The Bro Network Security Monitor

Robin Sommer

International Computer Science Institute, &
Lawrence Berkeley National Laboratory

robin@icsi.berkeley.edu
http://www.icir.org/robin

What is Bro?

What is Bro?

Packet Capture

What is Bro?

Packet Capture

Traffic Inspection

What is Bro?

Packet Capture

Traffic Inspection

Attack Detection

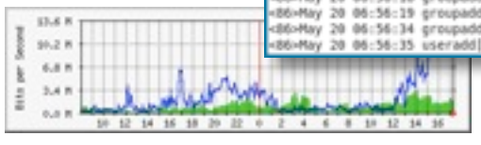
What is Bro?

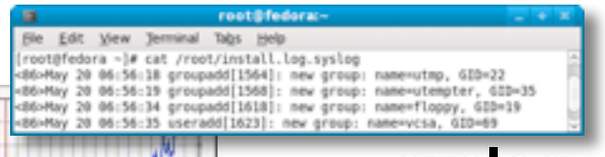
Packet Capture

Traffic Inspection

Attack Detection

NetFlow





syslog

Log Recording

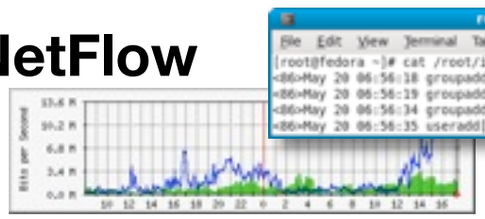
What is Bro?

Packet Capture

Traffic Inspection

Attack Detection

NetFlow



syslog

Log Recording

Flexibility
Abstraction
Data Structures

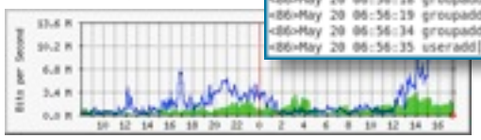
What is Bro?

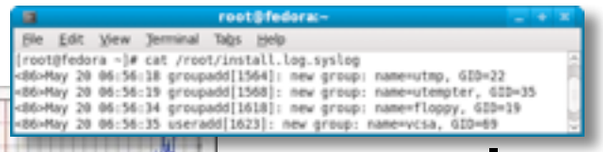
Packet Capture

Traffic Inspection

Attack Detection

NetFlow





syslog

Log Recording

Flexibility
Abstraction
Data Structures

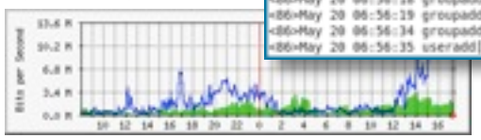
What is Bro?

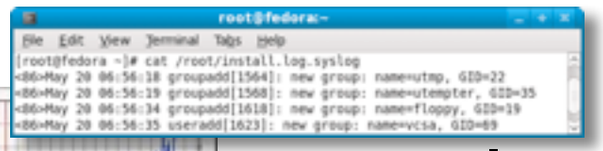
Packet Capture

Traffic Inspection

Attack Detection

NetFlow





syslog

Log Recording

Flexibility
Abstraction
Data Structures

What is Bro?

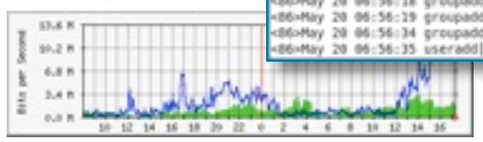
Packet Capture

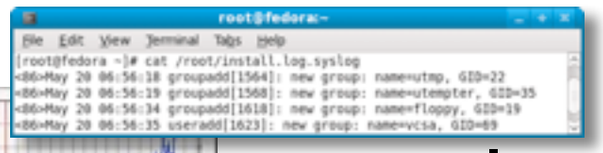
Traffic Inspection

Attack Detection

"Domain-specific Python"

NetFlow





syslog

Log Recording

Flexibility
Abstraction
Data Structures

Philosophy

Fundamentally different from other IDS.

Need to reset your idea of an IDS before starting to use Bro.

Real-time network analysis *framework.*

Primarily an IDS, but many use it for general traffic analysis.

Can accommodate a range of detection approaches.

Policy-neutral at the core.

Highly stateful.

Tracks extensive application-layer network state.

Supports forensics.

Extensively logs what it sees.

Bro History

Vern writes 1st line of code

Bro History

1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012

Vern writes 1st line of code

LBNL starts using Bro operationally

v0.2
1st CHANGES entry

v0.4
HTTP analysis
Scan detector
IP fragments
Linux support

v0.6
RegExps
Login analysis

v0.7a48
Consistent CHANGES

v0.7a90
Profiling
State Mgmt

v0.7a175/0.8aX
Signatures
SMTP
IPv6 support
User manual

0.8a37
Communication
Persistence
Namespaces
Log Rotation

v0.8aX/0.9aX
SSL/SMB
STABLE releases
BroLite

v1.0
BinPAC
IRC/RPC analyzers
64-bit support
Sane version numbers

v1.1/v1.2
when Stmt
Resource tuning
Broccoli
DPD

v1.3
Ctor expressions
GeoIP
Conn Compressor

v1.4
DHCP/BitTorrent
HTTP entities
NetFlow
Bro Lite Deprecated

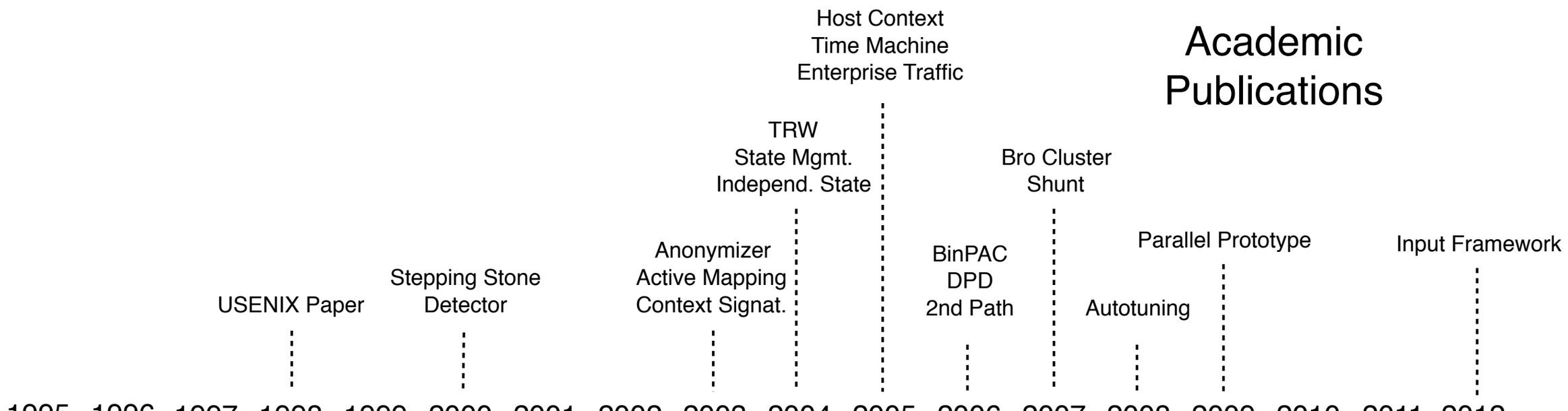
v1.5
BroControl

Bro SDCI

Bro 2.0
New Scripts

Bro 2.1
IPv6
Input Framework

Bro History


Academic Publications
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
USENIX Paper
Stepping Stone Detector
Anonymizer Active Mapping Context Signat.
TRW State Mgmt. Indepen. State
Host Context Time Machine Enterprise Traffic
BinPAC DPD 2nd Path
Bro Cluster Shunt
Autotuning
Parallel Prototype
Input Framework
Vern writes 1st line of code
LBNL starts using Bro operationally
v0.2 1st CHANGES entry
v0.4 HTTP analysis Scan detector IP fragments Linux support
v0.6 RegExps Login analysis
v0.7a48 Consistent CHANGES
v0.7a90 Profiling State Mgmt
v0.7a175/0.8aX Signatures SMTP IPv6 support User manual
0.8a37 Communication Persistence Namespaces Log Rotation
v0.8aX/0.9aX SSL/SMB STABLE releases BroLite
v1.0 BinPAC IRC/RPC analyzers 64-bit support Sane version numbers
v1.1/v1.2 *when* Stmt Resource tuning Broccoli DPD
v1.3 Ctor expressions GeoIP Conn Compressor
v1.4 DHCP/BitTorrent HTTP entities NetFlow Bro Lite Deprecated
v1.5 BroControl
Bro SDCI
Bro 2.0 New Scripts
Bro 2.1 IPv6 Input Framework

"Who's Using It?"

Installations across the US

Universities
Research Labs
Supercomputer Centers
Industry

Examples

Lawrence Berkeley National Lab
Indiana University
National Center for Supercomputing Applications
National Center for Atmospheric Research

... and many more sites

Fully integrated into *Security Onion*

Popular security-oriented Linux distribution

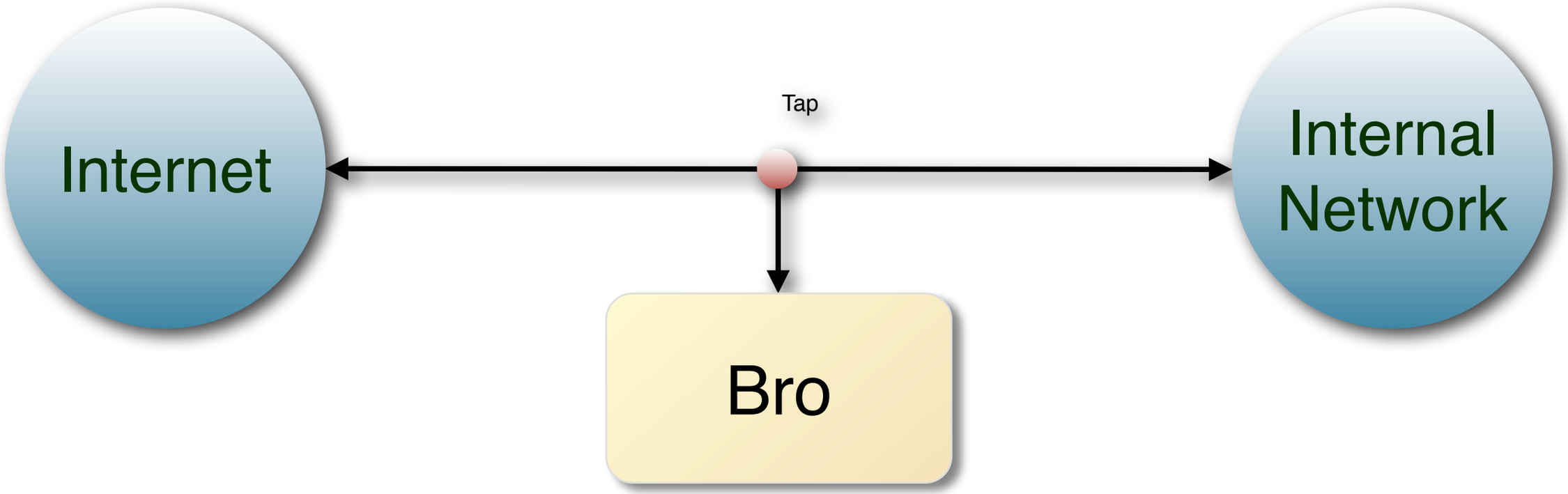
Recent User Meetings

Bro Workshop 2011 at NCSA
Bro Exchange 2012 at NCAR

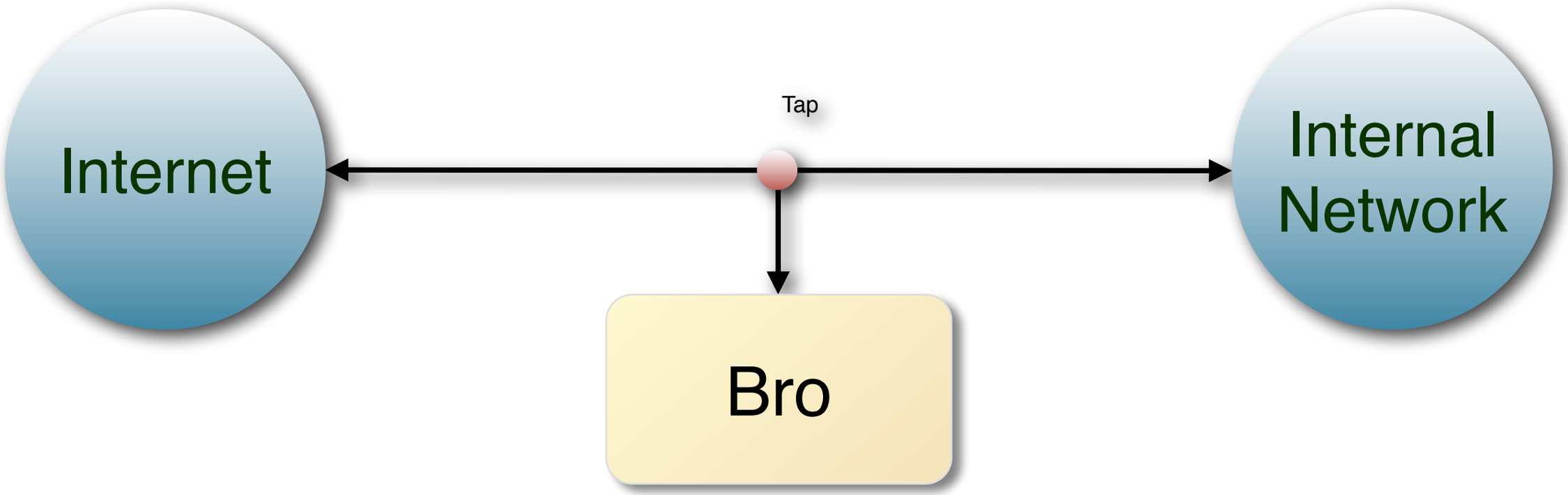
Each attended by about 50 operators from from 30-35 organizations

Deployment

Deployment



Deployment



Runs on commodity platforms.

- Standard PCs & NICs.
- Supports FreeBSD/Linux/OS X.

Example Logs

Example Logs

```
> bro -i en0
[ ... wait ...]
> cat conn.log
```

Example Logs

```
> bro -i en0
[ ... wait ...]
> cat conn.log
```

#fields ts	*id.orig_h*	*id.orig_p*	*id.resp_h*	*id.resp_p*	*proto*	*service*	*duration*
1144876741.1198	*192.150.186.169*	*53115*	*82.94.237.218*	*80*	*tcp*	*http*	*16.14929*
1144876612.6063	192.150.186.169	53090	198.189.255.82	80	tcp	http	4.437460
1144876596.5597	192.150.186.169	53051	193.203.227.129	80	tcp	http	0.372440
1144876606.7789	192.150.186.169	53082	198.189.255.73	80	tcp	http	0.597711
1144876741.4693	**192.150.186.169**	**53116**	**82.94.237.218**	**80**	**tcp**	**http**	**16.02667**
1144876745.6102	**192.150.186.169**	**53117**	**66.102.7.99**	**80**	**tcp**	**http**	**1.004346**
1144876605.6847	192.150.186.169	53075	207.151.118.143	80	tcp	http	0.029663

Example Logs

```
> bro -i en0
[ ... wait ...]
> cat conn.log
```

#fields ts	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service	duration
1144876741.1198	*192.150.186.169*	*53115*	*82.94.237.218*	*80*	*tcp*	*http*	*16.14929*
1144876612.6063	192.150.186.169	53090	198.189.255.82	80	tcp	http	4.437460
1144876596.5597	192.150.186.169	53051	193.203.227.129	80	tcp	http	0.372440
1144876606.7789	192.150.186.169	53082	198.189.255.73	80	tcp	http	0.597711
1144876741.4693	**192.150.186.169**	**53116**	**82.94.237.218**	**80**	**tcp**	**http**	**16.02667**
1144876745.6102	**192.150.186.169**	**53117**	**66.102.7.99**	**80**	**tcp**	**http**	**1.004346**
1144876605.6847	192.150.186.169	53075	207.151.118.143	80	tcp	http	0.029663

```
> cat http.log
```

Example Logs

```
> bro -i en0
[ ... wait ...]
> cat conn.log
```

#fields ts	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service	duration
1144876741.1198	192.150.186.169	53115	82.94.237.218	80	tcp	http	16.14929
1144876612.6063	192.150.186.169	53090	198.189.255.82	80	tcp	http	4.437460
1144876596.5597	192.150.186.169	53051	193.203.227.129	80	tcp	http	0.372440
1144876606.7789	192.150.186.169	53082	198.189.255.73	80	tcp	http	0.597711
1144876741.4693	**192.150.186.169**	**53116**	**82.94.237.218**	**80**	**tcp**	**http**	**16.02667**
1144876745.6102	**192.150.186.169**	**53117**	**66.102.7.99**	**80**	**tcp**	**http**	**1.004346**
1144876605.6847	192.150.186.169	53075	207.151.118.143	80	tcp	http	0.029663

```
> cat http.log
```

#fields ts	id.orig_h	id.orig_p [...]	host	uri	status_code	user_agent [...]
1144876741.6335	192.150.186.169	53116	docs.python.org	/lib/lib.css	200	Mozilla/5.0
1144876742.1687	192.150.186.169	53116	docs.python.org	/icons/previous.png	304	Mozilla/5.0
1144876741.2838	192.150.186.169	53115	docs.python.org	/lib/lib.html	200	Mozilla/5.0
1144876742.3337	192.150.186.169	53116	docs.python.org	/icons/up.png	304	Mozilla/5.0
1144876742.3337	192.150.186.169	53116	docs.python.org	/icons/next.png	304	Mozilla/5.0
1144876742.3337	192.150.186.169	53116	docs.python.org	/icons/contents.png	304	Mozilla/5.0
1144876742.3337	192.150.186.169	53116	docs.python.org	/icons/modules.png	304	Mozilla/5.0
1144876742.3338	192.150.186.169	53116	docs.python.org	/icons/index.png	304	Mozilla/5.0
1144876745.6144	192.150.186.169	53117	www.google.com	/	200	Mozilla/5.0

Example Logs

```
> bro -i en0
[ ... wait ...]
> cat conn.log
```

```
#fields ts          id.orig_h          id.orig_p  id.resp_h          id.resp_p proto  service  duration
1144876741.1198  192.150.186.169 53115      82.94.237.218   80        tcp    http     16.14929
1144876612.6063  192.150.186.169 53090      198.189.255.82  80        tcp    http     4.437460
```

```
[...] host                uri                        status_code  user_agent [...]
      docs.python.org     /lib/lib.css               200          Mozilla/5.0
      docs.python.org     /icons/previous.png        304          Mozilla/5.0
      docs.python.org     /lib/lib.html              200          Mozilla/5.0
      docs.python.org     /icons/up.png              304          Mozilla/5.0
      docs.python.org     /icons/next.png            304          Mozilla/5.0
      docs.python.org     /icons/contents.png        304          Mozilla/5.0
      docs.python.org     /icons/modules.png         304          Mozilla/5.0
      docs.python.org     /icons/index.png           304          Mozilla/5.0
       www.google.com     /                          200          Mozilla/5.0
```

```
1144876742.3338  192.150.186.169  53116        docs.python.org  /icons/index.png  304        Mozilla/5.0
1144876745.6144  192.150.186.169  53117         www.google.com  /                 200        Mozilla/5.0
```

Identifying HTTP Servers

Identifying HTTP Servers

Server Addresses

```
a198-189-255-200.deploy.akamaitechnolgies.com
a198-189-255-216.deploy.akamaitechnolgies.com
a198-189-255-217.deploy.akamaitechnolgies.com
a198-189-255-230.deploy.akamaitechnolgies.com
a198-189-255-225.deploy.akamaitechnolgies.com
a198-189-255-206.deploy.akamaitechnolgies.com
a198-189-255-201.deploy.akamaitechnolgies.com
a198-189-255-223.deploy.akamaitechnolgies.com
                  72.21.91.19
a198-189-255-208.deploy.akamaitechnolgies.com
a198-189-255-207.deploy.akamaitechnolgies.com
          nuq04s07-in-f27.1e100.net
 a184-28-157-55.deploy.akamaitechnologies.com
a198-189-255-224.deploy.akamaitechnolgies.com
a198-189-255-209.deploy.akamaitechnolgies.com
a198-189-255-222.deploy.akamaitechnolgies.com
a198-189-255-214.deploy.akamaitechnolgies.com
          nuq04s06-in-f27.1e100.net
        upload-lb.pmtpa.wikimedia.org
          nuq04s08-in-f27.1e100.net
```

Identifying HTTP Servers

Server Addresses

a198-189-255-200.deploy.akamaitechnolgies.com
a198-189-255-216.deploy.akamaitechnolgies.com
a198-189-255-217.deploy.akamaitechnolgies.com
a198-189-255-230.deploy.akamaitechnolgies.com
a198-189-255-225.deploy.akamaitechnolgies.com
a198-189-255-206.deploy.akamaitechnolgies.com
a198-189-255-201.deploy.akamaitechnolgies.com
a198-189-255-223.deploy.akamaitechnolgies.com
72.21.91.19
a198-189-255-208.deploy.akamaitechnolgies.com
a198-189-255-207.deploy.akamaitechnolgies.com
nuq04s07-in-f27.1e100.net
a184-28-157-55.deploy.akamaitechnologies.com
a198-189-255-224.deploy.akamaitechnolgies.com
a198-189-255-209.deploy.akamaitechnolgies.com
a198-189-255-222.deploy.akamaitechnolgies.com
a198-189-255-214.deploy.akamaitechnolgies.com
nuq04s06-in-f27.1e100.net
upload-lb.pmtpa.wikimedia.org
nuq04s08-in-f27.1e100.net

HTTP Host Headers

ad.doubleclick.net
ad.yieldmanager.com
b.scorecardresearch.com
clients1.google.com
googleads.g.doubleclick.net
graphics8.nytimes.com
l.yimg.com
liveupdate.symanteccliveupdate.com
mt0.google.com
pixel.quantserve.com
platform.twitter.com
profile.ak.fbcdn.net
s0.2mdn.net
safebrowsing-cache.google.com
static.ak.fbcdn.net
swcdn.apple.com
upload.wikimedia.org
www.facebook.com
www.google-analytics.com
www.google.com

File Content

File Content

```
192.168.1.102   GET     /skins-1.5/common/images/magnify-clip.png       image/png       -
192.168.1.102   GET     /skins-1.5/monobook/external.png        image/png       -
192.168.1.102   GET     /softw/90/update/avg9infoavi.ctf        text/plain      -
192.168.1.102   GET     /softw/90/update/avg9infowin.ctf        text/plain      -
192.168.1.102   GET     /softw/90/update/u7avi1777u1705ff.bin   application/x-dosexec
                                                                0210a9516dd34abc481683f877bd8680
192.168.1.102   GET     /softw/90/update/u7avi1778u1705z7.bin   application/x-dosexec
                                                                9bd8e3a274d8ada852bc3d9736116bf6
192.168.1.102   GET     /softw/90/update/u7iavi2511u2510ff.bin  application/x-dosexec
                                                                5e63f63fd955207610a56dbd89d8688f
192.168.1.102   GET     /softw/90/update/u7iavi2512u2511z7.bin  application/x-dosexec
                                                                a8e1ef490967ef7eb6641bef9eed4003
192.168.1.102   GET     /softw/90/update/x8xplsb2_118c8.bin     application/x-dosexec
                                                                e6915411c5550e9fbf33ef15fed75e5a
192.168.1.102   GET     /softw/90/update/x8xplsc_149d148c8.bin  application/x-dosexec
                                                                db5b04f3c45da4c0686c678bfd0e241c
192.168.1.102   GET     /sports/        text/html       -
```

Software Logging

Software Logging

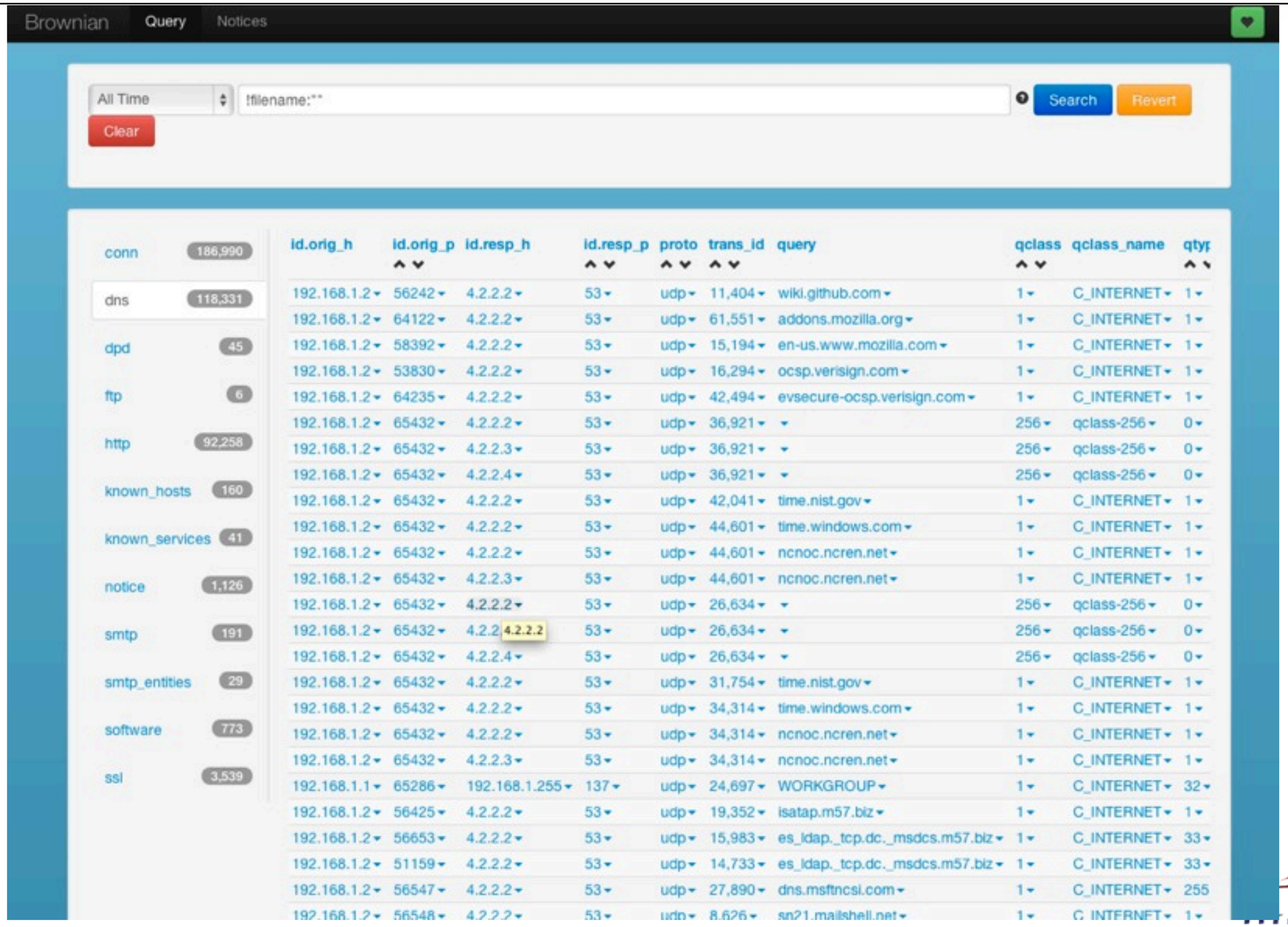
```
192.168.1.104   HTTP::BROWSER   Windows-Update-Agent    -       -       Windows-Update-Agent
65.54.95.64     HTTP::SERVER    Microsoft-IIS   6       0       Microsoft-IIS/6.0
65.54.95.64     HTTP::APPSERVER ASP.NET -       -       ASP.NET
65.55.184.16    HTTP::SERVER    Microsoft-IIS   7       0       Microsoft-IIS/7.0
65.55.184.16    HTTP::APPSERVER ASP.NET -       -       ASP.NET
192.168.1.102   HTTP::BROWSER   SCSDK   6       0       SCSDK-6.0.0
212.227.97.133  HTTP::SERVER    Apache  2       2       Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny3
212.227.97.133  HTTP::APPSERVER PHP     5       2       PHP/5.2.6-1+lenny3
87.106.1.47     HTTP::SERVER    Apache  2       2       Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny3
87.106.1.47     HTTP::APPSERVER PHP     5       2       PHP/5.2.6-1+lenny3
87.106.1.89     HTTP::SERVER    Apache  2       2       Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny3
87.106.1.89     HTTP::APPSERVER PHP     5       2       PHP/5.2.6-1+lenny3
87.106.12.47    HTTP::SERVER    Apache  2       2       Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny3
87.106.12.47    HTTP::APPSERVER PHP     5       2       PHP/5.2.6-1+lenny3
87.106.12.77    HTTP::SERVER    Apache  2       2       Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny3
87.106.12.77    HTTP::APPSERVER PHP     5       2       PHP/5.2.6-1+lenny3
87.106.66.233   HTTP::SERVER    Apache  2       0       Apache/2.0.54 (Debian GNU/Linux)
87.106.66.233   HTTP::APPSERVER PHP     4       3       PHP/4.3.10-22
87.106.9.29     HTTP::SERVER    Apache  2       2       Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny3
87.106.9.29     HTTP::APPSERVER PHP     5       2       PHP/5.2.6-1+lenny3
```

