01

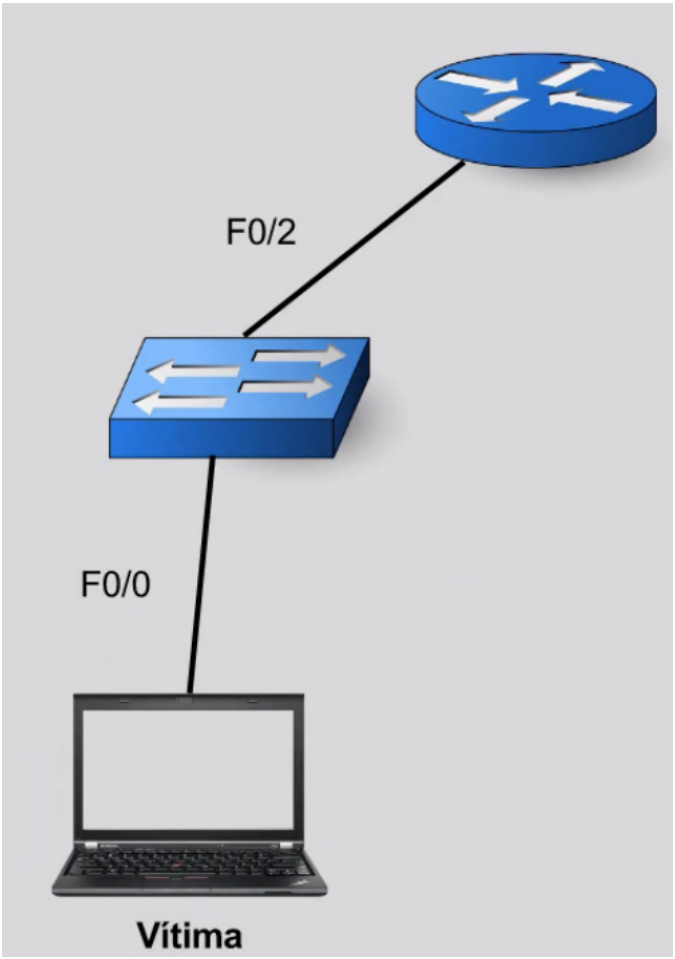
Como o protocolo ARP trabalha

Transcrição

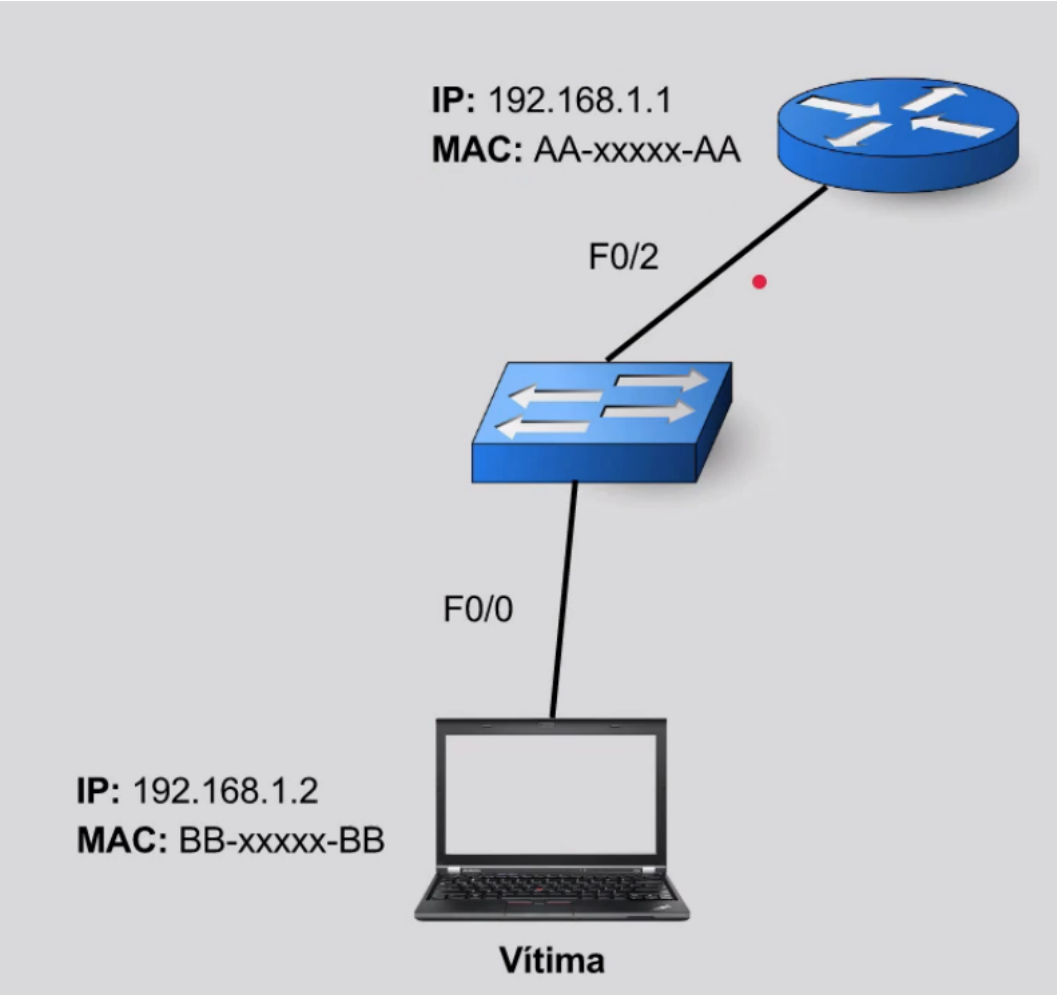
Anteriormente, vimos como o protocolo `ARP` ajuda na comunicação e mapeamento dos endereços IPs para os endereços mac. Vamos ver um pouco mais a fundo como esse protocolo funciona.

Suponha que João queira acessar um site de notícias, o Uol, por exemplo. E, pelo fato de esse site não estar na mesma rede que eu, ele precisa passar a informação pelo *default gateway*, o roteador. Ele encontrará uma forma de se comunicar com o servidor da Uol.

Teremos, então, o computador da vítima conectado a um switch, que estará conectado a um roteador.

