




Segurança da Informação

A photograph of a server room with blue ambient lighting. Rows of server racks are visible, with some racks having their doors open, revealing internal components. A semi-transparent white rectangular box is overlaid in the center of the image, containing the word "Wiretapping" in a bold, dark blue font.

Wiretapping



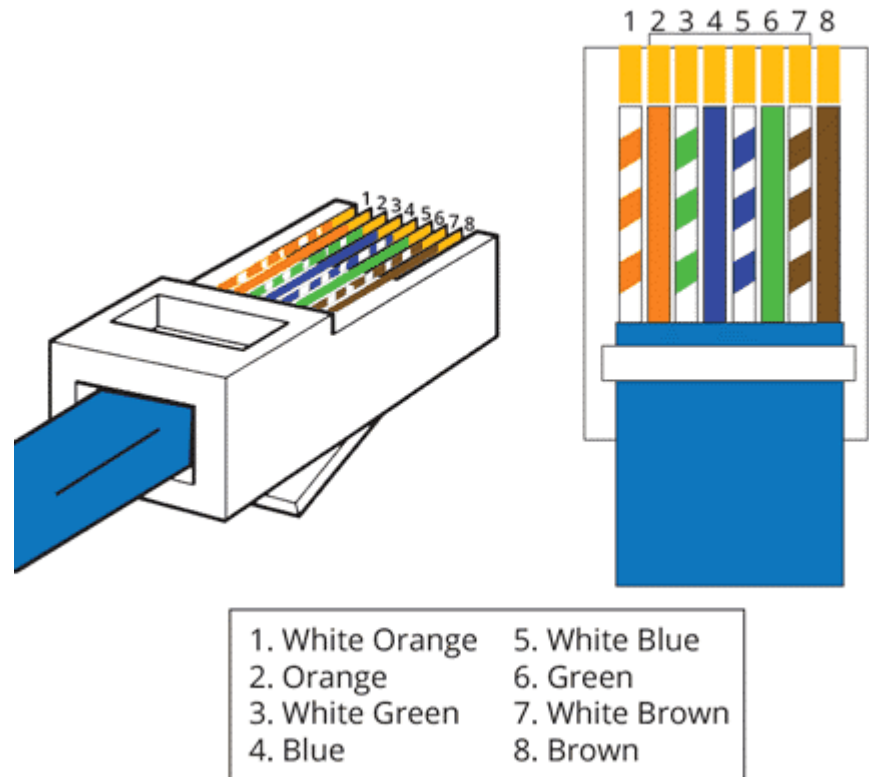
Quão fácil é espionar o tráfego de rede entre dois computadores? Seria suficiente simplesmente cortar e dividir o cabo de rede? A escuta telefônica é uma forma de conectar-se a um cabo de rede e começar a escutar. Durante a escuta, a comunicação original é “copiada” para o dispositivo de escuta do invasor. Os dados transmitidos não são modificados de forma alguma.

Ataque::Teoria

Camada física → modelo OSI

Cabo UTP ou STP
Par trançado

Exemplo: padrão
T568B





Ou seja...

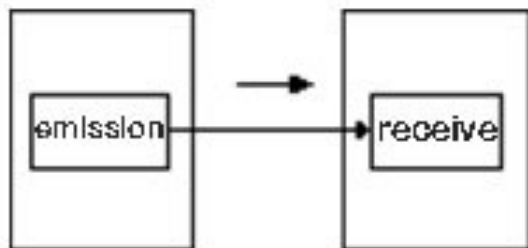
Velocidades de 10 Mb e 100 Mb → 2 pares de fios são utilizados para transmissão de dados

> laranja (ligado aos pinos 1 e 2) para transmissão (Tx)

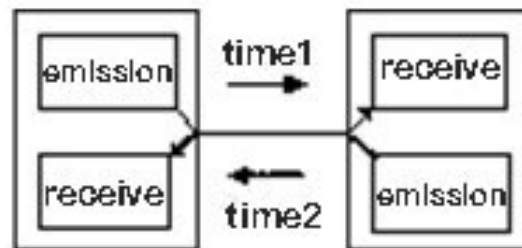
> verde (ligado aos pinos 3 e 6) para recepção (Rx).