SSL Certificate Logging

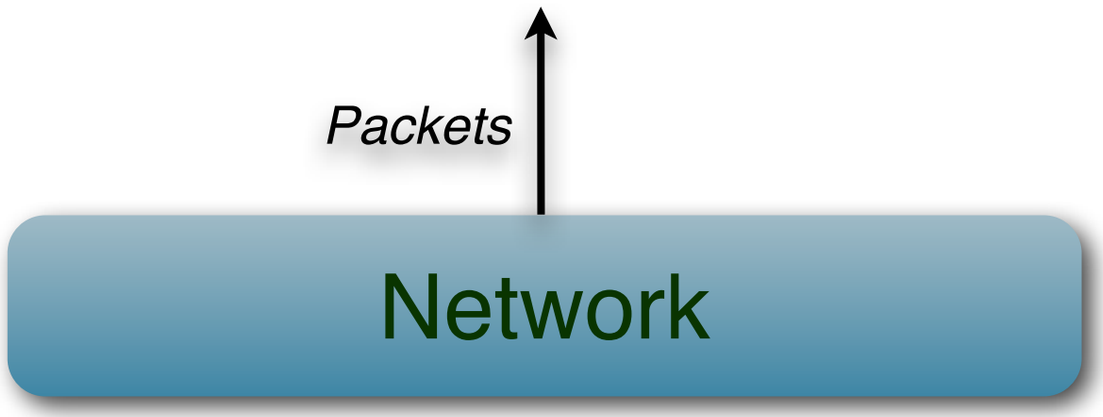
SSL Certificate Logging

```
65.55.184.16    CN=Microsoft Secure Server Authority,DC=redmond,DC=corp,DC=microsoft,DC=com
66.235.128.158  CN=Sun Microsystems Inc SSL CA,OU=Class 3 MPKI Secure Server CA,OU=VeriSign
65.55.184.155   CN=Microsoft Secure Server Authority,DC=redmond,DC=corp,DC=microsoft,DC=com
65.55.16.121    CN=Microsoft Secure Server Authority,DC=redmond,DC=corp,DC=microsoft,DC=com
65.54.186.79    CN=VeriSign Class 3 Extended Validation SSL CA,OU=Terms of use at
96.6.248.124    CN=Akamai Subordinate CA 3,O=Akamai Technologies Inc,C=US
96.6.245.186    CN=Akamai Subordinate CA 3,O=Akamai Technologies Inc,C=US
66.235.139.152  OU=Equifax Secure Certificate Authority,O=Equifax,C=US
65.54.234.75    CN=VeriSign Class 3 Secure Server CA,OU=Terms of use at
96.6.244.212    CN=Akamai Subordinate CA 3,O=Akamai Technologies Inc,C=US
216.223.0.208   CN=Network Solutions Certificate Authority,O=Network Solutions L.L.C.,C=US
98.137.50.24    OU=Equifax Secure Certificate Authority,O=Equifax,C=US
63.245.209.39   OU=Equifax Secure Certificate Authority,O=Equifax,C=US
65.55.184.27    CN=Microsoft Secure Server Authority,DC=redmond,DC=corp,DC=microsoft,DC=com
```

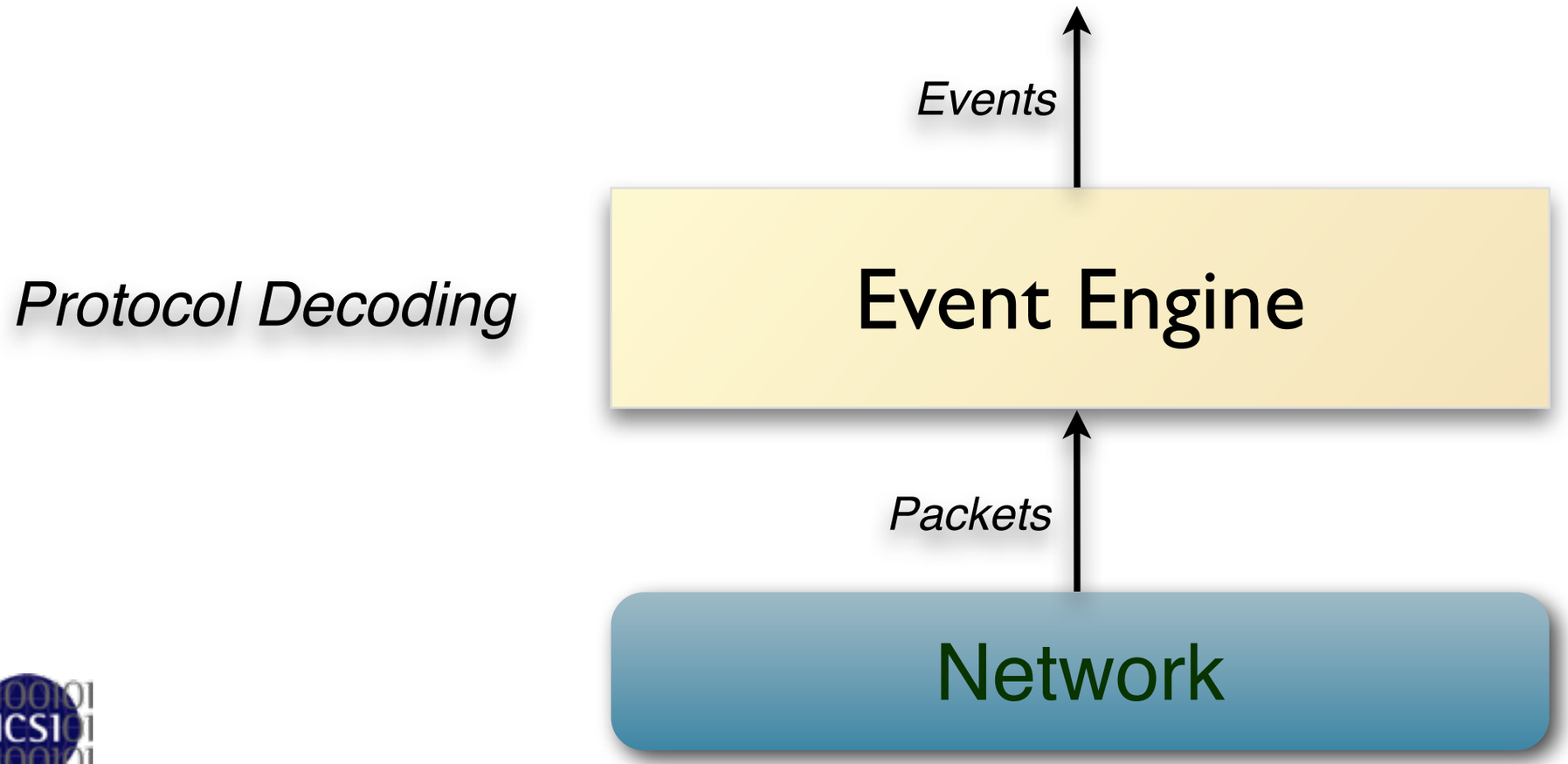
Brownian


Brownian
Query
Notices
All Time
!filename:*
Search
Revert
Clear
conn 186,990
dns 118,331
dpd 45
ftp 6
http 92,258
known_hosts 160
known_services 41
notice 1,126
smtp 191
smtp_entities 29
software 773
ssl 3,539
id.orig_h | id.orig_p | id.resp_h | id.resp_p | proto | trans_id | query | qclass | qclass_name | qtyp
192.168.1.2 | 56242 | 4.2.2.2 | 53 | udp | 11,404 | wiki.github.com | 1 | C_INTERNET | 1
192.168.1.2 | 64122 | 4.2.2.2 | 53 | udp | 61,551 | addons.mozilla.org | 1 | C_INTERNET | 1
192.168.1.2 | 58392 | 4.2.2.2 | 53 | udp | 15,194 | en-us.www.mozilla.com | 1 | C_INTERNET | 1
192.168.1.2 | 53830 | 4.2.2.2 | 53 | udp | 16,294 | ocsp.verisign.com | 1 | C_INTERNET | 1
192.168.1.2 | 64235 | 4.2.2.2 | 53 | udp | 42,494 | evsecure-ocsp.verisign.com | 1 | C_INTERNET | 1
192.168.1.2 | 65432 | 4.2.2.2 | 53 | udp | 36,921 | | 256 | qclass-256 | 0
192.168.1.2 | 65432 | 4.2.2.3 | 53 | udp | 36,921 | | 256 | qclass-256 | 0
192.168.1.2 | 65432 | 4.2.2.4 | 53 | udp | 36,921 | | 256 | qclass-256 | 0
192.168.1.2 | 65432 | 4.2.2.2 | 53 | udp | 42,041 | time.nist.gov | 1 | C_INTERNET | 1
192.168.1.2 | 65432 | 4.2.2.2 | 53 | udp | 44,601 | time.windows.com | 1 | C_INTERNET | 1
192.168.1.2 | 65432 | 4.2.2.2 | 53 | udp | 44,601 | ncnoc.ncren.net | 1 | C_INTERNET | 1
192.168.1.2 | 65432 | 4.2.2.3 | 53 | udp | 44,601 | ncnoc.ncren.net | 1 | C_INTERNET | 1
192.168.1.2 | 65432 | 4.2.2.2 | 53 | udp | 26,634 | | 256 | qclass-256 | 0
192.168.1.2 | 65432 | 4.2.2.2 | 53 | udp | 26,634 | | 256 | qclass-256 | 0
192.168.1.2 | 65432 | 4.2.2.4 | 53 | udp | 26,634 | | 256 | qclass-256 | 0
192.168.1.2 | 65432 | 4.2.2.2 | 53 | udp | 31,754 | time.nist.gov | 1 | C_INTERNET | 1
192.168.1.2 | 65432 | 4.2.2.2 | 53 | udp | 34,314 | time.windows.com | 1 | C_INTERNET | 1
192.168.1.2 | 65432 | 4.2.2.2 | 53 | udp | 34,314 | ncnoc.ncren.net | 1 | C_INTERNET | 1
192.168.1.2 | 65432 | 4.2.2.3 | 53 | udp | 34,314 | ncnoc.ncren.net | 1 | C_INTERNET | 1
192.168.1.1 | 65286 | 192.168.1.255 | 137 | udp | 24,697 | WORKGROUP | 1 | C_INTERNET | 32
192.168.1.2 | 56425 | 4.2.2.2 | 53 | udp | 19,352 | isatap.m57.biz | 1 | C_INTERNET | 1
192.168.1.2 | 56653 | 4.2.2.2 | 53 | udp | 15,983 | es_ldap._tcp.dc._msdcs.m57.biz | 1 | C_INTERNET | 33
192.168.1.2 | 51159 | 4.2.2.2 | 53 | udp | 14,733 | es_ldap._tcp.dc._msdcs.m57.biz | 1 | C_INTERNET | 33
192.168.1.2 | 56547 | 4.2.2.2 | 53 | udp | 27,890 | dns.msftncsi.com | 1 | C_INTERNET | 255
4.2.2.2

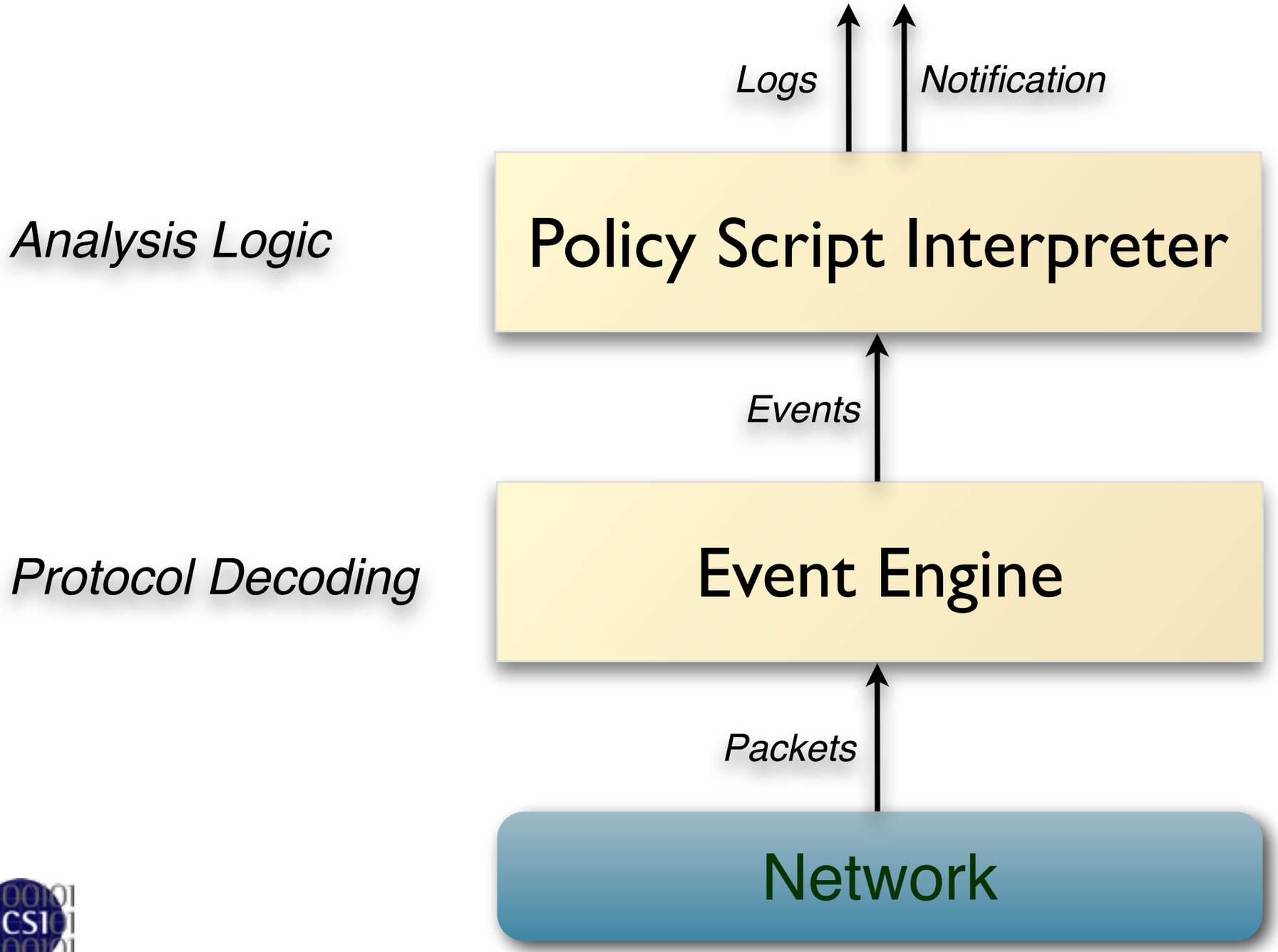
Architecture



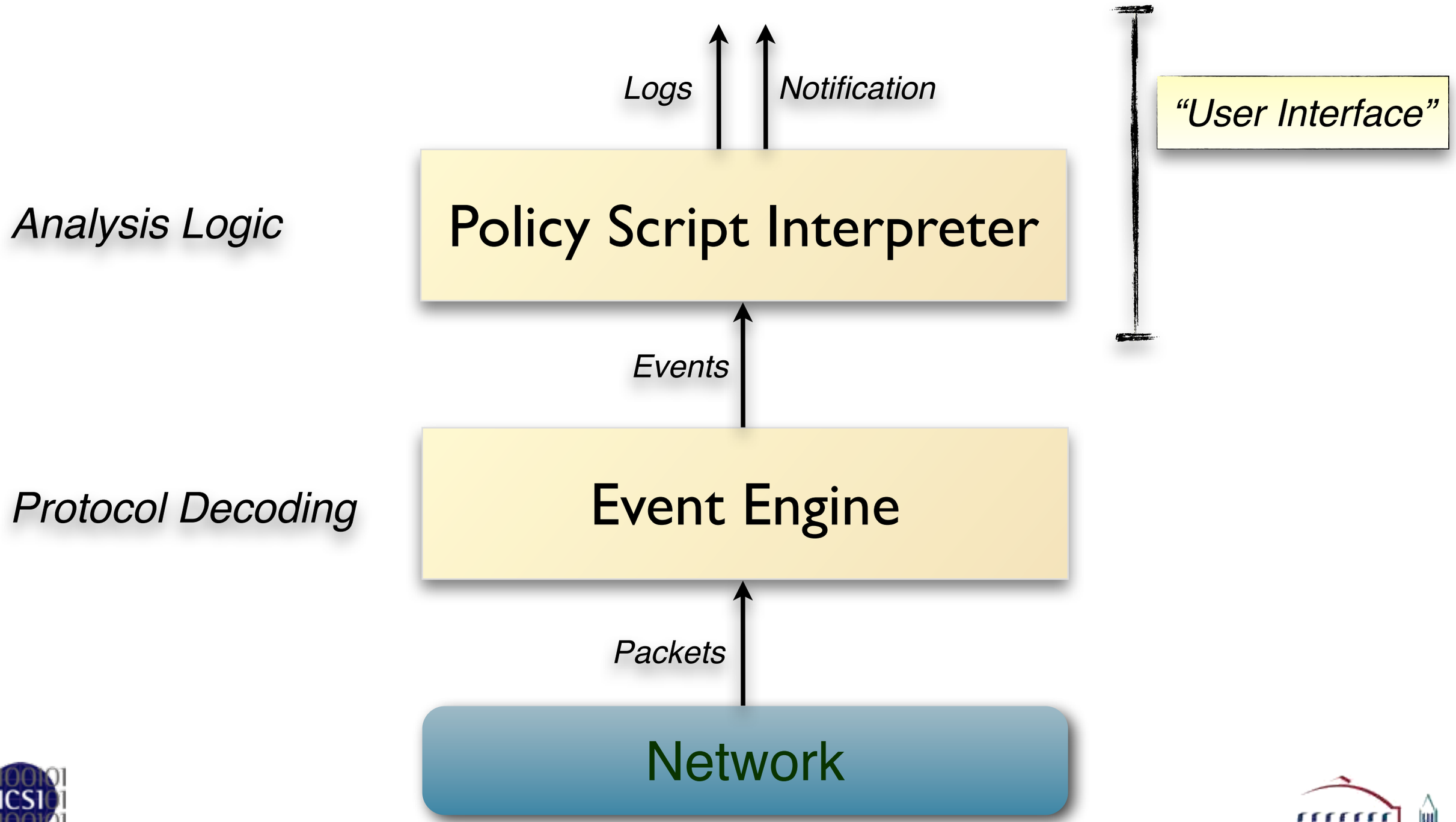
Architecture



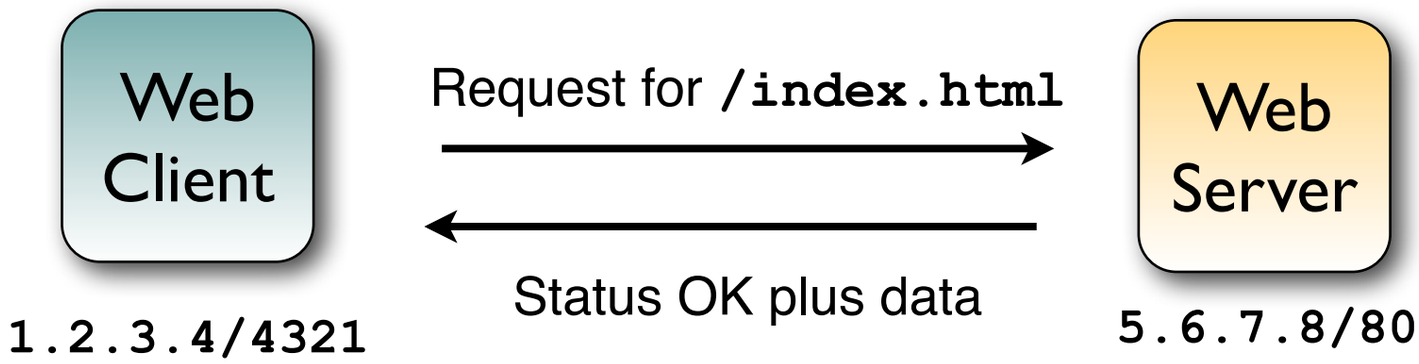
Architecture



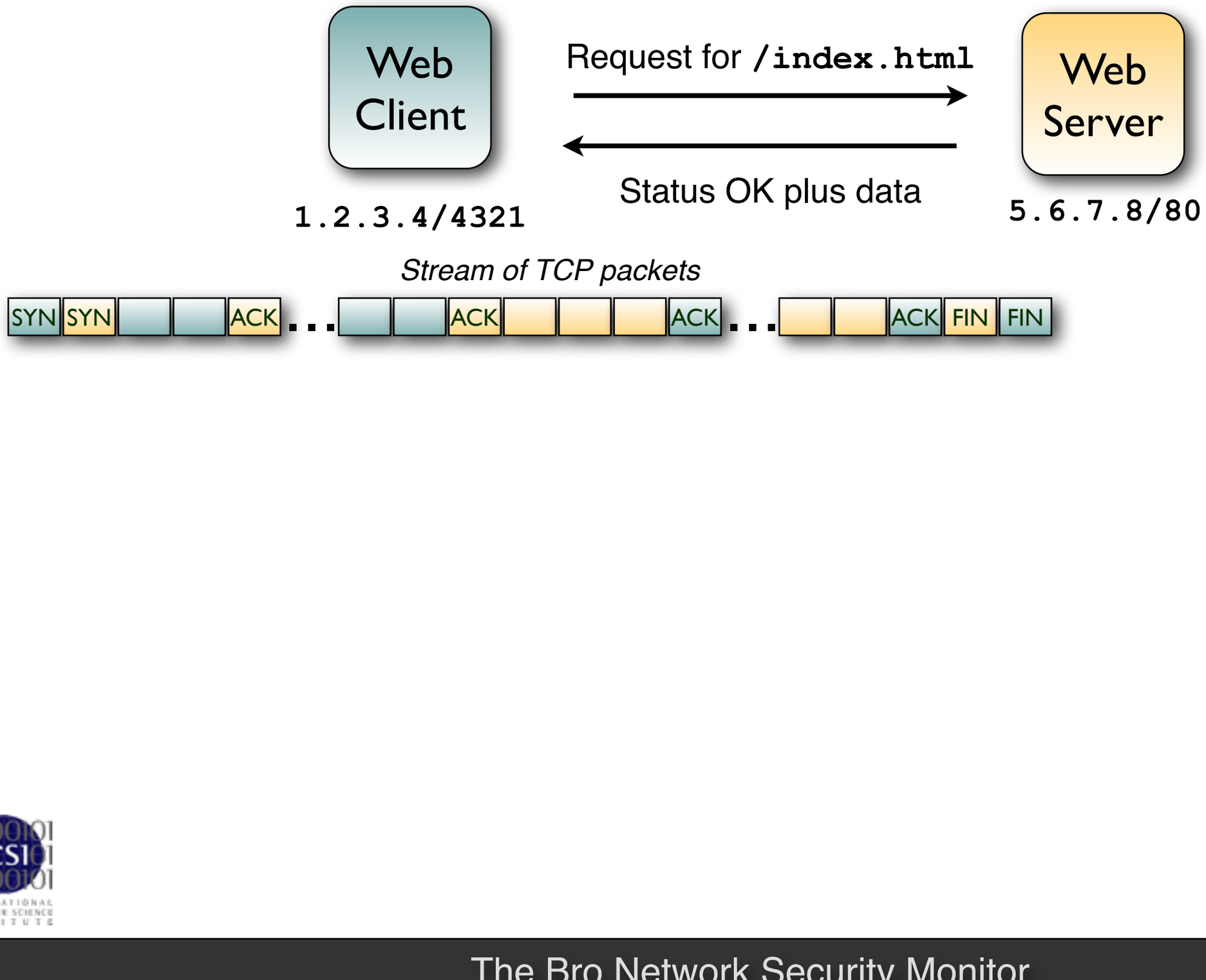
Architecture



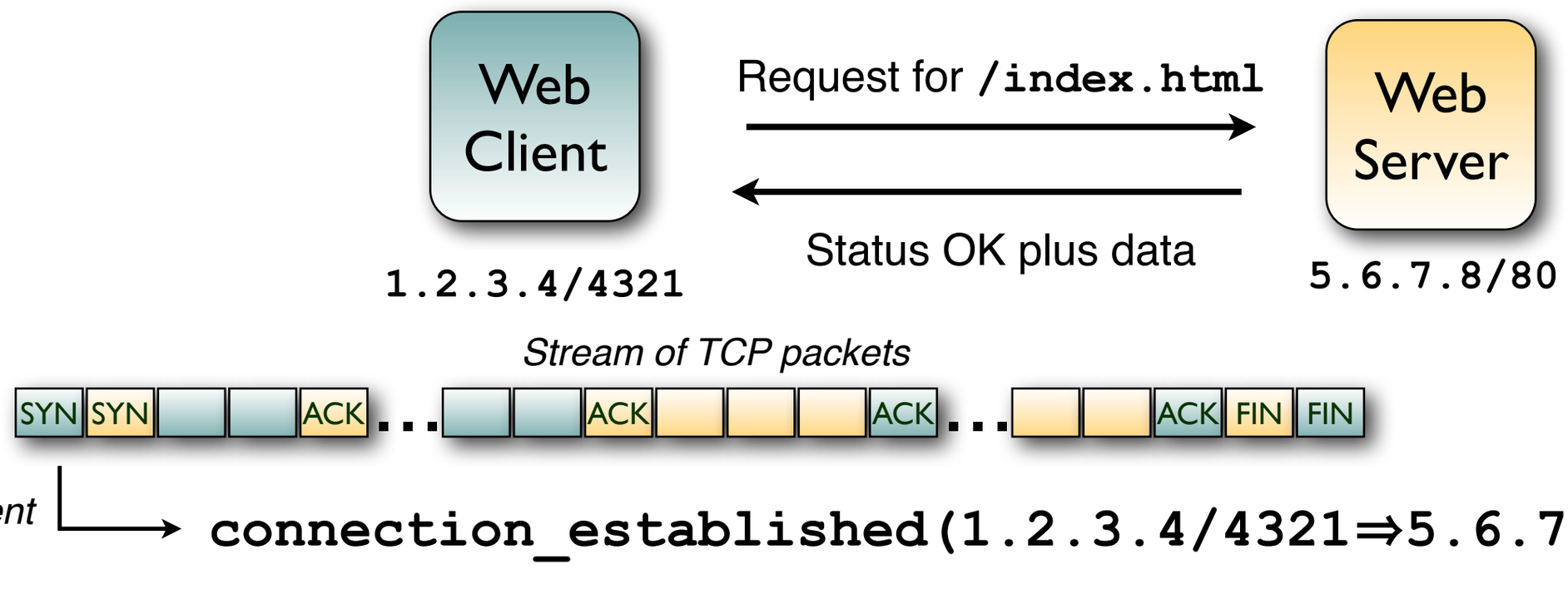
Event Model


Web Client
Request for /index.html
Web Server
Status OK plus data
1.2.3.4/4321
5.6.7.8/80