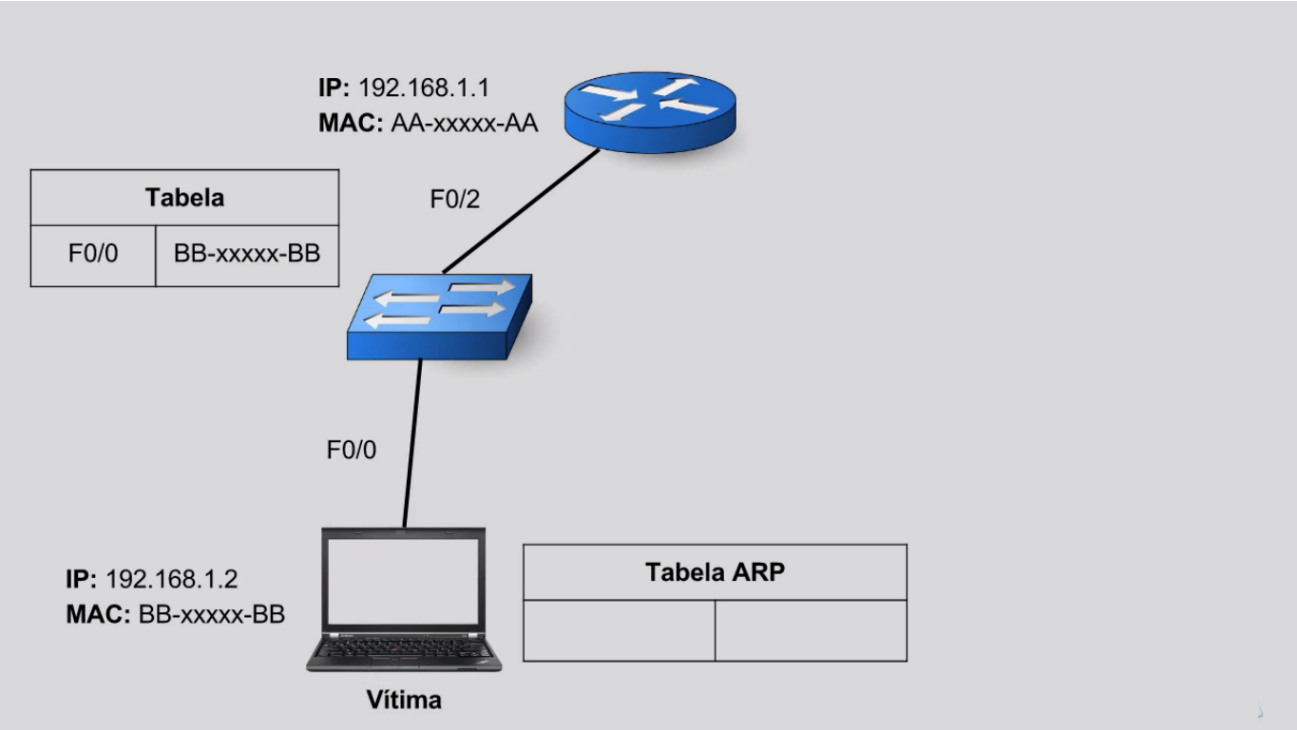


Atribuiremos endereços mac e IPS a eles. O computador da vítima terá IP `192.168.1.2` e mac `BB-xxxxx-BB` ; o roteador terá IP `192.168.1.1` e mac `AA-xxxxx-AA` .



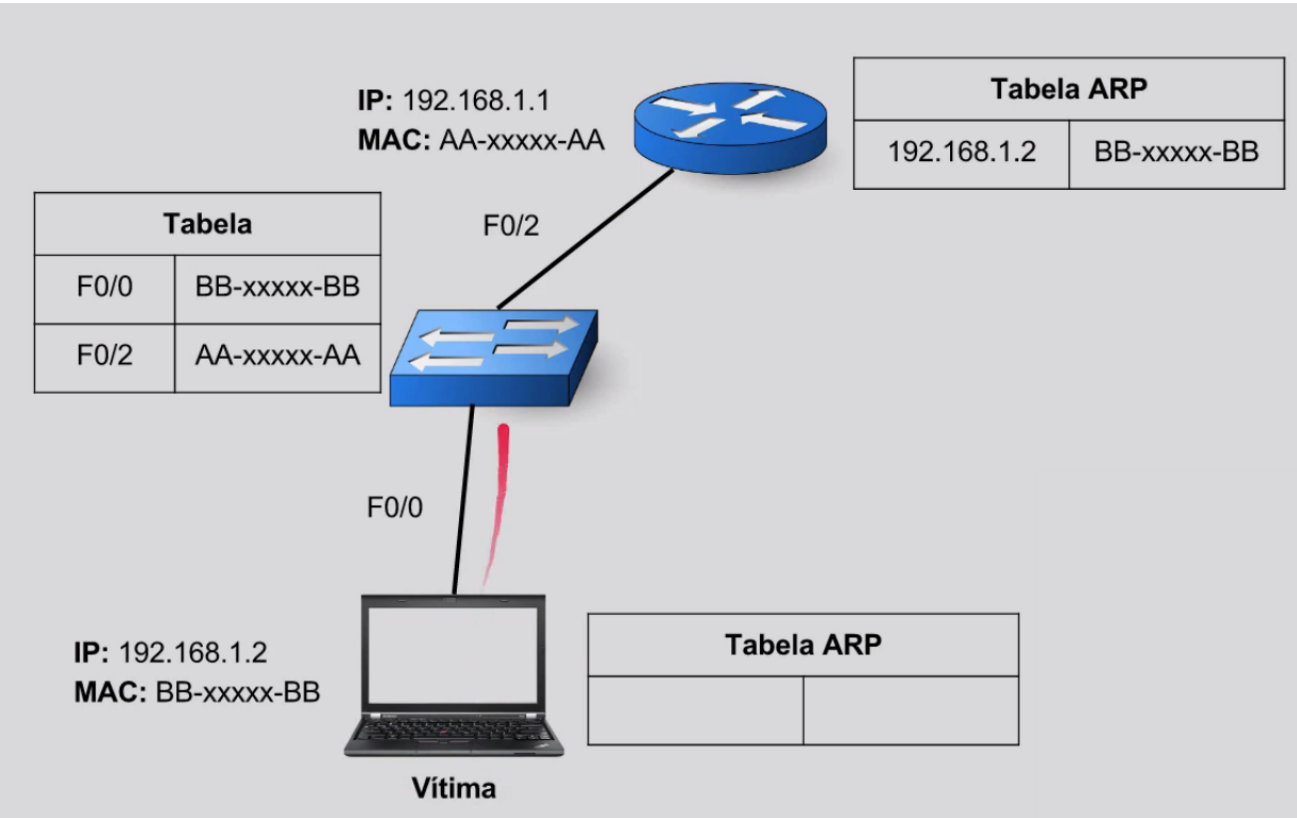
Quando o computador da vítima quiser mandar informação para o roteador, ele precisará olhar sua tabela `ARP`. Mas, por enquanto, ela está vazia, e não sabemos o mapeamento do endereço IP com o endereço mac referente ao roteador. Assim, ele precisará perguntar para todo mundo para tentar descobrir qual é o endereço mac do roteador.

