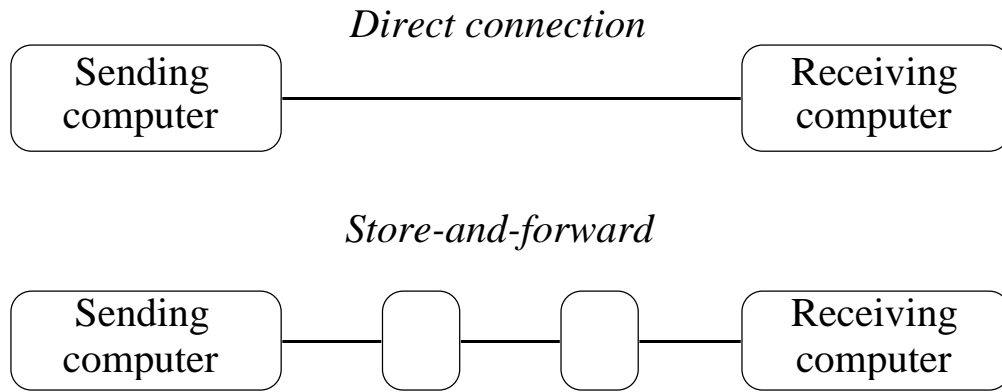
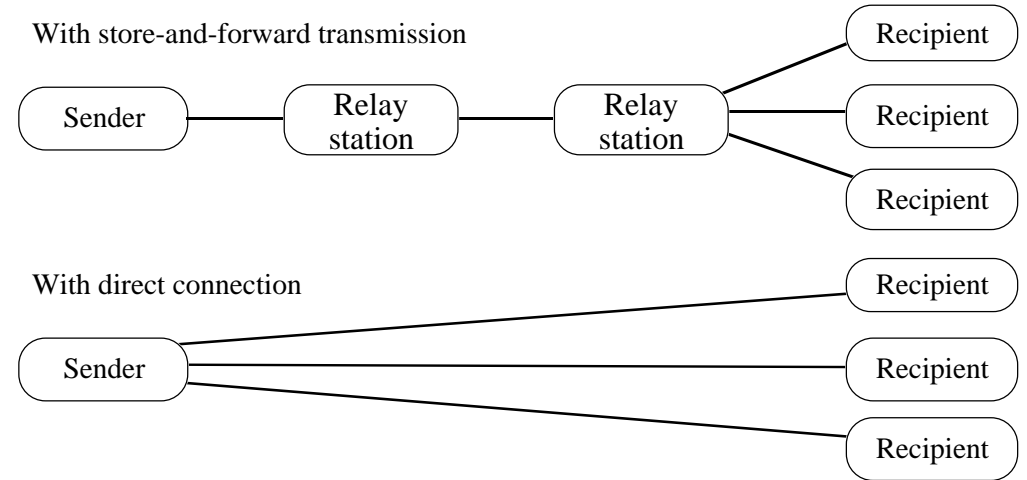


