# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



**PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 01-Jul-2004 | Quarterly | Apr 2002 - Jun 2002 |

**4. TITLE AND SUBTITLE**

Macroscopic Internet Data Collection and Analysis in Support of the NMS Community:

Progress Status and Management Report
for the period Apr 2002 - Jun 2002

**5a. CONTRACT NUMBER**
AO: L018/00

**5b. GRANT NUMBER**
N66001-01-1-8909

**5c. PROGRAM ELEMENT NUMBER**
0602301E

**6. AUTHOR(S)**

Dr. K. C. Claffy

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**
DI-MGMT-80227

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Cooperative Association for Internet Data Analysis (CAIDA)
University of California, San Diego (UCSD)
9500 Gilman Drive MS-0934
La Jolla, CA 92093-0934

**8. PERFORMING ORGANIZATION REPORT NUMBER**
CAIDA-NMS-05-Qtr#4

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

SPAWARSYSCEN SAN DIEGO
CODE D212
BLDG A33 ROOM 1602W
53560 HULL STREET
SAN DIEGO CA 92152-5001

**10. SPONSOR/MONITOR'S ACRONYM(S)**
DARPA

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION/AVAILABILITY STATEMENT**

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

This UCSD/CAIDA project focuses on advancing the capacity to monitor, depict, and predict traffic behavior on current and advanced networks, through developing and deploying tools to better engineer and operate networks and to identify traffic anomalies in real time. CAIDA will concentrate efforts in the development of tools to automate the discovery and visualization of Internet topology and peering relationships, monitor and analyze Internet traffic behavior on high speed links, detect and control resource use (security), and provide for storage and analysis of data collected in aforementioned efforts.

**15. SUBJECT TERMS**

network monitoring, network topology, network performance, network workload characterization, routing, CoralReef, skitter, OC48, Gigabit Ethernet, Domain Name Service (DNS), AS, Denial-of-Service, Code Red, Nimda

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | K.C. Claffy, Ph.D. |
| U | U | U | UU | 10 | 19b. TELEPHONE NUMBER *(Include area code)* (858)534-8333 |

**NMS Project Quarterly Report #Qtr4: 1-Apr-02 through 30-Jun-02**

SUBMITTED TO Receiving Officer
SPAWARSYSCEN - SAN DIEGO
e-mail address: nms@spawar.navy.mil

Nikhil Dave and Steve Fujii
Technical Representatives {nik, fujii}@spawar.navy.mil

Tiffany Townsend
Contract Specialist, Code 2211
SPAWARSYSCEN SAN DIEGO CONTRACTS D212
PHONE 619-553-5472
FAX 619-553-4464
tiffany.townsend@spawar.navy.mil

SUBMITTED BY
University of California, San Diego (UCSD)
9500 Gilman Drive
La Jolla, CA 92093-0505

Principal Investigator
Dr. Kimberly Claffy
PHONE 858-534-8333
FAX 858-822-0861
kc@caida.org

Contract/Financial Contact
Pamela J. Alexander
PHONE 858-534-0240
FAX 858-534-0280
pjalexander@ucsd.edu

**Quarterly Status Report #Qtr4**

# Macroscopic Internet Data Collection and Analysis in Support of the NMS Community

## 1.0 Purpose of Report

This status report is the quarterly cooperative agreement report that summarizes the effort expended by the UCSD's Cooperative Association for Internet Data Analysis (CAIDA)

program in support of SPAWARSYSCEN-SAN DIEGO and DARPA on Agreement N66001-01-1-8909 during April - June 2002.

**2.0 Project Members**

UCSD hours:
PI: 86.00
CAIDA Senior Staff: 980.40
CAIDA Staff: 1,716.73
Total Hours: **2,783.13**

**3.0 Project Description**

This UCSD/CAIDA project focuses on advancing the capacity to monitor, depict, and predict traffic behavior on current and advanced networks, through developing and deploying tools to better engineer and operate networks and to identify traffic anomalies in real time. CAIDA will concentrate efforts in the development of tools to automate the discovery and visualization of Internet topology and peering relationships, monitor and analyze Internet traffic behavior on high speed links, detect and control resource use (security), and provide for storage and analysis of data collected in aforementioned efforts.

