Data Plane Verification: Anteater and VeriFlow

Brighten Godfrey
University of Illinois at Urbana-Champaign

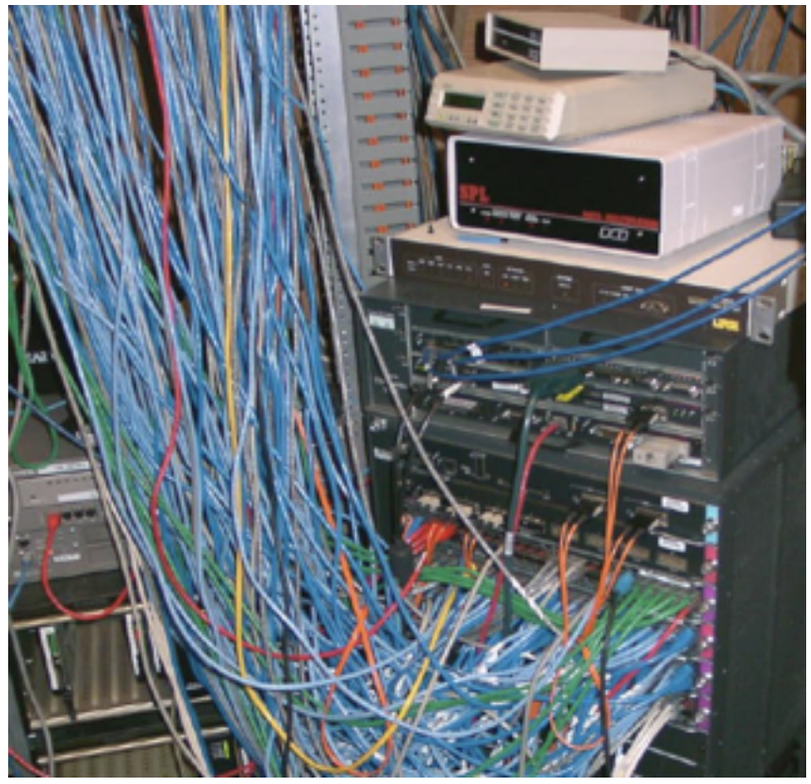
Work with Ahmed Khurshid, Haohui Mai, Kelvin Zou, Wenxuan Zhou, Rachit Agarwal, Matthew Caesar, and Sam King

December 5, 2013

Managing networks is challenging

Production networks are complex

- Security policies
- Traffic engineering
- Legacy devices
- Protocol inter-dependencies
- …



- Even well-managed networks have downtime & security vulnerabilities
- Few good tools to ensure all networking components working together correctly

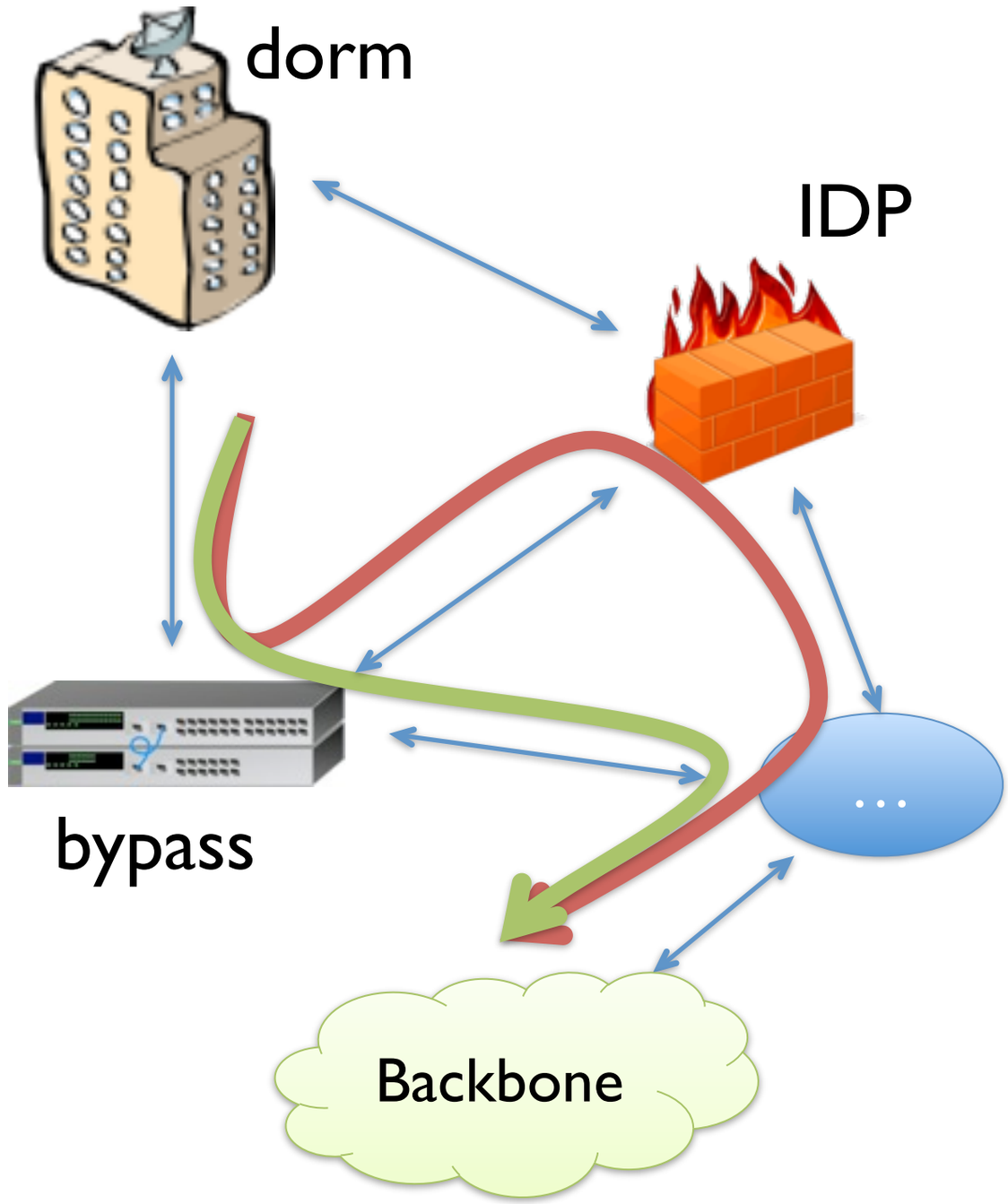
A real example from UIUC

Previously, an intrusion detection and prevention (IDP) device inspected all traffic to/from dorms

