

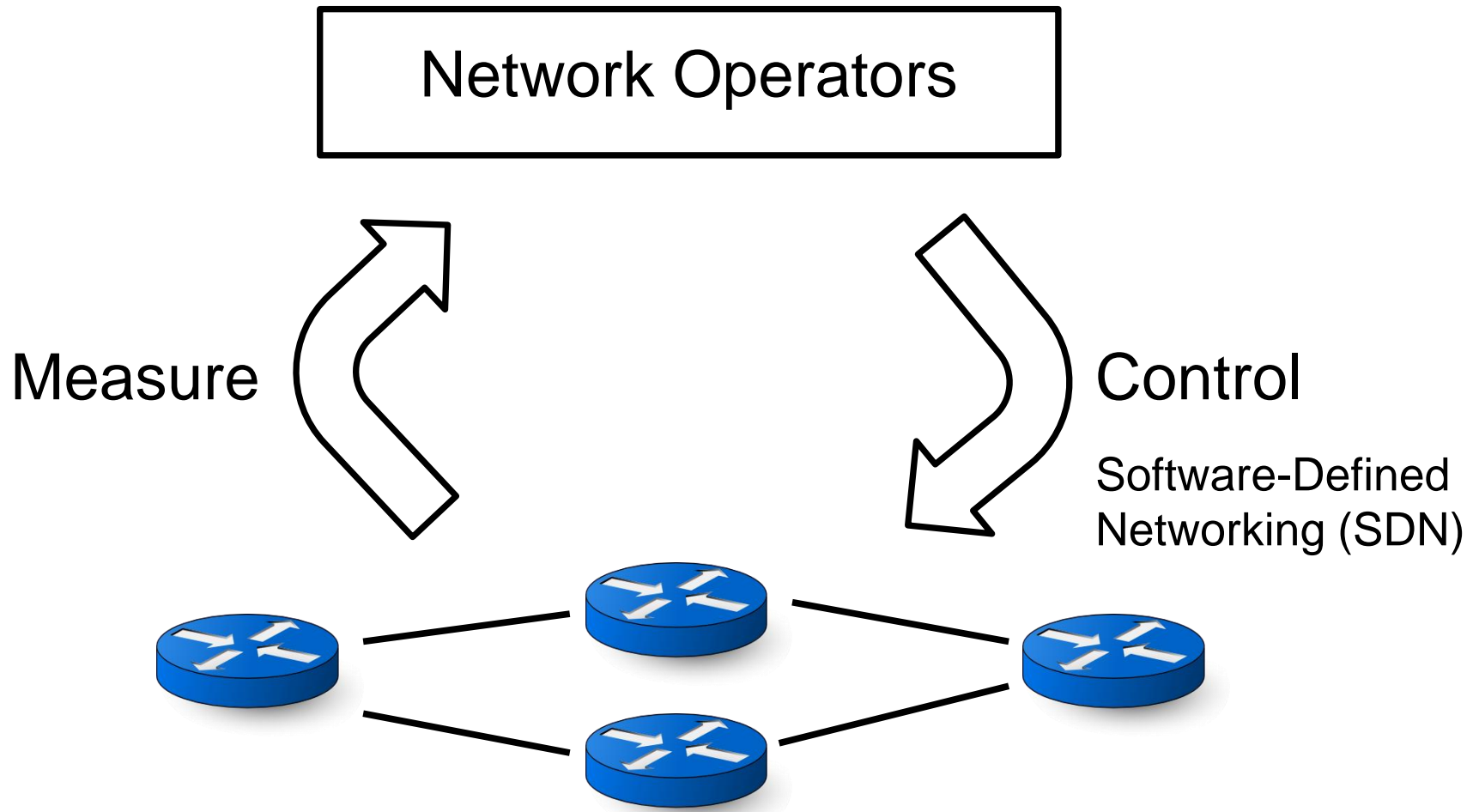


Declarative Network Path Queries

Srinivas Narayana
Princeton University