Procedimento de escuta

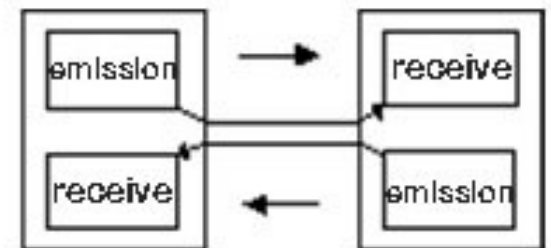
A espionagem ocorre apenas em um par de fios, o que significa que é half-duplex.




Simplex



Half duplex



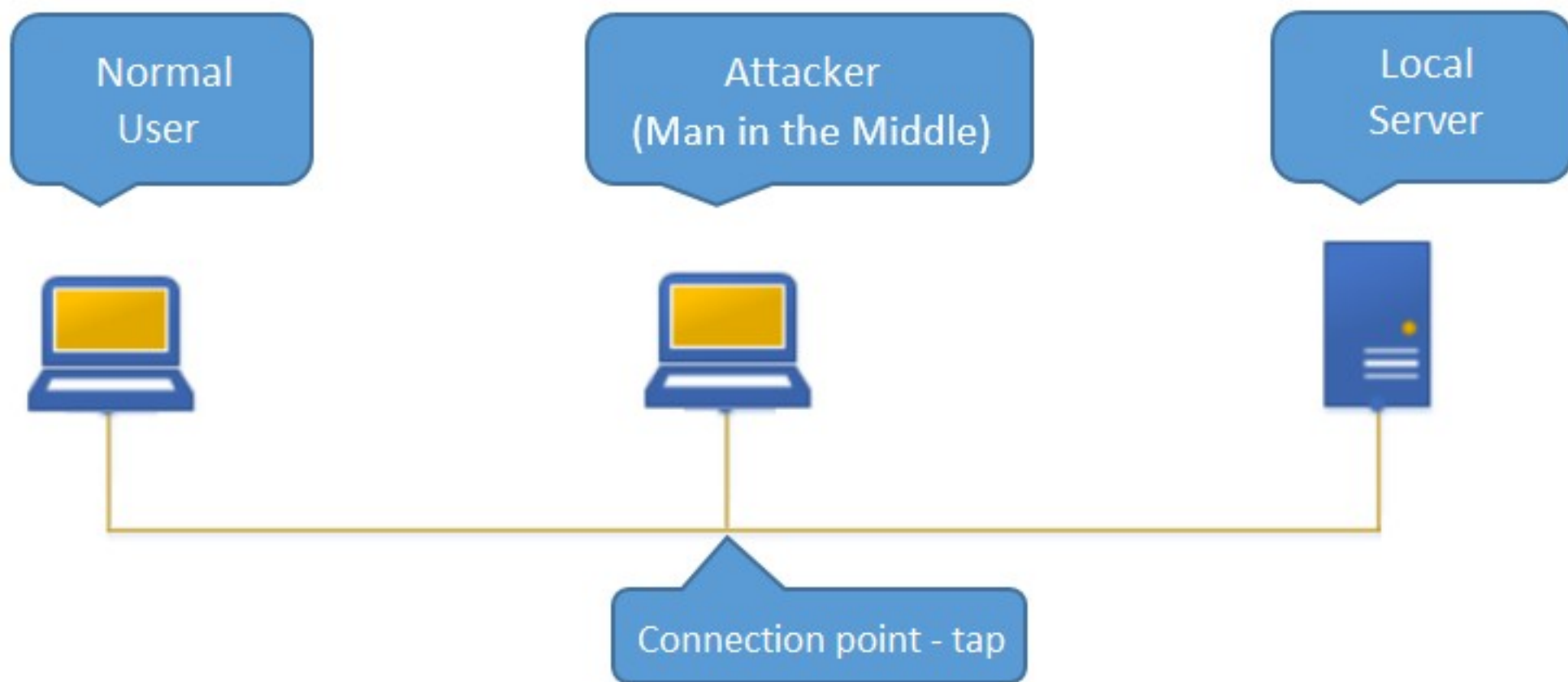
Full duplex

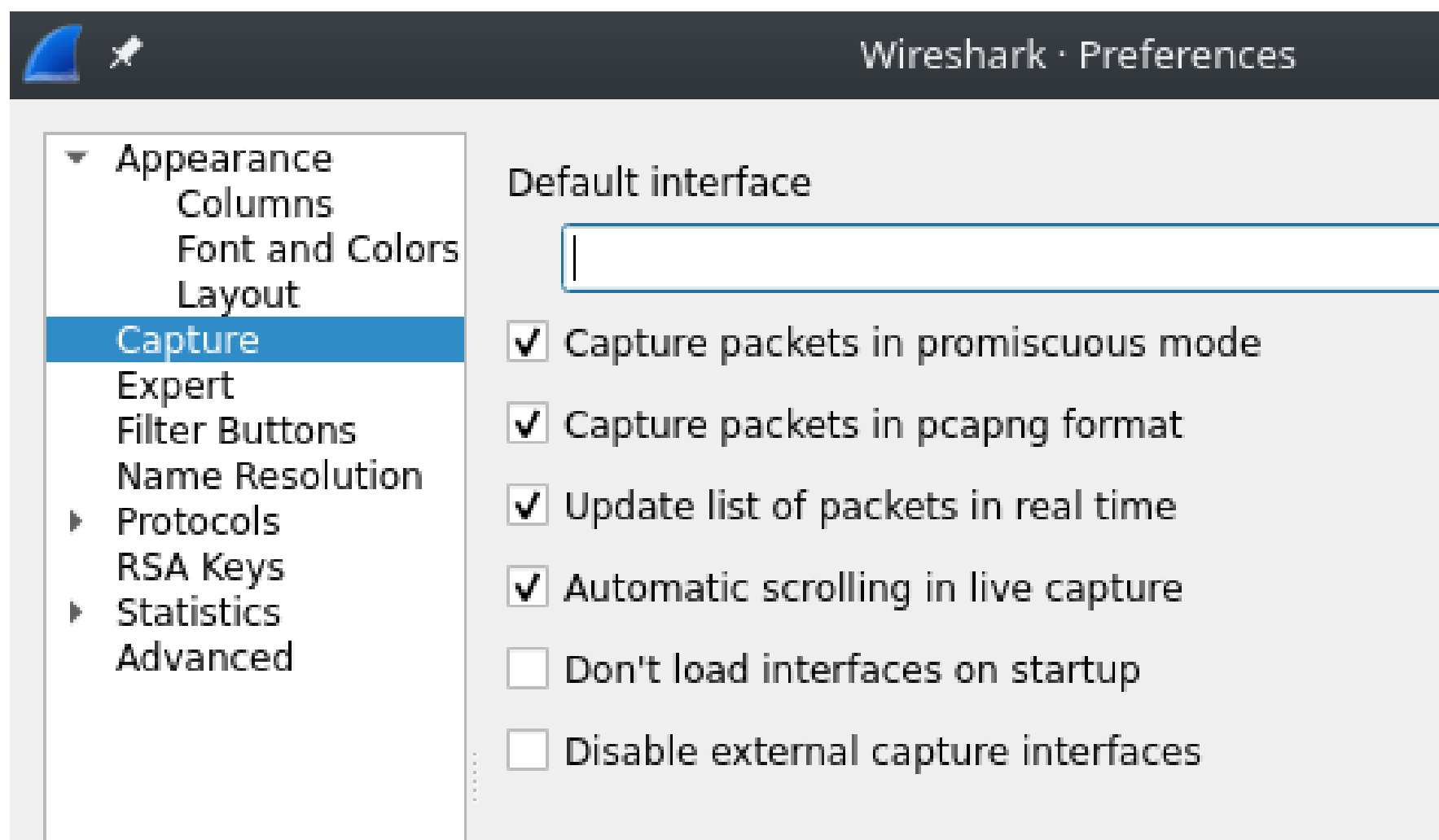
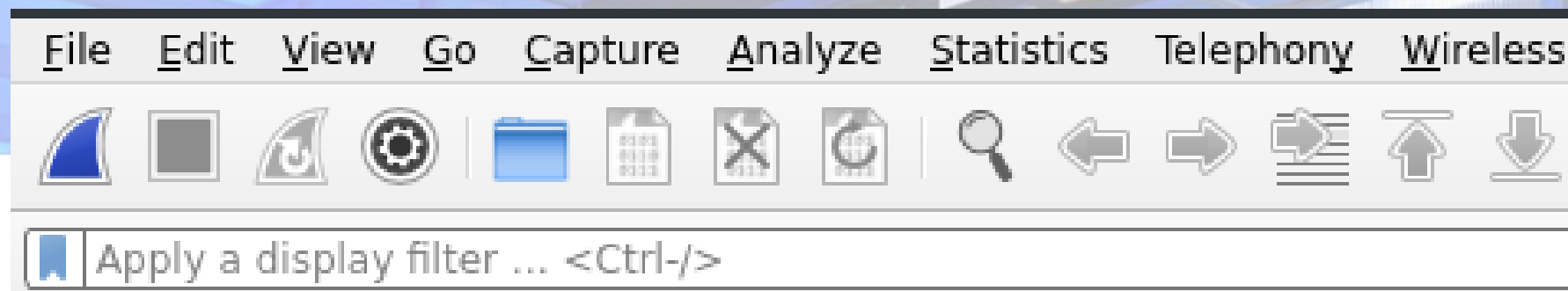


