1509

Bell Laboratories Cover Sheet for Technical Memorandum

The information contained herein is for the use of employees of Bell Laboratories and is not for publication (see GEI 13.9-3)

Title: **Network Administrator Tasks for UNIX File Transfer Networks**

Date: **11 September 1979**

TM: **79-3624-7**

Other Keywords: **networking**
distributed systems
system maintenance
monitoring
security

Author(s)	Location	Extension
H. Che	**MH 7C-317**	**4346**
G. W. R. Luderer	**MH 7C-309**	**4220**

Charging Case: **49343-11**
Filing Case: **49343**
40125-002

ABSTRACT

UNIX™ installations now exchange programs and files with each other via a utility program called *uucp*. *Uucp* sometimes fails because the network is lacking administrative attention. Based on our experience with file transfer using *uucp* among UNIX systems, we strongly recommend establishing Network Administrators for maintaining and monitoring the various networks.

We distinguish Private Networks comprised of systems owned by an organization from the Public Network that interconnects some of the members of Private Networks with each other. The Public Network would take the place of the current BTL UNIX Support Group *uucp* network. The tasks that each Private Network Administrator and the one Public Network Administrator should do are defined in detail.

As an aid for this task, we provide a new UNIX command *uusub* for network maintenance and monitoring. It allows definition of a subnetwork for which traffic and connection statistics are collected during *uucp* operation, and it can be used to print these data as formatted reports. We give an example of an automatically invoked monitoring procedure that periodically reports traffic statistics and connection status for a subnetwork.

Pages Text: 5	Other: 4	Total: 9	
No. Figures: 0	No. Tables: 0	No. Refs.: 10	

Bell Laboratories

subject: **Network Administrator Tasks for UNIX File Transfer Networks**
Case: **49343-11**
File: **49343 40125-002**

date: **11 September 1979**

from: **H. Che**
MH 3624
7C-317 x4346

G. W. R. Luderer
MH 3624
7C-309 x4220

TM: **79-3624-7**

ABSTRACT

UNIX™ installations now exchange programs and files with each other via a utility program called *uucp*. *Uucp* sometimes fails because the network is lacking administrative attention. Based on our experience with file transfer using *uucp* among UNIX systems, we strongly recommend establishing Network Administrators for maintaining and monitoring the various networks.

We distinguish Private Networks comprised of systems owned by an organization from the Public Network that interconnects some of the members of Private Networks with each other. The Public Network would take the place of the current BTL UNIX Support Group *uucp* network. The tasks that each Private Network Administrator and the one Public Network Administrator should do are defined in detail.

As an aid for this task, we provide a new UNIX command *uusub* for network maintenance and monitoring. It allows definition of a subnetwork for which traffic and connection statistics are collected during *uucp* operation, and it can be used to print these data as formatted reports. We give an example of an automatically invoked monitoring procedure that periodically reports traffic statistics and connection status for a subnetwork.

MEMORANDUM FOR FILE

1. INTRODUCTION

Uucp is a heavily used software package that permits copying of files among UNIX* systems, using either dial-up or hard-wired communication lines [NOW1]. It is the backbone of software distribution (e.g. via the "Stockroom" [ROS]) and the remote mail facility.

However, *uucp* is a network operation. As is the case with any network, failures occur due to overloading or broken connections. In its current state, *uucp* suffers from low credibility with

* UNIX is a trademark of Bell Laboratories.

users, since a considerable number of requests never get completed. Our experience has been that *uucp* failures are rarely due to malfunctioning software. Rather, we found that most failures are caused by a lack of network maintenance. It is the purpose of this paper to define a maintenance task, called the Network Administrator Task.

Several commands have been provided to aid the network administrator. There is a new command, called *uusub*, which can be used to define, exercise, and monitor a subnetwork, i. e. a subset of systems in the network. This command is explained in the Appendix. The *uustat* command provides status of the *uucp* requests and the accessibility of machines on the network [CHE1]. The *uuname* command has been modified to make use of a newly created administrators' file giving the user access to an on-line directory of *uucp* system names [CHE2].

Our latest work is concerned with a more secure send-only version of *uucp*, called *uuto* [CHE3]. It is planned to be used in the USG Public Network which is to supersede the current *uucp* network of Department 3644.

References [LUD1] and [LUD2] explain how our efforts on *uucp* relate to the centralized common UNIX support work of Departments 3644 and 3646.

2. NETWORK ADMINISTRATION

If a reliable *uucp* network is desired, personnel must be assigned for monitoring and maintaining the network. Monitoring means regular periodic observation to detect broken connections and frequent overload situations. Maintenance means corrective action to repair connections and improve the facilities.