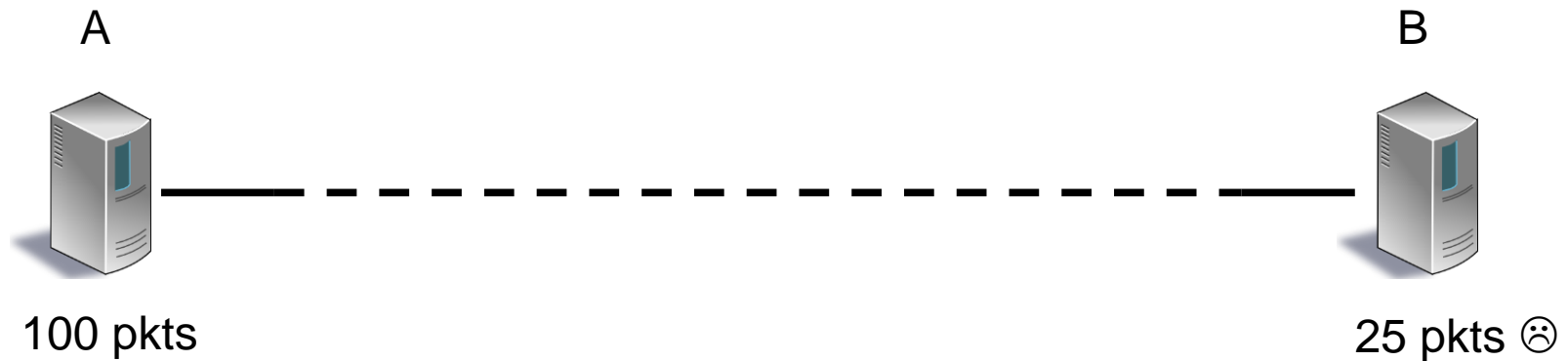


Management = Measure + Control



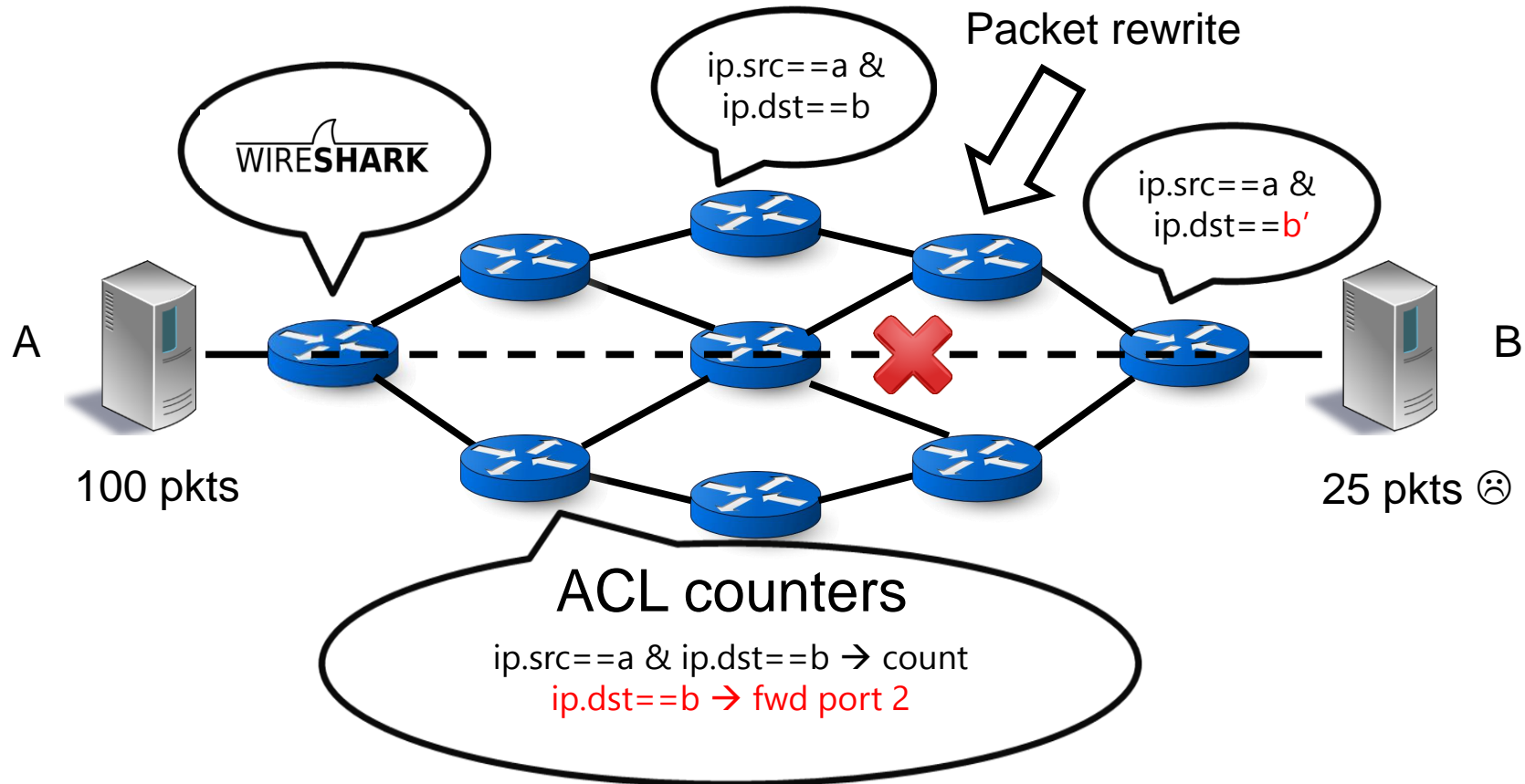
Example: Where's the Packet Loss?