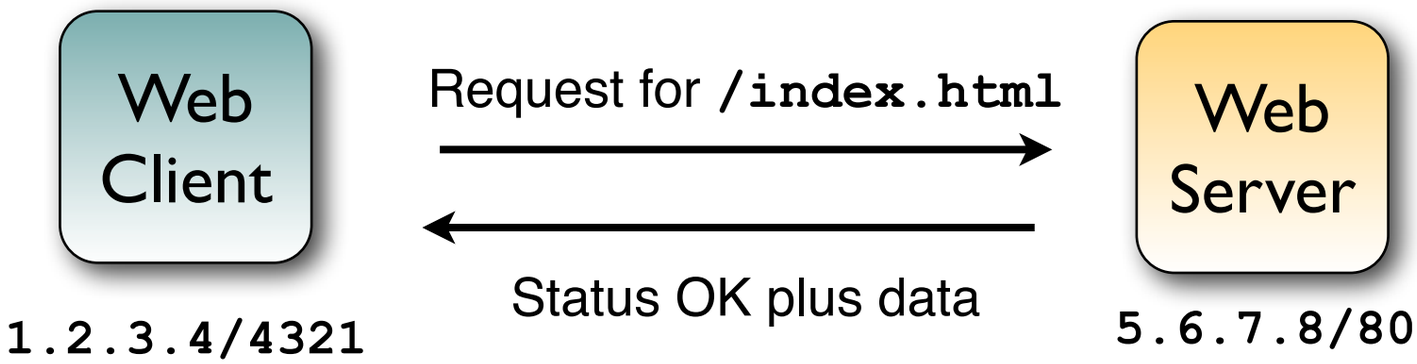
Event Model


Web Client
Request for /index.html
Web Server
Status OK plus data
1.2.3.4/4321
5.6.7.8/80
Stream of TCP packets
SYN
SYN
ACK
ACK
ACK
ACK
FIN
FIN

Event Model


Web Client
Request for /index.html
Web Server
Status OK plus data
1.2.3.4/4321
5.6.7.8/80
Stream of TCP packets
SYN
SYN
ACK
ACK
ACK
ACK
FIN
FIN
Event
connection established(1.2.3.4/4321⇒5.6.7.8/80)

Event Model



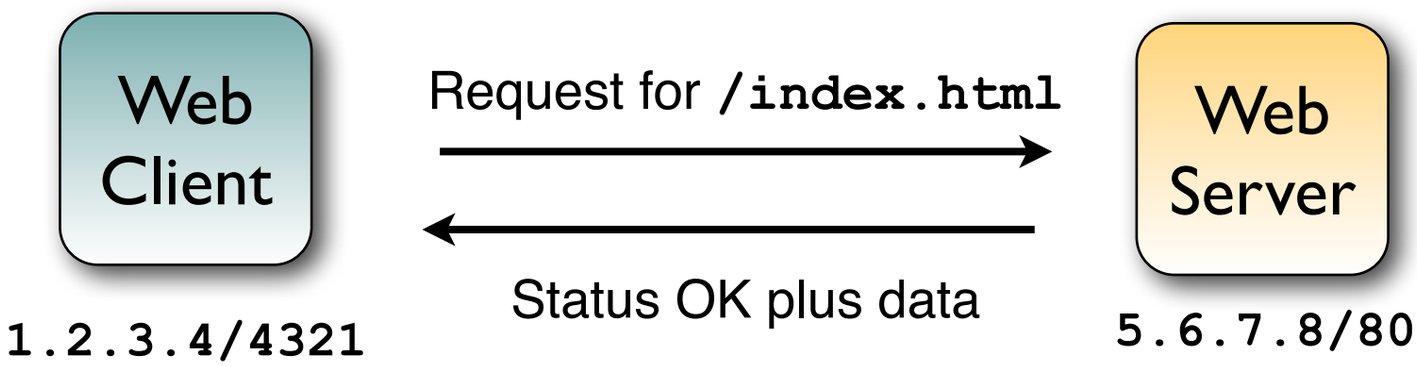
Stream of TCP packets

Event → `connection_established(1.2.3.4/4321⇒5.6.7.8/80)`

TCP stream reassembly for originator

Event → `http_request(1.2.3.4/4321⇒5.6.7.8/80, "GET", "/index.html")`

Event Model



Stream of TCP packets

Event → `connection_established(1.2.3.4/4321⇒5.6.7.8/80)`

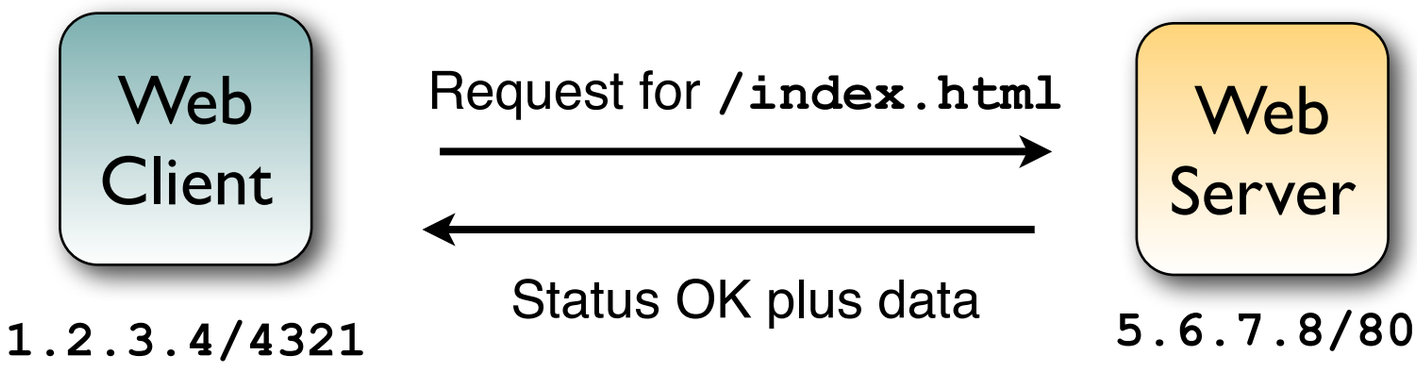
TCP stream reassembly for originator

Event → `http_request(1.2.3.4/4321⇒5.6.7.8/80, "GET", "/index.html")`

TCP stream reassembly for responder

Event → `http_reply(1.2.3.4/4321⇒5.6.7.8/80, 200, "OK", data)`

Event Model



Stream of TCP packets

Event → `connection established(1.2.3.4/4321⇒5.6.7.8/80)`

TCP stream reassembly for originator

Event → `http_request(1.2.3.4/4321⇒5.6.7.8/80, "GET", "/index.html")`

TCP stream reassembly for responder

Event → `http_reply(1.2.3.4/4321⇒5.6.7.8/80, 200, "OK", data)`

Event → `connection_finished(1.2.3.4/4321, 5.6.7.8/80)`

Script Example: Matching URLs

Task: Report all Web requests for files called "`passwd`".

Script Example: Matching URLs

Task: Report all Web requests for files called "`passwd`".

```
event http_request(c: connection,           # Connection.
                   method: string,          # HTTP method.
                   original_URI: string,    # Requested URL.
                   unescaped_URI: string,   # Decoded URL.
                   version: string)         # HTTP version.
{
    if ( method == "GET" && unescaped_URI == /.*passwd/ )
        NOTICE(...); # Alarm.
}
```

Script Example: Scan Detector

Task: Count failed connection attempts per source address.

Script Example: Scan Detector

Task: Count failed connection attempts per source address.

```
global attempts: table[addr] of count &default=0;

event connection_rejected(c: connection)
{
        local source = c$id$orig_h;      # Get source address.
        local n = ++attempts[source];    # Increase counter.
        if ( n == SOME_THRESHOLD )       # Check for threshold.
            NOTICE(...);                 # Alarm.
}
```

Distributed Scripts

Distributed Scripts

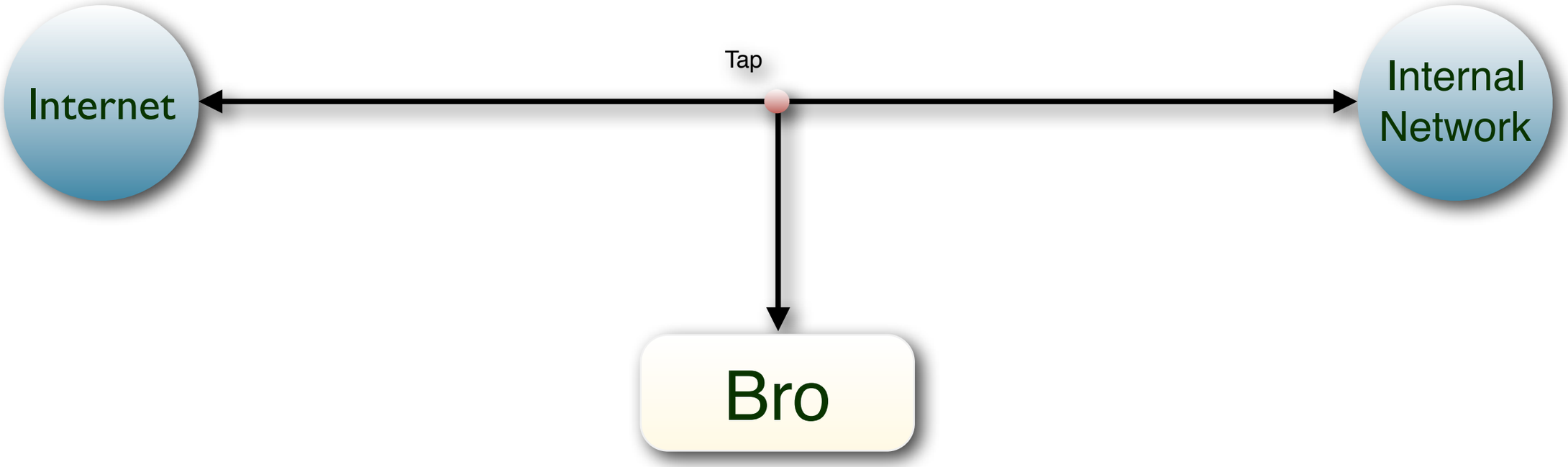
Bro comes with >10,000 lines of script code.

Prewritten functionality that's just loaded.

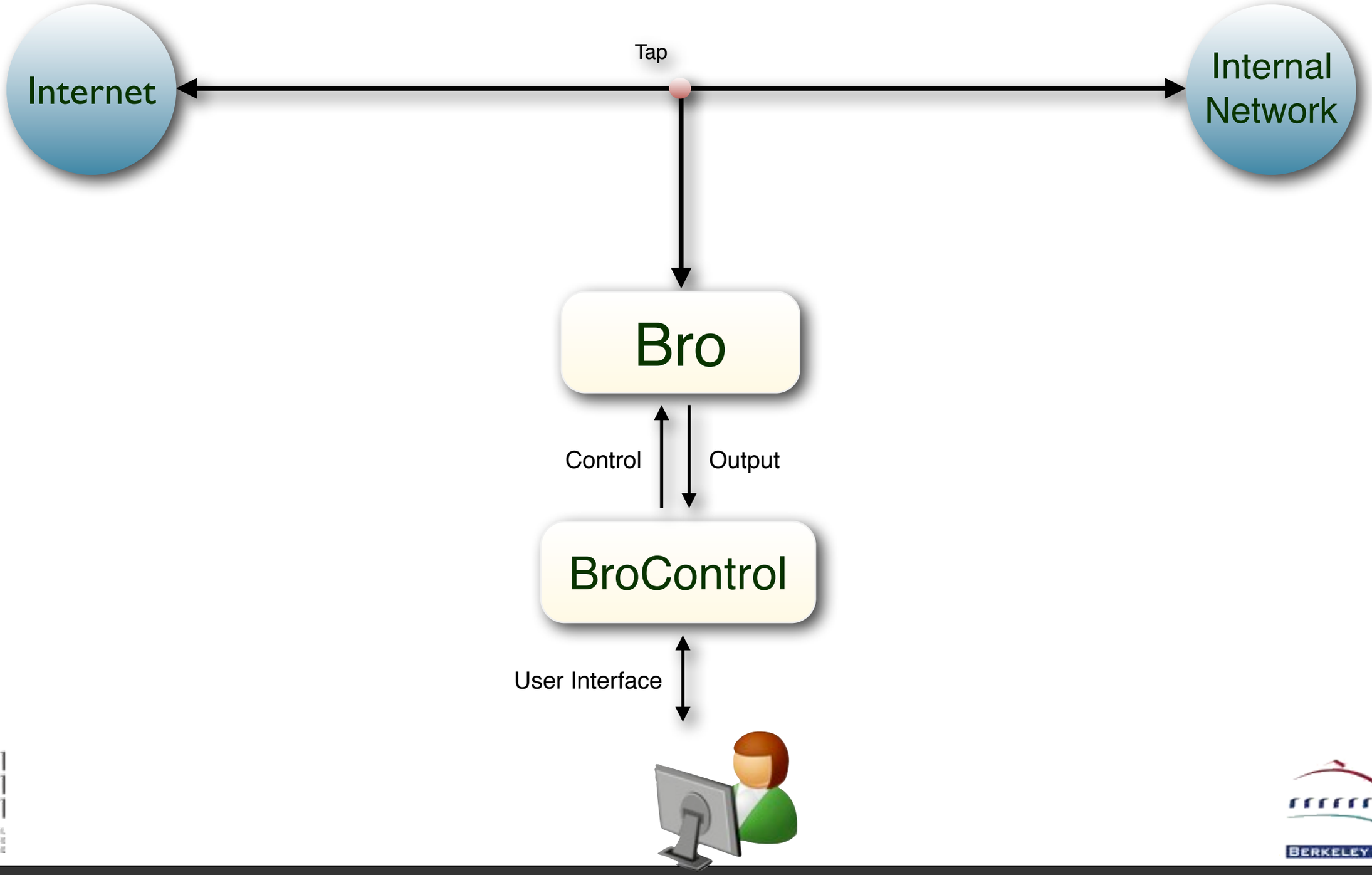
Scripts generate all the logs.

Amendable to extensive customization and extension.