Reference [LUD2] establishes the notions of Private Network (PRN) and Public Network (PUN). A PRN consists of the UNIX systems that an installation wants to communicate with on a frequent basis. Typically included in a PRN are five to ten systems owned by a laboratory, a department, a project, or a computer center. We envision that these organizations will build their own private networks using the centrally supported *uucp* software. The following task definition for a Private Network Administrator (PRNA) is intended as a guideline for organizations to establish their own Private Network Administrator, since Department 3644 will not be responsible for the administration of these PRNs. Distinct from but connected to these private networks is the Public Network, which would take the place of the current *uucp* network used, e.g., by the Department 3644 Stockroom. This PUN should be considerably smaller than the union of all PRNs (which is approximately the size of the current USG network), since at most one or two systems of each PRN are expected to become members of the PUN. The PUN would use *uuto* instead of *uucp*, and its login file would be administered by Department 3644 who would designate a Public Network Administrator (PUNA) for this network. The PRNA task and the PUNA task are defined separately below.

2.1 The Private Network Administrator (PRNA) Task

Perhaps most important for the Network Administrator Task to be done well is the need to make the fact of the PRNA's existence and role known to the users on the Private Network. Users should know that someone cares about *uucp*, and they should feel compelled to report any trouble with this facility without hesitation to the PRNA.

Uucp software is distributed with UNIX/TS and UNIX/RT system software. The PRNA is responsible for installing *uucp*, establishing the connections, monitoring the Private Network, and exchanging information with the PUNA *. The responsibilities of the PRNA are elaborated in the following subsections.

2.1.1 Establishing the Private Network As a first step, the PRNA has to define which systems should belong to the PRN. Next, he or she chooses the connections, installs null modems for hard-wired links, automatic calling units (ACUs) for systems to dial out. Several data files have

* Frequently, the person doing the system generation could also do the installation and set-up of *uucp* and its network. For ongoing maintenance of the network, however, one does not need a person with as much system experience as the system generator.

to be provided for *uucp*. The configuration (hardware) information is maintained in a file called *L-devices*. Access privileges depending on the system calling in are stored in the file *USERFILE*. The file *SYSFILE* contains the login information for each member system of the PRN. Installation procedures are detailed in [NOW2].

2.1.2 Monitoring the Private Network To establish periodic monitoring, a shell procedure with the *uusub* command (see Appendix for detail) should be included for each member system of the PRN and be installed in *crontab*. This *cron* entry runs at an established time (e.g. 7:00 AM) and mails its output to a central system where the PRNA may find the reports every morning (see Attachment 1 for an example of the shell procedure and a sample report). The systems to be monitored are defined as a "subnetwork". For monitoring connection attempts and traffic between these systems, their names have to be added to the PRN using the *uusub* command with the '-a' option (see Appendix). The connection statistics and the subnetwork utilization are thus reported to the administrator. We think the Network Administrator should spend a few minutes each morning to look over the reports. Failures should get immediate attention. Overloads may need prolonged observation.

2.1.3 Maintenance of the Private Network Should any abnormal situation occur in the PRN, the PRNA would locate the problem and take corrective action, if possible. For instance, if login fails in a member system, the administrator should find out the possible change of the login id or password. If the the connection fails most of time because of lack of ACUs, then an additional ACU should be ordered. If the traffic between two machines is persistently heavy, then the PRNA should consider connecting them via a direct line or installing higher speed modems.

2.1.4 External Members of Private Networks In certain cases it may be desirable to have systems which belong to more than one PRN. The PRNAs of the PRNs involved should keep each other informed about any changes that may impact their connection. For example, one computer center PRNA may want to monitor the connection to the 'research' machine if the connection is vital to the function of the computer center.

2.1.5 Membership in Public Network PRNs may have one or more of their systems as members in the PUN. Indeed, an organization may not have a PRN but carry only membership in the PUN. Even in this case we assume the existence of a PRNA, whose job boils down to what is described below.

