INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Minicurso

Análise de Redes usando Wireshark

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Apresentação

- Tadeu Ferreira Oliveira
- Professor do IFRN – SGA
- Graduado em Computação
- Msc. Em Sistemas de computação na área de redes em chip (Noc)
- Ex-coordenador e professor do curso superior de redes da faculdade Estácio em Natal

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Conteúdo

- O que é o wireshark
- Fundamentos de redes modelo TCP/IP
- Ferramentas básicas da interface
- Captura de pacotes em redes de switchs
- Captura de pacotes em redes wifi
- Análise de pacotes genéricos

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Conteúdo

- Análise de pacotes ARP
- Análise de protocolos sem criptografia HTTP/FTP/POP3
- Métodos de penetração em redes
  - Ataques Man-in-the-middle
  - DNS-Poisoning
  - ARP-spoofing

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Aviso Legal

Tenha sempre certeza de ter a autorização necessária para ouvir e capturar tráfego de rede

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

O que é o wireshark

- Surgiu a partir do Ethereal em 2006
- É usado para capturar e principalmente **analisar**tráfego de rede (Sniffer)
- Permite que um adm. de rede disseque os pacotes que passam em sua rede

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

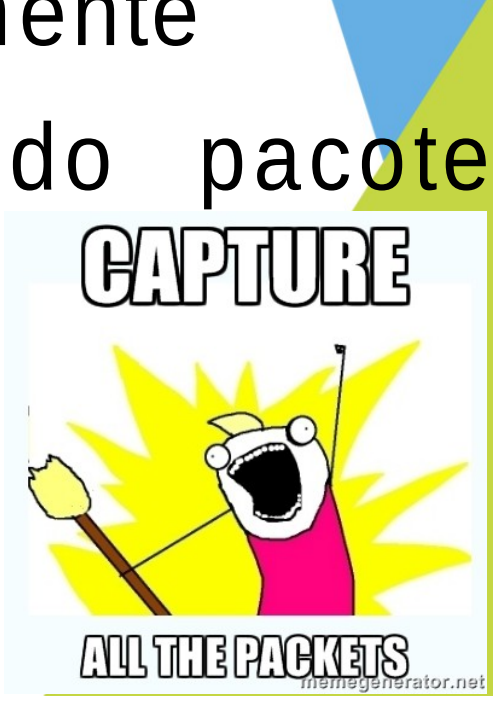
Sniffer

- É um programa de rede
- Capaz de capturar pacotes e armazena-los
- Pode operar em dois modos:
  - Normal
  - Promíscuo

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Sniffer promíscuo

- Em uma rede ethernet muitas vezes pacotes não direcionados a uma máquina podem ser visíveis
- Em uma máquina normal estes pacotes são descartados imediatamente
- No modo promíscuo todo pacote é recebido e processado



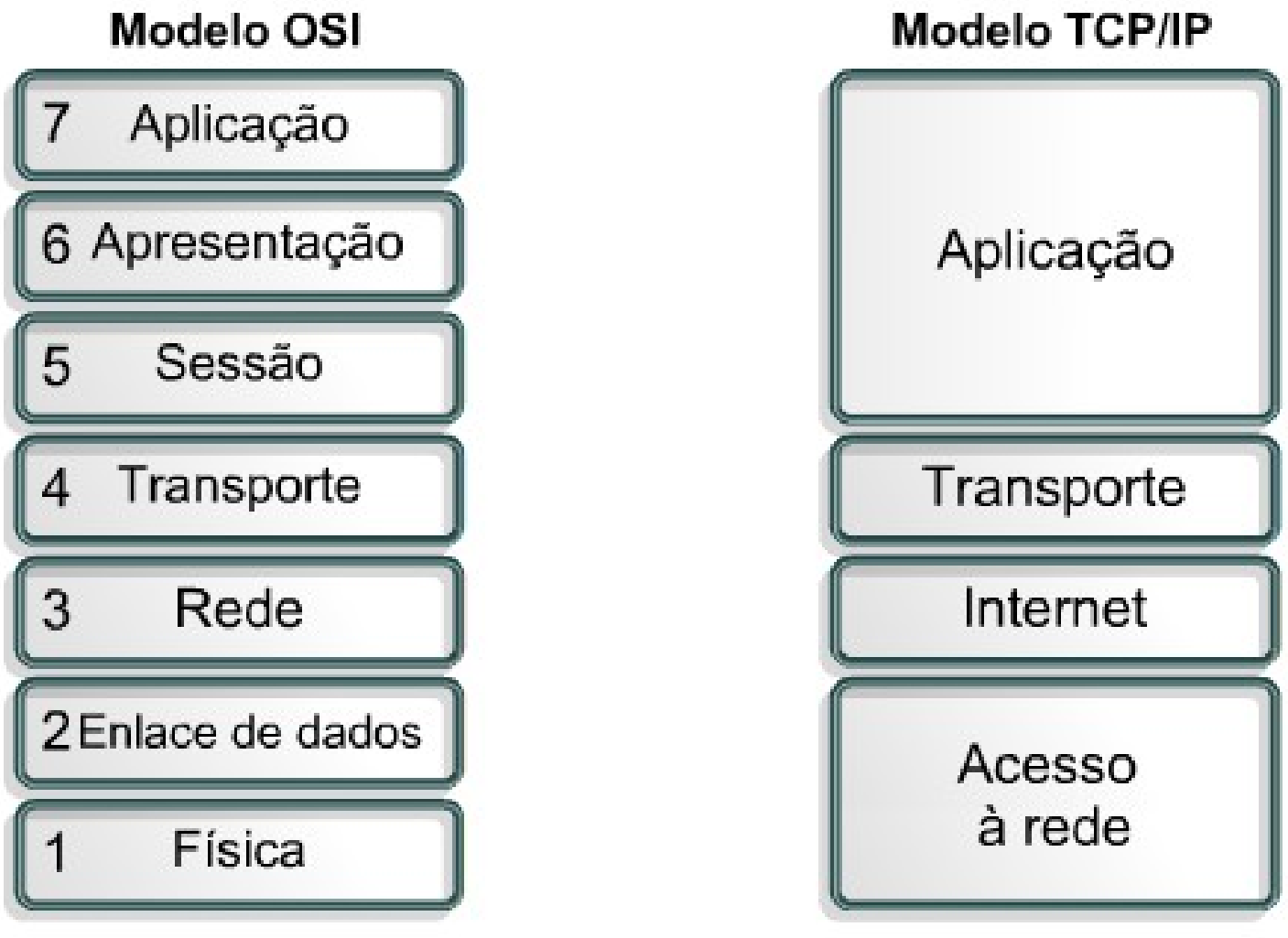
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Dissecar pacotes

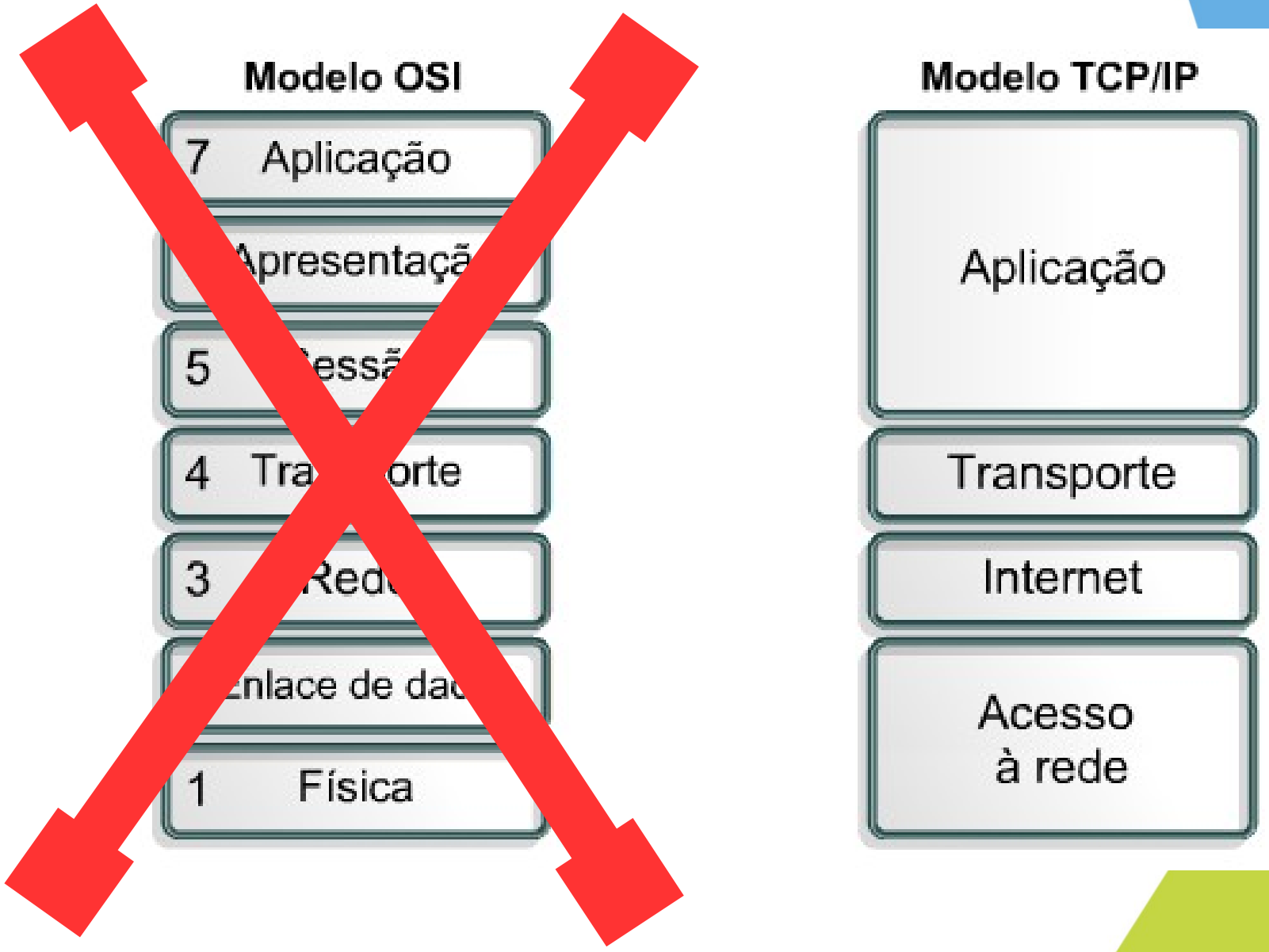
- É a atividade de avaliar cada bit dentro de um pacote de rede
- O pacote é dividido em suas partes e o profissional pode verificar cada atributo e o conteúdo do pacote

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Quem já viu essa imagem?