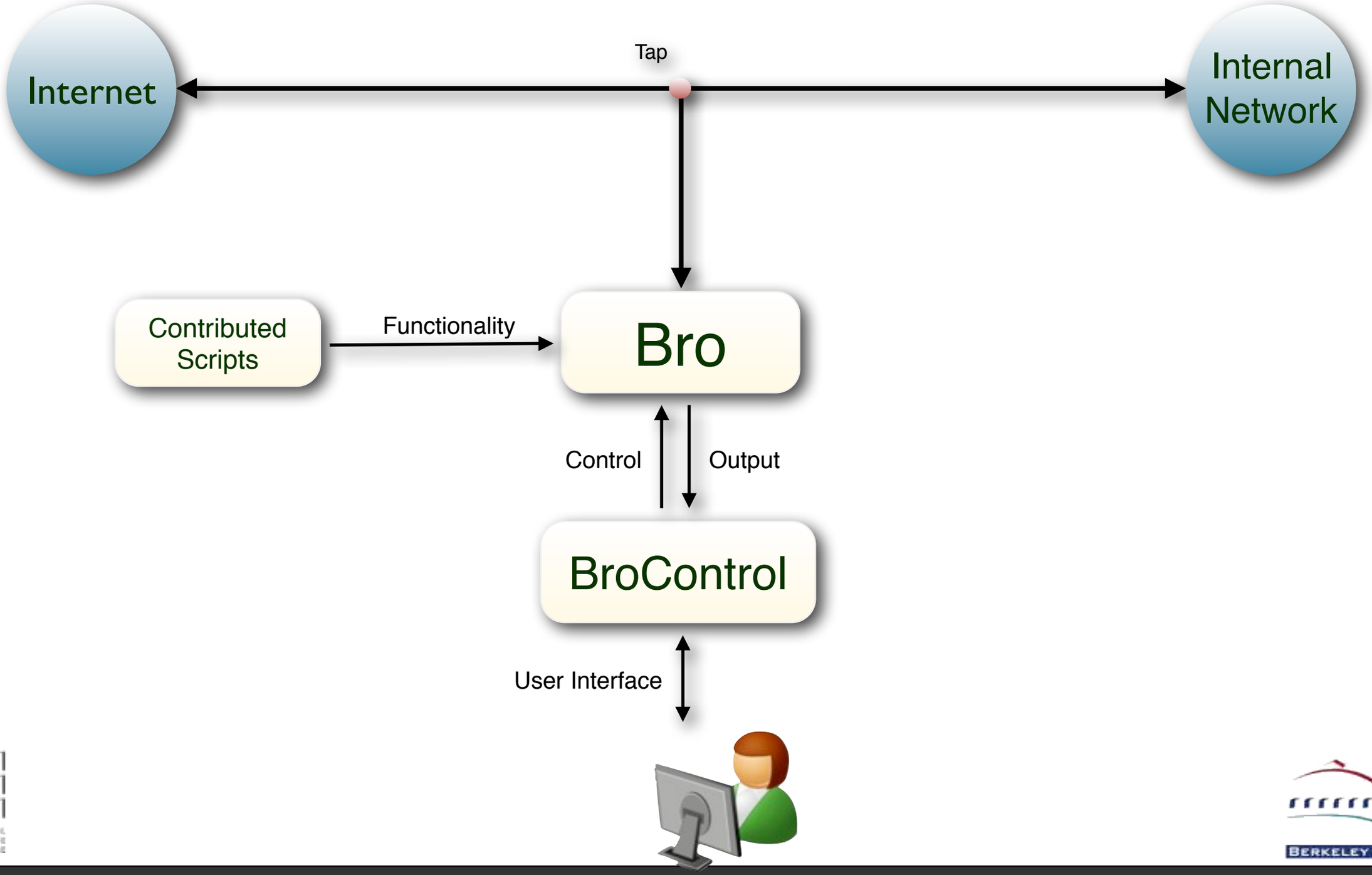
Bro Ecosystem



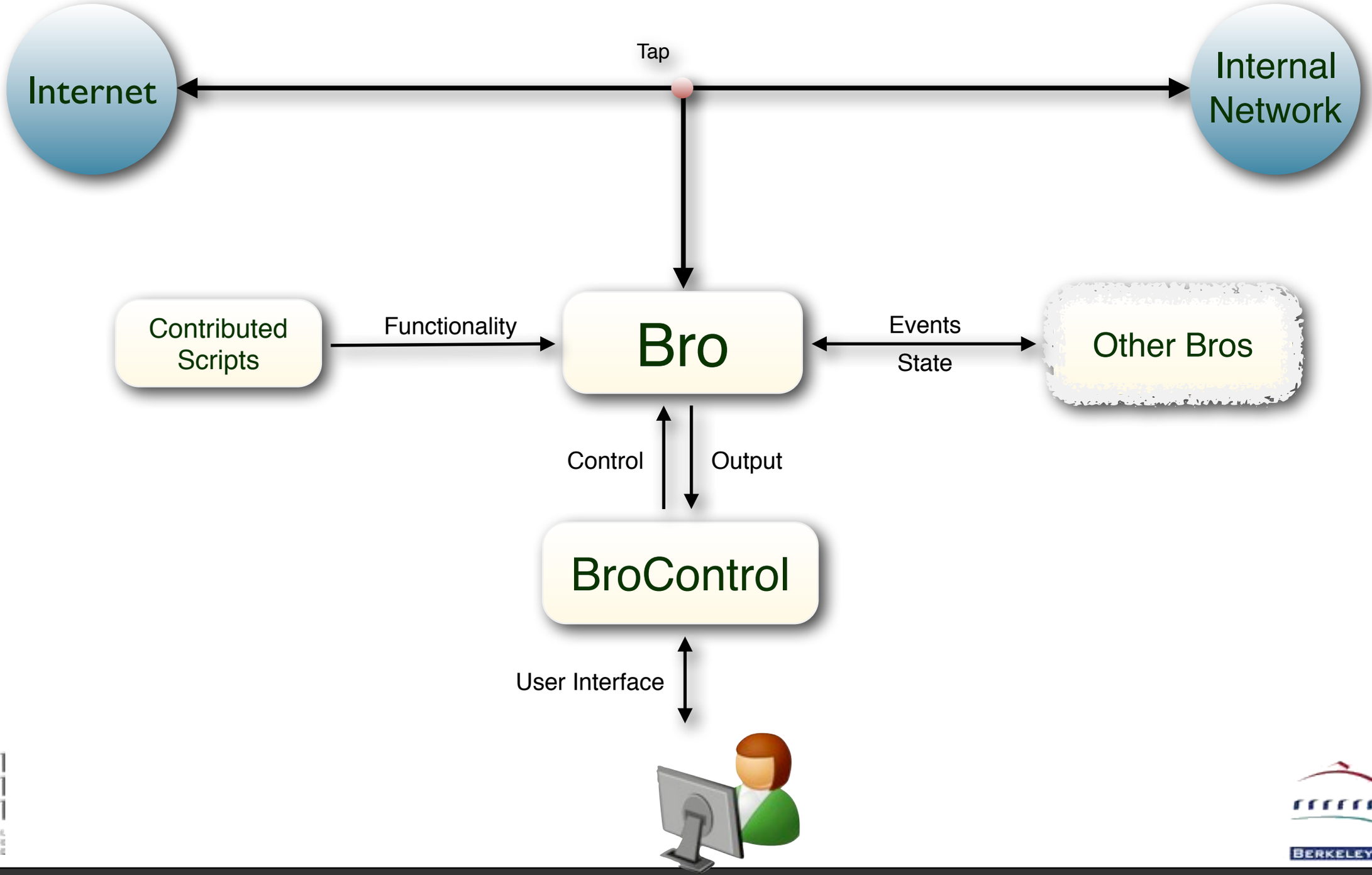
Bro Ecosystem



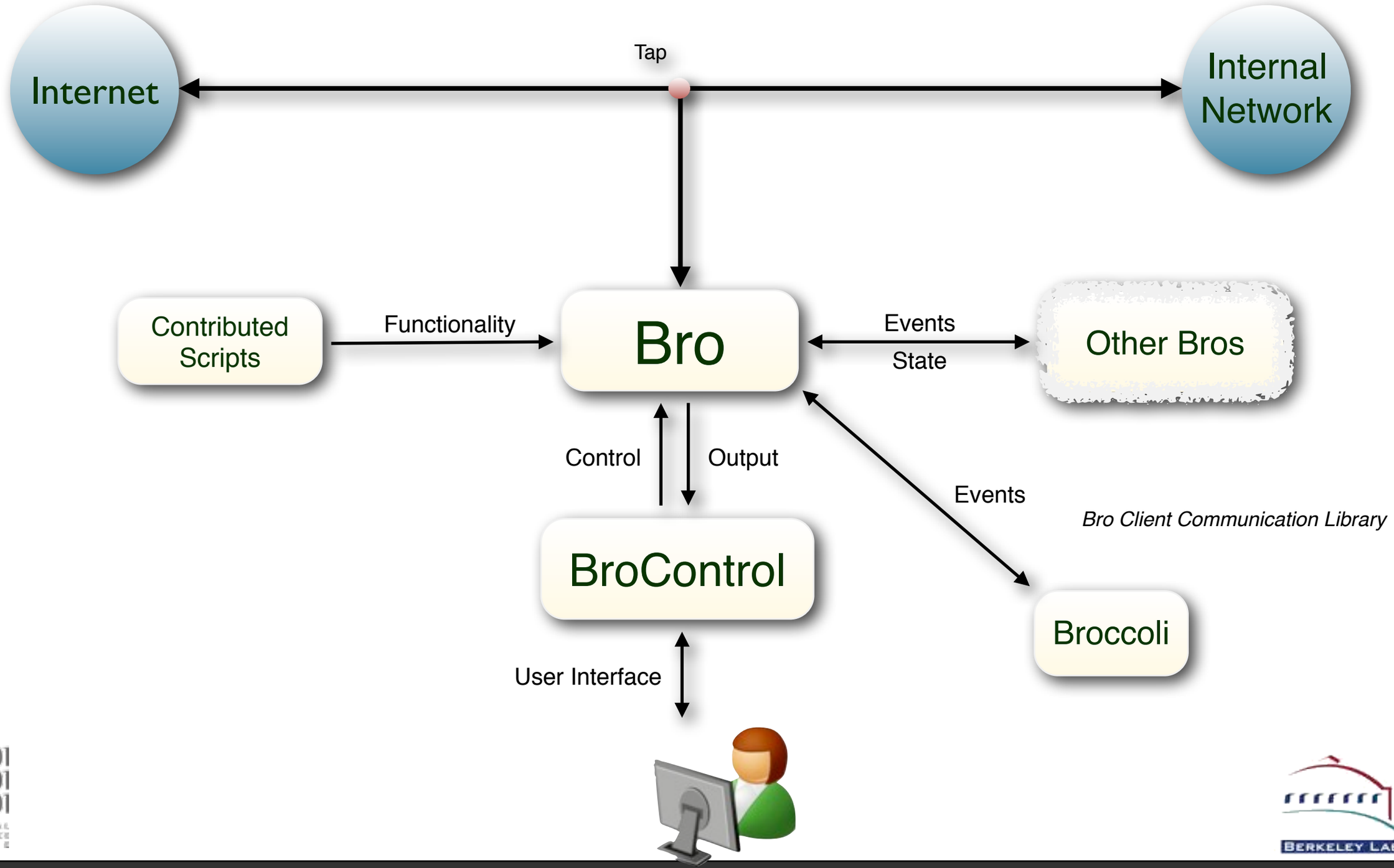
Bro Ecosystem



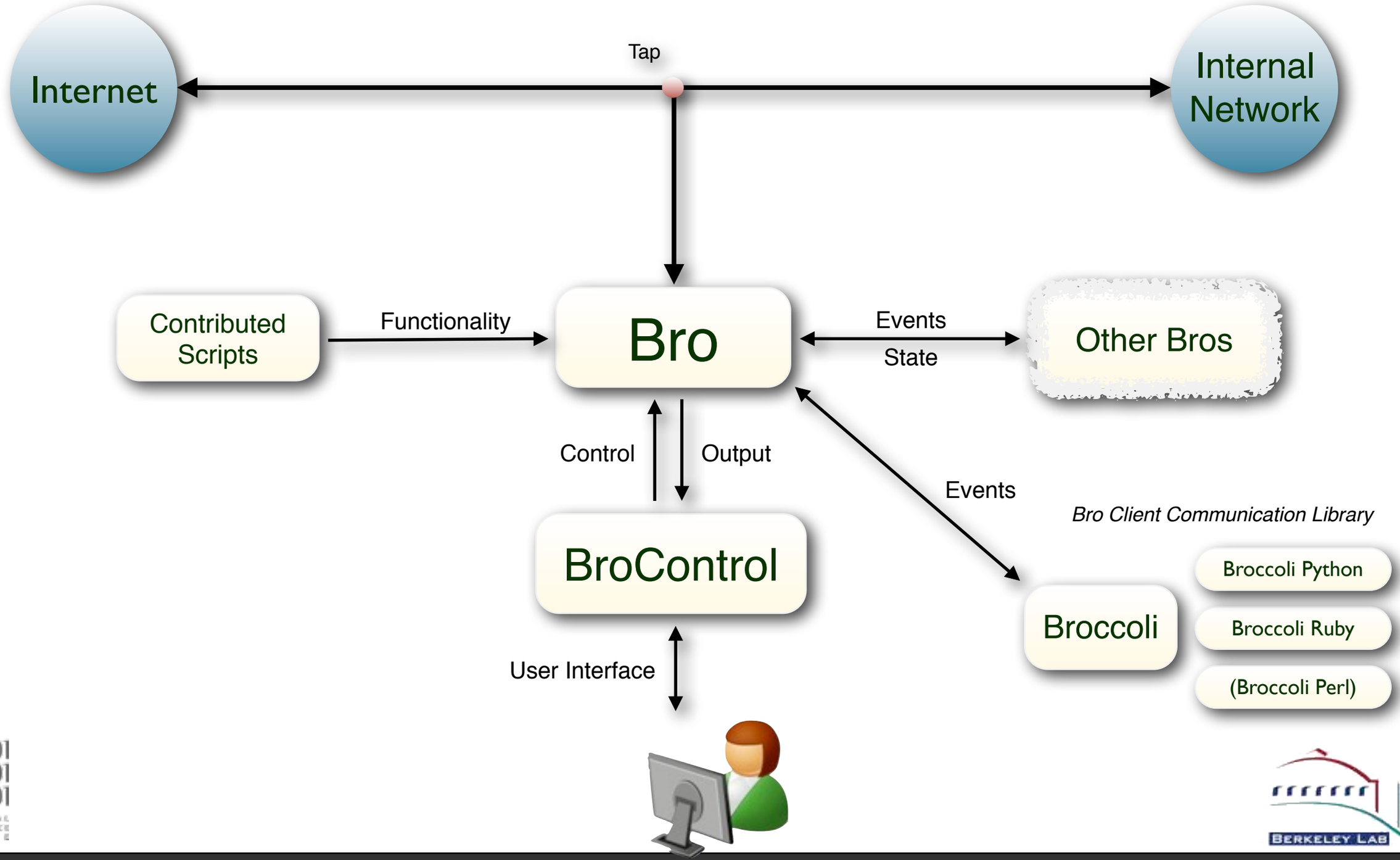
Bro Ecosystem



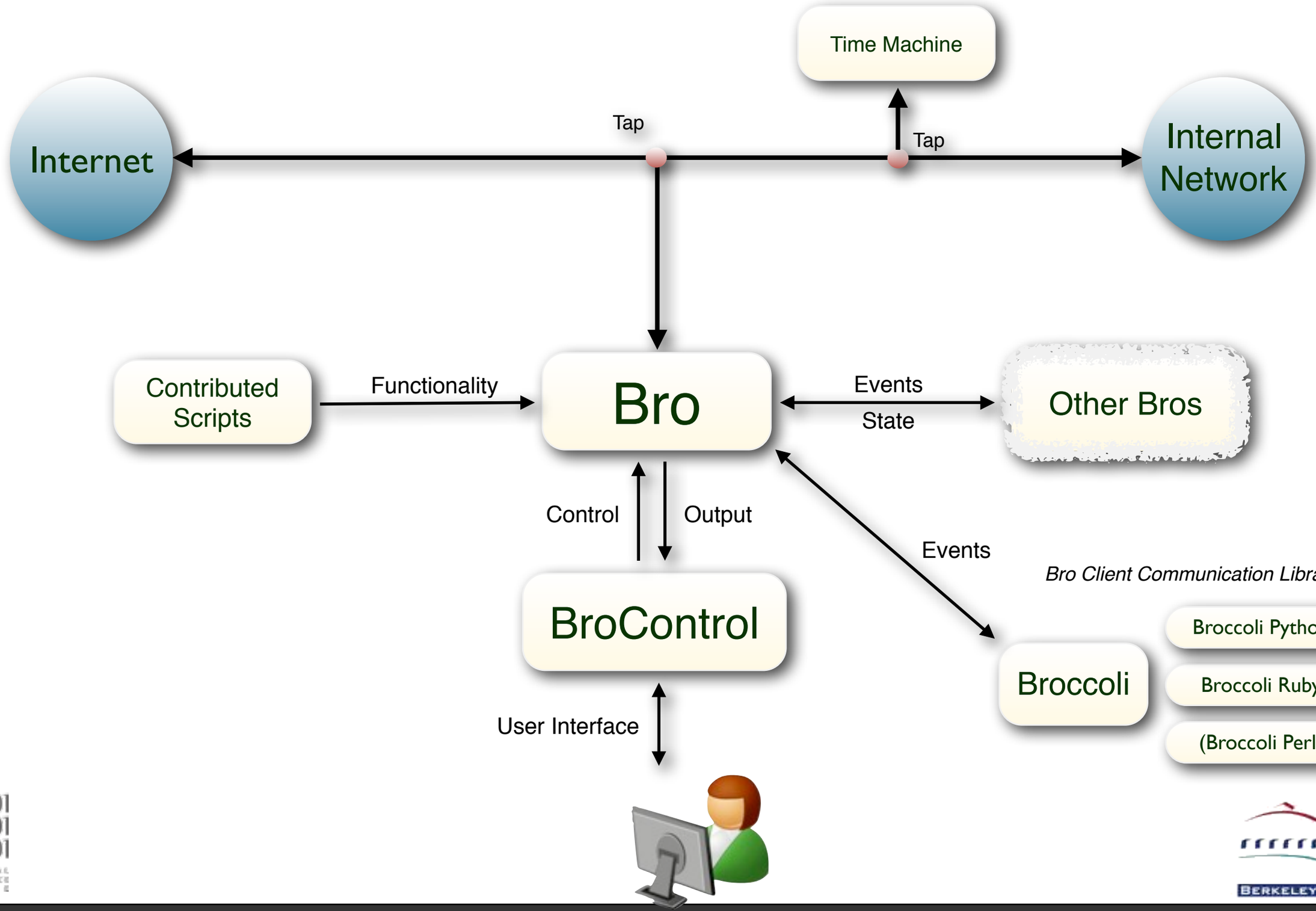
Bro Ecosystem



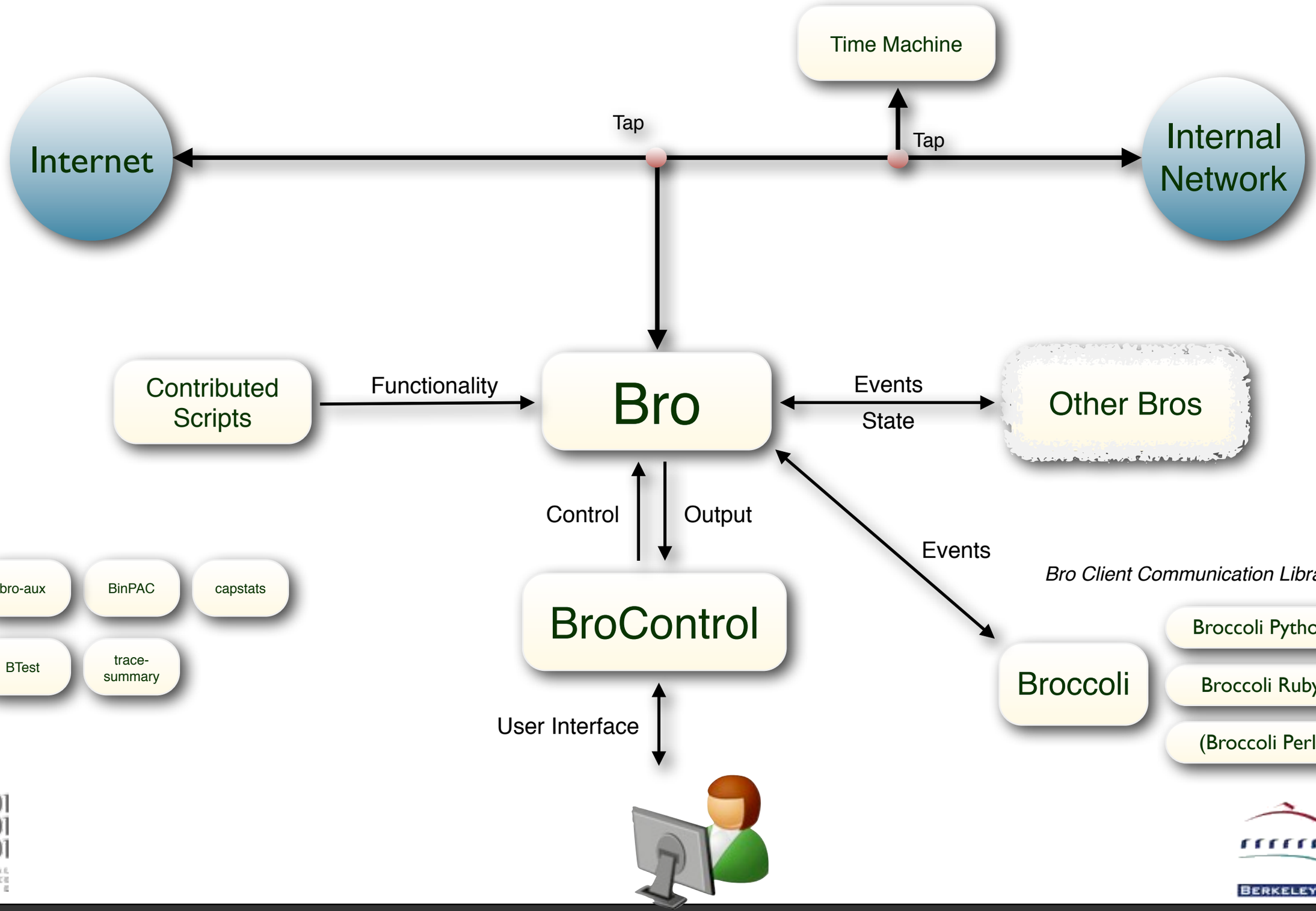
Bro Ecosystem



Bro Ecosystem



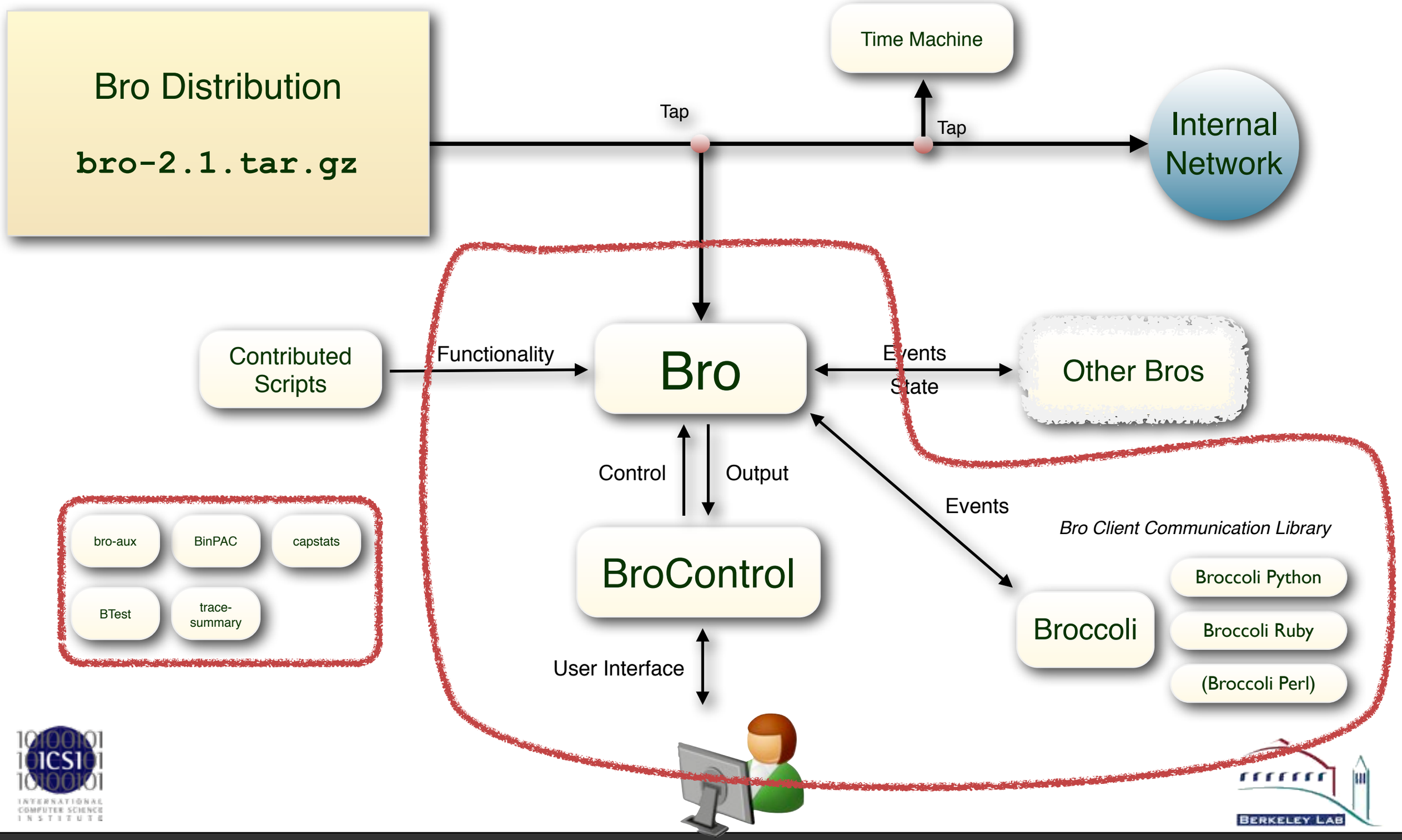
Bro Ecosystem



Bro Ecosystem

Bro Distribution

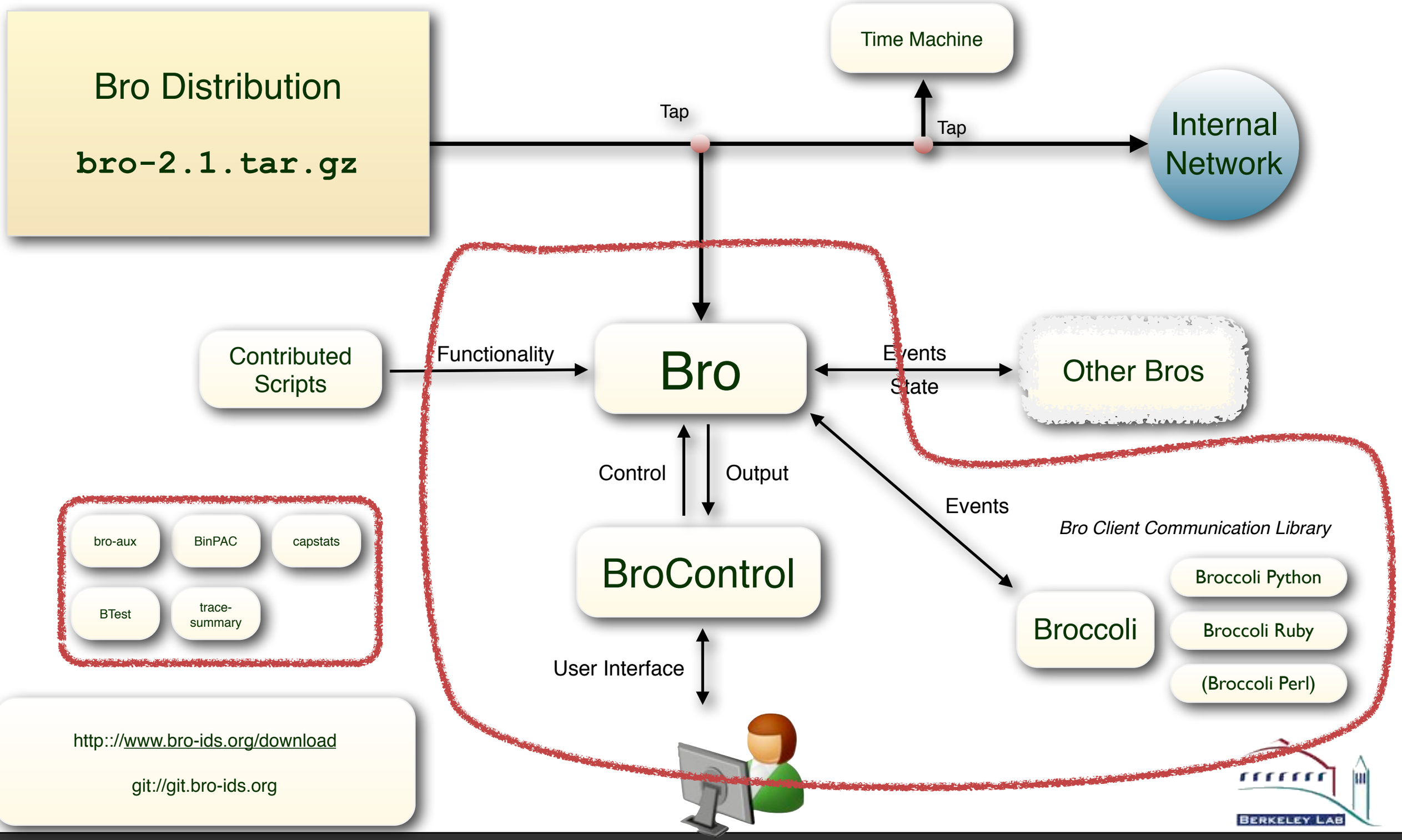
`bro-2.1.tar.gz`



Bro Ecosystem

Bro Distribution

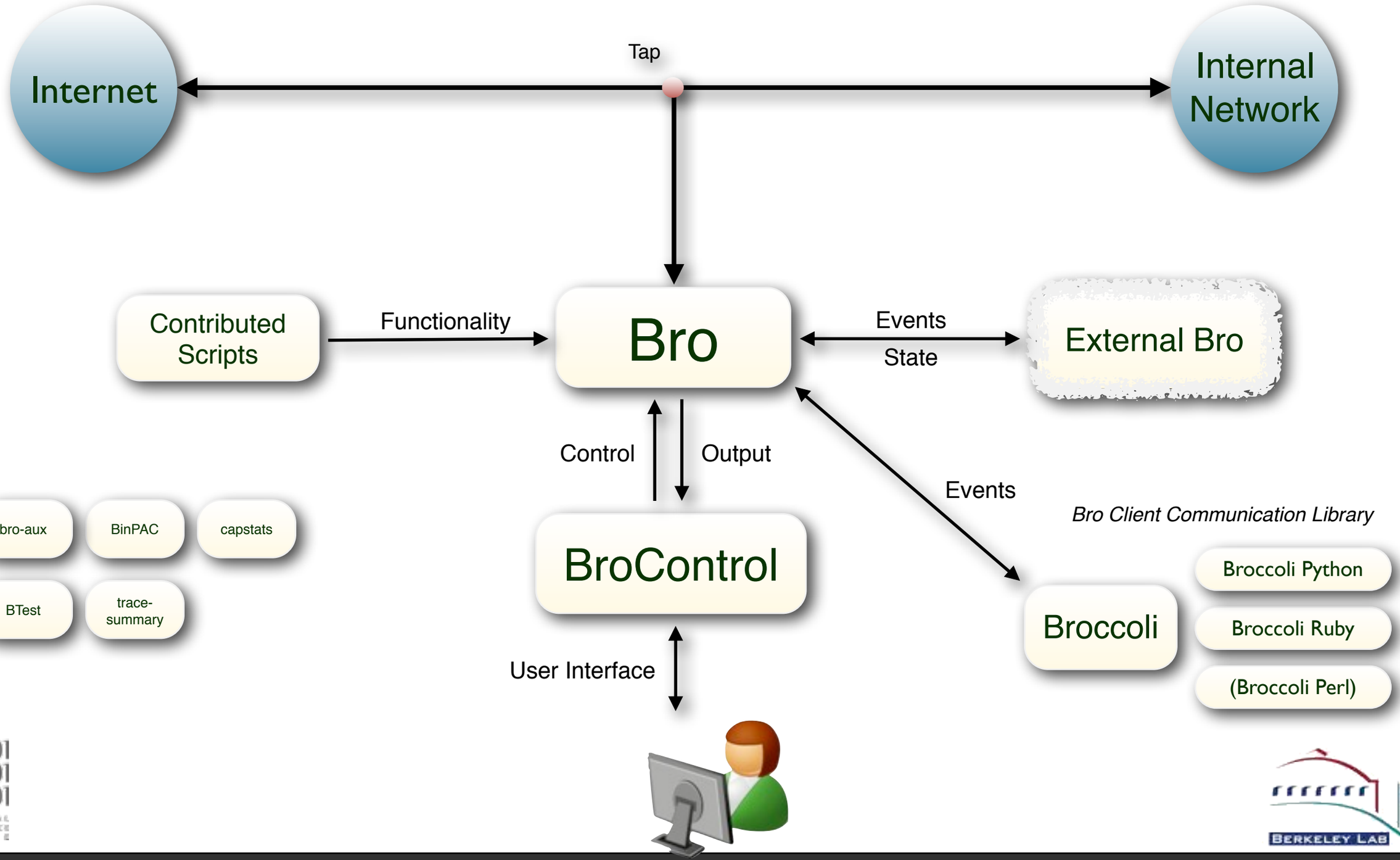
`bro-2.1.tar.gz`



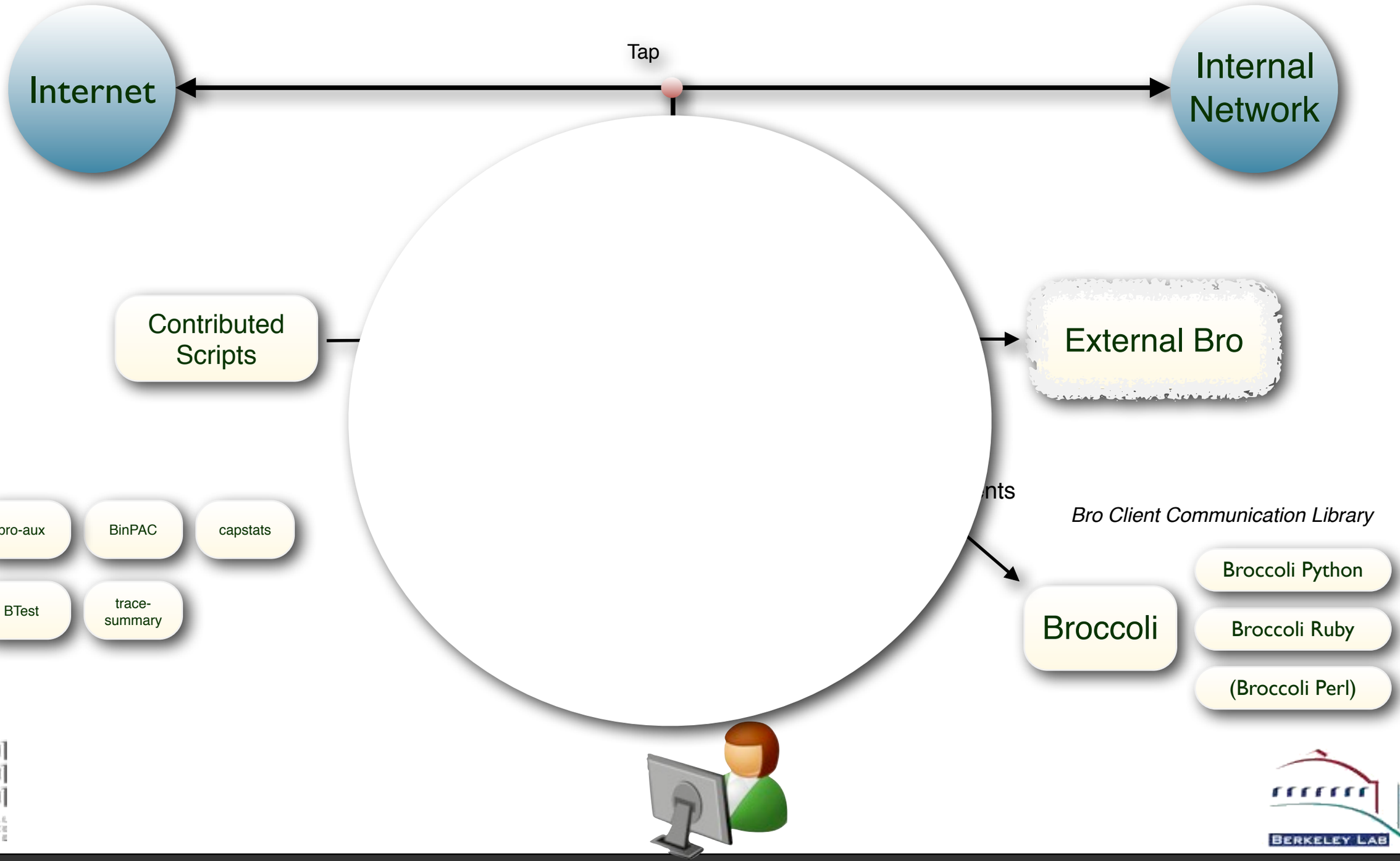
http:://www.bro-ids.org/download

git://git.bro-ids.org

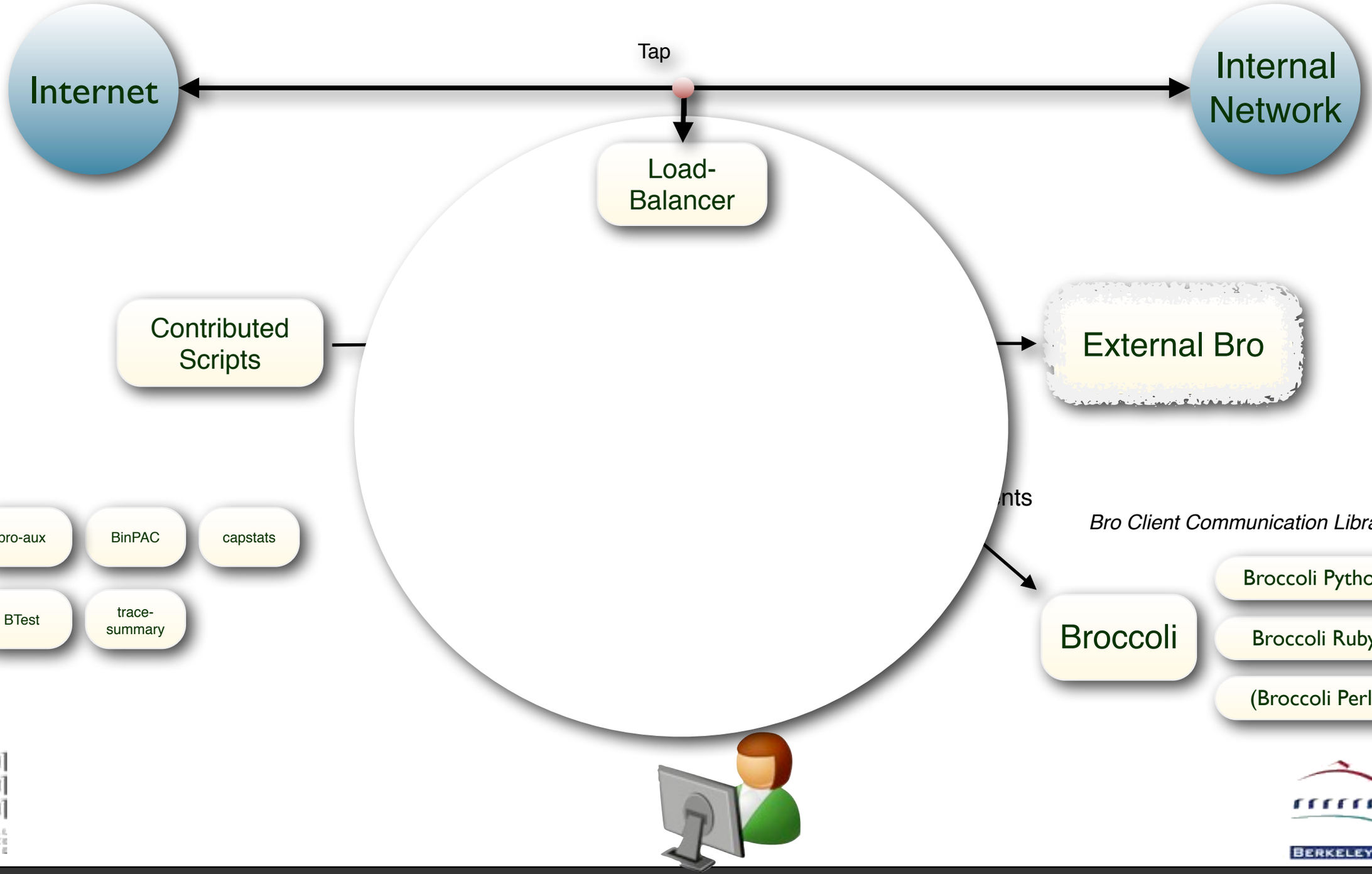
Bro *Cluster* Ecosystem



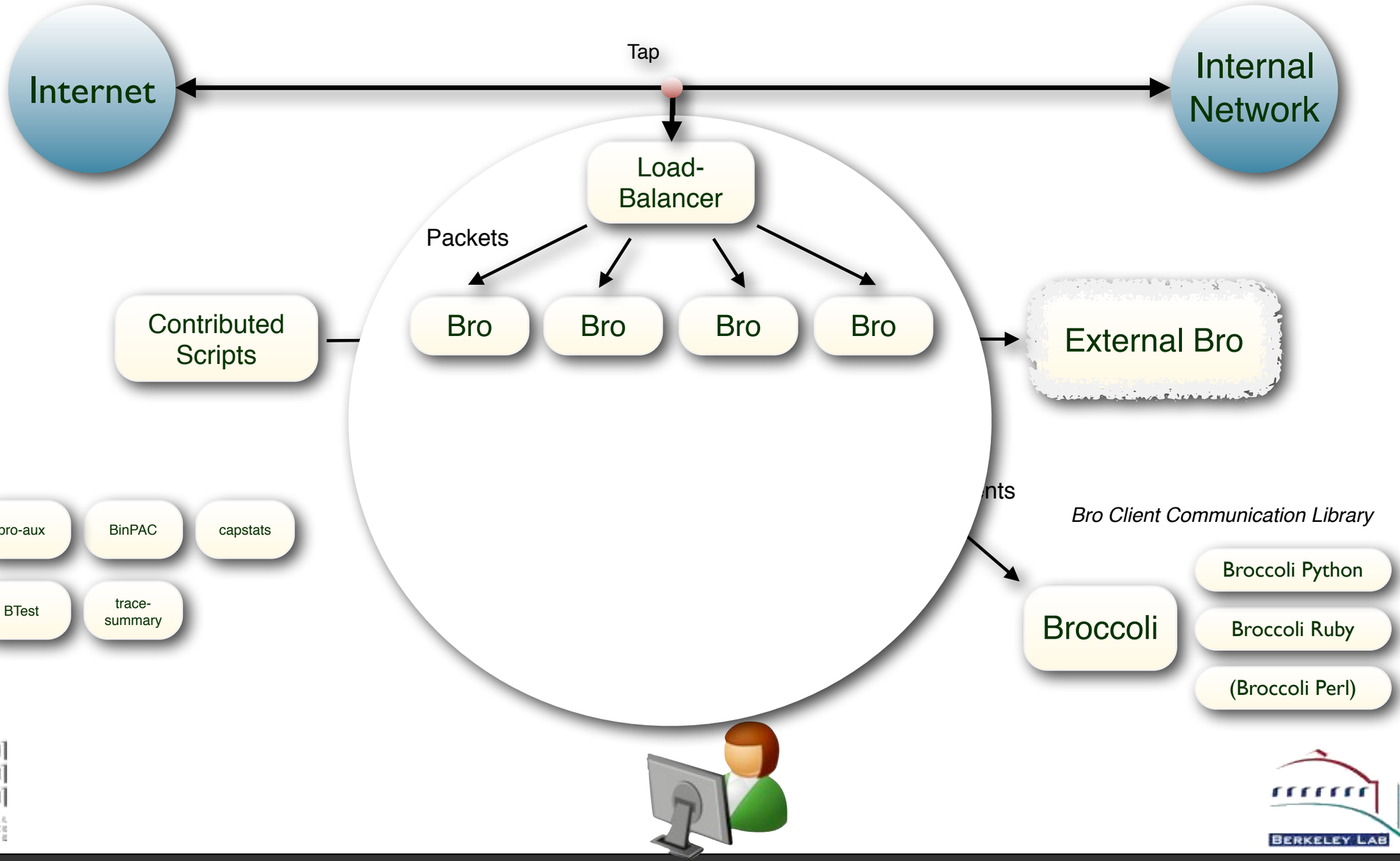
Bro *Cluster* Ecosystem



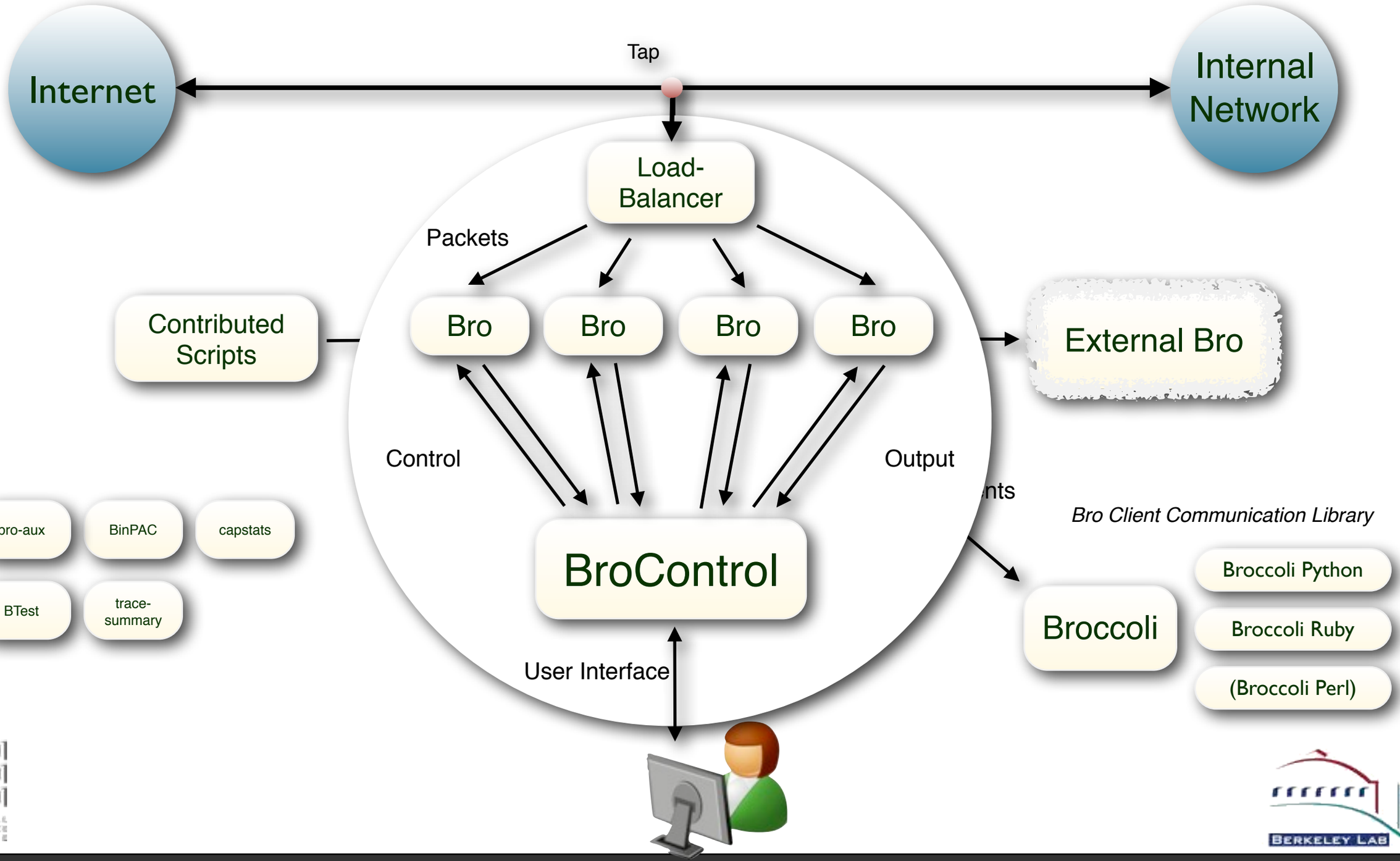
Bro *Cluster* Ecosystem



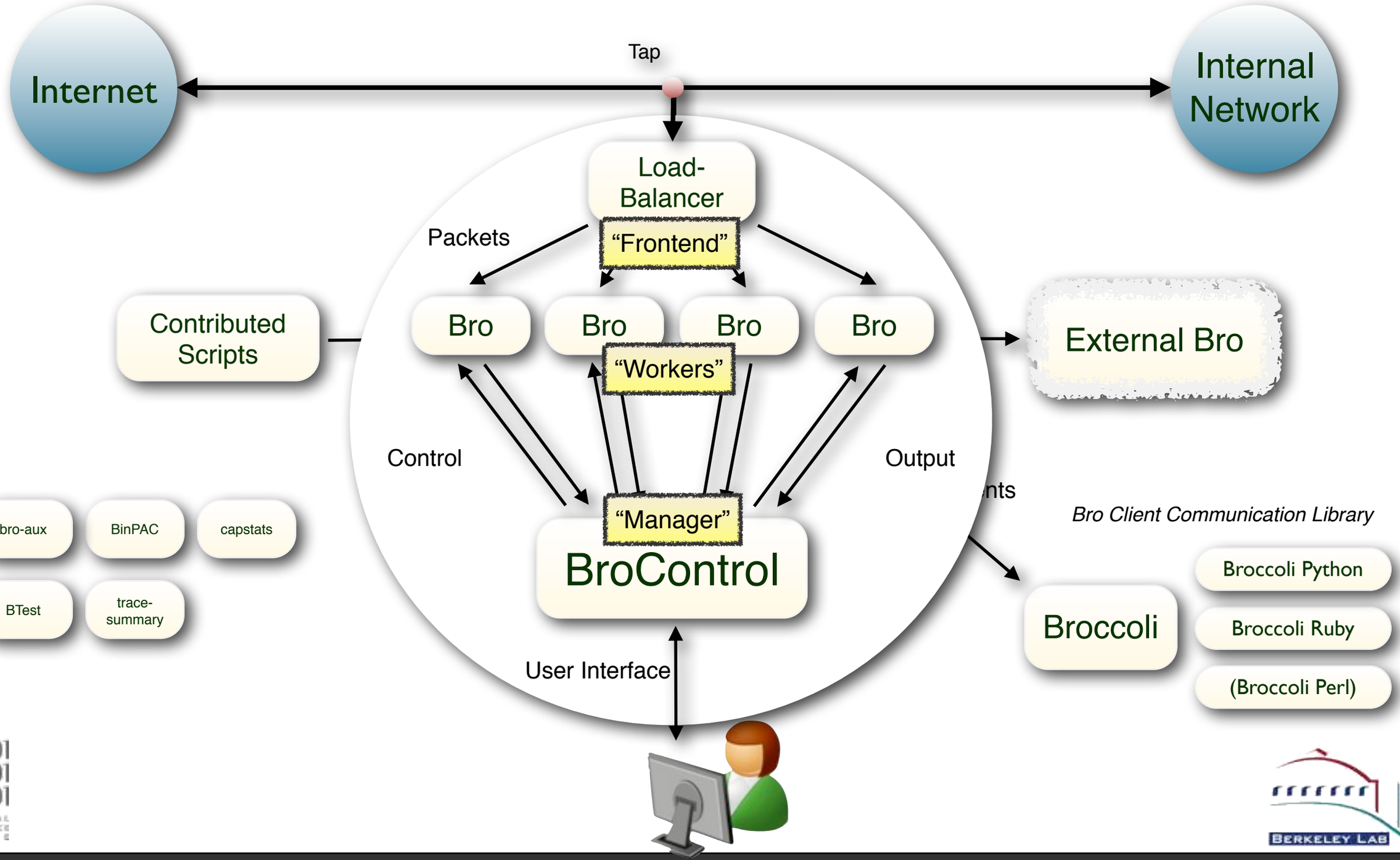
Bro *Cluster* Ecosystem



Bro *Cluster* Ecosystem



Bro *Cluster* Ecosystem

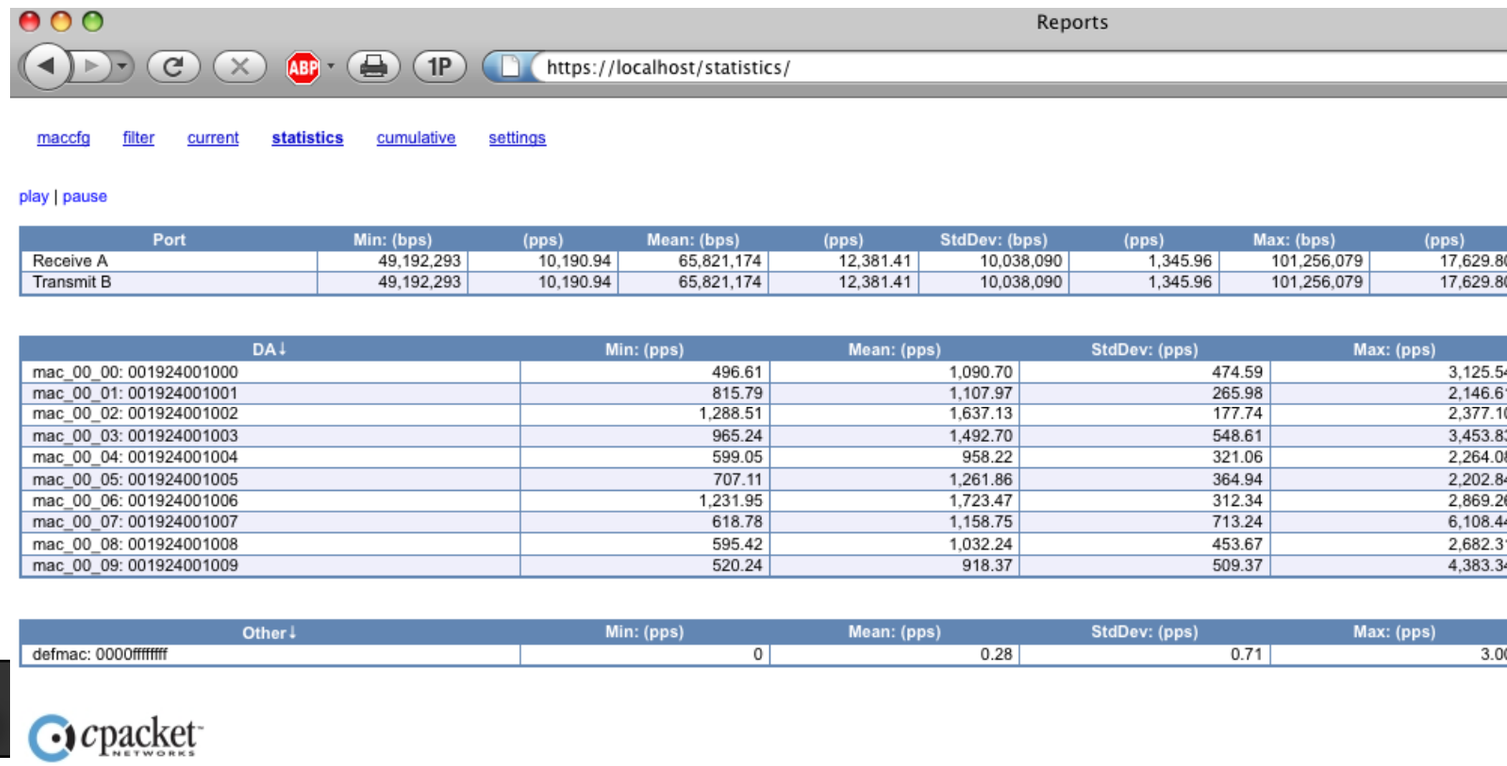


A Production Load-Balancer

cFlow: 10GE line-rate, stand-alone load-balancer

10 Gb/s in/out
Web & CLI
Filtering capabilities

Available from cPacket

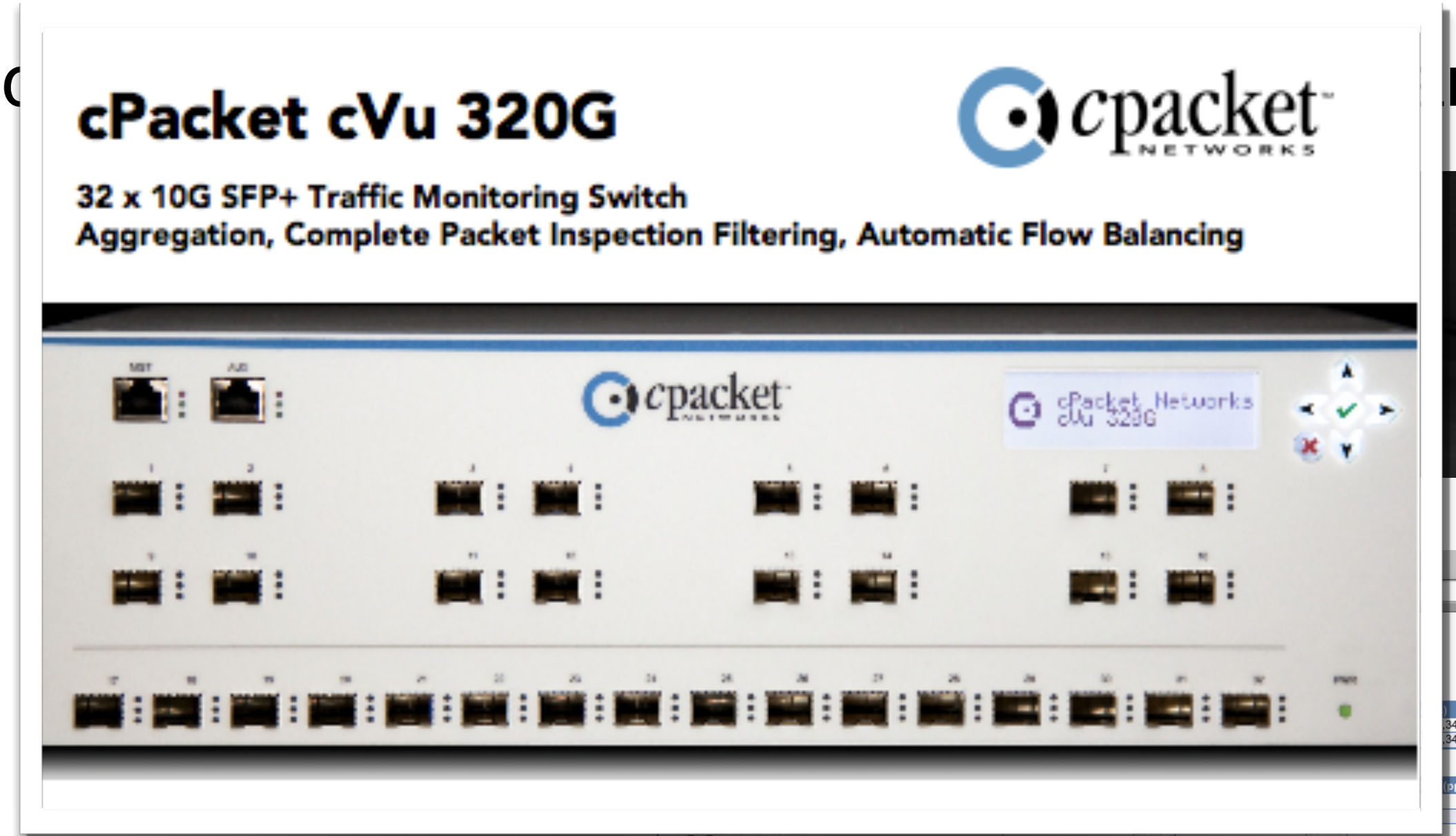


Port	Min: (bps)	(pps)	Mean: (bps)	(pps)	StdDev: (bps)	(pps)	Max: (bps)	(pps)
Receive A	49,192,293	10,190.94	65,821,174	12,381.41	10,038,090	1,345.96	101,256,079	17,629.8
