Please use a Screen or Video Capture software to save your works!

Warning: Your lab 5 must be completed before you can start this lab.

In Lab 5, you configured and ran the **Postfix** application for our MTA (a.k.a. SMTP server) on your Server and Client VMs.

That setup has some major drawbacks:

- It required an SMTP server (**MTA**) to be configured on each machine.
- The Message Store (**MS**) would also be unique to each machine - what a user received on one server would not exist on any other.

In this lab you will centralize some of this information, so that a user can send email from any machine in the network, and have incoming mail sent to a centralized messages store.

The diagram below (duplicate to lab 5) shows your basic setup of your email system:

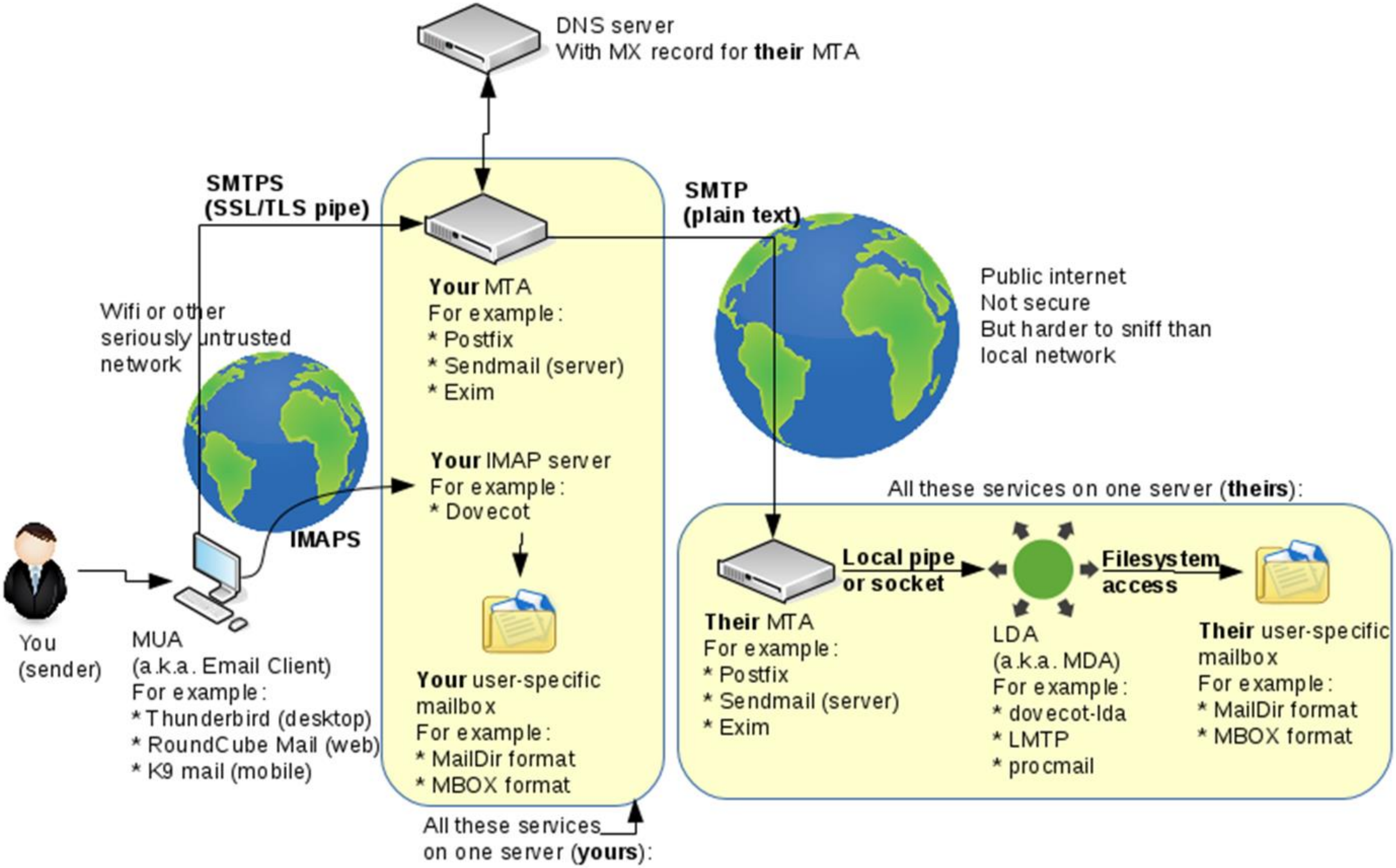


Diagram of **you** sending email to **them**

You will begin by modifying the existing **Postfix (MTA)** servers to make mail they send come from your domain (instead of each machine). Then you will add a record to your DNS server to allow mail to be sent to the domain itself, instead of the individual machines. Next, you will add a Local Delivery Agent (**LDA**) to your **Server VM** by installing **dovecot-lda**, configure it, and test it to make sure that is working correctly.

Finally, you will set up an **IMAP** server called **Dovecot** on your Server VM, so you can read your email from an MUA such as **Thunderbird** or a **Webmail** application. (You will set up a webmail application called **Roundcube** in a later lab).

Learning About the Services Involved in an Email Delivery

In reality, the terms **MTA, MDA, MUA, LDA** can actually be considered misleading since some of those services can be combined together to form a single entity (application), while other applications may operate as separate entities. There may be overlap, so if you don't find those acronyms helpful, don't worry too much about them. On the other hand, when referred to in diagrams, they can help to visualize those processes when trying to understand how an e-mail system works.

Here is an overview of those terms (from the Dovecot wiki). It is worth viewing this link.