Suspect: Faulty network device(s) along the way.



Example: Where's the Packet Loss?

Idea: "Follow" the path of packets through the network.



Example: Where's the Packet loss?

**Complex, Inaccurate
Join Procedure**
with multiple
datasets: traffic,
forwarding, topology

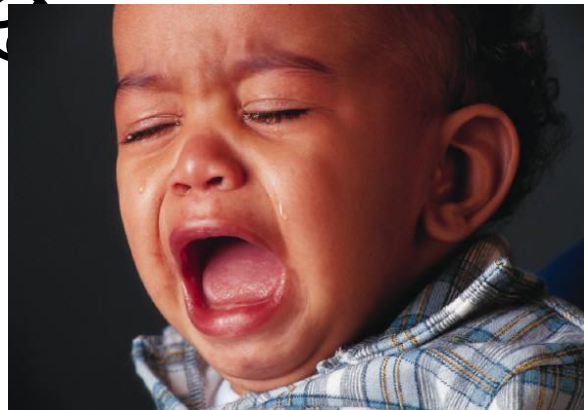
High Overhead
of collecting
(unnecessary) data
to answer a given
question



Example: Where's the Packet loss?

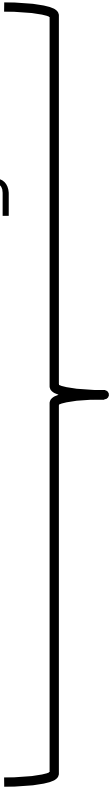
**Complex, Inaccurate
Join Procedure**
with multiple
datasets: traffic,
forwarding, topology

