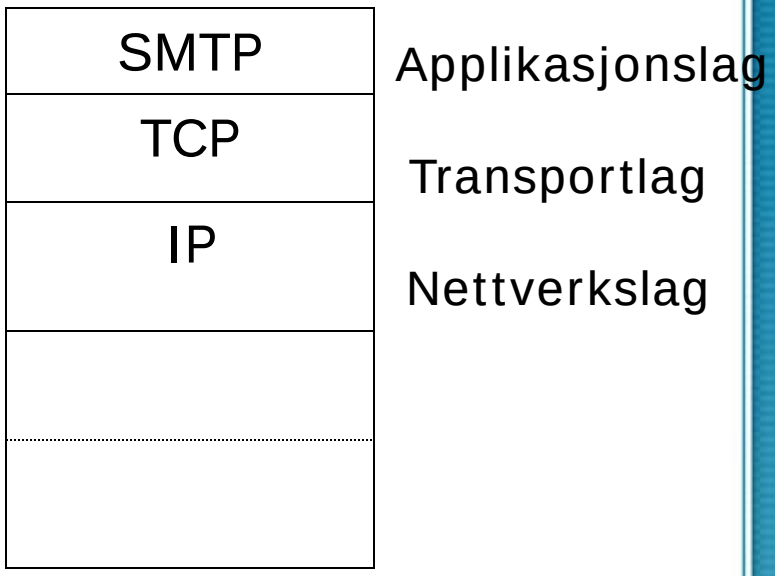
E-post

- Vanlig med todeling:
  - User Agent (UA):
    - E-post klient
  - Message Transfer Agent (MTA):
    - E-post tjener
    - Mottar meldinger fra UA´ s for videresending i nettverket.
    - Melding leveres til mottakers MTA
    - Store/forward funksjonalitet

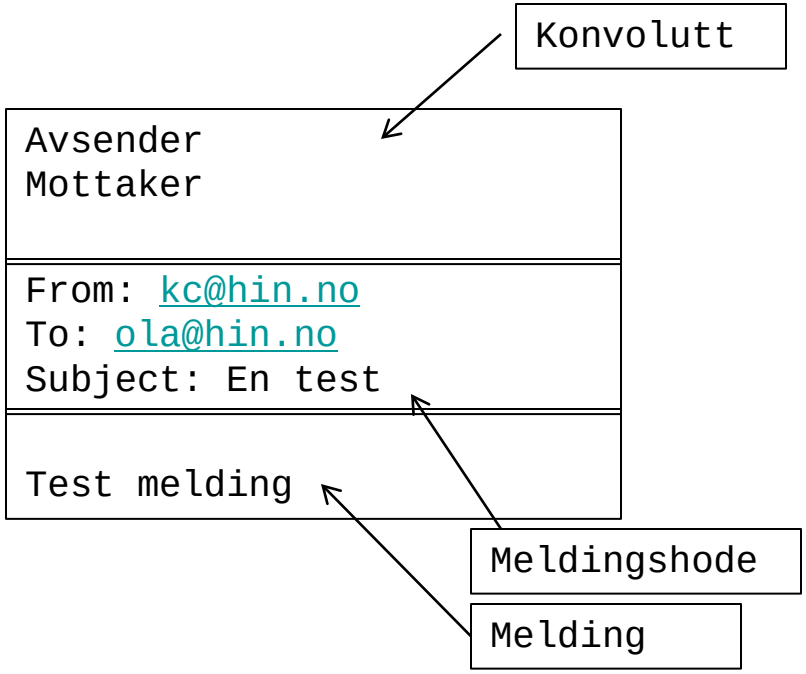
SMTP

- Simple Mail Transfer Protocol (SMTP) er en del av TCP/IP protokollpakke
  - En applikasjonsprotokoll.
  - SMTP benyttes for sending av post på Internet
  - SMTP benytter TCP som transportprotokoll.



