EBS OPERATIONAL RECOMMENDATIONS

Tony Bates

University of London Computer Centre

ABSTRACT

This paper defines a set of operational recommendations for an Ebone Boundary System (EBS) and the responsibilities of an EBS operating site. This is based on discussions within the Ebone Operations Team (EOT). This should act as guide when adding any new EBS sites.

February 1, 1993

EBS OPERATIONAL RECOMMENDATIONS

Tony Bates

University of London Computer Centre

1. INTRODUCTION

This short† paper lists some operational recommendations for an EBS in its configuration and operation. This paper is meant to be used as a basic guide when configuring your EBS. It follows discussions within the EOT regarding a collaborative operational approach to the management of the Ebone backbone. Refer to separate papers for a detailed description of the routing implementation used [1],[2] and the overall management model of Ebone [3].

2. ACCESS TO THE EBS

By ‘‘access to the EBS’’ I mean access for operational and administrative purposes. Currently all the EBSs in use are based on cisco routers††. These routers support two methods of access for management and operation, an interactive terminal (telnet) interface and an SNMP interface. The next two sub-sections describe the way these methods should be used and configured in the EBSs.

2.1. TELNET ACCESS

The routers support multiple telnet sessions and have the ability to run an authentication service known as TACACS†††. TACACS is a client/server based protocol that allows the router to interact with several servers holding account information for users of the router. It works on the basis of the normal Unix password file scheme with the advantage that you can hold the password file on several servers for backup. It is recommended that all the EBSs run TACACS. This gives extra functionality when looking at operational aspects of the router. You can actually see who did what and at what time by use of TACACS logging information.

- **Recommendation 1 — Each EBS must run TACACS.**

The higher level *enable* password will only be known by the EBS operator and the Ebone NOC.

2.1.1. TACACS SCHEME

With all the EBSs running TACACS it should be possible to create a flexible and resilient scheme for making sure that access to the EBS is possible at all time. It is recommended that each EBS site run at least one TACACS server locally to them.

- **Recommendation 2 — Each EBS site must run at least one TACACS server locally.**

With local servers in place each EBS can then use the other EBS site’s TACACS server as backup in case of failure. By use of a simple update procedure it should be possible to all the

† Short being the operative word. ;-)

†† cisco AGS+ routers — See [4] for more details.

††† TACACS code available from **ftp.cisco.com** as **xtacacsd.shar**.

TACACS password files at the EBS sites consistent. A mechanism for this is left for later discussion.

To make it easier for an EBS site an example of a possible TACACS configuration is given.

The text in **bold type** represents the areas of possible change in your local EBS configuration.

```
!
! TACACS commands needed
!
enable last-resort password
tacacs-server host 128.86.1.20
tacacs-server timeout 10
tacacs-server extended
tacacs-server authenticate connections
tacacs-server notify connections
!
```

2.1.2. DISTRIBUTED TACACS PASSWORD SCHEME

When operating and managing several routers in such a collaborative way the consistency of the password database is very important. Eventually an automated scheme for the update mechanism should be available to take care of this. In the interim it is recommended that all EBS operators update their EBS TACACS password by making use of the Ebone NOC mahine **tftp.ebone.net**. Each local TACACS machine could then rcp or NFS mount the TACACS password file.

- **Recommendation 3 — Keep TACACS password file consistent with** *tftp.ebone.net***.**

2.2. SNMP ACCESS TO THE EBS

The cisco router has a very large suite of ‘‘private enterprise’’ variables as well as the standard MIBII set which are very useful in terms and management and statistics. It has been agreed that all EBS operating sites should have SNMP access to all the EBSs. This would be done by having an ‘‘access-list’’ for a selected ‘‘read-only’’ (RO) community string. The obvious string appears to be **public**.

The access-list should have an entry for any requested host address that an EBS operator uses for SNMP management.

- **Recommendation 4 — Each EBS site must run an access-list controlled** *public* **RO community.**

2.3. STATISTICS GATHERING

Each EBS site must collect statistics for its local EBS. It is recommended that the data is stored according to the current IETF OPSTAT recommendation [6]. The statistics must be made publicly available so that the NOC can then analyse and present the statistics. As soon as there exists a publicly available statistics collection package using the OPSTAT format each EBS should run this. Until then however, **ad-hoc** packages should be used.