High Overhead
of collecting
(unnecessary) data
to answer a given
question



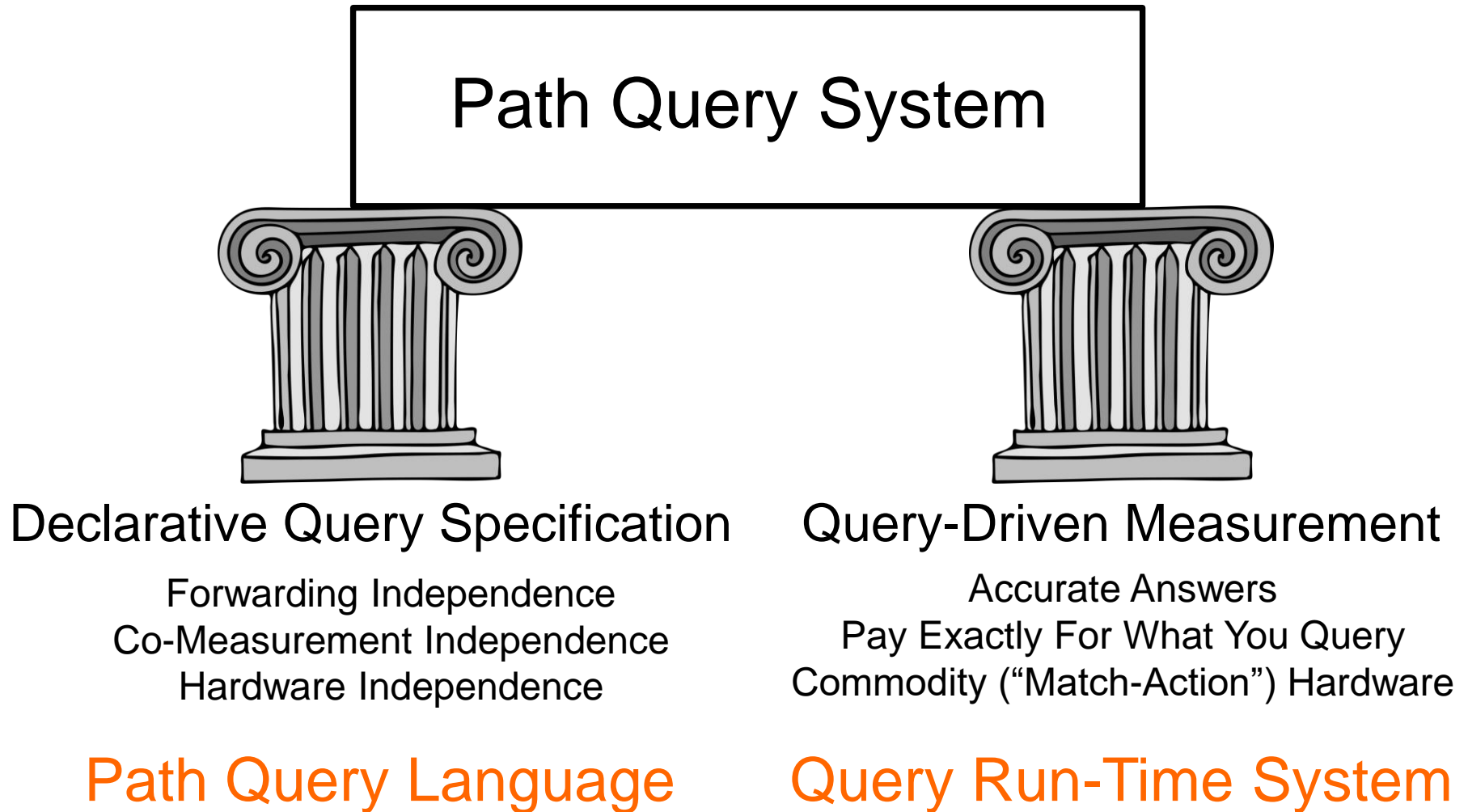
Lots of Measurement Use-Cases

- Traffic matrix
- Uneven load balancing
- DDoS source identification
- Port-level traffic matrix
- Congested link diagnosis
- Slice isolation
- Loop detection
- Middlebox traversal order
- Incorrect NAT rewrite
- Firewall evasion
- ...