In the diagram displayed above, the elements include:

- **User Account**. The individual who wants to send or receive mail messages.
- **MUA** (email client). This is the application that the individual uses to send or receive mail messages. It can be a **native application** or a **web application**. You will learn how to setup and use both types of these applications throughout the remainder of this course.
- Two **MTA** servers. These are the servers responsible for getting your emails to the destination server.

  - They are similar to routers (which route packets) but work on the **application** layer rather than the **network** layer.
  - In our example, there are only two MTAs - but there can be several.
  - You connect to your MTA over a **secure** connection, so your emails can't be read by the operators of the network you're connected to.
  - The mail message then travels the rest of the way to the destination MTA **unencrypted**, so anyone with access to the routers in-between can read all your emails. That is why many organizations will refuse to send you confidential information over email.
- **LDA/MDA** Server. This server will receive the email from the MTA, and will store it on disk in some format. **MailDir** and **MBOX** are the most popular mailbox formats.
- **IMAP/POP3** server(s). When sending an email, you send it to the destination using your MTA, but you also want to save it in your "**Sent**" folder for yourself. This is accomplished by a separate connection to either your **IMAP** or **POP3** server.
  - Thus, a situation can occur that although you sent your email successfully, it may never make it to your "Sent" folder - the second connection to your IMAP server is quite unrelated to the first connection to the **SMTP** server.
- **DNS** Server. A DNS server is also involved - it is needed to retrieve the address of the email server responsible for email for a particular domain. This is done with **MX** records.

Online References

Dovecot Community Documentation

Dovecot-lda

Configuring dovecot-lda with postfix

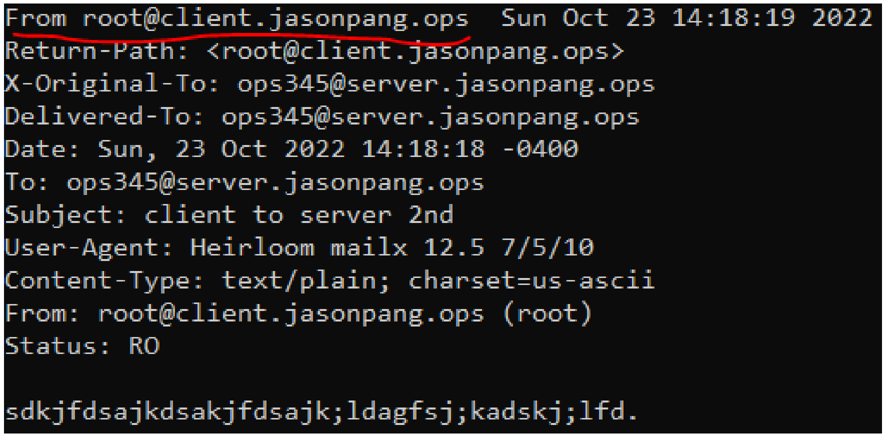
Case 1: Setup A Centralized Message Store

Setup Your MTA to Use Correct Domain

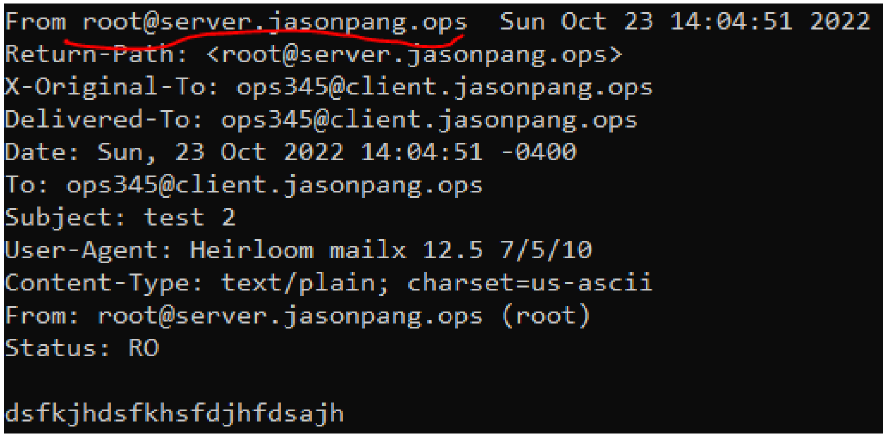
In Lab 5, both of your email servers were sending mail messages addressed from users of the actual machines themselves. This would be confusing for the receiver who might get emails from the same user such as ops345@client.yoursenecaid.ops, and ops345@server.yoursenecaid.ops. Which would they respond to? To avoid this problem from occurring, we can make all servers make the sent mail appear to come from a central location (usually the **domain**), and make incoming email sent to that address to be accessible from machines within our network.

Perform the following steps:

1. Issue the **mail** command to view the email messages you sent between your Client VM and Server VM in your lab 5. Notice that each is addressed from root on whichever machine sent it.

