REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 01-Jul-2004	**2. REPORT TYPE** Quarterly	**3. DATES COVERED** *(From - To)* Jul 2003 - Sep 2003

4. TITLE AND SUBTITLE

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

Progress Status and Management Report
for the period Jul 2003 - Sep 2003

5a. CONTRACT NUMBER
AO: L018/00

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

5c. PROGRAM ELEMENT NUMBER
0602301E

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
DI-MGMT-80227

6. AUTHOR(S)

Dr. K. C. Claffy

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-10-Qtr#9

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.
					19b. TELEPHONE NUMBER *(Include area code)*
U	U	U	UU	12	(858)534-8333

NMS Project Quarterly Report #Qtr9: 1-Jul-03 through 30-Sep-03

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 #Qtr9

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 July - September 2003.

2.0 Project Members

UCSD hours:
PI: 77.40
CAIDA Senior Staff: 258
CAIDA Staff: 352.60
Total Hours: **688**

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

Status	**Task**	**Notes**
Cancelled	**Task 1 Year 3**	Monitoring and archiving work now funded by NCS is reported here for continuity
Cancelled	**Task 2 Year 3**	
	Task 3 Year 3 Milestones:	
Complete	Report on DNS damage; suggest protection strategies.	**Dnstop tool offered to DNS operators**
Ongoing	Report on validity of BIND name server affinity	**Additional experiments run and analysis published**
Complete	Provide initial model of DNS behavior for NMS Integration Prototype	**Refinement of DNS Query Workload for simulations derived from real DNS root server traffic**
Ongoing	Document, package, and distribute passive tools (CoralReef and/or NeTraMet) and methods for their use to monitor the DNS infrastructure	**Updates to custom CoralReef application crl_delay released to Nikhil Dave**

