REPORT DOCUMENTATION PAGE

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION/AVAILABILITY STATEMENT

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
					19b. TELEPHONE NUMBER *(Include area code)*

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 #Qtr6

**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 October – December 2002.

2.0 Project Members

UCSD hours:
PI: 103.20
CAIDA Senior Staff: 192.19
CAIDA Staff: 607.02
Total Hours: **902.41**

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
Canceled	Add 5 additional skitter source sites	**Done**
Canceled	Add 5 workload monitor sites	**SOW changed to delete this milestone.**
Complete	Develop comprehensive website(s) for public availability of data	• root/gTLD DNS performance plots • skitter daily summaries • NMS project progress • CoralReef analysis of SDNAP

Status	Task 2 Year 2 Milestones:	Notes
Ongoing, but funded separately	Establish archive and interactive database for community access to skitter, mantra, routing, and	• research community collaborators • 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 by email, voice, and in person meetings. Gave many researchers individual feedback in pursuit of validation of their work.**
Ongoing	Work with the NMS community to design common experiments	**Ken Keys worked with Nikhil Dave to refine crl_delay**

5.0 Major Accomplishments and Results to Date

Task 1. Monitoring Task

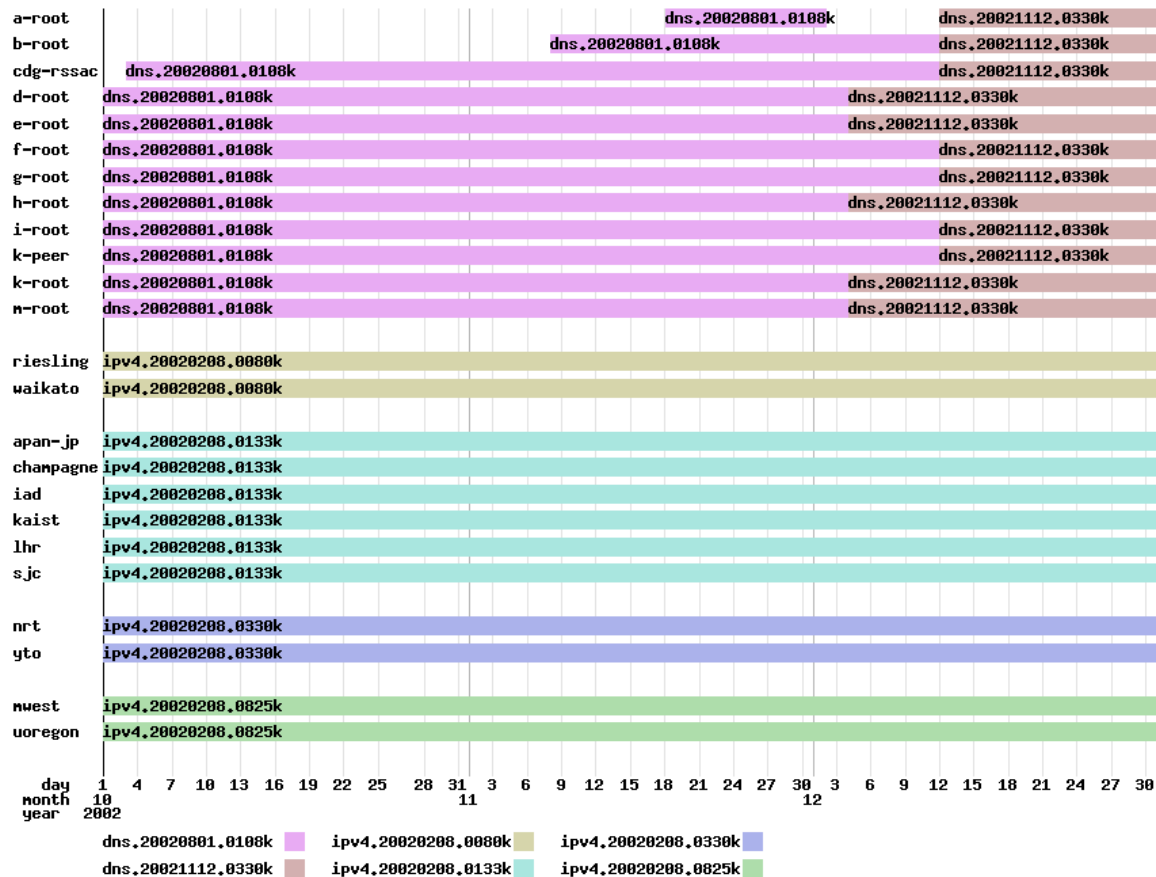## A. Topology Measurement Using Active Probes

