Network Working Group
Request for Comments: 1262

Internet Activities Board
Vinton G. Cerf/CNRI, Editor

October 1991

Guidelines for Internet Measurement Activities

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.

Summary

Measurement of the Internet is critical for future development, evolution and deployment planning. Internet-wide activities have the potential to interfere with normal operation and must be planned with care and made widely known beforehand. This document offers guidance to researchers planning Internet measurements.

This RFC represents IAB guidance for researchers considering measurement experiments on the Internet. This RFC does not represent a standard for the Internet but the Internet Activities Board strongly urges that Internet users follow the guidelines out of courtesy and professional consideration for the Internet community.

Guidelines

The Internet has undergone dramatic growth in connectivity, use, and quality of service over the past several years. As this growth continues and the Internet is used for increasingly diverse and demanding purposes, it is vital to collect data about a range of functions, from low-level packet switching services to considerations for the networking expectations of individual applications. Such data is vital to research and engineering planning activities, as well as to ensure the continued development of the operational infrastructure. Yet, it is also important that data collection activities do not interfere with the operational viability and stability of the network, and do not violate considerations regarding privacy, security, and acceptable use policies of the network. In this light, the Internet Activities Board offers the following basic guidelines for network measurement activities.

In general, any data collection activity should be undertaken with professional consideration of its impact on the services and users of the network, and activities should be planned to achieve operational

or research goals with minimal impact. In some cases, data may be collected continuously, for example to measure packet counts or the distribution of use of specific applications. In other cases, the planned investigations will be too demanding to be undertaken continuously, because of the intensity of effort required by the researcher or the traffic load on the underlying network infrastructure. Any data collection activity should be designed with careful consideration of this type of issue, and should be tested thoroughly before being deployed on the Internet. Any individual initiating a network measurement activity should alert the relevant service providers using mechanisms such as bulletin boards, mailing lists and individual mail communications.

Furthermore, the data being collected must not be gathered using break-ins to network systems or other illegal or unethical techniques. If a measurement activity might be construed as a possible security intrusion, the researcher should make it easy for a system administrator at a remote site to determine that the activity is not a break in attempt, by informing the CERT, making information about the study easily available by anonymous FTP or other means [1,2,3].

More specifically, an individual attempting a network measurement activity should ensure that the following conditions are met:

1) the data collected will not violate privacy, security, or acceptable use concerns,

2) if the aggregated data has a potential for privacy intrusions, the researcher must protect privacy, for example by limiting published statistics in such a fashion that individual users or institutions are not identified,

3) if the data collection activity may be construed to be a security violation, the researchers are strongly advised to inform the CERT in advance, and, if applicable, request some guidance,

4) the data collection does not unduly load or otherwise interfere with the network or attached machines, in particular, if at all feasible, non-invasive measurement, like passive monitoring, should be considered as the first choice,

5) if there is an operational impact, the service providers must be contacted,

6) the study goals, methodology, and plans are widely available, in a fashion that requires minimal effort to locate and retrieve,

and

7) if the activity would impose undue burden on a remote machine or network, the measurements should not be performed without prior explicit permission.

References

[1] Internet Activities Board, "Ethics and the Internet", RFC-1087, January 1989.

[2] Holbrook, P., and J. Reynolds, (Eds.), "Site Security Handbook", RFC-1244, FYI-8, CICnet and USC Information Sciences Institute, July 1991.

[3] Computer Emergency Response Team/Coordination Center (CERT/CC), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, Internet E-mail: cert@cert.sei.cmu.edu, Telephone: 412-268-7090 24-hour hotline.

Security Considerations

The body of this memo does discuss security issues related to network measurement, particularly the potential confusion of benign measurement with hostile security attacks.

Author's Address

Vinton G. Cerf
Chair of the IAB
Corporation for National Research Initiatives
1895 Preston White Drive, Suite 100
Reston, VA 22091

1-703-620-8990

VCerf@NRI.RESTON.VA.US