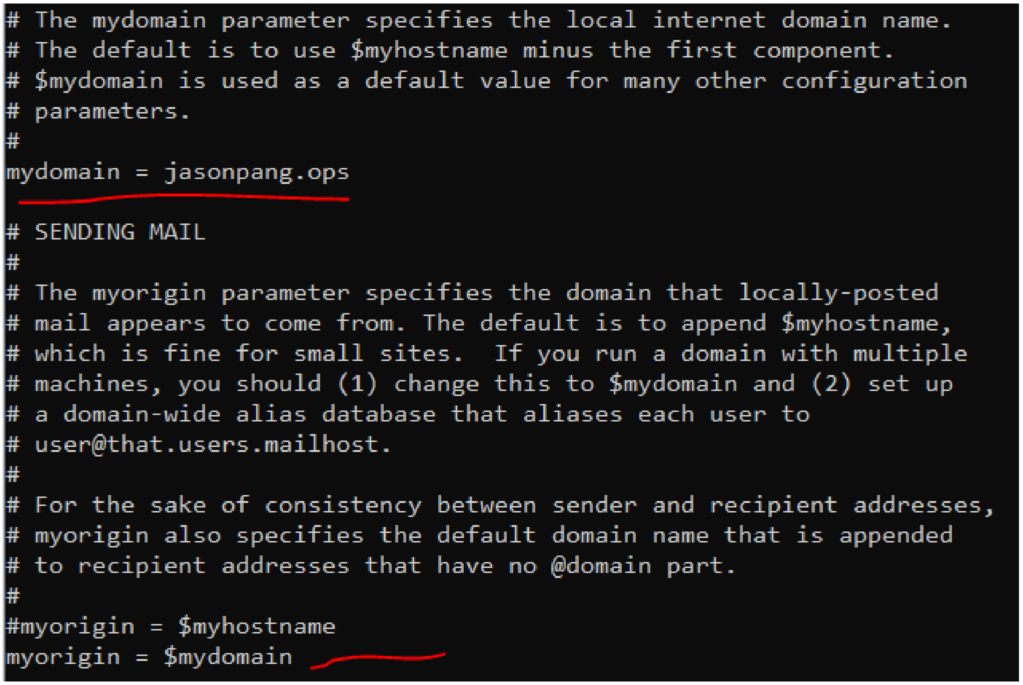


```
From root@client.jasonpang.ops  Sun Oct 23 14:18:19 2022
Return-Path: <root@client.jasonpang.ops>
X-Original-To: ops345@server.jasonpang.ops
Delivered-To: ops345@server.jasonpang.ops
Date: Sun, 23 Oct 2022 14:18:18 -0400
To: ops345@server.jasonpang.ops
Subject: client to server 2nd
User-Agent: Heirloom mailx 12.5 7/5/10
Content-Type: text/plain; charset=us-ascii
From: root@client.jasonpang.ops (root)
Status: RO

sdkjfdsajkdsakjfdsajk;ldagfsj;kadskj;lfd.
```



```
From root@server.jasonpang.ops  Sun Oct 23 14:04:51 2022
Return-Path: <root@server.jasonpang.ops>
X-Original-To: ops345@client.jasonpang.ops
Delivered-To: ops345@client.jasonpang.ops
Date: Sun, 23 Oct 2022 14:04:51 -0400
To: ops345@client.jasonpang.ops
Subject: test 2
User-Agent: Heirloom mailx 12.5 7/5/10
Content-Type: text/plain; charset=us-ascii
From: root@server.jasonpang.ops (root)
Status: RO

dsfkjhdsfkhsfdjhfdsajh
```

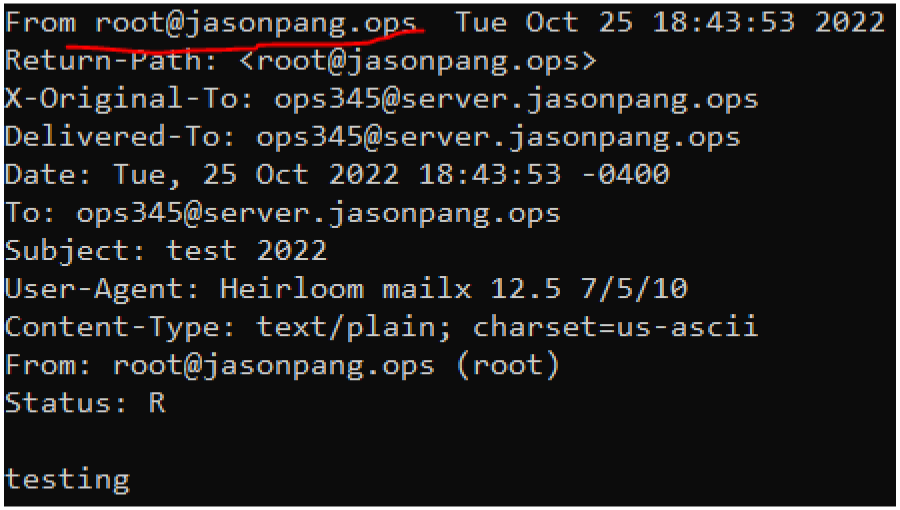
2. On both machines (Client VM and Server VM), edit the /etc/postfix/main.cf file to change the myorigin parameter from $myhostname to $mydomain. Restart the postfix service. (make sure you have the $mydomain value configured)