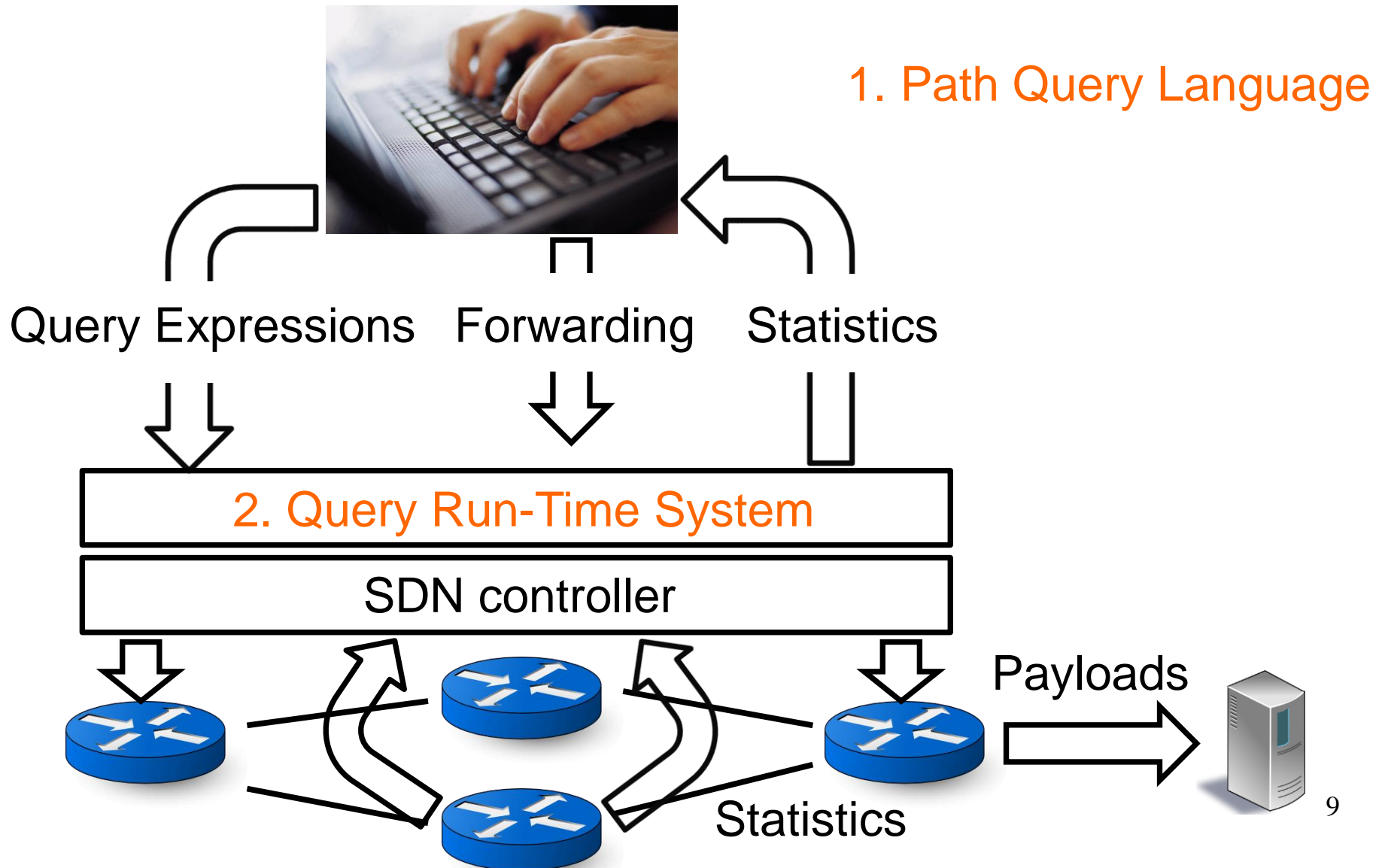


Resource management
Policy enforcement
Problem diagnosis

Solution Approach



Solution Approach



Path Query Language

- Single location tests:

srcip=10.0.0.1

inport=3

- Regular expression operators to combine tests:

sw=1 ^ sw=4

srcip=A ^ true* ^ dstip=B'

ingress() ^ ~(sw=firewall)* ^ egress()