SMTP

- RFC 821 og 822 omhandler SMTP
  - RFC 822 beskriver format på meldingshode
    - Beskriver alle felt i meldingshodet
  - SMTP tilføyer rutinginformasjon til en melding
    - Kan se veien en melding har gått på nettet fra sender til mottaker



SMTP

- Sending av post
  - E-post klient kontakter SMTP tjener (MTA)
  - SMTP tjener lytter på port 25
    - Tar i mot melding og plasserer melding i utkøen
    - Ved sending kontakter SMTP tjener på mottakersystemet og sender meldingen
    - Ved flere mottakere på samme system, send selve meldingen kun en gang

Sending av epost

```
root@ubuntu:~# telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 ubuntu ESMTP Postfix (Ubuntu)
helo kc.hin.no
250 ubuntu
mail from:kc@hin.no
250 2.1.0 Ok
rcpt to:vadmin
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
From: kc@hin.no
To: vadmin
Subject: Bare en test !

Test i dag !

.
250 2.0.0 Ok: queued as 640D5C1C2
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Epost meldingsformat

```
From kc@hin.no  Fri Mar  5 03:50:56 2010
Return-Path: <kc@hin.no>
X-Original-To: user
Delivered-To: user@dt.hin.no
Received: from dt.hin.no (localhost [127.0.0.1])
        by ubuntu8041.localdomain (Postfix) with SMTP id E52456D1D;
        Fri,  5 Mar 2010 03:48:38 -0500 (EST)
From:kc@hin.no
To:user@dt.hin.no
Subject: En testmelding
Message-Id: <20100305084902.E52456D1D@ubuntu8041.localdomain>
Date: Fri,  5 Mar 2010 03:48:38 -0500 (EST)

dettte er en test
```

Meldings format

```
Microsoft Mail Internet Headers Version 2.0
Received: from platon ([158.39.21.3]) by fjellheim.hin.no with Microsoft
    SMTPSVC(6.0.3790.3959);
     Fri, 5 Mar 2010 09:44:07 +0100
Received:
    from 158.39.21.7 by platon (InterScan VirusWall 6); 05. mars 2010 09:49:37
Received: from localhost (localhost.localdomain [127.0.0.1])by
    samson3.hin.no (Postfix) with ESMTP id 83E761E820for <kc@hin.no>; Fri,  5
    Mar 2010 09:44:06 +0100 (CET)
Received: from samson3.hin.no ([127.0.0.1])by localhost (samson3.hin.no
    [127.0.0.1]) (amavisd-new, port 10024)with LMTP id meET+bk1nt1W for
    <kc@hin.no>;Fri,  5 Mar 2010 09:44:06 +0100 (CET)
Received: from sokrates.hin.no (Sokrates.hin.no [158.39.21.2])by
    samson3.hin.no (Postfix) with ESMTP id 733581E815for <kc@hin.no>; Fri,  5
    Mar 2010 09:44:06 +0100 (CET)
Received: from ubuntu8041.localdomain ([158.39.26.37]) by sokrates.hin.no
    with Microsoft SMTPSVC(6.0.3790.3959); Fri, 5 Mar 2010 09:44:05 +0100
Received: from dt.hin.no (localhost [127.0.0.1])by ubuntu8041.localdomain
    (Postfix) with SMTP id E52456D1D;Fri,  5 Mar 2010 03:48:38 -0500 (EST)
From: "kc@hin.no" <kc@hin.no>
To: "user@dt.hin.no" <user@dt.hin.no>
Subject: En testmelding
Message-Id: <20100305084902.E52456D1D@ubuntu8041.localdomain>
Date: Fri,  5 Mar 2010 03:48:38 -0500 (EST)
X-OriginalArrivalTime:
    05 Mar 2010 08:44:05.0945  FILETIME=[03B2AA90:01CABC40]
X-TM-AS-Product-Ver: : ISVW-6.02.0.7165-6.0.0.1038-17230002
X-TM-AS-Result: : Yes-1,092000-0-31-1
X-TM-AS-Category-Info: : 31:0,000000
X-TM-AS-MatchedID: : 148033-148039-10002-10111
Return-Path: kc@hin.no
```

Vi ser hvilke tjenere som meldingen har passsert

SMTP

- Feilhåndtering ved sending av post
  - Ukjent mottaker
    - Send feilmelding til sender
  - Mottakersystem utilgjengelig
    - Legg melding i kø, prøv senere
    - Prøver en viss tid eller et antall feilforsøk.
- SMTP garanterer ikke mot tap av meldinger
  - Ingen ACK ved mottak av melding
  - SMTP betraktes likevel som leveransesikker

Adressering i SMTP

- SMTP benytter såkalt domene adressering: bruker@domene , eks.: kc@hin.no
  - MTA sender melding til et system som har forbindelse med *hin.no*.
  - Deretter sender MTA på *hin.no* meldingen til postkassen til bruker *kc*.
- Alias - flere navn tilknyttet samme postkasse.
  - Kan benyttes for å implementere adresselister, slik at man ved å sende post til et alias kan nå mange brukere (postkasser).

Ruting av post med SMTP

- Rutingen utføres av MTA.
  - På Internet vil DNS hjelpe til med å finne riktig tjener med forbindelse til det domenet som meldingen skal leveres til.
  - Når man sender post til en bruker ved hjelp av SMTP, gjøres det automatisk oppslag i en DNS tjener som returnerer et IP nummer.
  - MX post i DNS forteller hvilket system som tar imot epost for et domene

DNS MX records

- Angir hvilken tjener som skal ta i mot post for et gitt domene.
  - MTA spør DNS om MX informasjon om det aktuelle domenet.
  - DNS returnerer så IP adressen til den tjeneren som skal ta i mot meldingen.
  - Flere ulike tjenere kan angis som MX records med ulik prioritet. Benytter alternativ tjener dersom hovedtjener ikke tilgjengelig.

Sonefil eksempel: dt.hin.no

