

The logo for Nixu, consisting of the lowercase letters 'nixu' in a white, sans-serif font. The 'n' is lowercase, while 'i', 'x', and 'u' are uppercase. A thin white vertical line is positioned to the right of the text.

nixu

E-mail Protocols and Software

CONTENTS

- SMTP
- Interaction with DNS
- Sendmail
- IMAP and POP
- MIME
- Spam

History

- In the dawn of times (= before Internet) mail was transferred with UUCP-batch jobs from one machine to another
 - typical address...!mcvax!penet!clinet!riku
- With Internet TCP/IP - protocol became more common mean of delivery
 - typical address <Riku.Kalinen@nixu.fi>
- These two protocols were used simultaneously for a long time. With them existed (and still exists) other e-mail systems, like X.400, Memo, BITNET, ...
- Therefore most SMTP-programs are capable of routing messages between different protocols => complexity
- Current dominant MTA is Sendmail, because it comes with most standard UNIX-installations

SMTP-protocol

- “Push protocol”, i.e. sender initiates
- Server is at TCP-port 25
- Currently undeliverable messages can (and should) be queued
- Related Standards
 - RFC2821: Defines transfer-protocol
 - RFC2822: Defines message-form
 - These are updated by many other RFCs
 - RFC 1123: Internet Host Requirements
 - RFC 1870, 2821: SMTP Service Extensions
 - RFC 1891-1895: Even more extensions, now obsoleted by newer RFCs
 - RFCs 2045-2049: MIME

Mail agents

- Mail User Agents
 - MUAs are the source and destination of e-mail
 - Pine, Microsoft Outlook, MH, Mozilla, Elm, mail etc.
- Mail Transfer Agents
 - MTAs transport and route the messages from the sender's MUA to the recipient's MUA
 - This is applications level routing and similar to but not related to IP-routing
 - The decision is made based on the recipient's address
 - Spam blocking is an exception
 - The recipient's address may be changed
 - E.g. e-mail aliases, .forward

The e-Mail Message's Journey

- The message in the SMTP-standard consists of two parts
 - The envelope is information transmitted using SMTP protocol units
 - The contents includes the headers and body of the message
- The MUA receives the message from the end user and interprets the correct sender and receiver information
- The message is passed to the MTA for transportation over the network
 - Usually the message is first stored in a spool directory to wait until it can be transmitted to the next MTA
 - At the destination the message is placed into the recipient's mailbox
 - usually a file, can also be a directory or a database
- In practice the distinction between modern MTA and MUA software is not always clear

Sample SMTP Session Initiation

```
18 riku@mole $ telnet nixu-gw.nixu.fi 25
Trying 194.197.118.1...
Connected to nixu-gw.nixu.fi.
220 nixu-gw.nixu.fi ESMTP Sendmail 8.9.3/8.9.3; Tue, 13 Apr 1999 13:40:05 +0300
HELP
214-This is Sendmail version 8.9.3
214-Topics:
214-   HELO     EHLO     MAIL     RCPT     DATA
214-   RSET     NOOP     QUIT     HELP     VRFY
214-   EXPN     VERB     ETRN     DSN
214-For more info use "HELP <topic>".
214-To report bugs in the implementation send email to
214-   sendmail-bugs@sendmail.org.
214-For local information send email to Postmaster.
214 End of HELP info
EHLO mole.nixu.fi
250-nixu-gw.nixu.fi Hello mole.nixu.fi [194.197.118.22], pleased to meet you
250-8BITMIME
250-SIZE
250-DSN
250-XUSR
250 HELP
```

Sending the Message in SMTP

```
MAIL From: <riku@mole.nixu.fi>
250 <riku@mole.nixu.fi>... Sender ok
RCPT To: <Timo.Kiravuo@nixu.fi>
250 <Timo.Kiravuo@nixu.fi>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
From: <riku@mole.nixu.fi>
To: <Timo.Kiravuo@nixu.fi>
Subject: foobar
Demo material for SMTP course
.
250 NAA12630 Message accepted for delivery
QUIT
221 nixu-gw.nixu.fi closing connection
Connection closed by foreign host.
19 riku@mole $
```

The Message Structure

- The envelope contains the MTA's view of the sender and receiver
 - This is why you receive complaints about viruses and spam you have not sent
 - These are transported in the MAIL FROM and RCPT TO commands of the SMTP protocol
 - Notice the difference between the "From:" in the message headers and the "From" in the envelope
- Headers
 - From the beginning of the content until the first empty line
 - Format is "field-name: field body"
 - Some are mandatory, some not
- Body
 - After first empty line until the end of the message

