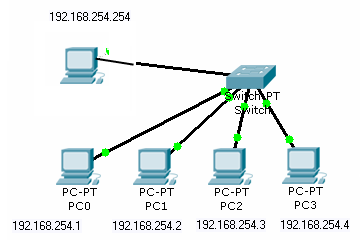
# Lab 7: E-mail Services and Protocols

## Topology Diagram



## Learning Objectives

Upon completion of this lab, you will be able to:

* Configure an e-mail server
* Configure the host computers for e-mail service
* Capture and analyze e-mail communication between the host computer and a mail server

## Background

E-mail is one of the most popular network services that uses a client/server model. The e-mail client is configured on a user’s computer, and configured to connect to an e-mail server. Most Internet service providers (ISPs) provide step-by-step instructions for using e-mail services; consequently, the typical user may be unaware of the complexities of e-mail or the protocols used.

In network environments where the MUA client (mail user agent) must connect to an e-mail server on another network to send and receive e-mail, the following three protocols are used:

* Simple Mail Transfer Protocol (SMTP). The SMTP server listens on well-known TCP port 25. SMTP is used to send e-mail messages from the external e-mail client to the e-mail server, deliver e-mail to local accounts, and relay e-mail between SMTP servers.
* Post Office Protocol version 3 (POPv3) — is used when an external e-mail client wishes to receive e-mail messages from the e-mail server. The POPv3 server listens on well-known TCP port 110. **In this lab you will use POP3 for delivery of e-mail to the client.**
* Internet Message Access Protocol (IMAP) An internet protocol that allows a central server to provide remote access to e-mail. Uses TCP port 143. Scenario

In this lab, you will configure and use an e-mail client application to connect to the **email-server** network services. You will monitor the communication with Wireshark and analyze the captured packets.

You will use the e-mail client **Mozilla Thunderbird** to connect to the server network service. You must create e-mail accounts on the server and then configure it.

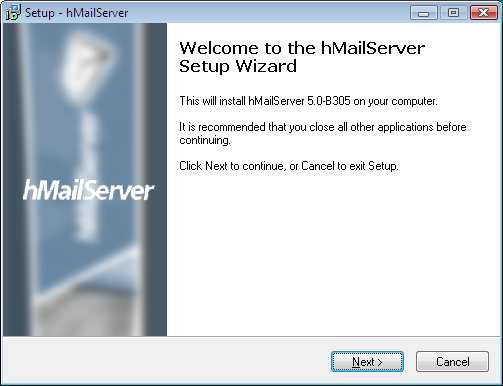
The e-mail server software you will use today is a freeware piece of software called **hMailserver** – a copy of the application is placed on the S; drive

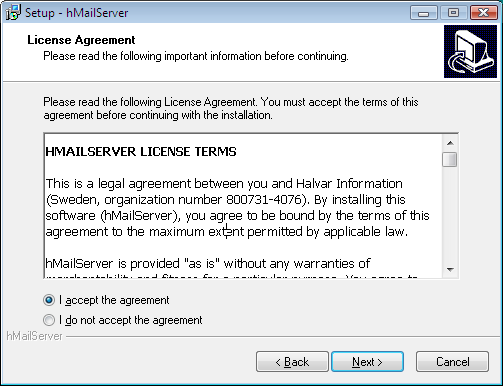
Additionally, download **Mozilla Thunderbird from the S: drive** and install it on each client PC. Ensure Wireshark is available on you PC and this lab handout is on the local drive.

## Task 1: Having downloaded all the necessary software to the local c: drive, remove the PCs from the college LAN and build the topology shown above. Set the necessary static IP addresses.

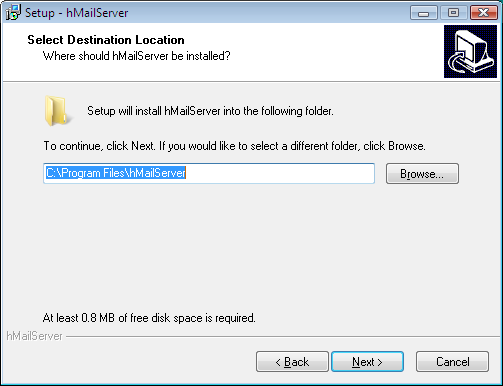
## Task 2: Install hMailserver on one PC – the other PC’s are clients.