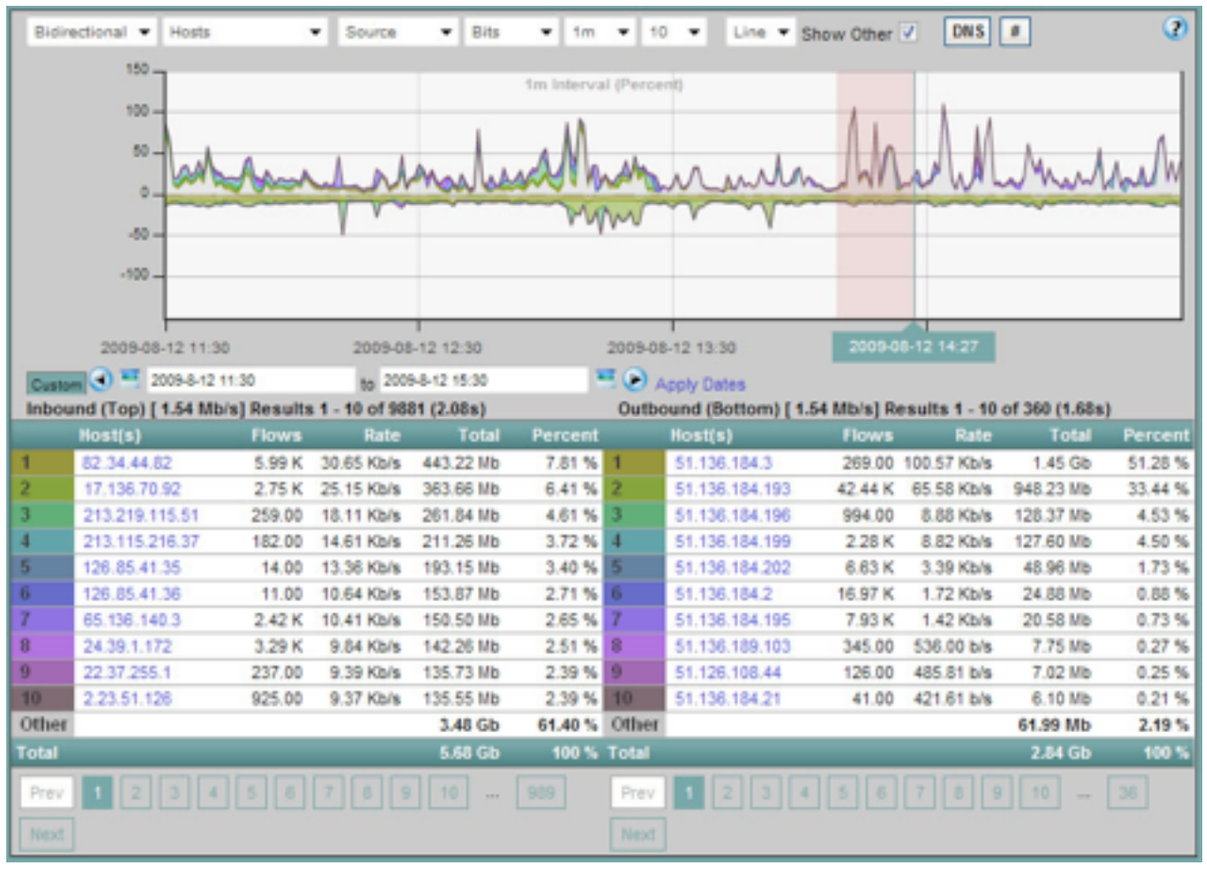
IDP couldn't handle load; added bypass

- IDP only inspected traffic between dorm and campus
- Seemingly simple changes

How do you know if it worked?



Understanding your network



	Host(s)	Flows	Rate	Total	Percent
1	82.34.44.82	5.99 K	30.65 Kb/s	443.22 Mb	7.81 %
2	17.136.70.92	2.75 K	25.15 Kb/s	363.66 Mb	6.41 %
3	213.219.115.51	259.00	18.11 Kb/s	261.84 Mb	4.61 %
4	213.115.216.37	182.00	14.61 Kb/s	211.26 Mb	3.72 %
5	126.85.41.35	14.00	13.36 Kb/s	193.15 Mb	3.40 %
6	126.85.41.36	11.00	10.64 Kb/s	153.87 Mb	2.71 %
7	65.136.140.3	2.42 K	10.41 Kb/s	150.50 Mb	2.65 %
8	24.39.1.172	3.29 K	9.84 Kb/s	142.26 Mb	2.51 %
9	22.37.255.1	237.00	9.39 Kb/s	135.73 Mb	2.39 %
10	2.23.51.126	925.00	9.37 Kb/s	135.55 Mb	2.39 %
Other				3.48 Gb	61.40 %
Total				5.68 Gb	100 %

	Host(s)	Flows	Rate	Total	Percent
1	51.136.184.3	269.00	100.57 Kb/s	1.45 Gb	51.28 %
2	51.136.184.193	42.44 K	65.58 Kb/s	948.23 Mb	33.44 %
3	51.136.184.196	994.00	8.88 Kb/s	128.37 Mb	4.53 %
4	51.136.184.199	2.28 K	8.82 Kb/s	127.60 Mb	4.50 %
5	51.136.184.202	6.63 K	3.39 Kb/s	48.96 Mb	1.73 %
6	51.136.184.2	16.97 K	1.72 Kb/s	24.88 Mb	0.88 %
7	51.136.184.195	7.93 K	1.42 Kb/s	20.58 Mb	0.73 %
8	51.136.189.103	345.00	536.00 b/s	7.75 Mb	0.27 %
9	51.126.108.44	126.00	485.81 b/s	7.02 Mb	0.25 %
10	51.136.184.21	41.00	421.61 b/s	6.10 Mb	0.21 %
Other				61.99 Mb	2.19 %
Total				2.84 Gb	100 %