**4.0 Performance Against Plan**

(Please note: Changes since the last reporting period are in boldface type, and links have been updated with new content.)

| **Status** | **Task 1 Year 2 Milestones:** | **Notes** |
|---|---|---|
| Complete | Add 5 additional skitter source sites | **Done** |
| Progress | Add 5 workload monitor sites | Added web page for accessing NeTraMet measurements |
| Complete | Develop comprehensive website(s) for public availability of data | • root/gTLD DNS performance plots<br>• skitter daily summaries<br>• NMS project progress<br>• CoralReef analysis of SDNAP |

| **Status** | **Task 2 Year 2 Milestones:** | **Notes** |
|---|---|---|
| Begun | Establish archive and interactive database for community access to skitter, mantra, routing, and | • research community collaborators<br>• skitter daily summaries |

| | | |
|---|---|---|
| | CoralReef data. | • Real-time workload characterization of SDNAP |
| Ongoing | Solicit community feedback regarding needed data types, formats, and dataset sizes. | **Discussions occurred at ARIN IX, as well as meetings and conference calls with Lucent, BCIT and Jaalam.** |
| Ongoing | Work with the NMS community to design common experiments | **Kc claffy met with NMS Pis George Riley and Robert Nowak. Ken Keys refined crl_delay for Nikhil Dave, and corresponded with Ron Nolte.** |