* Double-click on the downloaded file to launch the setup. The first dialog which is shown is the Welcome dialog, in this one, simply click Next.

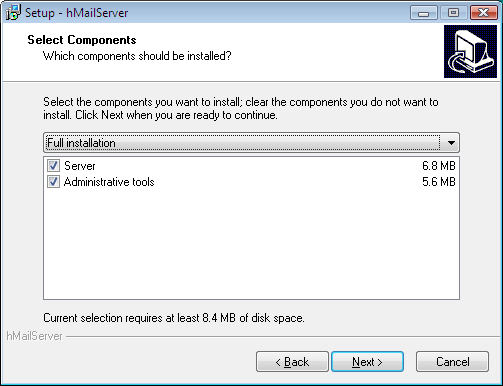


* The next step is to read the license agreement. If you don't accept the license agreement, please cancel the installation. If you agree, select "I accept the agreement" and click next.
* 

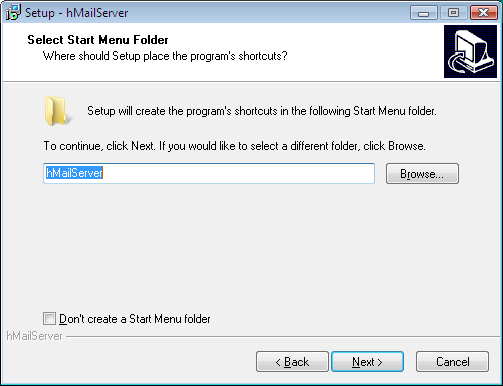
* Select the destination folder and click Next. You should select a local drive and not a network folder. It is possible to install hMailServer on removable devices, but you will not be able to run hMailServer from the device on another computer.



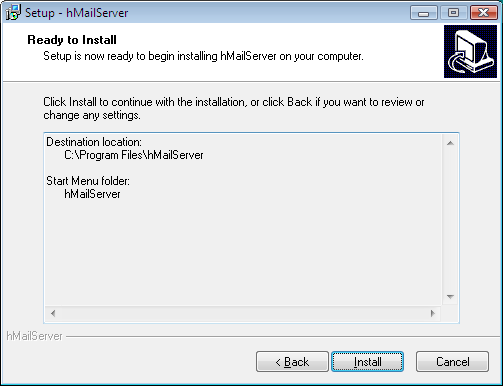
* Select which components you want to install and click Next. On the server, you should install all available components. If you have already installed the hMailServer server on another computer and you want to manage that remotely, you only need to install the Administrative tools.



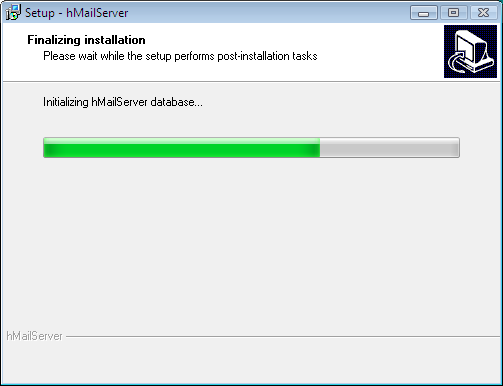
* Select which start menu folder you want to place the hMailServer icons in and click Next.



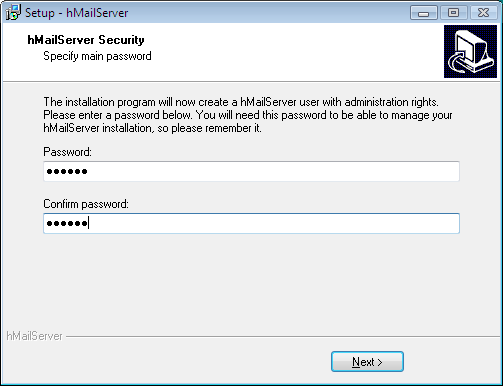
* Confirm that the settings are correct and then click Install to do the installation.



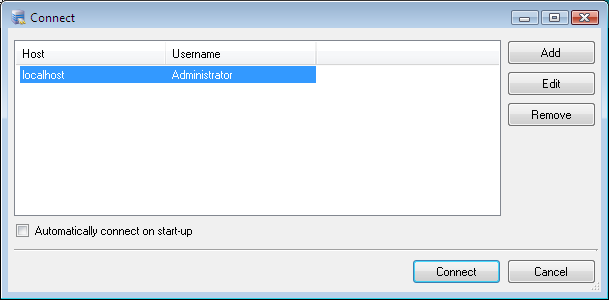
* Wait... The installation should take about 10-20 seconds.



