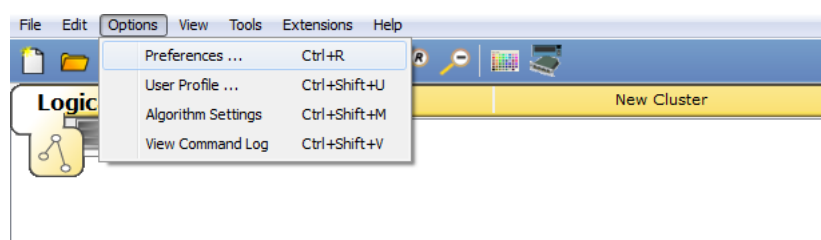
Já conversamos no curso de redes que fazer essas configurações seria um processo um pouco trabalhoso e demorado. Felizmente, o pessoal da Cisco já facilitou a nossa vida e não precisamos fazer esse trabalho. Podemos deletar esse notebook e fazer diferente. Clicaremos duas vezes sobre o switch para abrir a seguinte janela.



Trabalharemos na aba CLI .



Se preferir mudar a cor da fonte e do fundo, vá em Options > Preferences > Font



Interface Administrative Hide Font Miscellaneous Custom Interfaces Publishers

Dialogs

CLI Courier New 8

Headers Verdana 8

Workspace/Activity Wizard

Workspace Verdana 8

Activity Wizard Verdana 8

General Interface

File Menu Tahoma 8

Tab Switches Verdana 8

Tooltips Courier New 8

Button/Labels Verdana 8

Colors

Router IOS Text Black

Router IOS Background White

PC Console Text White

PC Console Background Black

Apply Reset

Interface Administrative Hide Font Miscellaneous Custom Interfaces Publishers

Dialogs

CLI Courier New 8

Headers Verdana 8

Workspace/Activity Wizard

Workspace Verdana 8

Activity Wizard Verdana 8

General Interface

File Menu Tahoma 8

Tab Switches Verdana 8

Tooltips Courier New 8

Button/Labels Verdana 8

Colors

Router IOS Text Green

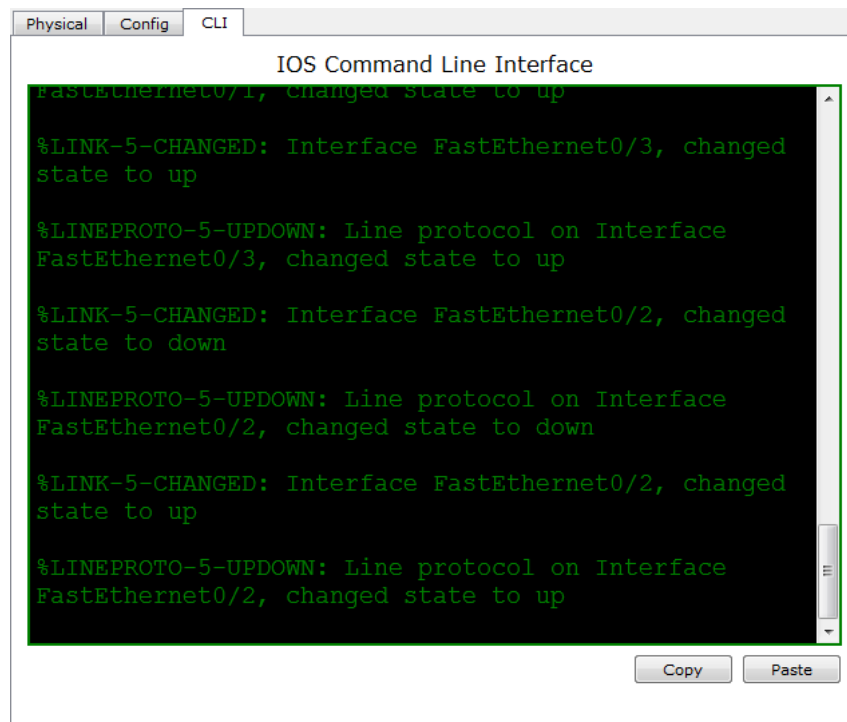
Router IOS Background Black

PC Console Text White

PC Console Background Black

Apply Reset

Escolhi deixar as fontes em verde com tamanho 14 e o fundo em preto. Ficará assim:



Vamos maximizar essa janela para usá-la melhor. Sabemos que o switch armazena os endereços mac em sua memória, para identificar qual está conectado a qual porta. Tentaremos ver essa tabela para tentar entender melhor como ela funciona. Digitaremos:

```
Switch>
Switch>enable
```

