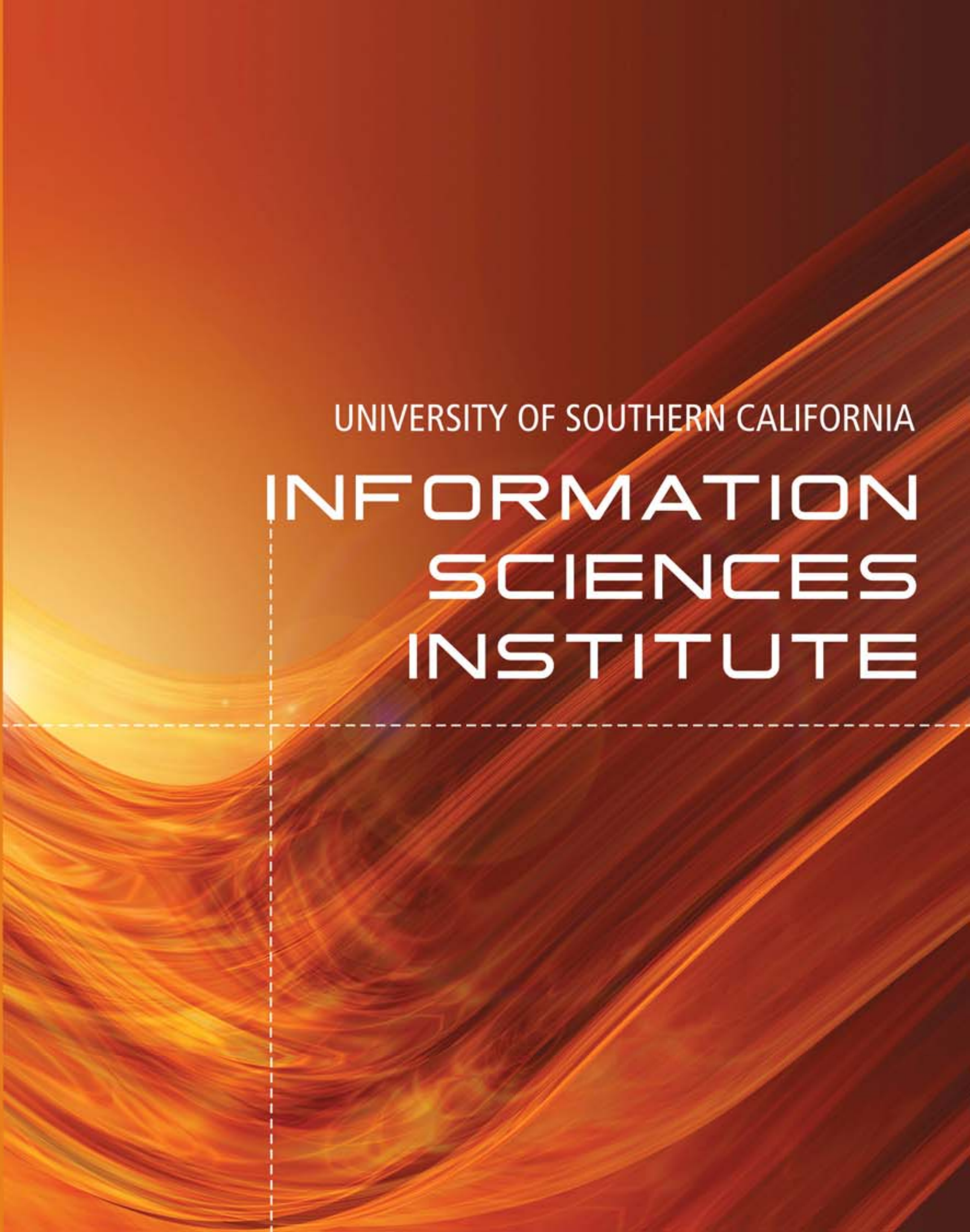
DETER Testbed for Security Experimentation

Ted Faber
USC/ISI



USC Viterbi
School of Engineering

Goal of This Talk

- **Familiarize security professionals with DETER testbed**
  - Recruit new users
  - Collect proposals of novel features to implement in DETER
- **What you'll hear**
  - Short overview of DETER testbed and community
  - Why use DETER
  - Short demo
  - New directions: federation and risky experiment support
  - Q & A: how can DETER fit your needs?

What Is DETER?

- **Security testbed located at USC/ISI and UC Berkeley**
  - Funded by NSF and DHS, started in 2004.
  - Joint project of USC/ISI, UC Berkeley and SPARTA
  - 204 Nodes at ISI, 96 Nodes at UC Berkeley, constantly adding more
  - Many tools for experimenters: GUIs, traffic generators, simulators, ...
  - Based on Emulab software, with focus on security experimentation
- **What DETER offers**
  - Exclusive access to multiple PCs and specialized hardware, running OS of your choice, for as long as needed
  - Tools for security experimentation
  - Large user community

Why Use DETER?

- **Accuracy: real-world experiments, not simulations**
  - Current network simulators do not correctly simulate security events
  - Difficult to convince reviewers about fidelity of custom simulators
- **Ease: Reuse real software for traffic and security**
  - Instead of writing novel traffic generators or simulators, use real client/server applications and real malicious code
  - Use/test existing security software and hardware and improve it
- **Learning: Understand novel phenomena/test hypotheses**
  - Observe behavior of malicious code, security software, or hosts under attacks

DETER Vs. Other Testbeds

- **Emulab, WAIL and DETER are based on the same software**
  - DETER has focus on security experimentation, tools to support it and staff willing to accommodate risky experiments
  - We are in the process of automating risky experiment containment
- **Synergy not competition**
  - Emulab users migrate to DETER when Emulab runs out of nodes
  - We ran federation experiments spanning all three testbeds
- **Easy transfer**
  - Experiments can be easily transferred between testbeds, but some DETER-specific tools may not run on other testbeds

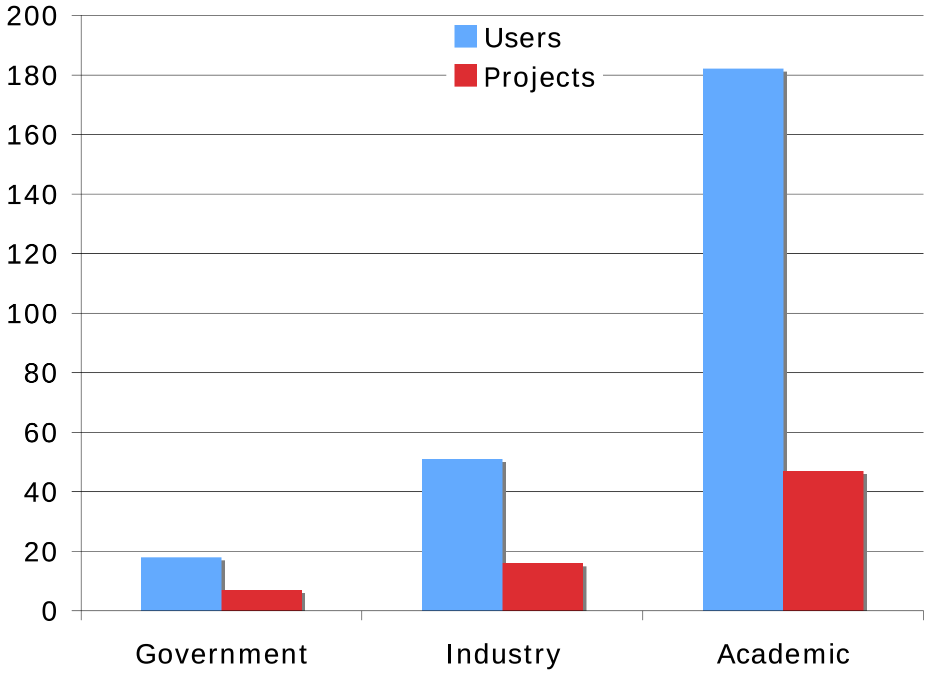
DETER Howto

- **You only need Web and SSH access to work on DETER**
- **Open a user account and apply for a project (www.deterlab.net)**
  - You can approve other users (e.g., your students) to join your projects
- **When you need to run experiments:**
  - Log on to www.deterlab.net
  - Draw a topology using the GUI on the page, or write it in NS
  - Start a new experiment with a given topology - nodes are assigned to you (approx. 10 min activation time)
  - Load software you need on nodes and run experiments
  - Existing experiments can be swapped in and out, and terminated when no longer needed

