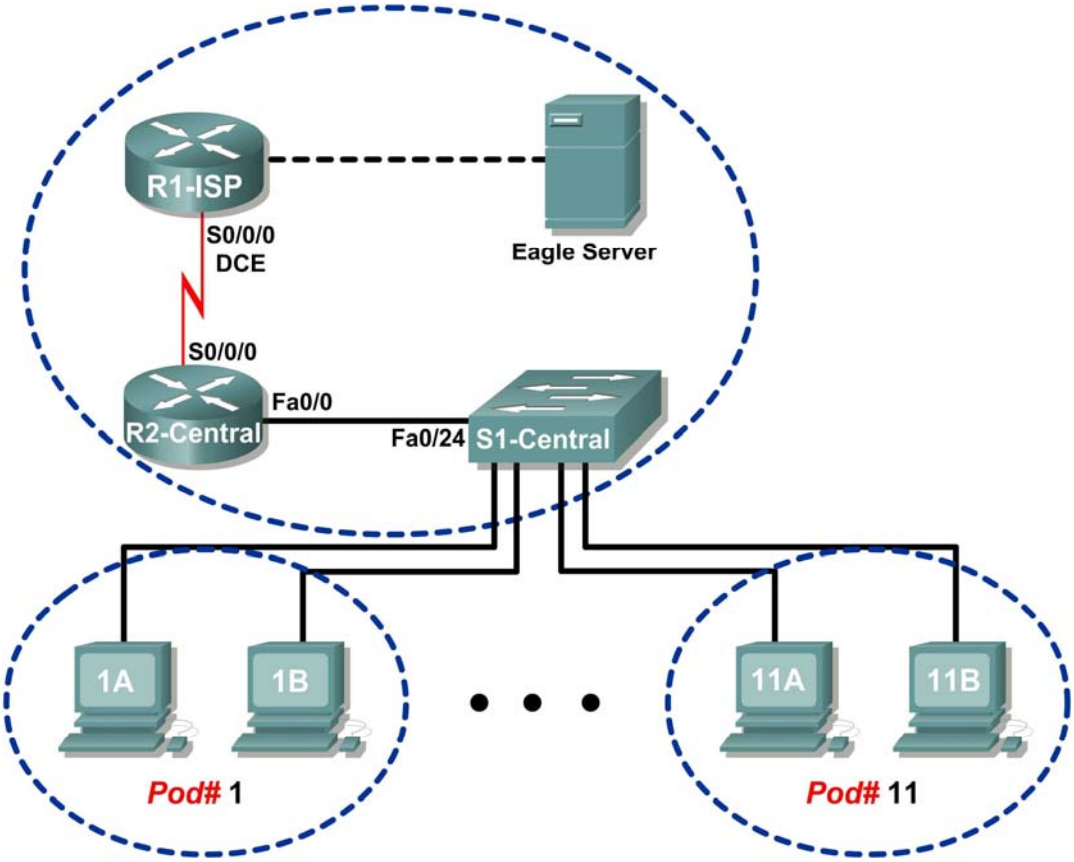
# Laboratório 3.4.3: Serviços de E-mail e Protocolos

## Diagrama de Topologia




## Tabela de Endereçamento

| Dispositivo | Interface | Endereço IP | Máscara de Sub-Rede | Gateway Padrão |
|---|---|---|---|---|
| **R1-ISP** | **S0/0/0** | 10.10.10.6 | 255.255.255.252 | *N/A* |
| | **Fa0/0** | 192.168.254.253 | 255.255.255.0 | *N/A* |
| **R2-Central** | **S0/0/0** | 10.10.10.5 | 255.255.255.252 | 10.10.10.6 |
| | **Fa0/0** | 172.16.255.254 | 255.255.0.0 | *N/A* |
| **Eagle Server** | *N/A* | 192.168.254.254 | 255.255.255.0 | 192.168.254.253 |
| | *N/A* | 172.31.24.254 | 255.255.255.0 | *N/A* |
| **host***Pod#***A** | *N/A* | **172.16.** *Pod#.*1 | 255.255.0.0 | 172.16.255.254 |
| **host***Pod#***B** | *N/A* | **172.16.** *Pod#.*2 | 255.255.0.0 | 172.16.255.254 |
| **S1-Central** | *N/A* | 172.16.254.1 | 255.255.0.0 | 172.16.255.254 |