<u>Approach</u>

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 31-Dec-02 (24 monitors active):

a-root		dns.20020801.0108k	dns.20021112.0330k
b-root		dns.20020801.0108k	dns.20021112.0330k
cdg-rssac	dns.20020801.0108k		dns.20021112.0330k
d-root	dns.20020801.0108k		dns.20021112.0330k
e-root	dns.20020801.0108k		dns.20021112.0330k
f-root	dns.20020801.0108k		dns.20021112.0330k
g-root	dns.20020801.0108k		dns.20021112.0330k
h-root	dns.20020801.0108k		dns.20021112.0330k
i-root	dns.20020801.0108k		dns.20021112.0330k
k-peer	dns.20020801.0108k		dns.20021112.0330k
k-root	dns.20020801.0108k		dns.20021112.0330k
m-root	dns.20020801.0108k		dns.20021112.0330k
riesling	ipv4.20020208.0080k		
waikato	ipv4.20020208.0080k		
apan-jp	ipv4.20020208.0133k		
champagne	ipv4.20020208.0133k		
iad	ipv4.20020208.0133k		
kaist	ipv4.20020208.0133k		
lhr	ipv4.20020208.0133k		
sjc	ipv4.20020208.0133k		
nrt	ipv4.20020208.0330k		
yto	ipv4.20020208.0330k		
mwest	ipv4.20020208.0825k		
uoregon	ipv4.20020208.0825k		

```
day    1  4  7  10 13 16 19 22 25  28 31  3  6  9  12 15 18 21 24 27  30 3  6  9  12 15 18 21 24 27 30
month  10                              11                              12
year   2002
```

Legend:
- dns.20020801.0108k
- dns.20021112.0330k
- ipv4.20020208.0080k
- ipv4.20020208.0133k
- ipv4.20020208.0330k
- ipv4.20020208.0825k

Topology Analysis Results:

B. Workload / Performance Measurement Using Passive Monitors

CAIDA deploys a passive monitor at the Metromedia Fiber Network (MFN) backbone in San Jose, CA. No OC48 traces collected during this reporting period.

DNS Queries

In January 2002, CAIDA began monitoring performance of the DNS root and gTLD nameservers from the vantage point of two NeTraMet monitors located in San Diego and San Jose. In the aftermath of the unusual denial of service (DoS) attack on the root nameservers reported by the Associated Press on October 23, CAIDA looked at its DNS performance data to provide some context and seek better understanding. It is worth noting that DoS attacks are an ongoing fact of life for the root nameservers as well as the

rest of the Internet structure. [4] This particular Dos attack was significant enough to get media attention. Even so, the user-visible impact on global network operation was slight.

C. Routing Measurement

No routing analysis results reported during this reporting period.

Task 2, Archiving and Storage Task

Approach for Archiving skitter Data and Making Data Available to Researchers

Requestor	Organization	Project
Wendy Garvin	Cisco Systems	Internet security triage
Thomas E. Daniels	Iowa State	Network traceback algorithms
Kave Salamatian	LIP6-Universite Pierre et marie Curie	Metropolis project
Shudong Jin	Boston University	IP connectivity
Krishna Phani Gummadi	University of Washington	Overlay networks
Minho Sung	Georgia Institute of Technology	Test hash-based traceback scheme
Xiaoxia Liu	George Mason University	Internet and regional economics
Dimitar Vasilev	Technological University, Sophia, Bulgaria	Core Internet weather maps
Wu Weidong	Huazhong university of Science and technology, Wuhan City, Hubei Province, China	Routing policy atoms
Lisa Amini	IBM Research	Routing research
Ratul Mahajan	University of Washington	RocketFuel project
Dequan Li	Institute of Software, Chinese Academy of Sciences	IP traceback algorithm for DdoS attack tracing.
Masafumi Oe	NARA Institute of Science and technology (NAIST)	BGP peering topology map and simulations
Yuchung Cheng	UCSD CSE	P2P network simulations
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	17
Master's students using skitter data	15
About publicly available skitter data: http://www.caida.org/cgi-bin/skitter_summary/main.pl	

Approach for Archiving CoralReef Data

1. CAIDA maintains a SDNAP report generator, publishing workload characterization results at http://www.caida.org/dynamic/analysis/workload/sdnap/0_0_/. Results are updated every 5 minutes.
2. 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

After multiple discussions with SPAWAR, NMS Program Director Sri Kumar and his staff as well as UCSD and CAIDA staff, we reached a mutually acceptable agreement to change our SOW to repurpose remaining funds to a new Task 3: Domain Name System (DNS) Infrastructure Model. Work on Tasks 1 and 2 continues under new funding from the National Communications System (NCS).