DETER Community

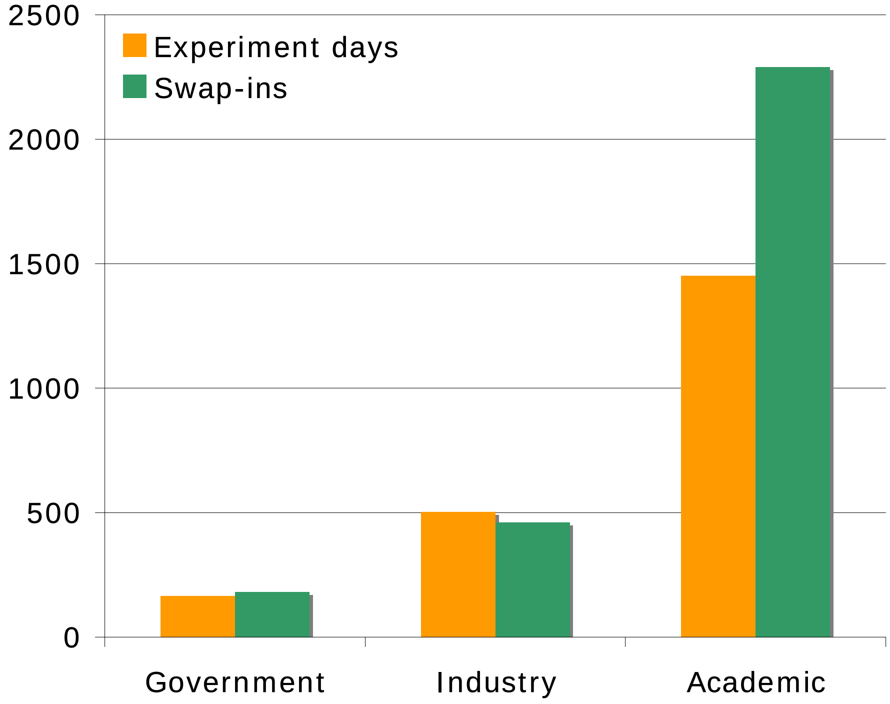
- **Many users in academia, industry and government**
- **Many tools for security experimentation**
  - Continually contributed by users
- **Great project diversity**
  - Opportunity to collaborate with other groups in your area of interest
  - Stand on shoulders of other users, reuse their wisdom
- **Mailing lists for users**
- **Monthly teleconference calls with user participation**
- **Yearly community workshop**

DETER Community

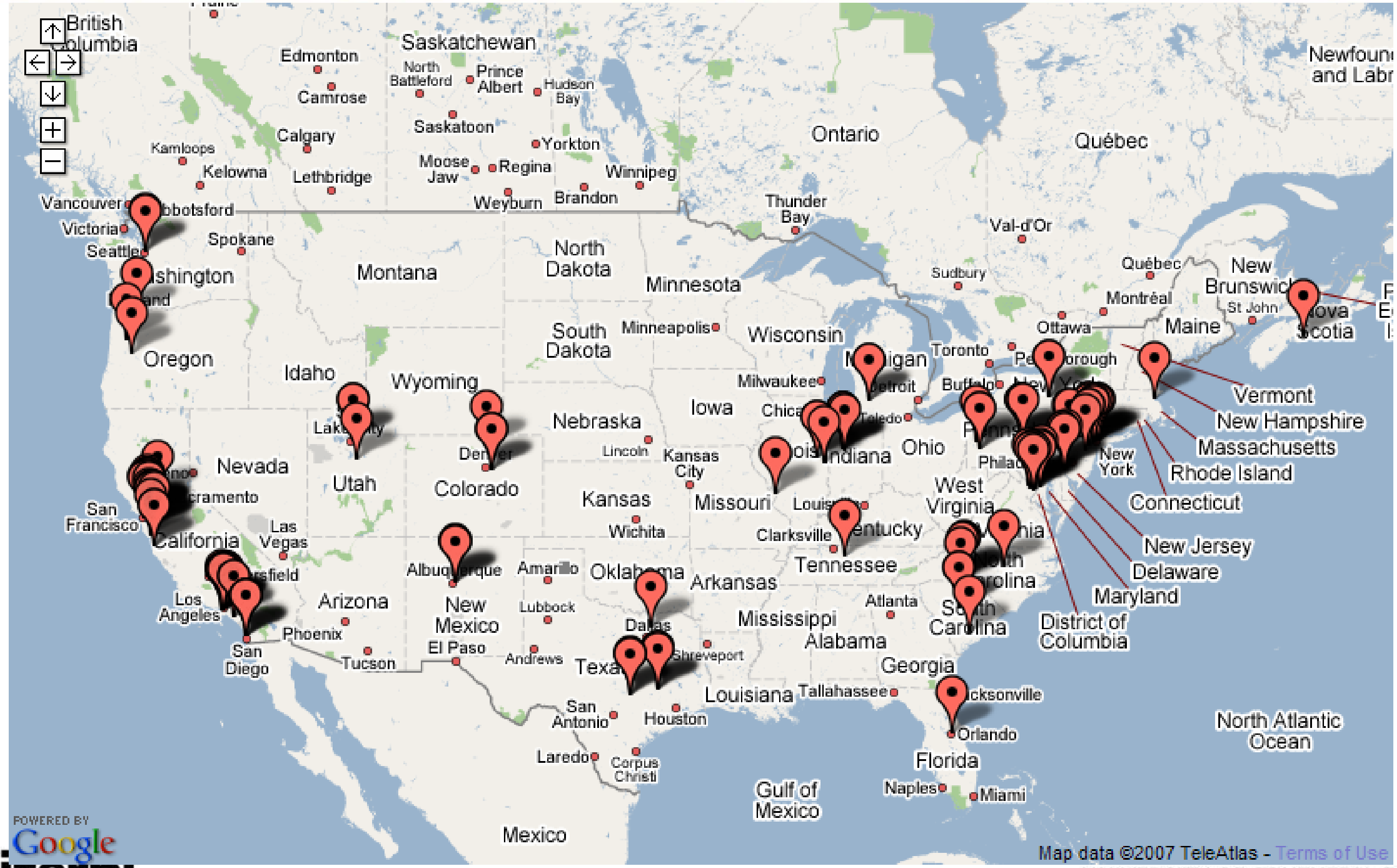


251 Users
70 Projects

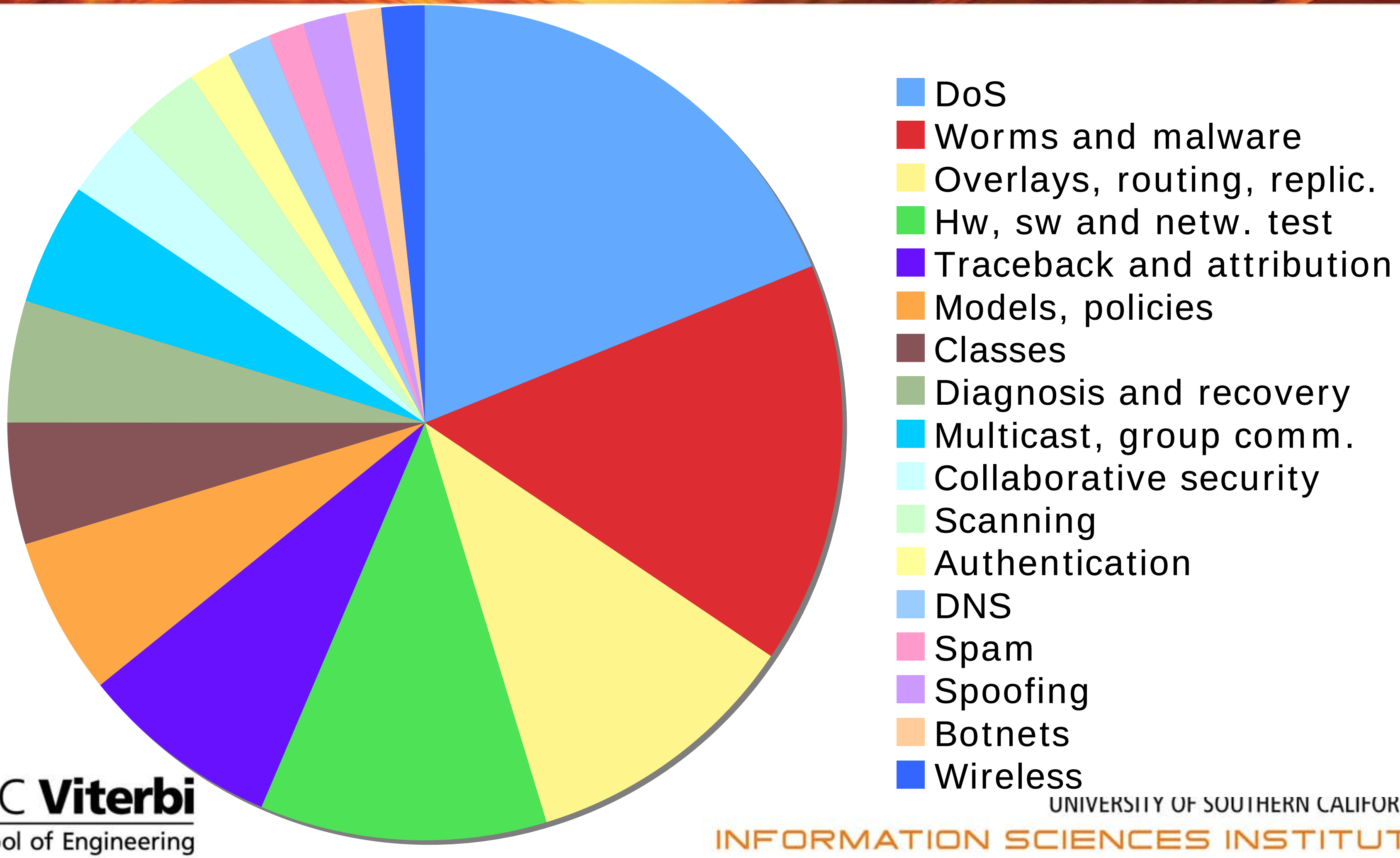
2119 Experiment days (~6 per day)
2933 Swap-ins



