System and Network Administration

Core Services:

email

Electronic Mail

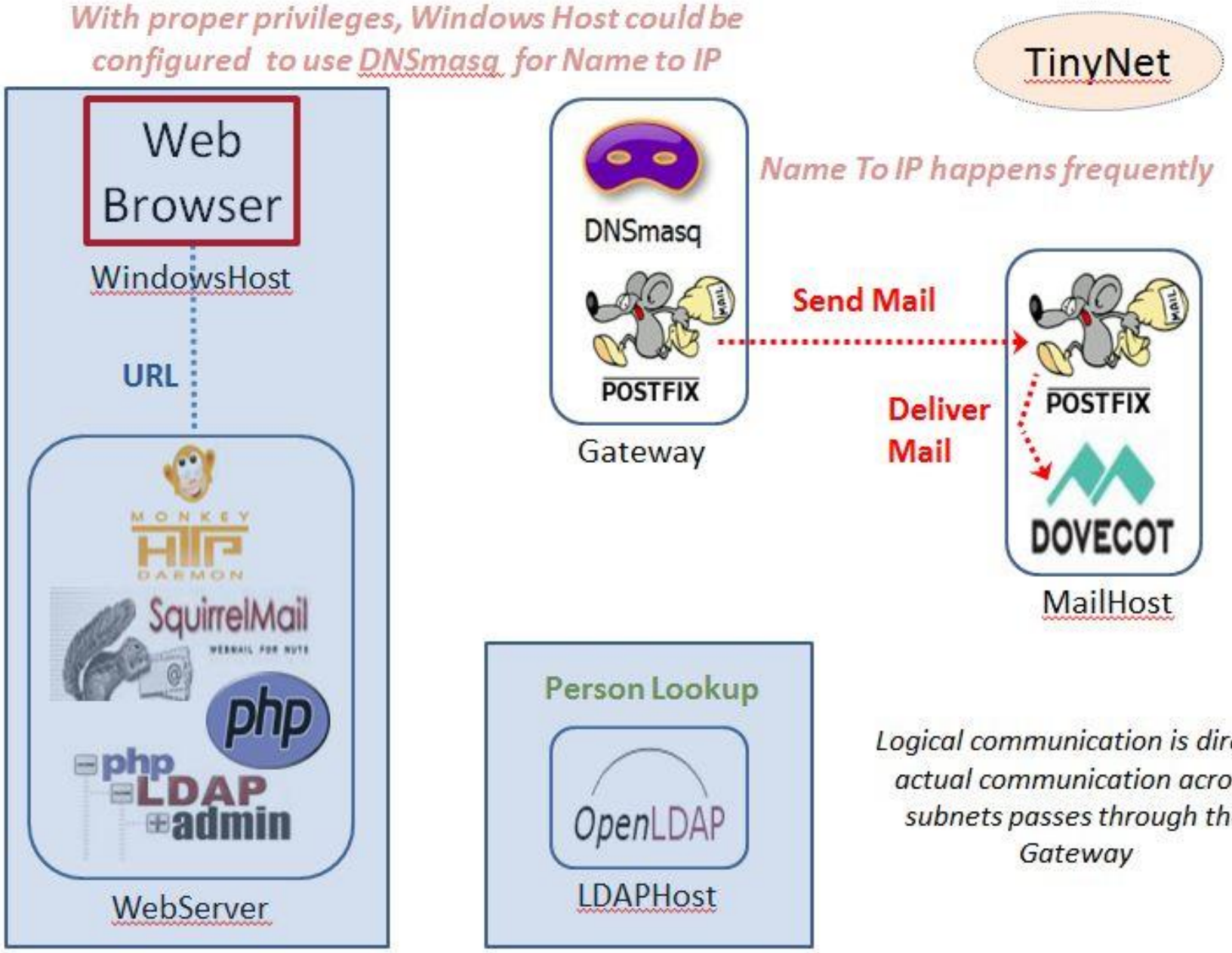
E-mail is the ***ONLY*** universal mission-critical application

- Each person/group will have various mission-critical applications
- But the only application that ***everyone*** depends on is e-mail

Keeping e-mail flowing is a required task for most system administrators.