Transmit B	49,192,293	10,190.94	65,821,174	12,381.41	10,038,090	1,345.96	101,256,079	17,629.8

DA↓	Min: (pps)	Mean: (pps)	StdDev: (pps)	Max: (pps)
mac_00_00: 001924001000	496.61	1,090.70	474.59	3,125.5
mac_00_01: 001924001001	815.79	1,107.97	265.98	2,146.6
mac_00_02: 001924001002	1,288.51	1,637.13	177.74	2,377.1
mac_00_03: 001924001003	965.24	1,492.70	548.61	3,453.8
mac_00_04: 001924001004	599.05	958.22	321.06	2,264.0
mac_00_05: 001924001005	707.11	1,261.86	364.94	2,202.8
mac_00_06: 001924001006	1,231.95	1,723.47	312.34	2,869.2
mac_00_07: 001924001007	618.78	1,158.75	713.24	6,108.4
mac_00_08: 001924001008	595.42	1,032.24	453.67	2,682.3
mac_00_09: 001924001009	520.24	918.37	509.37	4,383.3

Other↓	Min: (pps)	Mean: (pps)	StdDev: (pps)	Max: (pps)
defmac: 0000ffffffff	0	0.28	0.71	3.0

A Production Load-Balancer



Available from cPacket

			Max: (bps)	(pps)
			101,256,079	17,629.80
			101,256,079	17,629.80

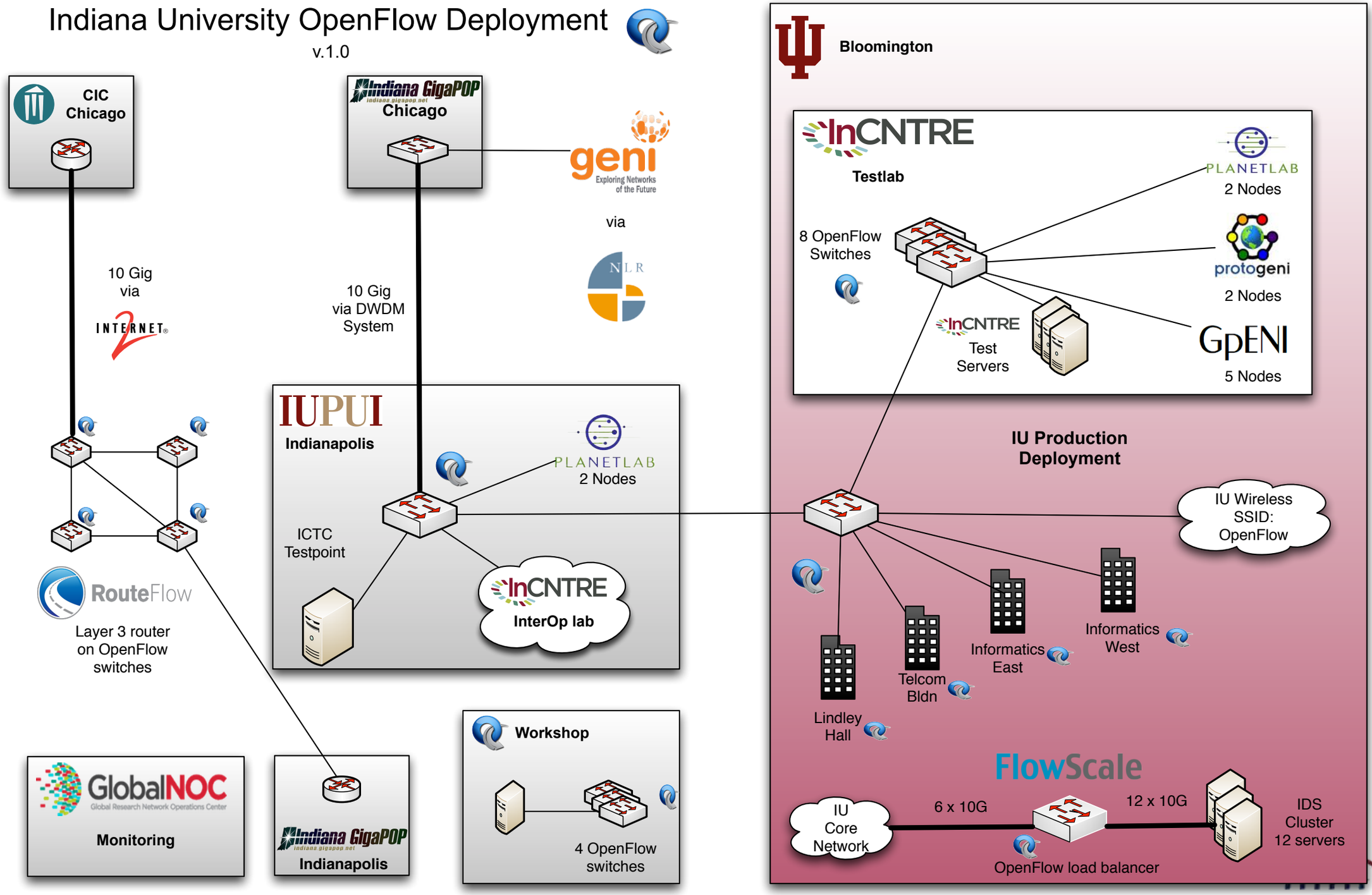
			(pps)	Max: (pps)
			474.59	3,125.54
			265.98	2,146.61
			177.74	2,377.10
mac_00_03: 001924001003	965.24	1,492.70	548.61	3,453.83
mac_00_04: 001924001004	599.05	958.22	321.06	2,264.08
mac_00_05: 001924001005	707.11	1,261.86	364.94	2,202.84
mac_00_06: 001924001006	1,231.95	1,723.47	312.34	2,869.26
mac_00_07: 001924001007	618.78	1,158.75	713.24	6,108.44
mac_00_08: 001924001008	595.42	1,032.24	453.67	2,682.31
mac_00_09: 001924001009	520.24	918.37	509.37	4,383.34

Other↓	Min: (pps)	Mean: (pps)	StdDev: (pps)	Max: (pps)
defmac: 0000ffffffff	0	0.28	0.71	3.00

