Broadmap

Bro Workshop 2011
NCSA, Urbana-Champaign, IL

Outline

Near- to Medium-term Roadmap

Current Research Projects

Workshop Wrap-Up

Version 2.0 Final

Version 2.0 Final

Timeline: Early December.

Default scripts rewritten from scratch.

New logging system.

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.

Upcoming

Upcoming

Bro 2.1

New user's guide.

Overhauled IPv6 support.

Logging extensions.

Binary logging/Postgresql/CouchDB/SQLite(?) / Threads.

Integration with REN-ISACs CIF.

Reaction framework.

New/improved analyzers.

Syslog/GridFTP/NFS/SMB/BitTorrent.

Extended test-suite.

Aiming for 3-4 months release cycle.

In Planning

In Planning

Comprehensive Bro Archive Network (CBAN)

Easy installation of 3rd party scripts.

In Planning

Comprehensive Bro Archive Network (CBAN)

Easy installation of 3rd party scripts.

File Analyzer

Protocol-independent file hashing, extraction, decompression, analysis, and reassembly.

In Planning

Comprehensive Bro Archive Network (CBAN)

Easy installation of 3rd party scripts.

File Analyzer

Protocol-independent file hashing, extraction, decompression, analysis, and reassembly.

Input Framework.

Real-time interface to external intelligence.

In Planning

In Planning

Deep Cluster

Pushing Bro deep into your network.

In Planning

Deep Cluster

Pushing Bro deep into your network.

Unified packet acquisition and control.

Plugin-based interface to platform capabilities.

In Planning

Deep Cluster

Pushing Bro deep into your network.

Unified packet acquisition and control.

Plugin-based interface to platform capabilities.

New/extended protocol analyzers.

Ongoing focus. Working on BinPAC++.

In Planning

Deep Cluster

Pushing Bro deep into your network.

Unified packet acquisition and control.

Plugin-based interface to platform capabilities.

New/extended protocol analyzers.

Ongoing focus. Working on BinPAC++.

Internal reorganization and cleanup.

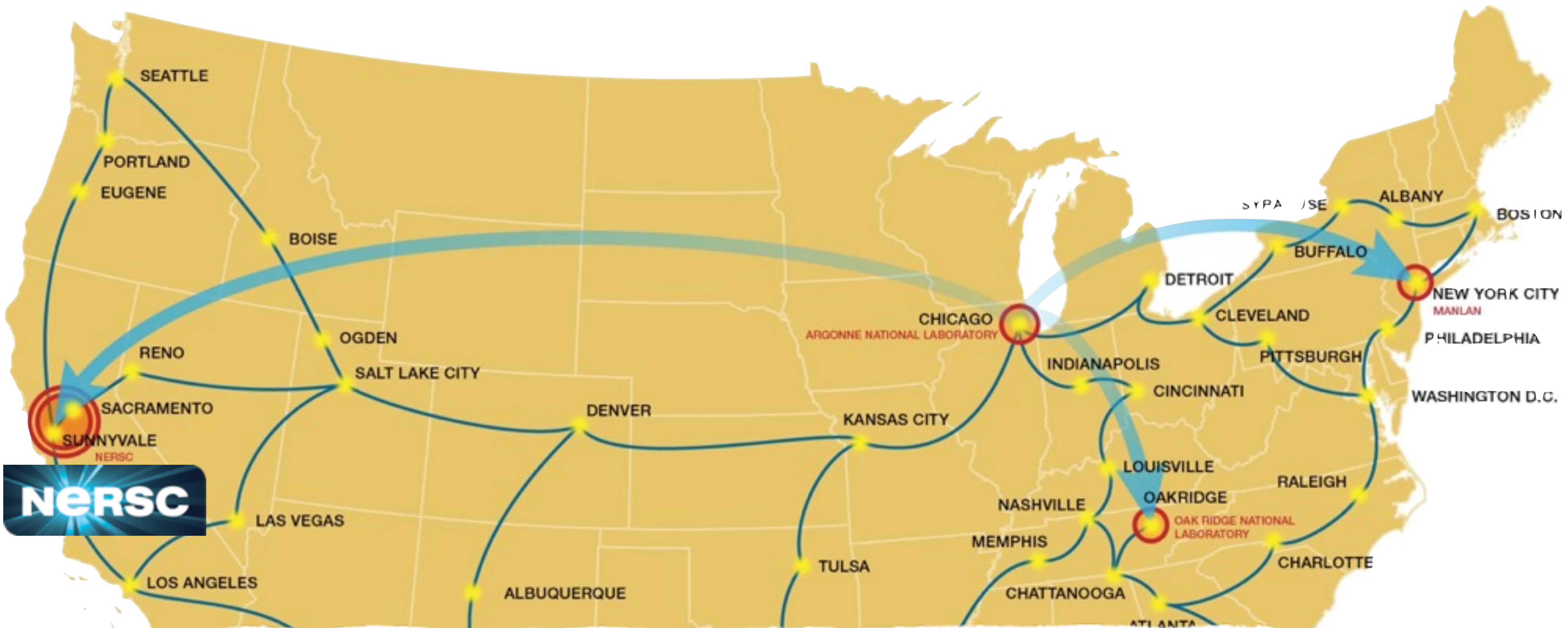
Move to a more modular structure.