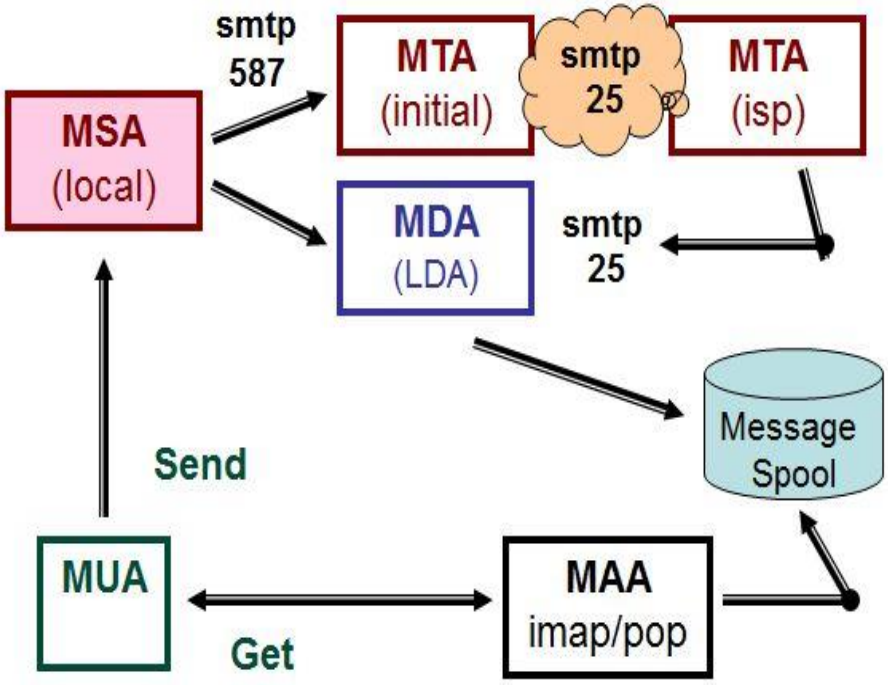
For the administrator this means:

- Choosing and configuring a mail transport agent
- Thinking through
  - the site's e-mail model,
  - user agents, and
  - hardware required to provide this critical service.