Ele entrará no modo privilégio.

```
Switch>
Switch>enable
Switch#
```

Nosso objetivo é ver a tabela de endereços mac. Então precisamos pedir que ele nos mostre (show) algo relacionado a mac- . Podemos dar um Tab para autocompletar.

```
Switch>
Switch>enable
Switch#show mac-
```

Ele nos devolverá o seguinte.

```
Switch>
Switch>enable
Switch#show mac-
Switch#show mac-adrress-table
```

Ao dar Enter , teremos o seguinte:


```
Switch>
Switch>enable
Switch#show mac-
Switch#show mac-address-table
          Mac Address Table
-----
Vlan      Mac Address      Type      Ports
----      -
```

Ainda não há nada nela, pois o switch acabou de ser conectado e ainda não sabe identificar onde está ninguém. Portanto, temos que pedir para os dispositivos se comunicarem para começar a popular essa tabela.

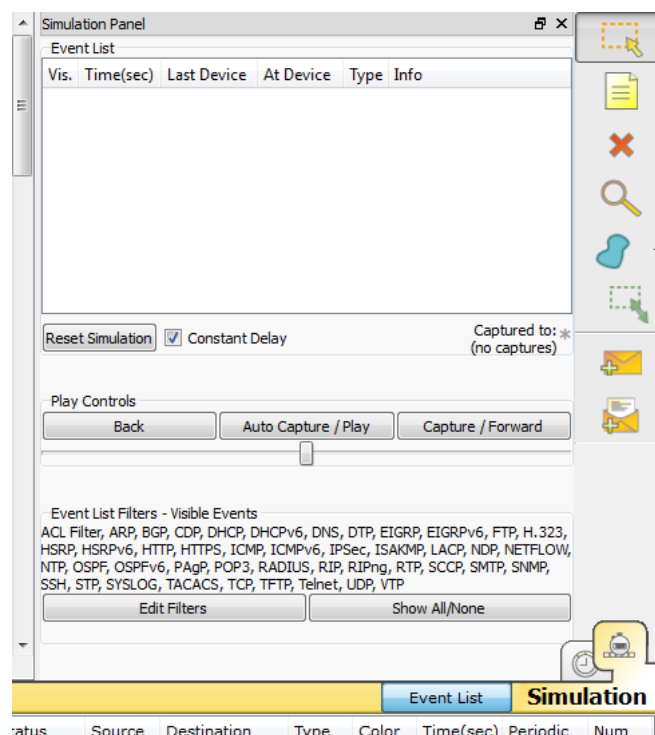
Quando a vítima vai se comunicar com o servidor, ela também não sabe onde ele está localizado. Então, precisa sair perguntando para todo mundo. Se abrirmos o prompt da vítima, (clicando duas vezes sobre ele e em Desktop > Command Prompt) veremos que ele busca em uma tabela arp . No prompt dele digitaremos:

```
PC>arp -a
```

Esse comando arp -a deve mostrar todas as entradas ARP que esse computador tem. Ao dar enter, veremos:

```
PC>arp -a
No ARP Entries Found
```

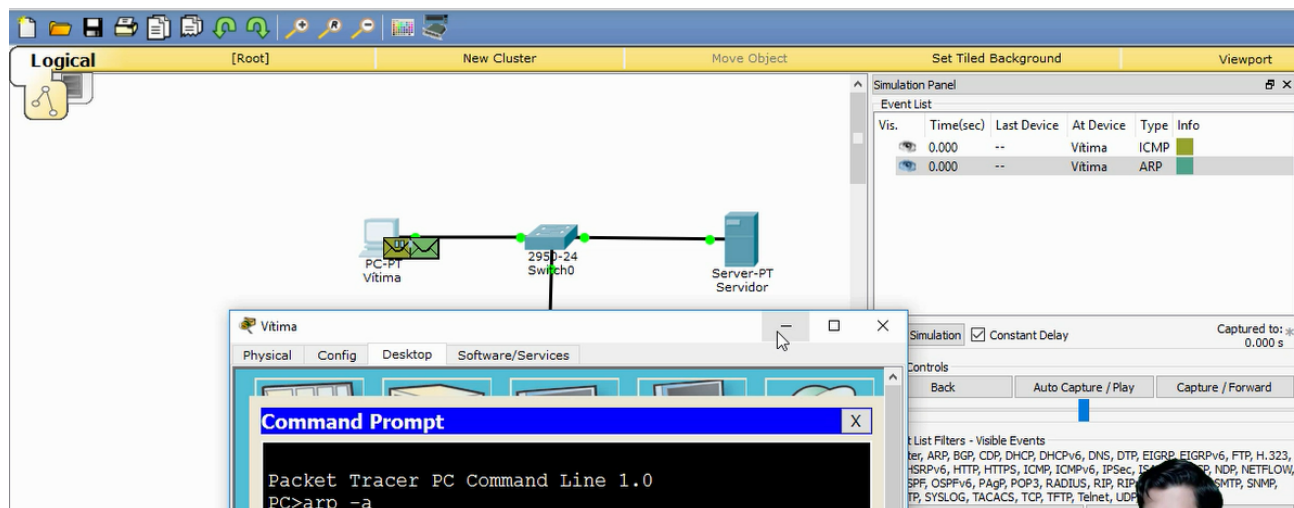
Ele também não tem nada, nem mesmo a referência do IP 192.168.56.103 , que é o do servidor. Então, esse computador deve mandar um protocolo ARP para todos os da rede, perguntando quem tem esse IP. Mudaremos a aba para Simulation no canto direito da tela, para ver todas as etapas do que acontecerá, bem como o que vai popular em cada lugar.