## Objetivos

Com a conclusão deste laboratório, você será capaz de:

- Configurar o computador para serviço de e-mail
- Capturar e analisar comunicação de e-mail entre o computador e um servidor de e-mail

## Contexto

O e-mail é um dos serviços de rede mais populares que utiliza um modelo cliente/servidor. O cliente de e-mail é configurado no computador de um usuário para se conectar a um servidor de e-mail. A maioria dos provedores de serviços de Internet (ISPs) fornece instruções passo a passo para uso dos serviços de e-mail; consequentemente, o usuário típico pode não estar conscientizado das complexidades do e-mail ou dos protocolos usados.

Em ambientes de rede onde o cliente MUA deve se conectar a um servidor de e-mail em outra rede para enviar e receber e-mail, os dois protocolos a seguir são usados:

- O Protocolo SMTP foi originalmente definido no RFC 821, em agosto de 1982, e passou por muitas modificações e aprimoramentos. O RFC 2821 de abril de 2001 consolida e atualiza antigos RFCs relacionados a e-mail. O servidor SMTP ouve a porta 25 TCP. O SMTP é usado para enviar mensagens de e-mail do cliente de e-mail externo ao servidor de e-mail, entregar e-mail a contas locais e retransmitir e-mail entre servidores SMTP.
- O Protocolo POPv3 — é usado quando um cliente de e-mail externo deseja receber mensagens de e-mail do servidor de e-mail. O servidor POPv3 ouve a porta 10 TCP bastante conhecida.
- **Protocolo de Acesso a Mensagens na Internet (IMAP)** — Um protocolo que permite a um servidor central fornecer acesso remoto a mensagens de e-mail. IMAP ouve a porta 143 TCP bastante conhecida.

Neste laboratório, você usará IMAP ao invés de POP para entrega de e-mail ao cliente.

Versões mais recentes de ambos os protocolos não devem ser usadas. Ainda, existem versões seguras de ambos os protocolos que empregam protocolo SSL/TSL para comunicação.

O e-mail está sujeito a múltiplas vulnerabilidades de seguranças de computador. Ataques de spam inundam as redes com e-mail inútil e não solicitado, consumindo largura de banda e recursos de rede. Servidores de e-mail tiveram inúmeras vulnerabilidades, que deixaram o computador exposto para uma possível exploração.

## Cenário

Neste laboratório, você irá configurar e usar uma aplicação de cliente de e-mail para se conectar aos serviços de rede do eagle-server. Você irá monitorar a comunicação com o Wireshark e analisar os pacotes capturados.

Um cliente de e-mail como o Outlook Express ou o Mozilla Thunderbird será usado para se conectar ao serviço de rede do eagle-server. O eagle-server possui serviços de e-mail SMTP pré-configurados, com contas de usuário capazes de enviar e receber mensagens externas de e-mail.

### Tarefa 1: Configurando o Computador para Serviço de E-mail

O laboratório deve estar configurado como mostra o Diagrama de Topologia e a tabela de endereço lógico. Caso não esteja, peça auxílio ao instrutor antes de prosseguir.

#### Passo 1: Fazer o download e instalar o Mozilla Thunderbird.

Caso o Thunderbird não esteja instalado no computador host pod, pode ser baixado do eagle-server.example.com. Veja Figura 1. O URL do download é `ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter3/`.