The PRNA is the contact person for the Public Network Administrator (PUNA, see below). It is the PRNA's first responsibility to inform the PUNA about any change in login access information of his PRN's member systems. In return, the PRNA will receive updated copies of the *SYSFILE* to install. This file is distinct from the PRN's *SYSFILE* mentioned above under 2.1.1. For systems which are members of the PUN and a PRN, the PRNA could merge the two *SYSFILEs*, if *uuto* is to be used for PRN and PUN. Additional system entries specific to this installation may be added; for example, there may be non-Bell-System installations. Furthermore, the PRNA should monitor the traffic between PRN systems and the members of the PUN. If he detects any connection failures, he has to report them to the PUNA (see below how this could be done). If there is substantial traffic between his system and some member systems, it seems appropriate to install an automatic monitoring procedure analogous to what has been said above under *Network Monitoring*, with the exception that *uuto* is used instead of *uucp*.

2.2 The Public Network Administration (PUNA) Task

For security reasons, the present Department 3644 (USG) *uucp* network, which comprises many of the Bell Labs UNIX systems, is likely to be converted soon to a send-only network using the new *uuto* command (see [CHE3], [LUD2]). It is envisioned that most PRNs will have at least one system (the program development system) as a member of this Public Network. There should be one Public Network Administrator (PUNA) in Department 3644 (who may be identical to 3644's PRNA) with responsibilities explained below.

The connectivity of the PUN determines, to a certain extent, the degree of security provided to its members. Consider a fully connected PUN, i.e. each member system can communicate with any other member. Admitting a new member to the network implies mutual security

agreements between each current member and the new member. Restricted connectivity, on the other hand, could be accomplished by letting each member system define and maintain its own special copy of the *SYSFILE*, thus restricting the systems it wants to communicate with.

As a policy for the PUN, we recommend full connectivity: members receive updated copies of the authoritative PUN copy of *SYSFILE* from the PUNA, and they commit to install this copy on their system. They may supplement this file with additional system entries but not reduce it. Membership in the PUN must be restricted to Bell System installations.

2.2.1 Establishing the Public Network The PUNA maintains a data base containing the login information (i.e. *SYSFILE*) and the PRNAs information (i.e. ADMIN file, see [CHE2]) of all PUN members. Since the *SYSFILE* contains some highly restricted information, the PUNA should take special caution when distributing it. The PUNA should send a letter to the management of each PUNA member installation informing about the security implications of PUN membership. The PUNA has also to inform all its members about any policy change (e.g., PUN is converted to the *uuto* command from the *uucp* command), new features or improvements, and bug fixes. We think that the Division 36 *Mini-System Newsletter* may be an appropriate place to advertise such information.

2.2.2 Maintaining the Public Network The main task of the PUNA is to keep the authoritative copy of the *SYSFILE* up-to-date, along with the administrators' file mentioned above. The UNIX system with these files thus holds a unique position in the PUN. Let us call it the "Central System". If the login information to access the Central System should change, the PUNA must notify all member systems' administrators.

A mode of operation must be found to maintain the PUN and minimize the burden on the Central System. We cannot imagine that, e.g., the Central System tries a test transmission of a file to each member system every night. It should be the responsibility of the member systems to exercise the connections they think are important to them. If they experience failures to login to another member system, they should report them to the PUNA as they have to report any change in the login access information of their own systems.

Finally, a way must be found to transmit updated copies of the *SYSFILE* securely from the Central System to all member systems. Transmission of the file in encrypted form is a possibility. The PUNA must initiate this mailing, whenever a change to the Central System's *SYSFILE* is made.

An appropriate way for reporting connection failure would be to establish a PUN trouble reporting system on the Central System, patterned after the USG trouble reporting system [MAR]. On connection failures which are suspect to changed login information, the PRNA of the system experiencing the failure should login to the Central System, say under a newly established loginid of *nwtrob*, and report that system A was unable to use *uuto* to system B. The PUNA has to periodically monitor the *nwtrob* file. In the example above,the PRNA should try to use *uuto* to system B. In case of success, system A probably has an out-of-date *SYSFILE* entry and should receive an up-to-date copy. If the Central System fails to reach system B, too, the PUNA should enter this fact into a "Broken Connections File" of *nwtrob*, e.g. with an entry like *System B found unaccessible since....* The PUNA may try to notify system B's administrator, who obviously failed to inform him.

2.2.3 Monitoring the Public Network As mentioned above, member systems should periodically exercise the connections to their more frequently accessed partners. The PUNA is primarily concerned with the monitoring of connections between the Central System and each member system in the PUN. This process could be automated following some algorithm. For example, there is little need to try out a connection that has recently been used successfully. An algorithm could cycle through the *SYSFILE* and call one system every night (rather than every system), skipping those systems that have been accessed by some *uuto* request during, say, the last seven days.