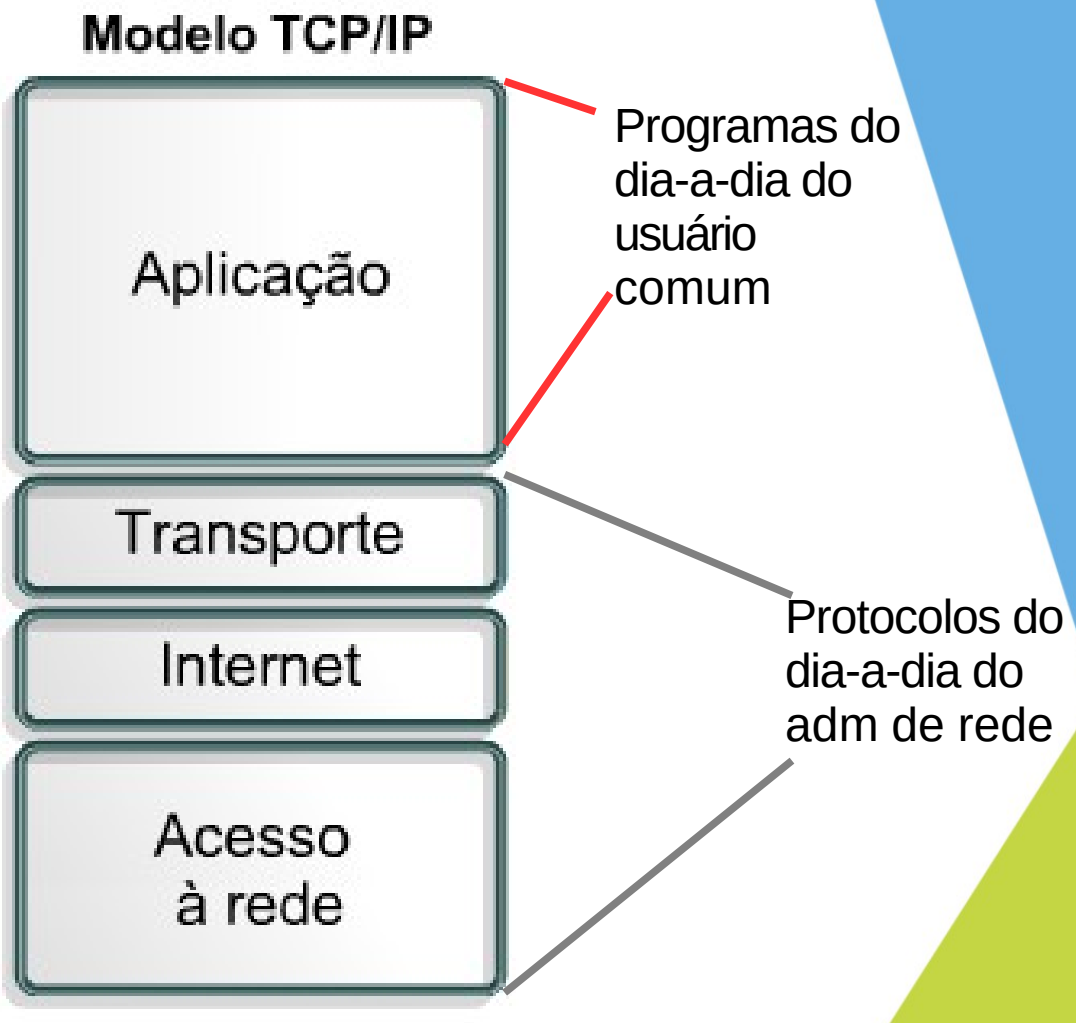


Fundamentos de redes modelo TCP/IP



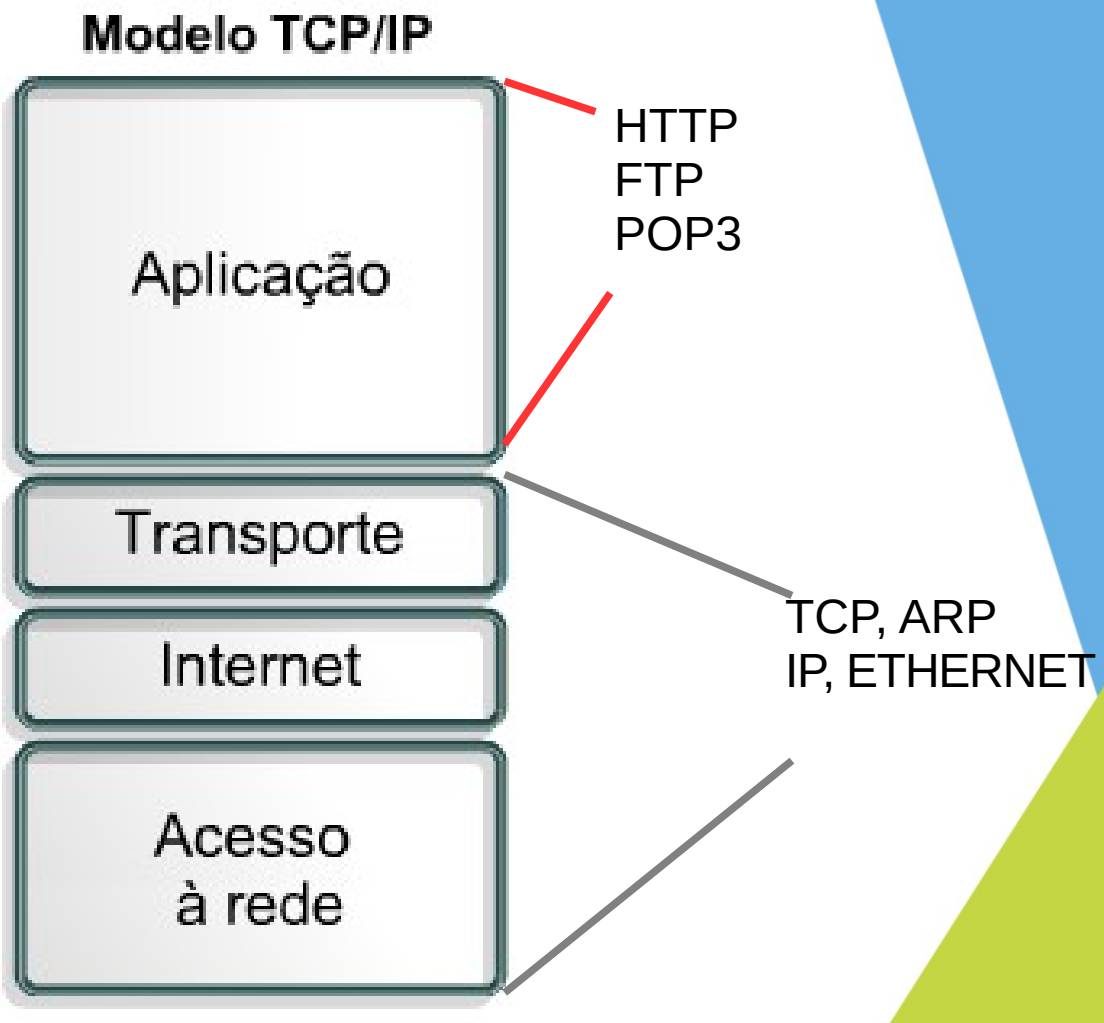
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Fundamentos de rede