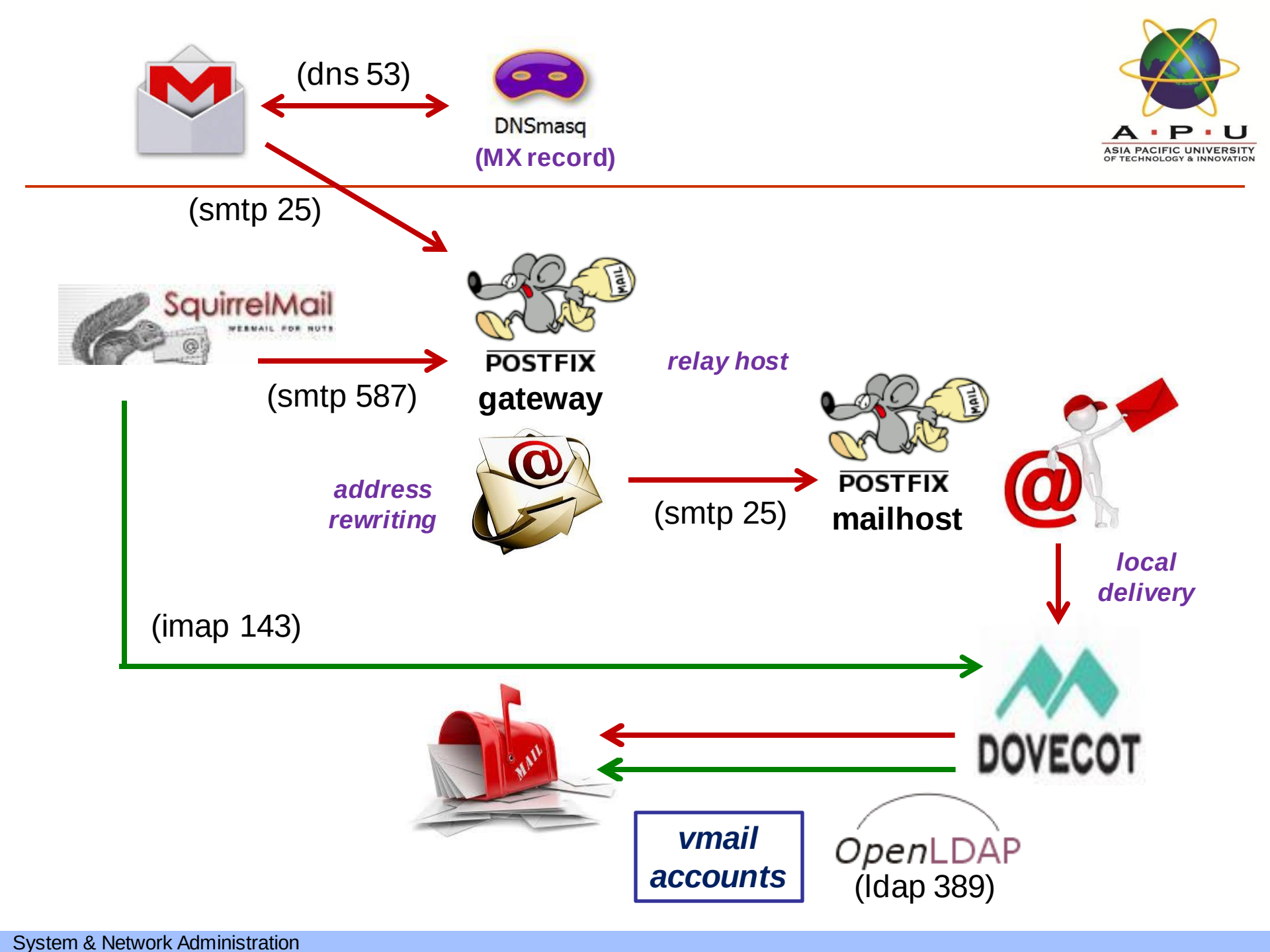

With proper privileges, Windows Host could be configured to use DNSmasq for Name to IP
TinyNet
Web Browser
WindowsHost
URL
DNSmasq
POSTFIX
Gateway
Name To IP happens frequently
Send Mail
Deliver Mail
POSTFIX
DOVECOT
MailHost
MONKEY HTTP DAEMON
SquirrelMail
php
php LDAP admin
WebServer
Person Lookup
OpenLDAP
LDAPHost
Logical communication is direct, actual communication across subnets passes through the Gateway

Mail - Abstract Architecture

In our setup, **SquirrelMail** is the **MUA**; **Postfix** on the Gateway is a **MTA**; **Postfix** on the Mailserver is the **MSA** when it receives mail from **SquirrelMail** and the **MDA** when it receives mail from **Postfix** on the Gateway; **Dovecot** on the MailServer is the **LDA** (called by **Postfix** for putting messages in mailboxes) and the **MAA** (imap server).



MUA – Mail User agent
MSA – Message Submission agent
MTA – Mail Transport agent
MDA – Mail Delivery agent
MAA – Mail Access agent


(dns 53)
DNSmasq
(MX record)
(smtp 25)
SquirrelMail
WEBMAIL FOR NUTS
(smtp 587)
POSTFIX
gateway
relay host
address
rewriting
(smtp 25)
POSTFIX
mailhost
local
delivery
(imap 143)
DOVECOT
vmail
accounts
OpenLDAP
(ldap 389)

Message, Envelope, Headers

The MSA places the message in an “envelope” for delivery.

- There is a header on the message and another header on the envelope.
  - These contain addresses and other information about the message.
    - Message headers can be (and are) easily forged by user.
- Users typically do not see the envelope.
  - Envelope headers are (normally) created, changed, and deleted by MTAs
- Every message is assigned a unique ID by each MTA that handles it.
  - This allows tracing the message from end to end (if log files are available).

EMail Overview – SMTP

1. sending end introduces itself
2. sending end tells who mail is from
3. sending end tells who mail is for
   If the destination user is valid / relaying is permitted, open a spool, and continue the process.
   More on this in a minute…
4. Sending end transfers data
5. Sending end closes connection