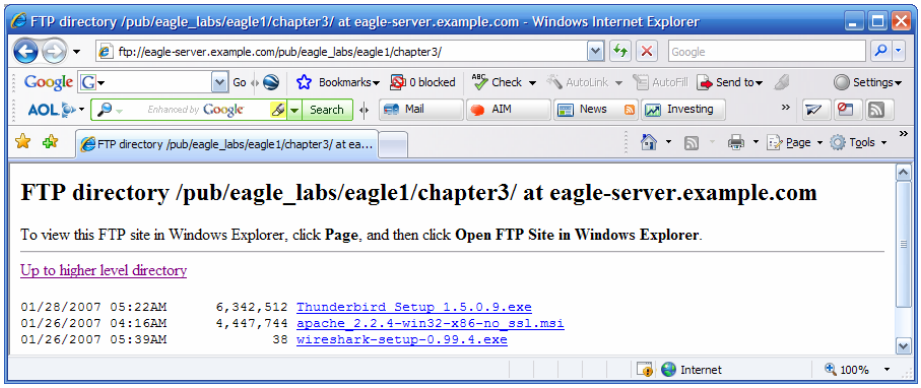



**Figura 1. Download FTP para Wireshark**

1. Clique duplo com o botão direito do mouse no nome do arquivo Thunderbird e, então, salve o arquivo ao computador pod host.

Nota: Dependendo da velocidade da conexão do link entre dois roteadores e da quantidade de estudantes baixando o arquivo, este download pode ser lento.

2. Quando o download do arquivo estiver completo, dê duplo clique no nome do arquivo e instale o Thunderbird com as configurações padrão.
3. Quando a instalação estiver completa, inicie o Thunderbird.

**Passo 2: Configurar o Thunderbird para receber e enviar mensagens de e-mail.**

1. Se levado às Opções de Importar, selecione **Não importar nada** e selecione **Próximo.**
2. Quando o Thunderbird for iniciado, as configurações de conta de e-mail devem estar feitas. Na Configuração da Nova Conta, selecione **Conta de e-mail** e selecione **Próximo**.
3. Preencha as informações de Conta como segue:

| Campo | Valor |
|---|---|
| Nome da Conta | O nome da conta é baseado no computador. Existe um total de 22 contas configuradas no Eagle Server, com o rótulo ccna[1..22]. Se este host estiver em Pod1, Host A, o nome da conta é `ccna1`. Se o host estiver em Pod 3, Host B, o nome da conta é `ccna6`. E por aí vai. |
| Seu Nome | Use o mesmo nome acima. |
| Endereço de e-mail | *Your_name*@example.com |
| Tipo de servidor de entrada sendo usado | `IMAP` |
| Servidor de Entrada (IMAP) | `Eagle-server.example.com` |
| Servidor de Saída (SMTP) | `Eagle-server.example.com` |
| Nome do Usuário de Entrada | Use o mesmo nome acima. |
| Nome da Conta | *Your_name*@eagle-server.example.com |

4. Quando o Thunderbird inicia, você pode ser estimulado a fornecer uma senha para a sua conta de e-mail. Nesta tela, selecione **Cancelar**

O cliente Thunderbird precisa ter a entrada no servidor SMTP desabilitada. Para fazer isso, selecione **Ferramentas > Configurações de Conta>Servidor de Saída (SMTP).** Depois, na tela do servidor de Saída, selecione **Editar**. Veja a Figura 2.