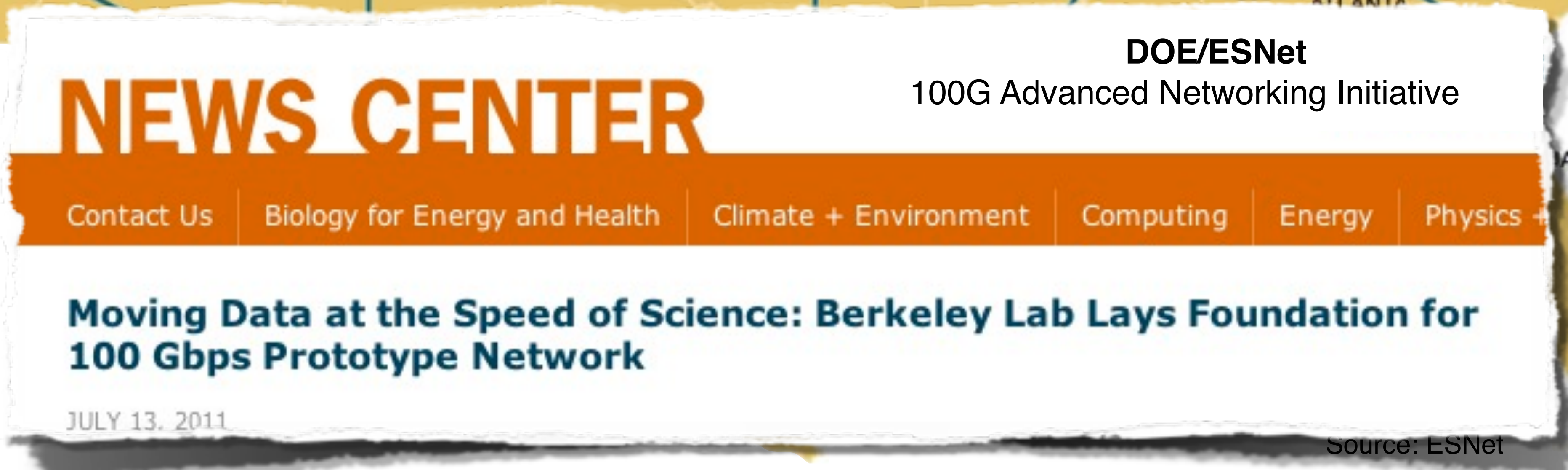
Current Research Projects

ICSI

INTERNATIONAL COMPUTER SCIENCE INSTITUTE

Next Stop: 100 Gb/s





NEWS CENTER

DOE/ESNet
100G Advanced Networking Initiative

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

Source: ESNet

100 Gb/s Load-balancer

100 Gb/s Load-balancer

U.S. DEPARTMENT OF ENERGY | Office of Science

100 Gb/s Load-balancer

SBIR Phase 2 to build prototype.

100 Gb/s Load-balancer

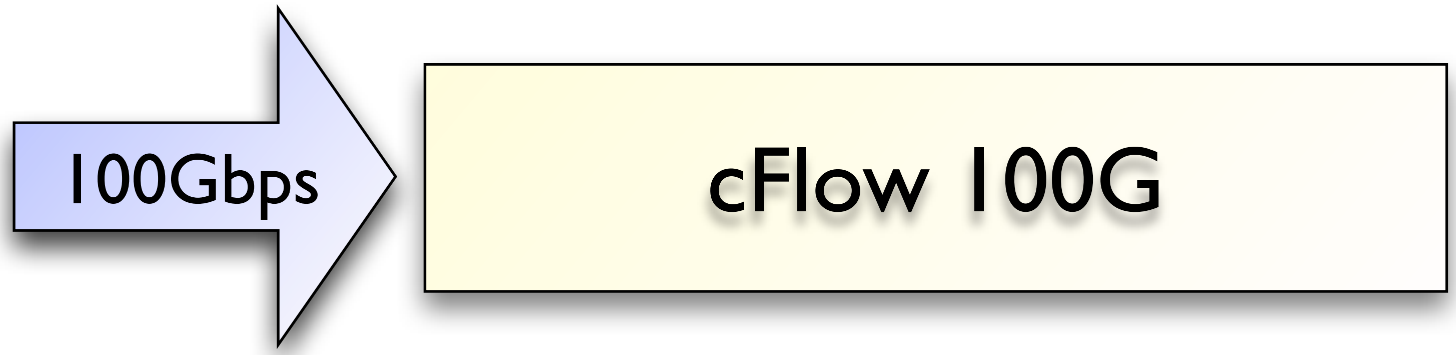
U.S. DEPARTMENT OF ENERGY | Office of Science