SMTP protocol

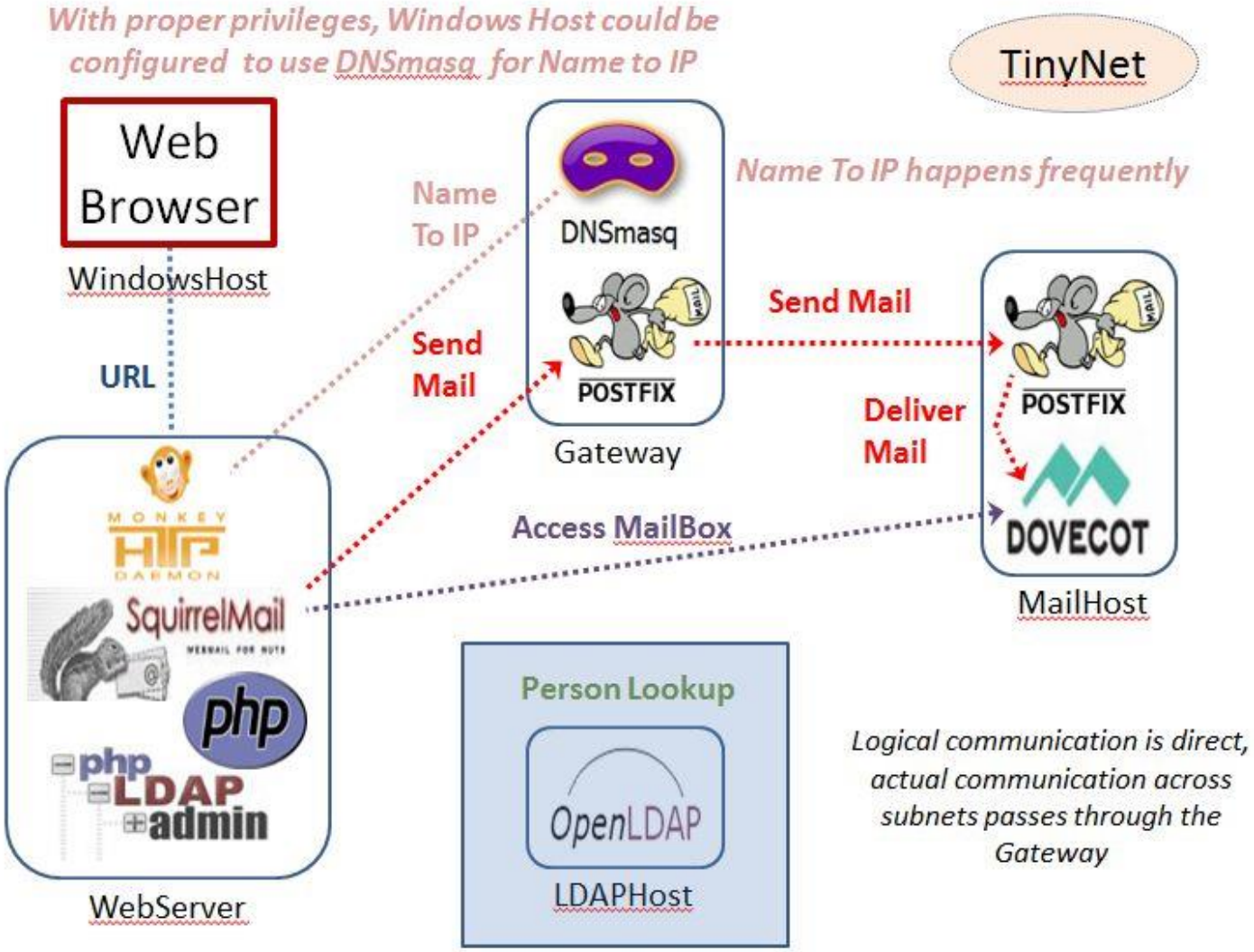
HELO – introduce yourself
  AUTH – authenticate this user
MAIL FROM – who
RCPT TO – (message to)
  VRFY – see if this user exists.
  EXPN – expand this address and tell me who it is
DATA – body of the message
  DSN – delivery status notice
  RSET – reset the connection
  NOOP – do nothing
VERB – verbose mode
QUIT – close the connection


Q
&
A

Web-based Mail

- A web-based mail client is a suite of CGI programs that act as a mail client using a web browser as the user interface.
- Requires obtaining and installing the needed CGI programs and supporting programs and adding them to the web server configuration
  - For example, SquirrelMail requires a webserver, PHP, and an IMAP server, as well as the SquirrelMail software.
- Web-based mail can be used from any client platform that has a web browser.