```
$ORIGIN dt.hin.no.
$TTL 86400      ; 1 day
@ IN SOA        bri.dt.hin.no. postmaster.dt.hin.no. (
                               2003022406 ; serial
                               28800      ; refresh (8 hours)
                               3600       ; retry (1 hour)
                               604800     ; expire (1 week)
                               86400      ; minimum (1 day)
                               )
                        NS      kark.hin.no.
                        NS      bri
                        MX      10      kark.hin.no.
                        MX      20      bri

bri                     A       192.168.100.1
gandalf                 A       192.168.100.2
www                     CNAME   gandalf
```

MX poster, angir hvilke systemer som tar imot epost for domenet

SMTP svakheter

- SMTP støtter kun 7 bits ASCII tekst i meldinger.
- SMTP støtter ikke vedlegg.
- MIME (Multipurpose Internet Mail Extension)
  - muliggjør sending post via SMTP med mer enn 7 biters ASCII.
  - MIME kan også angi at deler av en melding ikke er en melding (typisk for vedlegg).

MIME

- Beskrevet i RFC 1521 og 1522
  - Fem nye meldingsfelt i tillegg til RFC 822
    - MIME-Version:
    - Content-type: beskriver dataformatet som følger
    - Content-Transfer-Encoding:
    - Content-ID:
    - Content-Description:

E-post m/vedlegg