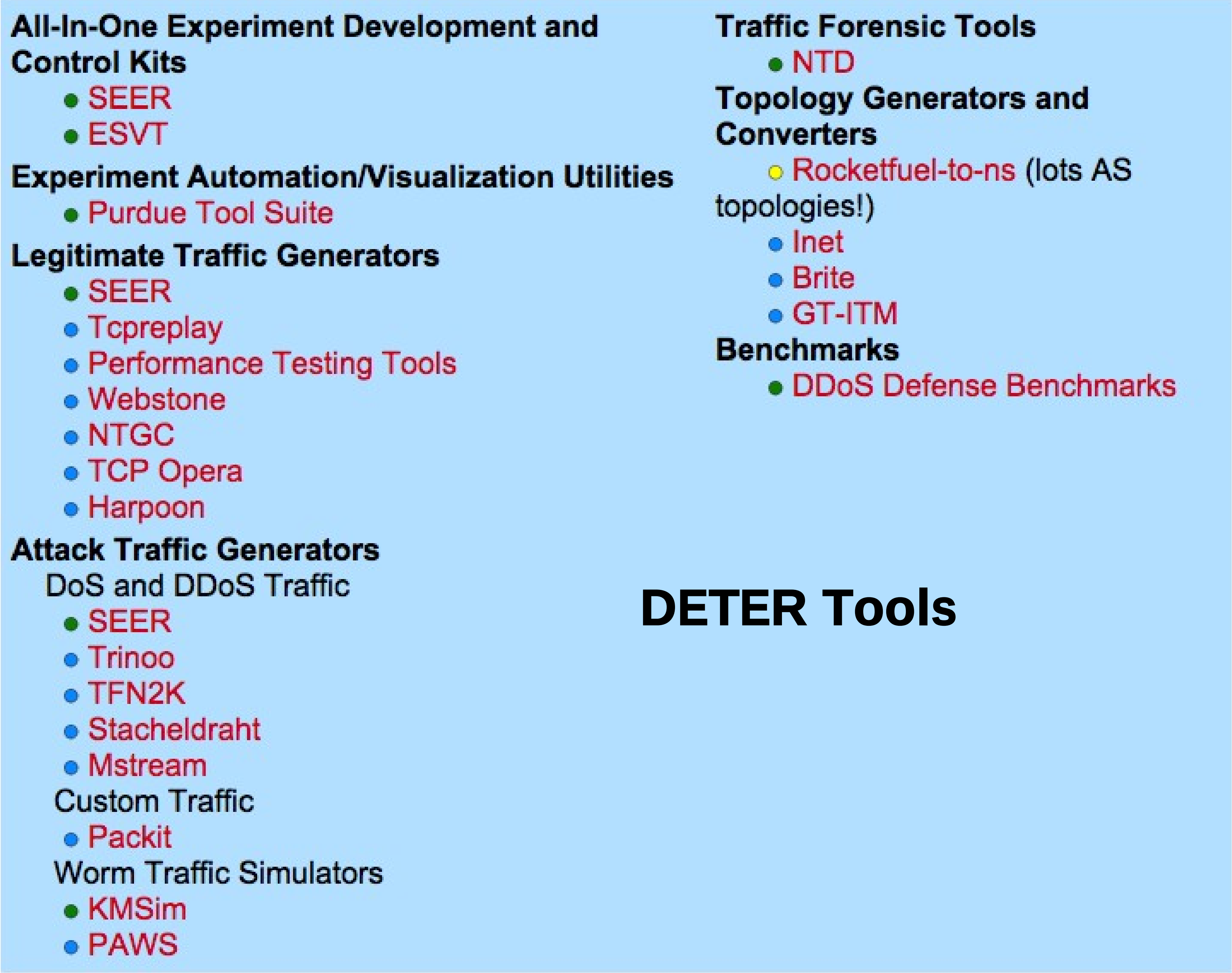
DETER Community



DETER Projects



DETER Tools



All-In-One Experiment Development and Control Kits

- SEER
- ESVT

Experiment Automation/Visualization Utilities

- Purdue Tool Suite

Legitimate Traffic Generators

- SEER
- Tcpreplay
- Performance Testing Tools
- Webstone
- NTGC
- TCP Opera
- Harpoon

Attack Traffic Generators

DoS and DDoS Traffic

- SEER
- Trinoo
- TFN2K
- Stacheldraht
- Mstream

Custom Traffic

- Packit

Worm Traffic Simulators

- KMSim
- PAWS

Traffic Forensic Tools

- NTD

Topology Generators and Converters

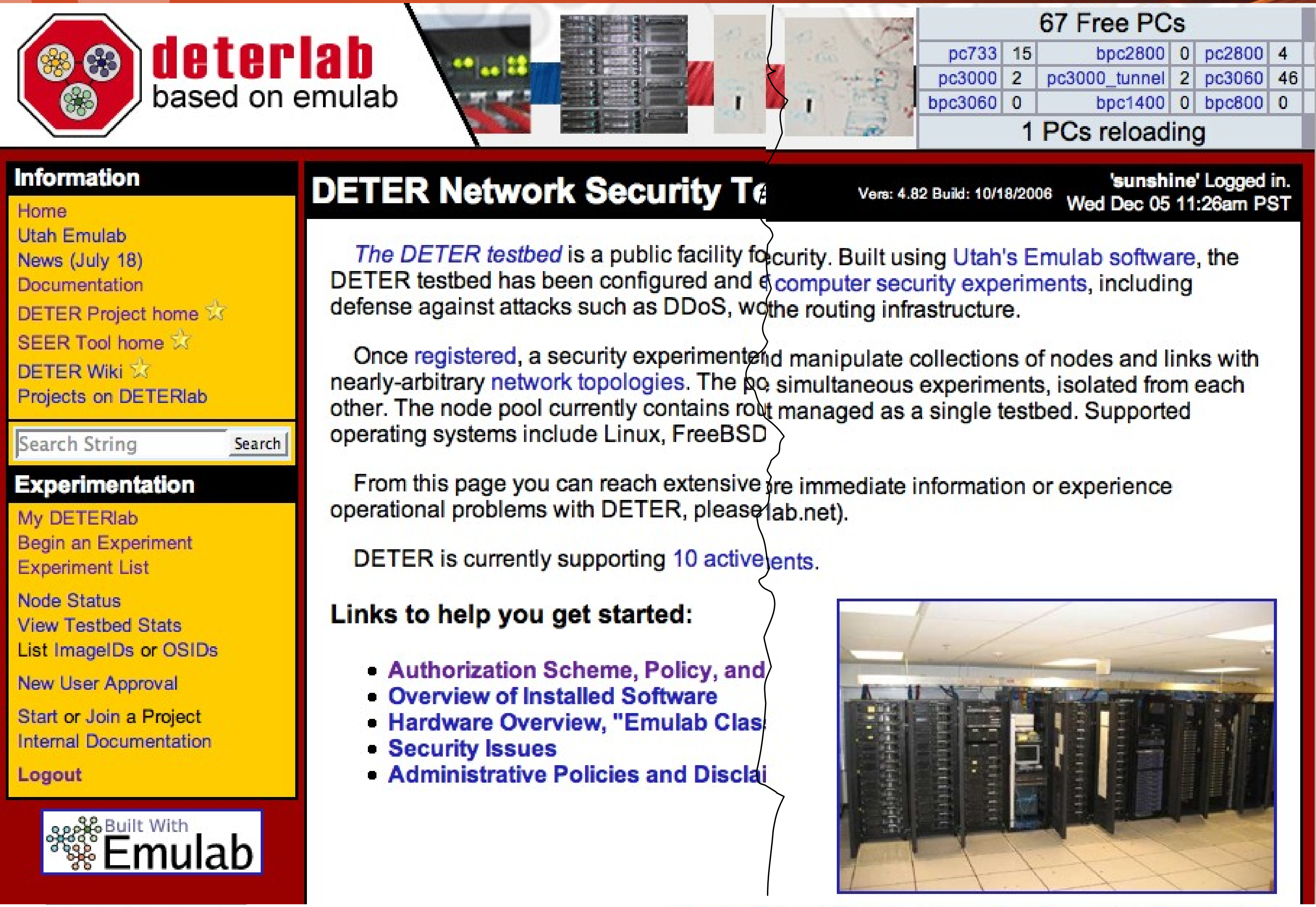
- Rocketfuel-to-ns (lots AS topologies!)
- Inet
- Brite
- GT-ITM

Benchmarks

- DDoS Defense Benchmarks

DETER Demo

- **Create a simple DoS experiment**
  - One Web client, one Web server, one attacker
  - Server has a bottleneck link
  - UDP flood attack with randomly sized packets (100 - 1,200B) targetting port 80 - pulsing shape (10 sec on, 20 sec off)
- **Start experiment using DETER Web page**
- **Populate traffic generators and visualize traffic using SEER**



67 Free PCs

pc733	15	bpc2800	0	pc2800	4
pc3000	2	pc3000_tunnel	2	pc3060	46
bpc3060	0	bpc1400	0	bpc800	0

1 PCs reloading

Information

- Home
- Utah Emulab
- News (July 18)
- Documentation
- DETER Project home ☆
- SEER Tool home ☆
- DETER Wiki ☆
- Projects on DETERlab

Search String [Search]

Experimentation

- My DETERlab
- Begin an Experiment
- Experiment List
- Node Status
- View Testbed Stats
- List ImageIDs or OSIDs
- New User Approval
- Start or Join a Project
- Internal Documentation
- Logout

DETER Network Security Te

Vers: 4.82 Build: 10/18/2006
'sunshine' Logged in.
Wed Dec 05 11:26am PST

The DETER testbed is a public facility fo curity. Built using Utah's Emulab software, the DETER testbed has been configured and e computer security experiments, including defense against attacks such as DDoS, wo the routing infrastructure.