INTERNATIONAL COMPUTER SCIENCE INSTITUTE

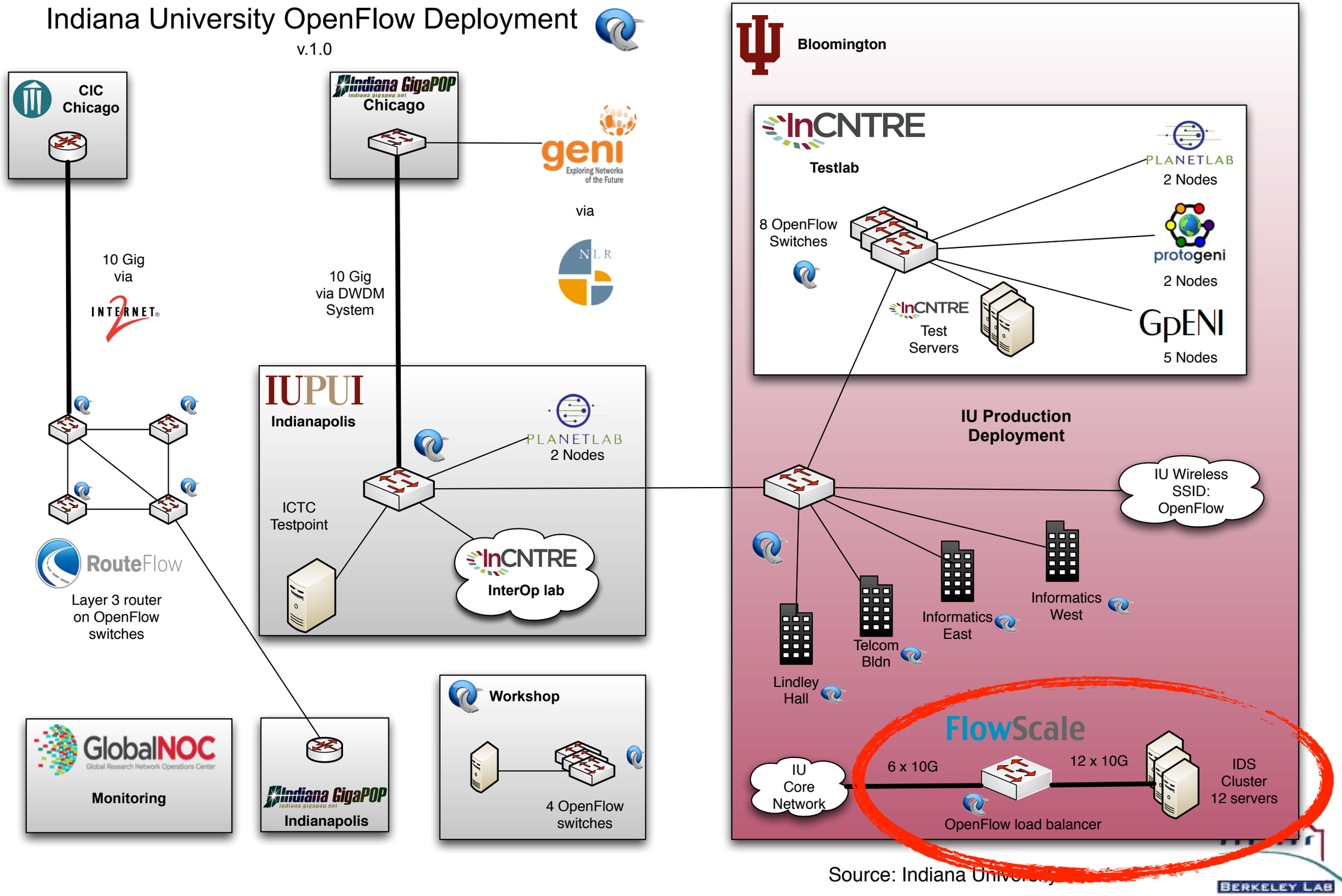
cpacket NETWORKS

Indiana University



Source: Indiana University

Indiana University



Source: Indiana University

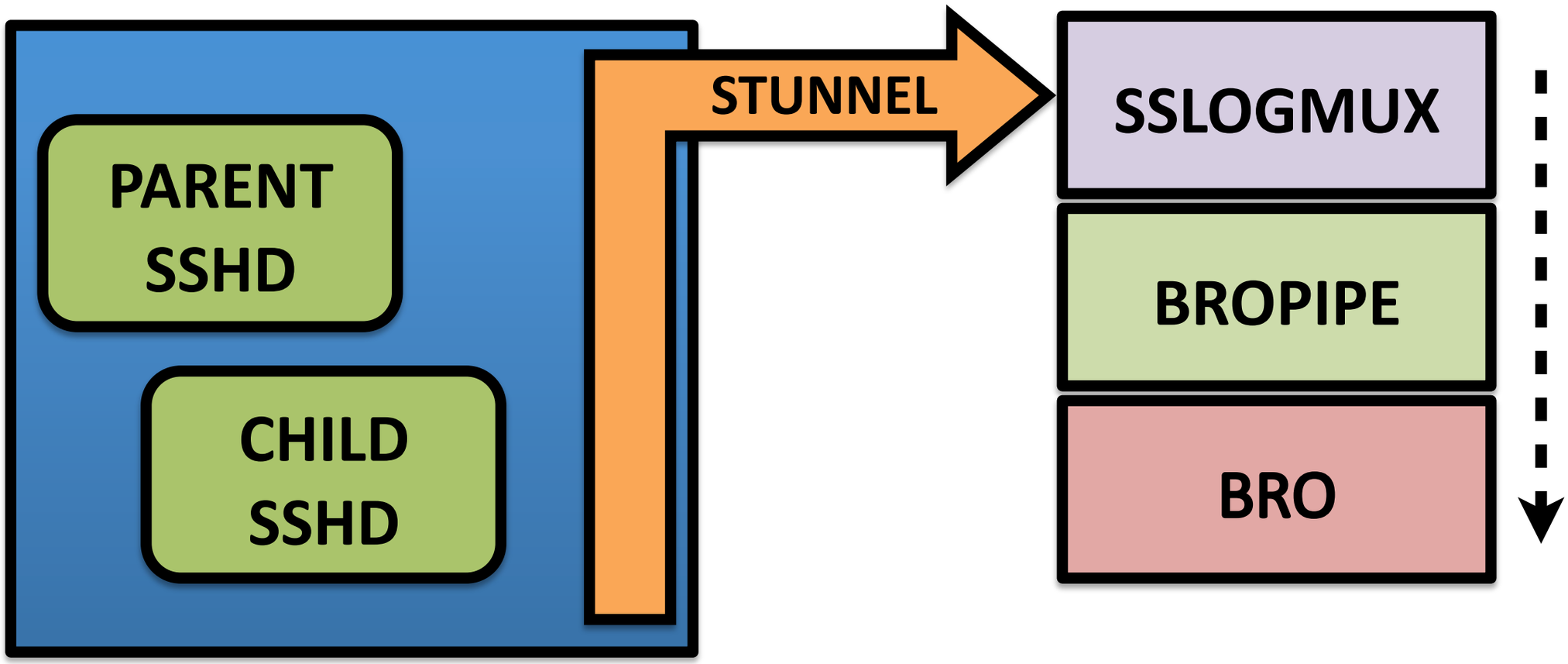
External Events: Broccoli

External Events: Broccoli

"Auditing SSHD"

External Events: Broccoli

"Auditing SSHD"



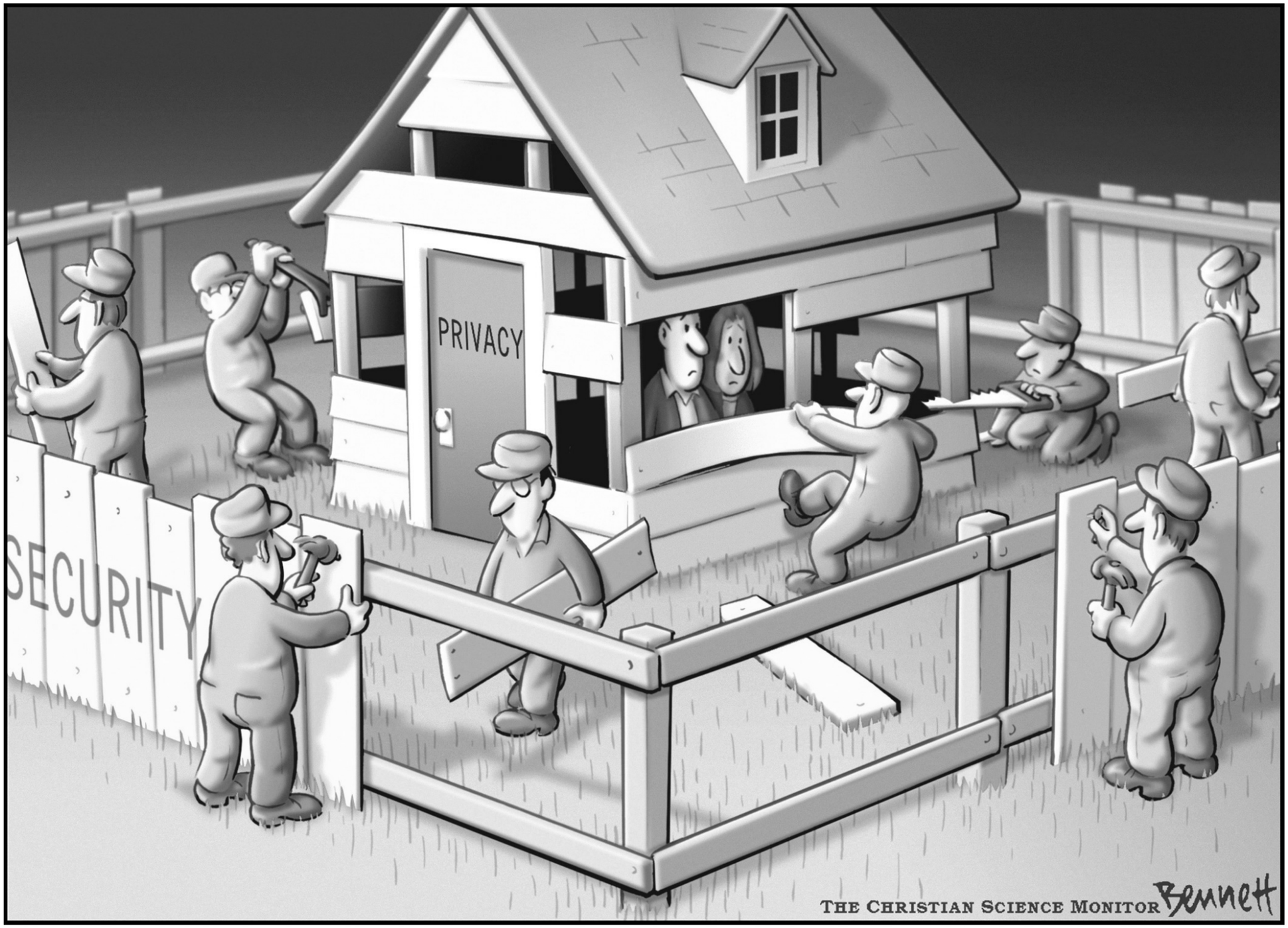
Source: Scott Campbell / NERSC

NERSC Computer Use Policies Form

Monitoring and Privacy

Users have no explicit or implicit expectation of privacy. NERSC retains the right to monitor the content of all activities on NERSC systems and networks and access any computer files without prior knowledge or consent of users, senders or recipients. NERSC may retain copies of any network traffic, computer files or messages indefinitely without prior knowledge or consent.

The Security Fence



Cartoon Courtesy Clay Bennett / The Christian Science Monitor

Version 2.0 (Jan 2012)

Version 2.0 (Jan 2012)

Default scripts rewritten from scratch.

Focus on ease of use and operational deployment.

New logging infrastructure.

New build and packaging system.

New auto-documentation system (Broxygen).

Lots of bugs fixed.

Obsolete code removed.

New development infrastructure.

New regression testing framework.

New web server.

New mailing lists.

New logo.

Just released ...

Just released ...

Bro 2.1

Comprehensive IPv6 support.

Tunnel decapsulation.

New logging formats (DataSeries / ElasticSearch)

Input Framework

Input Framework Example: Blacklists

IP	Reason	Timestamp
66.249.66.1	Connected to honeypot	1333252748
208.67.222.222	Too many DNS requests	1330235733
192.150.186.11	Sent spam	1333145108

User Interface

User Interface

```
type Index: record { ip: addr; };

type Value: record { reason:    string;
                     timestamp: time; };

global blacklist: table[addr] of Value;

Input::add_table(source="blacklist.tsv", idx=Index,
                 val=Value, destination=blacklist);
```

(Syntax simplified.)

User Interface

```
type Index: record { ip: addr; };

type Value: record { reason:    string;
                     timestamp: time; };

global blacklist: table[addr] of Value;

Input::add_table(source="blacklist.tsv", idx=Index,
                 val=Value, destination=blacklist);
```

(Syntax simplified.)

```
event connection_established(c: connection)
{
  if ( c$id$orig_h in blacklist )
       alarm(...)
}
```

Current Research

Performace: 100 Gb/s

DOE/ESNet
100G Advanced Networking Initiative

NEWS CENTER

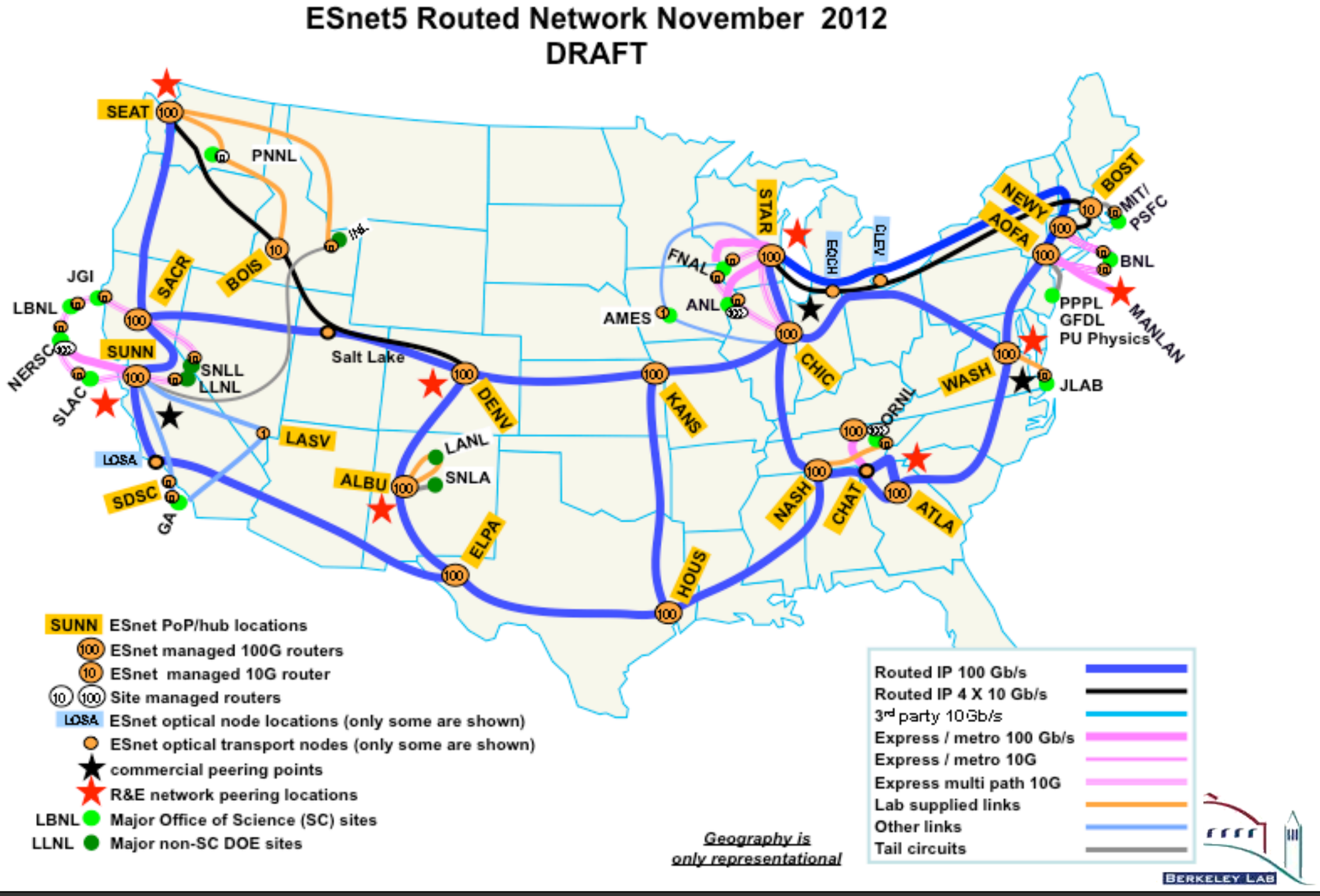
Contact Us | Biology for Energy and Health | Climate + Environment | Computing | Energy | Physics +

Moving Data at the Speed of Science: Berkeley Lab Lays Foundation for 100 Gbps Prototype Network

