*:96 Overheads

Part 3b: E-mail basics

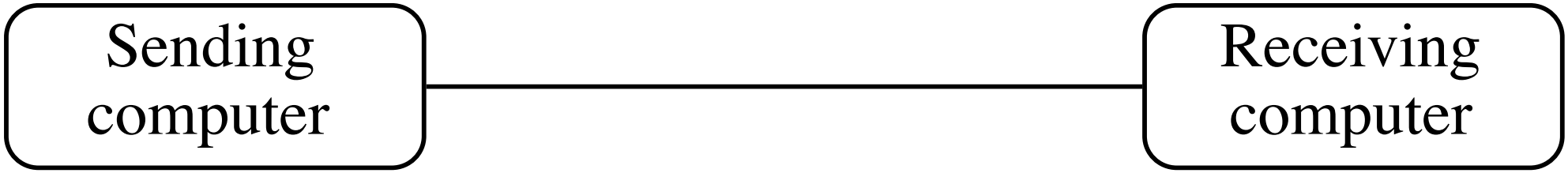
More about this course about Internet application protocols can be found at URL:

`http://www.dsv.su.se/~jpalme/internet-course/Int-app-prot-kurs.html`

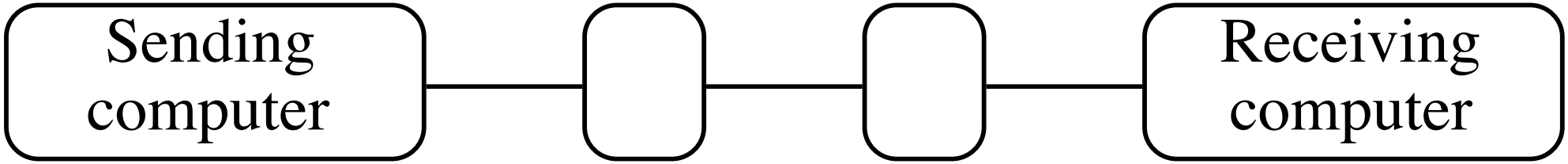
Last update: 29 Jan 2005

Direct connection and store-and-forward

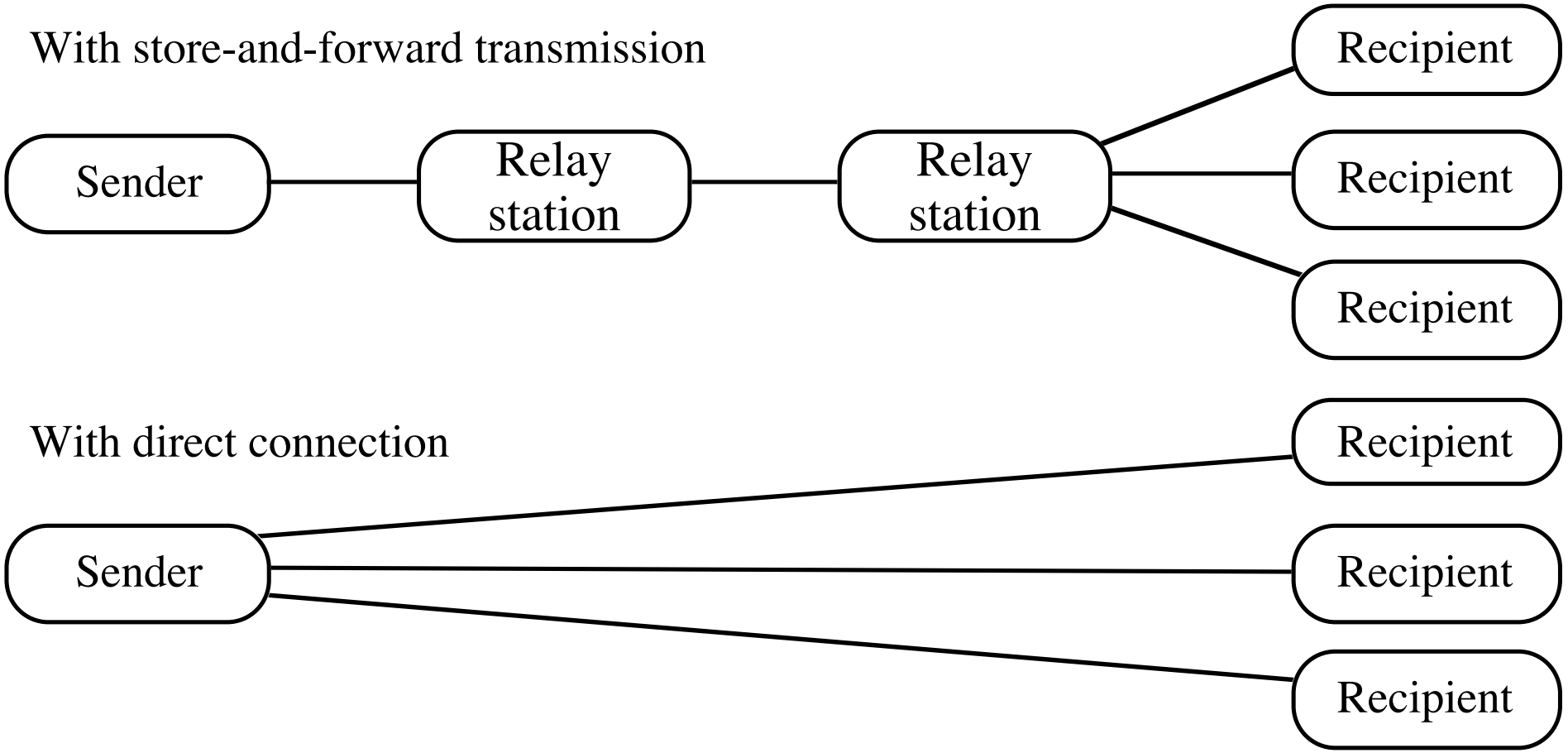
Direct connection



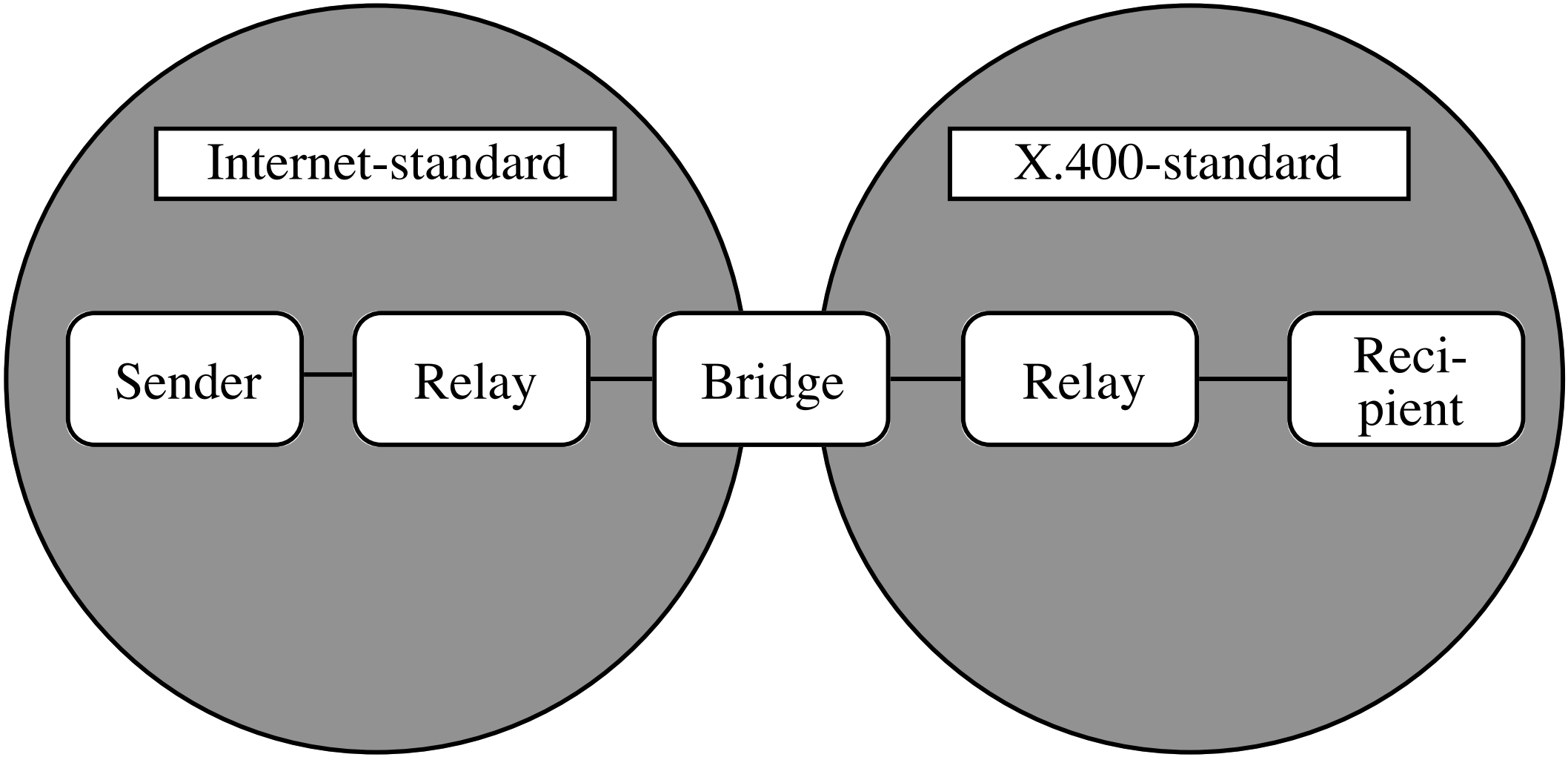
Store-and-forward



