RIPE Recommendation on IP Router Management

Version 3.1

ref.: ripe-37

D.Karrenberg

Purpose

RIPE is a cooperative effort among its members with no central funding. There is no centrally managed RIPE backbone with operations staff running responsible for connectivity. Thus operational problems have to be solved in a distributed manner. For this to work network configuration information, network status information and operational contact information must be available to operations staff of all RIPE members. With this information operations staff of a RIPE member can pinpoint the causes of a problem and contact the appropriate operations staff of another member quickly. Without this information, locating problems would either take people and time or be impossible.

The purpose of this recommendation is to give guidance to the RIPE member organizations on how to manage their IP routers in a way that provides a maximum of necessary information to other RIPE members while maintaining full operational authority over their own routers. This recommendation should be followed for all routers on links between RIPE member organizations. Most of the recommendations should also be applied to internal routers.

Router Access

All RIPE IP routers should be accessible using telnet from any other RIPE router; there should not be any restrictions, of any kind, between two routers. The non-privileged password should be well known and should be given to any RIPE operational staff asking for it. Router operators should consider to set up access-lists in order to avoid unallowed connections from the router. It should however always be possible to connect from a RIPE router to another one.

All RIPE router should be fully registered in the Domain Name system. When possible, all interfaces are registered under the same domain name.

TELNET Access

Most routers can be accessed by TELNET. Most of them are also capable of displaying a banner message before any authorization of the calling user is performed. This banner message should be used to verify which router has been reached and to provide a quick means to contact the responsible operational people.

Example:

```
amsterdam.NL.EU.net [1.55 90/08/21]

Problems: ip-oper@cwi.nl, phone +31 20 5924112

Authorized access only !!!


User Access Verification

Password:
```

The message should contain at least the following information:

- fully qualified domain name of the router
- e-mail address of operational staff responsible
- telephone numbers to reach operational staff in international format

Other useful information includes:

- version numbers of configuration information and the date/time of last change

Routers should support as many parallel TELNET sessions as practical but at least two. It is recommended that inactive TELNET sessions be timed out after 10 minutes.

ICMP Echo Service

All routers should support unrestricted ICMP Echo service to all networks they route to and from.

TCP Echo and Discard Service

These TCP services can be useful in determining performance and finding subtle networking problems. They should be supported. However these services should be used with care since they can generate network and router overload. In any case the link and router managers concerned should be asked for permission before any extensive testing is conducted.

SNMP Read Access

Routers should support SNMP read only access using an agreed community for operational diagnostics. This facilitates spotting all sorts of network errors especially those caused by routing problems. There can be different communities for other purposes.