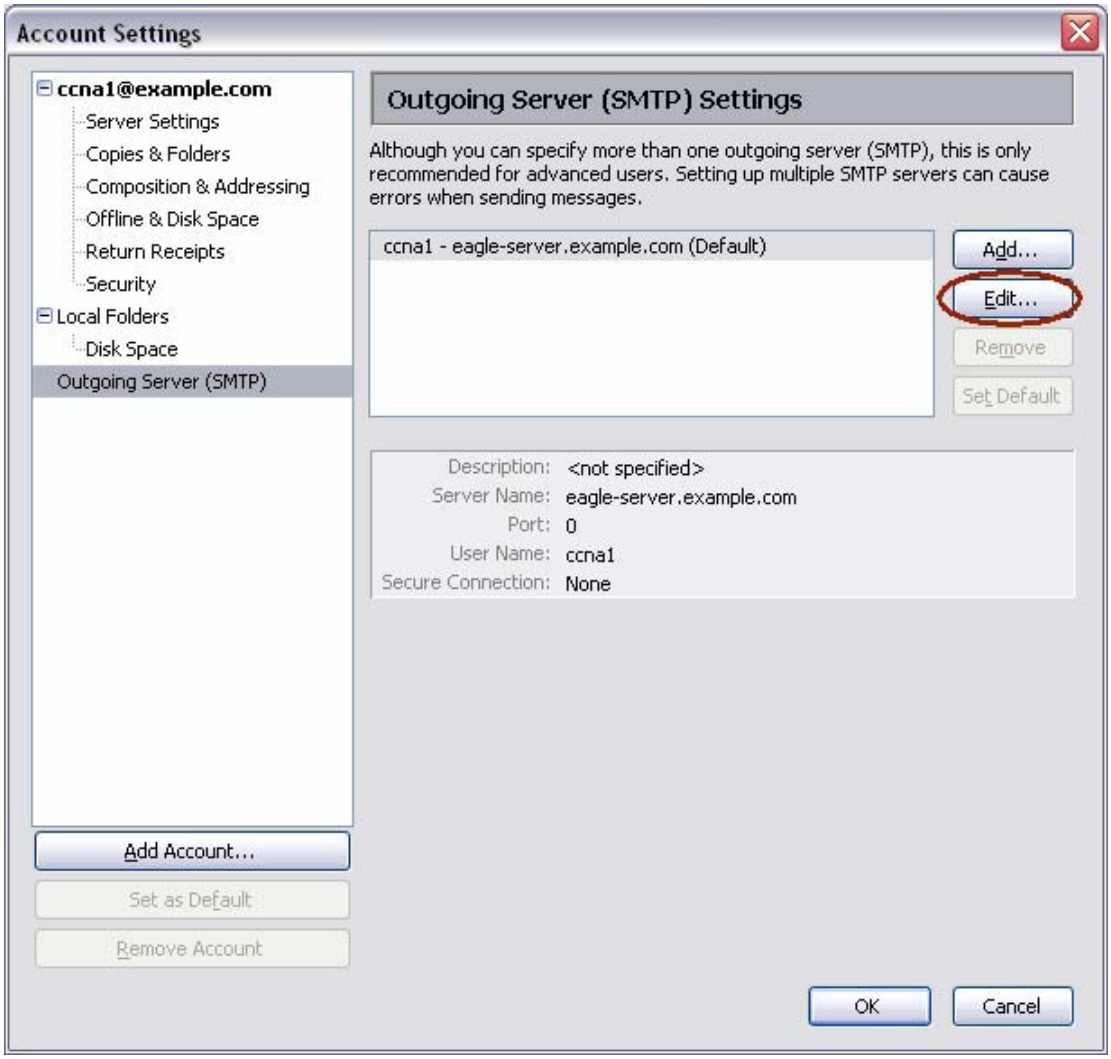



**Figura 2. Tela de Configurações de Servidor do Thunderbird**

Na tela Servidor SMTP, tire a seleção da caixa “Nome de Usuário e senha” e selecione OK nas duas telas. Veja a Figura 3.

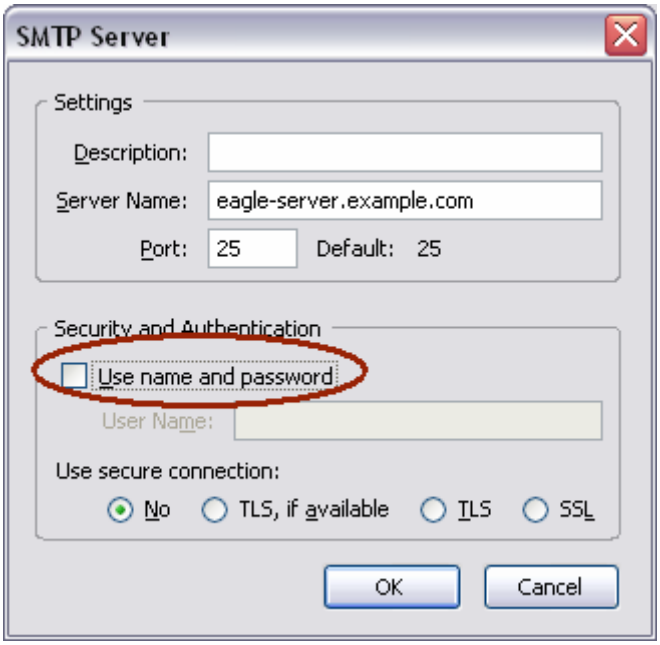



**Figura 3. Editar o servidor SMTP**

5. Você também pode desejar verificar as configurações da conta em **Ferramentas > Configurações de Conta**. Veja a Figura 4.