5.0 Major Accomplishments and Results to Date

Task 1. Monitoring Task

A. Topology Measurement Using Active Probes

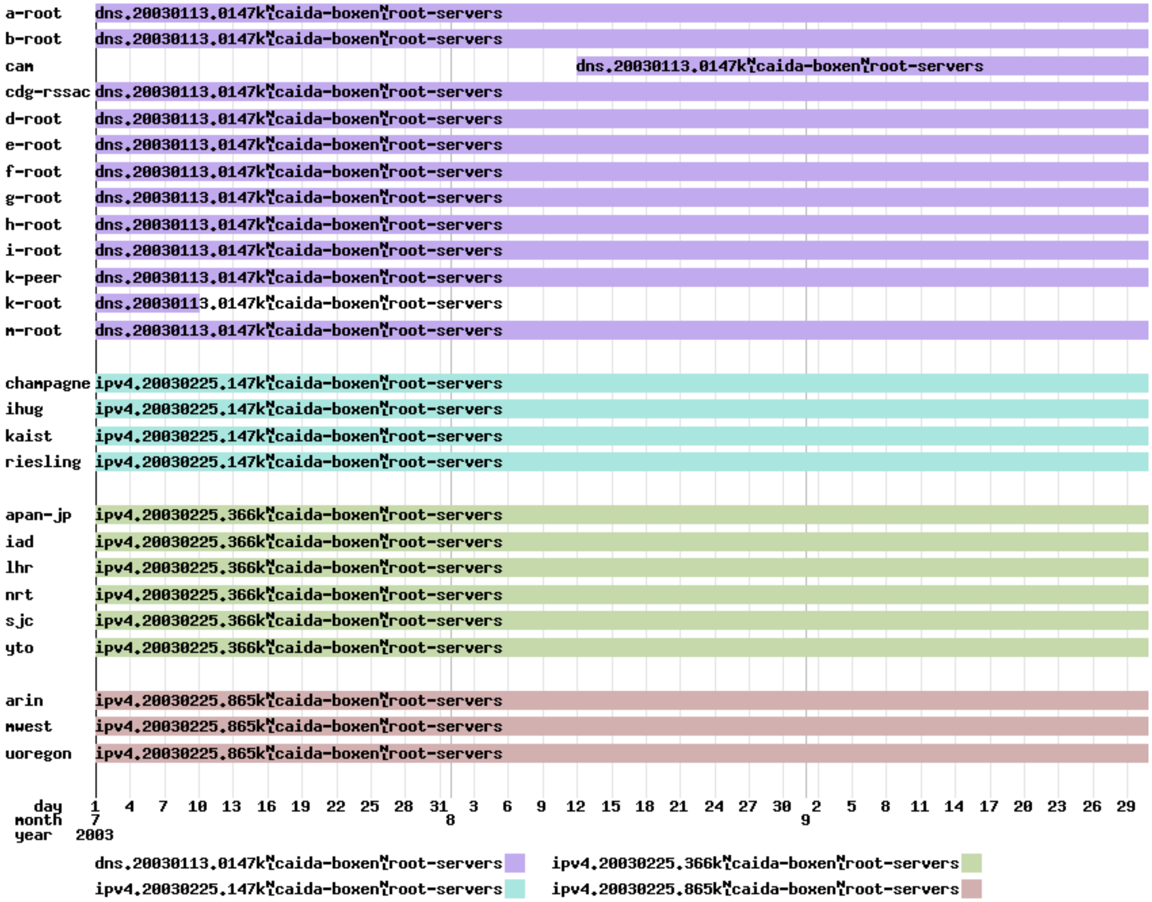
Approach

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-Sep-03 (25 monitors active):



B. Workload / Performance Measurement Using Passive Monitors

OC48 Traces were successfully captured from the Metromedia Fiber Network (MFN) backbone in San Jose, CA. Data was provided to CAIDA from the WAND Research Group (University of Waikato, New Zealand) using their deployed OC48 DAG interface card. Analysis results (provided below) used CAIDA's CoralReef software suite.

Task 2, Archiving and Storage Task

<u>Approach for Archiving skitter Data and Making Data Available to Researchers</u>

Requestor	Organization	Project
Vladimir Blogojevic	York University, UK	P2P topologies
Chun-0Sung Lee	Konkuk University, Korea	.KR DNS name servers
Mok Yeen Nam	University of Kent, UK	Large-scale overlay networks

Abraham Yaar	CMU	DDoS mitigation
Yusung Kim	KAIST	Overlay multicast or application layer multicast
Junghee Han	University of Michigan	Pathc redundancy
XiaoFeng Wang	CMU	DDoS countermeasures
Johnghyun Kim	University of Oklahoma	Computer worm simulation
Ahmad Suffian	Tokyo University and WIDE	Photonic Network
Roger Wattenhofer	ETHZ (Swiss Federal Institute of Technology)	Routing policies
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		6
Master's students using skitter data		4
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.

Task 3. Domain Name System (DNS) Infrastructure Model

About the dnstop tool:

The *dnstop* utility is useful for the discovery of names server misconfigurations. *dnstop* is a libpcap application (similar to tcpdump) that displays various tables of DNS traffic on your network, including tables of source and destination IP addresses, query types, top level domains and second level domains. The dnstop tool is written by Duane Wessels and maintained at the Measurement Factory (http://dnstop.measurement-factory.com/)

dnstop is a libpcap application (a la tcpdump) that displays various tables of DNS traffic on your network. Currently *dnstop* displays tables of:

- Source IP addresses
- Destination IP addresses
- Query types
- Top level domains
- Second level domains

6.0 Artifacts Developed During the Past Quarter

None

7.0 Issues

None.

8.0 Near-term Plan

The following work is planned for 01-Oct-03 through 31-Dec-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

No travel incurred expenses to this award during Year 3, Qtr 1, 1-Jul-03 through 30-Sep-03:

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

10.0 Equipment Purchases and Description

Cyclades remote server management cards were purchased to increase remote diagnosis capabilities for passive monitors.

11.0 Significant Events

- Discussions occurred with NMS PI Scott Jordan and his student Ngok Lam of UC Irvine about how best to acquire traffic data in order to investigate user leve behavior in perr-to-peer systems. CAIDA sent him anonymized tracefiles.
- CAIDA sent NMS PI Scott Jordan 12 CoralReef tracefiles, 6 for each direction, 10 minutes of data in each direction collected from the UCSD/SDSC external gateway. These files will support Scott's peer-to-peer studies.

12.0 Publications and Presentations:

1. The following papers were published:
   - D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, ``Inside the Slammer Worm,", IEEE Security and Privacy, vol. Aug 2003, Aug 2003.
2. The following presentations were given:
   a. "CAIDA projects related to Internet data visualization" (WIDE, Jul '03)
   b. "Network Telescopes" (DIMACS, Sep '03)
   c. "bandwidth estimation: measurement methodologies and applications" (National Collaboratory, Aug '03)
3. CAIDA prepared and submitted a Technical Report, Financial Report and Quad Chart for the IPTO 2003 Project Summary Collection.