Flow monitoring

Screenshot from Scrutinizer NetFlow & sFlow analyzer, snmp.co.uk/scrutinizer/

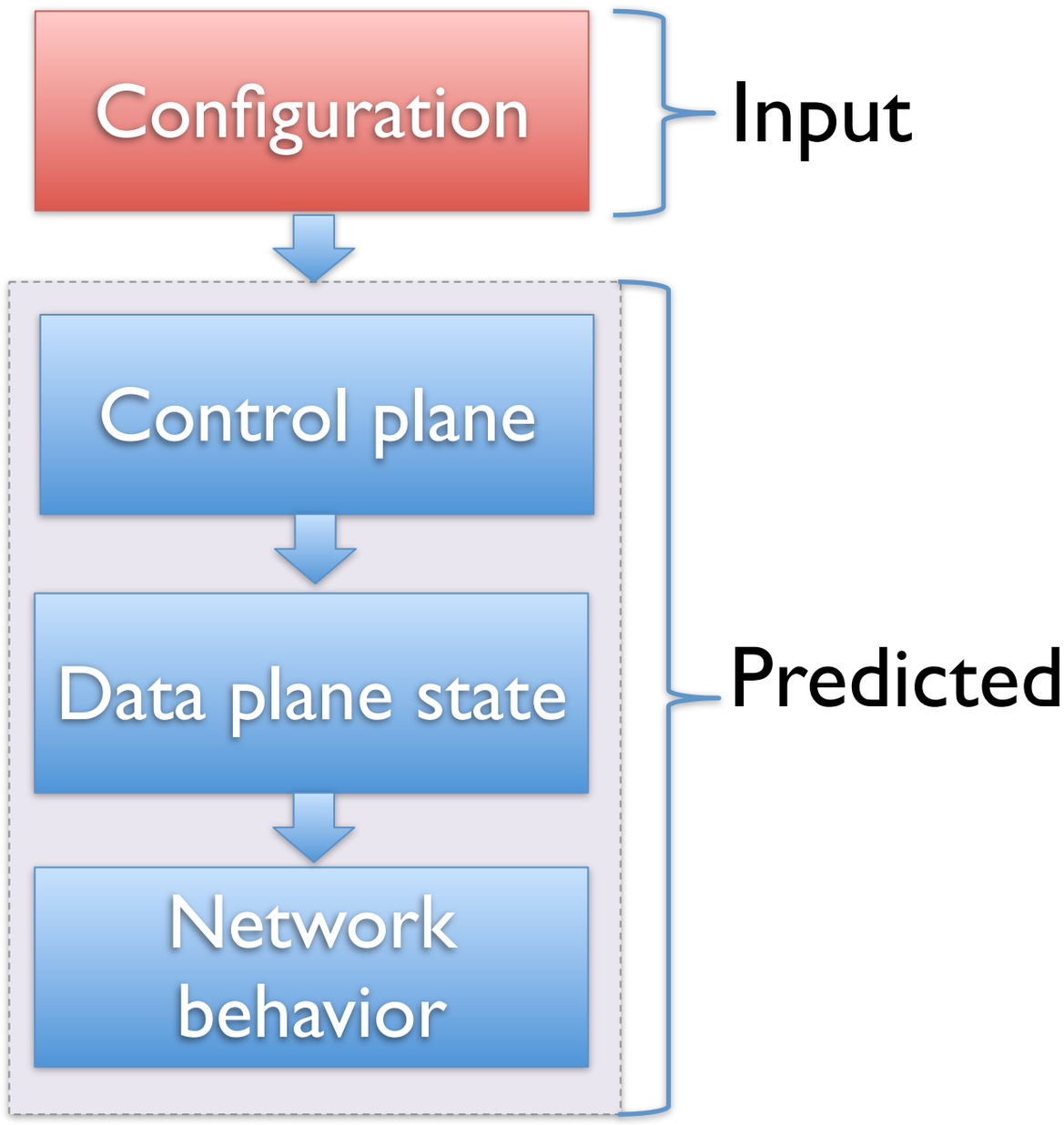
```
hostname bgpdA
password zebra
!
router bgp 8000
  bgp router-id 10.1.4.2

! for the link between A and B
  neighbor 10.1.2.3 remote-as 8000
  neighbor 10.1.2.3 update-source lo0

  network 10.0.0.0/7

! for the link between A and C
  neighbor 10.1.3.3 remote-as 7000
  neighbor 10.1.3.3 ebgp-multihop
  neighbor 10.1.3.3 next-hop-self
  neighbor 10.1.3.3 route-map PP out

! for link between A and D
  neighbor 10.1.4.3 remote-as 6000
  neighbor 10.1.4.3 ebgp-multihop
  neighbor 10.1.4.3 next-hop-self
  neighbor 10.1.4.3 route-map TagD in

! route update filtering
  ip community-list 1 permit 8000:1000
!
```

Configuration verification

Past approach: Config. verification

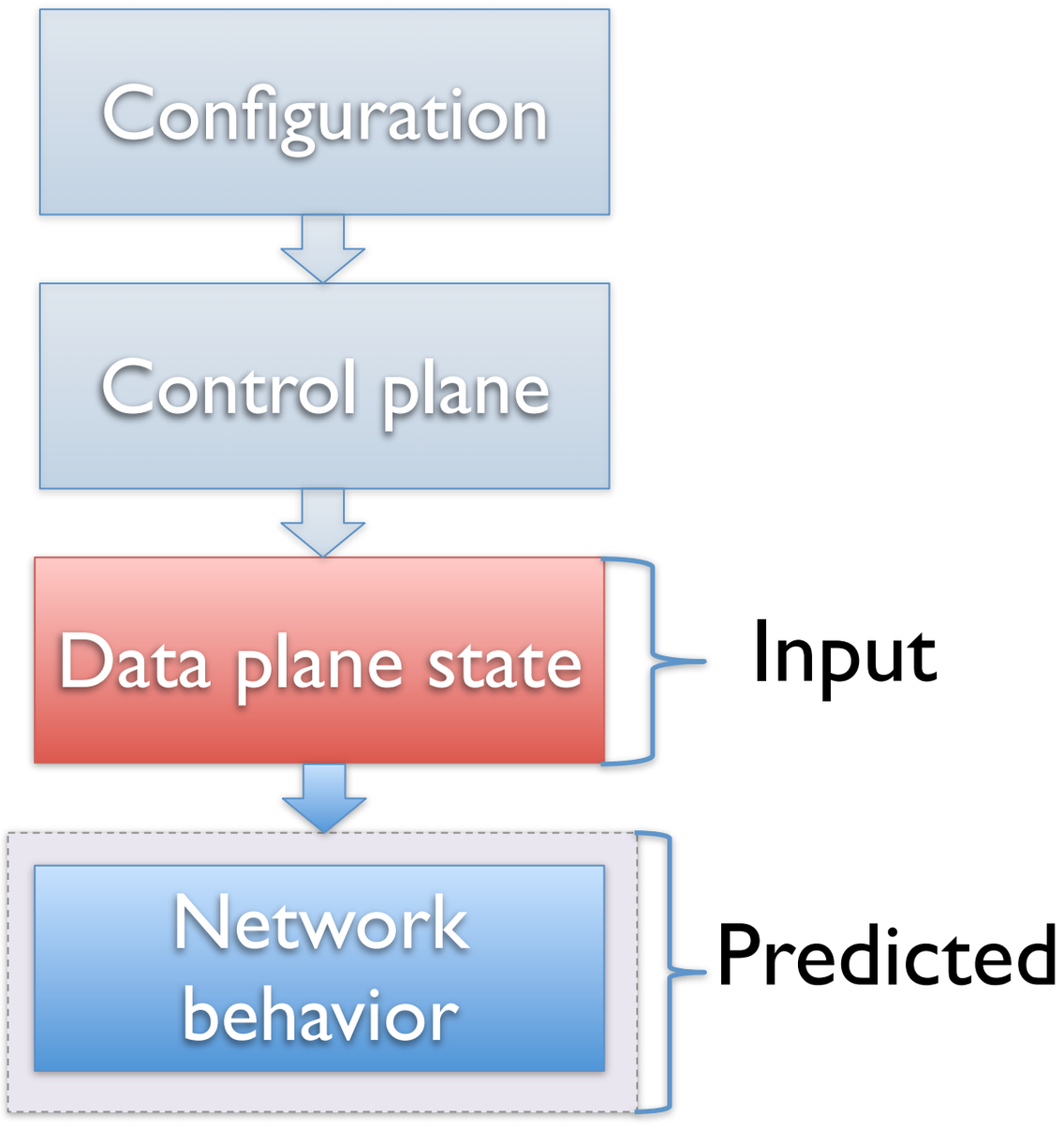
e.g.: RCC for BGP [Feamster & Balakrishnan, NSDI'05]