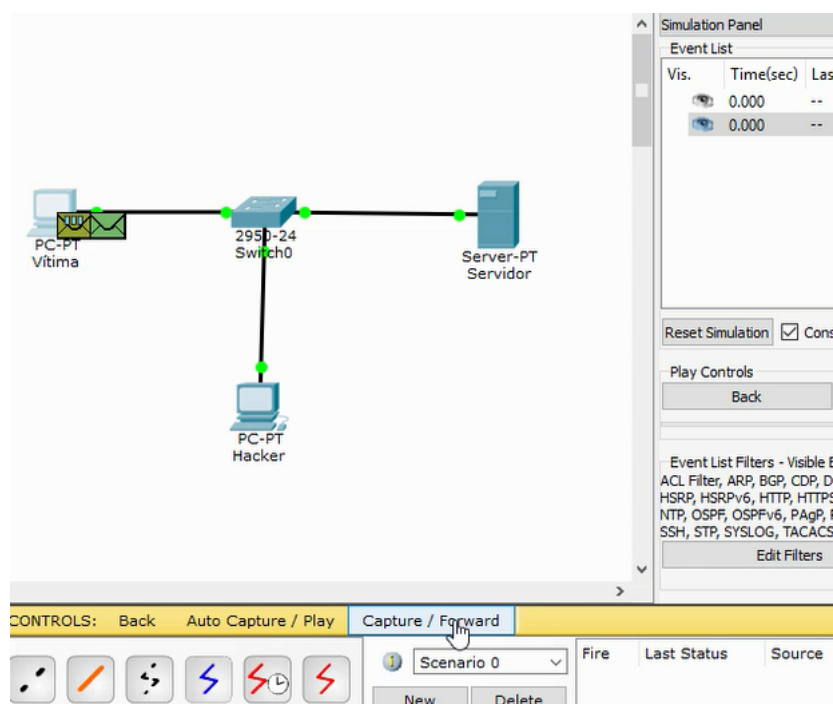
Faremos um ping para o servidor.

```
PC>arp -a
No ARP Entries Found
PC>ping 192.168.56.103
Pinging 192.168.56.103 with 32 bytes of data:
```

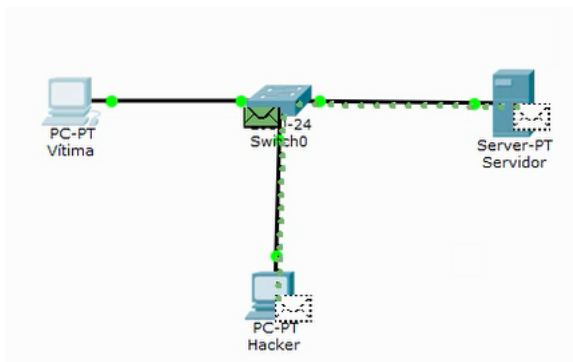
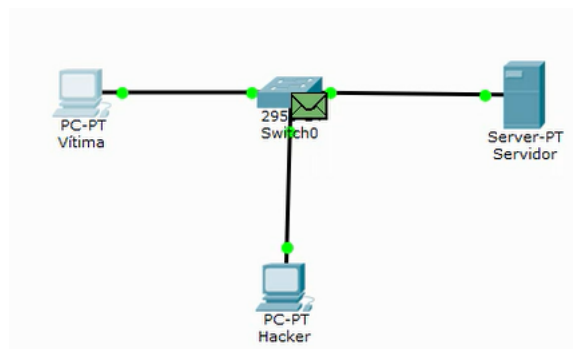
O computador da vítima manda um protocolo ARP para todo mundo, perguntando quem tem o IP do servidor.