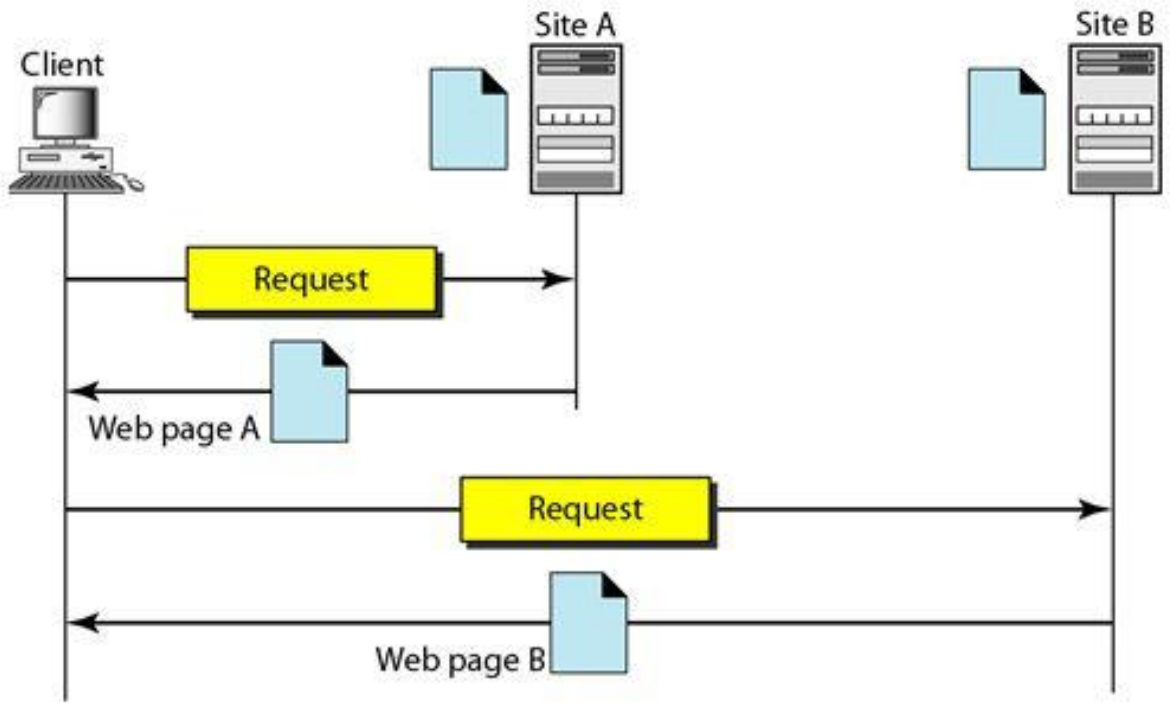
Configure Webmail



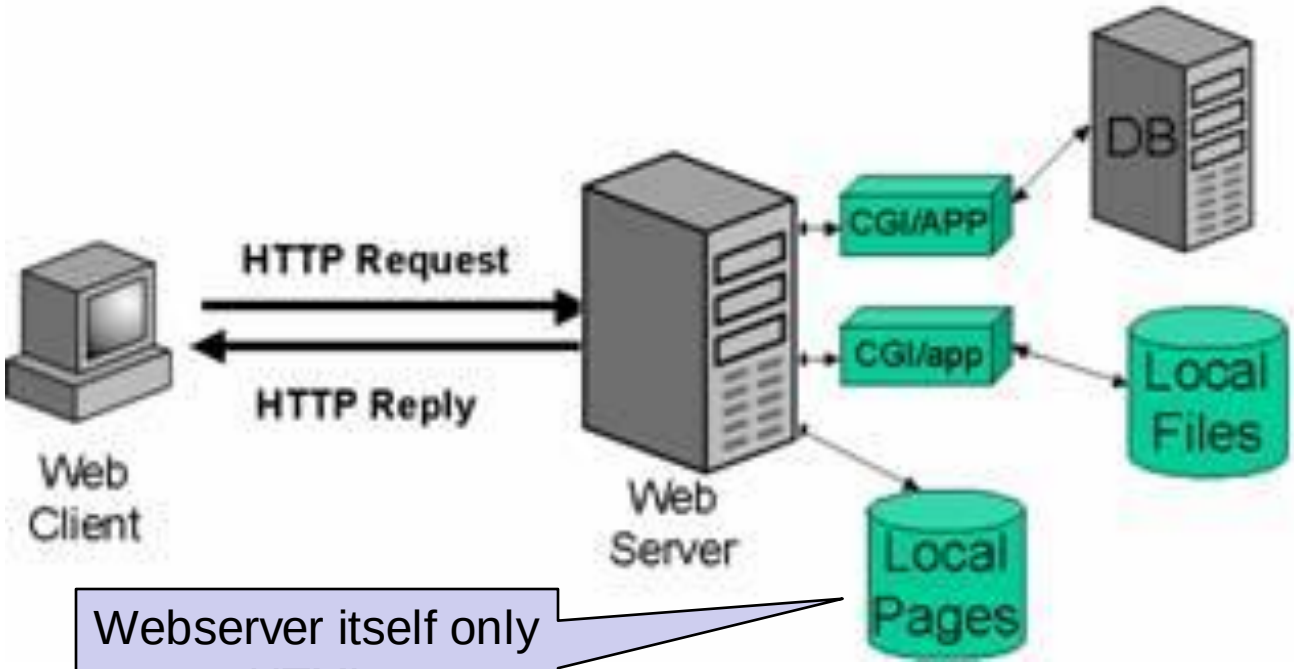
Web Services

- Uses HTML for message format and HTTP for message transport
- HTTP: TCP port 80
- HTTPS: TCP port 443 (SSL)