Assim, o computador lançará um protocolo `ARP` ao switch, que por sua vez, por não ter a resposta, perguntará a todas as suas portas quem tem o endereço desejado. Quando o computador se comunica com o switch, fornece o seu endereço mac para ele, que sabe que o pc está conectado à porta `F0/0`. A essa altura, as tabelas dos dispositivos estão assim:

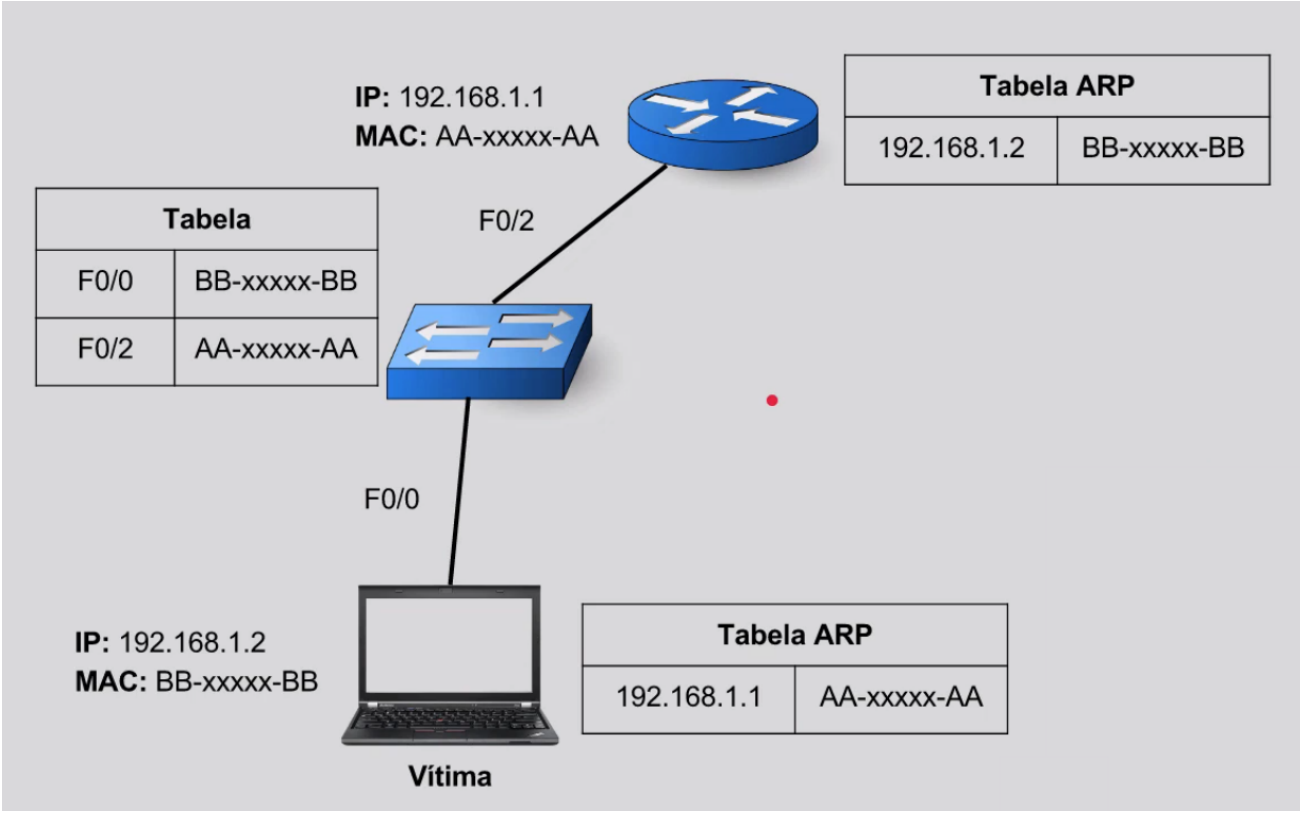


Quando o switch precisar devolver o endereço mac do roteador para o computador, já saberá onde