cpacket NETWORKS

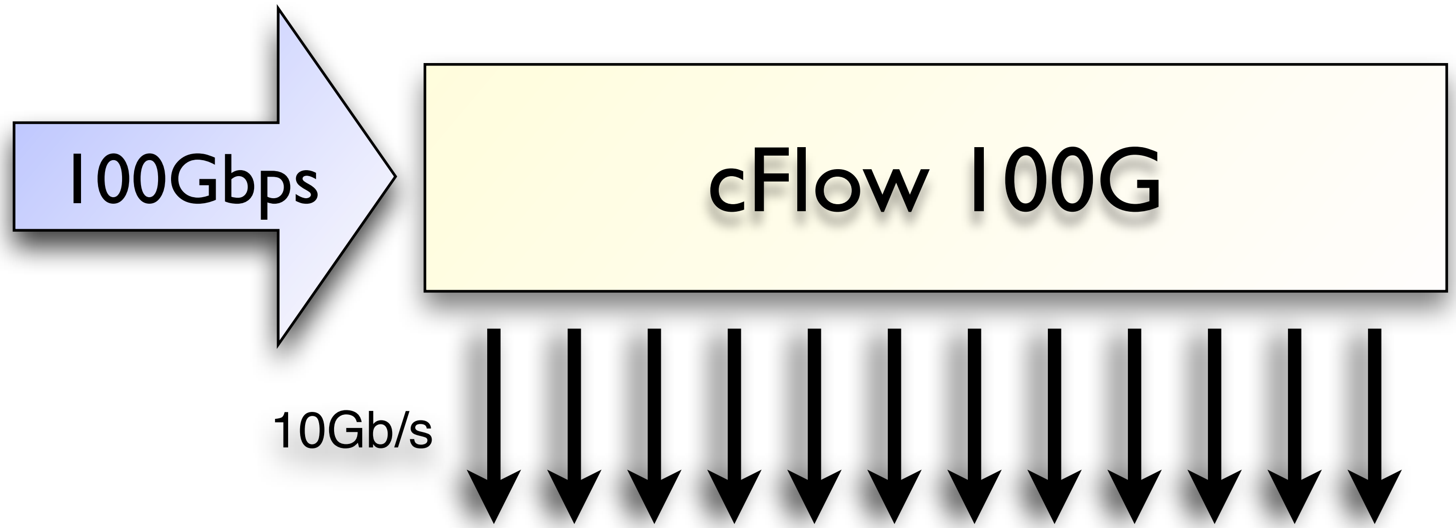
ICSI INTERNATIONAL COMPUTER SCIENCE INSTITUTE

NERSC

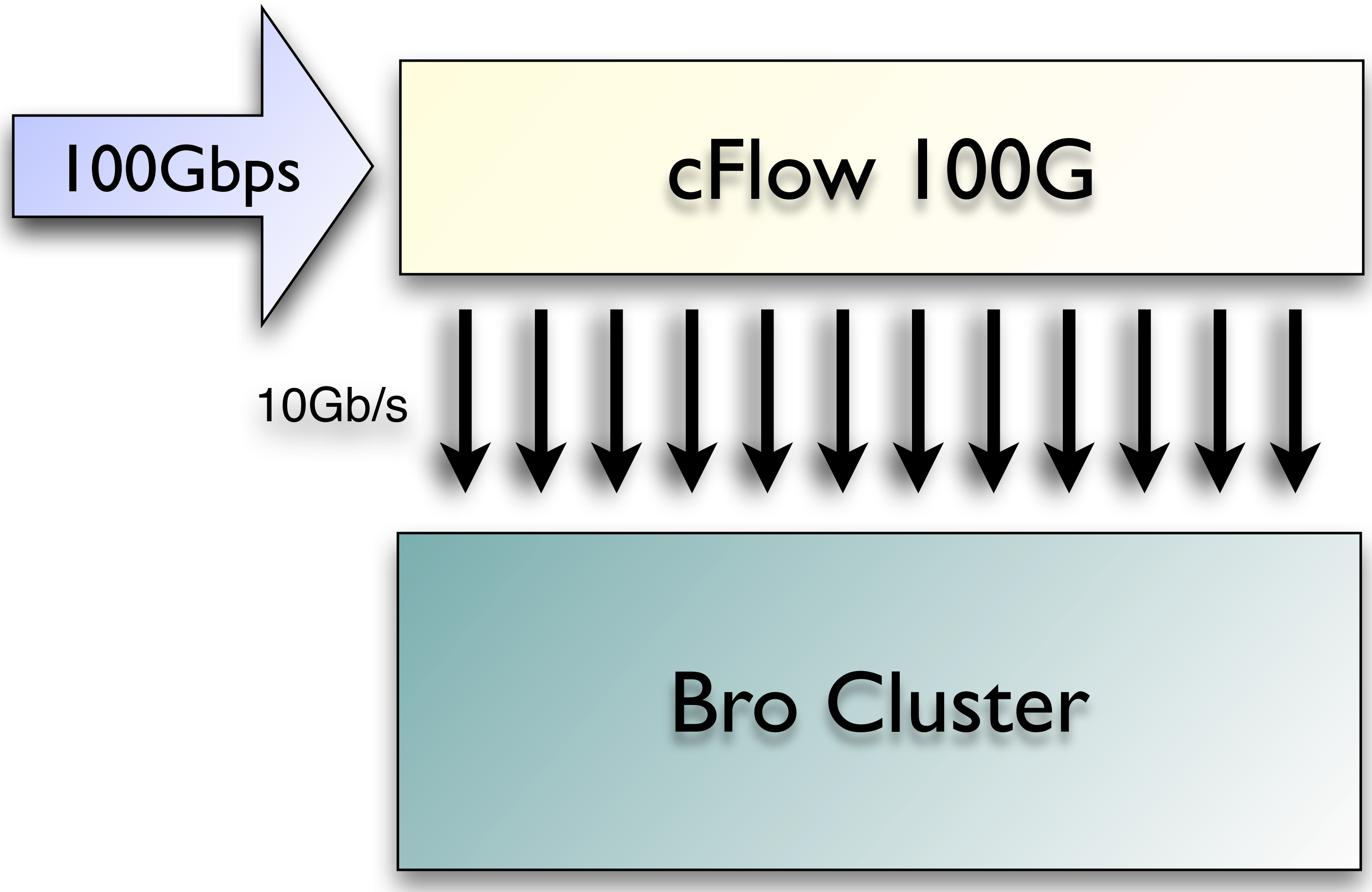
100 Gb/s Load-balancer



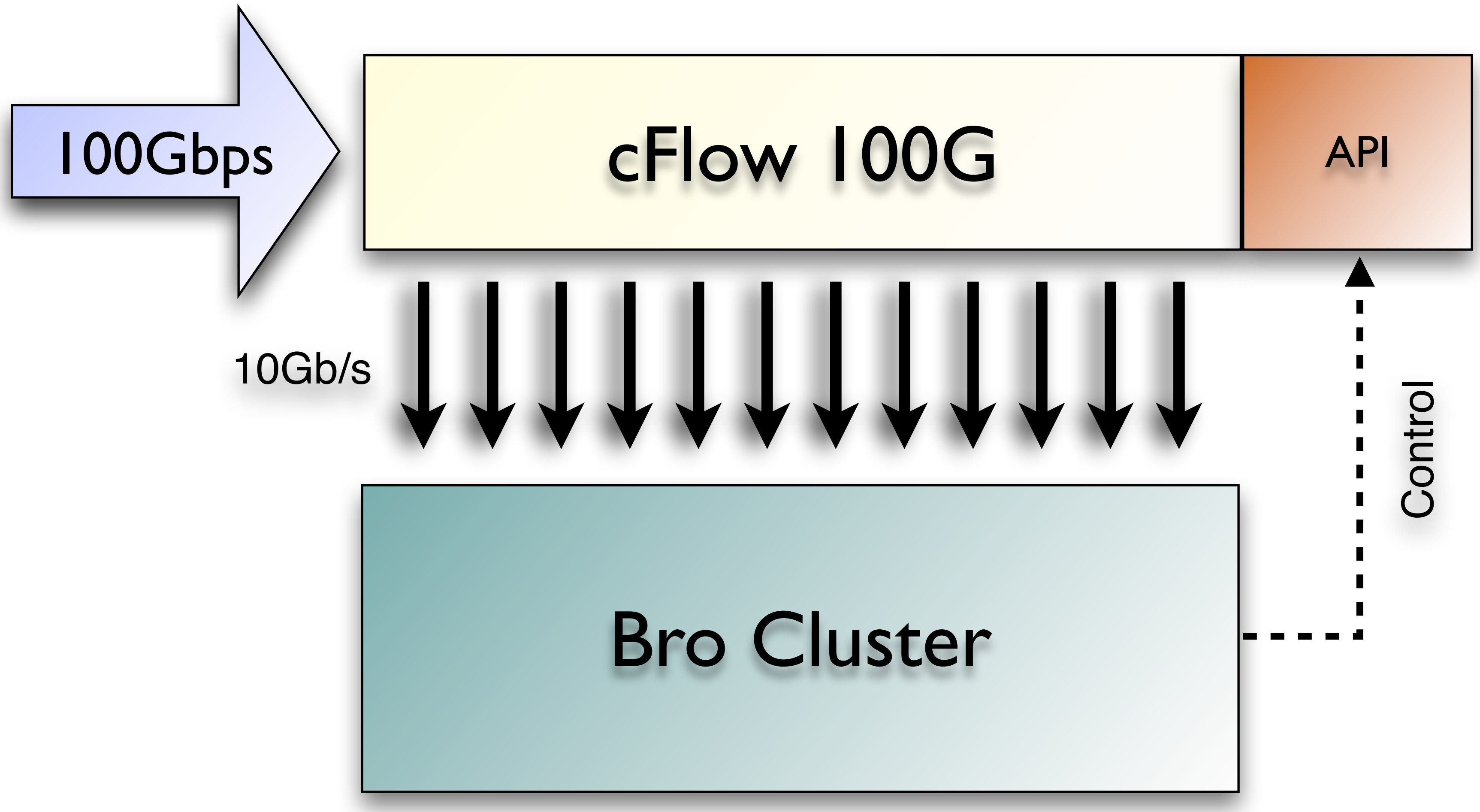
100 Gb/s Load-balancer



100 Gb/s Load-balancer



100 Gb/s Load-balancer



Concurrent Analysis

Concurrent Analysis

Bro is still single-threaded.