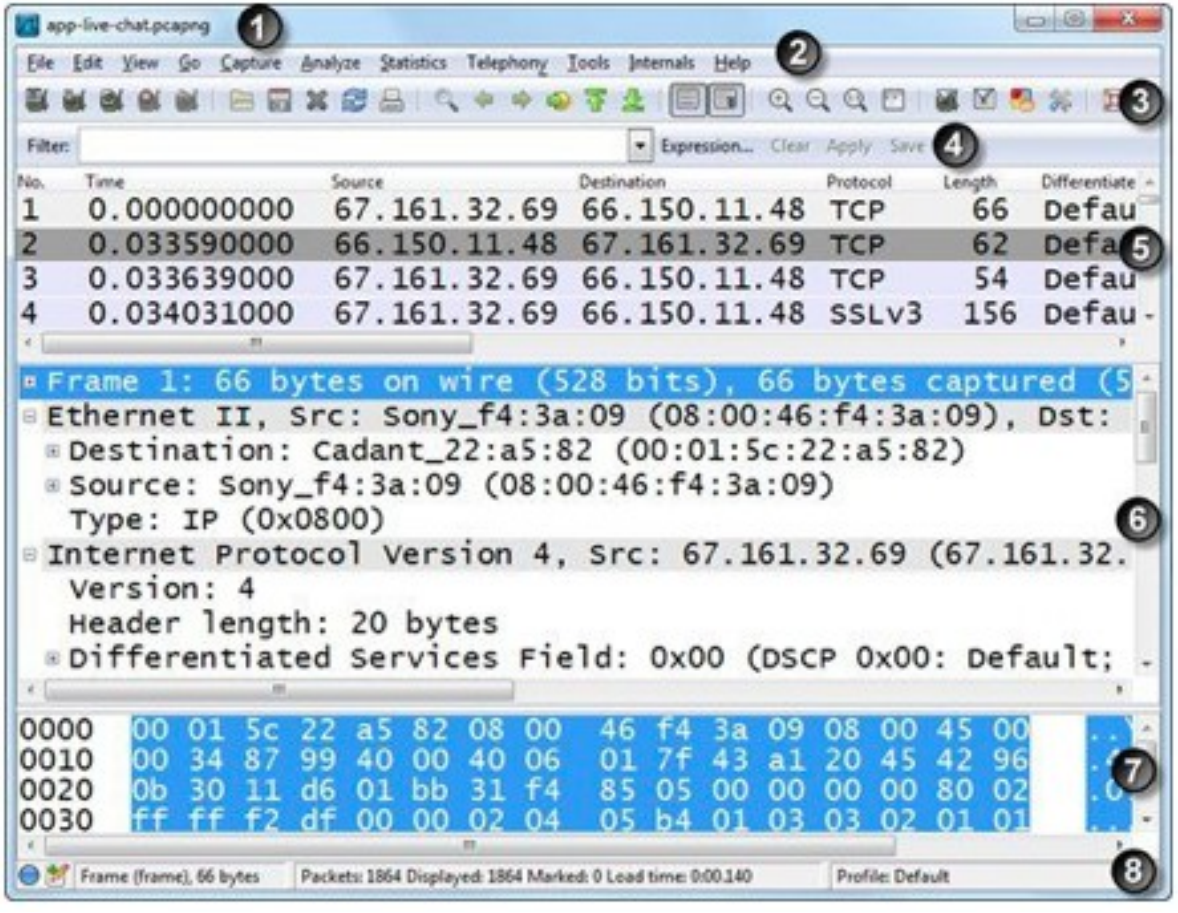
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Fundamentos de rede



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

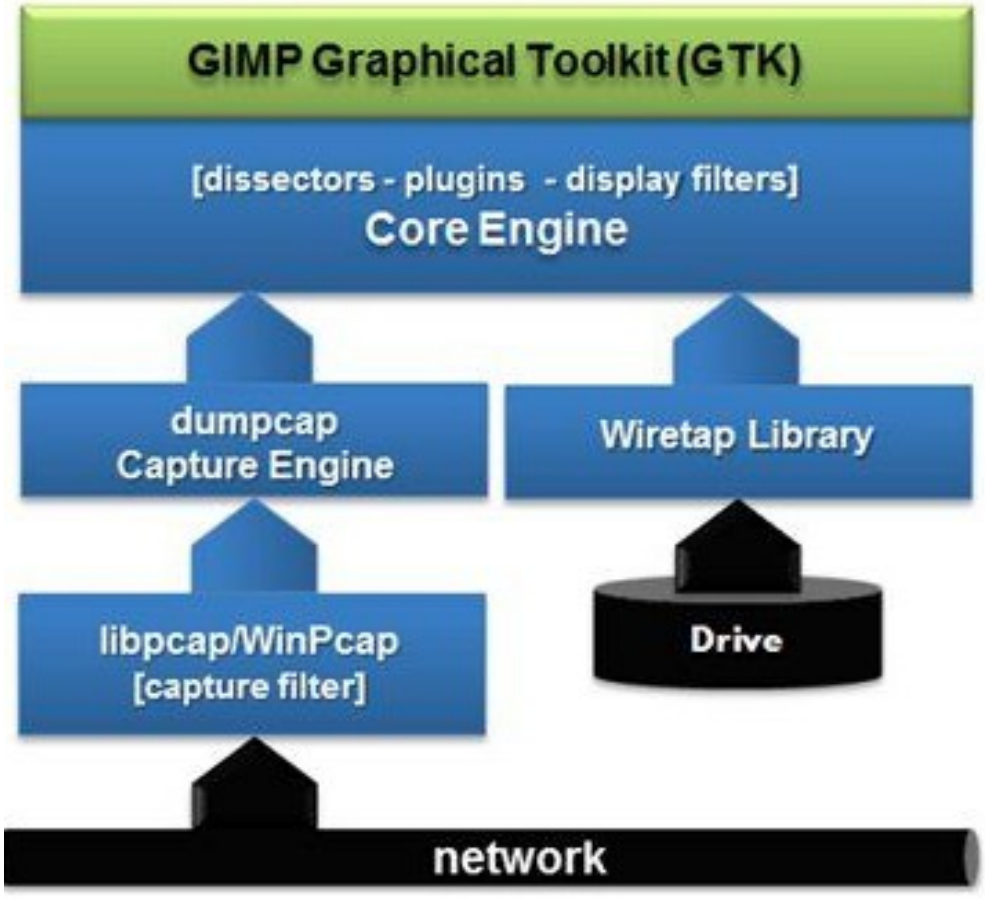
Ferramentas básicas da interface



1 Barra de Título
2 Menu Principal
3 Barra de ferramentas
4 Filtro de pacotes
5 Lista de pacotes exibidos
6 Painel de detalhes
7 Painel do pacote em bytes
8 Barra de status

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Componentes internos do wireshark



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Redes com hubs e switchs

- Um hub é um equipamento passivo
- Um switch é um equipamento ativo
- Os hubs estão em desuso em redes cabeadas hoje, mas é importante conhecer seu funcionamento

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

HUB

- É como usar um trio elétrico para dar um recado a uma pessoa
- O recado vai chegar, mas vai chegar a todo mundo que está ali naqu

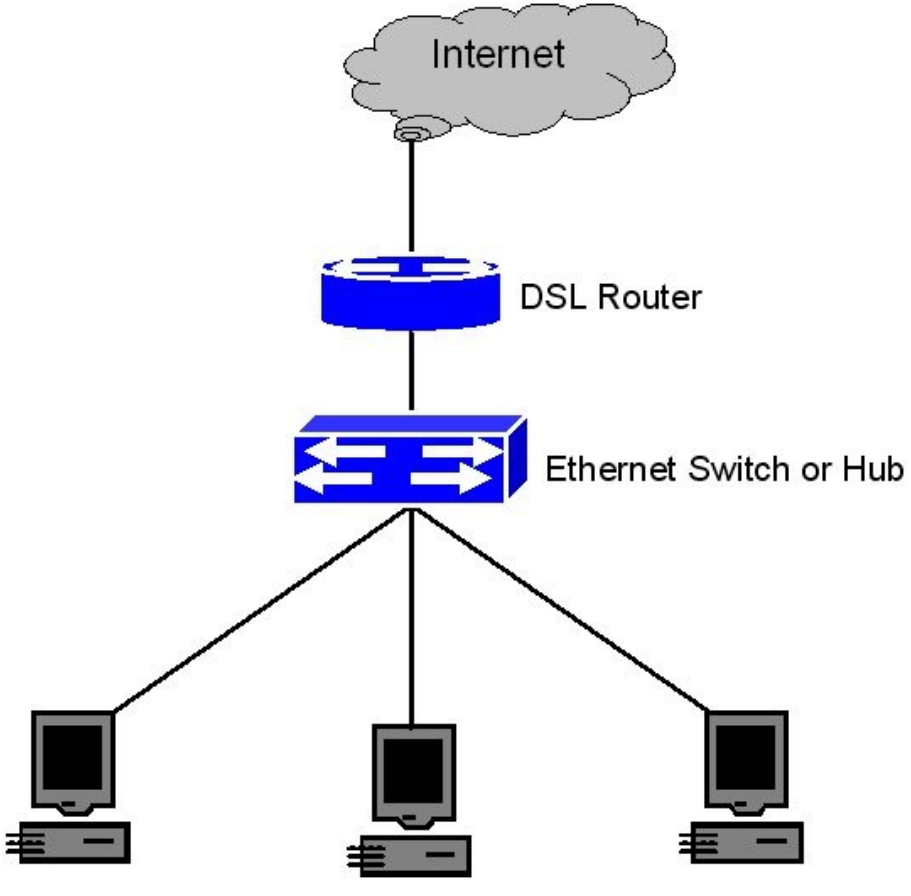
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Switch

- É como mandar uma carta
- Vai passar por alguém no meio do caminho mas só vai ser entregue ao destinatário

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Instalação típica em uma rede



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Captura de pacotes

- O wireshark pode funcionar no modo promíscuo ou no modo normal.
- Se a sua rede está usando um switch (que é mais provável)
- Você só verá o tráfego da sua máquina ou par a sua máquina
  - O modo promíscuo não faria diferença neste caso