## 5.0 Major Accomplishments and Results to Date

### Task 1. Monitoring Task

### A. Topology Measurement Using Active Probes

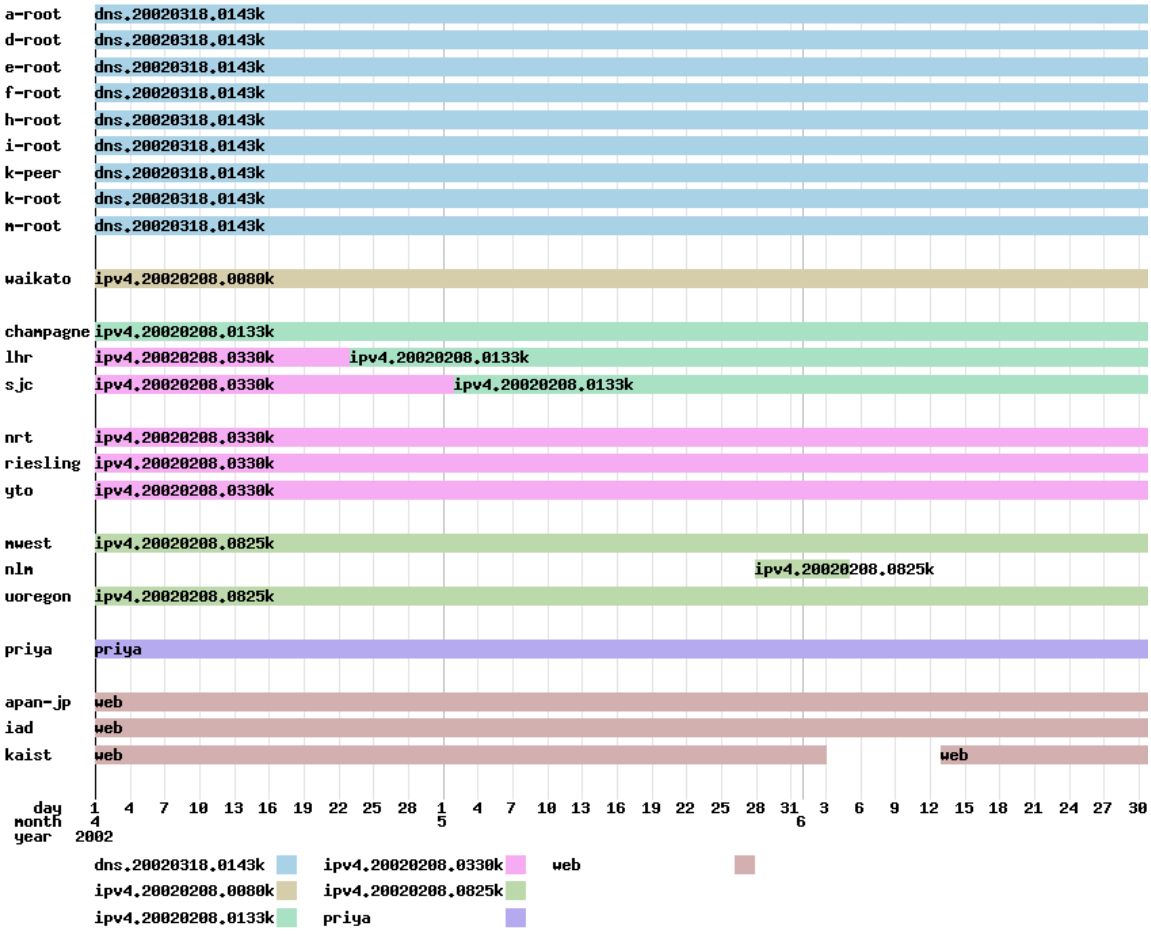
Approach

skitter is a CAIDA tool that measures both the forward path and round trip time (RTT) to a set of destination hosts by sending probe packets through the network. It does not require any configuration or cooperation from the remote sites on its target list. In order to reveal global IP topology, CAIDA's Macroscopic Topology Measurement and Mapping project builds software and infrastructure to:

- Collect forward path (layer 3) and RTT data
- Acquire infrastructure-wide global connectivity information
- Analyze the visibility and frequency of IP routing changes
- Visualize network-wide IP connectivity

An essential design goal of skitter is to execute its pervasive measurement while placing minimal load on the infrastructure and upon final destination hosts. To achieve this goal, skitter packets are small (52 bytes in length), and we restrict the frequency of probing to 1 packet every 2 minutes per destination and 300 packets per second to all destinations. To improve the accuracy of its round trip time calculations, CAIDA added a kernel module to the FreeBSD operating system platform used by its skitter monitors. Kernel timestamping does not solve the synchronization issue required for one-way measurements, but reduces variance caused by multitasking processing when taking round trip measurements. This feature helps to capture performance variations across the infrastructure more effectively. By comparing data from various sources, we can identify points of congestion and performance degradation or areas for potential improvements in the infrastructure.

*skitter* Monitor Status as of 30-Jun-02 (23 monitors active):




**Topology Analysis Results:**

**New Tools:** A new version of the Walrus 3D hyperbolic viewer was also released.

Walrus 0.6

CAIDA released Walrus 0.4, 0.5 and 0.6. This new version does layout calculations with extended precision (about 30 decimal digits instead of the 15 digits provided by the 64-bit 'double' type). CAIDA researcher Young Hyun notes that Walrus can selectively use extended precision in order to avoid the graphing performance hit. However, using extended precision doesn't always produce satisfactory layouts because there can still be artifacts of numerical instability leading up to the problematic nodes.

The latest version is 0.6, released on Apr 29, 2002:

- Added support for zooming the display. The user can zoom in toward the central node or zoom out from it to an arbitrary degree.
- Added support for turning depth cueing off.
- Fixed bug in which picking would sometimes become temporarily inaccurate after the window is resized.
- Fixed bug in which the display would lock up if the user executed a command through the keyboard while concurrently interacting with the mouse.

**B. Workload / Performance Measurement Using Passive Monitors**

OC48 traces can be captured from the Metromedia Fiber Network (MFN) backbone in San Jose, CA. No traces were collected during this reporting period (nor were there Any NMS PI requests for such traces.)

CoralReef crl_delay application:

CoralReef developer Ken Keys worked with Dr. Nikhil Dave (SPAWAR) to refine the crl_delay application for use in the RealBits Lab at SPAWAR. Ken also corresponded with SAIC contractor Ron Nolte concerning specifications for a new CoralReef application to simultaneously collect one-way delay data from two different interfaces.

NeTraMet Software Development:

CAIDA machine netramet.caida.org is configured to continuously record DNS response times. In order to make these measurements available to the NMS community, a daily cron job generates strip charts from collected measurements. In addition, CAIDA maintains a web page form allowing researchers to access graphs of root and gTLD DNS server performance measurements since January 2002.

**C. Routing Measurement**

CAIDA staff began to build a new 'core' exchange point graph using skitter data in conjunction with http://www.pch.net/documents/data/exchange-points/ep-in-addrs.txt . The most important question under investigation is: What percentage of exchange points does skitter see? Our current approach involves finding all intermediate nodes as well as destinations that go through all exchange points on the PCH list.