Cluster leverages advanced packet-level capabilities to exploit multi-core systems.

Concurrent Analysis

Bro is still single-threaded.

- Cluster leverages advanced packet-level capabilities to exploit multi-core systems.

Eventually, we want multi-threading.

- Scaling with number of cores.
- Transparent to the operator.

Concurrent Analysis

Bro is still single-threaded.

Cluster leverages advanced packet-level capabilities to exploit multi-core systems.

Eventually, we want multi-threading.

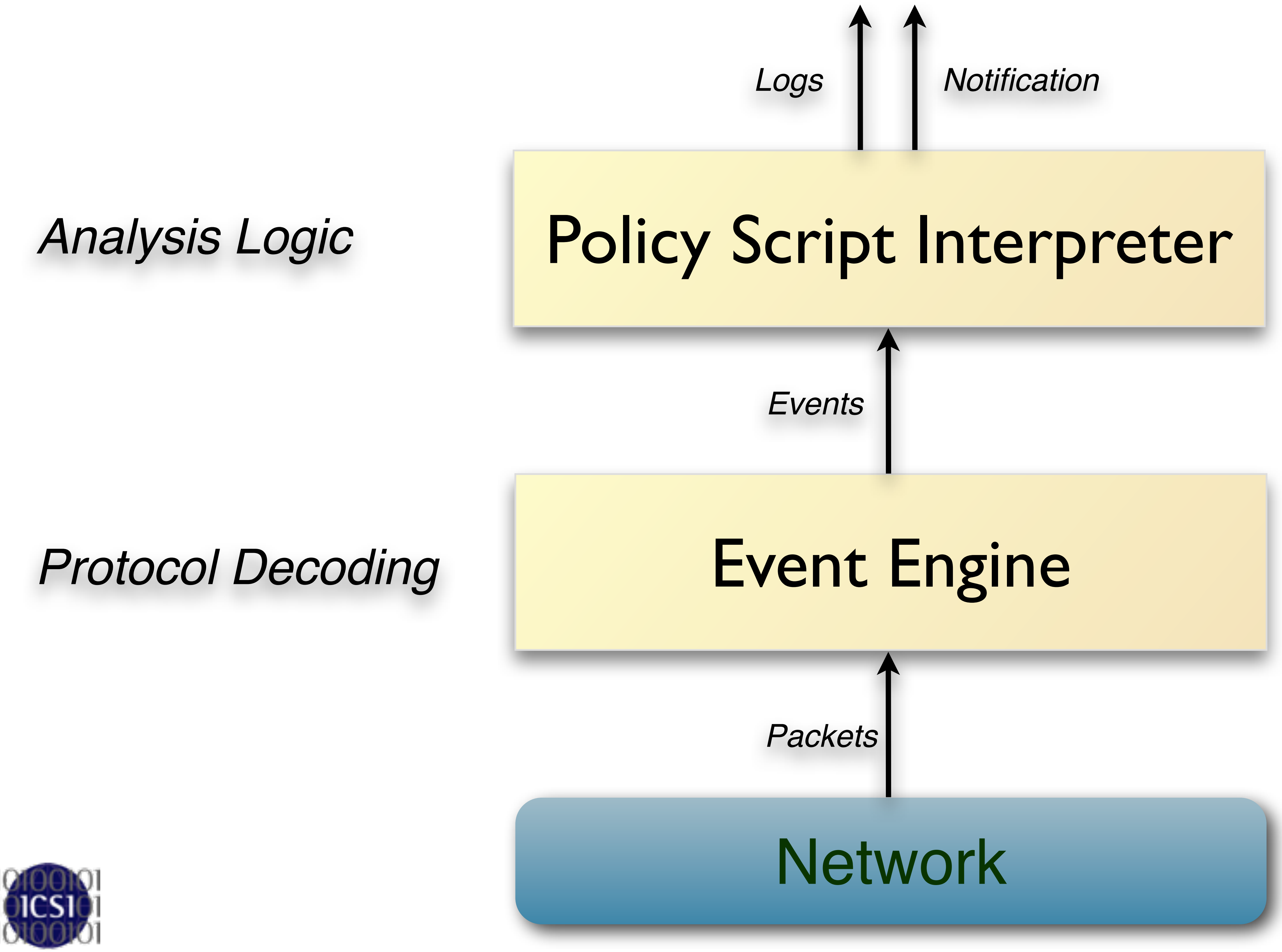
Scaling with number of cores.

Transparent to the operator.

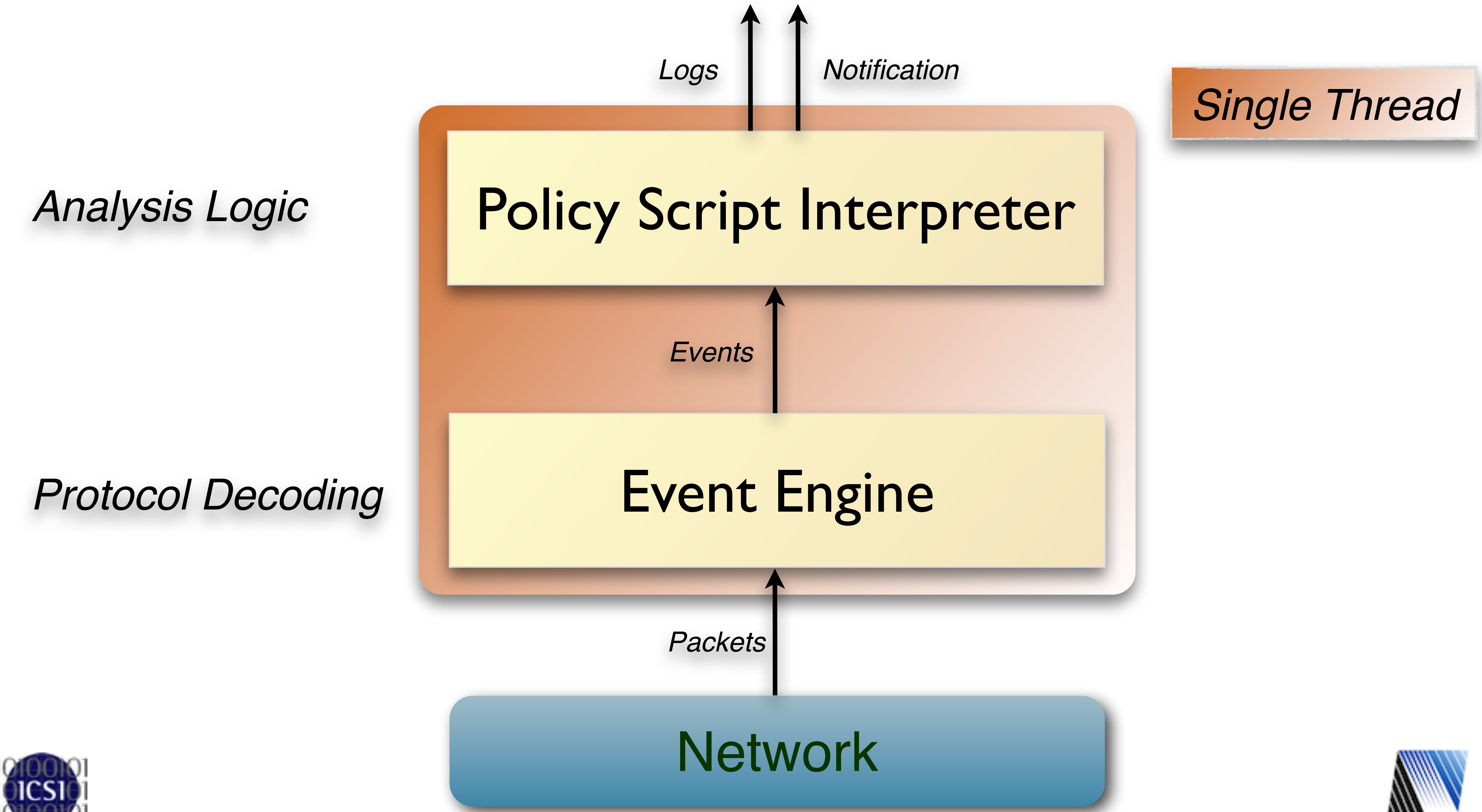
For some IDS, that's not so hard.