SMTP and DNS

- MXs
 - Mail eXchanger - records in DNS
 - Enables mail forwarding in cases where access to customers mail-server is limited
 - Example: part of sral.fi MXs

```
sral.fi. IN MX 1 bar.foo.fi.  
sral.fi. IN MX 10 smtp3.kolumbus.fi.
```
- Logic: Mail is transferred only closer to destination
 - Smaller MX-value means that machine is closer to destination
 - Machine with the smallest MX-value is tried first, then the machine with the next smallest and so on...

...SMTP and DNS

- Explicit MXs
 - Defined MXs
 - e.g. sral.fi. IN MX 1 bar.foo.fi.
- Implicit MXs
 - If a machine has an IP-address, is also has an implicit MX with value of 0
 - e.g. bar.foo.fi. IN A 193.209.237.254
- Wildcard-MXs
 - If a whole domain is handled by one server, it can be configured with a wildcard MX
 - Use with caution (wrong configuration causes “tennis tournaments”)!
 - e.g. *.wild.fi. IN MX 1 mail.wild.fi.

...SMTP and DNS

- Order of use: explicit-implicit-wildcard
 - If none found: Host unknown
- Errors in DNS are critical! Mail can not be delivered without functioning name service

...SMTP and DNS

- The right side of MX record has to be a name with an A-record
 - Especially the use of CNAME in MX record is wrong
 - Correct:

```
a-ok.fi. IN MX 1 machine.a-ok.fi.  
machine.a-ok.fi. IN A 192.0.0.2
```
 - Wrong:

```
wrongdoer.fi. IN MX 1 mail.wrongdoer.fi.  
mail.wrongdoer.fi. IN CNAME machine.wrongdoer.fi.  
machine.wrongdoer.fi. IN A 192.0.0.2
```
 - Unstable problem

...SMTP and DNS

- DNS-data can be misconfigured. (Easy !)
 - Different data in different servers
 - No MX records for machines which should receive mail
 - MX records for machines which do not receive mail
 - DNS-configuration lacks end-dots:

```
adjuster.fi. IN MX 10 smtp.isp.fi.adjuster.fi.
```
 - Many others

```
horse.foo.fi.      IN      A      222.333.444.555
```
- DNS and MTA configurations must agree almost completely or horrors will happen.

Sendmail

- The most common MTA and a reference implementation
- A rather complex and capable piece of software
 - Supports many message formats
 - Can route messages between different e-mail systems
- Three modes of operation
 - Daemon, which receives e-mail over SMTP at TCP port 25 and forwards it as needed
 - To a local user's mailbox
 - To a different host using SMTP
 - To a different mail system using some protocol (UUCP, X.400)
 - Local, operation initiated by the user's MUA, Sendmail receives the message and takes the appropriate action as previously
 - Housekeeping actions, e.g. when started under the alias "newaliases" sendmail reads the changes in mail alias configuration

Usage of Sendmail (might be dated)

- Heart of sendmail installation: configuration file
 - sendmail.cf
 - Too complex to cover here
- Start-up in system boot
 - /usr/lib/sendmail -bd -q30m
 - -bd: server mode
 - -q30m: process the mail queue in every 30 minutes

...Usage of Sendmail

- How to check status
 - Either telnet to SMTP-port

```
$ telnet server.company.fi 25
Trying...
Connected to server.company.fi.
220 server.company.fi ESMTP Sendmail ready
QUIT
```
 - or check process list

```
$ ps -ef | grep sendmail | grep -v grep
root 778 ... 0:04 sendmail: accepting connections
```

 - If sendmail is currently processing queues, there might be other processes running, but they don't have the "accepting connections"-string

...Usage of Sendmail

- Killing
 - Must be root
 - Check process-number from the output of above mentioned ps-command (1st number in line) and give it a kill-command

```
# kill 778
```
- Restart
 - Must be root
 - Use command `/usr/lib/sendmail -bd -q30m`
 - Check status

...Usage of Sendmail

- Forced processing of mail queue
 - Normally mail queue contains data
 - Contents of mail queue can be viewed with command `mailq` or `/usr/lib/sendmail -bp`
 - You can force immediate processing with command `/usr/lib/sendmail -q`
 - If you want to observe what happens use command `/usr/lib/sendmail -q -v`
- Configuration
 - Sendmail configuration is in file `sendmail.cf`
 - Do not edit, unless you know what you are doing!