```
Return-Path: kc@hin.no
Received:    from hin.no (FagPC040.hin.no [158.39.25.40]) by
limbo.hin.no (8.9.3/8.9.3) with ESMTP id NAA27311 for
<kc@limbo.hin.no>; Tue, 28 Mar 2000 13:45:42 +0200
Message-ID: 38E09A65.6F343001@hin.no
Date: Tue, 28 Mar 2000 13:41:25 +0200
From: Knut Collin kc@hin.no
Organization: Narvik College of Engineering
X-Mailer: Mozilla 4.7 [en] (WinNT; I)
X-Accept-Language: en
MIME-Version:  1.0
To:  kc@limbo.hin.no
Subject: Test med vedlegg
Content-Type: multipart/mixed; boundary="------------
3F16C8D68C8060505522B761”
Content-Type:                  application/msword; name="framdrift.doc"
Content-Transfer-Encoding:    base64
Content-Disposition:    inline; filename="framdrift.doc"
```

MIME

- Base-64 koding
  - Kodingsmekanisme definert for sending av binærfiler, *Base64*
    - Base-64 koding benyttes for koding av bitsekvenser fra binærfiler til ″ lovlige″ ASCII tegn
    - 6 og 6 biter blir konvertert til ett av 64 tegn
      - {A-Z, a-z, 0 − 9, / og + }
    - Garanterer at post systemet ikke endrer dataene

POP

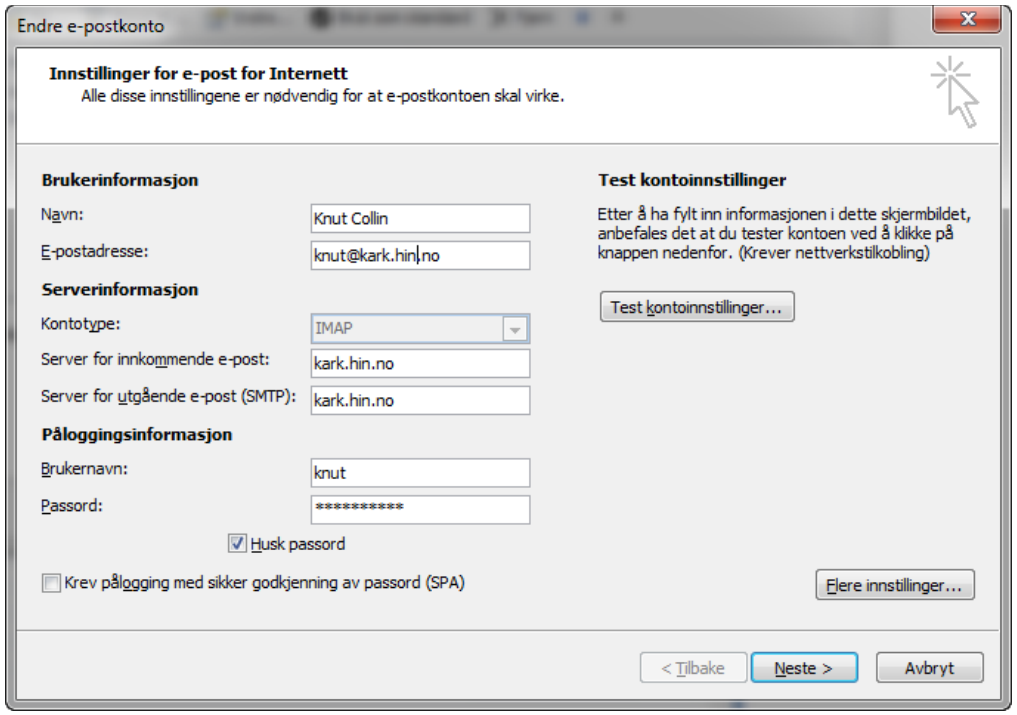
Post-Office Protocol (POP)

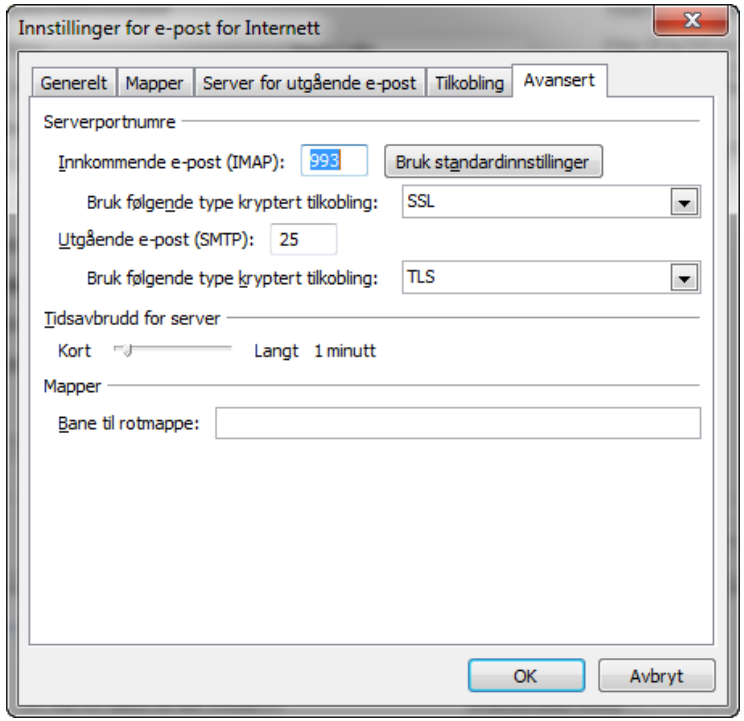
- Brukes for å lese og laste ned e-post fra en postkasse.
- POP2 (1985) og POP3 (1991).
- E-post klient kontakter POP tjener
- POP3 tjener lytter på port 110.
- Sikkerhet
  - POP3 sender all informasjon i klartekst inklusive passord