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

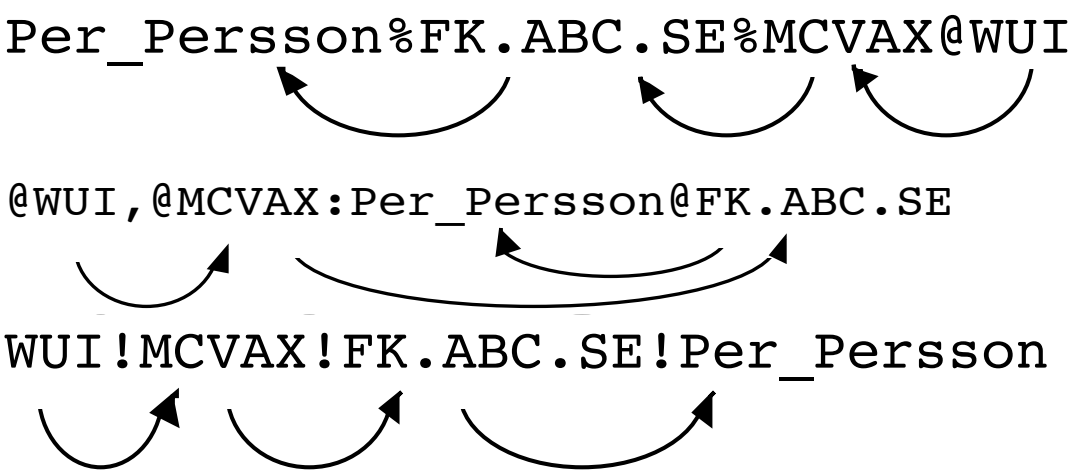
– No direct and immediate confirmation that the message has been delivered.

\+ 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.