Aliases File

- A feature of Sendmail and many other MTAs
- Contains mappings of one local user-id to mail addresses, these affect the left hand side of the e-mail address

```
postmaster: yllapito
root: yllapito
yllapito: kiravuo, samuli, sakke
rd: nasse, hessu, lisse@hut.fi
timo.kiravuo: kiravuo
birds-list: :include:/home/hessu/lists/birds
```

- The target can be:
 - A list of local or remote users
 - A file of mail addresses
 - A program

Procmail and .forward

- .forward is a feature of the Sendmail program is that the user may redirect his own e-mail to another address
 - An easy way to generate mail loops when the user makes two mailboxes to point to each other
 - When the message has collected enough "Received:" headers, it is bounced back to the sender
- The .forward -file may also direct the message to a program
- Procmail is one popular program that can process e-mail messages, e.g.
 - Distribute messages to different folders
 - Run them through a personal spam filter
 - Send an SMS message when an e-mail message matches some rule
 - Reply to the sender that the user is on vacation

Log files

- Sendmail keeps log of its activities through syslog (see. /etc/syslog.conf)
- Samples from log files
 - Message from riku at mole.nixu.fi
 - Actual message looks like this:

```
From: riku.kalinen@nixu.fi
To: oh2lwo@sral.fi
Cc: riku.kalinen@nixu.fi
Subject: Teshting
Please ignore
```

Log tracking, mole.nixu.fi

- **Message has been received**

```
Apr 13 14:26:04 mole sendmail[15822]: OAA15822:  
  from=riku, size=104, class=0, pri=60104, nrcpts=2,  
  msgid=<199904131125.OAA15822@mole.nixu.fi>,  
  relay=riku@localhost
```

- **Message sent for oh2lwo@sral.fi to bar.foo.fi**

```
Apr 13 14:26:06 mole sendmail[15822]: OAA15822:  
  to=oh2lwo@sral.fi, ctladdr=riku (1138/200),  
  delay=00:00:14, xdelay=00:00:02, mailer=esmtplib,  
  relay=bar.foo.fi. [193.209.237.254], stat=Sent  
  (OAA13538 Message accepted for delivery)
```

- **Message sent for riku@nixu.fi locally**

```
Apr 13 14:26:06 mole sendmail[15822]: OAA15822:  
  to=riku@nixu.fi, ctladdr=riku (1138/200),  
  delay=00:00:14, xdelay=00:00:00, mailer=local,  
  stat=Sent
```

Error situations and recovery

- Host unknown
 - string right from @-character is not found in DNS
 - Either a typo in address or
 - DNS configuration error
- User unknown
 - string left from @-character does not match with any user, mailing-list or alias in receiving machine
- Postmaster missing
 - Serious fault
 - If there is a MX entry, there must also be a postmaster
 - Makes problem solving a pain

...Error situations and recovery

- Too many hops
 - Seen with customers who have misconfigured sendmails
 - Mail goes to customer's server that does not know how to handle it
 - Customer's server sends mail to a "smarter" server: smtp.isp.fi
 - Which sends it back to customer's server...
 - After about 25 hops the mail bounces
 - Typical with misconfigured wildcard MXs
- Local configuration error
 - Receiving server did not know how to handle the mail
 - Typically disagreement between MTA configuration and DNS

...Error situations and recovery

- Connection timed out, no route to host
 - Mail gets queued and returns back to sender in few days
 - Typically packets are blocked by access lists
 - Could also be a bad network connection
- Connection refused
 - SMTP-port of receiving machine is not responding
- Sender domain must exist, relaying denied, client must resolve, RBL, ORBS, DUL, ...
 - Typical spam filter responses
 - Misconfigured or blacklisted sender

Message tracing

- Might be necessary for tracking fake-mail vandals or during normal error checking
- From headers
 - If the receiver saves the message with all the headers, is tracing far easier than from the log files
 - Take especially good look at the first Received: -fields
- From logs
 - Access is needed to all the machines that the message went through

Post Office Protocol (POP)

- Protocol for retrieving e-mail from a mail server
 - POP2 -> Standard in the mid 80's, requires SMTP to send messages (rfc937)
 - POP3 -> Newer version, can be used without SMTP (rfc1225 and others)
- Not intended to provide extensive manipulation
 - Operations of mail on the server:
 - download & delete