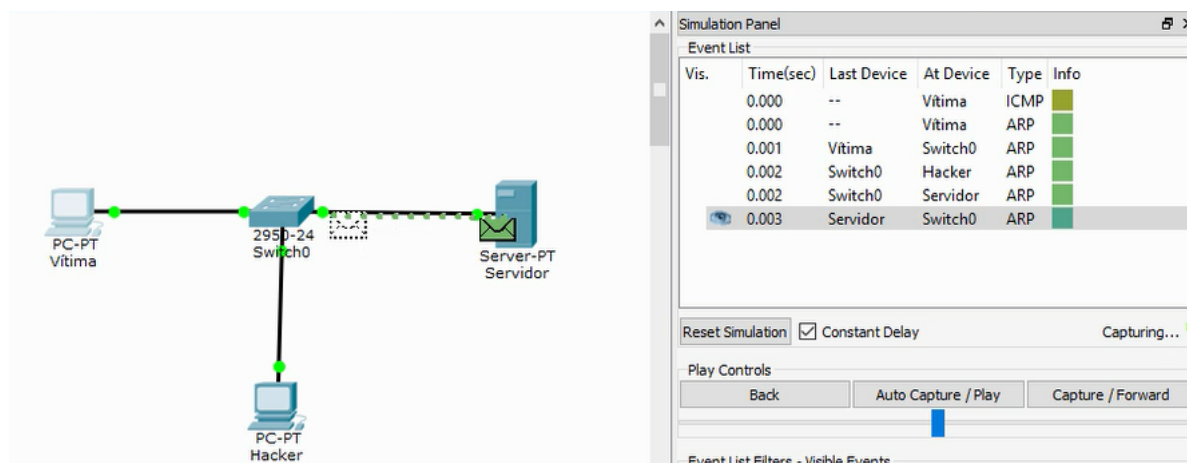
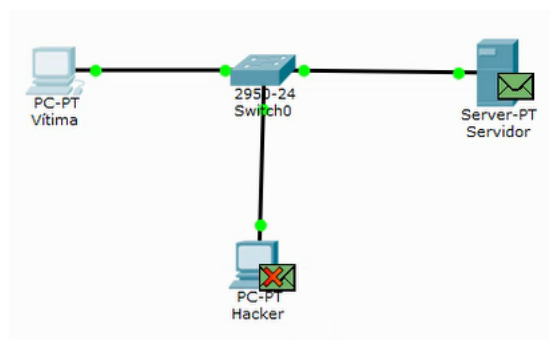
Podemos clicar em Capture / Forward , para acelerar o processo.



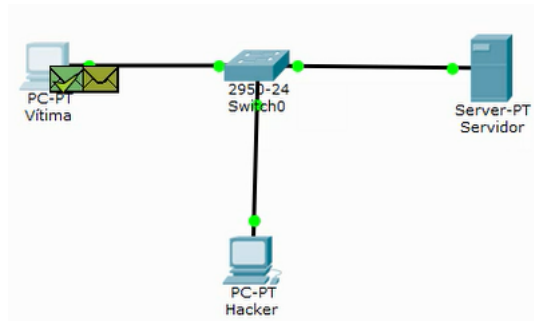
Quando a mensagem chega ao switch, ele também não sabe onde está esse IP. Então, ele pergunta para todas as suas portas.



Assim, ao receber a mensagem, o Hacker responde que não tem esse IP. Mas o servidor avisará que esse é o seu IP, e devolverá seu endereço mac, passando pelo switch novamente.



Assim, a informação sai do Vitima , passa pelo switch, vai para o servidor e retorna pelo switch.