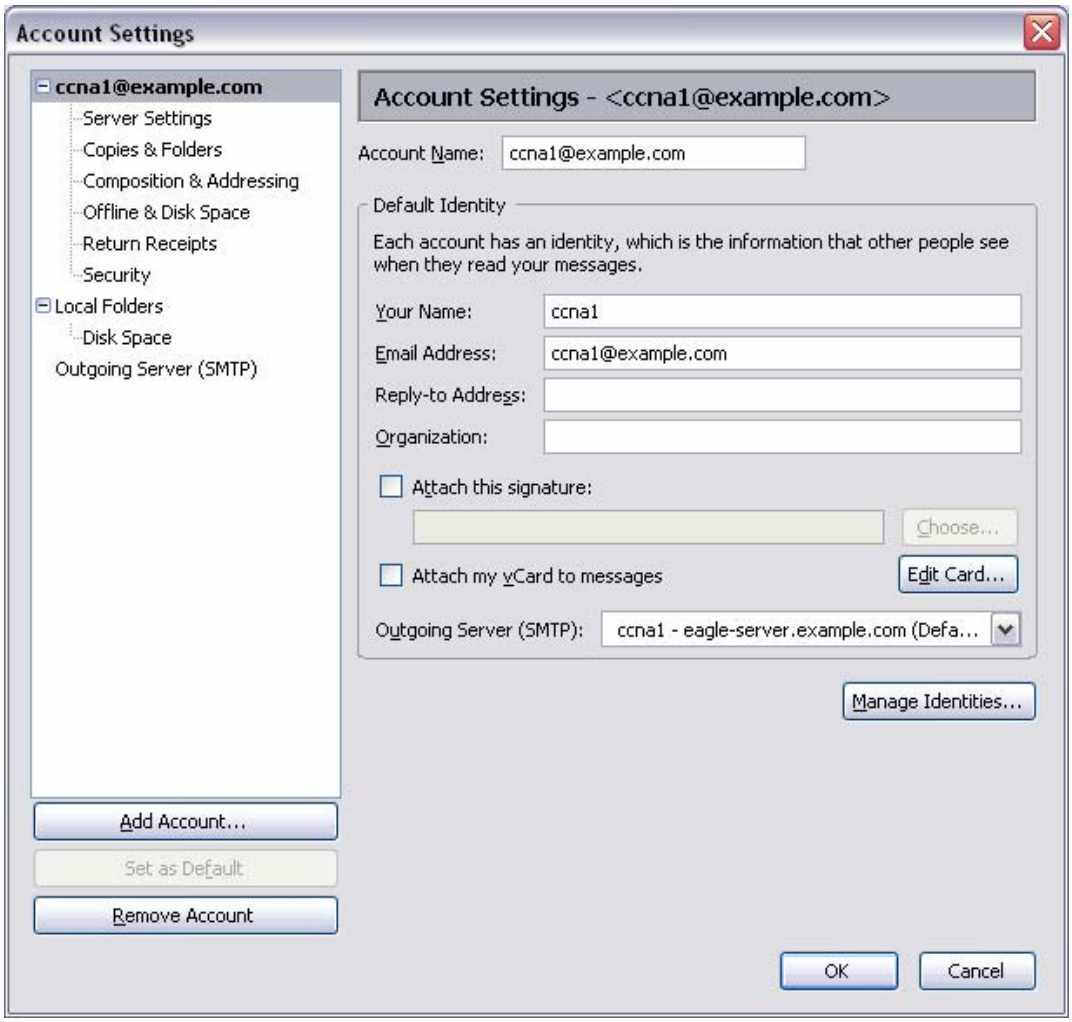



**Figura 4. Configurações de Conta do Thunderbird**

6. Na seção da esquerda da tela de Configurações de Conta, clique em **Configurações de Servidor**. Uma tela similar à exibida na Figura 5 será exibida.