For others, it is ...

Architecture



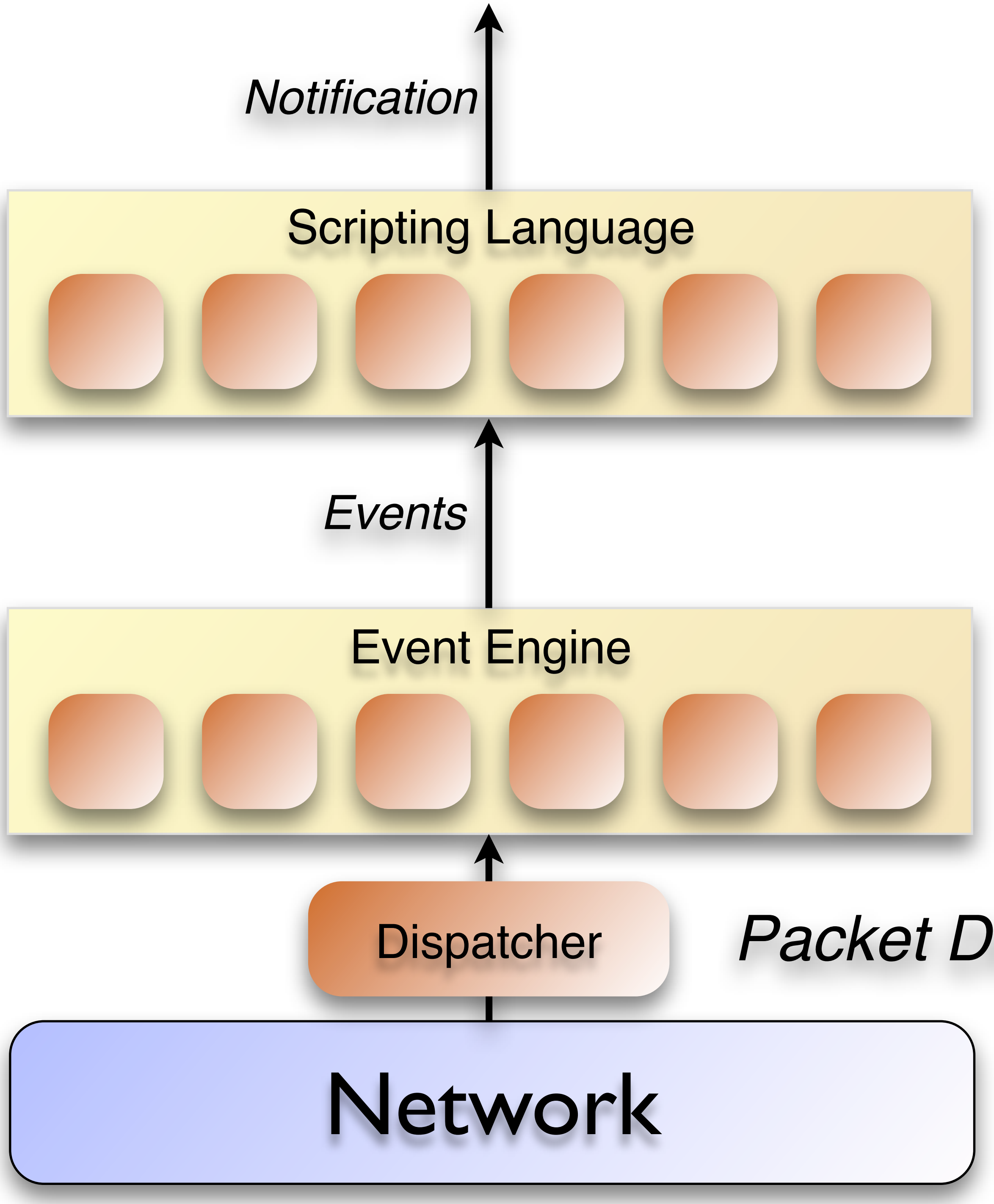
Architecture



Architecture

Detection Logic

Packet Analysis