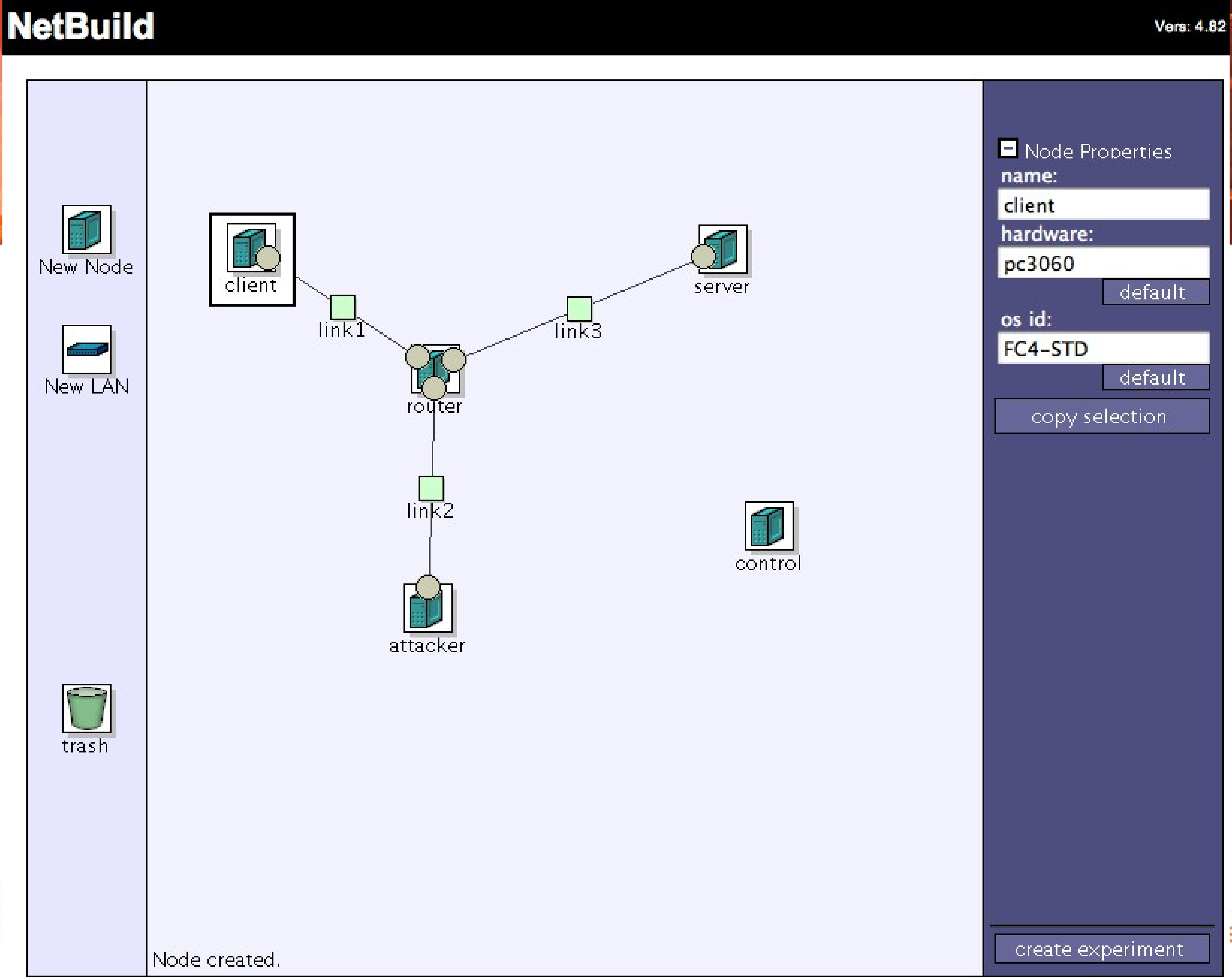
Once registered, a security experimenter d manipulate collections of nodes and links with nearly-arbitrary network topologies. The po simultaneous experiments, isolated from each other. The node pool currently contains rou t managed as a single testbed. Supported operating systems include Linux, FreeBSD

From this page you can reach extensive re immediate information or experience operational problems with DETER, please lab.net).

DETER is currently supporting 10 active ents.

Links to help you get started:

- **Authorization Scheme, Policy, and**
- **Overview of Installed Software**
- **Hardware Overview, "Emulab Clas**
- **Security Issues**
- **Administrative Policies and Disclai**

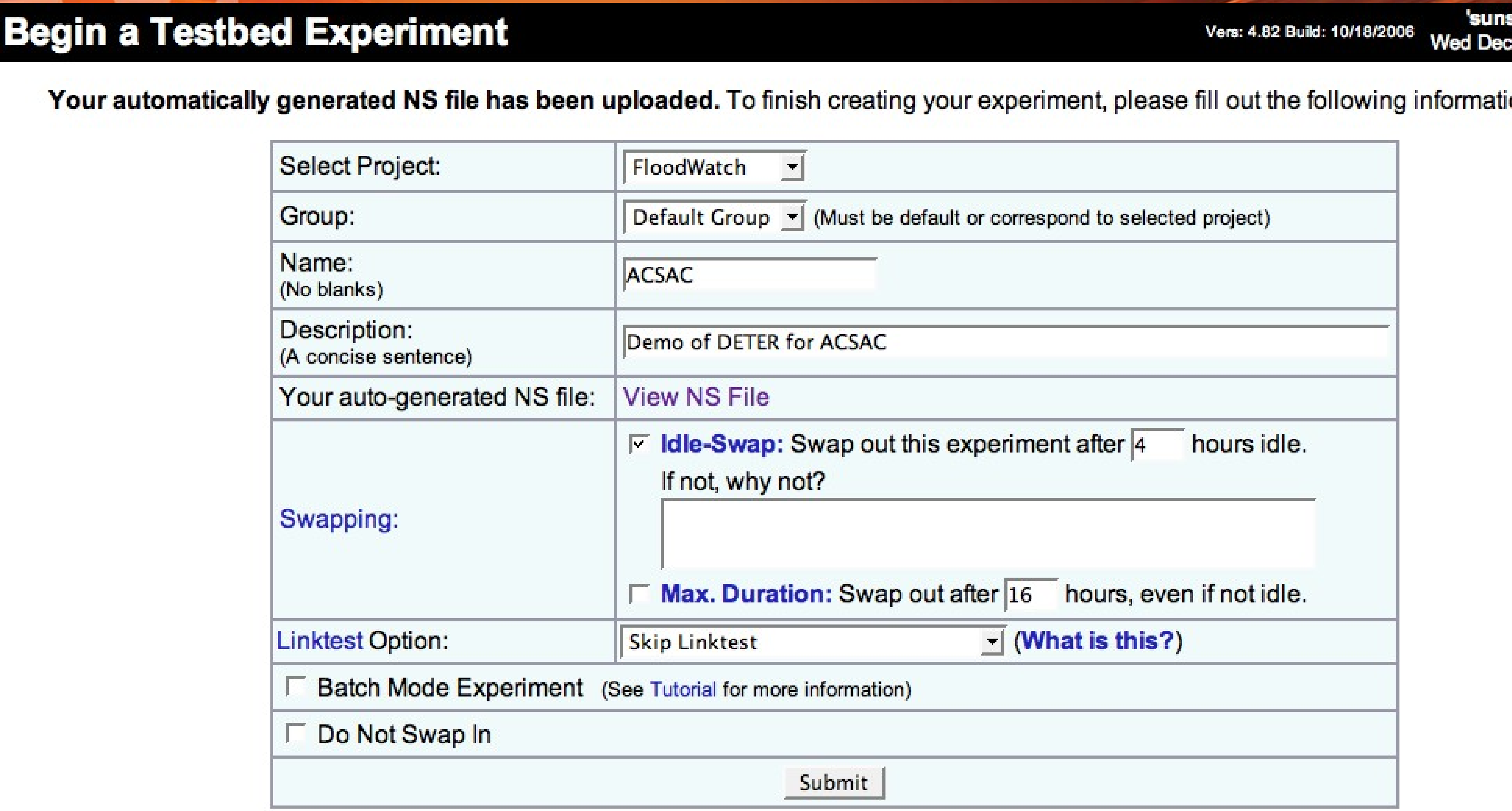


name: client

hardware: pc3060

os id: FC4-STD

Node created.