Each component of the page is retrieved separately and combined for display in the browser



Web server Architecture

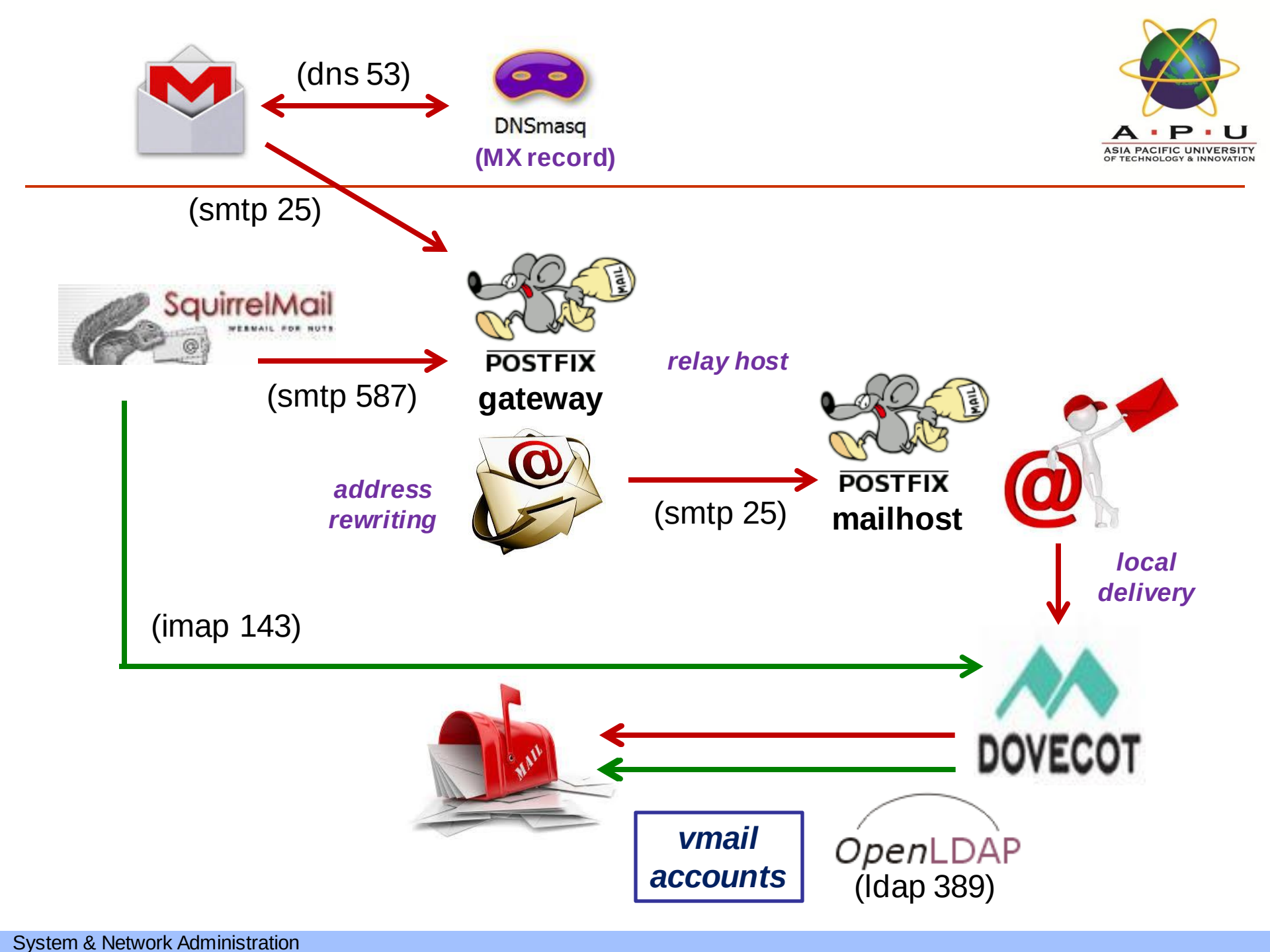


Webserver itself only serves HTML pages (DocumentRoot)

CGI/app
Can be written in any language, PHP, Python, C# (ASP.NET), and JavaScript are all popular