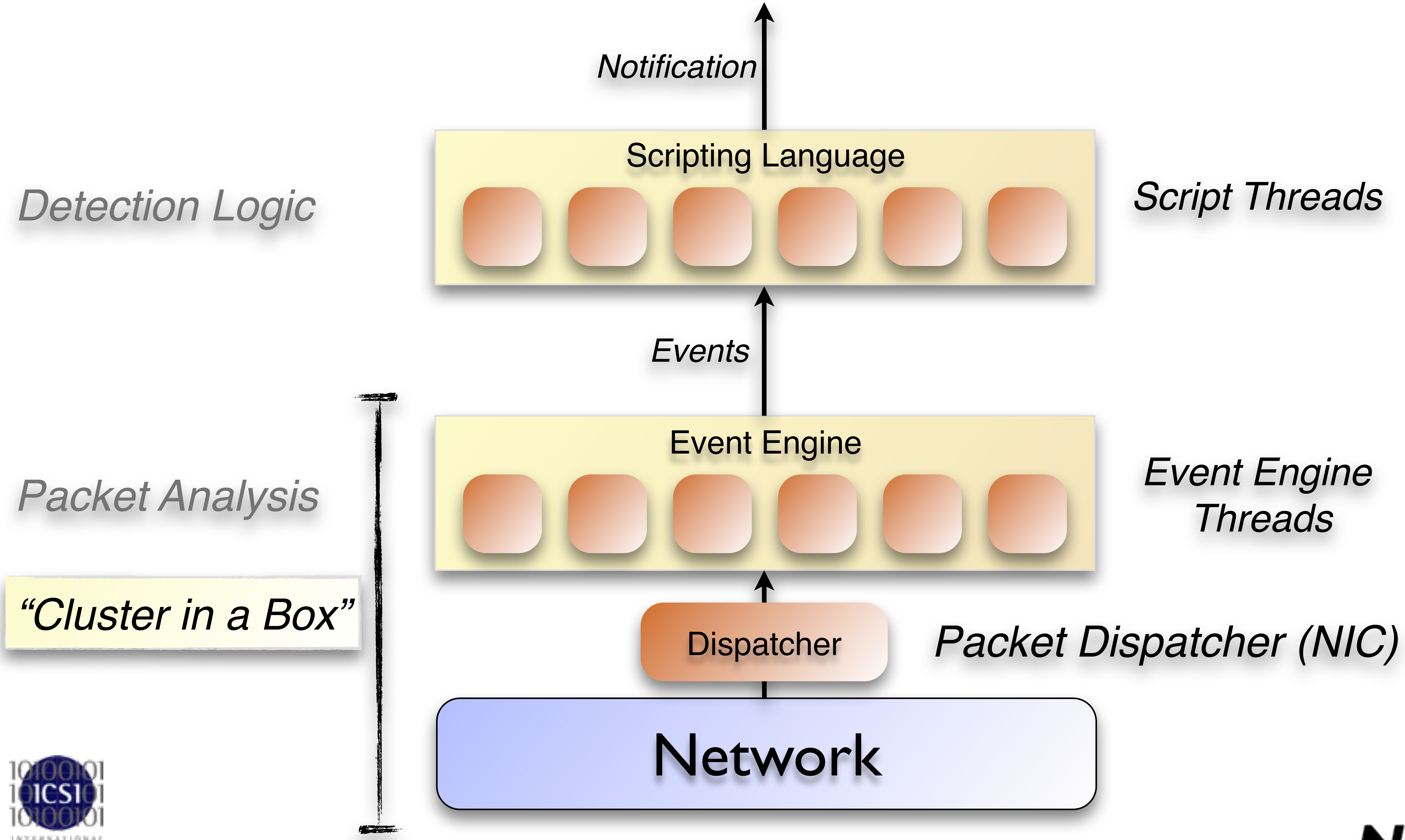


Script Threads

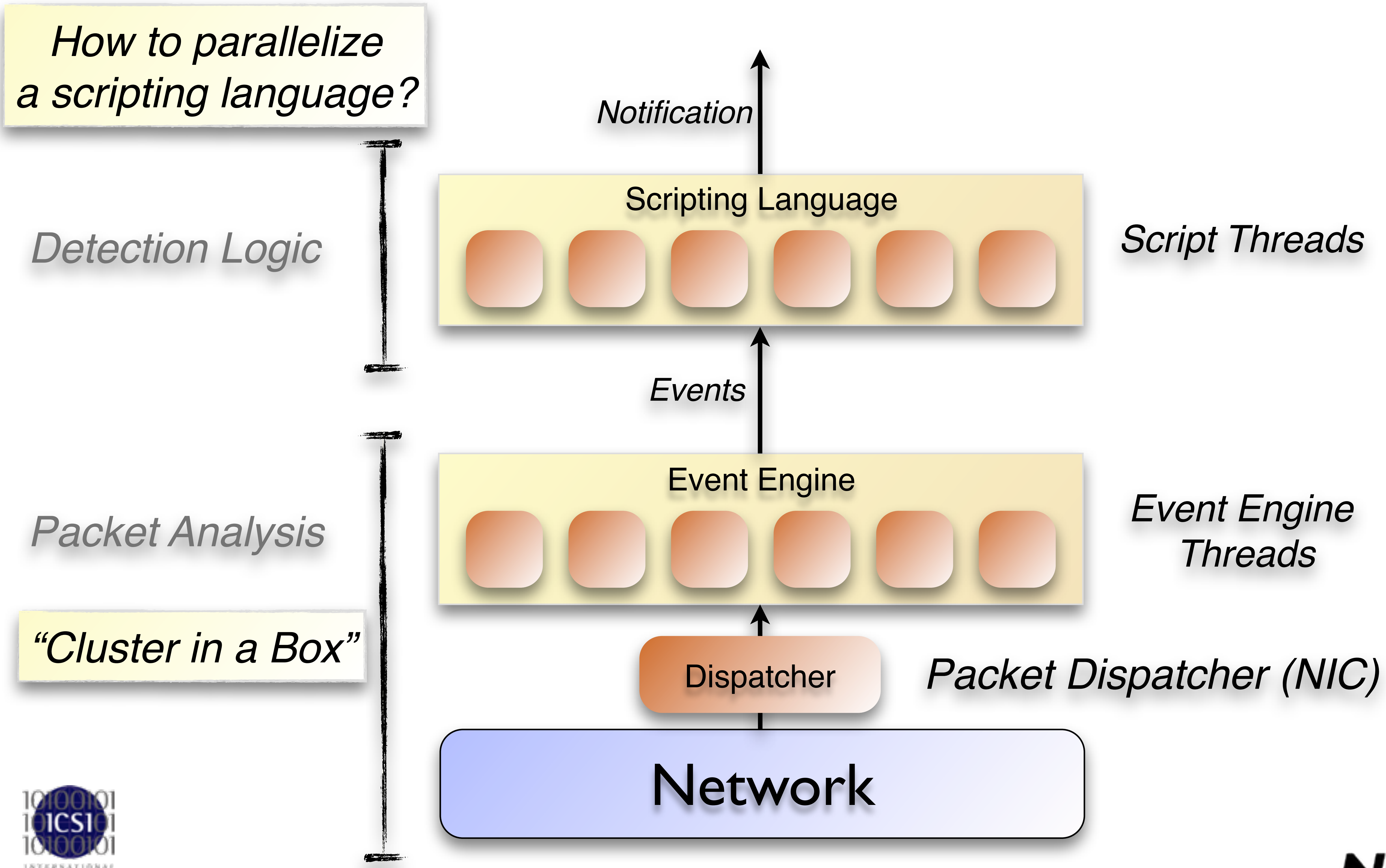
Event Engine Threads

Packet Dispatcher (NIC)