Margrave for firewalls [Nelson, Barratt, Dougherty, Fisler, Krishnamurthi, LISA'10]



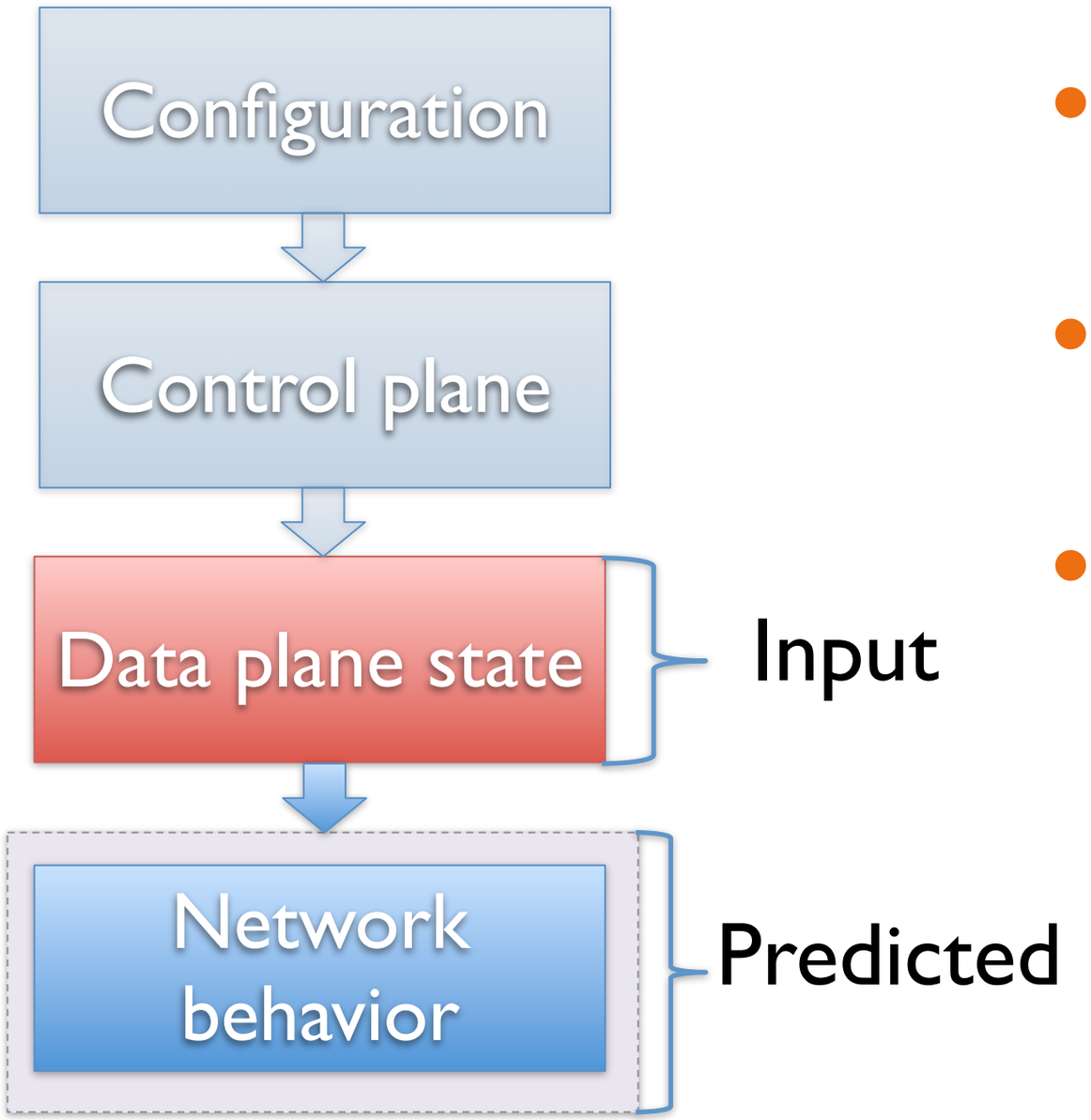
Data plane verification

Our approach: Verify the network as close as possible to its actual behavior



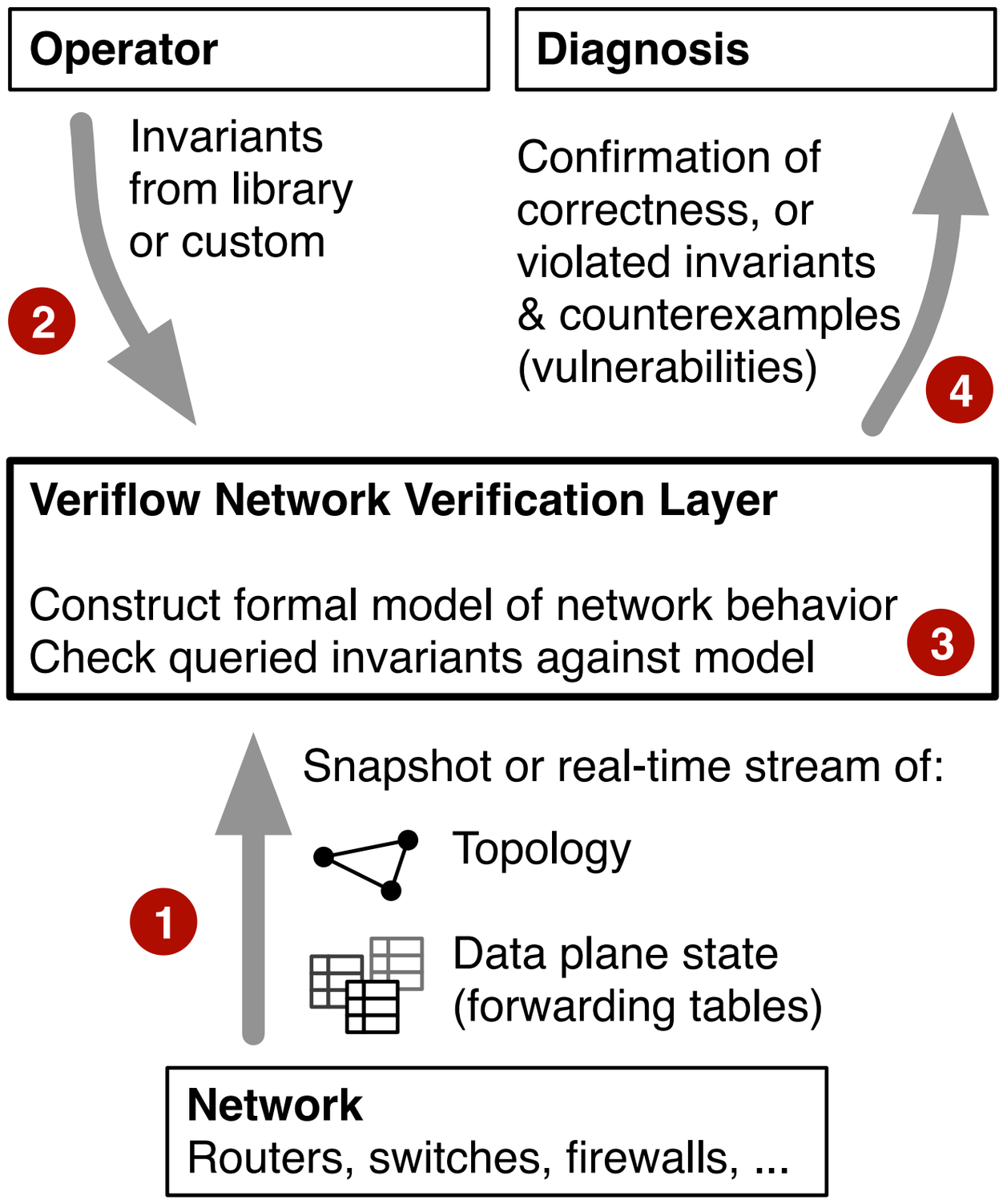
Data plane verification

Our approach: Verify the network as close as possible to its actual behavior



- Unified analysis across control software
- Catch bugs in control software
- Checks current snapshot