JULY 13, 2011

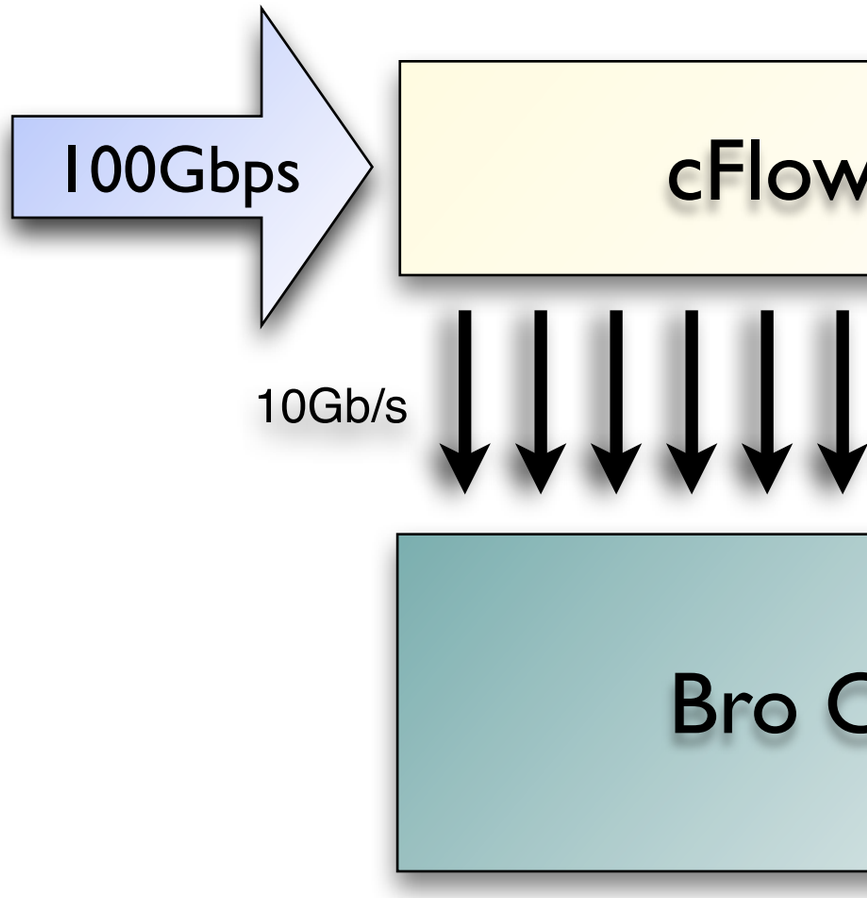
Source: ESNet

Production Backbone in Planing

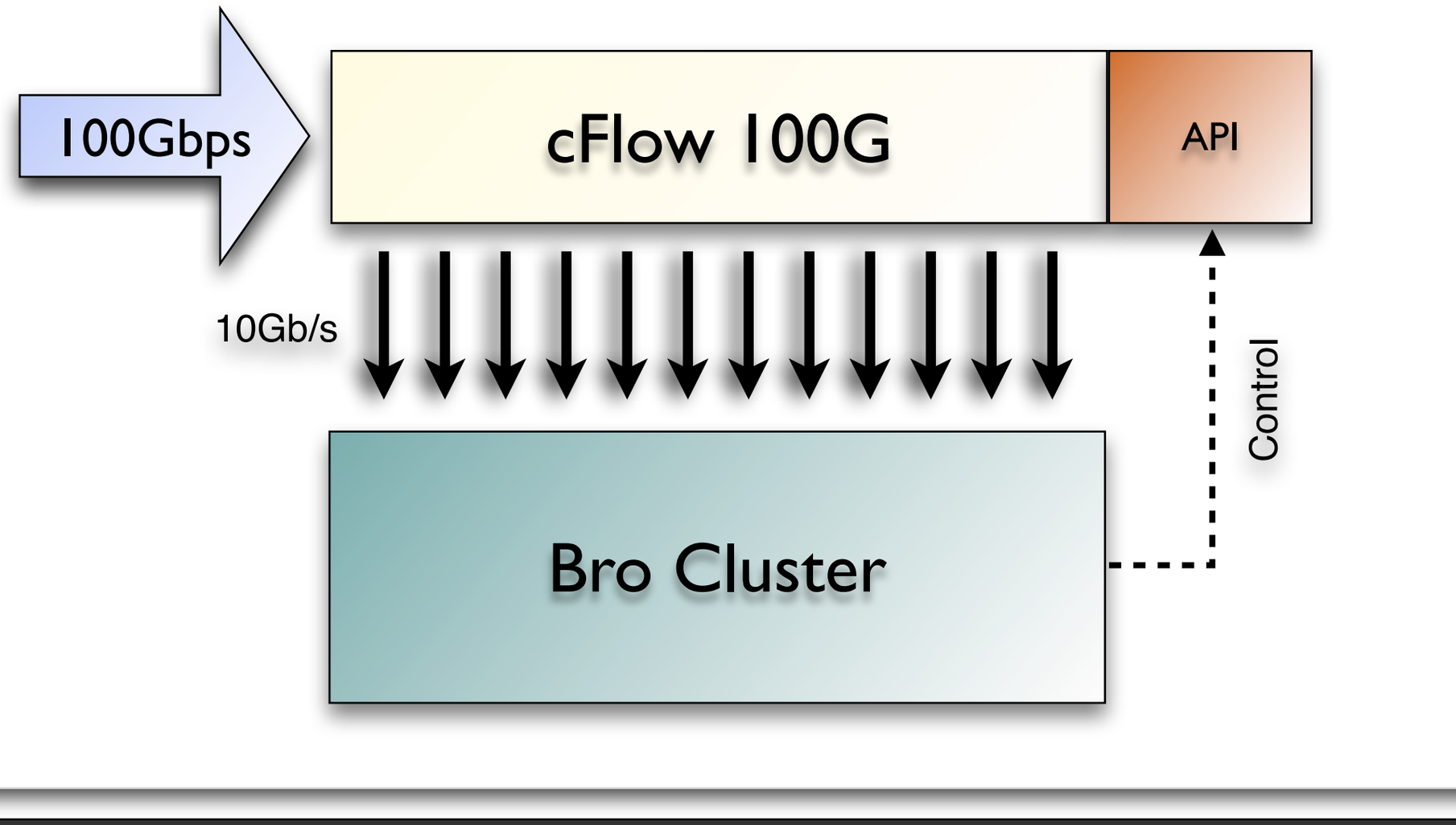


100 Gb/s Load-balancer

100 Gb/s Load-balancer



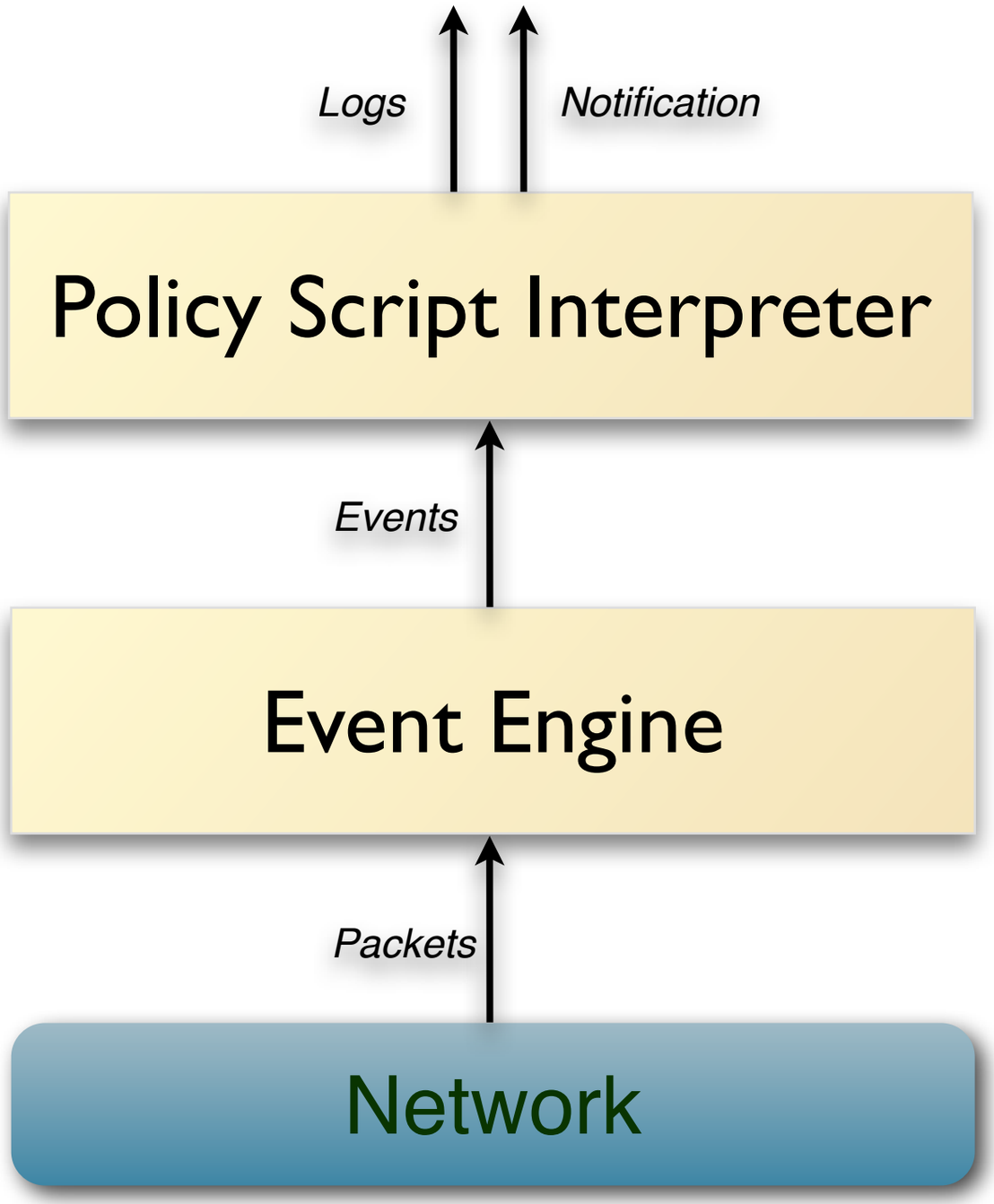
100 Gb/s Load-balancer



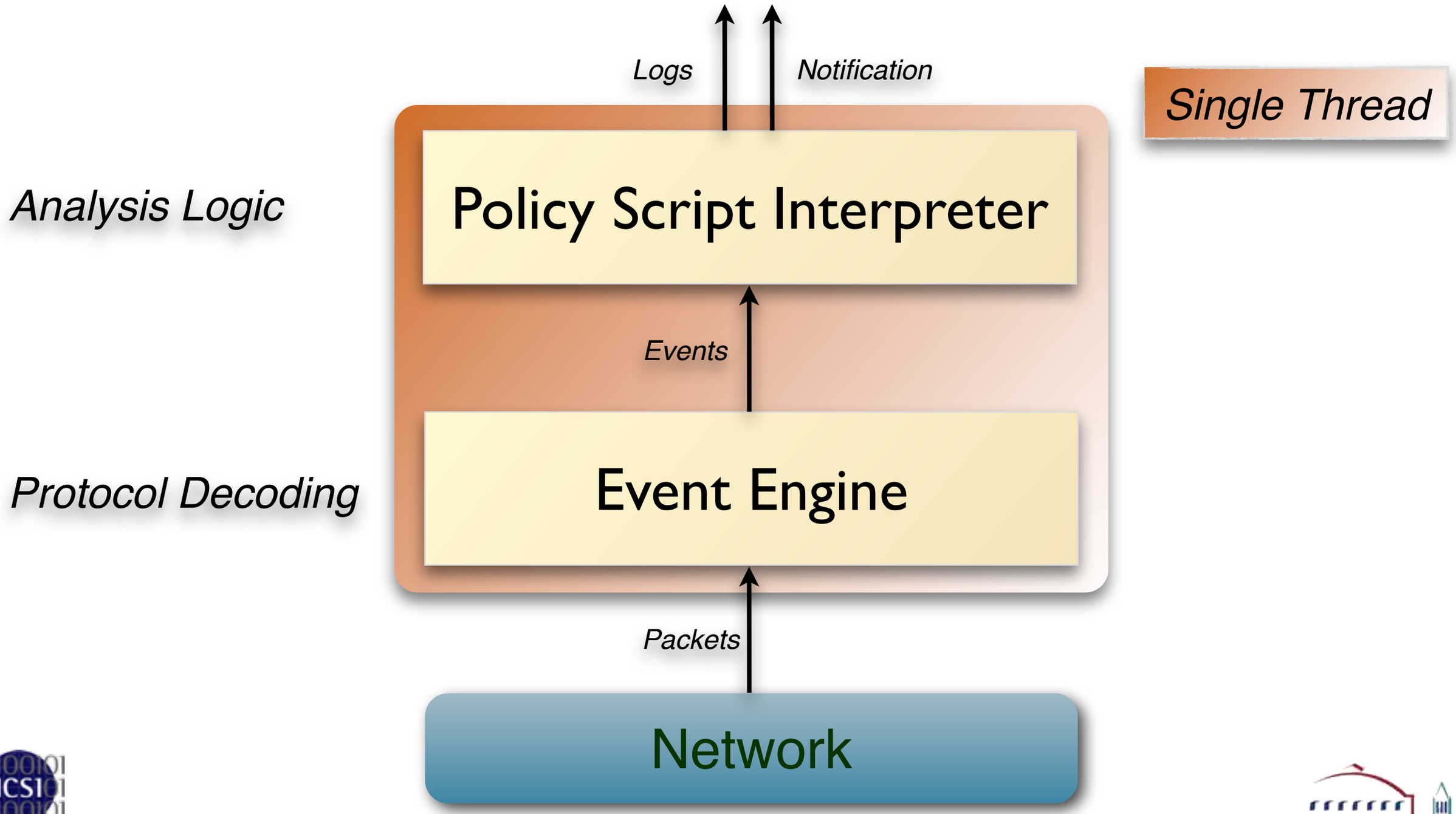
Concurrent Analysis

Analysis Logic

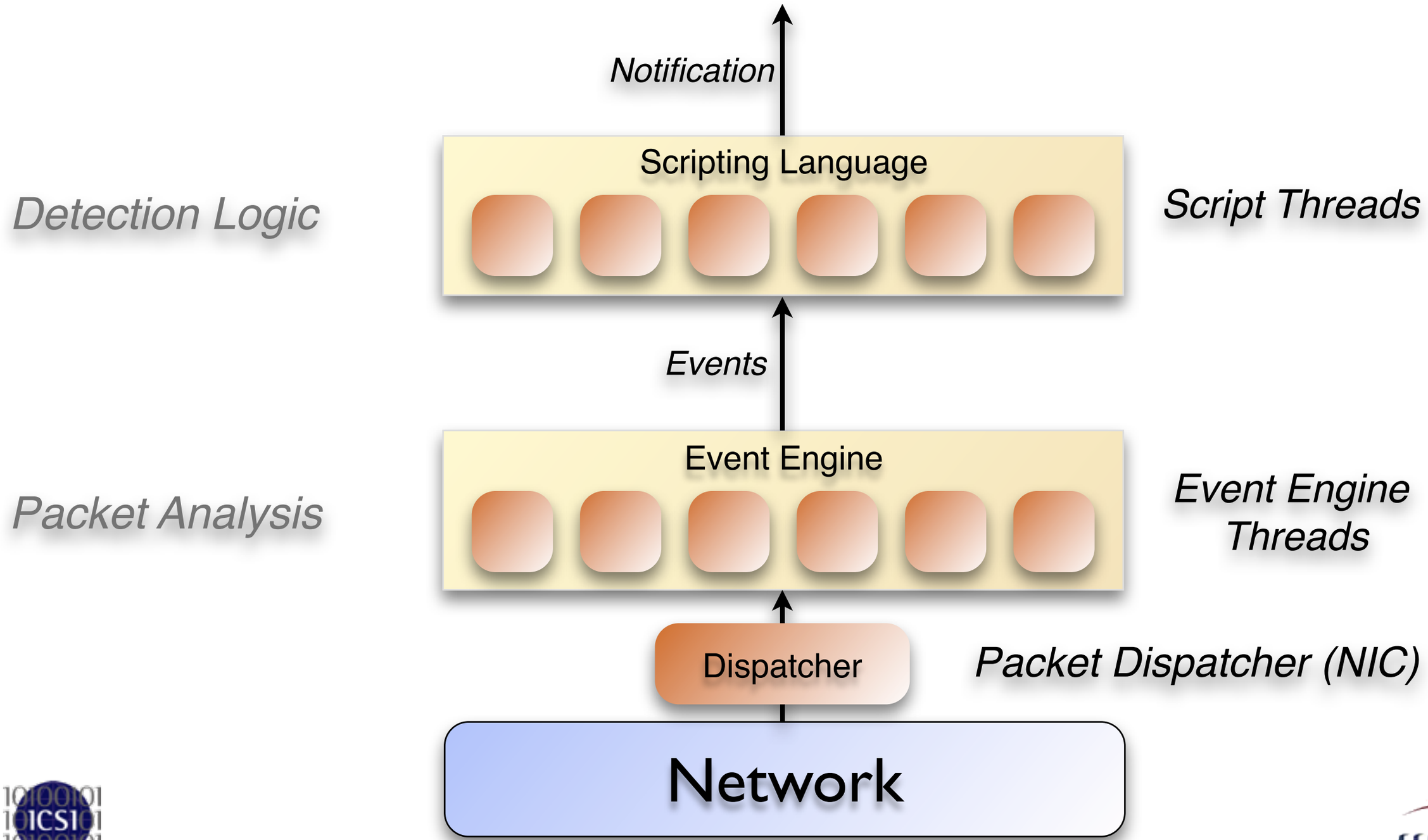
Protocol Decoding



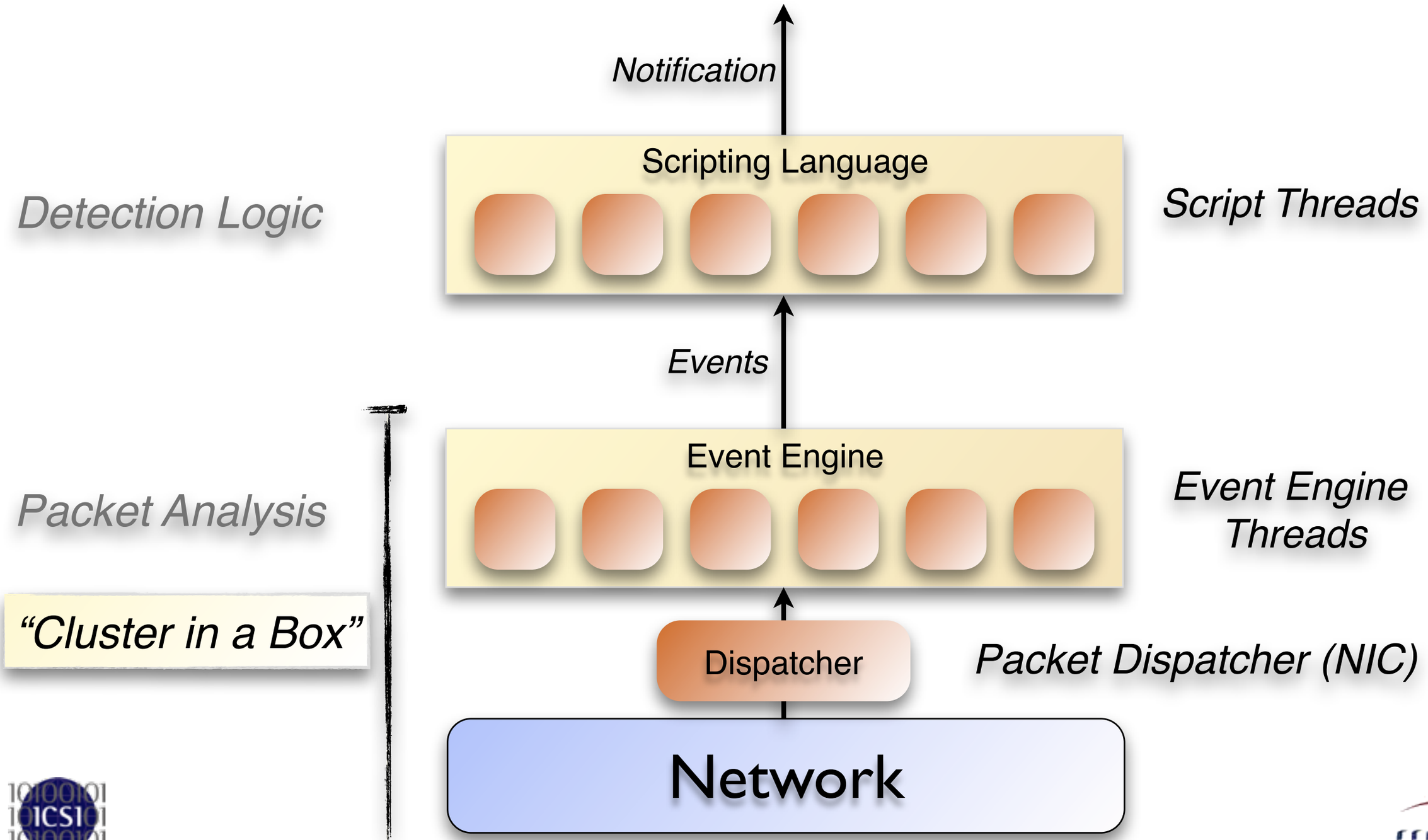
Concurrent Analysis



Architecture



Architecture



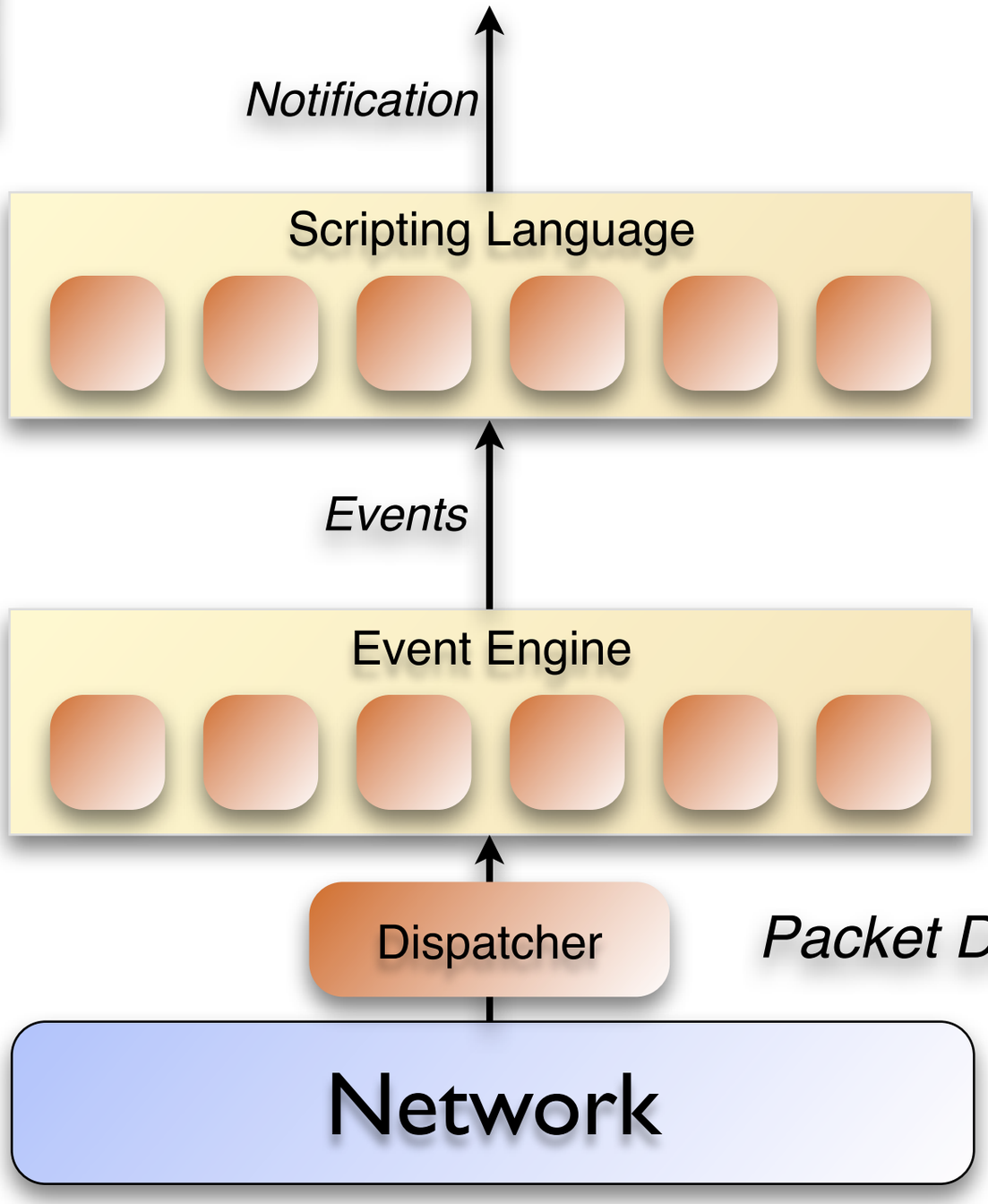
Architecture

How to parallelize a scripting language?

Detection Logic

Packet Analysis

"Cluster in a Box"



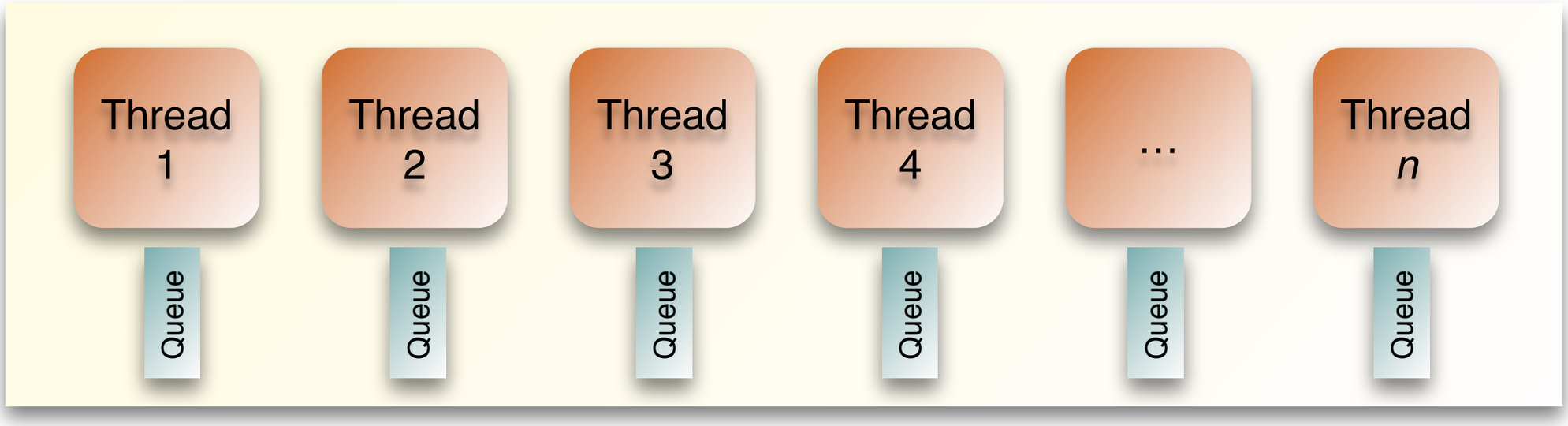
Script Threads

Event Engine Threads

Packet Dispatcher (NIC)