8.0 Near-term Plan

The following work is planned for 01-Jan-03 through 31-Mar-03:

General/Administrative Outreach and Reporting Plans

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

Task 3. DNS Analysis

Overall goals: Build a model of DNS behavior. Investigate whether the current design will scale to serve continued IP address space growth. Conduct controlled experiments to identify parameters crucial to proper DNS operation.

- Report on DNS damage from non-caching DNS clients or ill-formed (illegal) queries. Suggest strategies for protecting the DNS.
- Report on the validity of BIND name server affinity algorithm.
- Provide initial model of DNS behavior for NMS Integration Prototype

- Document, package, and distribute passive tools (CoralReef and/or NeTraMet) and methods for their use to monitor the DNS infrastructure.

9.0 Completed Travel

The following travel incurred expenses to this award and occurred during Year 2, Qtr 2, 1-Oct-02 through 31-Dec-02:

- kc claffy 11/12 – 11/15 Chicago – DARPA NMS meeting
- Margaret Murray 11/12-11/15 – DARPA NMS meeting

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

10.0 Equipment Purchases and Description

No equipment was purchased during this quarter.

11.0 Significant Events

- Kc claffy and Margaret Murray attended the NMS PI meeting November 14. Kc claffy gave a presentation on the October DNS root nameserver DOS attacks and participated the BGP breakout session.
- Ken Keys sent Nikhil Dave a new version of CoralReef application *plot_oneway* that plots ACK delays as well as oneway delays, and fixes some problems.
- Dr. Nikhil Dave' (2822) demonstrated DARPA NMS to CDR Richard Nguyen (04F-D1 LANT FLT BF Manager), Mr. Jim Hrin (165-3),Mr. Cecilio Nazareno (165-30) and Mr. Servo Soriano (165). The demo focused on candidate technologies from the DARPA NMS program for transition to Integrated Network Manger Pro (INM Pro) and related programs for network monitoring, diagnostics, and management. The demo showed current capabilities of DARPA NMS network monitoring and modeling technologies and identified ways these technologies could be applied/transitioned to INM Pro and the Joint Network Management System (JNMS). DARPA NMS technologies are currently being evaluated against COTS products by 165 and others in their quest for improved capability in wide area network management.

12.0 Publications and Presentations:

1. The following papers were published:
   a. C. Shannon, D. Moore, and k. claffy, ``Beyond Folklore: Observations on Fragmented Traffic,'', IEEE/ACM Transactions on Networking, Dec 2002.
   b. D. Moore, C. Shannon, and J. Brown, ``Code-Red: a case study on the spread and victims of an Internet worm,'', in IMW 2002, Marseille, France, Nov 2002, ACM SIGCOMM/USENIX Internet Measurement Workshop.
2. The following presentations were given:

a. "measurement and analysis activities relevant to networking researchers" (DARPA NMS PI, Nov '02)

b. "Toward Lowering the Load on DNS Root Nameservers" (NANOG, Oct '02)

3. CAIDA published analysis of October 2002 DNS root nameserver DOS attacks. (See: http://www.caida.org/projects/dns-analysis/oct02dos.xml)

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 Oct 2002 to 31 Dec 2002

Actual Costs Incurred: $ 1,158,579

Current Period:

UCSD
Labor Hours: 902.41 $ 33,097
ODC's: $ 12,056
IDC's: $ 23,479
TOTAL: **$ 68,632**

Cumulative to date:

Labor Hours: 19094.38 $ 697,796
ODC's: $ 77,547
IDC's: $ 383,236
TOTAL: **$ 1,158,579**

This revision of last quarter's cost curves reflects budgeting against the actual funds received instead of the budget plan for the total awarded amount.

Cost Curves for Oct - Dec 2002:

	ToDate Budget	ToDate Actual	ToDate Variance
Salaries & Benefits	146,726	33,097	113,629

Travel(DC)	6,786	2,033	4,753
Equipment (DC)	39,053	0	39,053
Other DC	24,293	10,023	14,270
Indirect Costs	77,025	23,479	53,546
Total	293,883	68,632	**225,251**

NMS Cost Curves Oct - Dec 2002