  - POP3S er SSL POP3, port 995

IMAP

- IMAP4 tillater e-post klienten å opprette
  - kataloger (mapper) på e-post tjeneren
  - E-post kan katalogiseres på e-posttjener
  - Enkelt med aksess fra forskjellige systemer
  - E-post lastes ikke ned til klienten
- Belaster e-post tjener mer enn POP
- IMAP tjener lytter på port 143
- IMAPS IMAP med SSL støtte port 993

Konfigurering Outlook

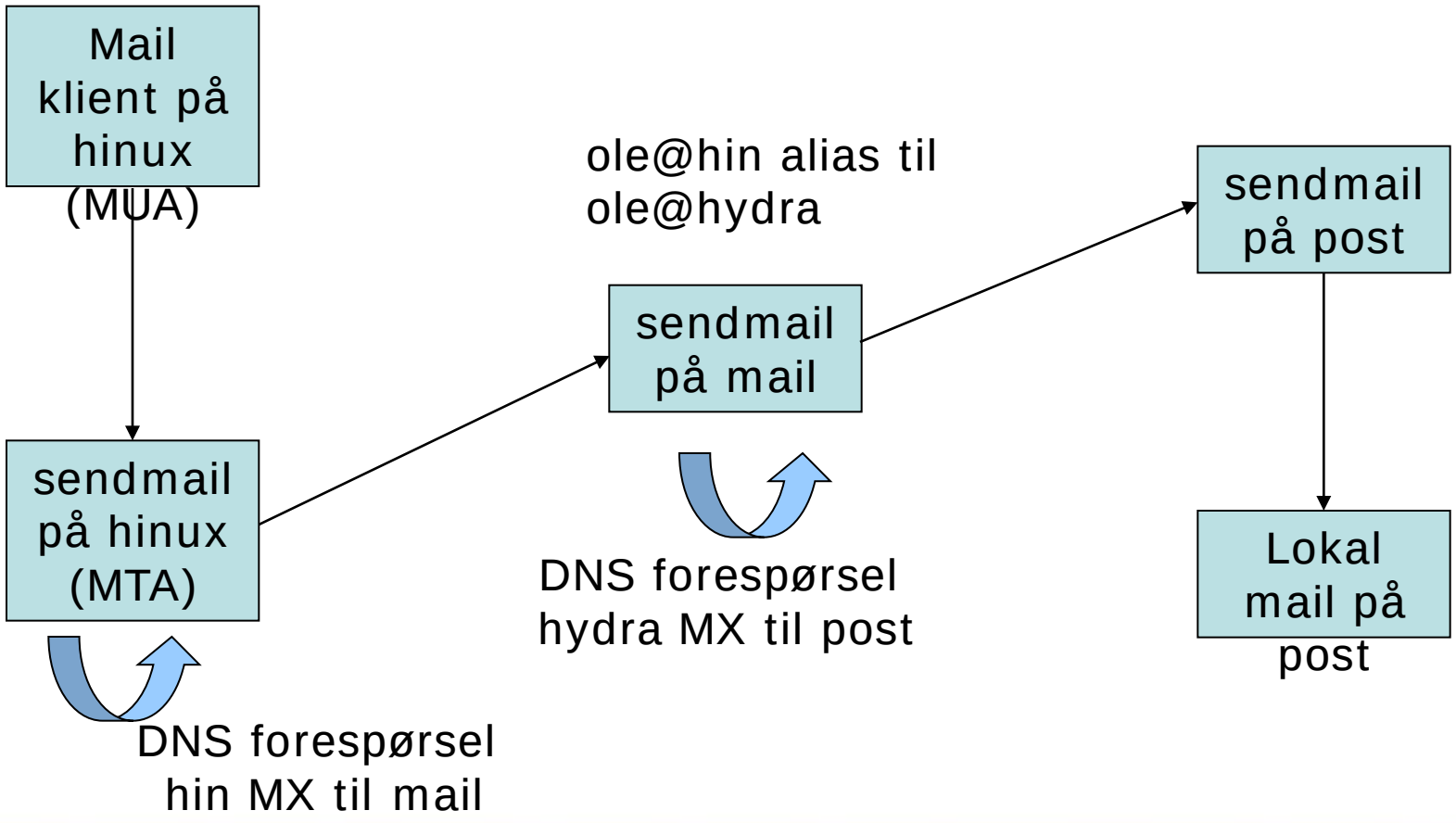




SMTP tjener

- Sendmail – mest kjente og benyttede SMTP tjener, www.sendmail.org
- Flere alternative SMTP tjenere på Linux
  - Qmail (læreboka) , Exim, Postfix
- Sendmail er standard installert på mange systemer for eksempel Fedora/RedHat
  - Tillater sending av post fra det lokale systemet og kun dette, aksepterer ikke post fra andre
- Sendmail er "arbeidshesten"
  - Programvaren som sørger for at en epost kommer fram til mottaker
- Postfix
  - Wietse Venema´s alternativ til sendmail, standard i Ubuntu

sendmail at work



alias

- /etc/aliases
  - Navn på mottaker av mail
  - Sendmail støtter lagring av alias navn ulike steder bl.a. i LDAP database
- Forteller hvem som skal motta post til et gitt brukernavn
  - Kan sette opp flere mottakere ala postlister
  - Oppretter assosiasjoner mellom et brukernavn og en epost konto
- For eksempel Ola.Nordmann@hin.no,
  - Ola.Normann kan i alias fillen peke til brukeren Ola

/etc/alias