**Task 2, Archiving and Storage Task**

Approach for Archiving skitter Data and Making Data Available to Researchers
The following table represents current users of skitter data.

| **Requestor** | **Organization** | **Project** |
|---|---|---|
| Eoin Lawless | Trinity College Dublin | Large network |

| | | |
|---|---|---|
| | | simulation |
| Aditya Akella | Carnegie Mellon U | Characterize peering points |
| Other collaborative projects at: http://www.caida.org/projects/nms/reports/skitter_comuse.xml | | |
| Previous collaborative projects at: http://www.caida.org/projects/nms/reports/prev_skitter_comuse.xml | | |
| PhD students using skitter data | | 2 |
| Master's students using skitter data | | 0 |
| About publicly available skitter data: http://www.caida.org/cgi-bin/skitter_summary/main.pl | | |

***Approach for Archiving CoralReef Data***

1. CAIDA added a new SDNAP report generator to work with new network environment configuration: http://www.caida.org/dynamic/analysis/workload/sdnap/0_0_/. A "monitor" often includes multiple taps (e.g., one inbound and one outbound); each of these tap interfaces can in turn contain multiple subinterfaces (e.g., VLANs, or ATM VPVCs). In the case of the SDNAP page, there's only one tap interface, with only one subinterface; it's labelled "0[0]". The main SDNAP report now contains a link to the newly repaired "0[0]" page that gives more detail on that subinterface.
2. CAIDA provides a demonstration of CoralReef data collection, analysis, and reporting at: http://www.caida.org/dynamic/analysis/workload/sdnap/. Results are updated every 5 minutes.
3. CAIDA archives CoralReef data for special purpose studies as needed, but must limit data collection to available disk space.

**6.0 Artifacts Developed During the Past Quarter**

None

**7.0 Issues**

We have been operating at a significant deficit based on notification of Year 2 funds. We received $352,875 in April and a $150,000 conadd in June. However, we did not receive funds for Year 2 Task 1, and are unable to complete Task 2 or the proposed conadd work without Task 1. Discussions with SPAWAR and DARPA are underway to resolve these issues.

**8.0 Near-term Plan**

The following work is planned for 01-Jul-02 through 30-Sep-02:

**General/Administrative Outreach and Reporting Plans**

- Submit Quarterly Report to SPAWAR covering progress, status and management.

**Task 1. Monitoring Task Plans**

- **A. Topology Measurement**

CAIDA will continue to collect and analyze data for its macroscopic topology project.

- **B. Workload Measurement**

  - CAIDA will continue to analyze traces gathered from OC48 links at Metromedia Fiber Network (MFN) in San Jose. We are trying to find other locations for OC48 traffic taps, but need additional funding for that.

  - Refinement of the CoralReef software suite will continue, (http://www.caida.org/tools/measurement/coralreef/ )

- **C. Routing Measurement**

CAIDA will continue to refine methodology and results from ongoing routing studies.

**Task 2, Archiving and Storage Task Plans**

- We will continue to collect and analyze data collected from skitter sources deployed in the field

- We will continue to make skitter topology and performance data available to researchers via password authentication for use in research and modeling: See: http://www.caida.org/projects/nms/reports/skitter_comuse.xml

- We will continue briefings to the Internet community on the purpose and results of skitter active monitoring and will solicit their feedback.

- We will refine the collection and archiving of skitter data

- We will make additional improvements to the Walrus viewer (partially funded by this project). See: http://www.caida.org/tools/visualization/walrus/

**9.0 Completed Travel**

The following travel incurred expenses to this award and occurred during Year 1, Qtr 4, 1-Apr-02 through 30-Jun-02:

- kc claffy 4/17 – 4/21 DARPA ITO NMS PI Meeting Baltimore, MD
- Nevil Brownlee 5/16 – 6/20 Sigmetrics Conference, Marina del Rey, CA

- Joerg Micheel 6/4 – 6/6 Work on OC48 monitor in San Jose, CA

Other related travel occurred but was not charged to this award.

**10.0 Equipment Purchases and Description**

A rack-mount computer for monitoring an OC48 backbone link at MFN in San Jose was purchased and installed. Data cartridges for storing visualization data were purchased.