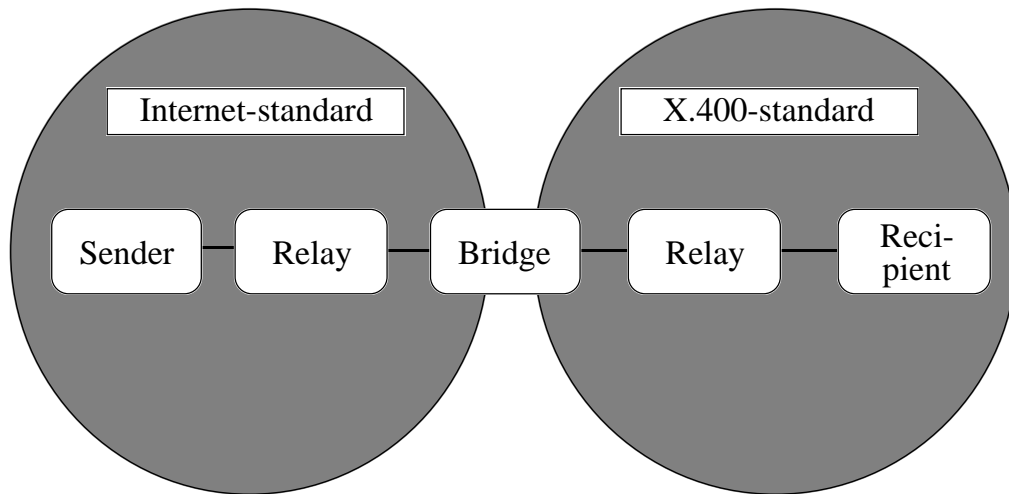
Direct connection and store-and-forward



Many distant recipients



Gateways' use of store-and-forward



Store-and-forward pros and cons

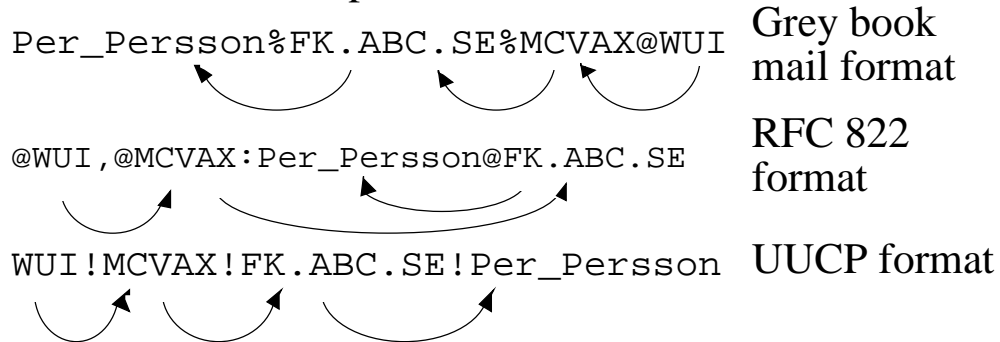
- + Distribution of tasks between specialized servers. But direct transmission can employ special routing information servers.
- + Reduced cost for message to many distant recipients.
- + Gateways usually store-and-forward-based.
- Reliability
- Can be more expensive because relayers must be paid.

Spooling - a limited kind of store-and-forward

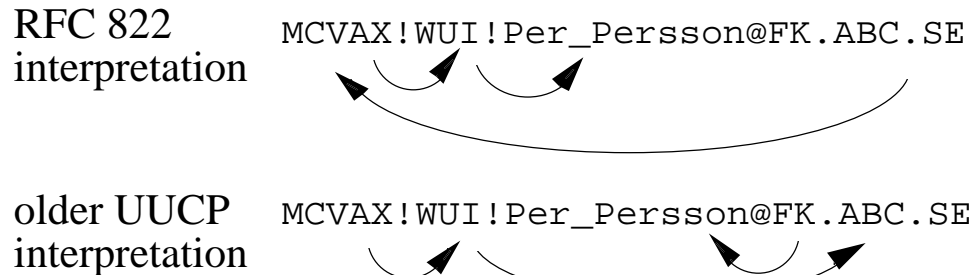
- No direct and immediate confirmation that the message has been delivered.
- + The sender need not wait during the transmission.
- + Temporary connection problems hidden from the user.

Absolute and relative addresses

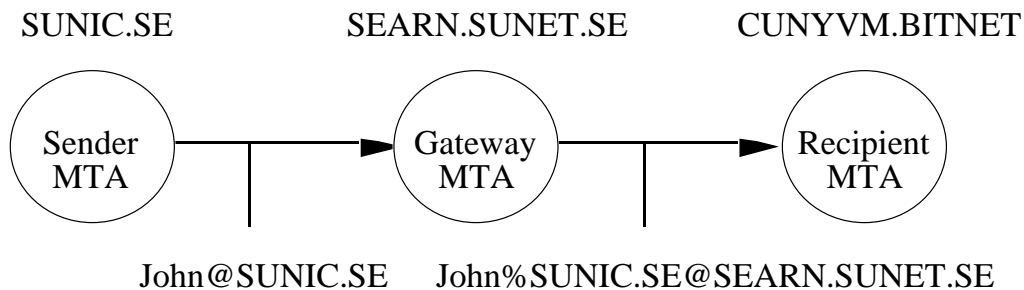
An *absolute address* is the same address for a certain recipient, irrespective of where the message is sent from. A *relative address* indicates one or more relay stations on the route to the recipients.