Architecture



Architecture

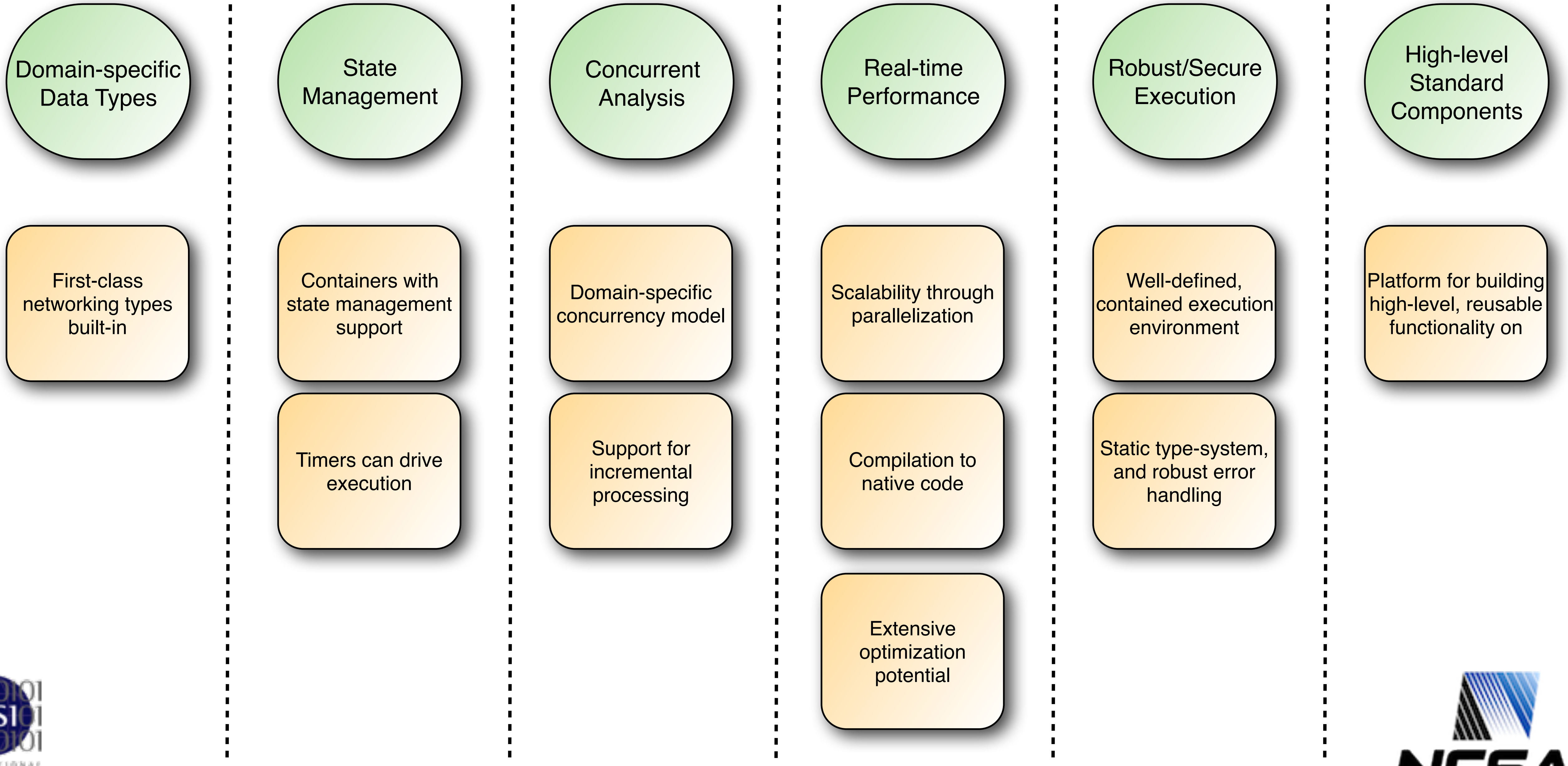


HILTI Abstract Machine

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

HILTI Abstract Machine

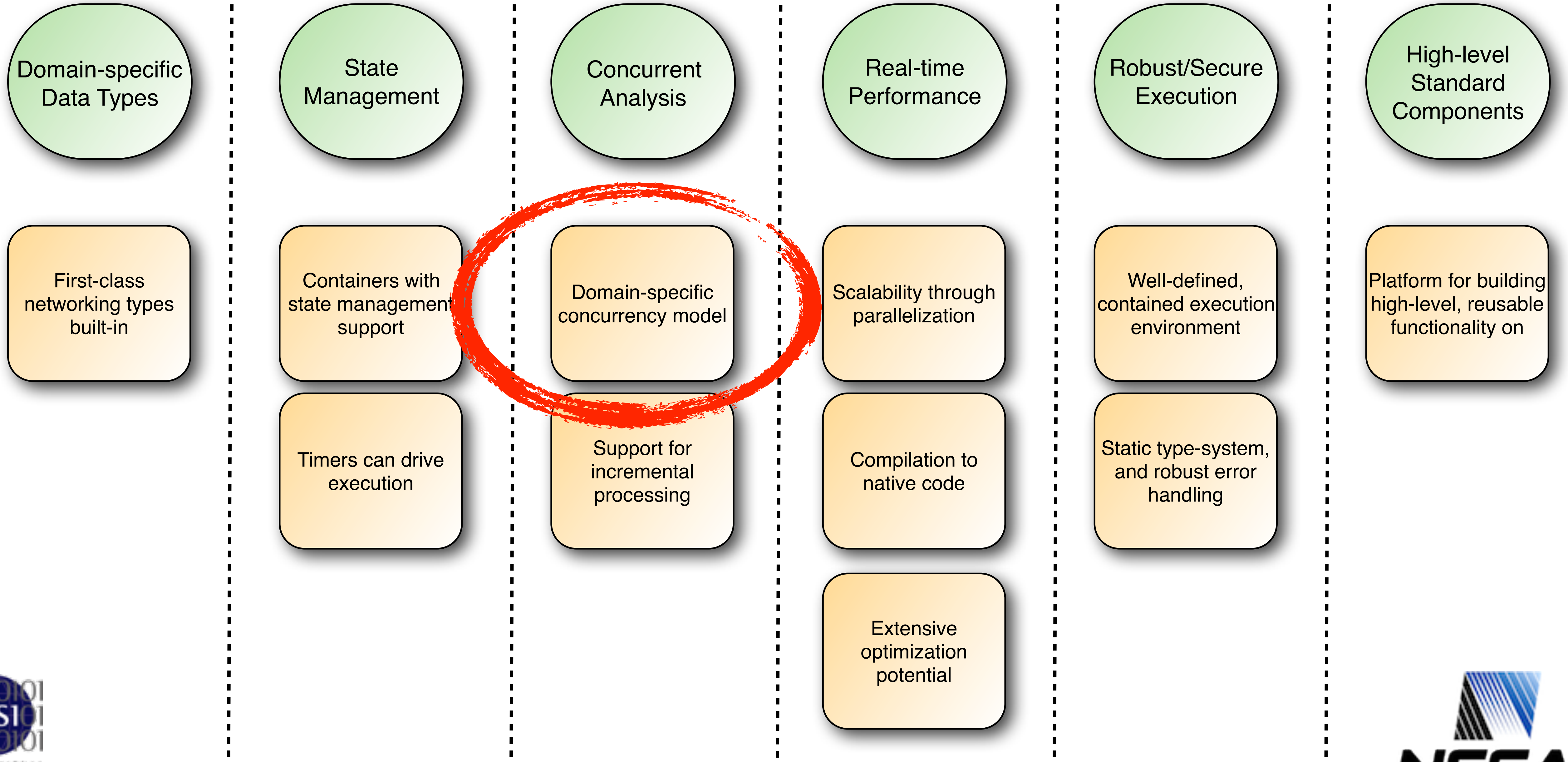
A **H**igh-Level **I**ntermediary **L**anguage for **T**raffic **I**nspection