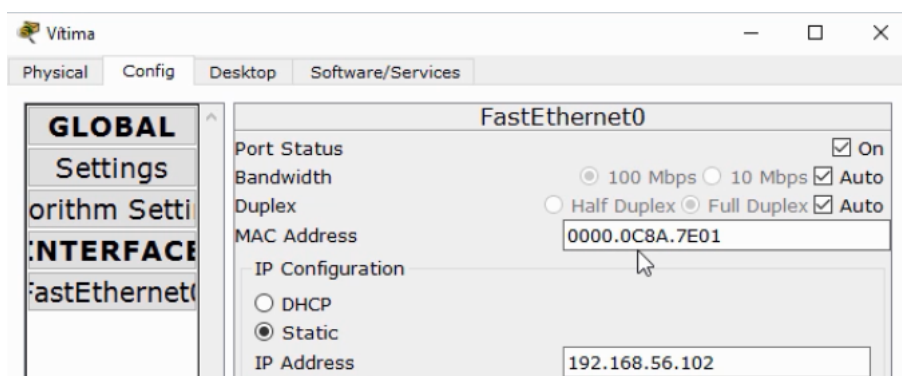
Com essa comunicação realizada, se pedirmos ao switch `show mac-address-table`, devemos conseguir ver o endereço mac da Vitima e do Servidor. Afinal, o ping passou pelo switch. Voltaremos à aba CLI do switch e daremos seta para cima, para repetir o comando anterior.

```
Switch#show mac-address-table
```

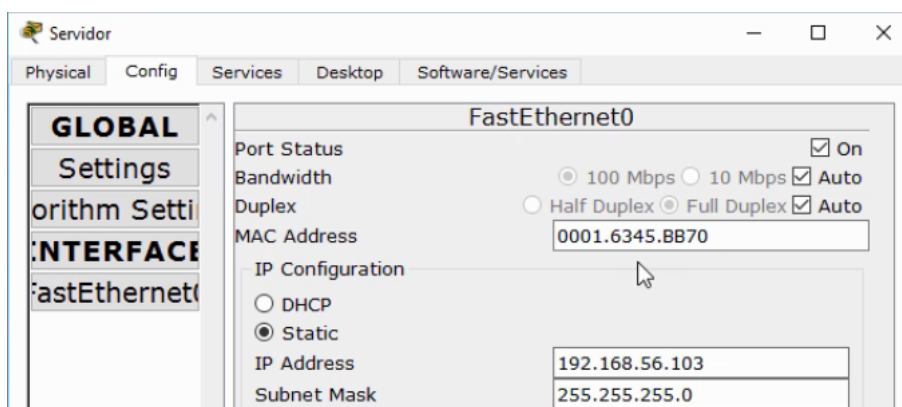
Mac Address Table

Vlan	Mac Address	Type	Ports
1	0000.0c8a.7e01	DYNAMIC	Fa0/1
1	0001.6345.bb70	DYNAMIC	Fa0/3

Podemos ver que a porta Fa0/1, ou FastEthernet0/1, está com o endereço mac 0000.0c8a.7e01. E a porta Fa0/3 está com o 0001.6345.bb70. Se quisermos confirmar essa informação, basta clicarmos duas vezes sobre o Vitima e em Config > FastEthernet.



É o mesmo endereço mac. Confirmando o do servidor, temos:



Temos certeza, então, de que o switch conseguiu apreender os endereços macs que esperávamos. Podemos parar a simulação.

A vítima não tinha a tabela ARP preenchida. Se voltarmos para o prompt, devemos ter algo nela. Afinal, tivemos o retorno do servidor via switch.

```
PC>arp-a
Internet Address      Physical Address      Type
192.168.56.103        001.6345.bb70         dynamic
```

Agora a tabela ARP tem um mapeamento com um IP e seu endereço mac correspondente. Então, da próxima vez em que Vítima precisar se comunicar com o Servidor, não será necessário enviar um protocolo ARP novamente. Já sabemos que tem o IP, não é preciso mandar a pergunta para todos os dispositivos da rede.

E como proteger o switch de o Hacker enviar aqueles endereços mac falsos. Precisaremos habilitar a segurança da porta, ou no inglês *port security*. Sabemos que o Hacker está na porta Fa0/2.

Vamos clicar no switch e configuraremos a interface. Para isso:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