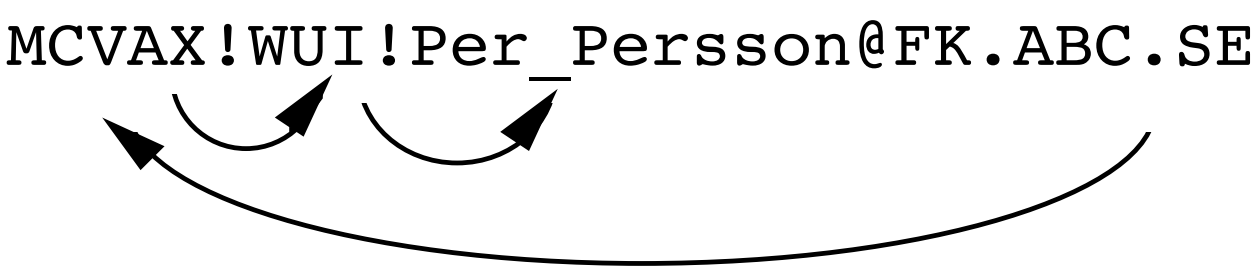
Grey book mail format

RFC 822 format

UUCP format

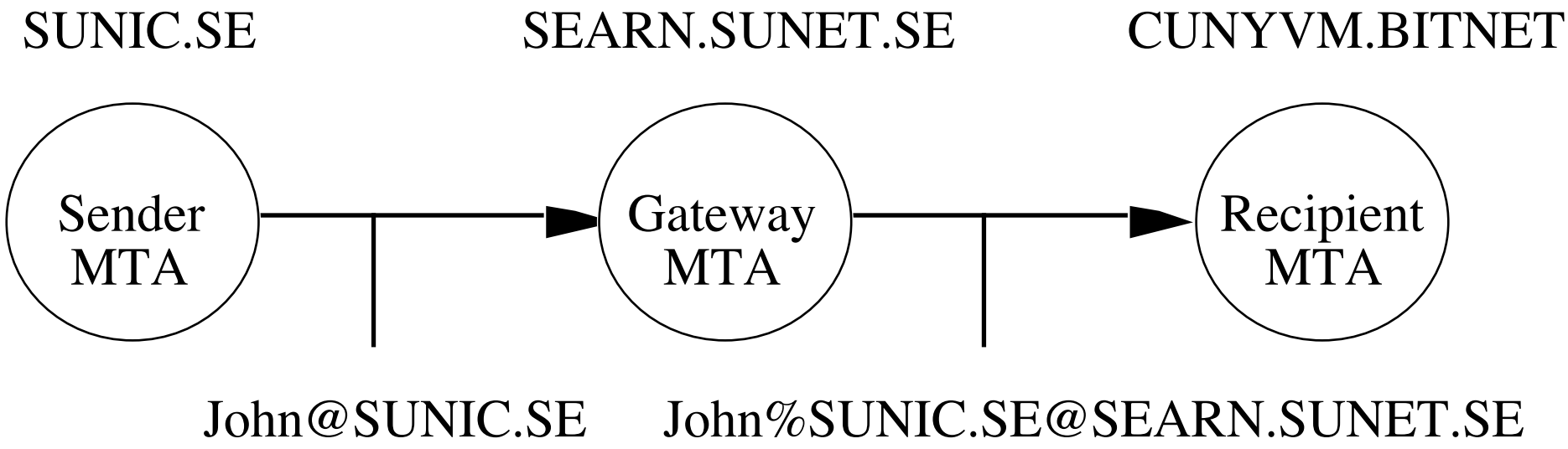
Mixed relative addressing

RFC 822 interpretation

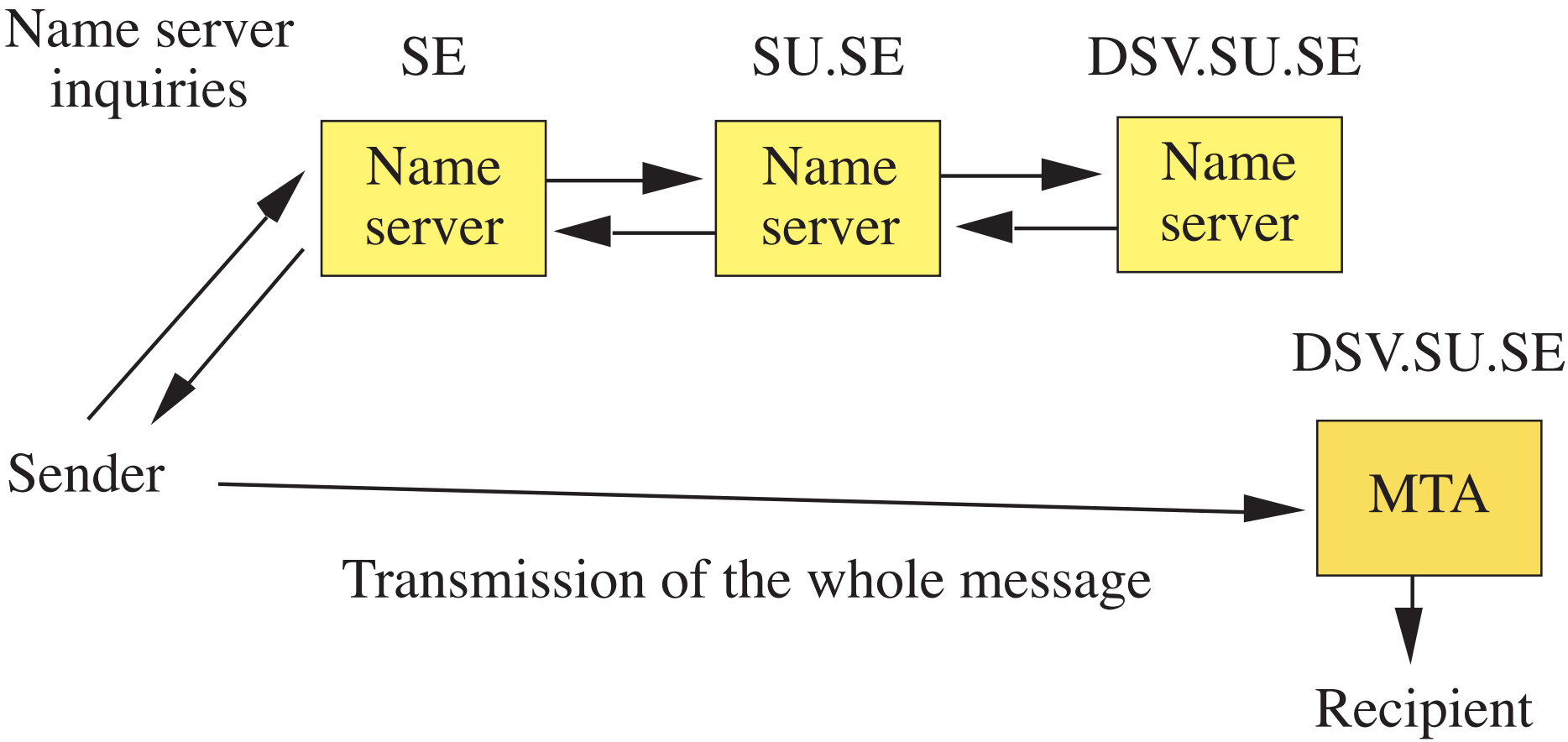


older UUCP interpretation

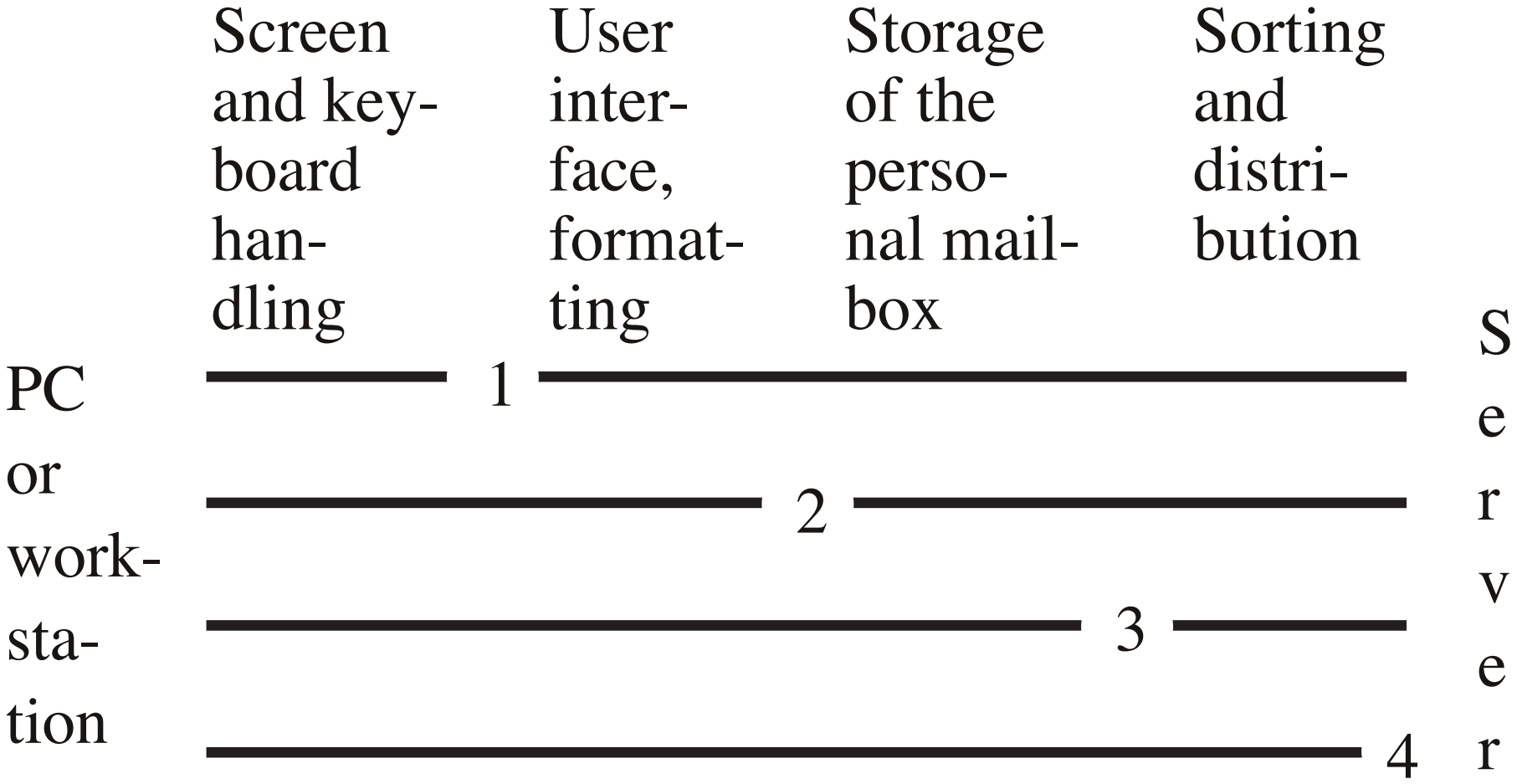
Why gateways produce relative addresses



Use of DNS servers for routing



PC-Server E-mail Architectures



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

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

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.

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

Certificate Authorities