```
# Basic system aliases -- these MUST be present.
MAILER-DAEMON:  postmaster
postmaster:     root
# General redirections for pseudo accounts.
bin:            root
daemon:         root
games:          root
# Well-known aliases.
manager:        root
operator:       root
# Person who should get root's mail
root:            kc
Knut.Collin :    kc
knut:            kc
```

newaliases

- Kommando som må kjøres hver gang endringer er gjort i alias filen

.forward filen

- .forward filen
  - Hver bruker kan videresende sin egen post ved hjelp av en .forward fil.
  - Filen skal inneholde en mottakeradresse evt. Flere
  - For eksempel

```
knutc@gmail.com
```

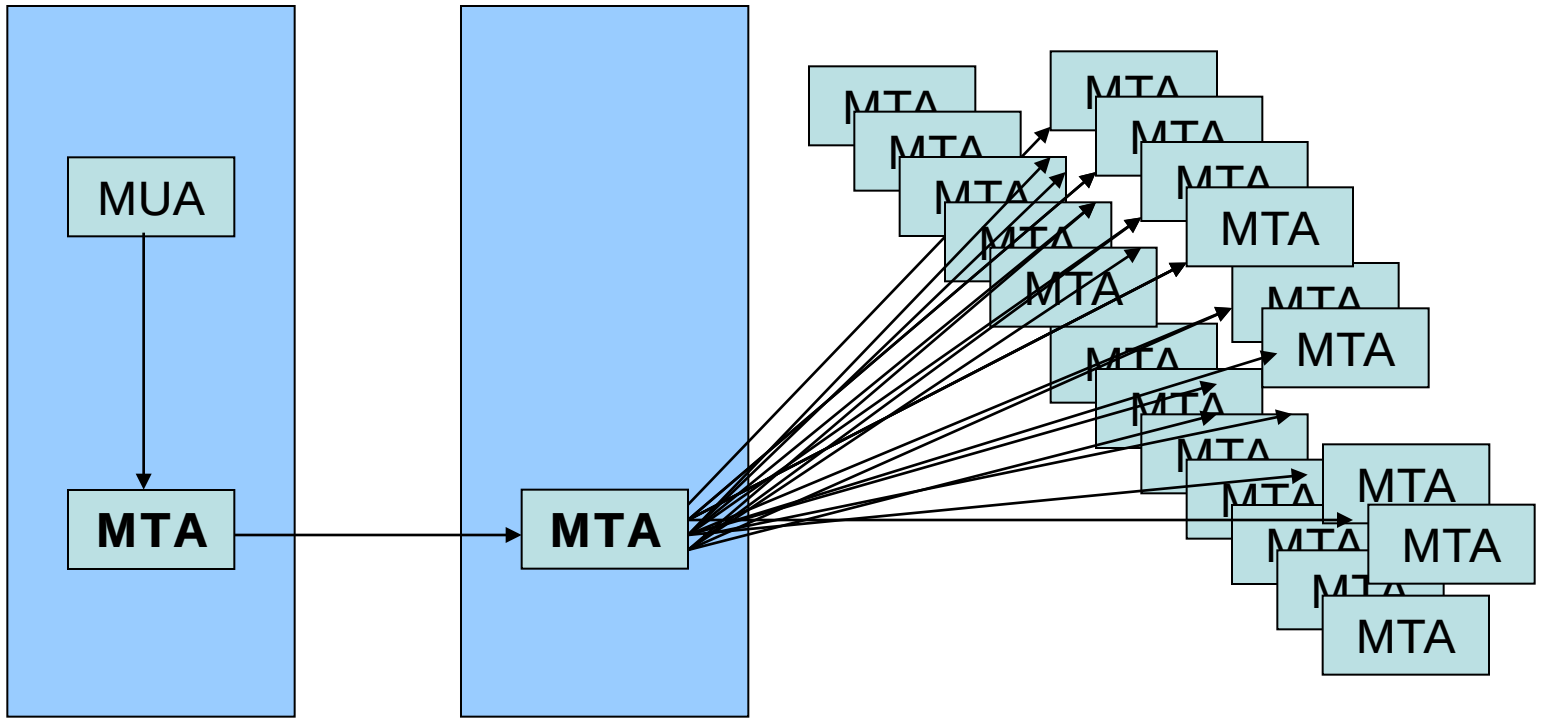
`postfix` konfigurering

- Viktige innstillinger i /etc/postfix/main.cf
- Domenenavn for utgående mail –
  - myorigin
- Domener som mail skal mottas for
  - mydestination
- Klienter som mail skal videresendes for
  - mynetworks