A interface que queremos configurar é a Fa0/2. Assim:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fa0/2
Switch(config-if)#
```

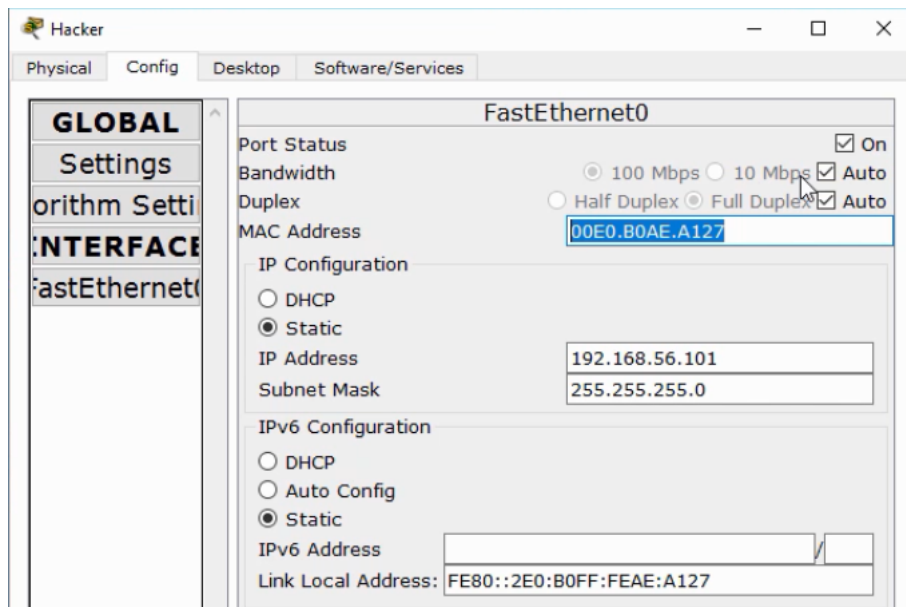
O conteúdo dos parênteses (config-if) indica que acessamos a configuração da interface. Temos que mudar a forma que essa porta trabalhará, avisando que ela está conectada a um dispositivo final. Colocaremos *switchport*, avisando que está trabalhando no modo de acesso (*mode access*).

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode access
```

Agora temos que habilitar a segurança da porta, com o *port-security*.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
```

Precisamos proteger essa porta de maneira a evitar aquela enxurrada de endereços mac. Podemos habilitar essa porta para somente um endereço mac. Como ele é um número de série e cada computador tem o seu, se outra máquina se conectar a essa porta, ela terá outro endereço mac. A teoria é que o switch não aceitará nessa porta um endereço mac diferente do que configurarmos. Para ilustrar isso, usaremos o computador do hacker. Clicaremos duas vezes sobre ele e na aba Config > FastEthernet.



Copiaremos esse endereço mac e voltaremos para as configurações do switch.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security ?
    mac-address      Secure mac address
    maximum          Max secure addresses
    violation         Security violation mode
    <cr>
```

Só queremos que o 00E0.B0AE.A127 seja o único aceito como endereço mac. Então:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security ?
    mac-address      Secure mac address
    maximum          Max secure addresses
    violation         Security violation mode
    <cr>
Switch(config-if)#switchport port-security mac-address 00E0.B0AE.A127
```

Agora, se usarmos o comando Ctrl + Z e pedir para show port-security, veja o que encontraremos:

```
Switch#show port-security interface fa0/2
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
```



```
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

A Port Security está habilitada, e a resposta dele à violação será Shutdown, ou seja, desligar a porta. Se ele perceber outro endereço mac, desligará imediatamente. Vamos ver se isso é verdade?

Clicaremos duas vezes sobre o Hacker e abriremos o prompt de comando para testar um ping.

```
PC>ping 192.168.56.103
```

```
Pinging 192.168.56.103 with 32 bytes of data:
```

```
Reply from 192.168.56.103: bytes=32 time=0s
```

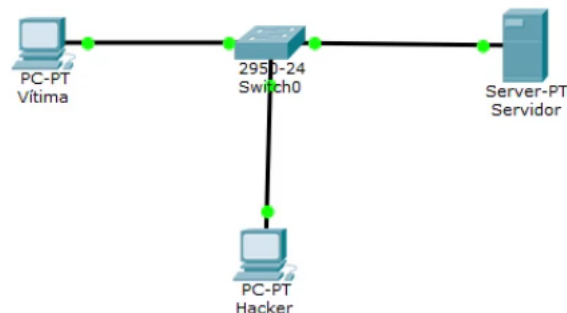
```
TTL=128
```

```
Reply from 192.168.56.103: bytes=32 time=1s
```