Architecture overview



Our Two Tools

Anteater

- [Mai, Khurshid, Agarwal, Caesar, Godfrey, King, SIGCOMM 2011]
- Offline verification of data plane

VeriFlow

- [Khurshid, Zhou, Caesar, Godfrey, HotSDN 2012 (best paper)]
- [Khurshid, Zou, Zhou, Caesar, Godfrey, NSDI 2013]
- Online real-time verification of data plane
- Interoperates with OpenFlow controller

VeriFlow's mission

Is it possible to check network-wide invariants in real time as the network evolves?

Not so simple

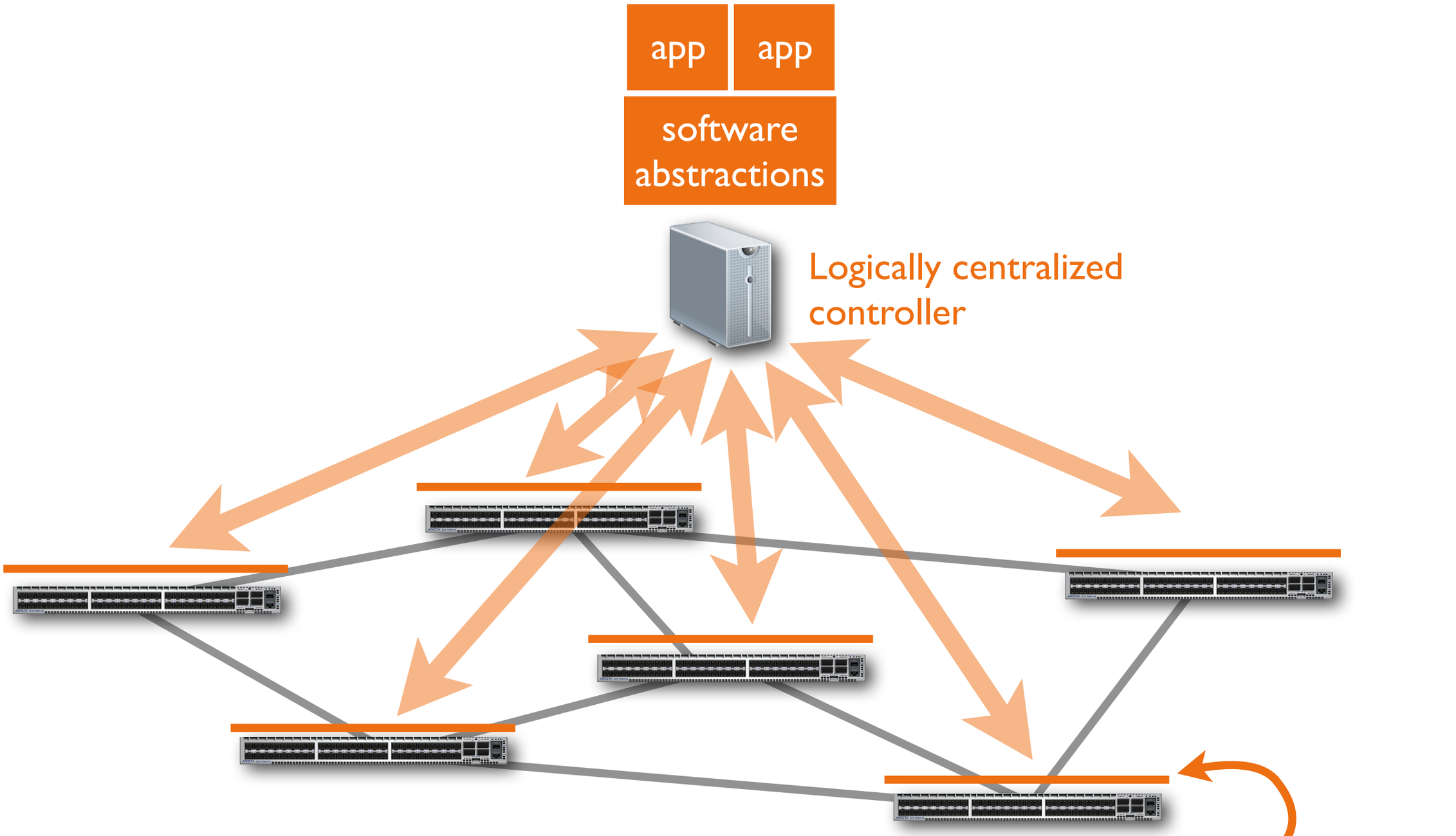
Challenge #1: Obtaining real time view of network

- Solution: interpose between Software Defined Networking (SDN) controller and routers/switches