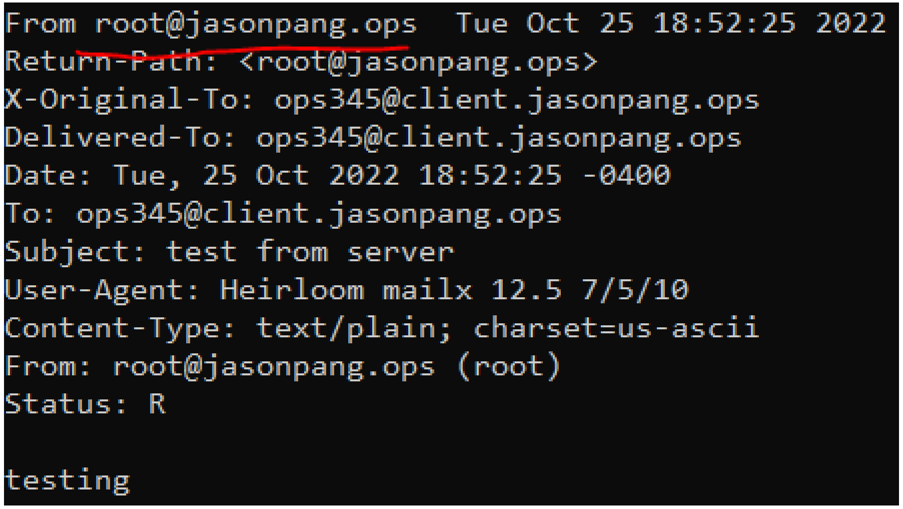
```
# The mydomain parameter specifies the local internet domain name.
# The default is to use $myhostname minus the first component.
# $mydomain is used as a default value for many other configuration
# parameters.
#
mydomain = jasonpang.ops

# SENDING MAIL
#
# The myorigin parameter specifies the domain that locally-posted
# mail appears to come from. The default is to append $myhostname,
# which is fine for small sites.  If you run a domain with multiple
# machines, you should (1) change this to $mydomain and (2) set up
# a domain-wide alias database that aliases each user to
# user@that.users.mailhost.
#
# For the sake of consistency between sender and recipient addresses,
# myorigin also specifies the default domain name that is appended
# to recipient addresses that have no @domain part.
#
#myorigin = $myhostname
myorigin = $mydomain
```

3. Now, send email messages (via the **mail** command) between both of your Client VM and Server VM machines, and view the mail messages by issuing **mail** in each VM. The sender address should now read that the received mail messages came from **root@yourdomain.ops**. If not delivered, check your iptables (tcp port 25, 53 and udp port 53) and DNS settings and try again.

   From server vm: mail -s "test from server" ops345@client.jasonpang.ops
   From client vm: mail -s "test from client" ops345@server.jasonpang.ops



```
From root@jasonpang.ops  Tue Oct 25 18:43:53 2022
Return-Path: <root@jasonpang.ops>
X-Original-To: ops345@server.jasonpang.ops
Delivered-To: ops345@server.jasonpang.ops
Date: Tue, 25 Oct 2022 18:43:53 -0400
To: ops345@server.jasonpang.ops
Subject: test 2022
User-Agent: Heirloom mailx 12.5 7/5/10
Content-Type: text/plain; charset=us-ascii
From: root@jasonpang.ops (root)
Status: R

testing
```



```
From root@jasonpang.ops  Tue Oct 25 18:52:25 2022
Return-Path: <root@jasonpang.ops>
X-Original-To: ops345@client.jasonpang.ops
Delivered-To: ops345@client.jasonpang.ops
Date: Tue, 25 Oct 2022 18:52:25 -0400
To: ops345@client.jasonpang.ops
Subject: test from server
User-Agent: Heirloom mailx 12.5 7/5/10
Content-Type: text/plain; charset=us-ascii
From: root@jasonpang.ops (root)
Status: R

testing
```

The next step is to configure what addresses that the server will receive email for. This is done using postfix by setting the **mydestination** parameter (configuration variable) to include **$mydomain** (this is assuming you've set up **mydomain, myorigin,** and **inet_interfaces** properly).

4. Edit the **/etc/postfix/main.cf** file for **Server VM ONLY**, scroll down to the line containing: **mydestination** and change line to the text shown below:

   mydestination = $mydomain, $myhostname, localhost.$mydomain, localhost

   if you want to receive email target to other domains, feel free to add to the variables.

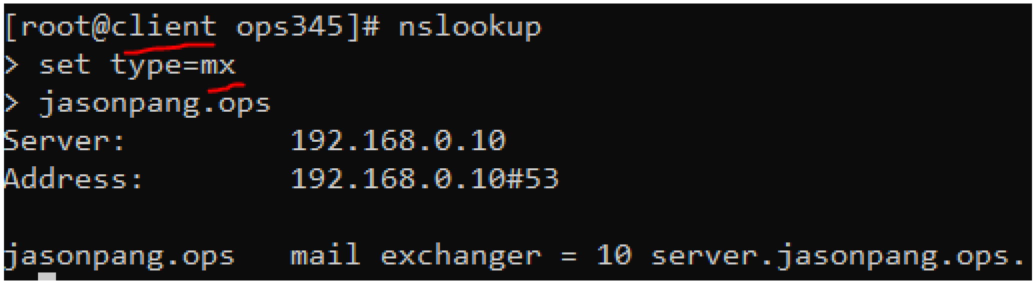
   mydestination = $mydomain, $myhostname, localhost.$mydomain, localhost, s00.ops345.com

   Note: Even though your machine's name is server.yoursenecaid.ops, your postfix MTA will also receive emails addressed to the domain called: yoursenecaid.ops and @s00.ops345.com
   For this to work, we need to add a DNS record that will point mail sent to the domain towards one of the SMTP servers configured to accept it. Either internally for your own .ops domain or externally, as the instructor demonstrated in class, who use a DDNS to point to the email server's IP address.