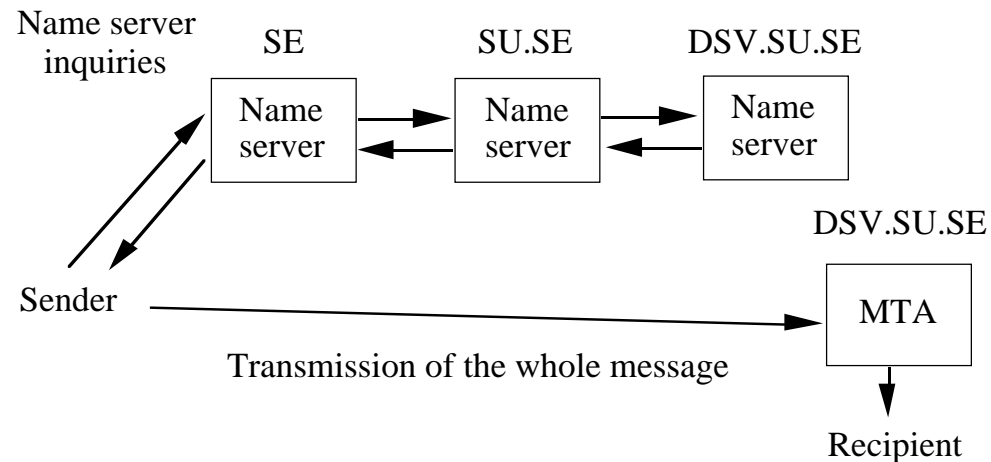
Mixed relative addressing



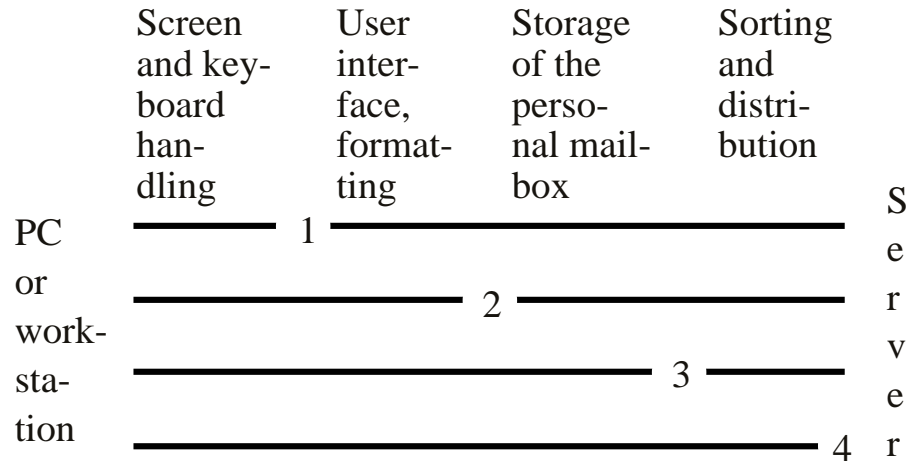
Why gateways produce relative addresses