2.2.4 Auditing An optional extension of the PUNA task is the auditing of member systems' *SYSFILE*s. On a random sampling basis, the PUNA could check whether the *SYSFILE* of each member system is properly access-protected (readable only by the local *uucp* owner). Furthermore, periodic password changes could be required, and the changing of passwords could be monitored. However, none of these measures are currently performed, and it seems questionable whether the more secure send-only facility would really necessitate more stringent procedures.

2.3 Conclusion

Based on our experience with file transfer using *uucp* among UNIX systems, we strongly recommend to establish Network Administrators for maintenance and monitoring of the various networks. We distinguish Private Networks comprised of systems owned by an organization from the Public Network that interconnects some of the systems of Private Networks with each other. The latter would take the place of the current BTL *uucp* network. The tasks that each Private Network Administrator and the one Public Network Administrator have to do have been explained in some detail.

We realize that our view of the described tasks is only a starting point. As the network administrators carry on with their jobs, better understanding will hopefully evolve, and the tasks may change. It is important, however, that a beginning be made and supervision appoint personnel to perform these functions, if it is felt necessary to have smoothly working file transfer operations. We hope that this paper has made it easier to get this job done.

H. Che

G. W. R. Luderer

MH-3624-HDC/GWRL-rjf

Atts.
APPENDIX: THE UUSUB COMMAND
Attachment 1: Sample Shell Procedure and Report
Attachment 2: Manual Page for the *uusub* Command

References

REFERENCES

[CHE1] Che, H., "Uustat - A UUCP Status Inquiry Program", 3624-791031.01MF, October 31, 1979.

[CHE2] Che, H., "UUCP Administrators' File and the UUNAME Command", 3624-791031.01PN, October 31, 1979.

[CHE3] Che, H., "A Send-Only UUCP Facility", 3624-791031.02MF, October 31, 1979.

[FRA] Fraser, A. G., "Datakit - A Modular Approach to Data Networks", TM 75-1273-9, September 10, 1975.

[LUD1] Luderer, G. W. R., "Department 3624's Workplan for Networking in 1979/80", 3624-790716.01MF, July 11, 1979.

[LUD2] Luderer, G. W. R., "Work Related to UNIX-to-UNIX File Transfer (UUCP) in Department 3624 - Retrospective and Outlook", TM 79-3624-8, 31 October 1979.

[MAR] Maranzano, J. F., "Trouble Reporting System for UNIX", September 24, 1974

[NOW1] Nowitz, D. A., Lesk, M. E., "A Dial-Up Network of UNIX Systems", TM 79-3782-2, June 1, 1979.

[NOW2] Nowitz, D. A., "Uucp - UNIX to UNIX copy Implementation Description", TM 78-1273-5, August 7, 1978.

[ROS] Rosenthal, V. H., "The USG UNIX Stockroom", 2524-790423.01MF, April 23, 1979.

APPENDIX: THE UUSUB COMMAND

This appendix describes the program provided to aid in the administrator task for a *uucp* subnetwork (PRN). The main facility is a new command called *uusub* which adds or deletes systems to the subnetwork being monitored. It also provides statistics on the connection status and the amount of traffic. *Uusub* works with two files: (1) the "L_sub" file that contains the connection status, and (2) the "R_sub" file that contains the traffic statistics. Before describing the syntax of the *uusub* command, we will discuss the structure of these two files.

The entry in the "L_sub" file is:

```
struct ub_l {
        char    sys[10];        /* system name */
        short   call;           /* # of calls made */
        short   ok;             /* # of successful connections */
        short   noacu;          /* # of times when ACU busy */
        short   login;          /* # of times LOGIN fails */
        short   nack;           /* # of times without answer */
};
```

When a new system is added to the subnetwork, an entry is created in the "L_sub" file with the proper system name. All other fields are initialized to zero. When a connection is attempted by the *uucp* daemon, the status is recorded in the corresponding record. All the status fields in the file "L_sub" can be reset by the *uusub* command as described below.

The entry in the "R_sub" file is:

```
struct ub_r {
        char    sys[10];        /* system name */
        short   sf;             /* # of files sent */
        long    sb;             /* # of bytes sent */
        short   rf;             /* # of files received */
        long    rb;             /* # of bytes received */
};
```

The syntax of the *uusub* command is:

uusub [options]

The options are:

−a*sys*	Add *sys* to the file "L_sub".
−d*sys*	Delete *sys* from the file "L_sub".
−r	Print the file "R_sub".
−l	Print the file "L_sub".
−f	Flush the "L_sub" file.
−c*sys*	Call system *sys*. If *sys* is specified as **all**, then exercise the call to all the systems in the subnetwork.
−u*hour*	Update the "R_sub" file by gathering the traffic statistics over the past *hour* hours.