5. Add an MX record to the forward lookup zone on host so that all incoming mail addressed to the domain is sent to your Server VM. Include the following in your zone file (forward lookup /var/named/mydb-for-yoursenecaid-ops). Replace the green part with your own value. Restart the "named" service

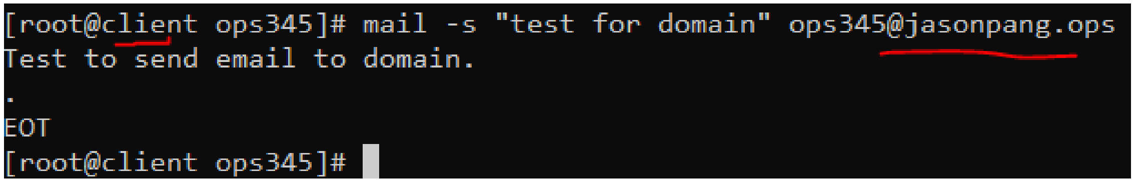
   ```
   @      IN      MX      10 server.jasonpang.ops.
   ```

6. Make sure you can confirm that your DNS can resolve the MX record. The value "10" means priority.

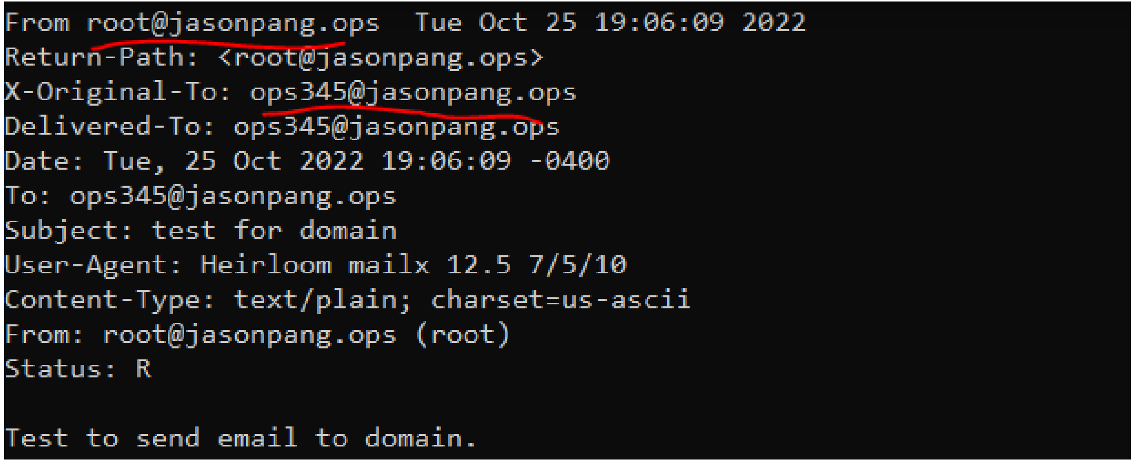


```
[root@client ops345]# nslookup
> set type=mx
> jasonpang.ops
Server:         192.168.0.10
Address:        192.168.0.10#53

jasonpang.ops   mail exchanger = 10 server.jasonpang.ops.
```

7. Send an email from your Client VM to ops345@yourdomain.ops
8. Confirm that it arrives on your Server VM machine



```
[root@client ops345]# mail -s "test for domain" ops345@jasonpang.ops
Test to send email to domain.
.
EOT
[root@client ops345]# 
```



```
From root@jasonpang.ops  Tue Oct 25 19:06:09 2022
Return-Path: <root@jasonpang.ops>
X-Original-To: ops345@jasonpang.ops
Delivered-To: ops345@jasonpang.ops
Date: Tue, 25 Oct 2022 19:06:09 -0400
To: ops345@jasonpang.ops
Subject: test for domain
User-Agent: Heirloom mailx 12.5 7/5/10
Content-Type: text/plain; charset=us-ascii
From: root@jasonpang.ops (root)
Status: R

Test to send email to domain.
```

Relay Email Through Another Server

When email is sent from either VM, it is addressed from the domain, but receiving MTAs might query why mail sent from Client VM doesn't match the address of the MX record for the domain. This would be a red-flag for potential spam. To avoid this, we can relay all mail sent from Client VM (or any other machine in our network) through Server VM so that it properly appears to come from the mail server that matches the MX record for the domain.

Perform the following steps:

1. Move to your **Client VM**.
2. Direct your **Client VM** MTA to relay mail through Server VM, by making the following editing change for the **/etc/postfix/main.cf** file:
   relayhost = server.<yourdomain>.ops
3. Restart the postfix service.
4. Next, you must instruct your **Server VM** machine to allow your Client VM machine to pass email through it by making the following editing change to the /etc/postfix/main.cf file:
   mynetworks = 192.168.0.0/24
5. Restart the postfix service.

All mail is now being delivered to a centralized location (and also appears to be coming from that same location), but a user would still have to access that server to retrieve it.

Install and Configure the Local Delivery Agent (LDA/MDA)

Postfix is capable of performing the function of an LDA, but its LDA capabilities are limited, thus postfix is generally not used for that purpose. Currently, the most popular LDA is LMTP, but we will be installing, configuring, and using an LDA called **Dovecot** since it is also popular and we will be setting up Dovecot as an

IMAP server later in this lab. Using both Postfix and Dovecot will actually increase the performance of our IMAP server.

Perform the following steps:

1. Move to your **Server VM**.
2. Dovecot wasn't installed when you installed your virtual machines in previous labs. Install the Dovecot application by issuing the following command:
   ```
   yum install dovecot
   ```
3. Edit your **/etc/postfix/main.cf** file and scroll down to (or search for) **mailbox_command**. Add the following line:
   ```
   mailbox_command = /usr/libexec/dovecot/dovecot-lda -f "$SENDER" -a "$RECIPIENT"
   ```
   NOTE: Do not replace any variables, those are set automatically by Postfix when it runs the LDA. If you are interested in learning more about the Dovecot application, you can read about dovecot-lda here and here.
4. Finally, edit the **/etc/dovecot/conf.d/10-mail.conf** file and indicate where you want your mail delivered by including the following line:
   ```
   mail_location = maildir:~/Maildir
   ```
5. Restart your postfix service.
6. The emails are still stored only on SERVER VM, but it will now easier for other machines/services to access.
7. Due to permissions on the directories where mail will now be stored, root will no longer receive mail. Check the logs for an indication as to why.