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO [illegible]

Captura de pacotes em um hub

- Simples
- Todos os pacotes da rede chegam a todos
- Muito inseguro
- Pouco comum hoje

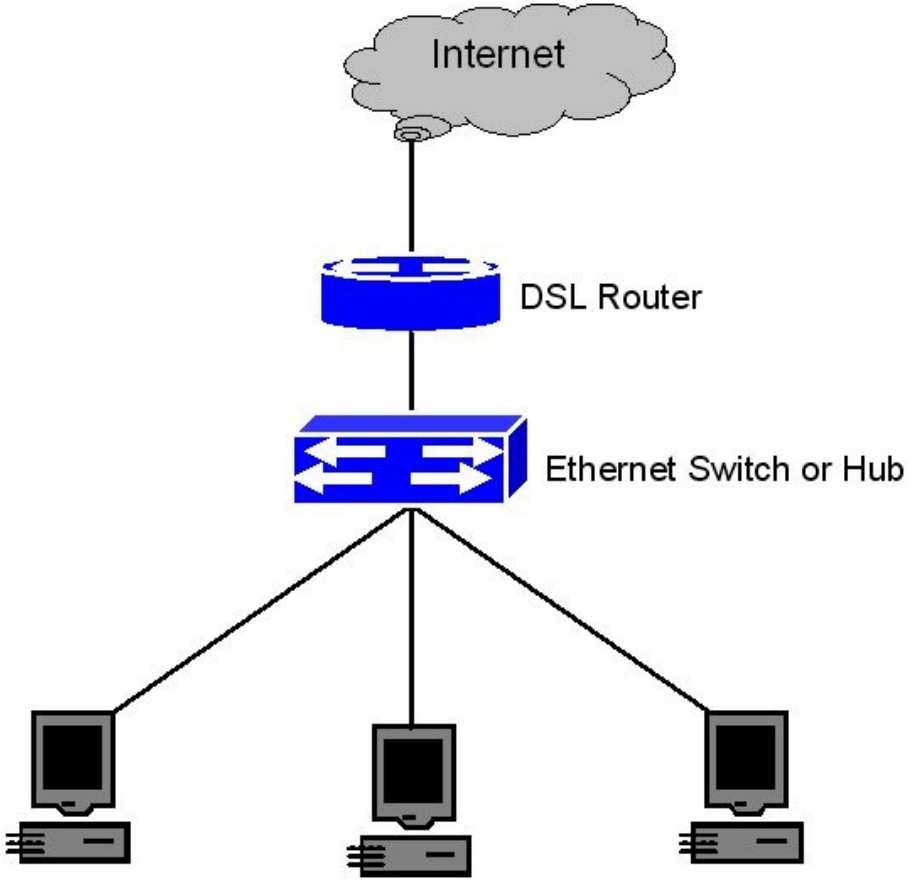
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Captura de pacotes em um switch

- Cascateamento
- Porta de uplink
- Espelhamento de porta
- Usando estes conceitos poderemos capturar todo ou quase todo tráfego de uma rede LAN

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Voltando ao nosso ambiente



Captura de pacotes em redes de switchs

- Além do espelhamento é possível capturar pacotes através de ataques ao funcionamento do switch e a alguns protocolos
- Veremos esses ataques mais pra frente...

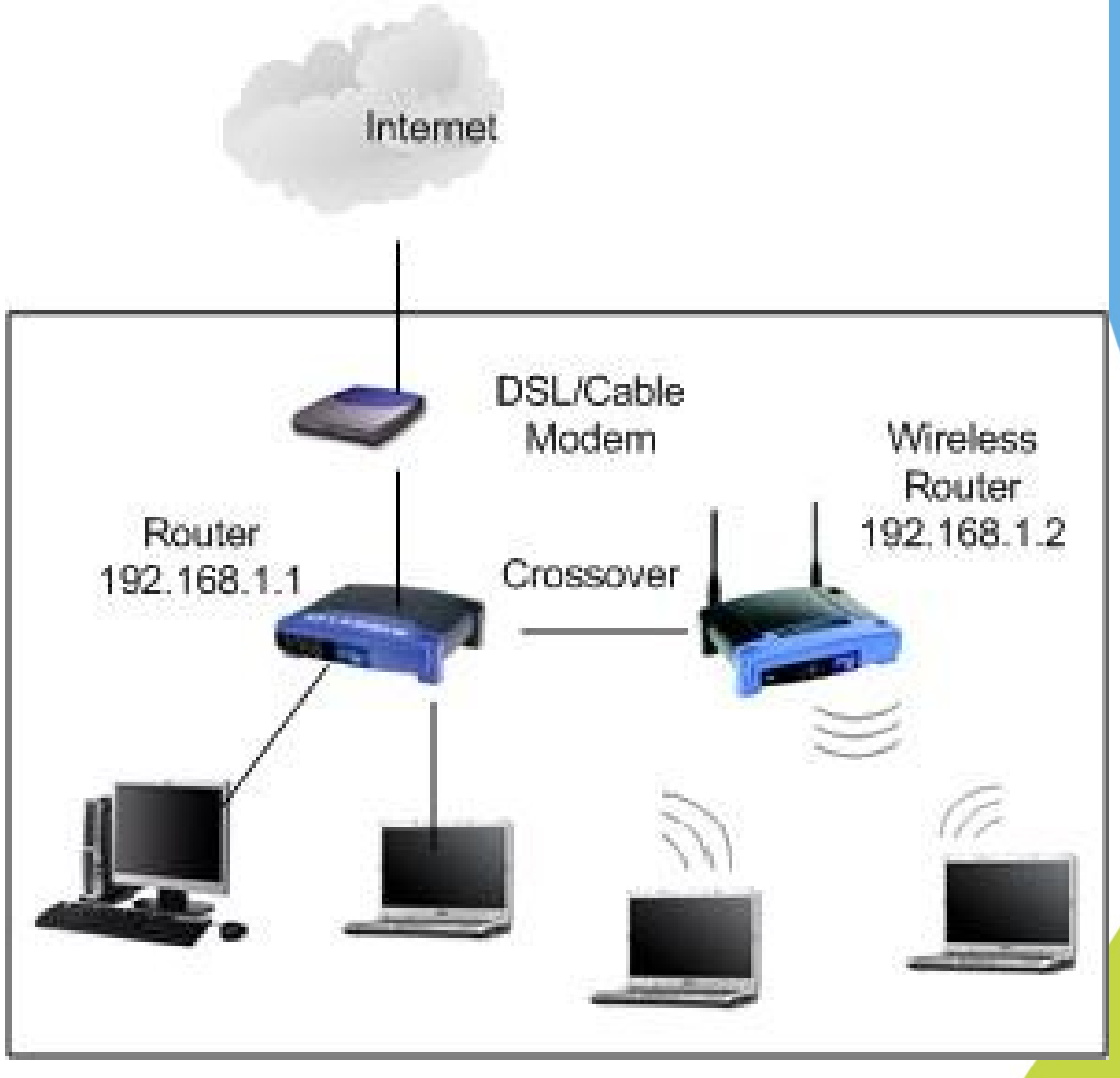
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Captura de pacotes em redes wifi

- Nas redes wifi há basicamente 2 situações be distintas
  - Redes abertas
  - Redes com chaves de acesso
- Vejamos como funciona uma rede aberta

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Redes wifi abertas



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Redes wifi abertas

- Como vimos nessas redes os access points funcionam como hubs
- Assim, a captura de pacotes é extremamente simplificada
- Bastando o sniffer estar em um local sem obstáculos para o access point

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Redes wifi criptografadas

- WEP (Wired Equivalente Privacy)
  - Senha única para todos os equipamentos
  - Baixa complexidade da senha
  - Fácil ataque usando técnicas de força bruta ou
  - FMS e Chopping
    - sem entrar em detalhes há ferramentas gratuitas que quebram estas senhas em minutos.
  - Uma vez que se esteja autenticado é possível ver todos os pacotes, como em uma rede aberta