- SQL-like grouping operators for aggregation

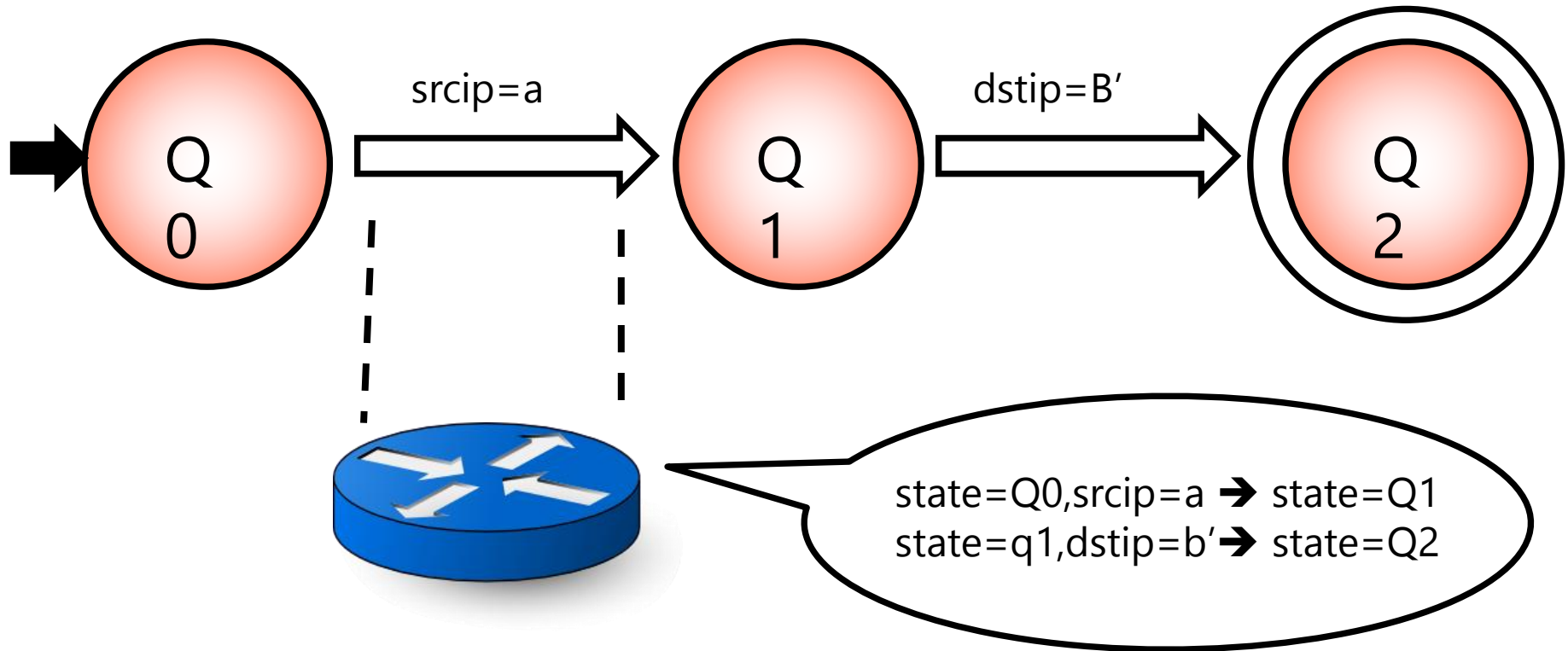
in_group(ingress(), [sw])

^ true*

^ out_group(egress(), [sw])

Query Run-Time System

- $\text{srcip} = a \wedge \text{dstip} = B'$



- Each packet carries its own DFA state
 - Packet satisfies query iff it reaches accepting states

Evaluation

- Prototype on Pyretic + NetKAT + OpenVSwitch
 - Publicly available: <http://frenetic-lang.org/pyretic/>
- Queries: traffic matrix, DDoS detection, per-hop packet loss, firewall evasion, slice isolation, congested link
- Metrics and results on Stanford (*all queries* together):
 - Compile time: 5 seconds
 - # Rules: ~ 650
 - # State bytes: 2 bytes

Queries? 😊

<http://www.cs.princeton.edu/~narayana/pathqueries>