13.0 FINANCIAL INFORMATION:

Contract #: N66001-01-1-8909

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

Ceiling Value: $ 21,726,160

Current Obligated Funds: $1,726,160

Reporting Period: 1 Jul 2003 to 30 Sep 2003

Actual Costs Incurred: $ 940,065.00

Current Period:

UCSD
Labor Hours: 688 $ 24,115
ODC's: $ -461
IDC's: $ 11,335
TOTAL: **$ 34,989**

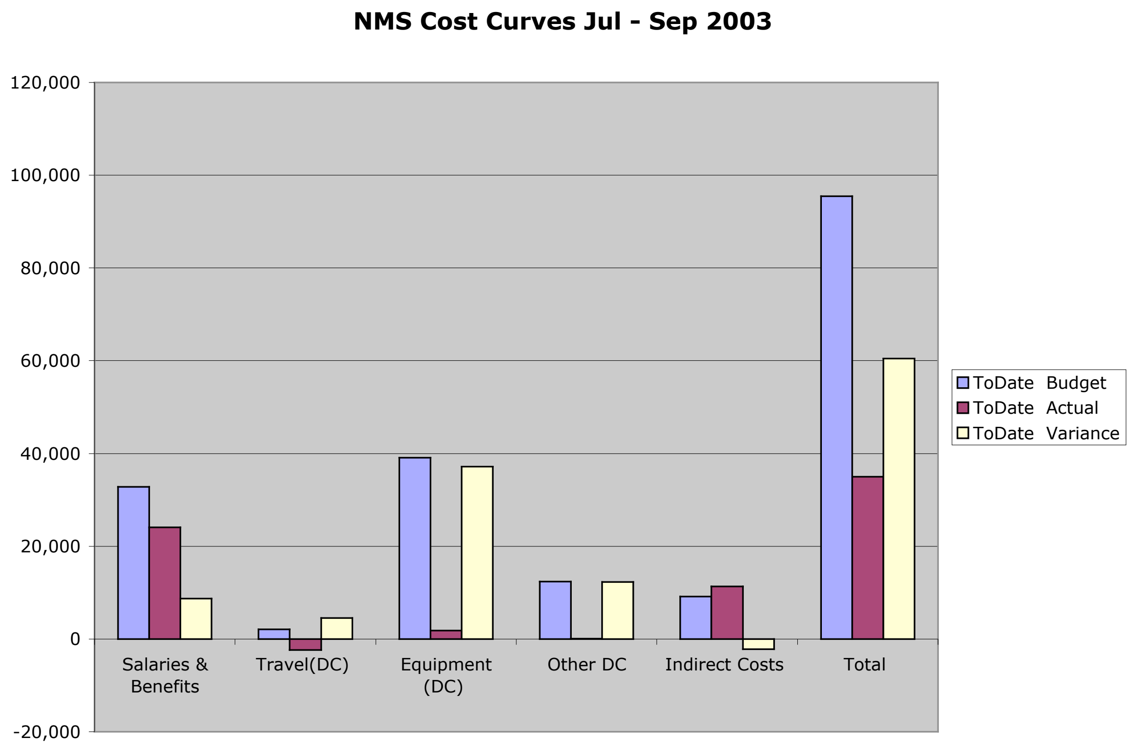
Cumulative to date:

Labor Hours: 21,880.78 $ 802,738
ODC's: $ 81,630
IDC's: $ 438,964
TOTAL: **$ 1,323,332**

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 Jul - Sep 2003:

	ToDate Budget	**ToDate Actual**	**ToDate Variance**
Salaries & Benefits	32,802	24,115	8,687
Travel(DC)	2,112	-2,384	4,496
Equipment (DC)	39,053	1,857	37,196
Other DC	12,367	66	12,301
Indirect Costs	9,153	11,335	-2,182
Total	95,487	34,989	**60,498**


NMS Cost Curves Jul - Sep 2003
Salaries & Benefits
Travel(DC)
Equipment (DC)
Other DC
Indirect Costs
Total
□ ToDate Budget
■ ToDate Actual
□ ToDate Variance