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

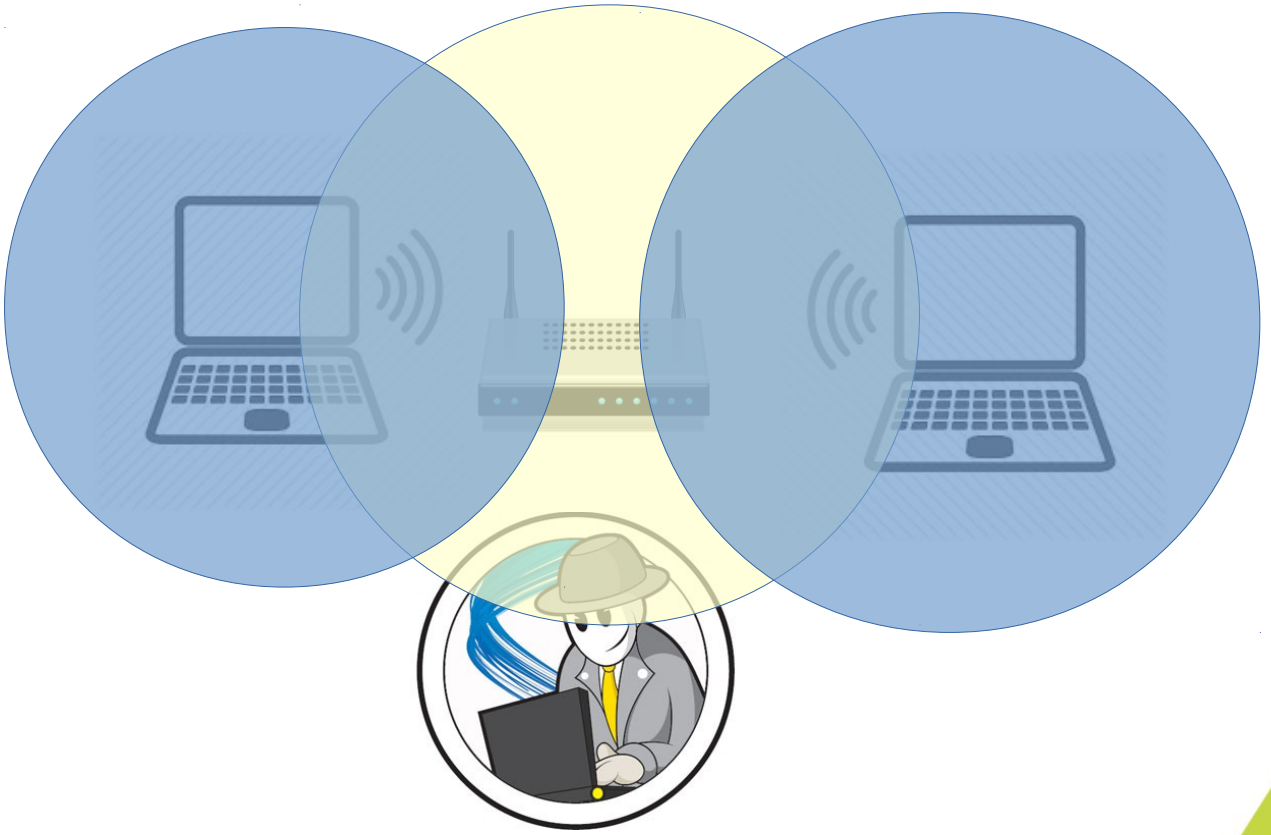
Redes wifi criptografadas

- WPA (Wifi protected access)
  - Há vários modos de autenticação que vão desde uma senha PSK (pre shared key)
  - Até certificados digitais
- Neste tipo de rede a quebra para acesso é mais complexa
- O padrão WPA2 é considerado hoje um padrão com segurança aceitável de redes sem fio
- O wireshark consegue decriptar WPA2 PSK, mas não o padrão enterprise

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Captura de pacotes em wifi

- O problema da estação fantasma



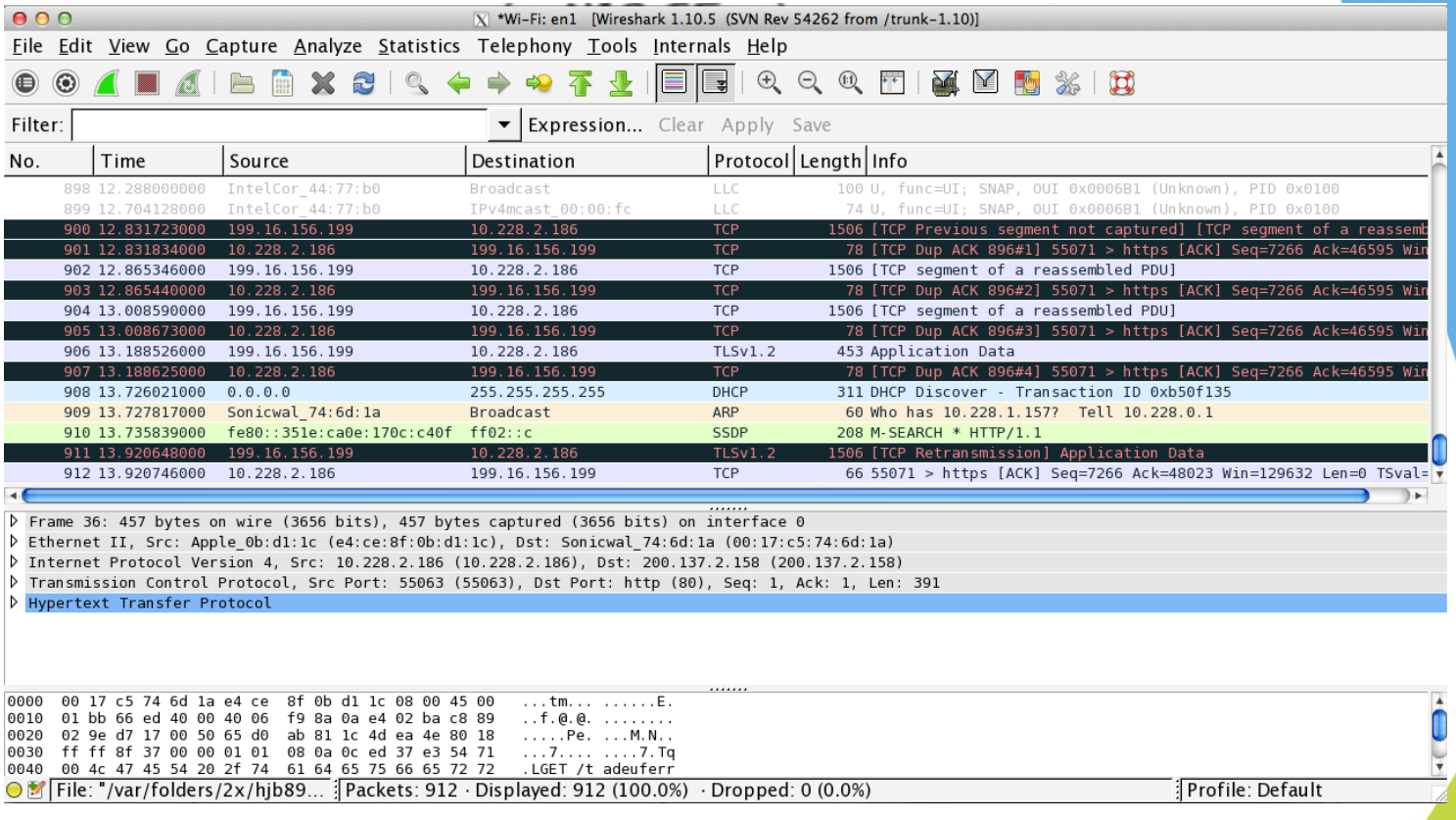
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Análise de pacotes genéricos

- Vamos iniciar nossa primeira prática de análise de pacotes.
- Tenha certeza que o cache do seu browser está vazio. Isso garante que nossas requisições vão necessariamente ser feitas ao servidor de destino, e não serão respondidas pela cache local. (No firefox faça Ferramentas → Limpar histórico Recente)
- Abra o Wireshark
- Clique no botão “List Available Capture Interfaces” à esquerda.
- Inicie a captura clicando em START na placa de rede conectada à rede
- Use o browser para acessar a URL: **http://docente.ifrn.edu.br/tadeuferreira**
- Pare o capturador de pacotes Wireshark clicando no botão “Stop Running Live Capture” você deve ter uma tela como a mostrada abaixo

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Captura do wireshark



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Painel de detalhes

- No.:
  - Um número sequencial dos pacotes capturados pelo wireshark
- Time:
  - Momento em que o pacote foi capturado.
- Source:
  - Ip ou endereço MAC de origem do pacote
- Destination:
  - Ip ou endereço MAC de destino do pacote
- Protocol:
  - O protocolo que está sendo usado neste pacote (exibirá o protocolo de mais alto nível. Ex.: se um pacote usa o protocolo TCP e HTTP será exibido HTTP pois este está mais acima no modelo de camadas)
- Info:
  - Um resumo das informações que podem ser relevantes para aquele tipo de pacote.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Vamos analisar nossos pacotes

- Painel de lista de pacotes
- Painel de detalhes do pacote
- As camadas TCP/IP e o wireshark
- Filtro de pacotes