cada um está. Quando o protocolo chegar ao roteador, ele se identificará como o portador do IP que o switch está buscando e devolverá seu endereço mac para permitir a comunicação. Então, ele aproveitará para atualizar sua tabela `ARP` que quem o está buscando tem IP `192.168.1.1` e endereço mac `BB-xxxxx-BB`.

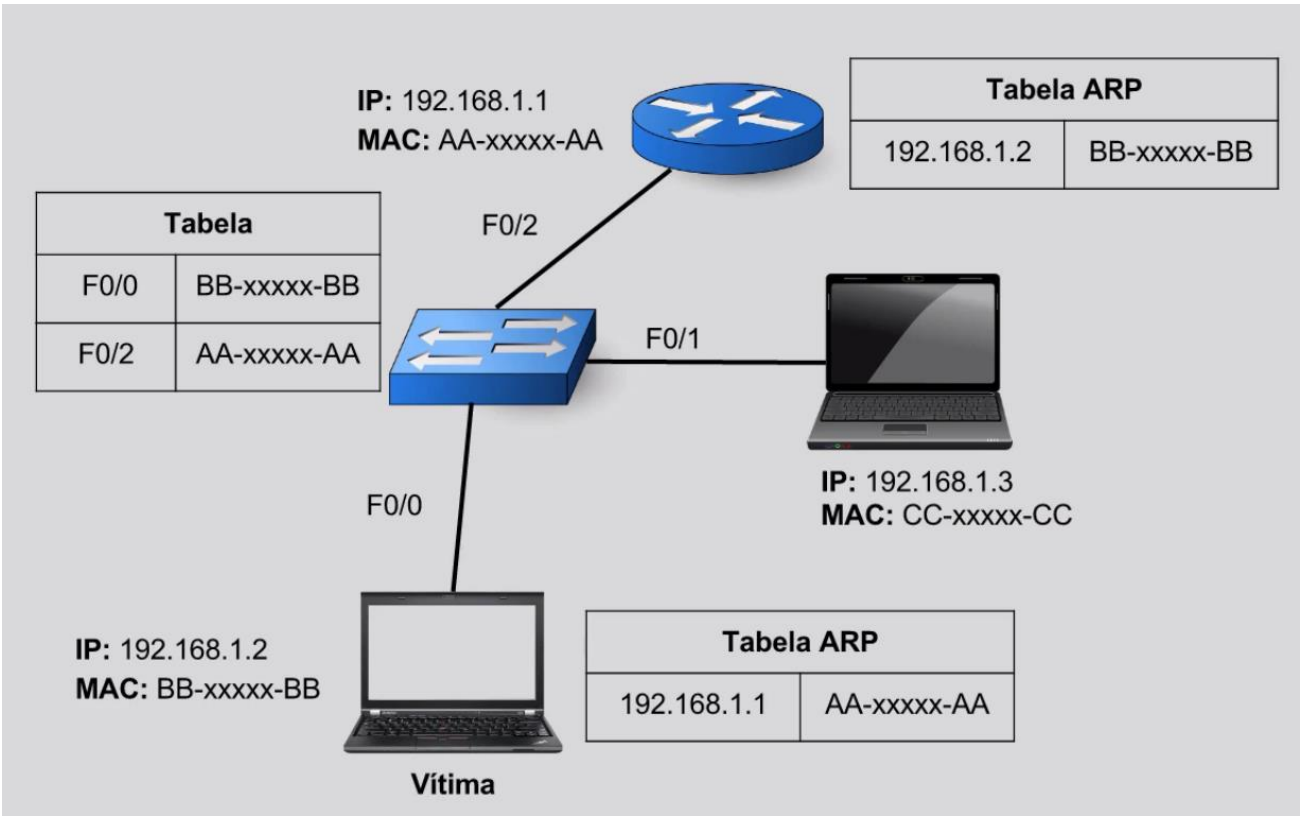
Por sua vez, o switch aproveitará essa comunicação para salvar o endereço mac do roteador em sua tabela. As tabelas ficarão assim:



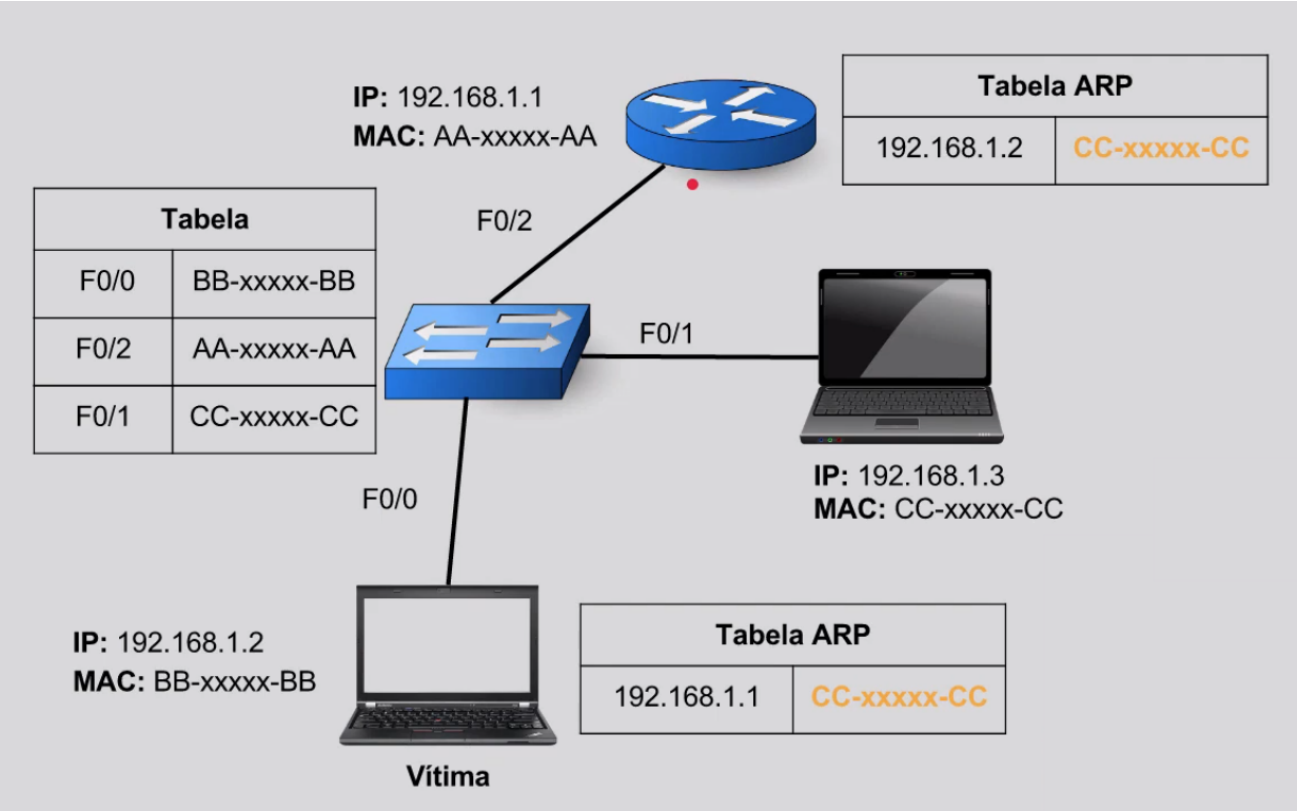
O switch sabe que a mensagem do `AA-xxxxx-AA` é destinado ao `BB-xxxxx-BB`, que já está em sua tabela, lembrando que o switch lê apenas endereços mac. Agora o computador saberá que o IP `192.168.1.1` está pareado com o endereço mac `AA-xxxxx-AA`.