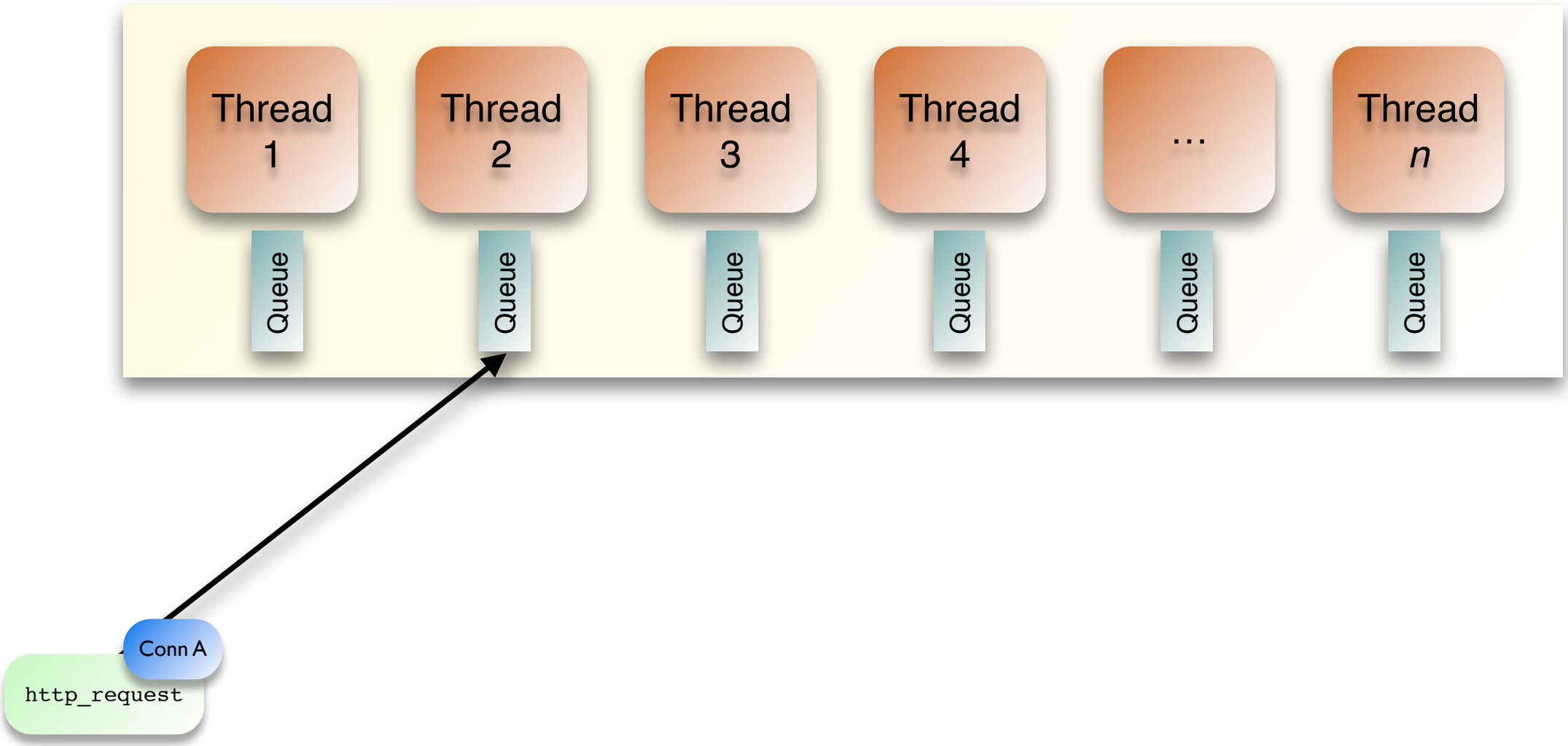
Parallel Event Scheduling

Threaded Script Interpreter



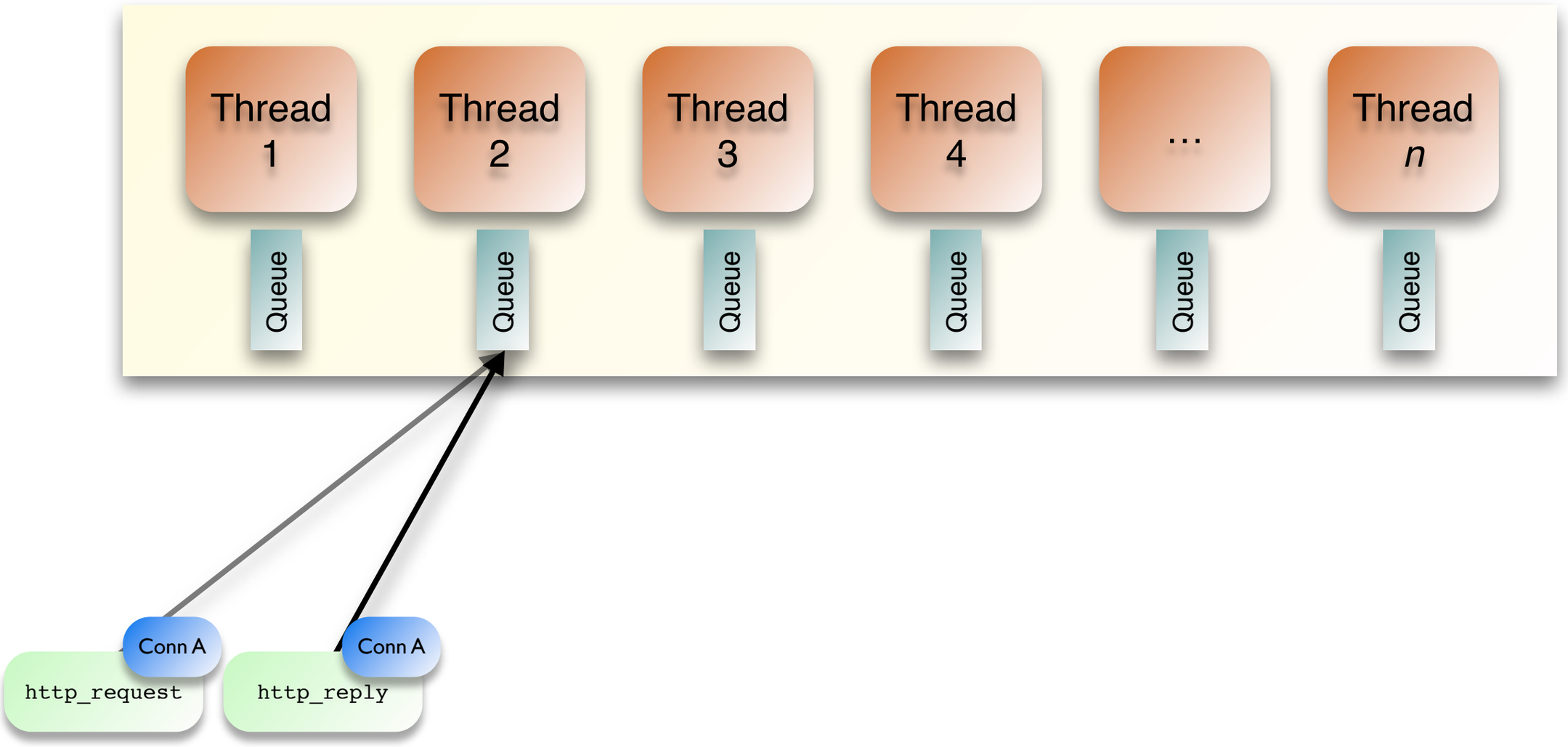
Parallel Event Scheduling

Threaded Script Interpreter



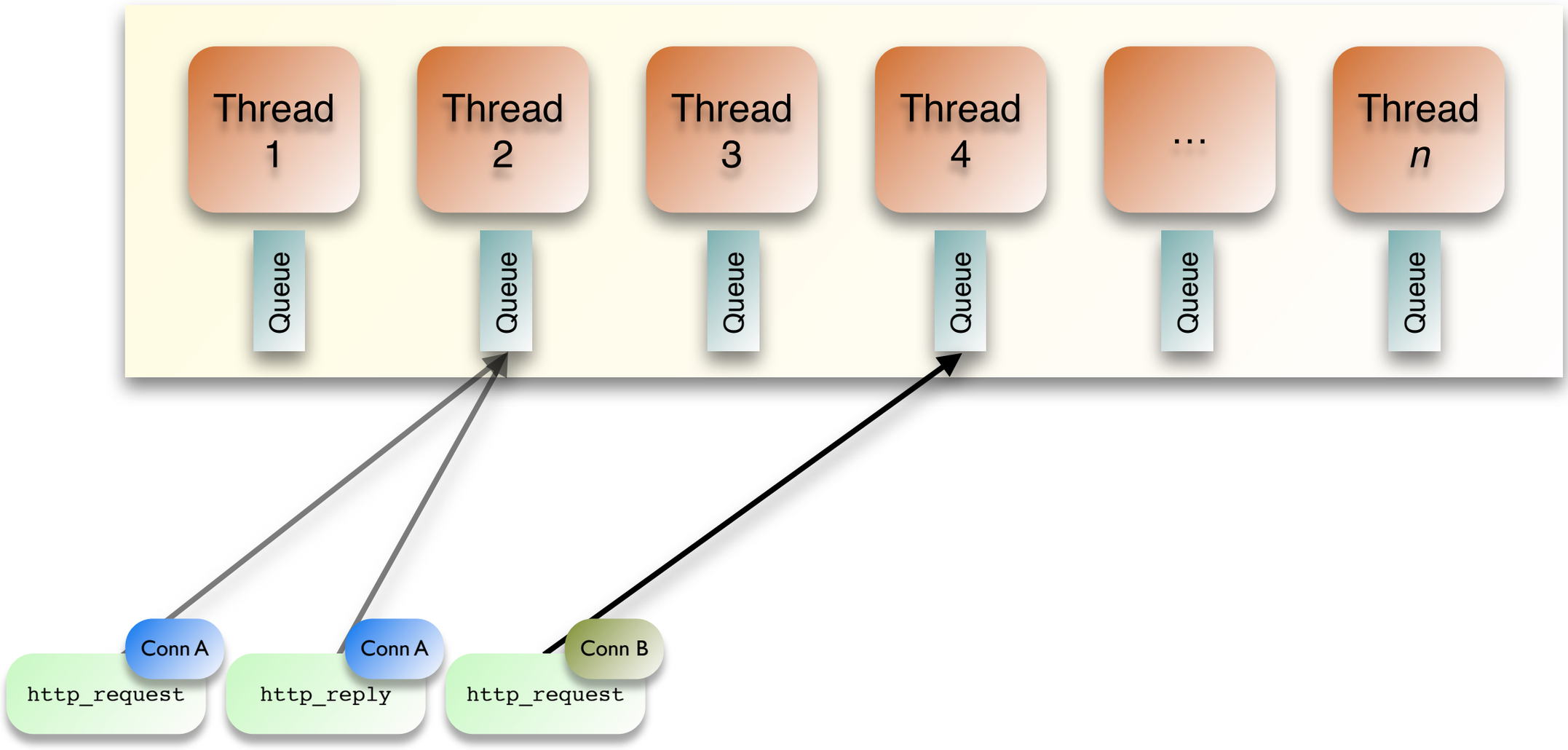
Parallel Event Scheduling

Threaded Script Interpreter



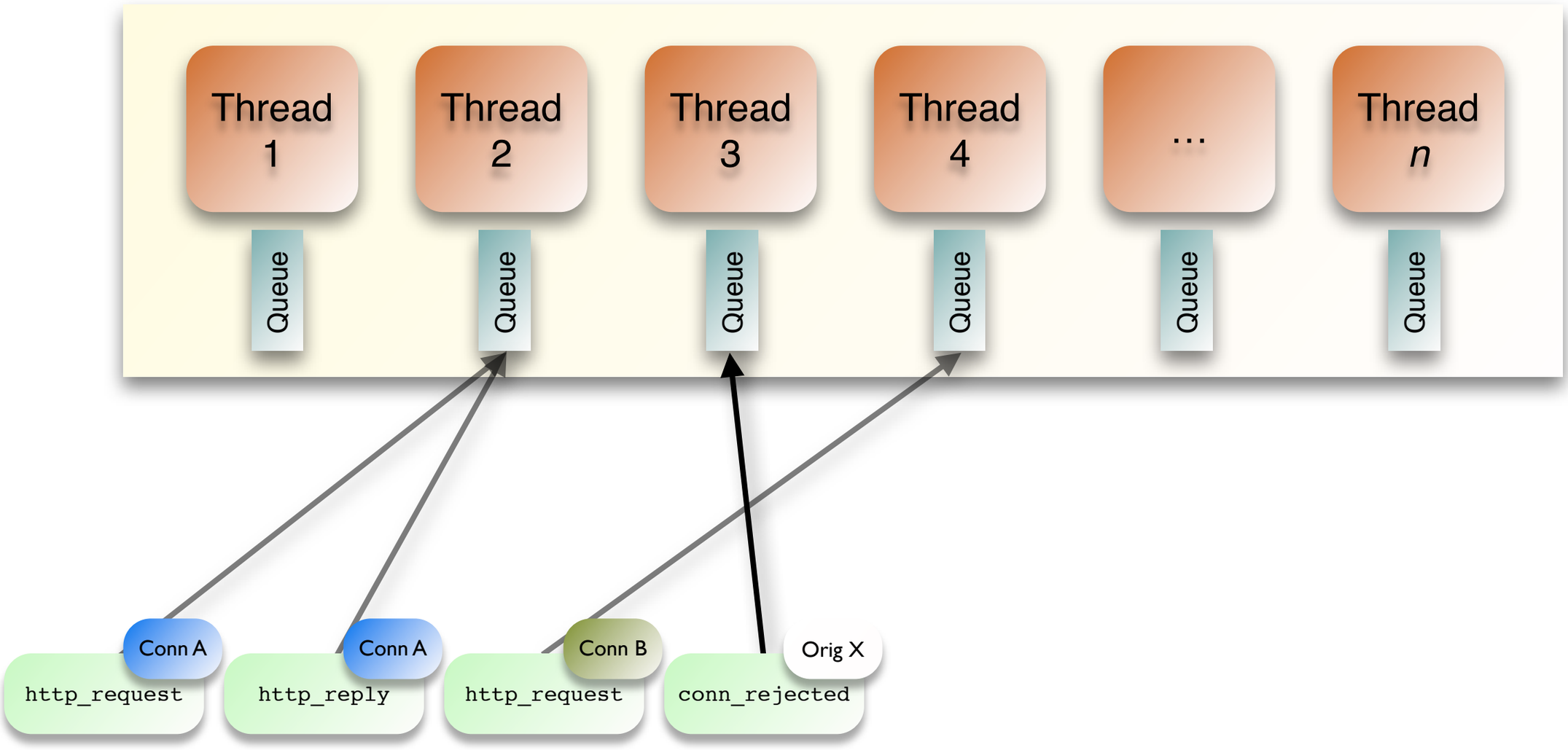
Parallel Event Scheduling

Threaded Script Interpreter



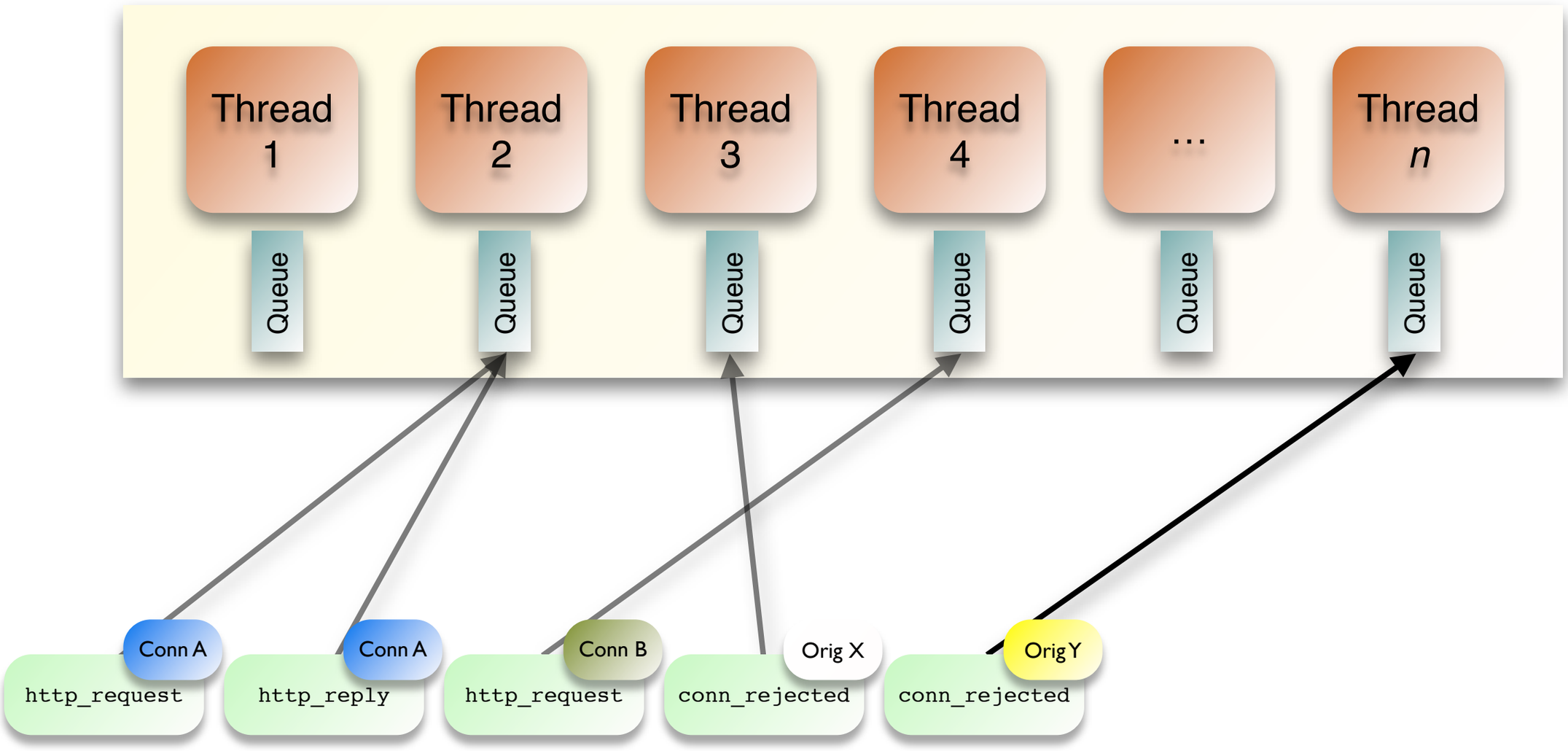
Parallel Event Scheduling

Threaded Script Interpreter



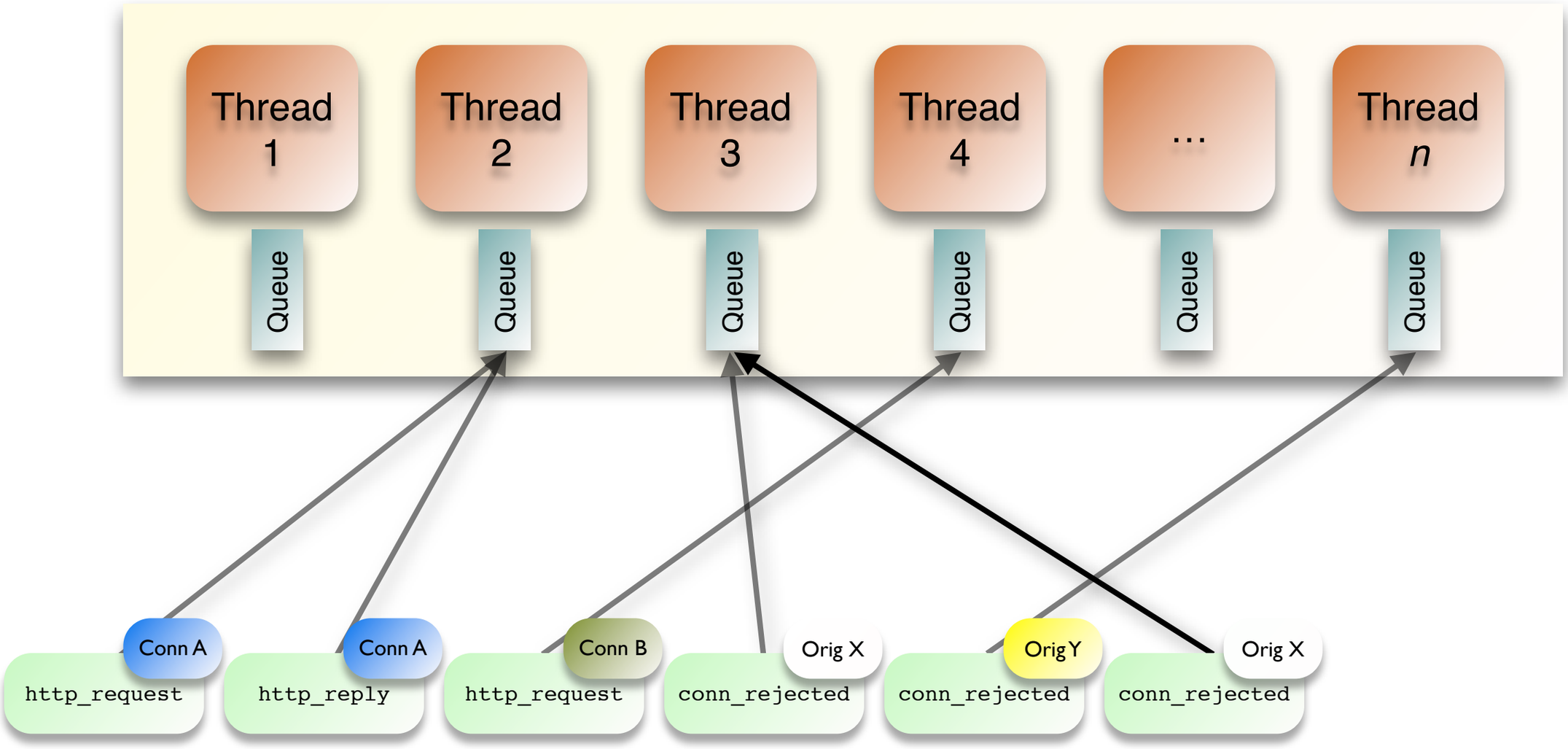
Parallel Event Scheduling

Threaded Script Interpreter



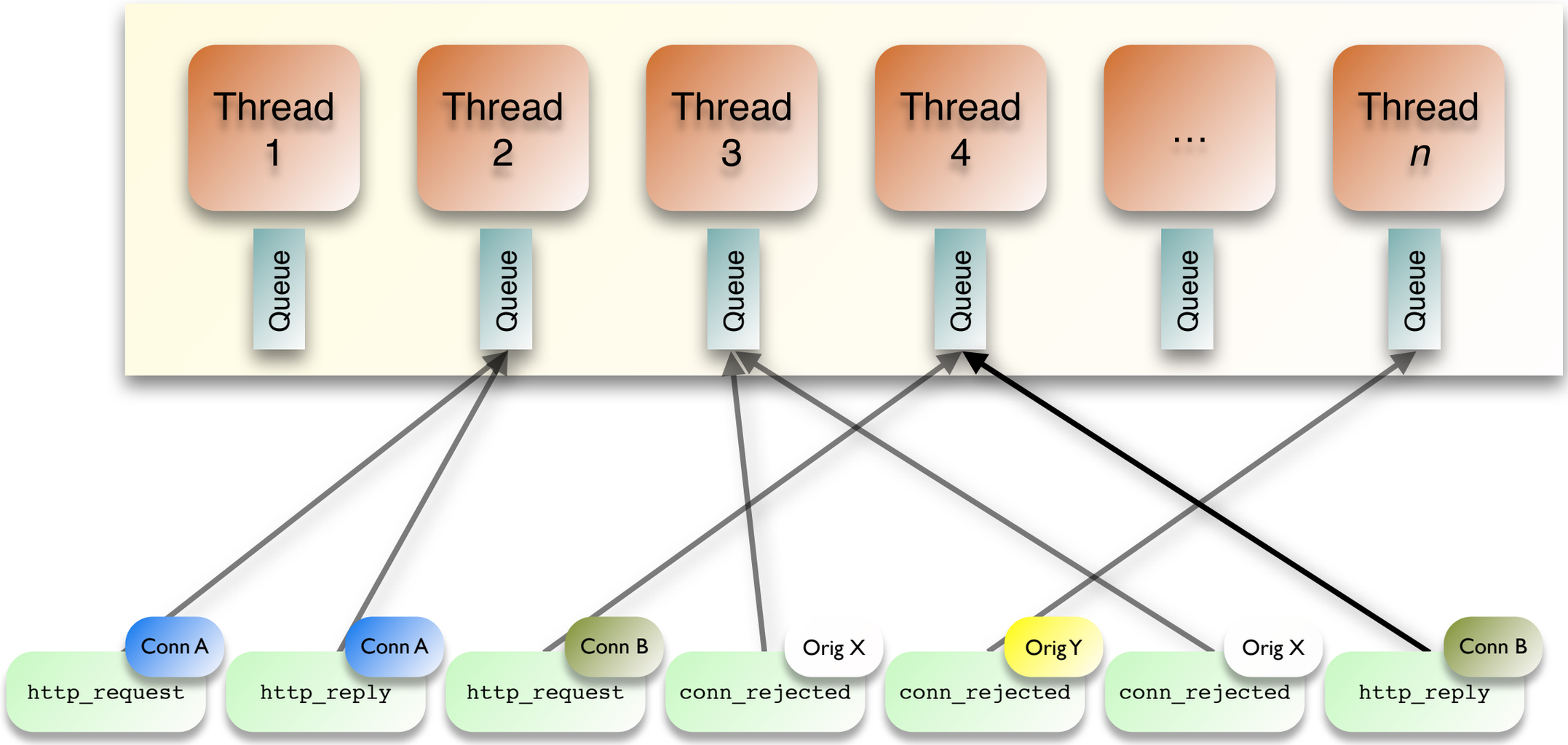
Parallel Event Scheduling

Threaded Script Interpreter



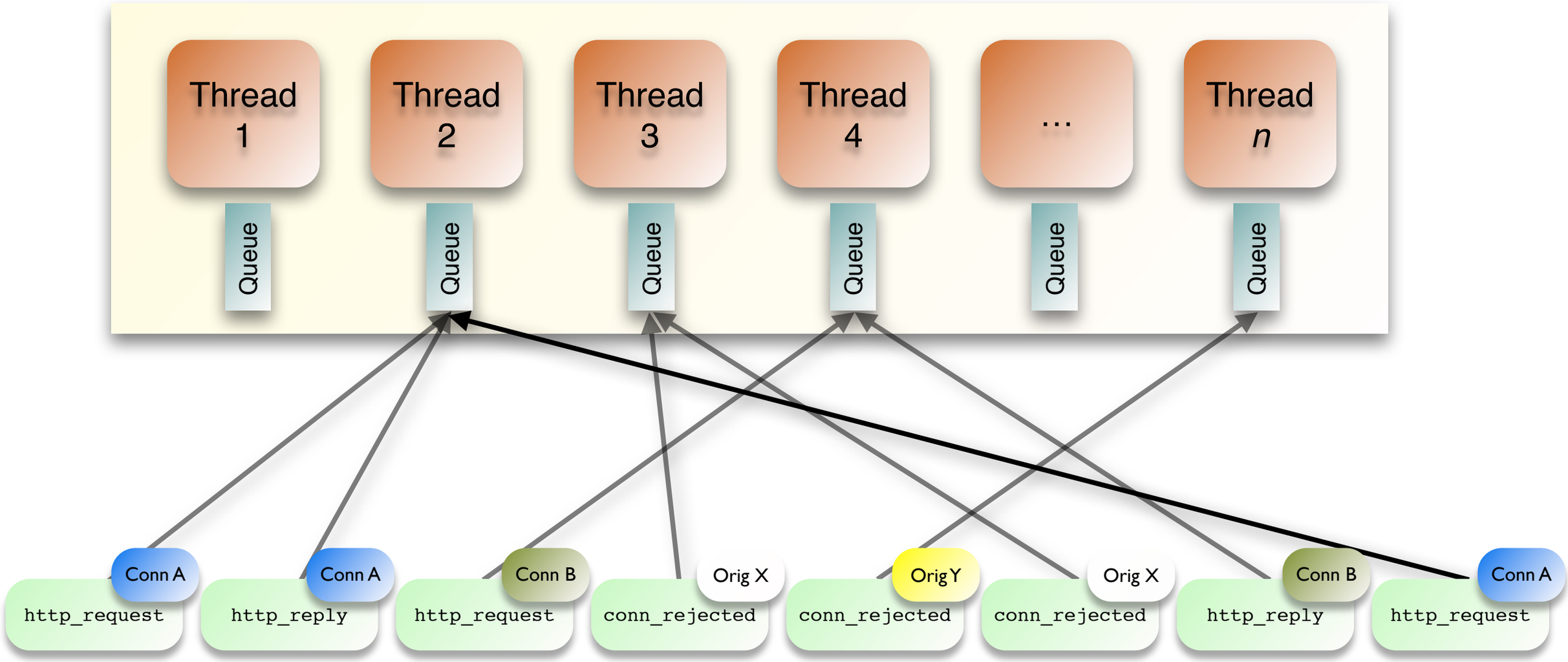
Parallel Event Scheduling

Threaded Script Interpreter



Parallel Event Scheduling

Threaded Script Interpreter



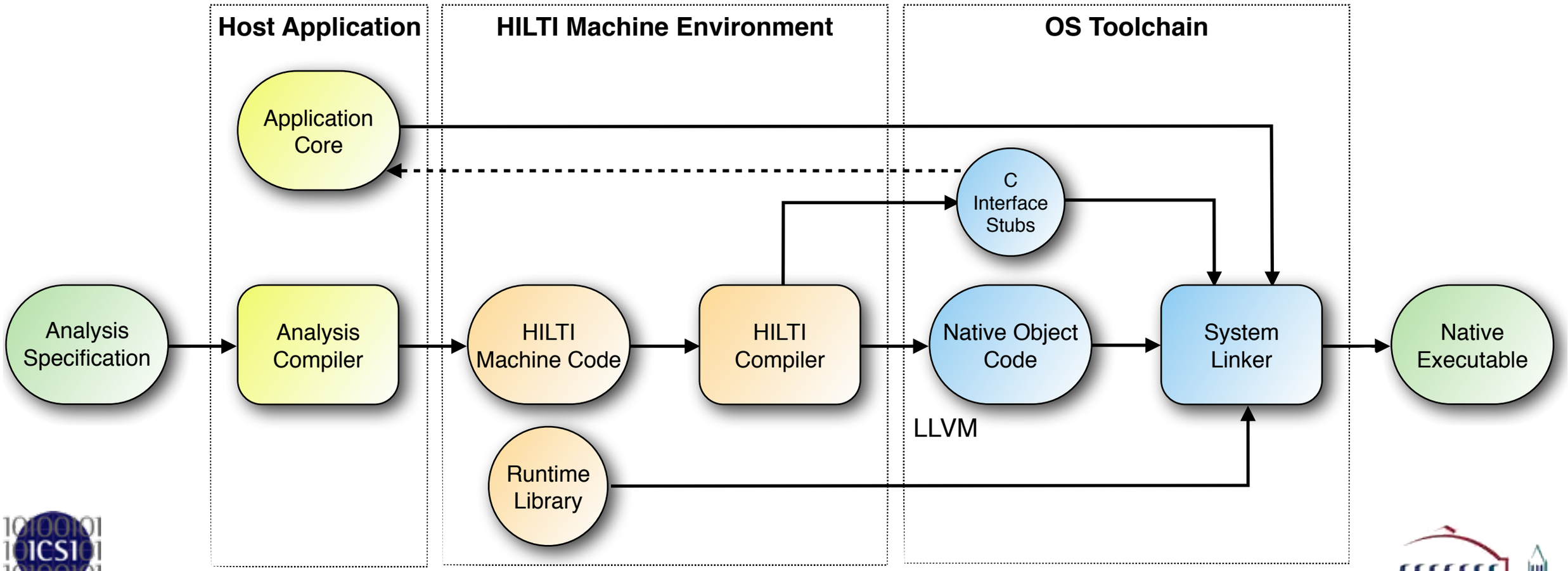
Improving Bro's Performance

Bottlenecks: Single-thread structure & Script interpretation

Improving Bro's Performance

Bottlenecks: Single-thread structure & Script interpretation

A **H**igh-Level **I**ntermediary **L**anguage for **T**raffic **I**nspection



BinPAC: "Yacc for Network Protocols"

BinPAC: "Yacc for Network Protocols"

```
type SMB_header = record {
        protocol        : bytestring &length = 4;
        command         : uint8;
        status          : SMB_error(err_status_type);
        flags           : uint8;
        flags2          : uint16;
        pad             : padding[12];
        tid             : uint16;
        pid             : uint16;
        uid             : uint16;
        mid             : uint16;
} &let {
        err_status_type = (flags2 >> 14) & 1;
        unicode         = (flags2 >> 15) & 1;
} &byteorder = littleendian;

type SMB_error (err_status_type: int) = case err_status_type of {
        0 -> dos_error: SMB_dos_error;
        1 -> status: int32;
};

type SMB_dos_error = record {
        error_class     : uint8;
        reserved        : uint8;
        error           : uint16;
};
```

Next-generation BinPAC

Next-generation BinPAC

```
type Message = unit(body_default: bool) {
  headers    : list<Header(self)>;
  end_of_hdr: /\r?\n/;
  body       : Body([...])

};
```

HTTP Message

Next-generation BinPAC

```
type Message = unit(body_default: bool) {
  headers    : list<Header(self)>;
  end_of_hdr: /\r?\n/;
  body       : Body([...])

};
```

HTTP Message

```
const HeaderName  = /[^:\r\n]+/;
const HeaderValue = /[^\r\n]*/;

type Header = unit(msg: Message) {
  name    : HeaderName;
          : /:[\t ]*/;
  content: HeaderValue;
          : NewLine;

};
```

HTTP Header

Next-generation BinPAC

```
type Message = unit(body_default: bool) {
  headers    : list<Header(self)>;
  end_of_hdr: NewLine;
  body       : Body(self, self.delivery_mode)
                 if ( self.has_body );

  on end_of_hdr {
    if ( self?.content_length )
      self.delivery_mode = DeliveryMode::Length;

    if ( self.content_type.startswith("multipart/") )
        [... Parse boundary ...]
  }

  [...]

  var content_length: uint64;
  var content_type: bytes;
  var delivery_mode: DeliveryMode;
  var has_body: bool;
  var multipart_boundary: bytes;
  var transfer_encoding: bytes;
};
```

HTTP Message

```
const HeaderName  = /[^:\r\n]+/;
const HeaderValue = /[^\r\n]*/;

type Header = unit(msg: Message) {
  name    : HeaderName &convert=to_lower;
          : /:[\t ]*/;
  content: HeaderValue;
          : NewLine;

  on content {
    if ( self.name == "content-length" ) {
      msg.content_length = to_uint(self.content);
      msg.has_body = True;
    }

    if ( self.name == "transfer-encoding" ) {
      msg.transfer_encoding = self.content;
      msg.has_body = True;
    }

    if ( self.name == "content-type" )
      msg.content_type = self.content;
};
```

HTTP Header

Next-generation BinPAC

BinPAC++

- Streamlined usage.
- Adding semantics to syntax.
- Decoding layers of protocols.
- Robust error handling.
- Fully usable outside of Bro.
- *Compiles to HILTI.*

```
type Message = unit(body_de
  headers    : list<Header(s
  end_of_hdr: NewLine;
  body       : Body(self, se
                 if ( self.h

  on end_of_hdr {
    if ( self?.content_leng
      self.delivery_mode =

    if ( self.content_type.
        [... Parse boundary
  }

  [...]

  var content_length: uint6
  var content_type: bytes;
  var delivery_mode: DeliveryMode;
  var has_body: bool;
  var multipart_boundary: bytes;
  var transfer_encoding: bytes;
};
```

HTTP Message

```
:\r\n]+/;
\r\n]*/;

: Message) {
convert=to_lower;

;

'content-length" ) {
h = to_uint(self.content);
ue;

'transfer-encoding" ) {
oding = self.content;
  msg.has_body = True;
}

if ( self.name == "content-type" )
  msg.content_type = self.content;
};
```

HTTP Header

Outlook & Conclusion

More Things in the Bro Queue ...

More Things in the Bro Queue ...

Comprehensive File Analysis

Intelligence Framework

Metrics Framework

Database interface

Packet Filter Framework

New/improved protocol analyzers
SMB/GridFTP/Modbus/DNP3

Reaction Framework

Load-balancer Interface

The Curse of Success ...

The Curse of Success ...

Success can be kind of problematic in research ...

- Bro is now used operationally by many sites.
- Demands of operations community hard to meet for small team.

The Curse of Success ...

Success can be kind of problematic in research ...

- Bro is now used operationally by many sites.
- Demands of operations community hard to meet for small team.

Aiming to establish sustainable development model.

- Modernize the system to make usage and contributions easier.
- Develop a community around the project.

The Curse of Success ...

Success can be kind of problematic in research ...

- Bro is now used operationally by many sites.
- Demands of operations community hard to meet for small team.

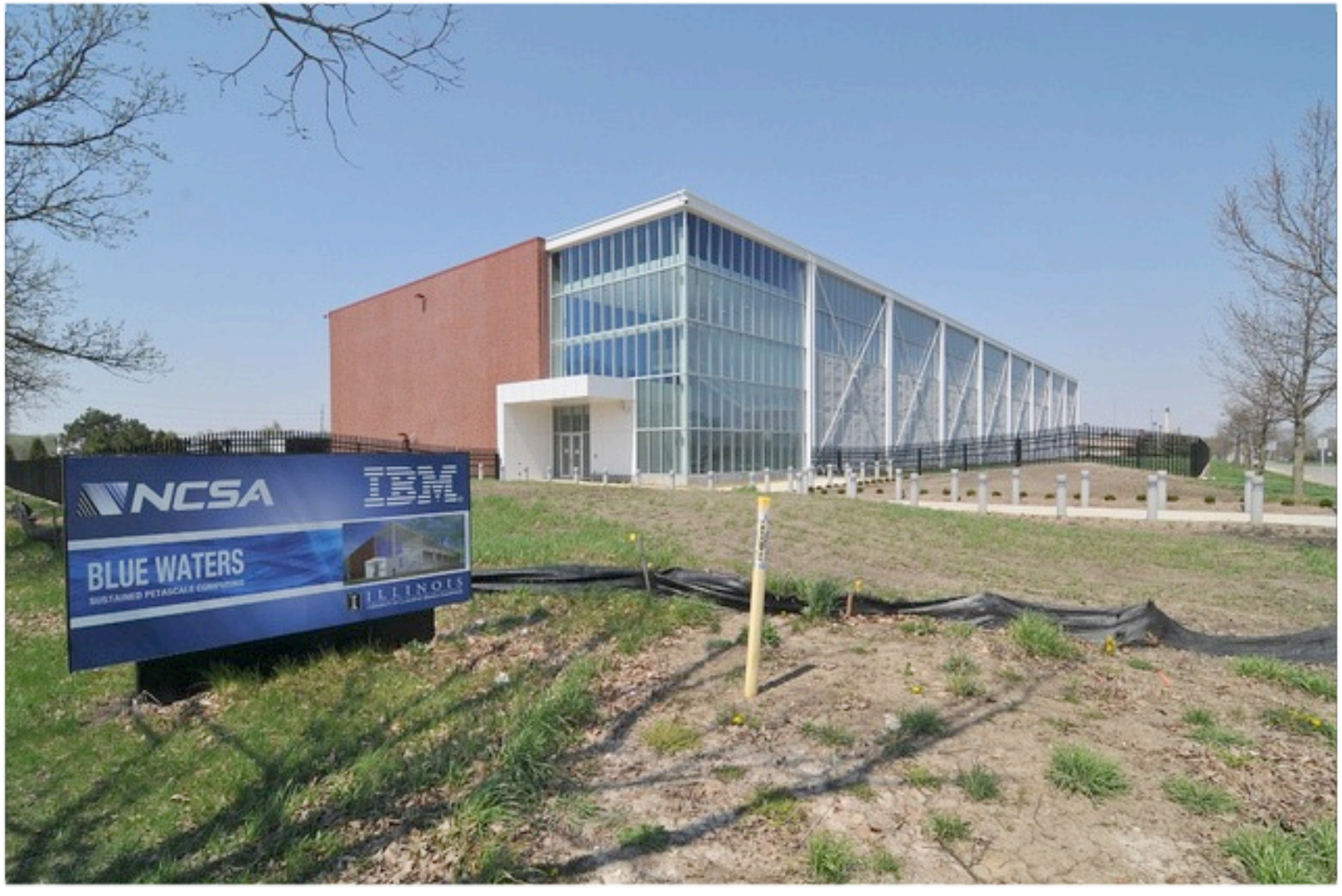
Aiming to establish sustainable development model.

- Modernize the system to make usage and contributions easier.
- Develop a community around the project.

NSF supports work through a 3-year *engineering* grant.

- Bro changed a lot over the couples years.
- Collaboration with National Center for Supercomputing Applications.

Target: Blue Waters @ NCSA



Target: Blue Waters @ NCSA

10 PF/s peak performance

>1 PF/s sustained on applications
>300,000 cores
>1 Petabyte memory
>10 Petabyte disk storage
>0.5 Exabyte archival storage

Hosted in 88,000-square-foot facility

Summary

Summary

Bro will keep bridging the research/operations gap.

We have plenty more ideas ...

Summary

Bro will keep bridging the research/operations gap.

We have plenty more ideas ...

Long-term goal is a sustainable development model.

We are planing to offer commercial services and support.

Summary

Bro will keep bridging the research/operations gap.

We have plenty more ideas ...

Long-term goal is a sustainable development model.

We are planing to offer commercial services and support.

```
www.bro-ids.org
blog.bro-ids.org
git.bro-ids.org
tracker.bro-ids.org
@Bro_IDS on Twitter
```

Summary


```
www.bro-ids.org
blog.bro-ids.org
git.bro-ids.org
tracker.bro-ids.org
@Bro_IDS on Twitter
```