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Filtro de pacotes

- Por protocolo
- Por origem e destino
- Por endereço MAC
- Por rede wifi

Endereçamento de Rede

ARP e Endereço de LAN

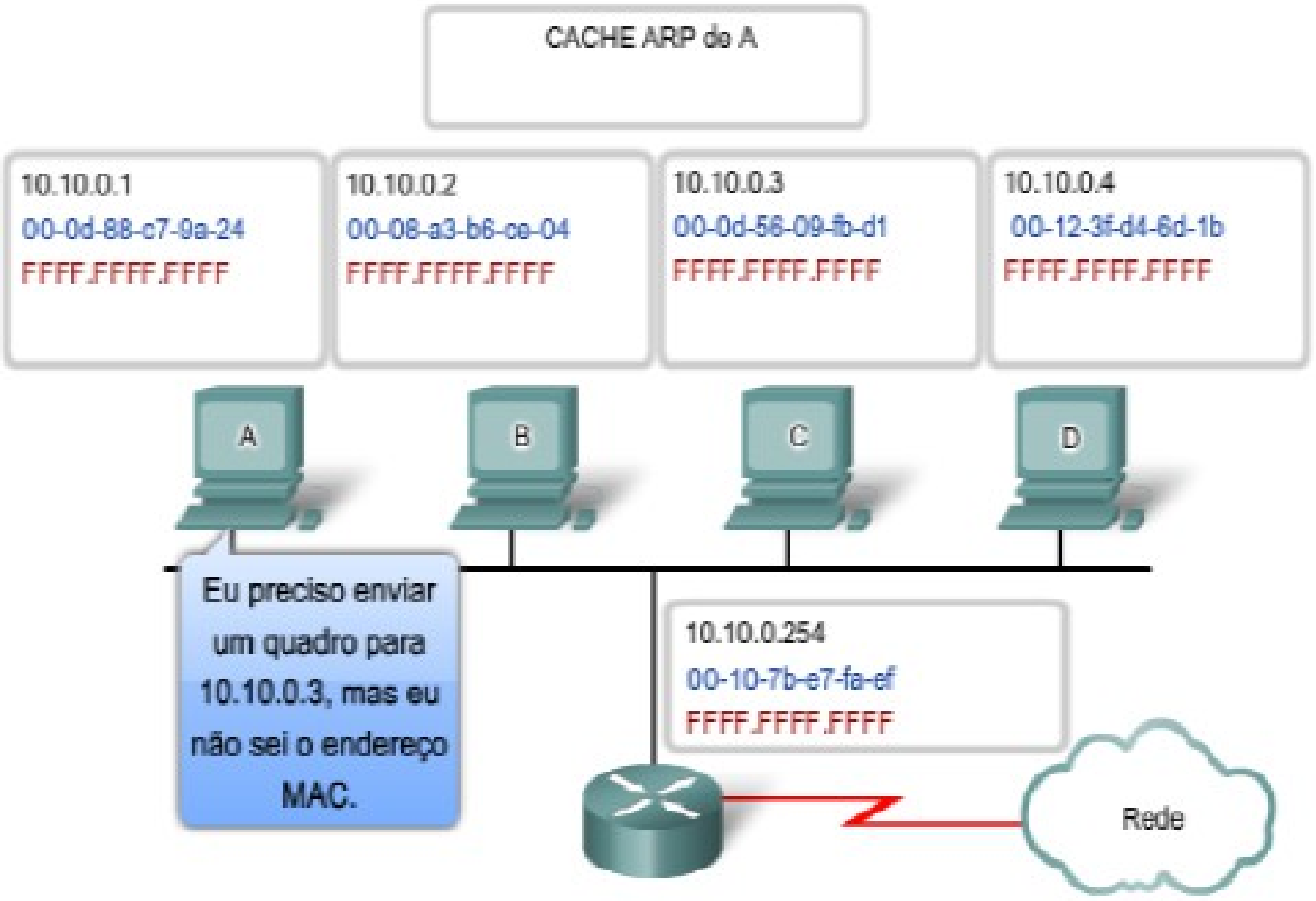
Objetivos

- Manter uma tabela com os endereços MAC's conhecidos
- Obter o endereço MAC dos equipamentos na mesma rede que se conheça o endereço IP
  - Resolver endereços IP para MAC

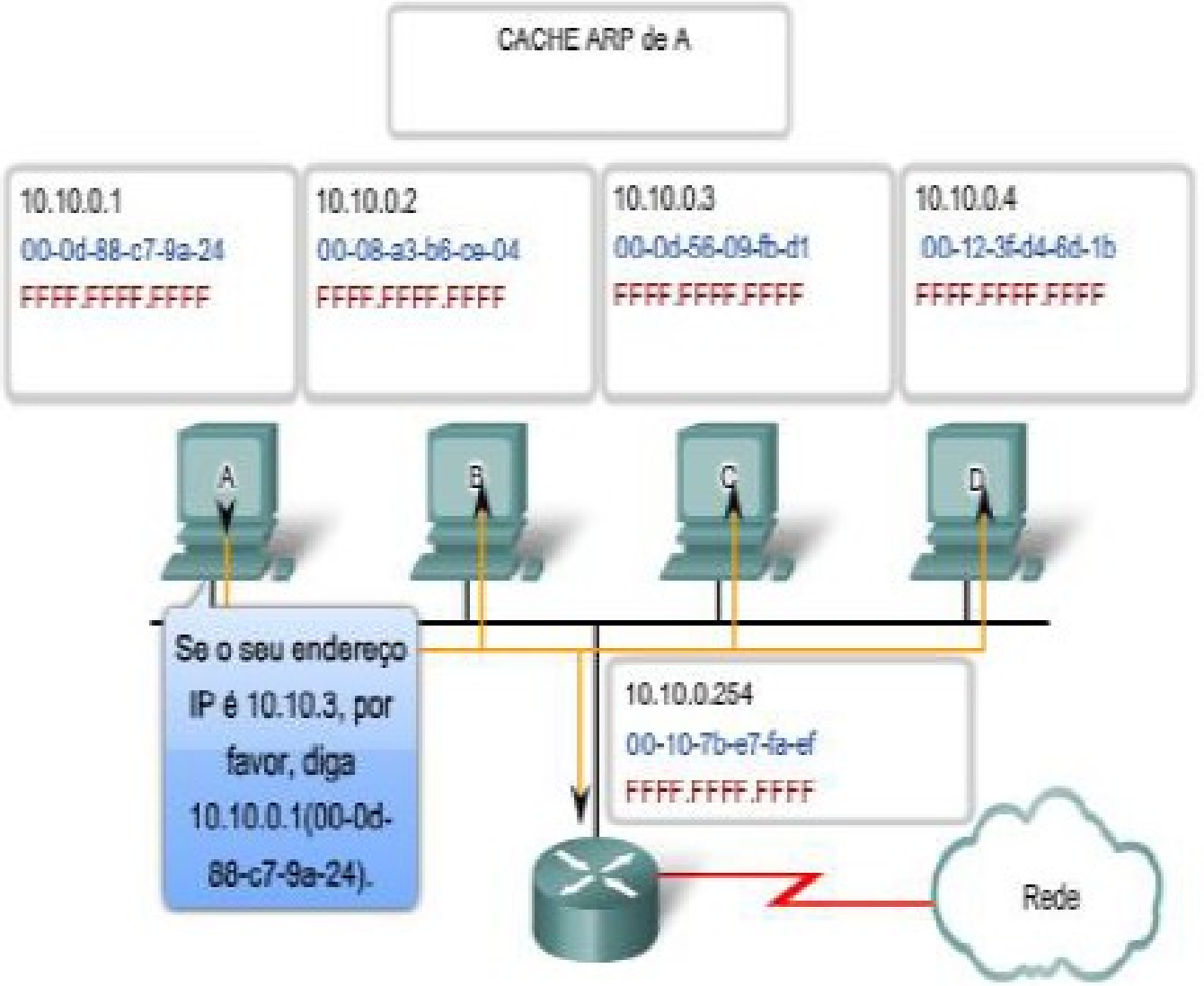
Uso do ARP

- Um pacote vem da camada de rede apenas com um endereço IP
- As camadas superiores não conhecem nada c endereçamento MAC
- A camada de enlace precisa descobrir o endereço MAC do IP

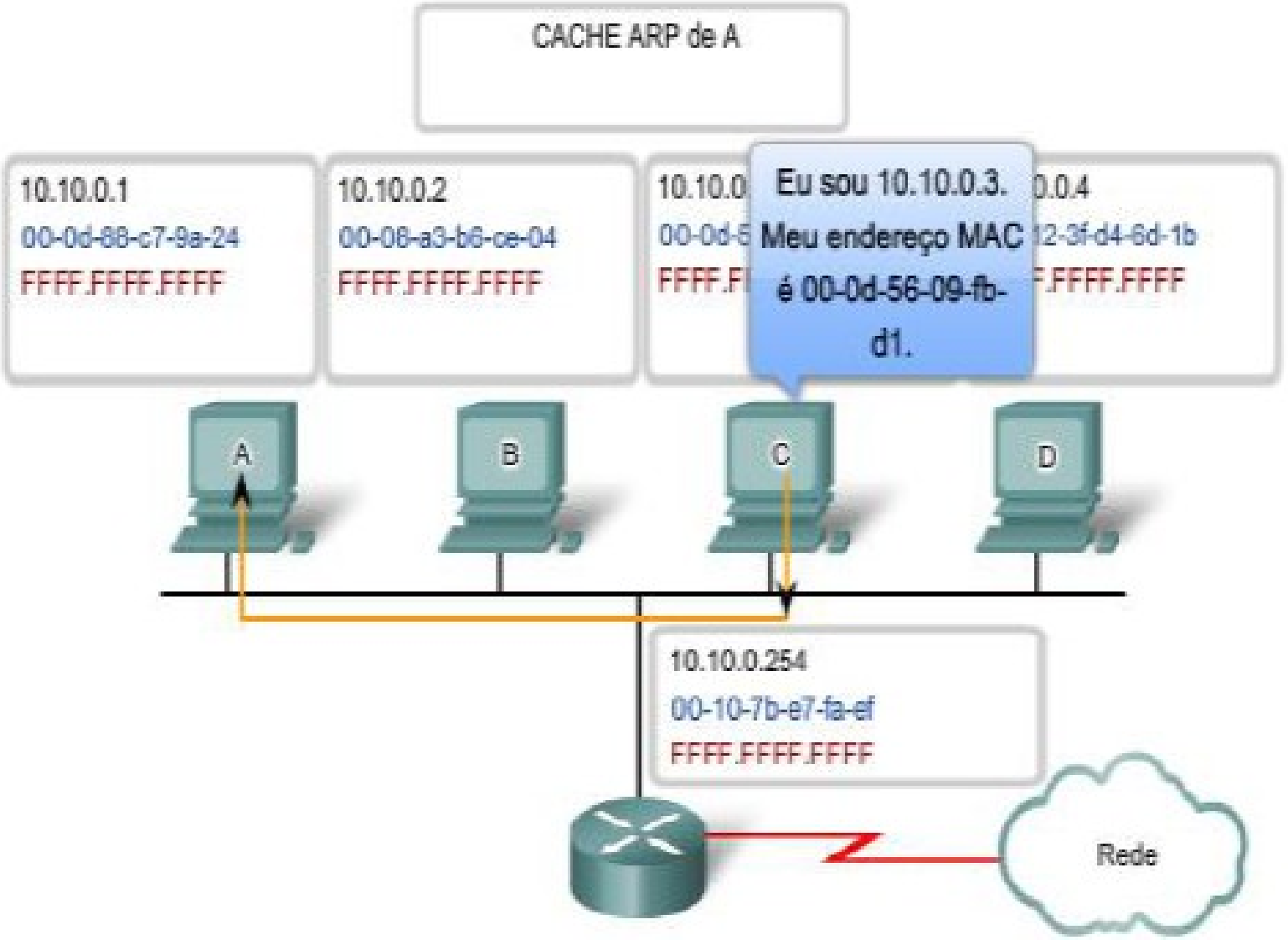
Passo a Passo (1)