O protocolo `ARP` não verifica quem envia cada informação – e um hacker pode se aproveitar disso. Ele vai se colocar no meio dessa comunicação, na porta `f0/1` e tentar enganar tanto a vítima quanto o roteador.



O hacker dirá para a vítima que o IP que ele está buscando possui o endereço mac `CC-xxxxx-CC`, que é seu próprio mac. E ele insistirá na mensagem, como uma criança pequena com os pais no supermercado, que insiste até que eles comprem o produto desejado. Usando a persistência do protocolo `ARP`, o hacker enviará essa mensagem até que a tabela `ARP` da vítima esteja atualizada com o seu endereço mac. Com essa comunicação, o switch vai armazenar a informação de que o endereço mac `CC-xxxxx-CC` está na porta `f0/1`. Ele repetirá o processo até convencer o roteador de que o endereço mac correspondente ao IP `192.168.1.2` é também o seu, `CC-xxxxx-CC`.



Assim que os dois dispositivos estiverem convencidos de que o endereço mac do hacker é o que eles procuram, ele passará a intermediar toda a comunicação. Suponha que a vítima queira acessar um site da internet, como a da Uol. Sabemos que ela terá que passar a informação para o roteador, usando como referência o endereço mac de sua tabela `ARP`. Entretanto, o endereço que ela tem agora é o do hacker! Assim, ele encaminha esse pacote de informação para o hacker, via switch. Este, por sua vez, olha esse pacote de informação e o endereço mac, que é tudo que ele consegue ler, e, sabendo que o endereço indicado está na porta `f0/1`, manda o pacote para lá. Ou seja, direto para o hacker.

O hacker vai agir como um cara bacana, e vai deixar a vítima acessar as páginas desejadas da internet, mandando o pedido para o roteador. O roteador verá que essa requisição veio de um dispositivo com o IP `192.168.1.2`, e segundo sua tabela `ARP`, o endereço mac correspondente é `CC-xxxxx-CC`. Então ele devolve a resposta para o switch, encaminhando para o hacker novamente, quem realmente tem o mac `CC-xxxxx-CC`.

Como o hacker quer que a vítima leia a informação pedida, fará o encaminhamento. Percebe o que aconteceu? O hacker consegue ver tudo o que a vítima manda para o roteador, e tudo que ele devolve. O hacker se colocou no meio da comunicação, e por isso esse tipo de ataque é chamado de *man-in-the-middle* ("o homem no meio da comunicação"), também referida como MITM.

Nosso próximo passo é executar esse ataque como o hacker faria. Até lá!