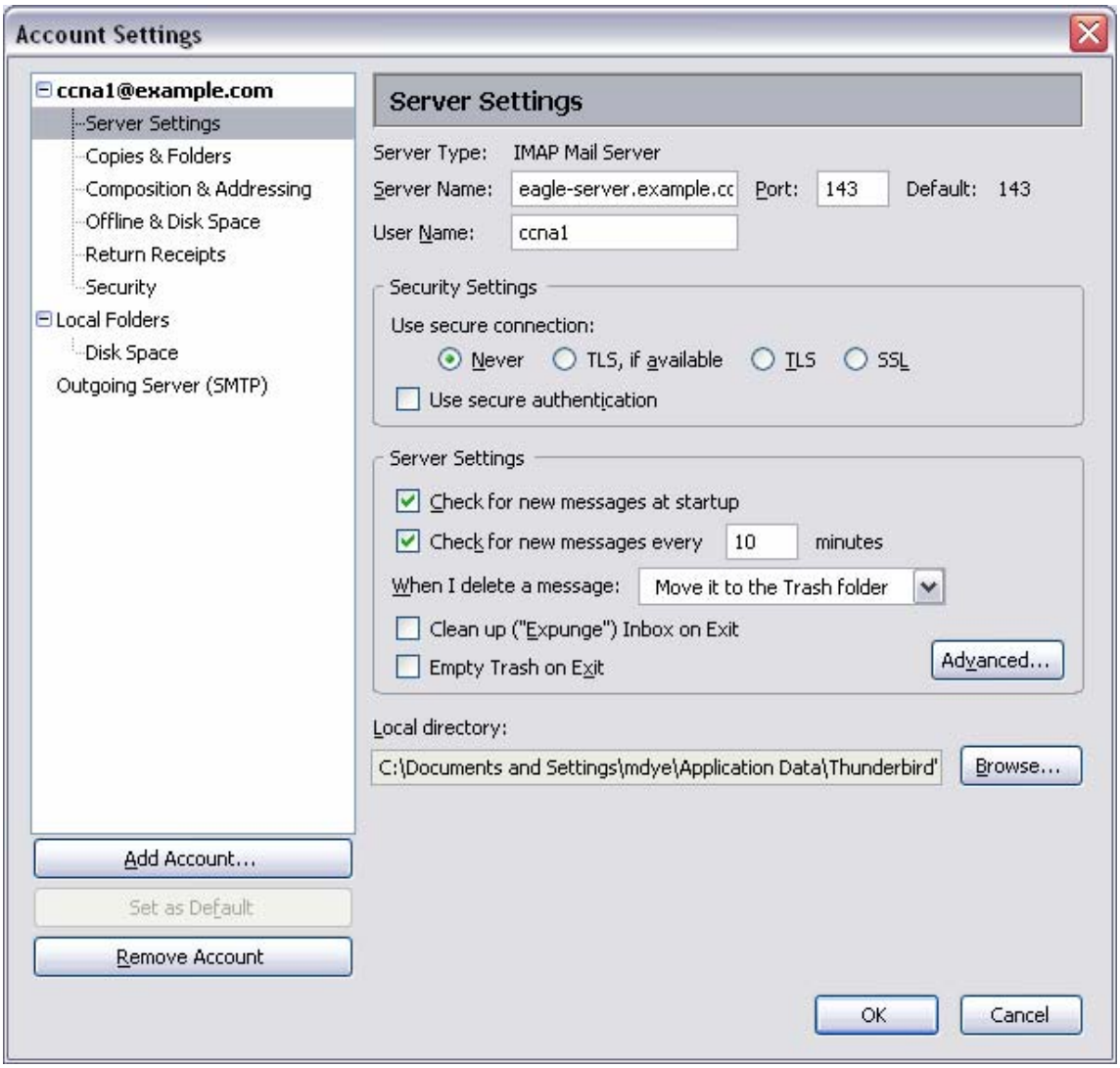



**Figura 5. Tela de Configurações do Servidor Thunderbird**

Qual é o propósito do protocolo SMTP e qual é o número de porta TCP?