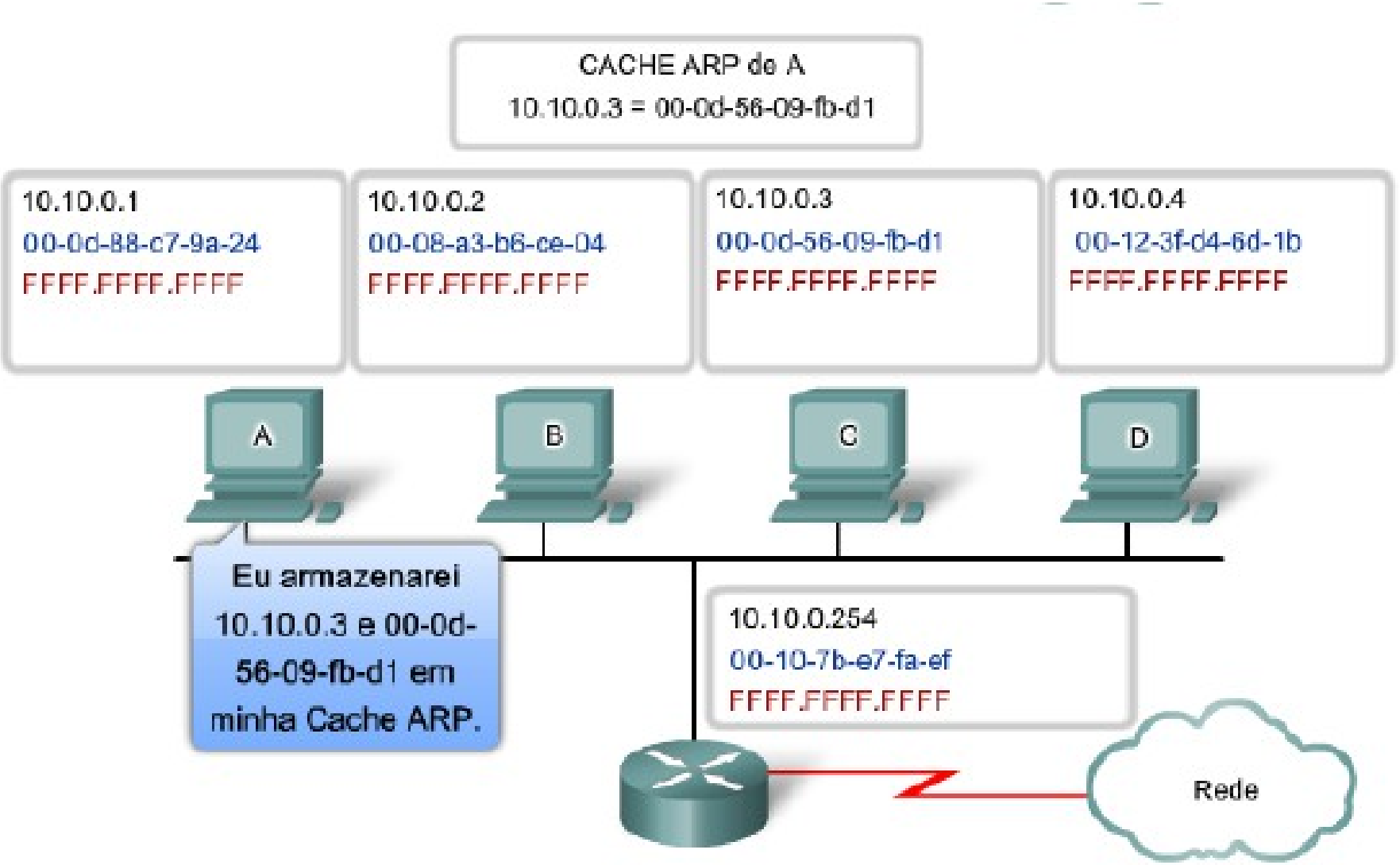
Passo a Passo (2)



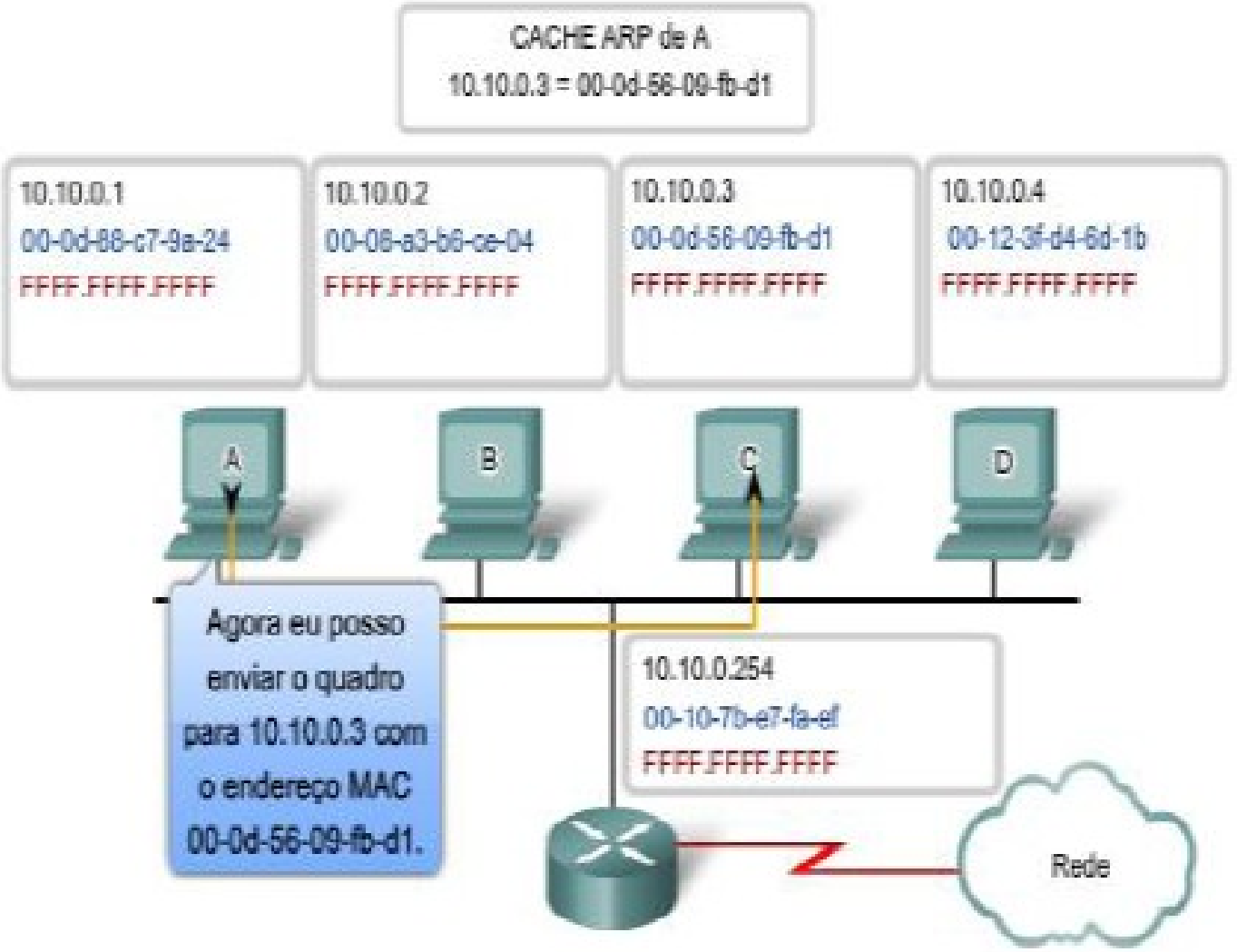
Passo a Passo (3)



Passo a Passo (4)



Passo a Passo (5)



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Análise de pacotes ARP

- Baixe o exemplo:
  - arp.cap.zip
- O que podemos descobrir com o ARP?
  - Fabricantes
  - Máquinas que estão na rede
  - Estratégias para MAC Spoofing
- Analisemos o pacote arp