```
myorigin = $mydomain
mydestination = $myhostname localhost.$mydomain localhost $mydomain
mynetworks = 168.100.189.0/28, 127.0.0.0/8
```

Benytt **`postfix reload`** ved endring i noen av filene

SPAM – eksempel på åpent epost rele



SPAM kilde

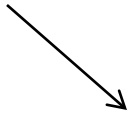
Et åpent mail rele, aksepterer post fra usikre kilder og videresender disse

Mottakere på Internett

postfix antispam

- HELO begrensninger
  - Spammere dropper ofte SMTP HELO kommandoen som initierer SMTP forbindelsen eller sender ugyldig informasjon
  - Postfix settes opp til å forkaste slike oppkoblinger

```
smtpd_delay_reject = yes
smtpd_helo_required = yes
smtpd_helo_restrictions =
   permit_mynetworks,
   check_helo_access
   hash:/usr/local/etc/postfix/helo_access,
   reject_non_fqdn_hostname,
   reject_invalid_hostname,
   permit
```



```
Whitelist/Blacklist

woozle.honeypot.net     OK
honeypot.net            REJECT
208.162.254.122         REJECT
```

postfix antispam

- Avsender begrensninger
  - Tillater autentiserte brukere og brukere på eget nettverk
  - Ikke tillat ugyldige epost adresser og ukjente domener