Begin a Testbed Experiment

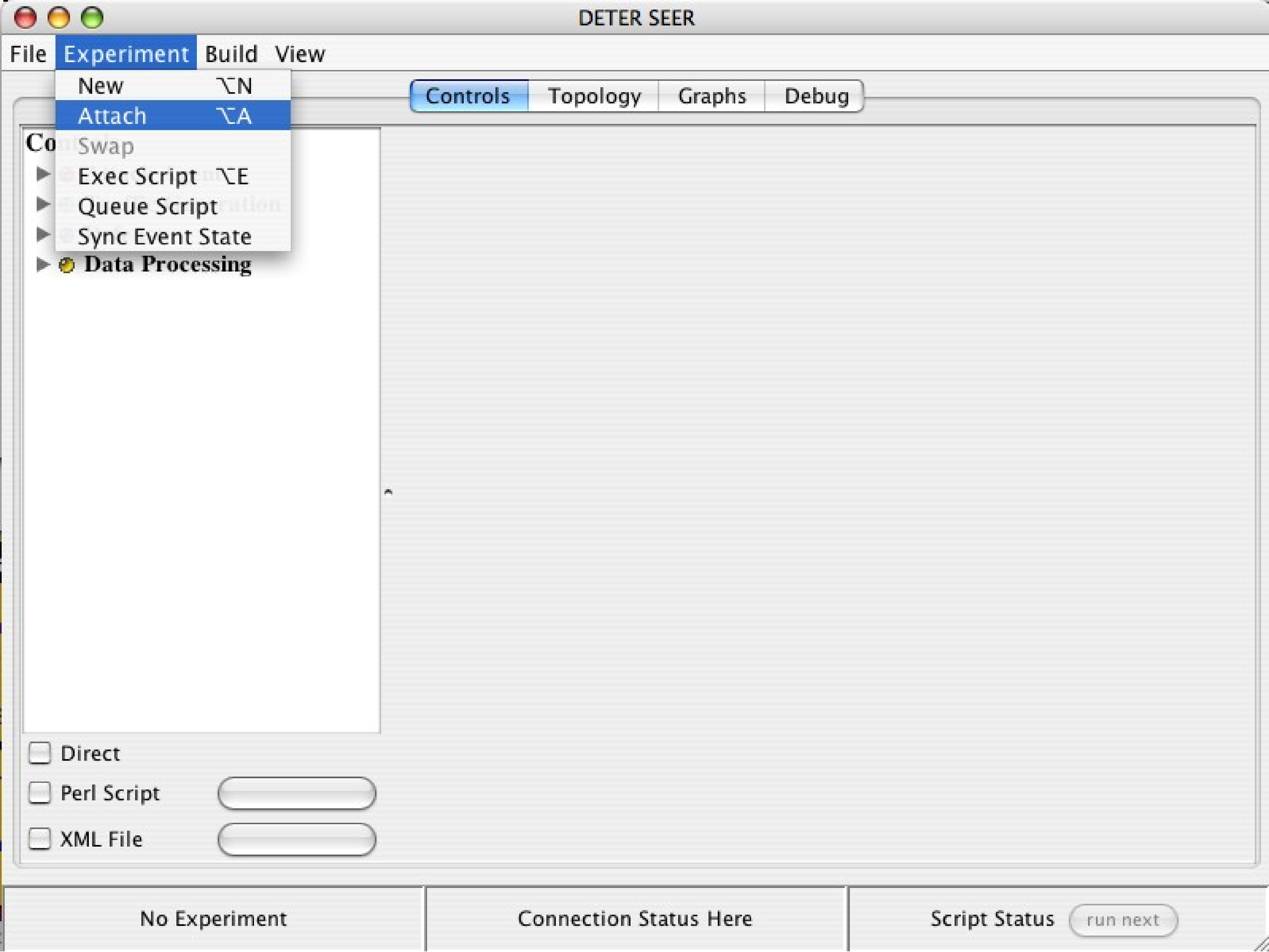
Vers: 4.82 Build: 10/18/2006

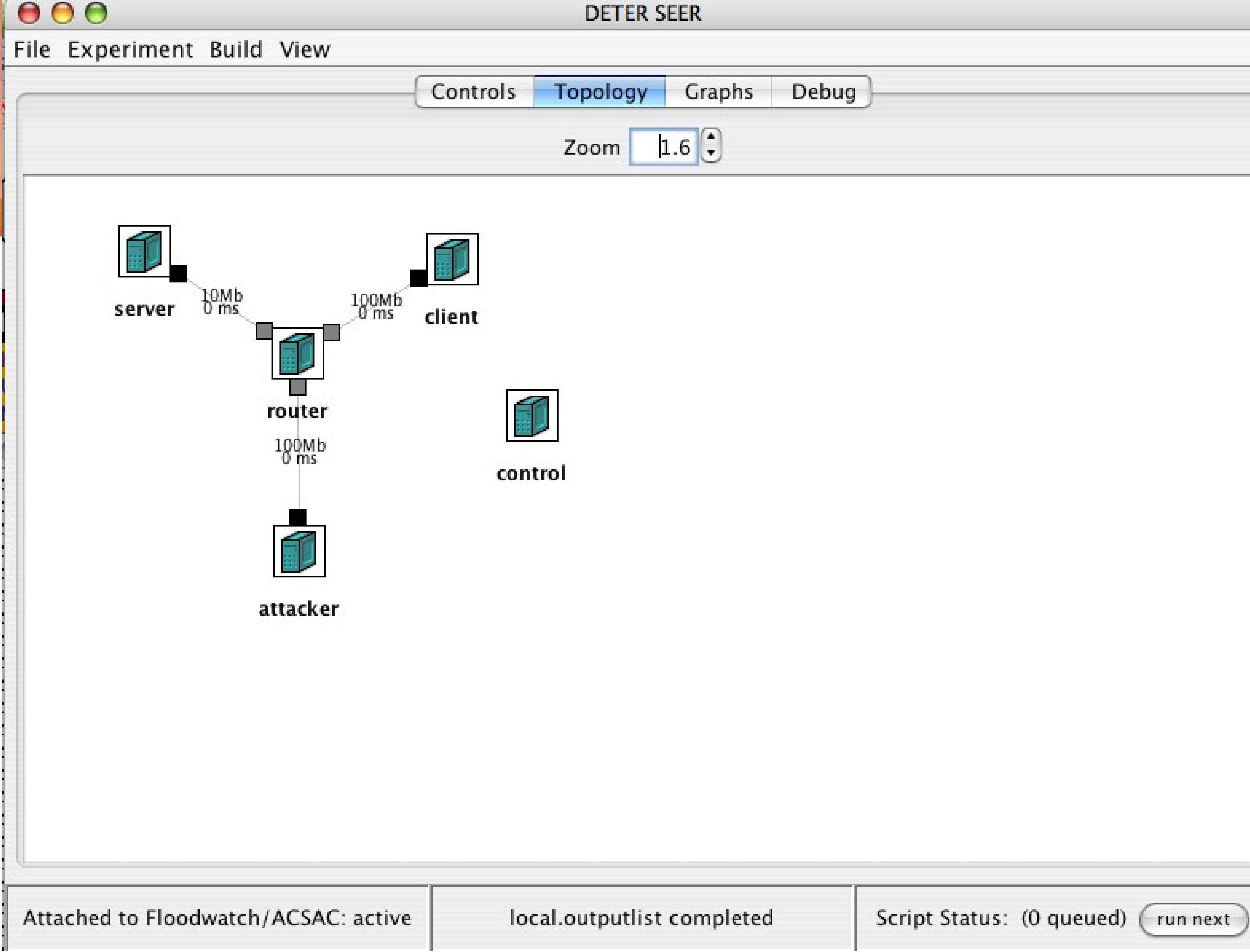
'suns

Wed Dec

Your automatically generated NS file has been uploaded. To finish creating your experiment, please fill out the following informati

Select Project:	FloodWatch ▾
Group:	Default Group ▾ (Must be default or correspond to selected project)
Name: (No blanks)	ACSAC
Description: (A concise sentence)	Demo of DETER for ACSAC
Your auto-generated NS file:	View NS File
Swapping:	☑ **Idle-Swap:** Swap out this experiment after 4 hours idle. If not, why not? ☐ **Max. Duration:** Swap out after 16 hours, even if not idle.
Linktest Option:	Skip Linktest ▾ (**What is this?**)
☐ Batch Mode Experiment (See Tutorial for more information)	
☐ Do Not Swap In	
Submit	