Domain-specific Data Types	State Management	Concurrent Analysis	Real-time Performance	Robust/Secure Execution	High-level Standard Components
First-class networking types built-in	Containers with state management support	Domain-specific concurrency model	Scalability through parallelization	Well-defined, contained execution environment	Platform for building high-level, reusable functionality on
	Timers can drive execution	Support for incremental processing	Compilation to native code	Static type-system, and robust error handling	
			Extensive optimization potential		

HILTI Abstract Machine

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



Domain-specific Data Types
- First-class networking types built-in

State Management
- Containers with state management support
- Timers can drive execution

Concurrent Analysis
- Domain-specific concurrency model
- Support for incremental processing

Real-time Performance
- Scalability through parallelization
- Compilation to native code
- Extensive optimization potential

Robust/Secure Execution
- Well-defined, contained execution environment
- Static type-system, and robust error handling

High-level Standard Components
- Platform for building high-level, reusable functionality on

Workshop Wrap Up

Thanks for coming to the
Bro Workshop 2011!

Workshop Wrap Up

Thanks for coming to the Bro Workshop 2011!

Thanks to NSF for subsidizing workshop attendance.

Building a Community

http://www.bro-ids.org

Building a Community

Our goal is to build a larger “Bro Community”.

Users: Exchange of experiences and functionality.

Developers: External contributions will be crucial.

http://www.bro-ids.org

Building a Community

Our goal is to build a larger “Bro Community”.

Users:	Exchange of experiences and functionality.
Developers:	External contributions will be crucial.

New community resources.

- Mailing lists / Blog / Twitter / IRC.
- Contributed scripts repository.

http://www.bro-ids.org

Building a Community

Our goal is to build a larger “Bro Community”.

Users:	Exchange of experiences and functionality.
Developers:	External contributions will be crucial.

New community resources.

Mailing lists / Blog / Twitter / IRC.
Contributed scripts repository.

Open development model.

All code in public git repositories.
Extensive use of issue tracker.

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

Helping the Bro Project

Helping the Bro Project

Tell us!

Helping the Bro Project

Tell us!

Tell others!

Helping the Bro Project

Tell us!

Tell others!

Help others!

Helping the Bro Project

Tell us!

Tell others!

Help others!

Contribute!

Shameless Plug

Shameless Plug

All of the Bro 2.0 work was only possible with the support from National Science Foundation.

Shameless Plug

All of the Bro 2.0 work was only possible with the support from National Science Foundation.

We can continue with that for a bit, but only for so long. And we have many more ideas anyway.

Shameless Plug

All of the Bro 2.0 work was only possible with the support from National Science Foundation.

We can continue with that for a bit, but only for so long. And we have many more ideas anyway.

We are looking for more funding to keep the team together, and potentially expand it further.

Shameless Plug

All of the Bro 2.0 work was only possible with the support from National Science Foundation.

We can continue with that for a bit, but only for so long. And we have many more ideas anyway.

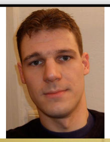
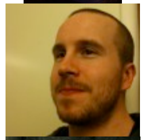
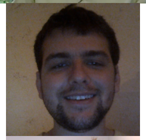
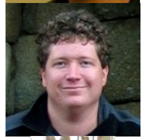
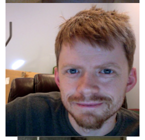
We are looking for more funding to keep the team together, and potentially expand it further.

Any ideas? Let us know.

Thanks for Coming!

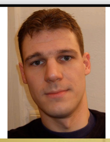
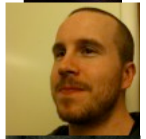
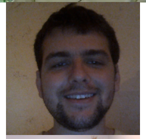
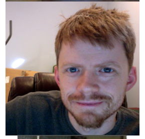
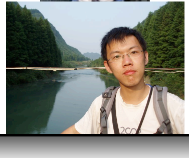
Thanks for Coming!

Homepage	`www.bro-ids.org`
Twitter	@`BRO_IDS`
Contact	`info@bro-ids.org` User mailing list
Development	`git.bro-ids.org` Developer's mailing list Commit notification list

Vern Paxson		Gregor Maier	
Jim Barlow		Jonathan Siwek	
Gilbert Clark		Adam Slagell	
Seth Hall		Robin Sommer	
Christian Kreibich		Daniel Thayer	
Hui Lin		Matthias Vallentin	

Thanks for Coming!

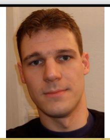
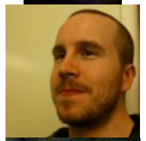
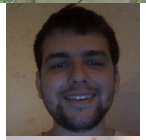
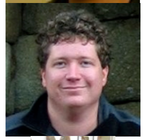
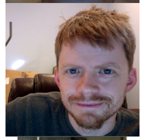
Homepage	`www.bro-ids.org`
Twitter	@`BRO_IDS`
Contact	`info@bro-ids.org` User mailing list
Development	`git.bro-ids.org` Developer's mailing list Commit notification list

Vern Paxson		Gregor Maier	
Jim Barlow		Jonathan Siwek	
Gilbert Clark		Adam Slagell	
Seth Hall		Robin Sommer	
Christian Kreibich		Daniel Thayer	
Hui Lin		Matthias Vallentin	

Please fill out our survey.

Thanks for Coming!

Homepage	www.bro-ids.org
Twitter	@BRO_IDS
Contact	info@bro-ids.org User mailing list
Development	git.bro-ids.org Developer's mailing list Commit notification list

Vern Paxson		Gregor Maier	
Jim Barlow		Jonathan Siwek	
Gilbert Clark		Adam Slagell	
Seth Hall		Robin Sommer	
Christian Kreibich		Daniel Thayer	
Hui Lin		Matthias Vallentin	

Please fill out our survey.

Bro Tutorial at ACSAC 2011
One day version of this workshop.

December 5–9, 2011 | Buena Vista Palace Hotel & Spa | Orlando, Florida, USA