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Protocolos sem criptografia

- Facilitam a vida de um sniffer
- Facilitam a vida do atacante
- Exemplos:
  - HTTP
  - FTP
  - POP3

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Análise de protocolos sem criptografia HTTP

- O que podemos descobrir?
  - Servidor
  - Versão
  - Possíveis ataques
  - CVE Common Vulnerabilities and Exposures

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Análise de tráfego http

- Baixe o exemplo
  - http.cap
- Lendo informações básicas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Análise de tráfego HTTP

- Baixe o exemplo
  - senhahttp.cap
- Tente descobrir a senha do usuário deste site

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Outro exemplo

- Telnet
- Um protocolo antigo substituído pelo SSH
- Vejamos um exemplo:
- Baixe o exemplo:
  - telnet.cap

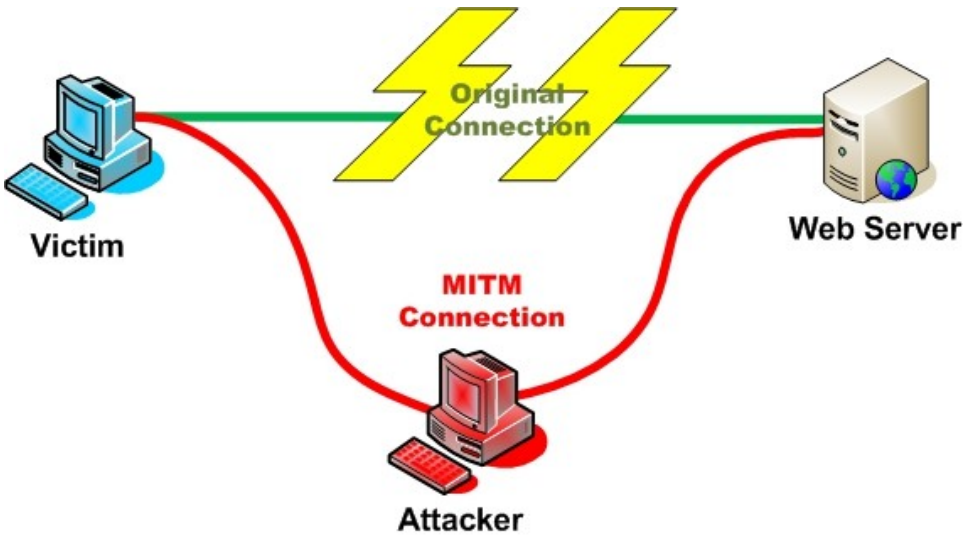
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Métodos de penetração em redes

- Ataques Man-in-the-middle
- DNS-spoofing
- ARP-spoofing

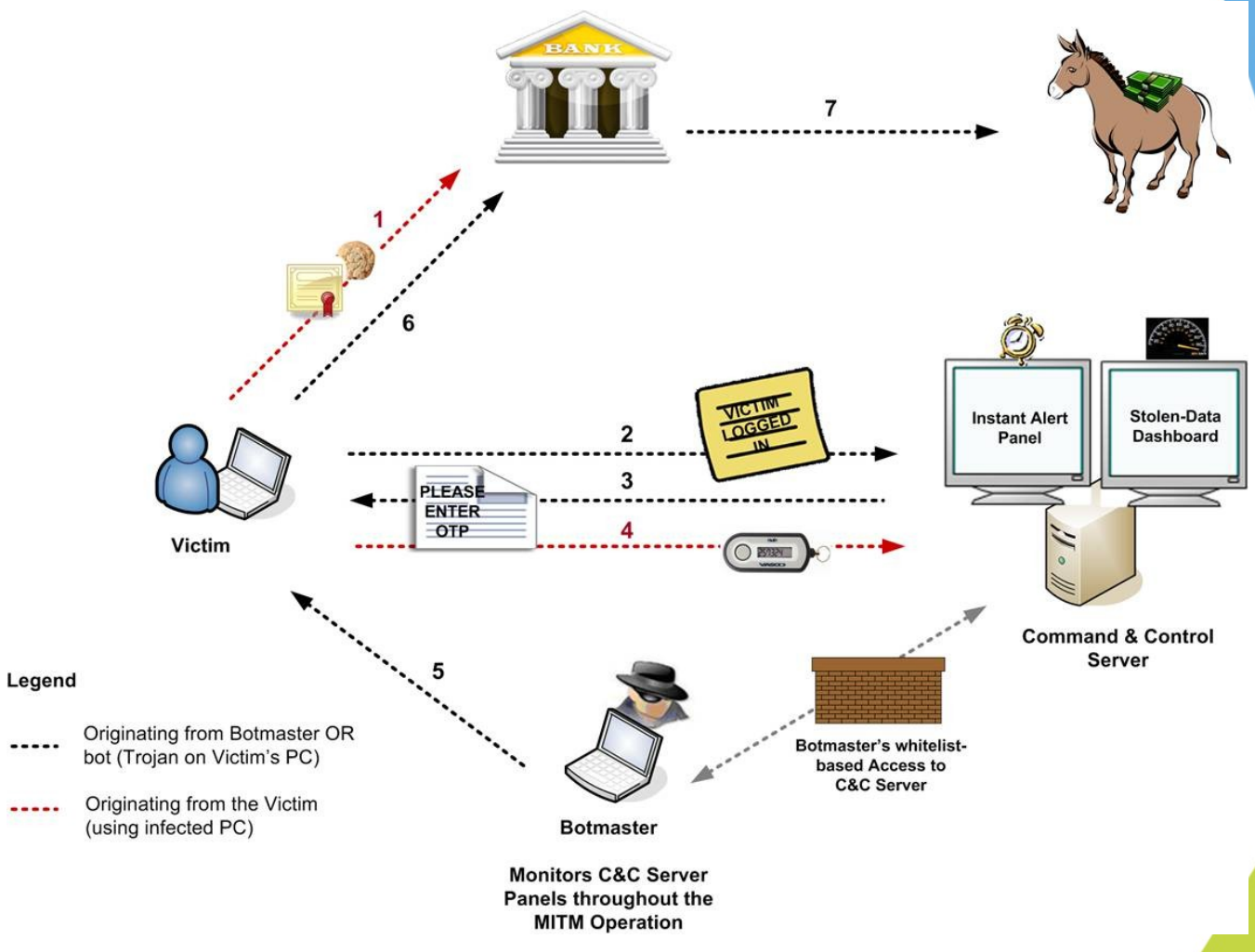
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Ataques Man-in-the-middle



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

man in the middle (token)



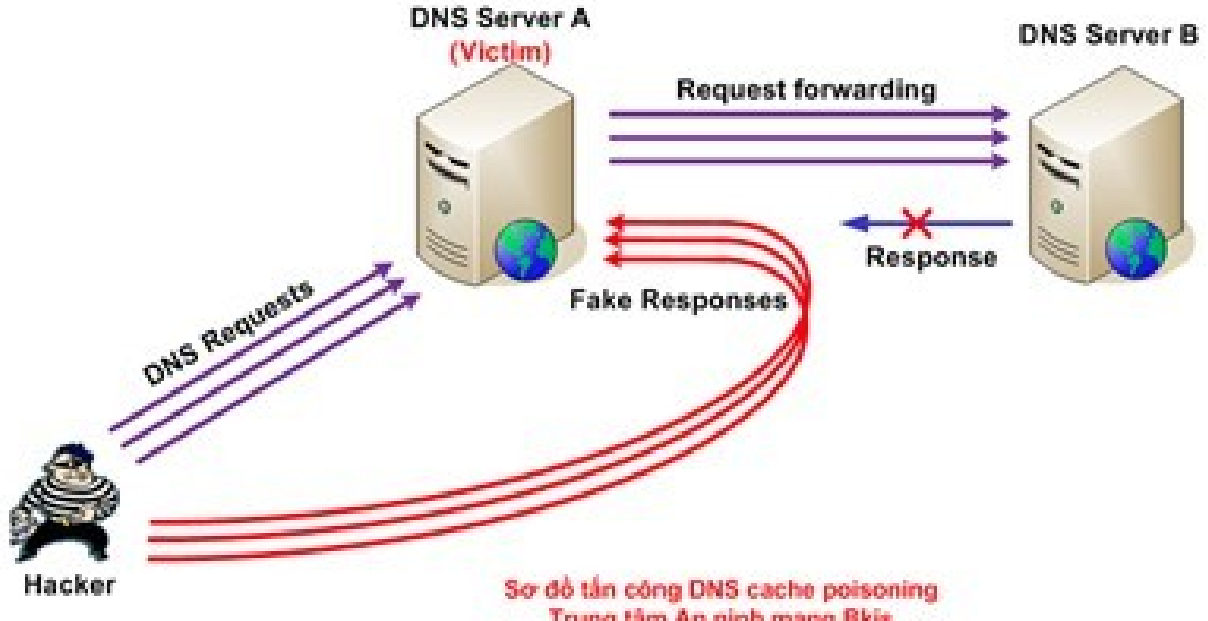
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

DNS-Poisonning

- Uma forma muito comum de ataques a usuários comuns
- O atacante compromete a forma como o client descobr IPs a partir de nomes
- Pode ser feito no servidor DNS ou na máquina local do cliente usando o arquivo HOSTS

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

DNS Poisoning



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

ARP-spoofing