* After the files have been installed, you need to provide the installation program with a main hMailServer password. In 4.3 and later, a main password is used to increase security. The password can be anything you like as long as it's longer than 5 characters. You will need the password later on when performing server administration, so don't forget it. You only need to specify the password the first time you install hMailServer



* After you have finished the installation, it's time to start hMailServer Administrator (found in the start menu). The first thing which appears is the Connect dialog. This dialog allows you to connect to different hMailServer installations in your network. Normally, you will want to connect to localhost. Select localhost, and click Connect. In the password dialog, enter your main hMailServer password and click OK.



## Task 3: Configure hMailServer

1. From the Start menu, select hMailServer Administrator  
   Now the hMailServer Administrator - Connect dialog is opened. This dialog allows you to connect to different hMailServer services.
2. Double-click on the "localhost" host name to connect to the hMailServer instance running on localhost.
3. In the password dialog, specify the password you specified during the installation of hMailServer - the main hMailServer administration password, and then click OK
4. Now hMailServer Administrator is started.

## Domains & Accounts

Every hMailServer domain should be connected to an internet domain. Say that you're the owner of the domain hcit.com, then you should add hcit.com as a domain in hMailAdmin:

1. Start hMailAdmin.
2. Click Add domain.
3. Enter hcit.com as domain name.
4. Click Save

The next step is to add accounts to your server. The normal setup is to have one account per email address you want to be able to send and receive email from. If you want the addresses fergus@hcit.com , simply add this to hMailAdmin: Add an account for each client PC.

1. Start hMailAdmin
2. Expand the Domains node in the tree to the left
3. Click on the domain hcit.com
4. Click Add account
5. Enter fergus as the account address, set the password and click Save

## Specifying public host name

For an email server to work properly, it needs to know its public name on the Internet. This is normally something like mailserver.hcit.com. Since there is no good way for software to automatically detect the public host name of the computer where it is running, you need to tell hMailServer what public hostname to use. While it's possible to run hMailServer without telling it its public hostname, some email servers will reject email from you if you don't specify it.

1. Start hMailAdmin
2. In the tree to the left, go to Settings -> Protocols -> SMTP
3. To the right, the SMTP settings are now shown. Click on the Delivery of e-mail tab.
4. Under host name, enter the public hostname, mailserver.hcit.com, of the computer where hMailServer is running.
5. Save the change

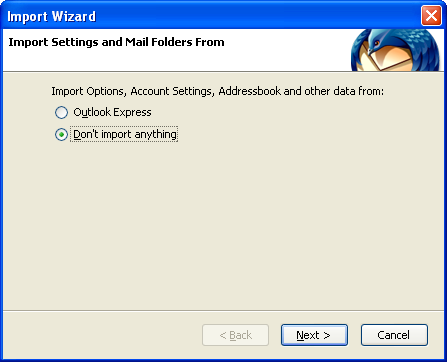
## Turn off SMTP authentication

1. Open Settings/Advanced/IP Ranges and make sure the SMTP authentication settings are unchecked for both the My Computer and Internet ranges.
2. Finally turn of Auto-Ban

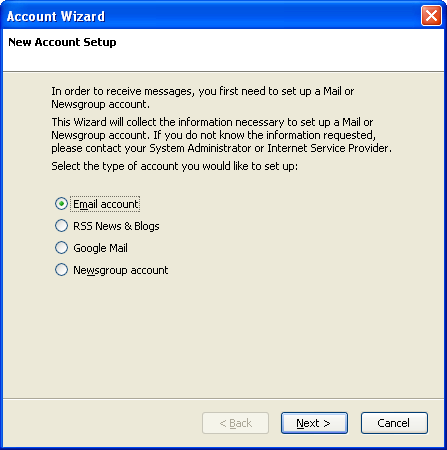
Task 4: Configure the Client Computers for E-mail Service.

Step 2: Configure Thunderbird to receive and send e-mail messages.

1. Install Mozilla Thunderbird. During the install process you will be asked if you wish to import settings – don’t import any existing settings.