Use of name servers for routing

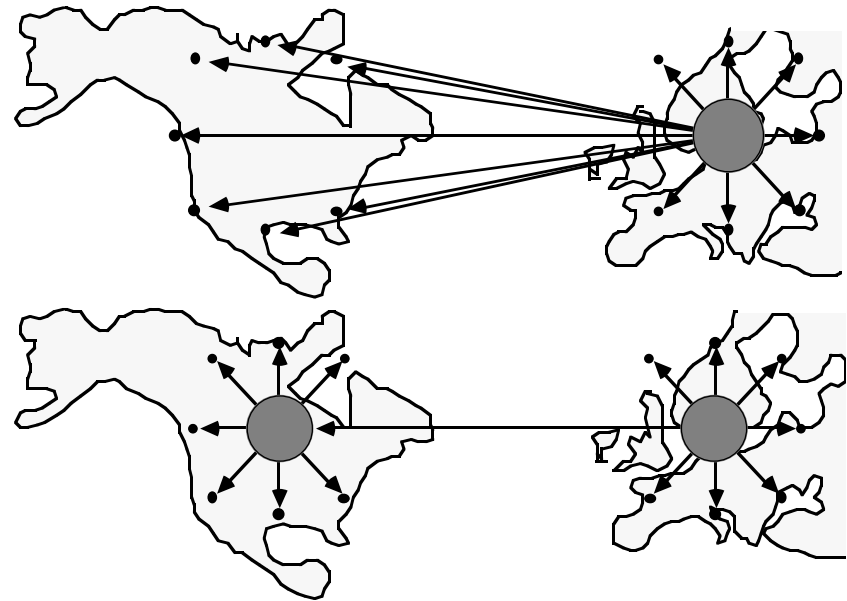


PC-Server E-mail Architectures

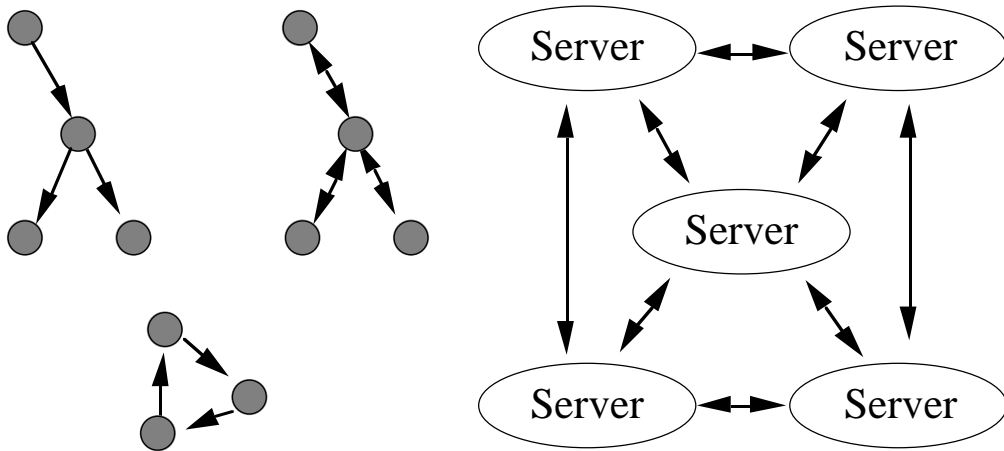


Protocols: POP (3), IMAP (2, 3)