Internet Message Access Protocol (IMAP)

- A protocol for retrieving e-mail messages
- There is three operational modes in IMAP:
 - offline: fetch and delete
 - online: interactive
 - disconnected: cache copy
- Several RFC's: 1730, 2060, 2061....
- Server - Client Modes
 - Reliable data stream: TCP/IP
 - Mail repository: status flags on mail
 - All/part of the message is copied

Online Mode

- Search for message headers/bodies, no need for download
- Messages left on server
- Selective fetch :
 - e.g., message header, body, or part of the body
 - server based search, minimizes download; low bandwidth lines
 - e.g., large messages; audio, video
- Possibility to manipulate inbox
- Folder management
 - folders can persist on server

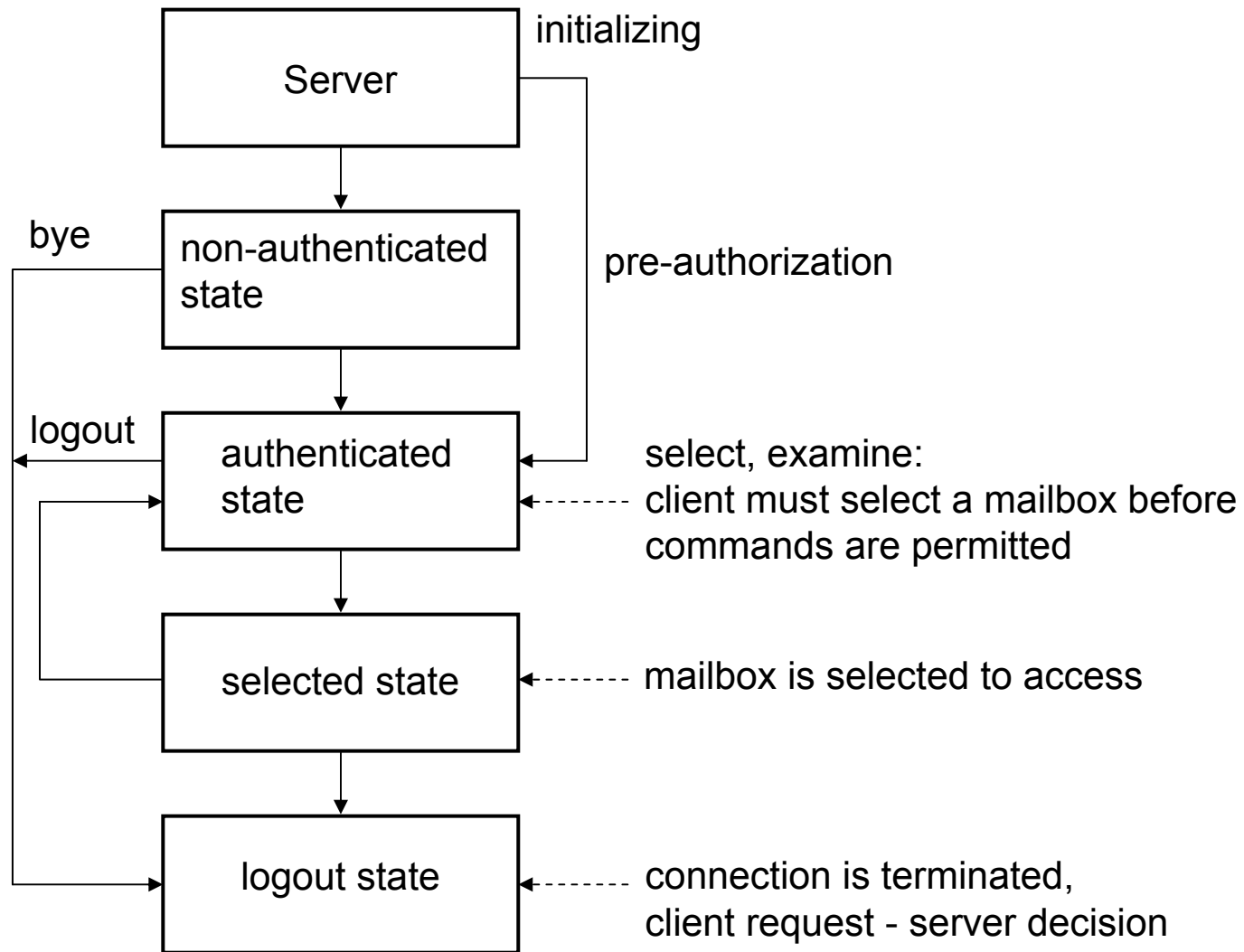
Online & Disconnected Modes

- Remote folder manipulation:
 - appending messages to a remote folder
 - message status flags
 - shared folders, simultaneous update
 - new mail notification
- Multiple folder support :
 - manipulating remote folders
 - list/create/delete/rename, remote folder management
 - hierarchies
 - Non e-mail data, e.g., net news and document accessing.
- Disconnected operations support
 - Messages are operated based on unique message-id