1. Select to setup an E-mail account.



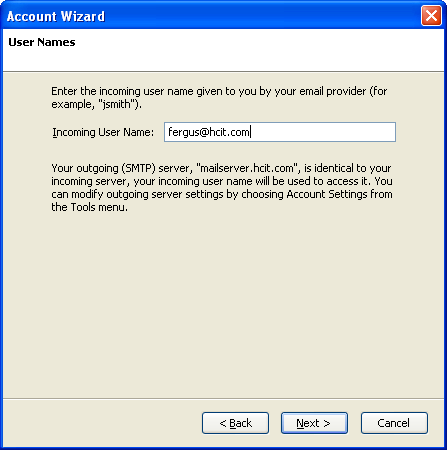
1. Enter you display name and your email address.



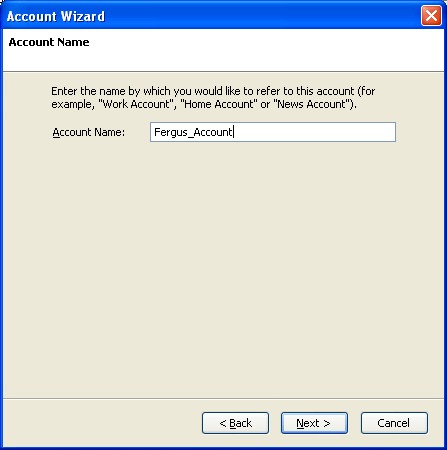
1. Fill in the server information and select the POP protocol. We don’t have a DNS server running to resolve our e-mail server domain name “mailserver.hcit.com” to an IP address so we will simply insert the IP address of the server for both the Incoming and Outgoing Servers.



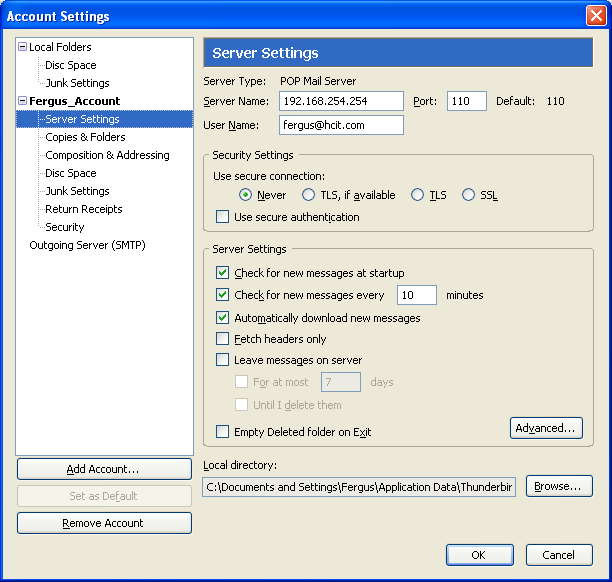
1. Enter your incoming user name – enter your e-mail address.



1. Use the default account name.



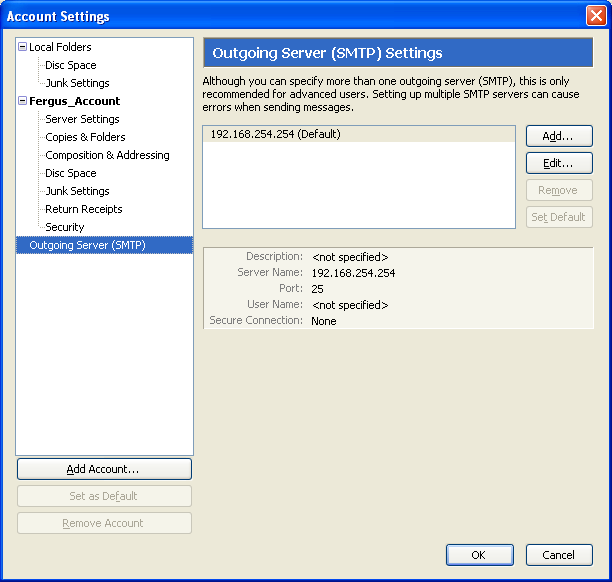
7. Verify account settings from **Tools > Account Settings**.