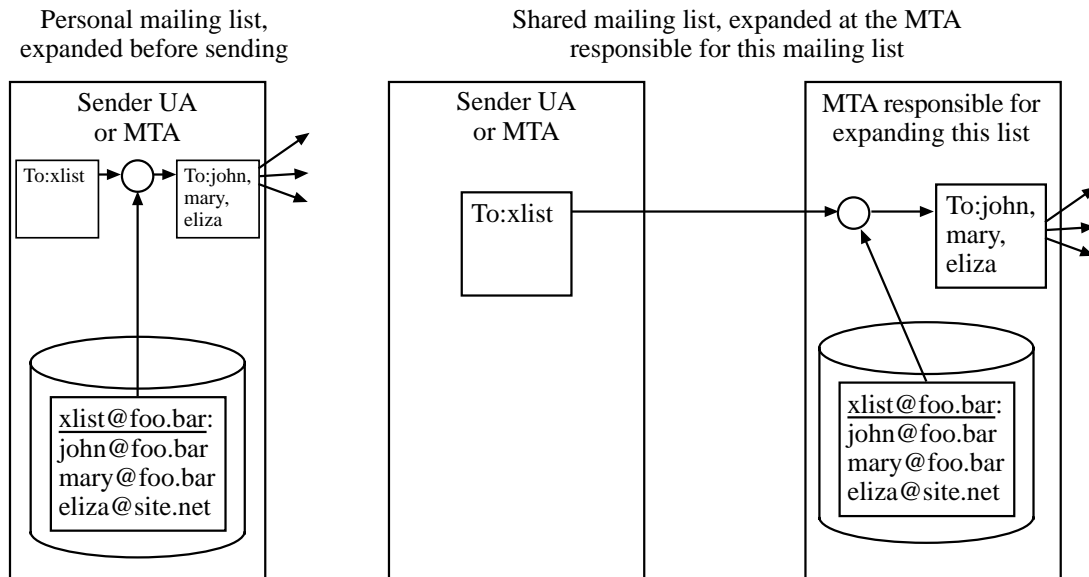
Nested distribution lists



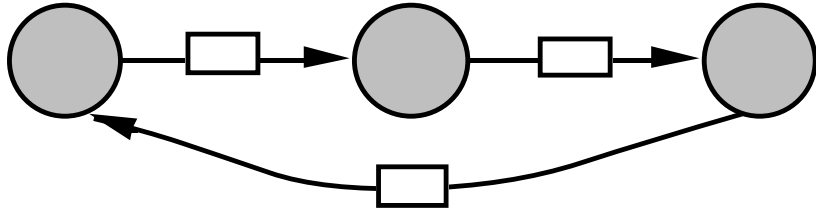
Modes of distribution to many recipients



Expansion of Nested Mailing Lists



Loop control for Nested Distribution Lists



- (1) Full expansion by the originating UA or MTA.
 - (2a) Trace list on the envelope, use to stop incoming messages.
 - (2b) Trace list on the envelope, use to stop outgoing messages.
 - (3) Registration system.
 - (4a) Storing Message-ID-s with DL expanders.
 - (4b) Storing content checksums with DL expanders.
- X.400: Primarily 2a, Listserv: 4a and 4b, Usenet News: 4a

List Headers (RFC 2369)

Meta-standard! Not specify a protocol, but specify how a mail header can specify a protocol for common actions on mailing lists:

List-Subscribe: <mailto:ietf-xml-mime-request@imc.org?body=subscribe>

List-Unsubscribe: <mailto:ietf-xml-mime-request@imc.org?body=unsubscribe>

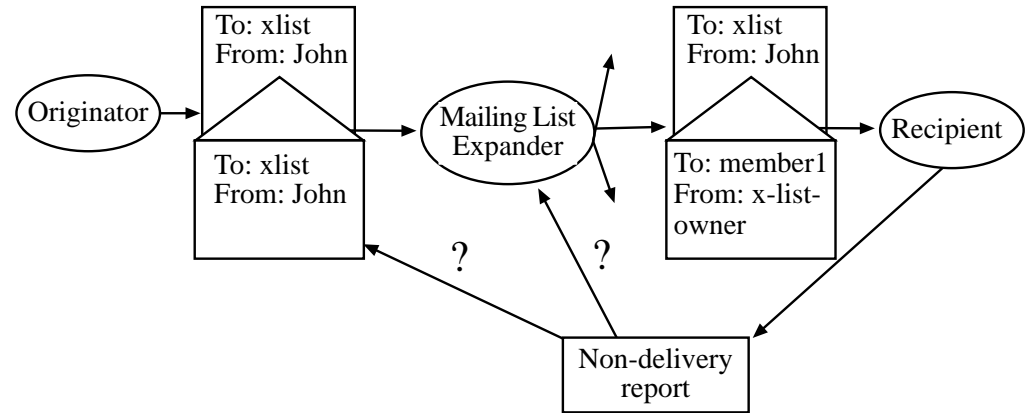
List-Help: <http://www.imc.org/ietf-xml-mime/>

List-Archive: <http://www.imc.org/ietf-xml-mime/mail-archive/>

List-ID: <ietf-xml-mime.imc.org>

Distribution Lists in Internet Mail

- No standardized loop control for nested lists
- “-request”-convention
- SMTP sender = address of list maintainer
- Non-delivery reports sent to SMTP sender



Public/secret key encryption

encrypted text = f_1 (original text)

original text = f_2 (encrypted text)

Can f_2 be derived from f_1 ?

