                 Principles of Operation for the TPC.INT Subdomain:
                       Remote Printing -- Administrative Policies

Status of this Memo

   This memo provides information for the Internet community. It does
   not specify an Internet standard. Distribution of this memo is
   unlimited.

Introduction

   This document defines the administrative policies for the operation
   of remote printer facilities within the context of the tpc.int
   subdomain. The document describes different approaches to resource
   recovery for remote printer server sites and includes discussions of
   issues pertaining to auditing, security, and denial of access.

   The technical procedures for remote printing are defined in [1]. The
   general principles of operation for the tpc.int subdomain are defined
   in [2]. An overview of the remote printing facility is returned when
   electronic mail is sent to tpc-faq@town.hall.org.

Overview of Remote Printing in the TPC.INT Subdomain

   The remote printing facility allows a user to image documents on a
   remote printer, defined as a G3-compatible facsimile device connected
   to the public telephone network. The user sends electronic mail to
   an address which includes the phone number associated with the target
   G3-compatible facsimile device. Using the Domain Name System, the
   Internet message-handling infrastructure routes the message to a
   remote printer server, which provides access to devices within a
   specified range of the telephone system numbering plan. The message
   is imaged on the target remote printer and an acknowledgement is sent
   back to the initiator of the message.

   The remote printing facility is concerned with outreach, integrating
   the e-mail and G3-compatible facsimile communities into a common
   communications environment. By providing easy access to remote
   printing recipients, enterprise-wide access is enhanced, regardless
   of the kind of institution (e.g., commercial, educational, or
   government), or the size of institution (e.g., global, regional, or

local). Remote printing allows an organization to make it easier for
electronic mail users to communicate with the personnel in the
organization who are users of G3-compatible facsimile but not e-mail,
providing a valuable bridge between the two types of technology.

Models of Operation for Remote Printing Servers

Remote printer servers in the tpc.int subdomain consume resources
that are typically recovered from neither the initiator nor the
recipient of the remote printing service. Owing to a lack of
widespread authentication facilities in the Internet and connected
message handling domains, it is not currently possible to identify
the initiator with certainty. Since the request was not initiated by
the recipient, it is inappropriate for a remote printer gateway to
accept a request and then attempt to charge the receiver of the
message before imaging the document on the remote printer.

Several models of resource recovery for remote printer operation are
possible in the tpc.int subdomain:

    Community Library Model
    Neighborhood Grocery Model
    Local Newspaper Model

In the Community Library model, an organization would register a
remote printer gateway willing to place calls to all devices located
within the organization's telephone system. Other operators may
determine that the costs of servicing the immediate vicinity (or even
a larger area) are minimal and register to serve a portion of the
telephone address space as a community service.

The Community Library model can apply to a neighborhood, or to an
organization such as a government R&D Center, a university, or a
corporation. The library model does not recover costs from the
particpants, but runs the remote printer as a community service.

In the Neighborhood Grocery model, a commercial organization
contracts with specific end users, offering to register their
individual fax numbers in the namespace. This service bureau model
could be conducted with or without cost recovery from the owner of
the remote printer device.

The Local Newspaper model recovers the resources needed to operate
the remote printer service from a third party not directly connected
with the message exchange. When a document is successfully imaged on
a remote printer, there are two actions that result. First, a cover
sheet is constructed and prepended to the document imaged on the
remote printer. Second, a notification is sent back to the

initiator. An Internet site running a remote printer server
registered in the tpc.int subdomain is permitted to acknowledge a
sponsor in both cases.

Specifically, up to one-third of the area of the cover sheet may be
used for acknowledgement of the sponsor, and up to 250 bytes of ASCII
text acknowledging the sponsor may be appended to the notification
returned to the initiator.   Any such sponsor acknowledgement is
subject to applicable regulations governing the content and form of
such acknowledgements.

The words "paid advertisement" should be prominently displayed in the
area containing the message if money has changed hands for the
transaction. If an organization uses the local newspaper model
simply to transmit community service messages, then the words "paid
advertisement" need not be displayed.

Auditing and Security

A remote printer server should maintain a log for auditing and
security. This log may contain at most the following information:

    1) the date the message was received;
    2) the "From" and "Message-ID" fields;
    3) the size of the body;
    4) the identity (telephone number) of the printer;
    5) any telephony-related information, such as call
       duration;
    6) any G3-related information, such recipient ID.

This information is the most that can be kept and may be further
limited by legal authority with jurisdiction at the site.

The purpose of the log is to maintain accountability and security.
It is considered a violation of the privacy of the initiator and the
recipient of the remote printer services to divulge such logs unless
required by legal authority with jurisdiction at the site. In
particular, it is a violation of privacy to divulge, either directly
or indirectly, such information for the compilation of lists for
marketing purposes.

It is permissible, however, to furnish interested parties with
summary reports that indicate the number of calls, average length,
and other summary information provided that such summary information
could not be used to identify individual initiators or recipients or
their calling patterns. For example, a remote printer gateway might
furnish an interested party with a report of the number of calls per
day and hours logged to a specific local area exchange.

Remote printer servers operate in a public service capacity and must strictly respect the privacy of the contents of messages. Unless required by technical or legal considerations, the content of messages shall not be monitored or disclosed.

Denial of Access

Internet sites registered in the tpc.int subdomain may deny access based on the source but not the destination of the message. If an Internet site feels that it is inappropriate to provide access to a particular destination, then it should re-register itself accordingly.

Denial of access based on source should be made only if required by legal authority with jurisdiction at the site or because of abuse. In all cases, denial of access should result in a notification returned to the initiator indicating the policy that was violated. However, if repeated attempts continue to be made by the source, repeated notifications are not necessary. Denial of access should be distinguished from the inability to provide access. For example, improperly formatted messages will prevent access.

Denial of access can occur due to problems in a single message or set of messages or because of consistent patterns of abuse. Examples of denial on a single message might include an attempt to transmit an extremely long document, such as a 100-page memo. Such a document might violate local policies limiting the number of pages or transmission time.

A more serious problem is long-term abuse of facilities. A remote printer server might choose to impose a usage limit on a daily or monthly basis. Such limits should be chosen to balance the desire to encourage legitimate users with the need to prevent consistent abuse.

At present, it is the responsibility for each Internet site running a remote printer server to define a local policy for denial of access. This policy should be based on objective criteria, and those criteria should be registered with the tpc.int subdomain secretariat at the e-mail address tpc-admin@town.hall.org.

Security Considerations

Security issues are not discussed in this memo.

References

   [1] Malamud, C., and M. Rose, "Principles of Operation for the
       TPC.INT Subdomain: Remote Printing -- Technical Procedures", RFC
       1528, Dover Beach Consulting, Inc., Internet Multicasting
       Service, October 1993.

   [2] Malamud, C., and M. Rose, "Principles of Operation for the
       TPC.INT Subdomain: General Principles and Policy", RFC 1530,
       Internet Multicasting Service, Dover Beach Consulting, Inc.,
       October 1993.

Authors' Addresses

   Carl Malamud
   Internet Multicasting Service
   Suite 1155, The National Press Building
   Washington, DC 20045
   US

   Phone: +1 202 628 2044
   Fax: +1 202 628 2042
   Email: carl@malamud.com

   Marshall T. Rose
   Dover Beach Consulting, Inc.
   420 Whisman Court
   Mountain View, CA 94043-2186
   US

   Phone: +1 415 968 1052
   Fax: +1 415 968 2510
   Email: mrose@dbc.mtview.ca.us