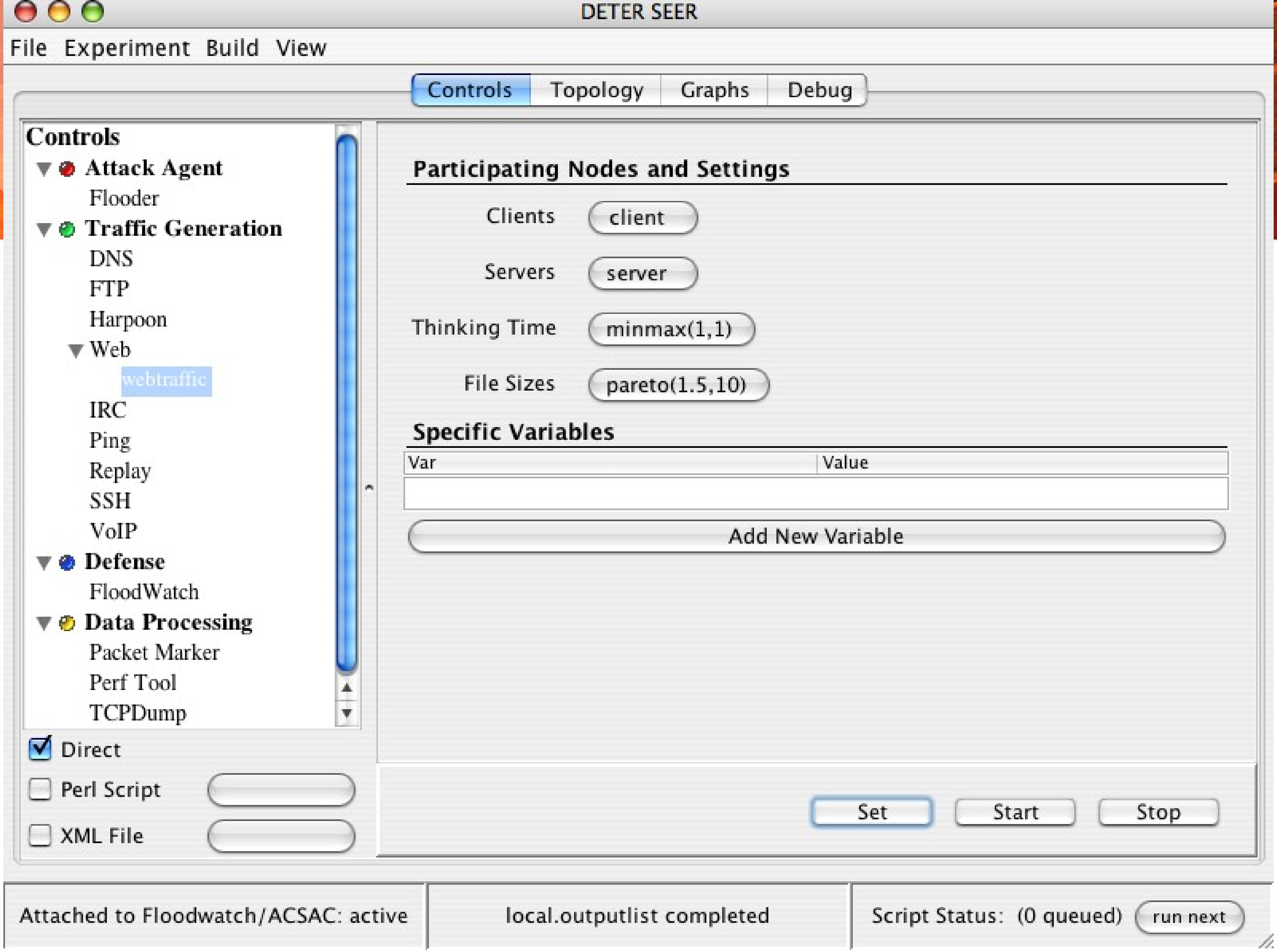

DETER SEER
File
Experiment
Build
View
New ⌥N
Attach ⌥A
Swap
Exec Script ⌥E
Queue Script
Sync Event State
Controls
Topology
Graphs
Debug
Co
Data Processing
□ Direct
□ Perl Script
□ XML File
No Experiment
Connection Status Here
Script Status
run next



Attached to Floodwatch/ACSAC: active

local.outputlist completed

Script Status: (0 queued)



Participating Nodes and Settings

Clients	client
Servers	server
Thinking Time	minmax(1,1)
File Sizes	pareto(1.5,10)

Specific Variables

Var	Value

☑ Direct

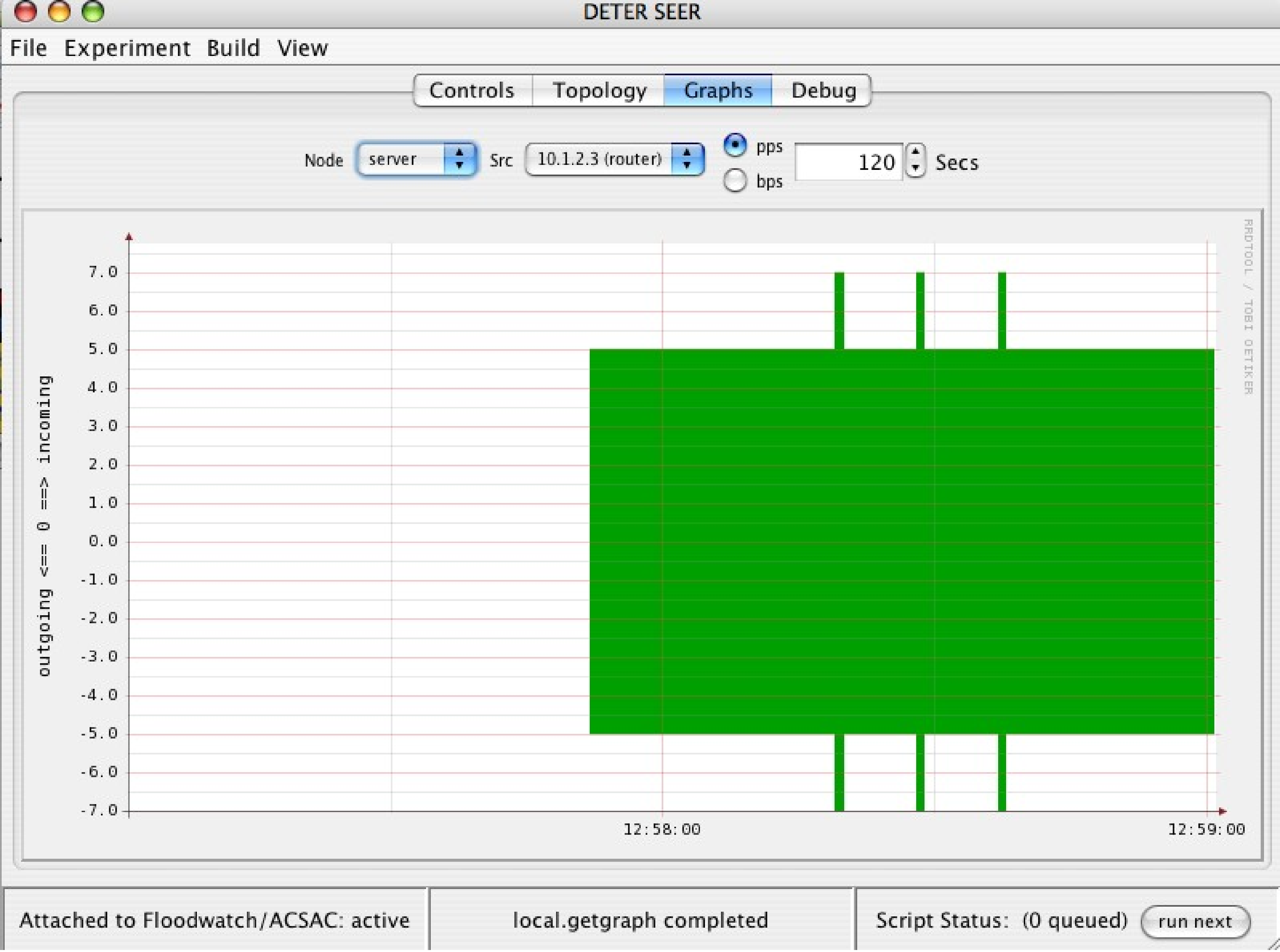
□ Perl Script

□ XML File

Attached to Floodwatch/ACSAC: active

local.outputlist completed

Script Status: (0 queued)



Node server

Src 10.1.2.3 (router)