Pros and cons of public key encryption

- + Solves partly key transportation problem
- More CPU-time consuming

Authentication, authorization

- To verify the sender of a message
- Payments, agreements
- UA-UA or MTA-MTA



Authentication methods

- (a) Passwords
- (b) Specially designed networks
- (c) Public key cryptography

Digital Signatures and Digital Seals

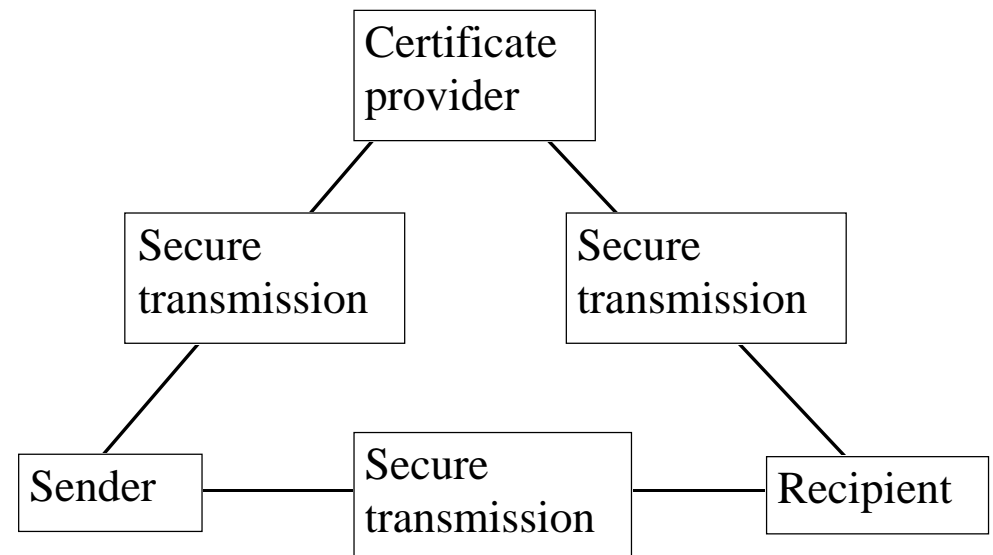
Methods: Secret key encryption of signature or checksum, which anyone can decrypt with public key

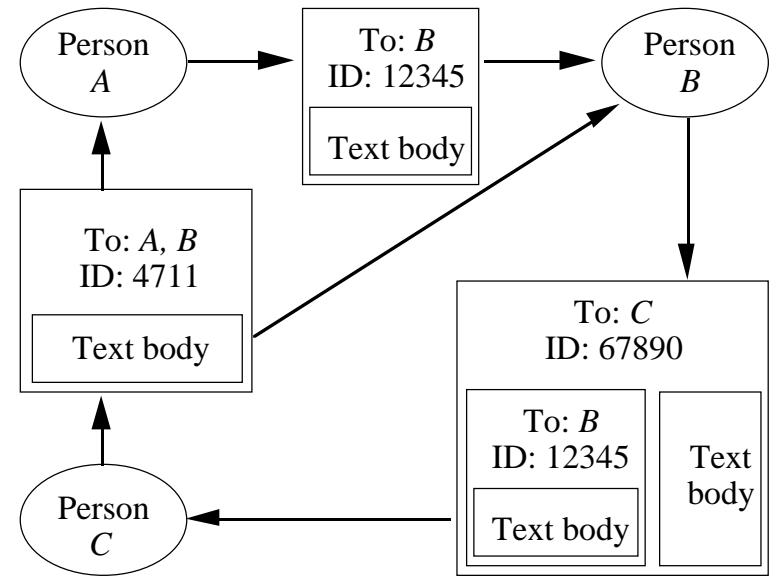
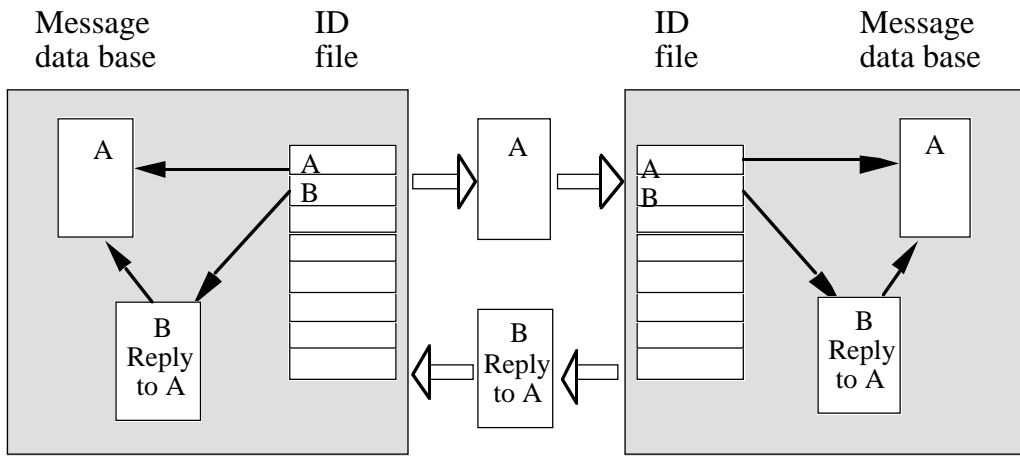
- Number of interactions
- Need of a neutral third party
- Bilateral or open to groups