Case 2: USING THUNDERBIRD (MUA) FOR CLIENT VM and SERVER VM MACHINES

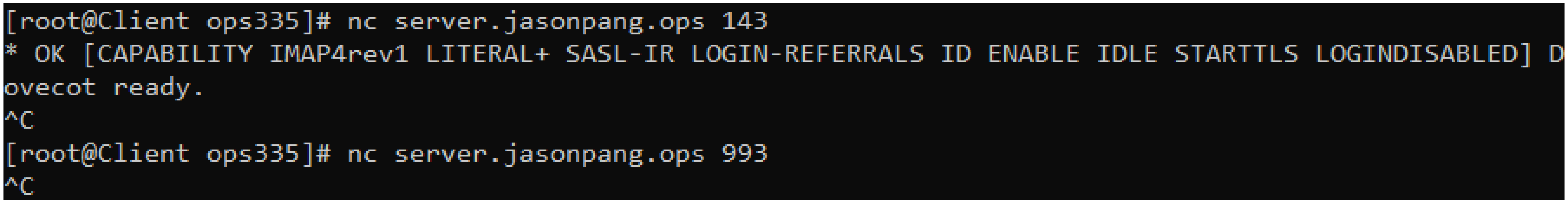
Accessing Received Mail Messages on SERVER VM via IMAP

First, we will set up the IMAP server so we can read email. The current way we have configured our mail server on our SERVER VM machine should allow all the email for anyaccount@yoursenecaid.ops be delivered to our Server VM machine. We will set up Dovecot with IMAP to get easy access to that email.

Perform the following steps:

1. On server vm, the configuration file for the Dovecot service (which is not the same thing as dovecot-lda) is: **/etc/dovecot/dovecot.conf**. Modify the **protocols** option so that Dovecot will work with IMAP connections, no POP3 or LMTP.
2. Start the dovecot service, and ensure it will always start automatically when the machine boots.
3. Use the ss command to confirm the service is listening, and use nc on the host to confirm you can connect to it. Note: port 993 is secured, we didn't configure the secure connection, thus, 993 won't respond.

   ```
   ss -antp | grep dovecot
   ```

   ```
   [root@Client ops335]# nc server.jasonpang.ops 143
   * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS LOGINDISABLED] D
   ovecot ready.
   ^C
   [root@Client ops335]# nc server.jasonpang.ops 993
   ^C
   ```

4. You'll probably fail, so using the information gathered from ss, modify the firewall on Server VM to allow IMAP connections from your local network and try nc again. Once it works, do not forget to save this change so it will still be there the next time you reboot.

   ```
   iptables -I INPUT -p tcp --dport 143 -j ACCEPT
   ```

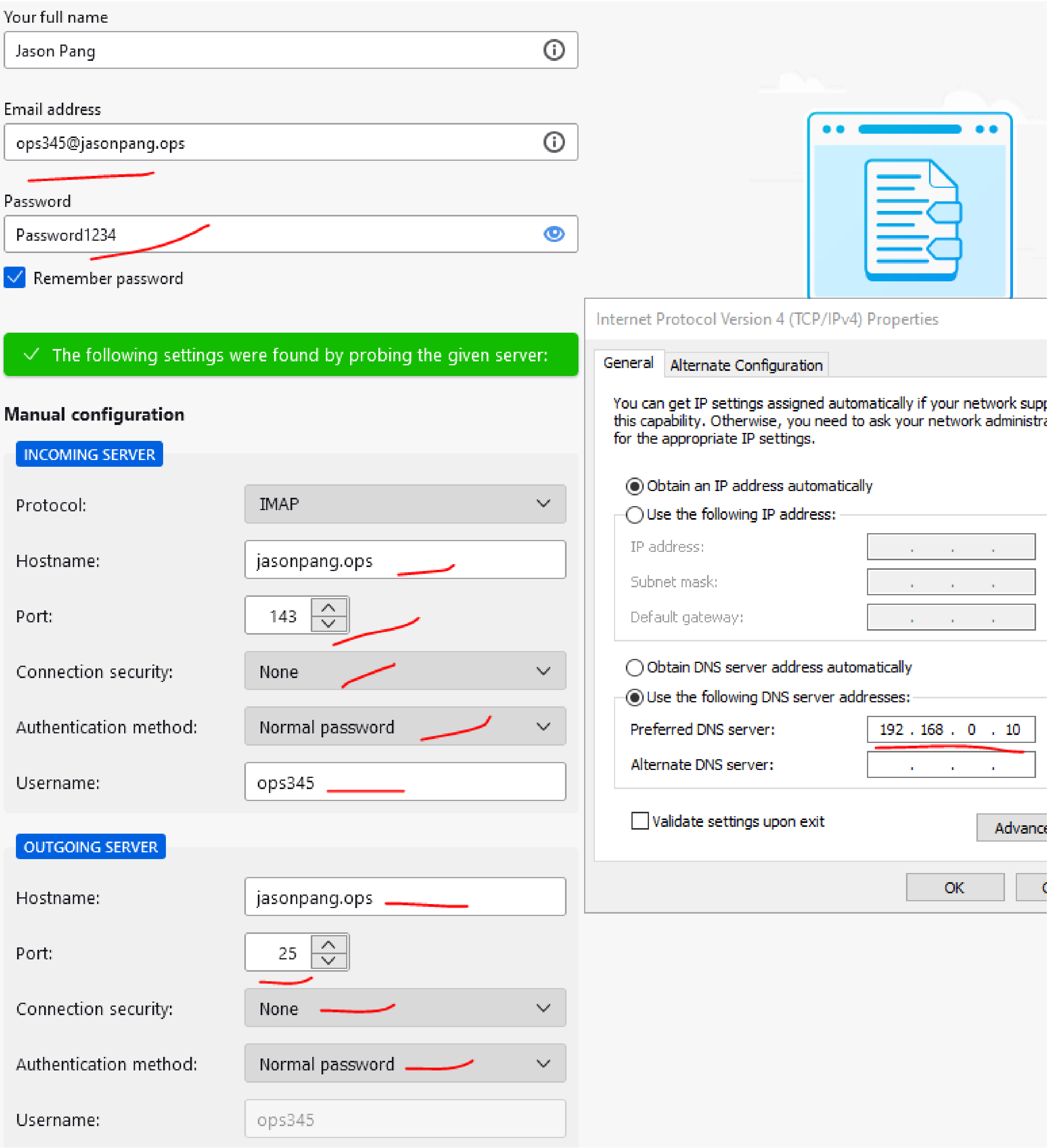
   ```
   iptables -I INPUT -p tcp --dport 993 -j ACCEPT
   ```
   # 993 is the secure port, it won't work here.