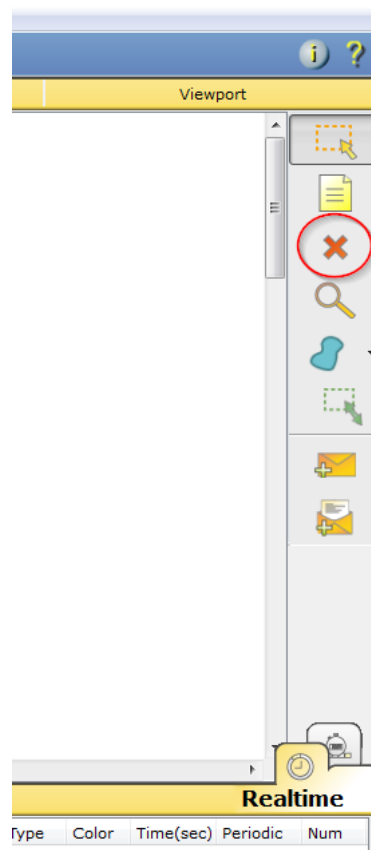
```
TTL=128
```

```
...
```

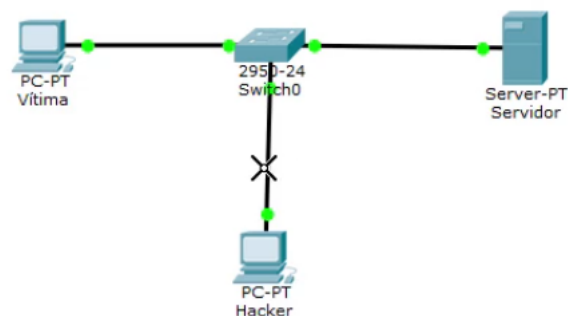
A comunicação está funcionando bem e as portas estão verdinhas, indicando seu funcionamento.



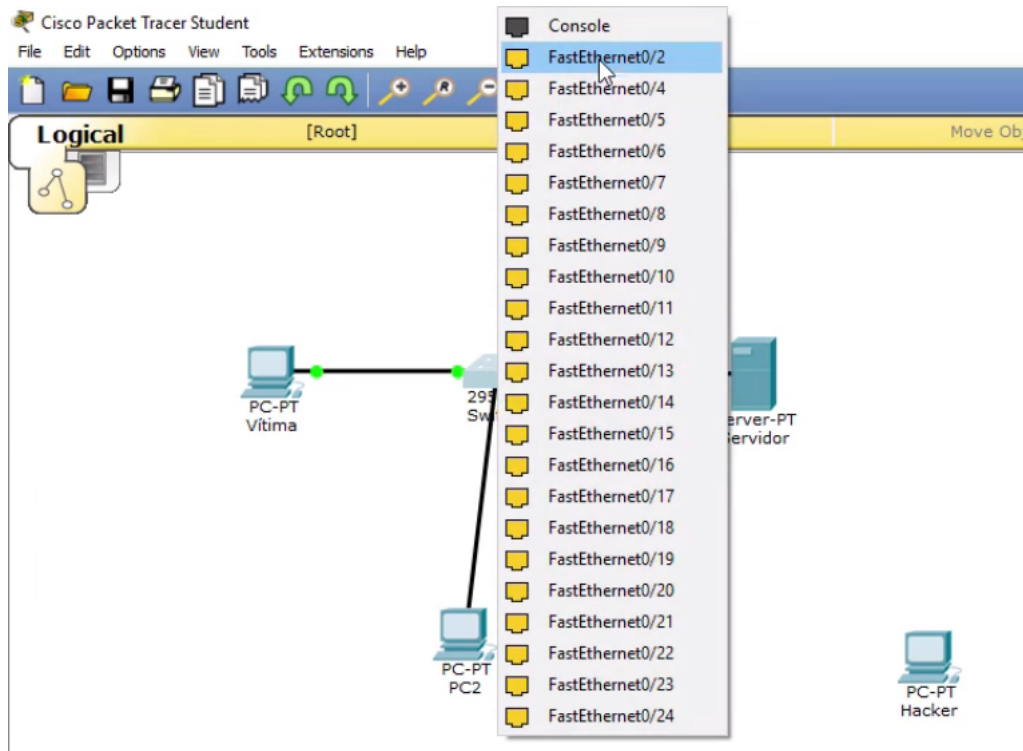
Conectaremos outro computador, com um IP diferente a essa porta. Para isso, iremos deletar a conexão entre o switch e Hacker. Há um ícone de x na barra lateral do programa.



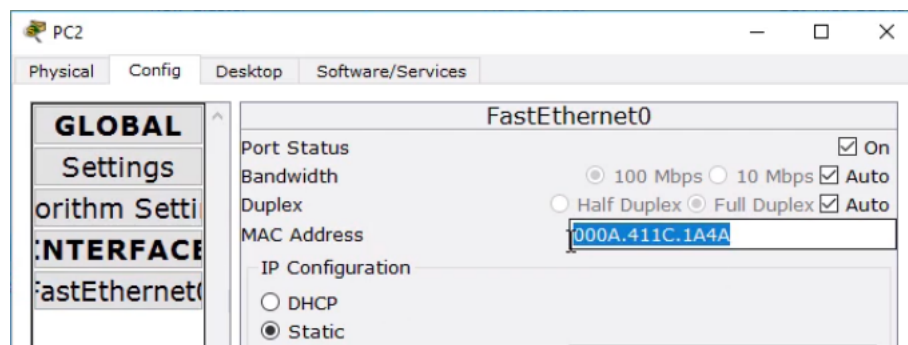
Clicaremos nele, e em seguida na conexão entre Hacker e o switch, deletando-a.