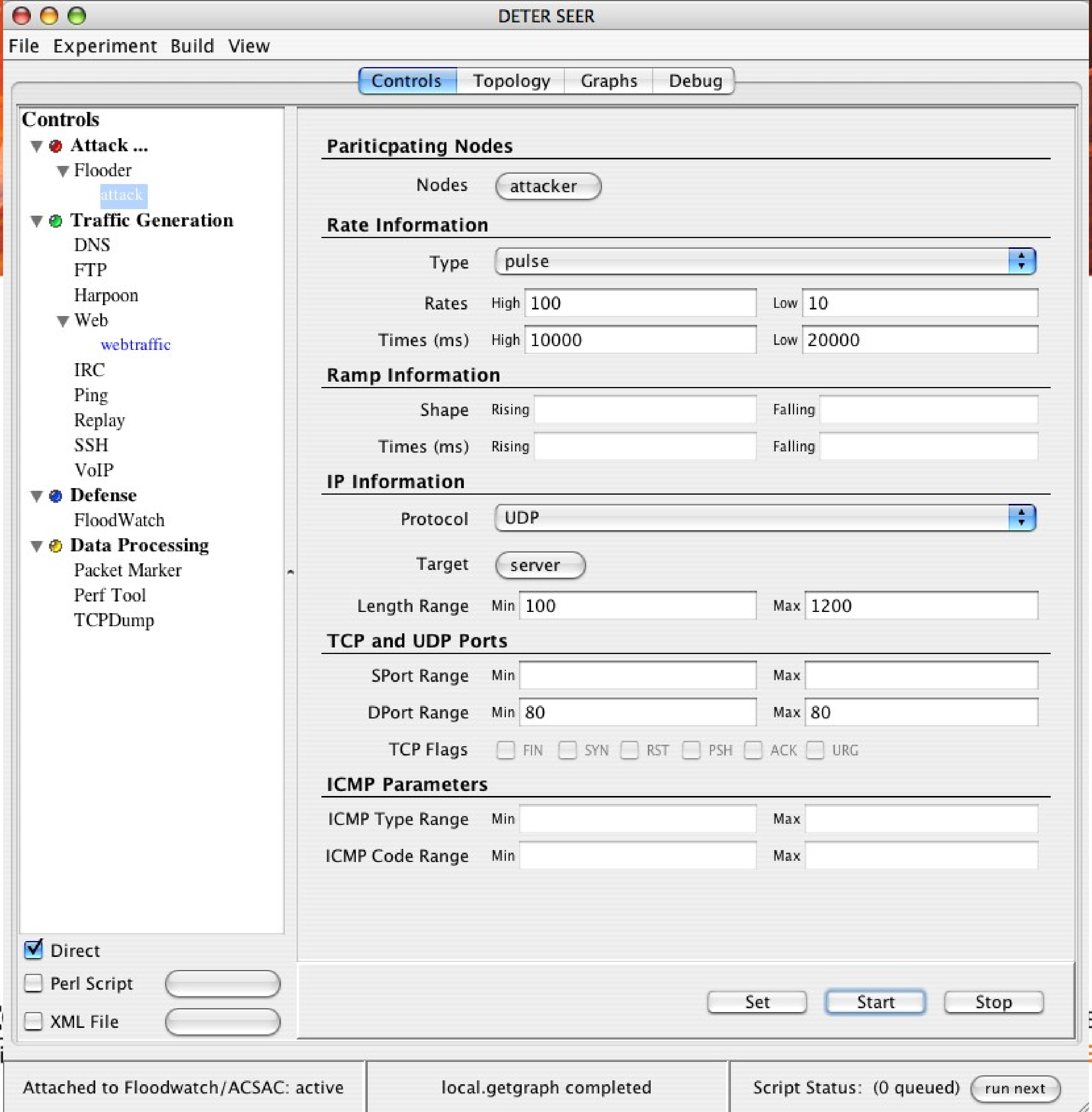
● pps
○ bps

120 Secs

Attached to Floodwatch/ACSAC: active

local.getgraph completed

Script Status: (0 queued)



☑ Direct
□ Perl Script
□ XML File

Particpating Nodes

Nodes: attacker

Rate Information

Type: pulse

Rates	High	100	Low	10
Times (ms)	High	10000	Low	20000

Ramp Information

Shape	Rising		Falling	
Times (ms)	Rising		Falling	

IP Information

Protocol: UDP

Target: server

Length Range	Min	100	Max	1200

TCP and UDP Ports

SPort Range	Min		Max	
DPort Range	Min	80	Max	80

TCP Flags: □ FIN □ SYN □ RST □ PSH □ ACK □ URG

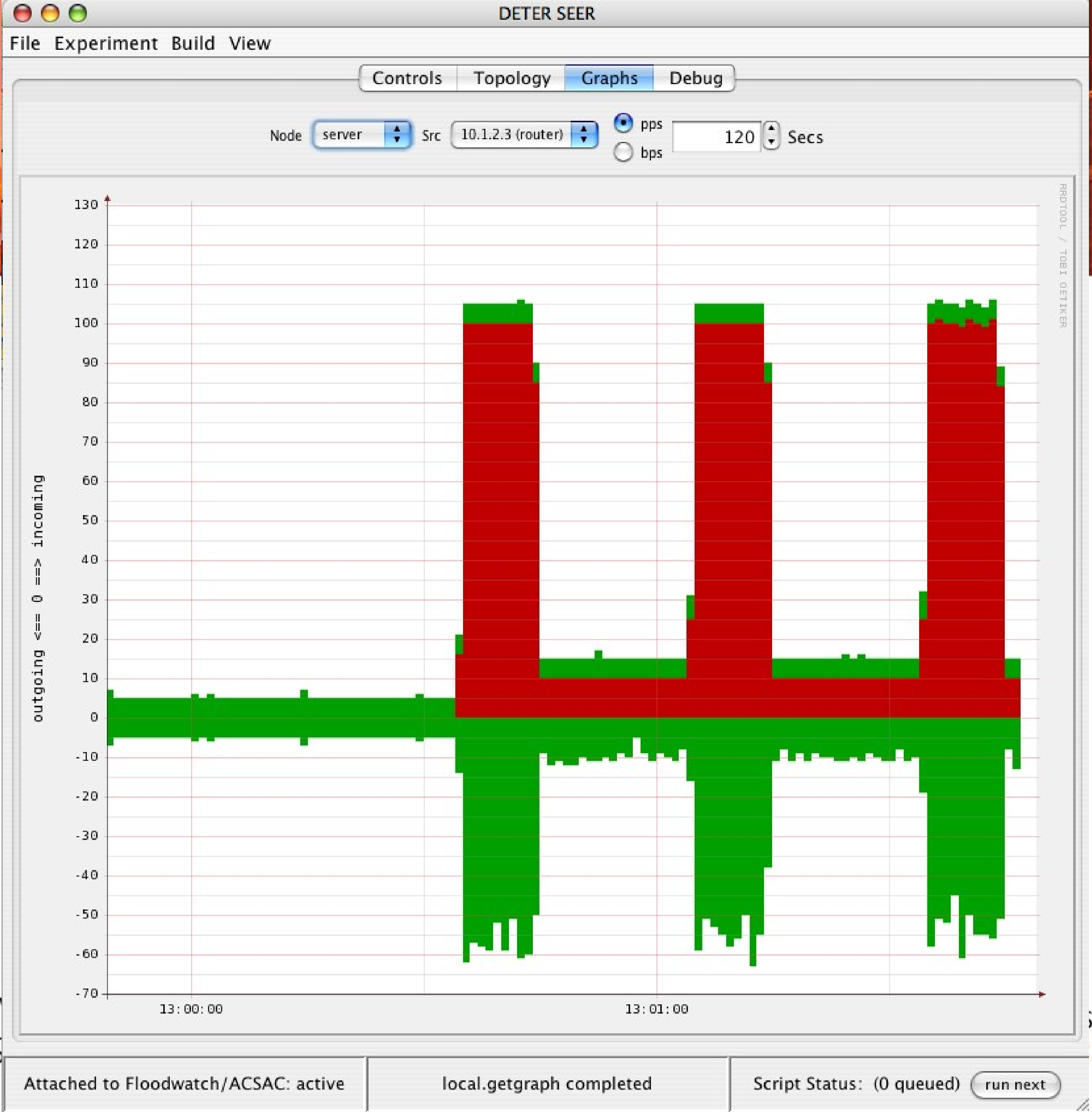
ICMP Parameters

ICMP Type Range	Min		Max	
ICMP Code Range	Min		Max	

Attached to Floodwatch/ACSAC: active

local.getgraph completed

Script Status: (0 queued)



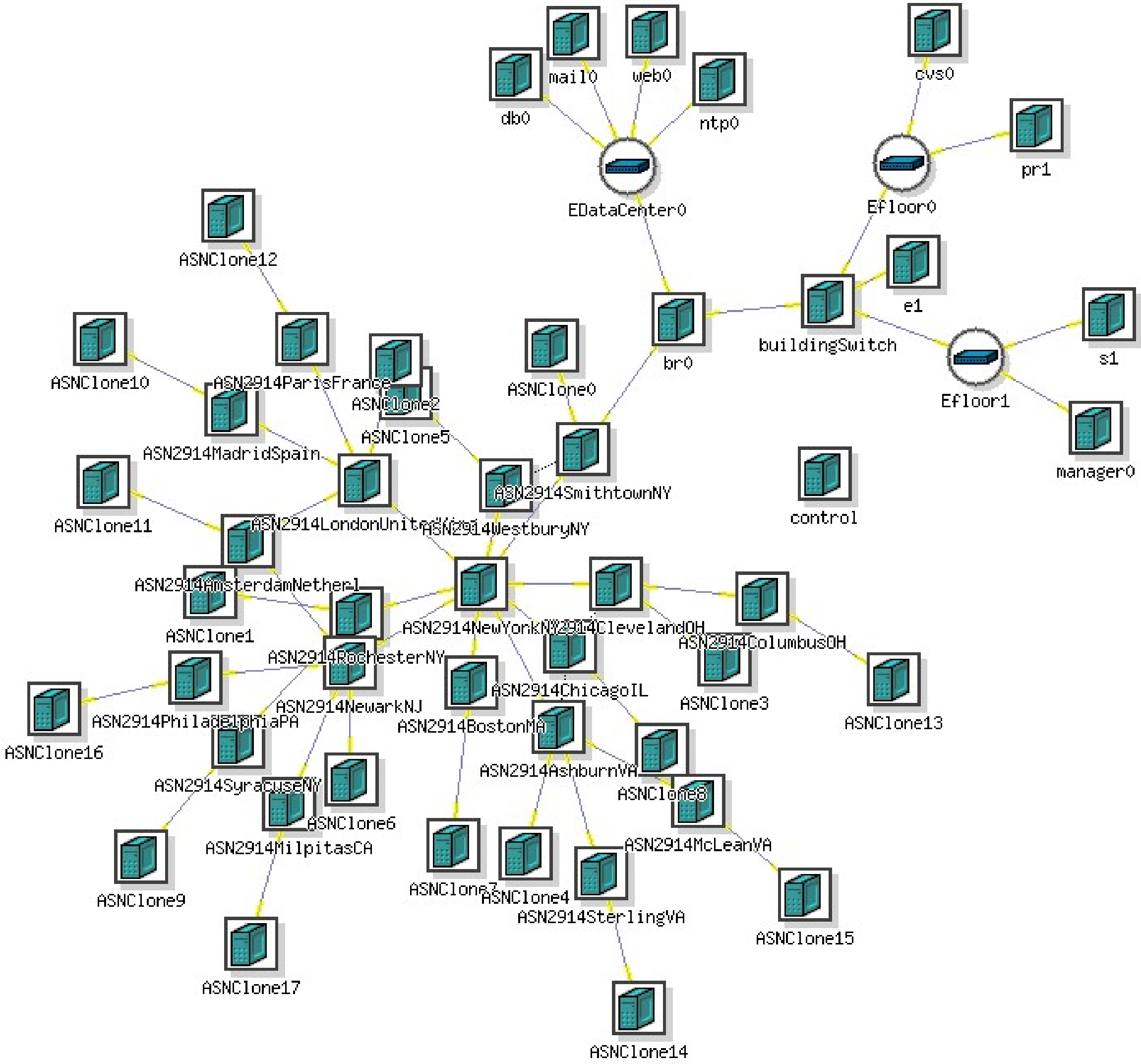
Node server Src 10.1.2.3 (router) ● pps ○ bps 120 Secs