Thunderbird Server Settings

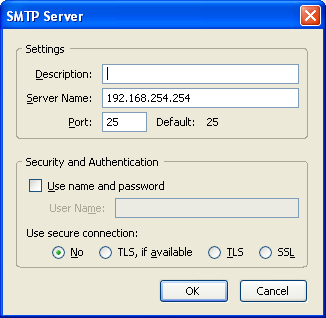
8. When Thunderbird starts, you may be prompted for a password for your email account. At this screen select “**Cancel**”

The Thunderbird client needs to have SMTP server login disabled. To do this, select **Tools > Account Settings>Outgoing Server (SMTP).** Then from the Outgoing server screen, select **Edit**.



Outgoing Server (SMTP) Settings Screen

At the SMTP Server screen, uncheck the “**Use name and password**” box and select **OK** at the two screens.



Task 4: Capture and Analyze E-mail Communication between the Host Computer and an E-mail Server.

Step 1: Send an uncaptured e-mail.

1. Install Wireshark
2. Ask another student in the class for his or her e-mail name.
3. Using this name, compose and send a friendly message to the student.

Step 2: Start Wireshark captures.

When you are certain that the e-mail operation is working properly for both sending and receiving, start a Wireshark capture. Wireshark will display captures based on packet type.

Step 3: Analyze a Wireshark capture session of SMTP.

1. Using the e-mail client, again send and receive e-mail to a classmate. This time, however, the e-mail transactions will be captured.
2. After sending and receiving one e-mail message, stop the Wireshark capture. A partial Wireshark capture of an outgoing e-mail message using SMTP is shown in Figure 5.

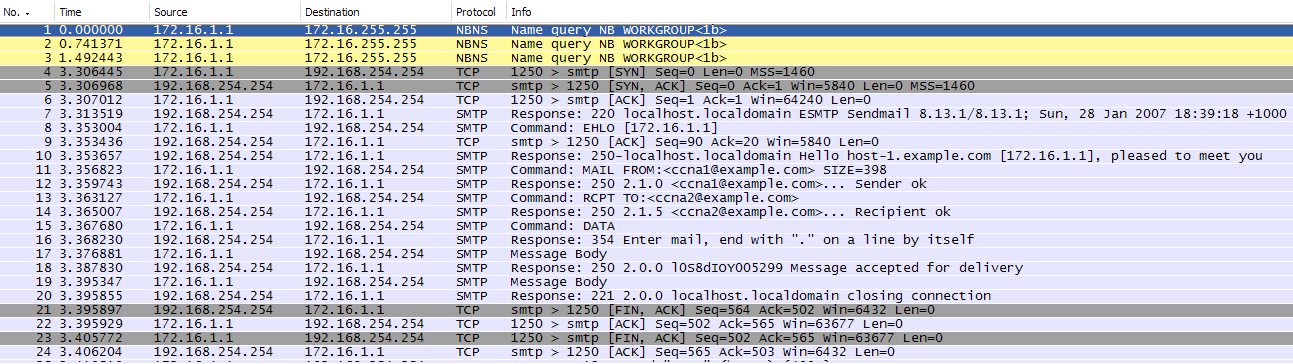


Figure 5. SMTP Capture

1. Highlight the first SMTP capture in the top Wireshark window. In Figure 5, this is line number 7.
2. In the second Wireshark window, expand the Simple Mail Transfer Protocol record.

There are many different types of SMTP servers. Malicious attackers can gain valuable knowledge simply by learning the SMTP server type and version.

What is the SMTP server name and version?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E-mail client applications send commands to e-mail servers, and e-mail servers send responses. In every first SMTP exchange, the e-mail client sends the command **EHLO**. The syntax may vary between clients, however, and the command may also be **HELO** or **HELLO**. The e-mail server must respond to the command.

What is the SMTP server response to the EHLO command?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The next exchanges between the e-mail client and server contain e-mail information. Using your Wireshark capture, fill in the e-mail server responses to the e-mail client commands:

|  |  |
| --- | --- |
| **E-mail Client** | **E-mail Server** |
| MAIL FROM:,ccna1@excmaple.com> |  |
| RCPT TO:<ccna2@example.com> |  |
| DATA |  |
| (message body is sent) |  |

What are the contents of the last message body from the e-mail client?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

How does the e-mail server respond?

\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Task 4: Clean Up

Remove Thunderbird and HMailserver and put your PC back on the college network.