Offline Mode

- For minimum connect time & disk usage
- Copied mail can be deleted from the server (configurable)

States of an IMAP server



Multipurpose Internet Mail Extensions

- A standard to use in e-mail
 - Text other than US-ASCII
 - Non-textual data formats
 - Multipart messages
 - Textual header information using characters other than US-ASCII
- Several standards and extensions
 - 2045 MIME Part One: Format of Internet Message Bodies
 - 2046 MIME Part Two: Media Types
 - 2047 MIME Part Three: Message Header Extensions for Non-ASCII Text
 - 2048 MIME Part Four: Registration Procedures
 - 2049 MIME Part Five: Conformance Criteria and Examples
- MIME types are also used by other protocols and services
 - E.g. HTTP

MIME Message (simplified)

```
FROM: "MS Security Center" <aytnddhiqp@support_msdn.net>  
TO: "Partner" <partner@support_msdn.net>  
SUBJECT: Current Net Security Patch  
Mime-Version: 1.0  
Content-Type: multipart/mixed; boundary="dgrvzwnprd"
```

```
--dgrvzwnprd  
Content-Type: multipart/related;  
    boundary="jtdukndxczlsbnv";  
        type="multipart/alternative"
```

```
--jtdukndxczlsbnv  
Content-Type: text/plain  
Content-Transfer-Encoding: quoted-printable
```

Microsoft Partner

this is the latest version of security update, the...

MIME Message (cont.)

```
--jtdukndxczlsbnv
Content-Type: text/html
Content-Transfer-Encoding: quoted-printable
  <HTML>...
--jtdukndxczlsbnv--
--dgrvzwnprd
Content-Type: image/gif
Content-Transfer-Encoding: base64

R0lGODlhAA7APcAAP///+rp6puSp6GZrDUjUUC6Zn53mFJMdb...

--dgrvzwnprd
Content-Type: application/x-msdownload;
  name="Install65.exe"
Content-Transfer-Encoding: base64

TVqQAAMAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAA...
--dgrvzwnprd--
```

MIME

- The body of the message can contain multiple data objects
- Some objects can be alternative to each other
 - E.g. text and HTML representation for the message text
 - The sender can not know the capabilities of the receiver's MUA
- Binary data is coded so that it can pass through the 7-bit e-mail system
 - Some SMTP protocol implementations can not handle 8-bit data
 - Base-64 is usually used for binary data
 - Quoted-printable is used to encode the individual special characters in text data

- Headers have their own coding

```
From: =?GB2312?B?za/R1cHB18s=?=  
<info@shanghaity.com>
```

```
Subject: =?GB2312?B?za/R1cHB18vT68T6ubK2ybn6x+w=?=
```

Spam

- Unsolicited advertising
 - A real problem because of huge volume (100-200 messages per day)
- Usually sent from an e-mail server that allows relaying
 - The server accepts a message, that is not from a domain served by the server and is not targeted towards such domain
 - Spam senders usually falsify the sender address
 - The server used receives one message with plenty of recipients and it has to bear the burden of delivery

Solutions to Combat Spam

- Basic checks
 - The e-mail server should verify that either the sender or receiver address of a message matches the server's domains
 - This prevents a lot of relaying
 - Sending host's IP address should have a reverse DNS record
- Server blacklists
 - Known servers that send or relay spam
- Bayesian (artificial intelligence) filtering
 - The system learns to recognize spam
 - Currently considered a promising approach
- Legal solutions
- For more information see <http://spam.abuse.net/>

E-mail Viruses

- Malicious programs that use e-mail to spread from user to user
- Typically take advantage of features and security weaknesses of e-mail MUAs to activate their own code
- Can transmit files, destroy data etc.
- Solutions
 - Constantly updated anti-virus software that identifies known viruses
 - Using an MUA that is not vulnerable