The *uusub* command should be protected, e.g., it can only be initiated by the user "uucp" or the superuser. Note that the *uucp* daemons (*uucico*) have recorded all file transfer transactions in a log file called "SYSLOG". *Uusub* with the −u option scans this log file and prepares a statistical report. See the following attachments for how to use the *uusub* command.

ATTACHMENT 1: A Sample Shell Procedure and Report

For periodic monitoring of the subnetwork defined in *L_sub*, an entry can be set up in the system's file for periodically executed procedures, *crontab*, (see *cron(1M)* in UNIX Programmer's Manual):

```
1 7 * * * su uucp -c "/usr/lib/uucp/uudemon.day"
```

This line will be executed every morning at 7:01 AM. The invoked *shell* procedure *uudemon.day* contains the following commands:

```
: 'perform once per day at 0701 hours'
cd /usr/lib/uucp
uuclean -p -m -n168 > /dev/null 2> /dev/null
uuclean -d.XQTDIR -p -n72 > /dev/null 2> /dev/null
uustat -c168 > /dev/null 2> /dev/null
uusub -call -u24
uusub -l -r > daily_report
uusub -f
cd /usr/spool/uucp
mv LOGFILE temp
uniq -c temp >> Log-WEEK
rm temp
```

To get the daily report produced by the above procedure, the PRNA could invoke

```
pr /usr/lib/uucp/daily_report
```

The following report is obtained from the Department 3644 PRN, monitored by the system *mhtsa* over a period of five days. The subnetwork is defined in *L_sub* as containing four systems.

sysname	sfile	sbyte	rfile	rbyte
mhtsb	16	32295	2	12311
mhrtc	0	0	1	242
mhtse	6	111237	0	0
minimou	7	167039	2	188

sysname	#call	#ok	latest-oktime	#noacu	#login	#nack	#other
mhtsb	79	72	(11/26-15:35)	0	4	3	0
mhrtc	34	21	(11/26-8:10)	0	2	11	0
mhtse	10	0	(11/2-13:59)	0	0	0	10
minimou	145	109	(11/26-16:51)	0	20	16	0

The report comes in two parts. The first part reports for each system the number of files sent *(sfile)* and bytes sent *(sbyte)*, and the number of files received and bytes received, respectively *(rfile, rbyte)*. The second part of the report gives connection statistics for each system in the subnetwork. The exact meaning of the data is explained in the attached manual page for the *uusub* command. The last line of the report shows that of the 145 calls made to system *minimou*, 109 succeeded, with 20 failures being attributable to login changes and 16 to no answer from remote hardware. The last successful access was on 11/26 at 16:51.

NAME

uusub − monitor uucp network

SYNOPSIS

uusub [options]

DESCRIPTION

Uusub defines a uucp subnetwork and monitors the connection and traffic among the members of the subnetwork. The following options are available:

- **−a***sys* Add *sys* to the subnetwork.
- **−d***sys* Delete *sys* from the subnetwork.
- **−l** Report the statistics on connections.
- **−r** Report the statistics on traffic amount.
- **−f** Flush the connection statistics.
- **−u***hr* Gather the traffic statistics over the past *hr* hours.
- **−c***sys* Exercise the connection to the system *sys*. If *sys* is specified as **all**, then exercise the connection to all the systems in the subnetwork.

The meanings of the connections report are:

sys #call #ok time #dev #login #nack #other

where *sys* is the remote system name, *#call* is the number of times the local system tries to call *sys* since the last flush was done, *#ok* is the number of successful connections, *time* is the the latest successful connect time, *#dev* is the number of unsuccessful connections because of no available device (e.g. ACU), *#login* is the number of unsuccessful connections because of login failure, *#nack* is the number of unsuccessful connections because of no response (e.g. line busy, system down), and *#other* is the number of unsuccessful connections because of other reasons.

the meanings of the traffic statistics are:

sfile sbyte rfile rbyte

where sfile is the number of files sent and sbyte is the number of bytes sent over the period of time indicated in the latest *uusub* command with the **−u***hr* option. Similarly, *rfile* and *rbyte* are the numbers of files and bytes received.

The command

uusub −call −u24

is typically started by *cron*(1M) once a day.

FILES

/usr/spool/uucp/SYSLOG system log file
/usr/lib/uucp/L_sub connection statistics
/usr/lib/uucp/R_sub traffic statistics

SEE ALSO

uucp(1C), uustat(1C)