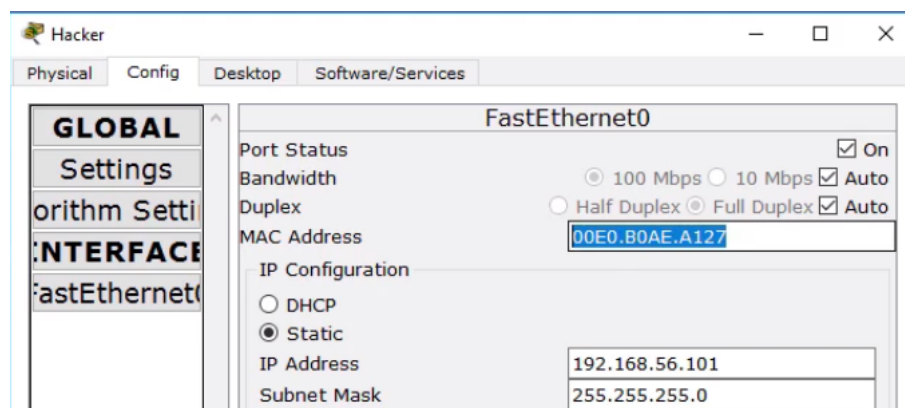
Depois, vamos arrastar o Hacker para o lado, e adicionaremos uma nova máquina em seu lugar.



Ele será conectado à porta `fa0/2`, pois foi essa que configuramos e, portanto, essa que precisamos testar. Essa conexão demora um pouco para ser carregada, pois a simulação do programa é bem próxima da vida real. Enquanto isso, clicaremos duas vezes sobre esse novo computador para configurá-lo. Seu endereço de IP será `192.168.56.102`. Em Config podemos ver seu endereço mac: `000A.411C.1A4A`.



Vamos conferir qual é o endereço mac do Hacker ?

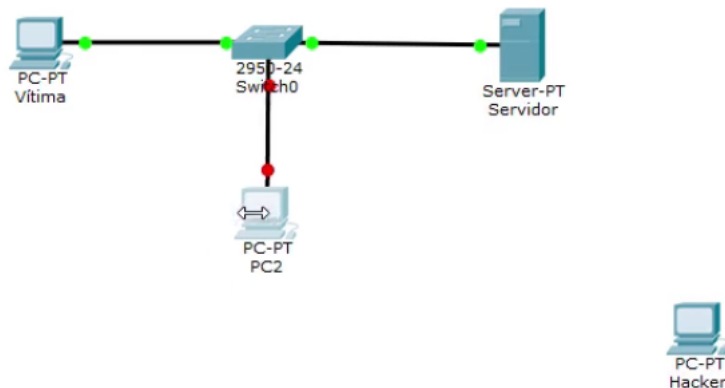


Comparando os dois, sabemos que `000A.411C.1A4A` é bem diferente de `00E0.B0AE.A127`. Como a porta está configurada para aceitar apenas a do Hacker, se iniciarmos uma comunicação com esse computador, a porta deve desligar. Para ter certeza, iremos ao prompt de comando do computador e faremos um `ping`.

```
PC>ping 192.168.56.103
```

```
Pinging 192.168.56.103 with 32 bytes of data:
```

Quando olhamos novamente para o switch, veja só o que aconteceu:



A porta está desligada! Quando abrirmos novamente o CLI do switch, veremos:

```
Switch#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
```

A fa0/2 foi administrativamente desabilitada. Se pedirmos para ver a interface de segurança dessa porta, teremos:

```
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
```

```
Switch#show port-security interface fa0/2
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 000A.411C.1A4A:1
Security Violation Count : 1
```

Note que a `Security Violation Count` agora é `1`. Isso mostra que o switch detectou um endereço mac diferente do programado, o que é considerado uma violação de segurança.

Desta maneira, aquele ataque que enche a memória do switch com endereços mac falsos deixará de ser efetivo. Só precisamos configurar a porta para aceitar um endereço específico, e caso ela receba vários endereços falsos, simplesmente será desabilitada.