_____

_____

## Tarefa 2: Capturando e Analisando Comunicação de E-mail entre o Computador e um Servidor de E-mail

### Passo 1: Enviar um e-mail não capturado.

1. Peça o nome de e-mail de outro aluno na sala.
2. Para criar e enviar um e-mail, selecione o ícone “Escrever”. Usando este nome, cada um de vocês deve compor e enviar uma mensagem de e-mail um para o outro.
3. Quando os e-mails tiverem sido enviados, verifique seu e-mail. Para verificar seu e-mail, você deve estar conectado. Se você não tiver conectado anteriormente, insira **cisco** como a senha. Observe que esta é a senha padrão que está incorporada ao servidor Eagle.

### Passo 2: Iniciar as capturas do Wireshark.

Quando estiver certo de que a operação do e-mail está funcionando de maneira adequada para envio e recebimento, inicie uma captura Wireshark. O Wireshark exibirá capturas baseadas no tipo de pacote.

### Passo 3: Analisar uma sessão de captura Wireshark de SMTP.

1. Usando o cliente de e-mail, envie e receba novamente um e-mail a um colega. Desta vez, entretanto, as transações de e-mail serão capturadas.
2. Após enviar e receber uma mensagem de e-mail, pare a captura Wireshark. Uma captura Wireshark parcial de uma mensagem de e-mail em saída usando o SMTP é exibida na Figura 6.

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 0.000000 | 172.16.1.1 | 172.16.255.255 | NBNS | Name query NB WORKGROUP<1b> |
| 2 | 0.741371 | 172.16.1.1 | 172.16.255.255 | NBNS | Name query NB WORKGROUP<1b> |
| 3 | 1.492443 | 172.16.1.1 | 172.16.255.255 | NBNS | Name query NB WORKGROUP<1b> |
| 4 | 3.306445 | 172.16.1.1 | 192.168.254.254 | TCP | 1250 > smtp [SYN] Seq=0 Len=0 MSS=1460 |
| 5 | 3.306968 | 192.168.254.254 | 172.16.1.1 | TCP | smtp > 1250 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=14 |
| 6 | 3.307012 | 172.16.1.1 | 192.168.254.254 | TCP | 1250 > smtp [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 7 | 3.313519 | 192.168.254.254 | 172.16.1.1 | SMTP | Response: 220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13 |
| 8 | 3.353004 | 172.16.1.1 | 192.168.254.254 | SMTP | Command: EHLO [172.16.1.1] |
| 9 | 3.353436 | 192.168.254.254 | 172.16.1.1 | TCP | smtp > 1250 [ACK] Seq=90 Ack=20 Win=5840 Len=0 |
| 10 | 3.353657 | 192.168.254.254 | 172.16.1.1 | SMTP | Response: 250-localhost.localdomain Hello host-1.example.com [1 |
| 11 | 3.356823 | 172.16.1.1 | 192.168.254.254 | SMTP | Command: MAIL FROM:<ccna1@example.com> SIZE=398 |
| 12 | 3.359743 | 192.168.254.254 | 172.16.1.1 | SMTP | Response: 250 2.1.0 <ccna1@example.com>... Sender ok |
| 13 | 3.363127 | 172.16.1.1 | 192.168.254.254 | SMTP | Command: RCPT TO:<ccna2@example.com> |
| 14 | 3.365007 | 192.168.254.254 | 172.16.1.1 | SMTP | Response: 250 2.1.5 <ccna2@example.com>... Recipient ok |
| 15 | 3.367680 | 172.16.1.1 | 192.168.254.254 | SMTP | Command: DATA |
| 16 | 3.368230 | 192.168.254.254 | 172.16.1.1 | SMTP | Response: 354 Enter mail, end with "." on a line by itself |
| 17 | 3.376881 | 172.16.1.1 | 192.168.254.254 | SMTP | Message Body |
| 18 | 3.387830 | 192.168.254.254 | 172.16.1.1 | SMTP | Response: 250 2.0.0 l0S8dIOY005299 Message accepted for delive |
| 19 | 3.395347 | 172.16.1.1 | 192.168.254.254 | SMTP | Message Body |
| 20 | 3.395855 | 192.168.254.254 | 172.16.1.1 | SMTP | Response: 221 2.0.0 localhost.localdomain closing connection |
| 21 | 3.395897 | 192.168.254.254 | 172.16.1.1 | TCP | smtp > 1250 [FIN, ACK] Seq=564 Ack=502 Win=6432 Len=0 |
| 22 | 3.395929 | 172.16.1.1 | 192.168.254.254 | TCP | 1250 > smtp [ACK] Seq=502 Ack=565 Win=63677 Len=0 |
| 23 | 3.405772 | 172.16.1.1 | 192.168.254.254 | TCP | 1250 > smtp [FIN, ACK] Seq=502 Ack=565 Win=63677 Len=0 |
| 24 | 3.406204 | 192.168.254.254 | 172.16.1.1 | TCP | smtp > 1250 [ACK] Seq=565 Ack=503 Win=6432 Len=0 |