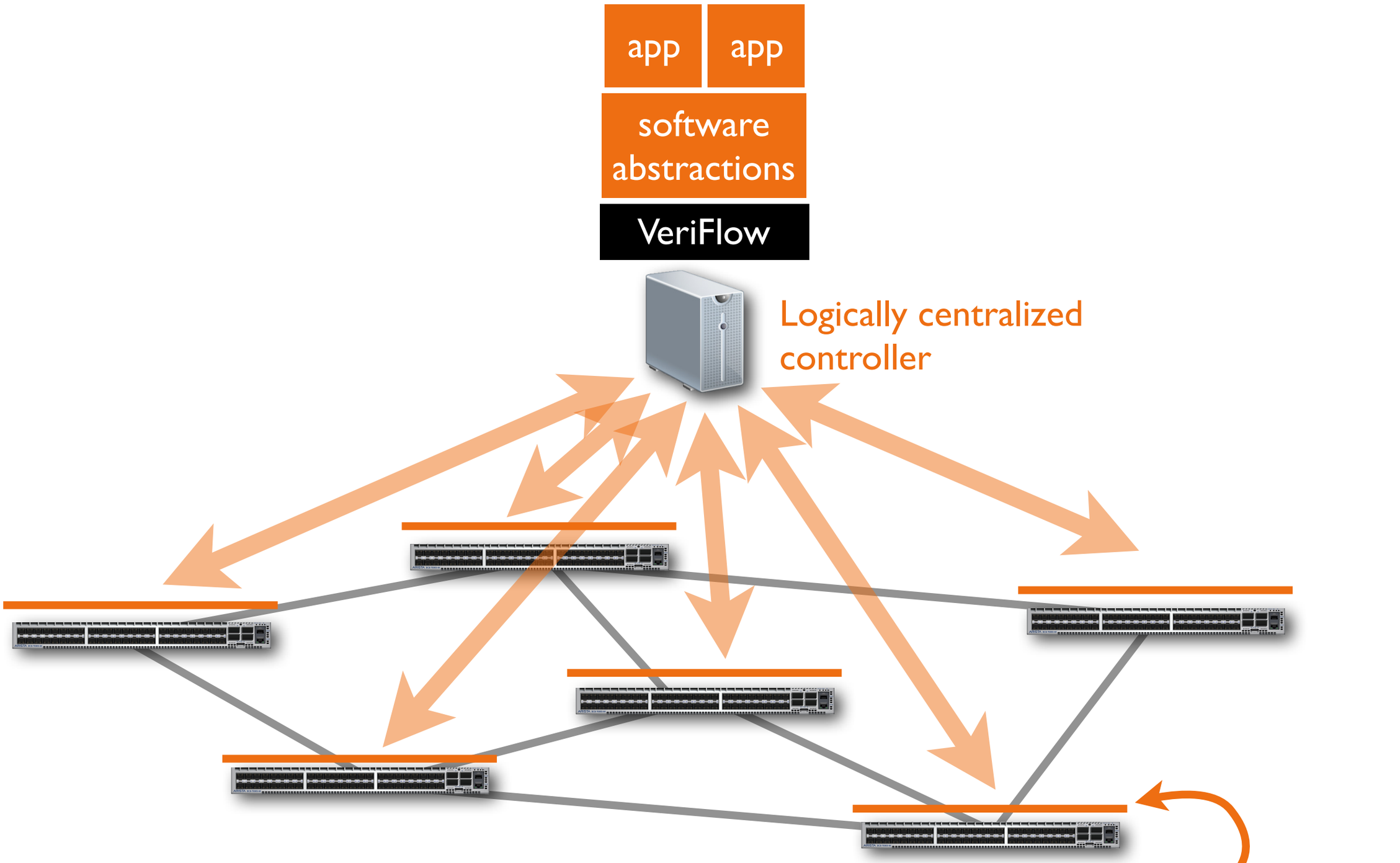
Challenge #2: Verification speed

- Past tools too slow and/or not incremental
- Solution: Algorithms :-)

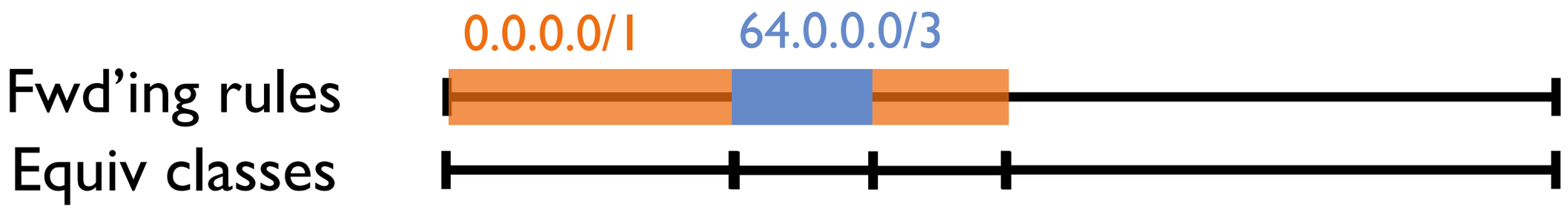
VeriFlow architecture



VeriFlow architecture

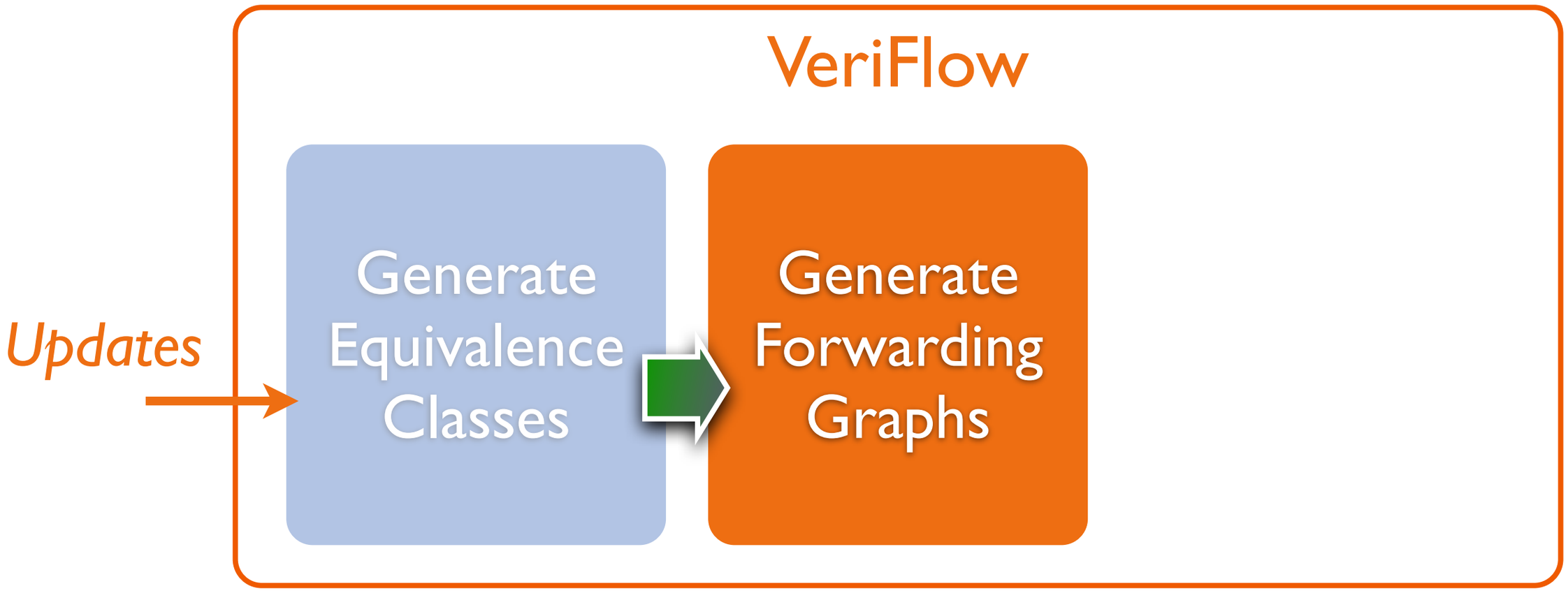


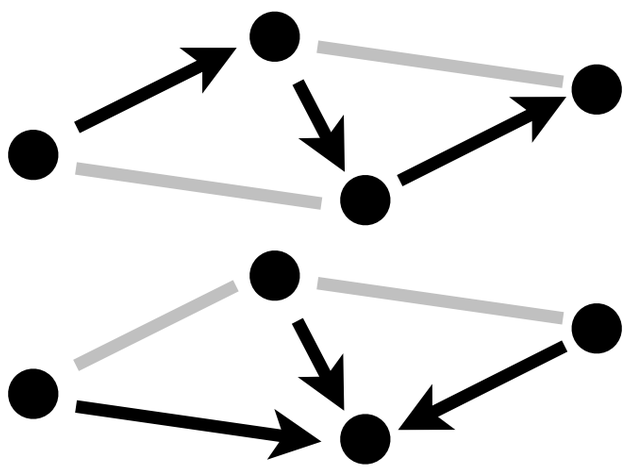
Verifying invariants quickly



Find only equivalence classes affected by the update via a multidimensional trie data structure