5. If you can connect - it's now time to do something “**wrong**”, that is allow connections to our IMAP server over an unencrypted connection.
6. Edit the **/etc/dovecot/conf.d/10-auth.conf** file and set **disable_plaintext_auth** to **no**.
   Then edit the **/etc/dovecot/conf.d/10-ssl.conf** file and set **ssl** to **yes**.
   Note: This combination of parameters will allow your username and password to be sent over the internet in plain text, for anyone interested to look at. In a later lab we'll set up secure SMTP and IMAP connections, for now this is all we have time for.
7. Restart dovecot so the changes take effect.

Connecting to IMAP Servers Using Thunderbird

Perform the following steps:

1. On your Azure Windows VM and install latest Thunderbird. (Create a new Windows VM, if not yet already, choose 2 vCore and 4GB memory or higher for performance. This VM will only stay for this lab for few hours, to be removed at the end.), return to the Mail Account Setup dialog box of Thunderbird.
2. Set up a new email account. You will be using account settings to connect to your Client VM for SMTP and Server VM for IMAP. Use no encryption, and use normal password authentication for IMAP. Refer to the diagram below for reference:
3. Check mark the “I understand the risks” when prompted.



Your full name: Jason Pang

Email address: ops345@jasonpang.ops

Password: Password1234

☑ Remember password

✓ The following settings were found by probing the given server:

Manual configuration

INCOMING SERVER

Protocol:	IMAP
Hostname:	jasonpang.ops
Port:	143
Connection security:	None
Authentication method:	Normal password
Username:	ops345

OUTGOING SERVER

Hostname:	jasonpang.ops
Port:	25
Connection security:	None
Authentication method:	Normal password
Username:	ops345

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supp
this capability. Otherwise, you need to ask your network administra
for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

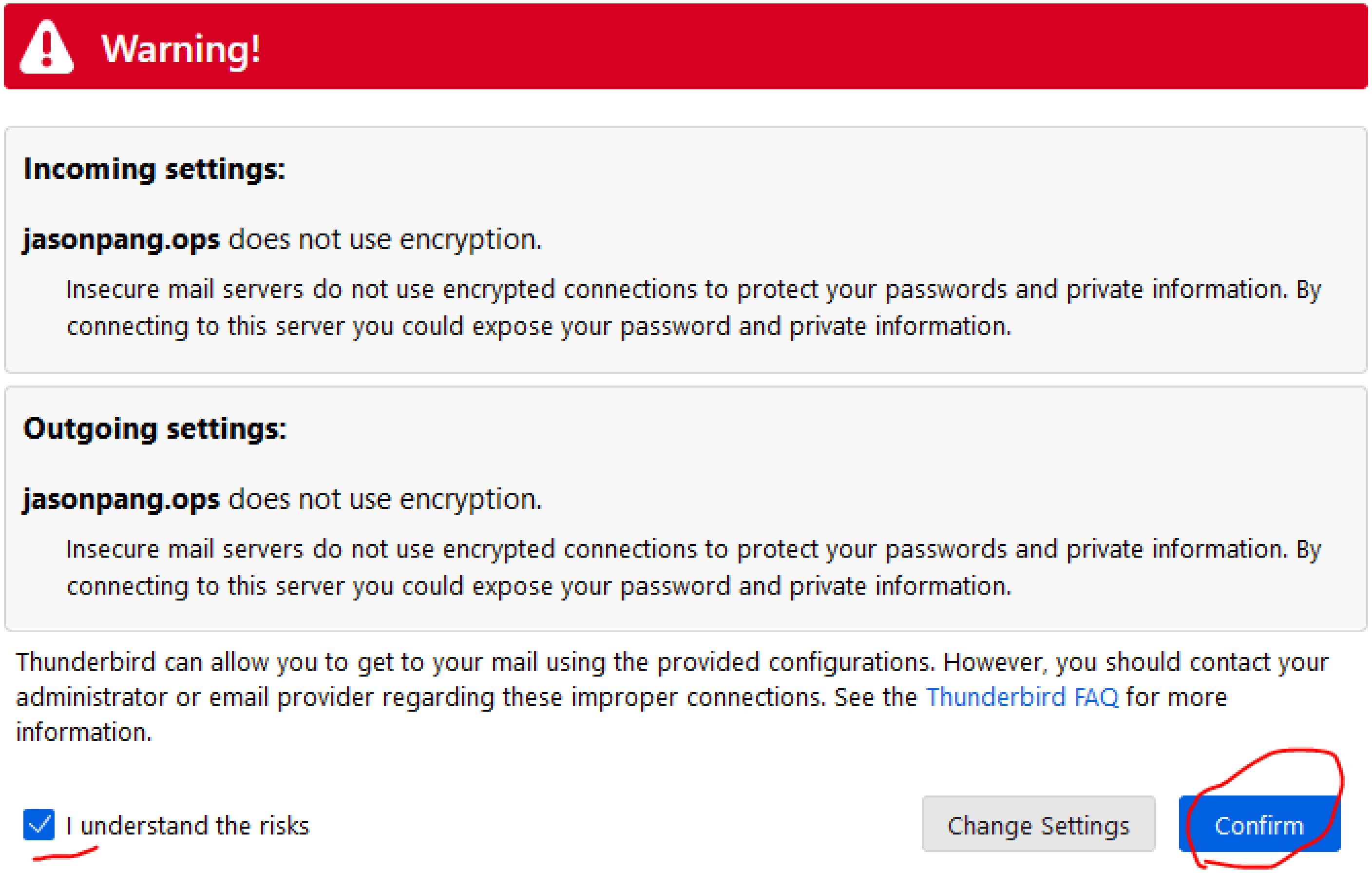
IP address:	. . .
Subnet mask:	. . .
Default gateway:	. . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	192 . 168 . 0 . 10
Alternate DNS server:	. . .