**11.0 Significant Events**

- Andre Broido and kc claffy attended additional sessions of the Institute of Pure and Applied Mathematics (IPAM) workshop (May 13-17) (June 9-14). Kc claffy also arranged for Joe Abley of MFN to participate and provide an ISP's perspective.
- On April 4, 2002, kc claffy attended a meeting hosted by the National Communications System (NCS) to discuss homeland security issues. Dr. Pete Fonash, John Todd, and Inette Furey also attended. Their goal is to achieve a synoptic view of the Internet and a better understanding of what could disrupt or deny services to critical facilities.
- kc claffy and Nevil Brownlee presented at the DNS WG meeting at RIPE: http://www.ripe.net/ripe/meetings/current/ripe-42/.
- kc claffy attended the Asilomar Conference.
- Arranged to accept Robert Nowak (Rice University) student Ryan King as a summer intern.
- Visited Telus and Jaalam in Vancouver. http://www.jaalam.com/index.asp .
- kc claffy visited British Columbia Institute of Technology (BCIT) to discuss possible collaborations (May 8).
- Working to get approval from MFN to give raw trace data to NMS Pis.
- Participated in UCSD student Ju Wang's qualifying exam on DOS attack methods.
- Started arrangements to hire six summer interns.
- Visited Georgia Tech: gave "Internet Myths" talk. Met with NMS PI George Riley to discuss collaborations.
- Brad Huffaker presented at the workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection at Johns Hopkins University http://www.mts.jhu.edu/~cidwkshop/ (June 11-13, 2002).
- Help NSF with panel review June 25-26.

**12.0 Publications and Presentations:**

1. The following poster paper was at the SIGMETRICS conference in June 2002:
   a. Nevil Brownlee and kc claffy. "Internet Stream Size Distributions."
2. The following presentations were given:
   a. "Inter-domain routing evolution - Episode II: Dark Space" (ARIN IX, Apr '02) Andre Broido.
   b. "Maya 4.0 Introduction Seminar" (SDSC, Apr '02) Oliver Jakubiec.

c. "DNS Damage: Measurements at a Root Server " (RIPE, May 2, 2002) kc claffy.
d. "An analysis of the DNS traffic at f.root-servers.net" (RIPE, May 2, 2002) Nevil Brownlee.
e. "Topology Discovery by Active Probing" (Workshop on statistical and Machine Learning techniques in Computer Intrusion Detection, Johns Hopkins University, June 11-13), Brad Huffaker.
f. Andre Broido presented preliminary results of his "Internet Invariants" study. (IPAM, Jun 14)

3. The following paper was submitted:
   a. Marina Fomenkov. "A Longitudinal study of Internet traffic from 1998 – 2001." Submitted to Communications, Internet and Information Technology (CIIT 2002).
4. The following paper was accepted:
   a. D. Moore, C. Shannon and J. Brown. "Code Red: a Case Study on the Spread and Victims of an Internet Worm". IMW to be held in Marseille, FR November 2002.

**13.0 FINANCIAL INFORMATION:**

Contract #: N66001-01-1-8909

Contract Period of Performance: 5 Jun 2001 to 5 Jun 2004

Ceiling Value: $ 1,726,160

Current Obligated Funds: $1,726,160

Reporting Period: 1 Apr 2002 to 30 Jun 2002

Actual Costs Incurred: $ 1,083,551

**Current Period:**

UCSD
Labor Hours: 2,783.13 hrs $ 171,257
ODC's: $ 16,044
IDC's: $ 55,702
TOTAL: **$ 171,257**

**Cumulative to date:**

Labor Hours: 146,110.77 $ 579,186
ODC's: $ 53,957
IDC's: $ 313,317

TOTAL: **$ 946,460**

**Cost Curves for Apr - Jun 2002:**

| | ToDate Budget | ToDate Actual | ToDate Variance |
|---|---|---|---|
| **Salaries & Benefits** | 19,652 | 99,511 | **-79,859** |
| **Travel(DC)** | 7,361 | 5,497 | **1,864** |
| **Equipment (DC)** | 30,226 | 8,435 | **21,791** |
| **Other DC** | 25,987 | 2,112 | **23,875** |
| **Indirect Costs** | 24,085 | 55,702 | **-31,617** |
| **Total** | 107,311 | 171,257 | **-63,946** |

See Section 7.0 Issues for an explanation of the discrepancy between spending level and budget.