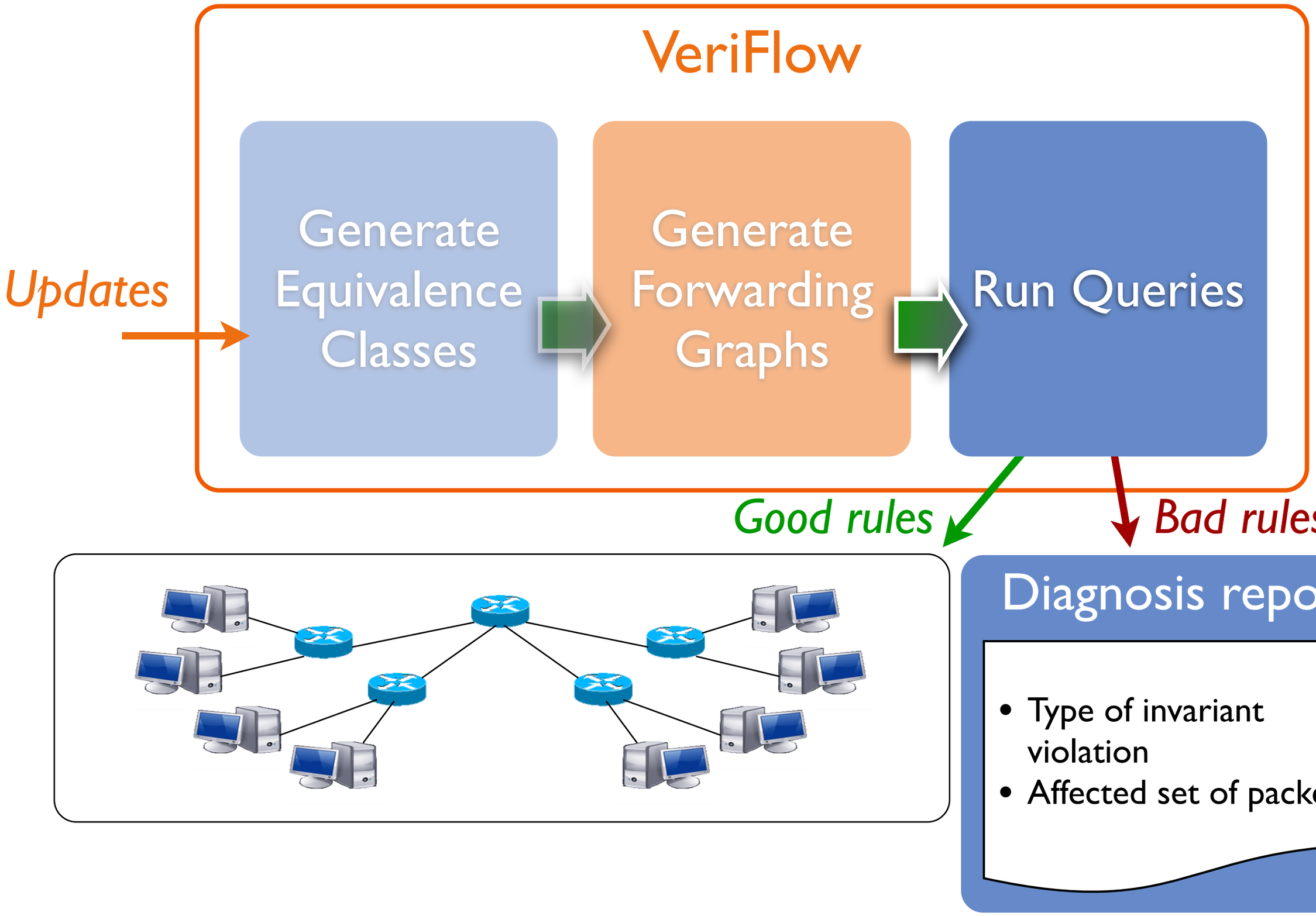
Verifying invariants quickly





All the info to answer queries!

