Compendium 9 extra:
Not allowed during the exam

Last revision: 3 Feb 2001

Font Size Comparisons as Shown on Screen.......................................................................................2
E-mail Basics Overheads............................................................................................................................3
The Multipart/related Content-Type.......................................................................................................10
Font Size Comparisons as shown on Screen

Jacob Palme <jpalme@dsv.su.se>
Last change: 2001-02-01

Fonts marked with an asterisk in the table below are unreadable with some web browsers on some platforms.

With Explorer 5.0,
10 pt corresponds to 12 px and
12 pt corresponds to 16 px.

<table>
<thead>
<tr>
<th>Times 7 pt *</th>
<th>Times 8 pt *</th>
<th>Times 9 pt *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Times 10 pt</td>
<td>Times 12 pt</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Verdana 7 pt *</th>
<th>Verdana 8 pt *</th>
<th>Verdana 9 pt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verdana 10 pt</td>
<td>Verdana 12 pt</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Times xx-small</th>
<th>Times x-small *1</th>
<th>Times small</th>
</tr>
</thead>
<tbody>
<tr>
<td>Times medium</td>
<td>Times large</td>
<td>Times smaller</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Times larger</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Verdana xx-small</th>
<th>Verdana x-small *</th>
<th>Verdana small</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verdana medium</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Anonymity server

From: A
To: B

From: P1234
To: B

Some Listserv commands

subscribe       Join a distribution list
unsubscribe     Leave a distribution list
list            Get a list of distribution lists available from this list server
list global     Get a list of distribution lists available everywhere
review          Get more information about one particular list
query           Find out your own subscription settings to a list

More Listserv commands

set             Change your subscriptions settings to a list
confirm         Confirm that you want to stay on a list
stats           Get statistics on a list
register        Register your name and e-mail address with a list server

Listserv retrieval commands

index           Get a list of available documents
get             Get a document
afd             Subscribe to a copy of a document, every time it is changed
query file      Get more information about a particular document
give           Send a document to someone else than yourself
pw              Change your password
### Risks
- Denial of service
- Masquerade
- Nonauthorized access
- Data modification or destruction
- Traffic analysis
- Deduction of information
- Illegal activities

### Cryptographic Security Services
- Encrypted transmission of data
- Digital signatures
- Digital seals
- Digital authentication
- Digital authorization

---

**Explanation of undesirable non-delivery notification**

**Direct connection and store-and-forward**

1. **Direct connection**
   - Sending computer
   - Receiving computer

2. **Store-and-forward**
   - Sending computer
   - Intermediate nodes
   - Receiving computer
Gateways’ use of store-and-forward

Many distant recipients

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.

**Per_Persson%FK.ABC.SE%MCVAX@WUI**

- Grey book mail format
- RFC 822 format
- UUCP format

Why gateways produce relative addresses

**SUNIC.SE** | **SEARN.SUNET.SE** | **CUNYVM.BITNET**

- Sender MTA
- Gateway MTA
- Recipient MTA

Problems with replies with relative addressing

Person A → Person B → Person C

Person A

Person B → Person C

Person A → Person B → Person C

Person A

Person B → Person C

Similar problem with distribution lists

**Distribution list**

Person A

Person B
Use of name servers for routing

Sender

Name server

SE

Name server

SU.SE

Name server

DSV.SU.SE

DSV.SU.SE

MTA

Recipient

Transmission of the whole message

Client-server architectures

<table>
<thead>
<tr>
<th>Screen and keyboard handling</th>
<th>User interface formatting</th>
<th>Storage of the personal mailbox</th>
<th>Sorting and distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC</td>
<td>1</td>
<td>Server</td>
<td></td>
</tr>
<tr>
<td>or Workstation</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td></td>
<td>Server</td>
</tr>
</tbody>
</table>

Protocols: P3, P7, POP, IMAP

Modes of distribution to many recipients

Nested distribution lists
Loop control for Nested Distribution Lists

1. Full expansion by the originating UA.
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: 4b have seen.

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

<table>
<thead>
<tr>
<th>The verifier</th>
<th>The identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate a random number.</td>
<td>Decrypt the encrypted number.</td>
</tr>
<tr>
<td>Encrypt it using the public key of the identifier.</td>
<td>Return the decrypted number.</td>
</tr>
<tr>
<td>Send the encrypted random number to the identifier.</td>
<td>Check that the initial random number is returned.</td>
</tr>
</tbody>
</table>
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
The Multipart/Related Content Type

The Multipart/related content type is designed when you are sending several files, which are related by URL-links. It is used, for example, to send HTML, SGML and XML with embedded pictures or applets as separate files.

Each file is a separate body part. Each body part is labelled by either Content-ID or Content-Location. The URL referring to the body part from another body part, is of the URL type "cid:" to refer to a Content-ID, or can be any kind of URL (absolute or relative) to refer to a Content-Location with the same content.

Example (abbreviated):

<table>
<thead>
<tr>
<th>Content-Type: Multipart/related</th>
<th>The compound object of the HTML text and the embedded message.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type: Text/html</td>
<td>The main text in HTL format.</td>
</tr>
<tr>
<td>&lt;IMG SRC=&quot;cid:1*<a href="mailto:foo@bar.net">foo@bar.net</a>&quot;</td>
<td>Link to an embedded image using a &quot;cid:&quot; type URL.</td>
</tr>
<tr>
<td>&lt;IMG SRC=&quot;picture.gif&quot;</td>
<td>Link to an embedded image using a relative URL.</td>
</tr>
<tr>
<td>Content-Type: Image/gif</td>
<td>The first embedded image, identified by a Content-ID.</td>
</tr>
<tr>
<td>Content-ID: 1*<a href="mailto:foo@bar.net">foo@bar.net</a></td>
<td></td>
</tr>
<tr>
<td>Content-Type: Image/gif</td>
<td>The second embedded image, identified by a Content-Location URL.</td>
</tr>
<tr>
<td>Content-Location: picture.gif</td>
<td></td>
</tr>
</tbody>
</table>

Since some mailers do not support this, messages are usually sent using multipart/alternative, with plain text in the first branch and HTML in the second branch. This can be done in two ways:

**With the multipart/alternative inside the multipart/related:**

<table>
<thead>
<tr>
<th>Content-Type: Multipart/related</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type: Multipart/alternative</td>
</tr>
<tr>
<td>Content-Type: Text/plain</td>
</tr>
<tr>
<td>Content-Type: Text/html</td>
</tr>
<tr>
<td>Content-Type: Image/gif</td>
</tr>
<tr>
<td>Content-ID: 1*<a href="mailto:foo@bar.net">foo@bar.net</a></td>
</tr>
</tbody>
</table>

**With the multipart/alternative outside the multipart/related:**

<table>
<thead>
<tr>
<th>Content-Type: Multipart/alternative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type: Text/plain</td>
</tr>
<tr>
<td>Content-Type: Text/html</td>
</tr>
<tr>
<td>Content-Type: Multipart/related</td>
</tr>
<tr>
<td>Content-Type: Image/gif</td>
</tr>
</tbody>
</table>

Some mailers send messages using each of these methods, so a good mailer will have to be able to receive messages in both formats.