For complete traffic information *ip accounting* should be run on the EBSs. However, until we have CSC/4 processors in the EBSs this will not be implemented.

- **Recommendation 5 — SNMP statistics should be stored in IETF OPSTAT format.**
- **Recommendation 6 — Each EBS should run** *ip accounting* **as soon as CSC/4 processors are fitted.**

3. TROUBLE TICKETS

For a well run and well maintained network, a ‘‘Trouble Ticket’’ system is essential. Currently, there appears to be a lack of a good generic trouble ticket system available†. However, several EBS sites have already adopted there own somewhat **ad-hoc** systems. This is not a problem providing they conform to the same standard presentation format as described in the RIPE recommendation on operational contacts [5]. All ticket information should be archived and made available to the Ebone NOC for reference.

- **Recommendation 7 — Each EBS site must issue tickets in the RIPE recommended format. They should be made available via a local archive.**

A **trouble-ticket research group** has been set up within the EOT to review this matter in more depth.

4. OUT-OF-BAND ACCESS

Each EBS must provide some form of out-of-based access to the EBS or EBSs at there site. This should direct access to the console port of the EBS. This information should be made available to the Ebone NOC.

- **Recommendation 8 — Each EBS site must provide out-of-band access to the EBS.**

5. EBS LOGGING

All EBS logging information should be written to a local file using syslog. It is recommended that the logging level is set to **debug**.

- **Recommendation 9 — Each EBS must log router messages to a local syslog server.**

The text in **`bold type`** represents the areas of possible change in your local cisco configuration followed by your local syslog configuration.

```
!
! Local syslogger
logging 128.86.1.20
logging monitor debugging
!

#
# Write all cisco logging messages to file
#
local7.debugging                         /usr/adm/cisco/log
#
```

† The ones that are available, currently rely too much on a proprietary RDMS.

6. OPERATIONAL MAILING LISTS

All EBS operators should be on the EOT list **eot@ebone.net**. This list should be used whenever discussing generalised Ebone operational issues. For reaching the EBS operators at the local EBS site it is recommended that the local EBS site maintain a mailing of the relevant EBS operators. It is recommended that this list is known as ‘‘**ebs-ops@EBS.site**’’. This information can then further be distributed by the EBS if required.

- **Recommendation 10 — Each EBS site must support a local mail fan-out of** *ebs-ops@EBS.site*

For an outage that will effect more than just the Ebone core it is recommended that the RIPE provided mailing list **ripe-op@ripe.net** be used.

7. MAINTENANCE WINDOWS

It has been decided that a ‘‘maintenance window’’ be created whereby essential engineering and configuration can take place at a local EBS site. This should be done in such a way as not to clash with any other EBSs window. The table below shows the current Ebone Maintenance windows. All times are in UTC.

EBS Site	Warning Deadline	Maintenance Window
ULCC	Friday	Tuesday 07:00 - 09:00
CERN	Monday	Wednesday 16:00 - 18:00
CNUSC	Friday	Tuesday 04:00 - 06:00
SARA	Thursday	Monday 16:00 - 20:00
KTH	Tuesday	Thursday 18:00 - 20:00

The **warning deadline** means noon of the day quoted which is at least one full working day before the maintenance day when notice should be given of any outage at a particular EBS. It is recommended that any outage outside of these time is restricted only to extremely critical problems that cannot be resolved inside the maintenance window.

- **Recommendation 11 — Each EBS site must publish it's maintenance window and announce any changes before the warning deadline.**

8. REFERENCES

[1] T. Bates, P. Lothberg, "Ebone-92 IP routing model", June 1992.

[2] J. Heinanen, "Ebone CLNS routing model", September 1992.

[3] B. Stockman, "Mangement and Operations of the EBONE", April 1992.

[4] B. Stockman, "EBONE Boundary System Technical Specification", April 1992.

[5] D. Karrenberg, "RIPE Recommendation on Operational Contacts", April 1992.

[6] B. Stockman, "A Model for Common Operational Statistics", March 1992. RFC 1404.