**Figura 6. Captura SMTP**

3. Destaque a primeira captura SMTP na janela superior do Wireshark. Na Figura 6, esta é a linha número 7.
4. Na segunda janela do Wireshark, expanda o registro do Simple Mail Transfer Protocol.

   Existem muitos tipos diferentes de servidores SMTP. Ataques maliciosos podem obter conhecimento valioso simplesmente ao conhecer o tipo e a versão do servidor SMTP.

Qual é o nome e a versão do servidor SMTP?

_____

Aplicações de cliente de e-mail enviam comandos a servidores de e-mail e servidores de e-mail enviam respostas. Em toda primeira troca SMTP, o cliente de e-mail envia o comando **EHLO**. No entanto, a sintaxe pode variar entre os clientes e o comando também pode ser **HELO** ou **HELLO**. O servidor de e-mail deve responder ao comando.

Qual é a resposta do servidor SMTP ao comando EHLO?

_____

As próximas trocas entre o cliente de e-mail e o servidor contêm informações de e-mail. Usando sua captura Wireshark, preencha as respostas do servidor de e-mail aos comandos do cliente de e-mail:

| Cliente de E-mail | Servidor de E-mail |
|---|---|
| MAIL DE:,ccna1@excmaple.com> | |
| RCPT PARA:<ccna2@example.com> | |
| DADOS | |
| (corpo da mensagem é enviado) | |

Qual é o conteúdo do corpo da última mensagem do cliente de e-mail?

_____

Como o servidor de e-mail responde?

_____

## Tarefa 3: Desafio

Utilize um computador que tenha acesso à Internet. Procure o nome do servidor SMTP e descubra se a versão possui falhas ou vulnerabilidades conhecidas. Existe uma nova versão disponível?

## Tarefa 4: Reflexão

O e-mail é provavelmente o serviço de rede mais comum usado. Entender o fluxo de tráfego com o protocolo SMTP o ajudará a entender como o protocolo gerencia a conexão de dados cliente/servidor. O e-mail também pode passar por problemas de configuração. Há algum problema com o cliente de e-mail ou o servidor de e-mail? Uma maneira simples de testar a operação do servidor SMTP é usar o utilitário Telnet da linha de comando Windows para fazer a conexão Telnet ao servidor SMTP.

1. Para testar a operação SMTP, abra a janela de linha de comando Windows e inicie uma sessão Telnet com o servidor SMTP.

```
C:\>telnet eagle-server.example.com 25
220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13.1; Sun, 28 Jan
2007 20:41:0
3 +1000
HELO eagle-server.example.com
250 localhost.localdomain Hello [172.16.1.2], prazer em conhecer
```

```
MAIL De: ccna2@example.com
250 2.1.0 ccna2@example.com... Remetente ok
RCPT Para: instructor@example.com
250 2.1.5 instructor@example.com... Destinatário ok
DADOS
354 Favor iniciar entrada de mail.
teste de servidor SMTP de e-mail...
.
250 Mail em fila para entrega.
SAIR
221 Fechando conexão. Adeus.
Conexão ao host perdida.
C:\ >
```

## Tarefa 5: Limpeza

Se o Thunderbird foi instalado no computador para este laboratório, o instrutor pode querer que o aplicativo seja removido. Para remover o Thunderbird, clique em **Iniciar > Painel de Controle > Adicionar ou Remover Programas**. Clique em **Thunderbird** e depois clique em **Remover**.

A menos que não solicitado pelo instrutor, desligue os computadores. Remova qualquer coisa que tenha sido trazida ao laboratório e deixe a sala pronta para a próxima aula.