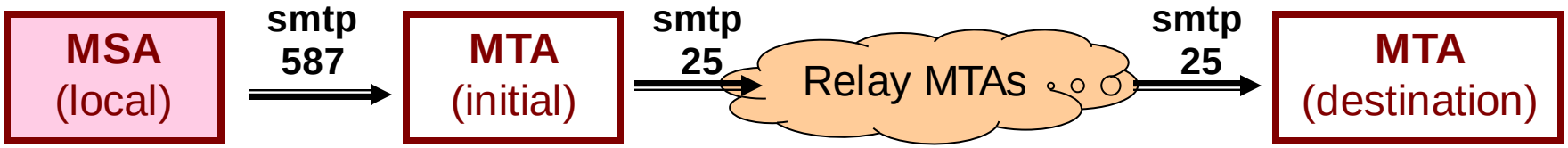
Virtual Hosts :
Multiple Web sites managed by a single server

- `monkey` is the TinyNet default server
- `apache` is the most popular
- `lighttpd` is preferred by many
- Internet Information Server (IIS) is Microsoft


(dns 53)
DNSmasq
(MX record)
(smtp 25)
SquirrelMail
WEBMAIL FOR NUTS
(smtp 587)
POSTFIX
gateway
relay host
address
rewriting
(smtp 25)
POSTFIX
mailhost
local
delivery
(imap 143)
DOVECOT
vmail
accounts
OpenLDAP
(ldap 389)


Q
&
A

RFC 2476 + RFC 4409: Message Submission



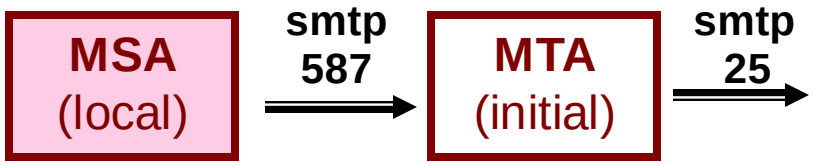
Defines the difference between **mail transfer** and **message submission**:

- Submission is intended to be from client to initial server.
  - SMTP protocol, port 587
- Transfer is intended to be server to server (relay)
  - SMTP protocol, port 25

Allows administrators to run two distinct services configured optimally for each purpose rather than a single MTA service that has to make allowances for different types of use

Email – Submission

MSA port 587 should be limited to internal hosts



- MSA converts mail to “canonical form”, for example by adding @domain to mail submitted with a simple user name
- MSA does other address rewriting, for example changing user@host.domain to Given.Family@domain (masquerading)
- MSA authenticates clients: able to require encryption and SMTP authentication for port 587 sessions

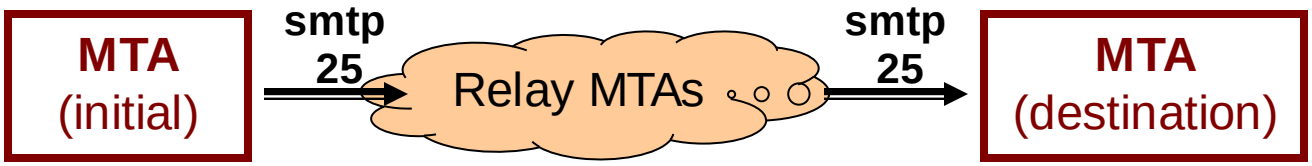
DNS Necessities

- **Canonical name for hosts**
  - lookup record - Name to IP
- **MX records**
  - so MTAs can find the address to connect to

```
example.com  IN  MX  10  mailhost.example.com.
```

  - MSAs don't really need MX, initial MTA can be hard coded
- **Mailserver reverse lookup record** - IP to Name
  - for validation purposes

Relaying



- MX (Mail eXchanger) record
  - priority allows multiple possibilities for getting mail delivered
- MTA configuration
  - Accept mail for certain destinations, then pass it along
- open relay = bad netizen
  - likely to be used for spam

Many different configurations are possible

- Local delivery for users with an account on the system
- Local delivery for virtual users (no account on the system)
- Virtual hosting for domains, mail delivered to local user (virtual or actual)
- Mail sent to a gateway then forwarded on to individual mailservers – MUA talks to configured gateway MSA
- Local mail sent to local mailserver, external mail sent to gateway – MUA talks to `localhost`

Weird and wonderful combinations will work!

Lots of decisions to make, Lots of documentation to read

How complicated is it?

- **postfix**
  - sets 530+ defaults
- **sendmail**:
  - 55+ features
  - 180+ defines, many with several distinct options

  these are used to configure
    - 18 classes
    - 16 rulesets
    - 15 macros
    - 9 m4 diversions (subroutines)
- **dovecot**:
  - About 150 defaults plus (2*7) database options


Q
&
A

Troubleshooting

- Stop! Don't Rush
- Make one change at a time – test
- Start at one end, move up or down the network layers
- Communicate regularly
- Work as a team
- Document before and changes

Requires skills of

–Mechanic

–Sociologist

–Researcher

Problems?? Check the “4 peas”

- Paths
- Permissions
- Ports
- Parsing (typos)

Correcting Faults

1. **Gather evidence**
2. **Make an informed guess**

   (just fix it, see if it works --

   BUT be able to go back to the previous and original !!)
3. **Try to reproduce the error**

Troubleshooting

It is best to test a network service locally first.