Verifying invariants quickly



Evaluation

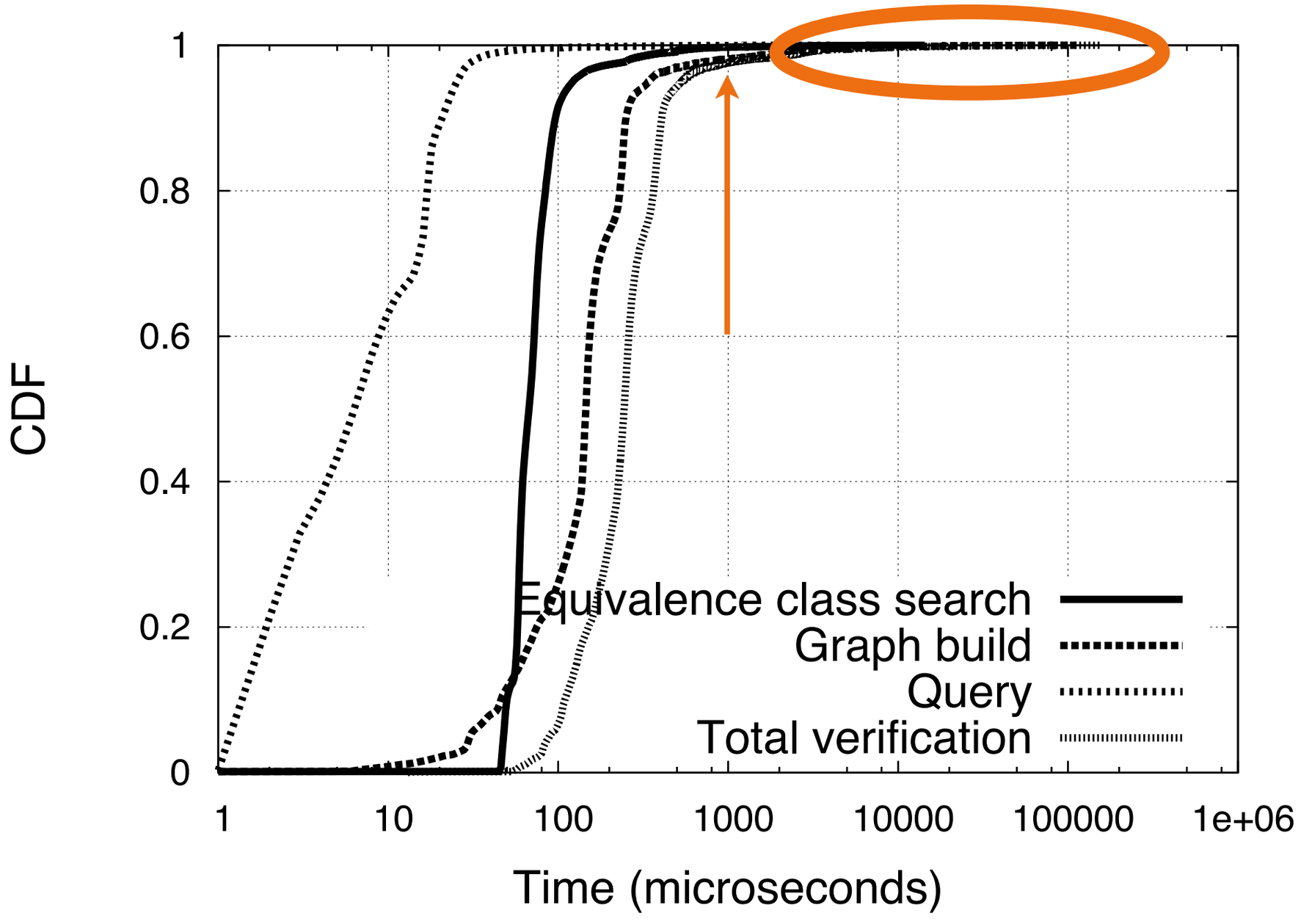
Simulated network

- Real-world BGP routing tables (RIBs) from RouteViews totaling 5 million RIB entries
- Injected into 172-router network (AS 1755 topology)

Measure time to process each forwarding change

- 90,000 updates from Route Views
- Check for loops and black holes

Microbenchmark latency



97.8% of updates verified within 1 ms

Deployment

UIUC deployment

Deployed Anteater and VeriFlow in University of Illinois campus backbone

- 244 routers, serving 70,000+ machines
- Predominantly OSPF, BGP, and static routing
- State collected via vty scripts

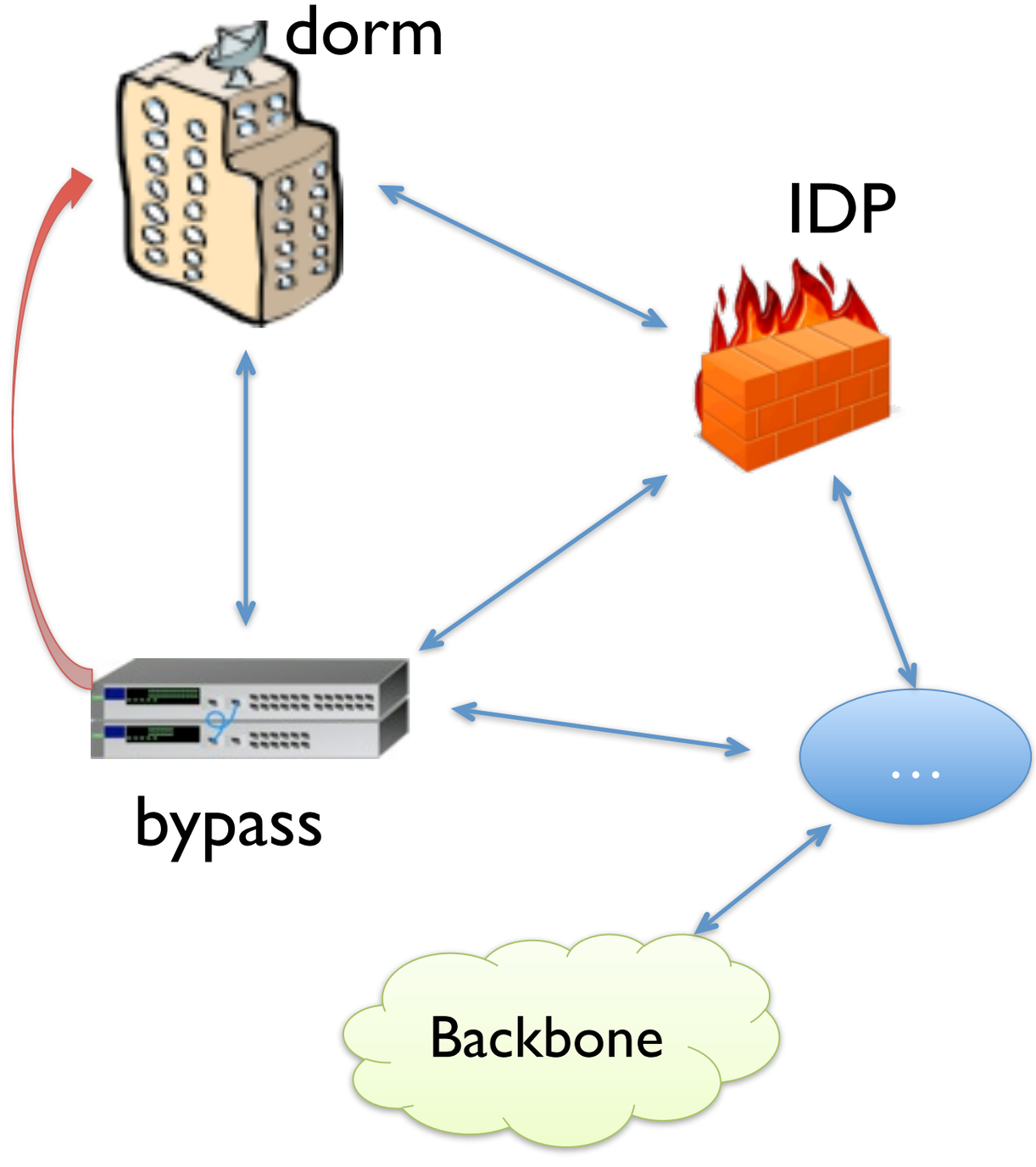
Forwarding loops

IDP was overloaded, operator introduced bypass

- IDP only inspected traffic for campus

bypass routed campus traffic to IDP through static routes

Introduced 9 loops



Errors discovered

Loops in internal network

Externally-exploitable DoS vulnerability

Packet loss due to ‘stale’ configs

Inconsistent security policy: over-exposure of router management interface

Duplicate IP addresses on router interfaces

Router vendor software error: faulty config output

Related work

Configuration verification

- [Al-Shaer2004, Bartal1999, Benson2009, Feamster2005, Yuan2006]

Data plane verification

- Static reachability in IP networks [Bush'03, Xie'05]
- FlowChecker [Al-Shaer, Al-Haj, SafeConfig '10]
- ConfigChecker [Al-Shaer, Al-Saleh, SafeConfig '11]
- Header Space Analysis [Kazemian, Varghese, and McKeown, NSDI '12]
- NetPlumber [Kazemian, Chang, Zeng, Varghese, McKeown, Whyte, NSDI '13]

What we've seen

Data plane verification is valuable

- Unified network-wide analysis across protocols
- Demonstrated effectiveness in large campus network

Real-time verification is feasible

- millisecond timescales enabled by SDN + algorithms

Thanks!