Attached to Floodwatch/ACSAC: active

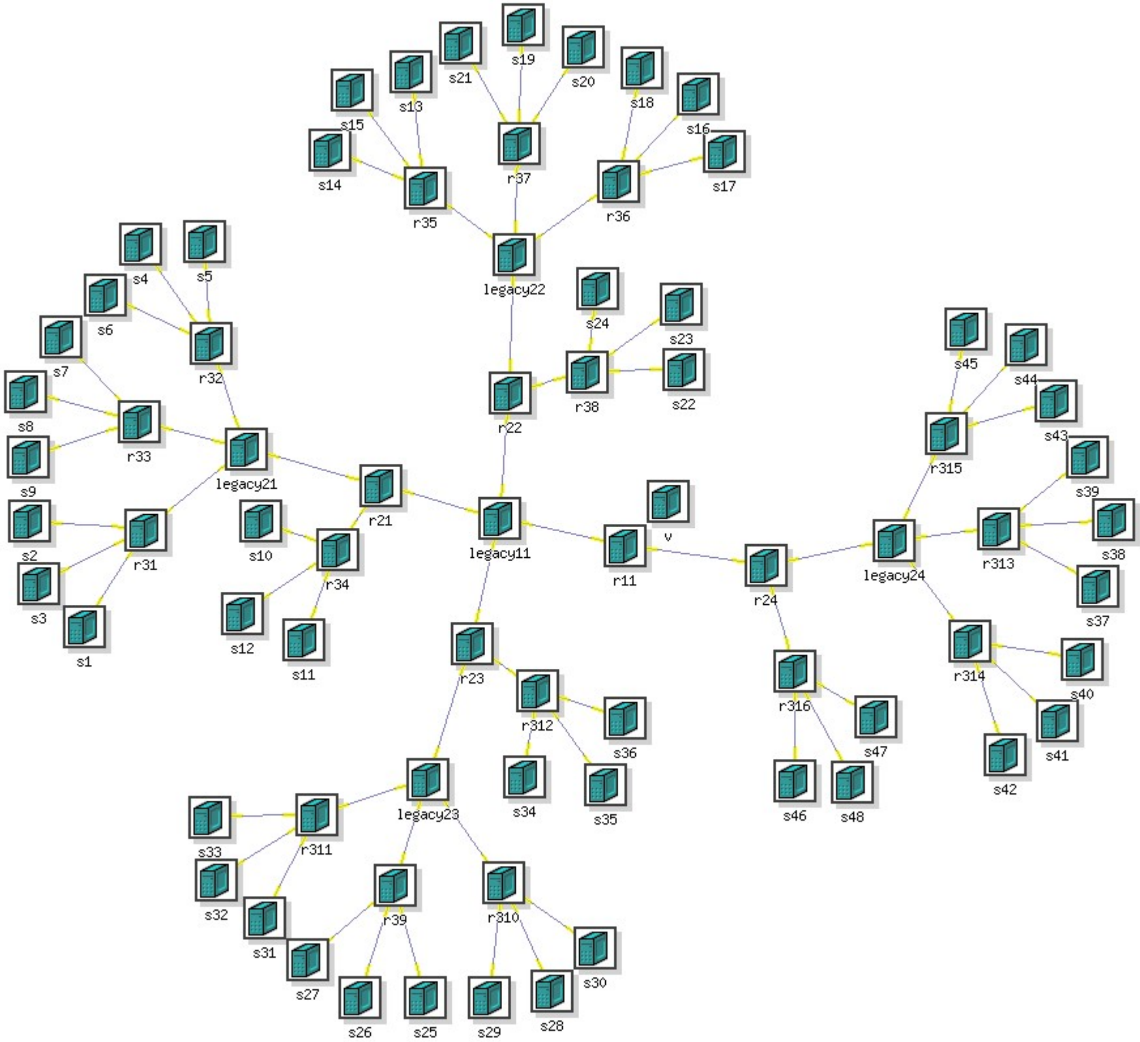
local.getgraph completed

Script Status: (0 queued)

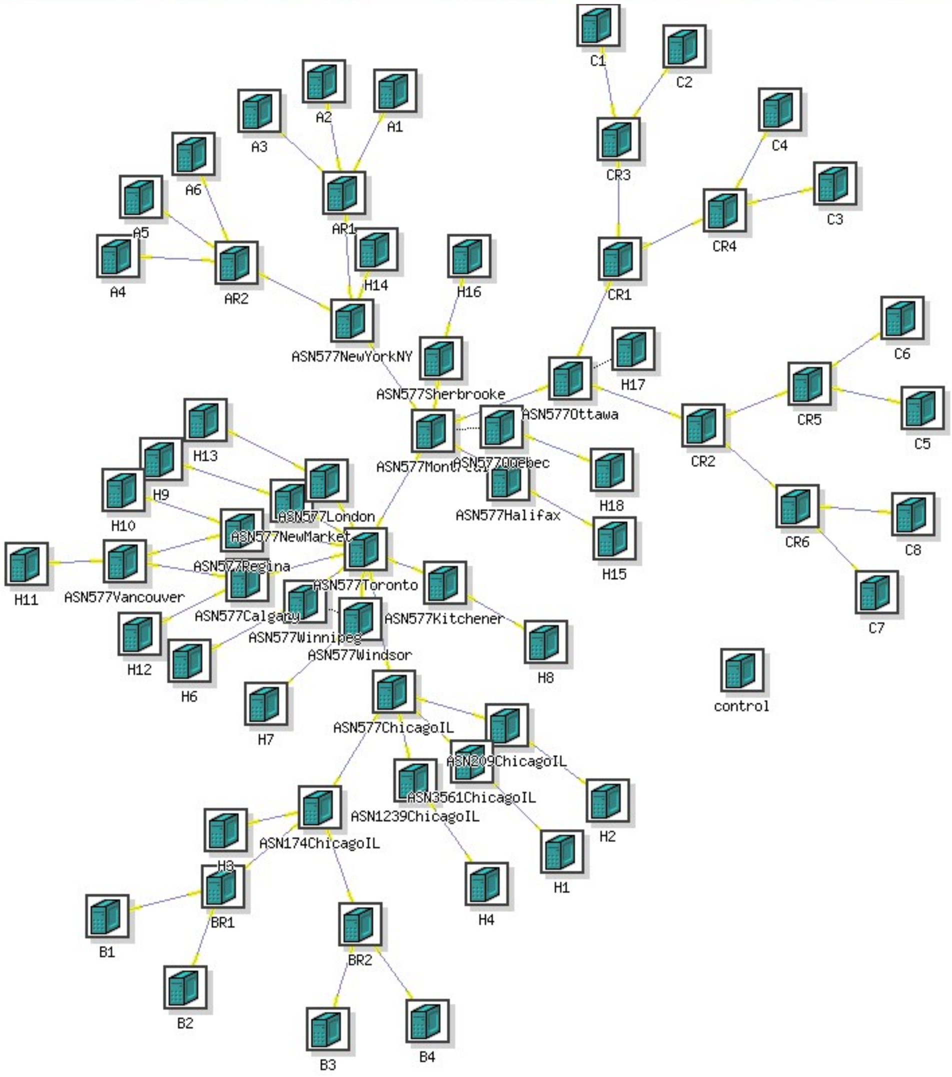
More Complex Experiments



More Complex Experiments



More Complex Experiments



New Developments

- **Federation with other testbeds**
  - Current experiments run with minimal changes
  - Ran 210-node experiment on 3 testbeds: DETER (80), Emulab(70), WAIL (60)
- **Support for risky experiments**
  - Experiments will be able to run self-propagating code (e.g., Slammer) AND preserve outside connectivity
  - Experiments will be able to interact with the outside directly
  - Containment techniques to guarantee security of testbed and security to the Internet
  - Building a library of malicious code via Metasploit

For More Information

- **DETERlab Page**
  - http://www.deterlab.net
  - Log on to testbed, documentation and tutorials
- **DETER Project Page**
  - http://www.isi.edu/deter
  - Information about DETER project and its results
- **My email**
  - Ted Faber (faber@isi.edu)