- Use `netstat -an` to check that the port number associated with the service is active and in the LISTENING state.
- Check which IP address the port is bound to -- some services may only be bound to use one or another interface .
- Check is if the service responds at all by trying the service using a local client, which does not involve host-to-host connectivity.
  - The local service is naturally found at the localhost address (127.0.0.1, or just identify localhost as the hostname).
- Examine the log using `tail -f`
  - shows all messages received and sent by the server

Troubleshooting Scenario: Webserver

If the web server will not start for no apparent reason:

1. make sure that the pid file doesn't already exist

```
ls -l /var/run/httpd.pid
-rw-------  1 root sys Feb 14 19:23 /var/run/httpd.pid
```

2. If the file exists while the server is stopped then delete it

```
rm /var/run/httpd.pid
```

3. restart the service ... for example

```
/etc/rc.d/apache restart
```

4. Use `netstat -an` to check that port 80 is active and in the LISTENING state.

Troubleshooting Scenario (cont.)

5. try the local service – you don't even need a browser

```
telnet localhost 80
GET /
```

6. Examine the log using `tail -f`

shows all messages received and sent by the server

Still having problems?

(a) Increase the Loglevel verbosity, for example from...

LogLevel warn to **LogLevel debug**

(b) restart the service - examine the log using `tail -f`

Still having problems?

(c) Start the process from the shell to capture console logging

- Look at the rc.d startup script to find the actual command that is being executed, and run it yourself from the command line

```
/usr/sbin/apachectl start

dynamic linker : /usr/sbin/httpd : could not open libmhash.so.2
/usr/sbin/apachectl: 29125 Killed
/usr/sbin/apachectl start: httpd could not be started
```

- we find that the apache server couldn't start because it couldn't locate a linked library

Missing Libraries

- If you are missing a library, use the command

  `find / -name "libname*"`

  using the library name from the error message.
- If it exists, fix it with a symlink to the path specified in the error message, or put the symlink in /usr/lib or /usr/local/lib if it is not already there.
- Lots of times the library is called libxyz.so.2.0.0 when the program wants libxyz.so so this is pretty easy

Troubleshooting Scenario (cont.)

(d) Doublecheck this using ldd like so...

```
cd /usr/sbin

ldd ./httpd

./httpd needs:
    libldap.so.2 => /var/opt/lib/libldap.so.2
    /usr/lib/libcurl.so.2
    /usr/lib/libgnuintl.so.4
dynamic linker : ./httpd : could not open libmhash.so.2
```

in this scenario we know that libmhash.so.2 resides in /var/opt//lib/ so we found a missing symbolic link

Troubleshooting Scenario (cont.)

(e) Fix by creating a symlink to the library

```
ln -s /usr/lib/libmhash.so.2 /var/opt/lib/libmhash.so.2
```

(f) and try it again

```
ldd ./httpd

./httpd needs:
    libldap.so.2 => /var/opt/lib/libldap.so.2
    libmhash.so.2 => /var/opt/lib/libmhash.so.2
    /usr/lib/libcurl.so.2
    /usr/lib/libgnuintl.so.4
```

Diagnosis

Be systematic:

- **start with simple things, progressing to more complicated causes or factors**
- **always eliminate the obvious first**

- **use a log, conceptual map, etc.**
- **gather information that can be subject to *association and deduction***
- **establish (recall) cause and effect**
- **be able to go back to the previous and original**

Diagnosis (cont'd)

Requires skills of

–Mechanic

–Sociologist

–Researcher

Play detective:

- pay attention to facts
- read documentation
- talk to others
- old bug and problem reports – local and googled
- system logs
- simple tests and experiments
  - **know your tools, e.g., ping, netstat, ifconfig, ethtool, lsof, locate, tcpdump, wireshark**

Correcting Faults (cont'd)

Then change management

- **decide**
- **map out repercussions**
- **revise policy if necessary, incorporating user comments**
- **inform users of impending change**
- **lock the system to avoid incomplete reconfiguration**
- **make the changes**
- **unlock the system**
- **inform users that all is done**

Then revision control for configurations

everything should be documented


Q
&
A