Isso ocorre porque os farejadores só funcionam em uma direção.

Para full-duplex é necessário utilizar 2 conexões (taps) e duas placas de rede.

No nosso caso, utilizaremos o par laranja Tx+ e Tx- para escuta, o que significa que interceptaremos os pacotes enviados pelo usuário ao servidor.







:::: Placa de rede em modo promíscuo



:::: Implementar no Lab

PC → Cabo → Roteador

Decapar o cabo

→ Conectar os 2 pares laranja no
Keystone (obedecendo o mesmo padrão)



:::: Implementar no Lab

No keystone, conectar um cabo de rede ligado na máquina que está executando o Wireshark em modo promíscuo.



:::: Implementar no Lab

Agora um invasor interfere no caminho como o chamado Man in the Middle, que quer interceptar o tráfego.

Depois que o invasor se conectar ao soquete de dados preparado, os pacotes enviados pelo usuário serão propagados também para o laptop do invasor, capturando os dados transmitidos com a ferramenta de detecção Wireshark:



:::: Implementar no Lab

Agora um invasor interfere no caminho como o chamado Man in the Middle, que quer interceptar o tráfego.

O invasor captura todos os dados transmitidos do usuário para o roteador.

E se o usuário estivesse configurando o roteador TP-Link no momento em que o invasor interceptou o tráfego?



:::: Implementar no Lab

O que fazer após o ataque?



:::: Como detectar o ataque?

- > Medir parâmetros físicos do cabo
- > Quais?
- > impedância

A photograph of a server room with blue ambient lighting. Rows of server racks are visible, with some racks having glass doors that show internal components. The room has a high ceiling with exposed metal beams and cables.

Dúvidas?
henrique.mohr@sertao.ifrs.edu.br