```
smtpd_sender_restrictions =
  permit_sasl_authenticated,
  permit_mynetworks,
  reject_non_fqdn_sender,
  reject_unknown_sender_domain,
  permit
```

postfix antispam

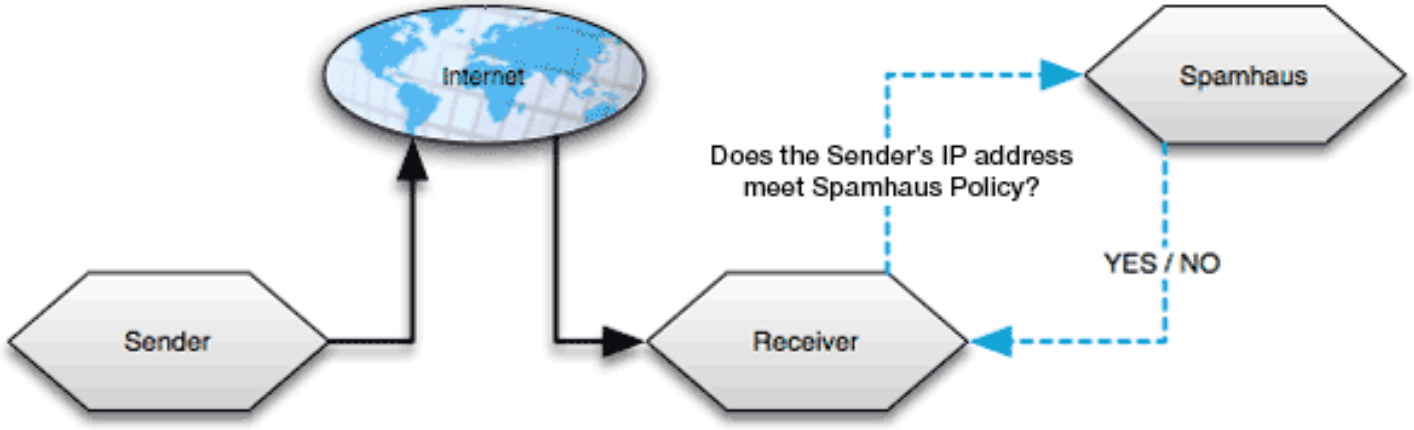
- Mottaker begrensninger
  - Verifiser at klienten har tillatelse til å sende til mottakeren

```
smtpd_recipient_restrictions =
   reject_unauth_pipelining,
   reject_non_fqdn_recipient,
   reject_unknown_recipient_domain,
   permit_mynetworks,
   permit_sasl_authenticated,
   reject_unauth_destination,
   check_sender_access   hash:/usr/local/etc/postfix/sender_access,
   check_recipient_access hash:/usr/local/etc/postfix/recipient_access,
permit
```

NB! Uten denne er postfix et åpent m

DNSBL Filtrering

- Svartelister benyttes for å avgjøre om avsender er kategorisert som utsender av spam
  - Aktuelle svartelister SORBS, dsbl, ordb, Spamhaus
  - Sammenligning på adressen
    - http://en.wikipedia.org/wiki/Comparison_of_DNS_blacklists



postfix antispam

- Mottaker begrensninger
  - Verifiser at klienten har tillatelse til å sende til mottakeren
  -

```
smtpd_recipient_restrictions =
   reject_rbl_client relays.ordb.org,
   reject_rbl_client list.dsbl.org,
   reject_rbl_client sbl-xbl.spamhaus.org,
   check_policy_service unix:private/spfpolicy
   check_policy_service inet:127.0.0.1:10023
   permit
```

Grålisting

- Grålisting
  - ved mottak av mail vil postfix se om mottaker og avsender er registrert tidigere
  - Hvis ikke sendes en SMTP feilmelding ″ Postboks utilgjengelig″ i en kort tidsperiode
    - Normale mailtjenere vil prøve på nytt og lykkes til slutt
      - Mottaker og avsender registreres slik at dette skjer kun første gang
    - Spammere har ikke tid til dette
  - Stopper effektivt store mengder spam !!

  - Grålisting benyttes på HiN, stopper effektivt ca 90-95% av all spam
    - Mest effektive teknikk pr i dag

postfix antispam

- SPF (Sender Policy Framework)
  - Et domene kan publisere i DNS hvilke systemer som tillates å sende ut mail fra domenet
    - SMTP tjenerne registreres i DNS ved hjelp av TXT poster
  - Postfix kan sjekke dette ved mottak av mail fra domenet
  - For eksempel for webtv.net er SPF posten
    - "v=spf1 ip4:209.240.192.0/19 -all"
    - Mail fra joe@webtv.net fra IP 64.4.32.7 er dermed forfalsket og kan avvises

postfix antispam / virusskanning

- Innholdsfiltrering
  - Analyse av innhold for å avgjøre om spam eller innholder virus
  - SpamAssasin
    - Open source verktøy for identifisering av spam
  - ClamAV for antivirus