Three levels of protection of message transmission:

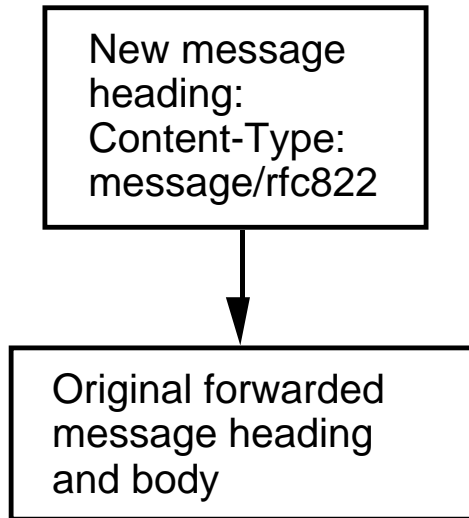
- (1) The agents identify each other using noninvertible forms of ordinary passwords. This is called *weak authentication*.
- (2) The agents identify each other using public key encryption algorithms. This is called *strong authentication*.
- (3) Strong authentication is combined with encryption of all messages during the whole transmission.

Certificate Authorities

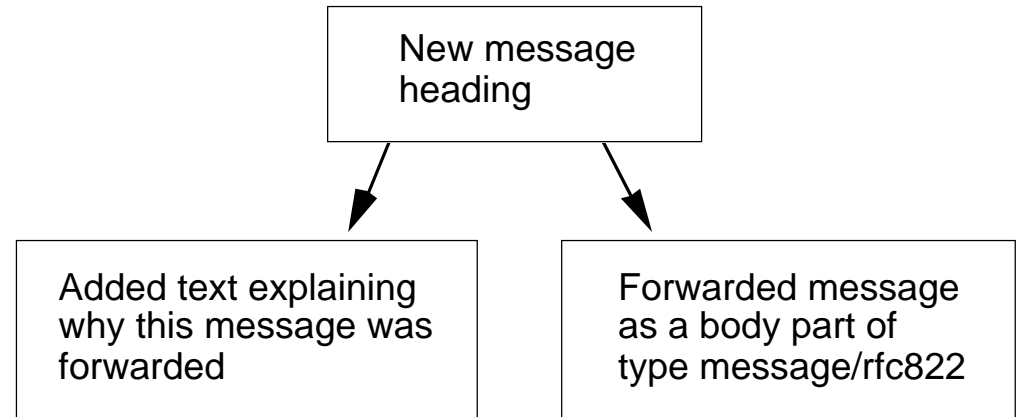




Forwarding with a MIME Message/rfc822



Forwarding with a MIME multipart message

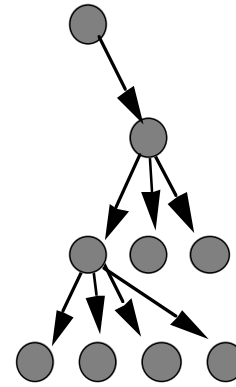


Methods of e-mail forwarding

- (a) Add new Resent-headers to the original message. Example of a message header with Resent-headers:
- (b) The forwarded message is made into a body part of type message/rfc822 in a new multipart message:
- (c) The text of the forwarded message is simply copied into the text of the new message.

Which method is best if the forwarded message had a digital seal?

Distribution lists



Usenet News distribution method