□ Validate settings upon exit



Warning!

Incoming settings:

jasonpang.ops does not use encryption.

Insecure mail servers do not use encrypted connections to protect your passwords and private information. By connecting to this server you could expose your password and private information.

Outgoing settings:

jasonpang.ops does not use encryption.

Insecure mail servers do not use encrypted connections to protect your passwords and private information. By connecting to this server you could expose your password and private information.

Thunderbird can allow you to get to your mail using the provided configurations. However, you should contact your administrator or email provider regarding these improper connections. See the Thunderbird FAQ for more information.

☑ I understand the risks

4. Try to connect to your IMAP server with Thunderbird by clicking on your **Inbox**.
5. If nothing happens, then check the Thunderbird Activity Manager for any errors. If the connection is successful, you should see the Trash box appear below Inbox.
6. Use the Thunderbird application to send an email to your own email address. If you've done everything right, it will send the message successfully
7. Verify that your message has been sent. Check your own email and look at **/var/log/maillog** on server VM (your email server).

8. Due to the firewall and spam filtering in the commercial email providers / vendors, you email may not be able to send out. As long as you can see the sending log from your mail server, that deems enough for the purpose of the lab. (Never try to send an email to Seneca email system. You may get penalized.)

Sending a Mail Message from the temporary Windows VM (Using Thunderbird)

Perform the following steps:

1. Use the **telnet** commands to confirm your service is listening on the correct ports/interfaces. You will probably have to open the appropriate firewall port on **Server VM** to allow incoming **SMTP** connections.

   ```
   telnet jasonpang.ops 143
   telnet jasonpang.ops 25
   telnet jasonpang.ops 53
   ```

   Note: You should be able to send email to any regular user on **Server VM** using the email address **ops345@yoursenecaid.ops** using the Thunderbird application on your Windows VM.
2. Create a new account on your **Server VM** using only your first name.

   ```
   adduser jason
   passwd jason
   ```
3. We will use this account as a one-time "test" if the mail message has been received on your SERVER VM machine (from your CLIENT VM machine).

   Note: It is **important** that you **don't** create this same account name on your Client VM machine, since you want to easily identify the difference between the sending and receiving SMTP servers.

4. Use the new account in Thunderbird to send an email to **firstname@yoursenecaid.ops** and then check the contents of **/home/firstname/Maildir/new/** on your **Server VM**. There should be a file there with the contents of your email.
5. If there is no file, then check the log file **/var/log/maillog** to see what went wrong.
6. If you can see a file in the **/home/firstname/Maildir/new/** directory, then review the procedures on how you got the email server working (since you have performed many steps and set up many services).
7. Refer to the diagram at the top of this lab. Which services have you currently set up?

Encountering error messages when sending email?

If you cannot properly receive/sent e-mail messages, check the /var/log/syslog file for errors.

If you locate an error message in that file such as: Fatal: Error reading configuration: Invalid settings..., then add the following parameter in /etc/dovecot/dovecot.conf:

postmaster_address = DOMAIN (where DOMAIN is actually your domain).

After you have saved those changes, then restart your dovecot service. This problem can also be resolved by properly setting the hostname of your machine to include the domain.

Once everything tested working. Remove the newly created Windows VM.

Save the captured file(s) as OPS345_Lab06_yourusername and upload to Blackboard.

If it is video recordings, upload to OneDrive and share with jason.pang@senecacollege.ca

Troubleshooting items if not working.

Iptables:

```
iptables -I INPUT -p tcp --dport=53 -j ACCEPT
iptables -I INPUT -p udp --dport=53 -j ACCEPT
iptables -I INPUT -p tcp --dport=25 -j ACCEPT
```

Hostname of VM:

```
vi /etc/hostname
systemctl restart systemd-hostnamed
```

DNS server:

Are you able to do: `nslookup server.yoursenecaid.ops 192.168.0.10`

Is the first DNS as 192.168.0.10? `vi /etc/resolv.conf`

Are all the required elements installed?

```
yum install bind*
yum install nc
yum install mailx
```