Realizing a Source Authentic Internet

Toby Ehrenkranz, Jun Li, and Patrick McDaniel

SecureComm
September 8, 2010

University of Oregon
Network Security Research Lab
http://netsec.cs.uoregon.edu

Pennsylvania State University
Systems and Internet Infrastructure Security
http://siis.cse.psu.edu

This material is based upon work supported by the USA National Science Foundation under Grant No. 0520326. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

What's The Problem?

- Cannot identify spoofing packets
- IP spoofing is key for a variety of attacks
  - DNS amplification attacks, DNS cache poisoning
  - Resetting TCP connections
  - Spam filter circumvention
- Attackers are able to spoof from a greater portion of the Internet than before
  - 2005: ~20% of netblocks
  - 2009: ~30% of netblocks

Ideal Spoofing Defense

- Effective in identifying and stopping spoofing packets
- Resistant against manipulation
- Efficient in terms of overhead
- Independent of specific routing protocol
- Easily deployable

Existing Defense Mechanisms

- Host based (active/passive)
- Router based (preventive/reactive)
- Hybrid

- Details in:

  Toby Ehrenkranz and Jun Li, "On the state of IP spoofing defense," ACM Transactions on Internet Technology, vol. 9, no. 2, May 2009.

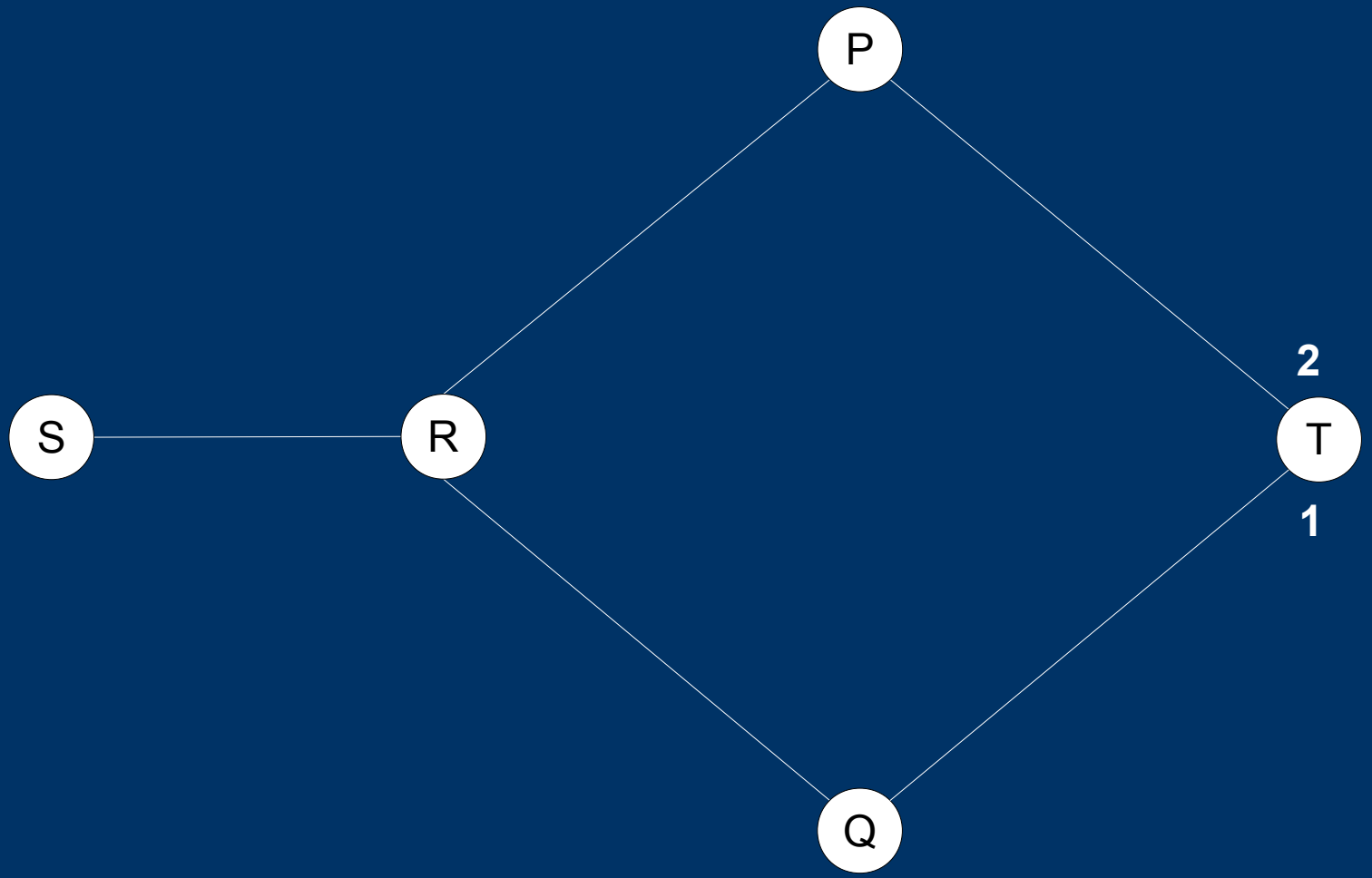
SAVE: Source Address Validity Enforcement

- Provides routers an incoming table, to know which direction packets should come from
- Updates travel the same path as legitimate traffic, informing routers of incoming direction
- Lightweight and scalable
- Only requires an existing forwarding table

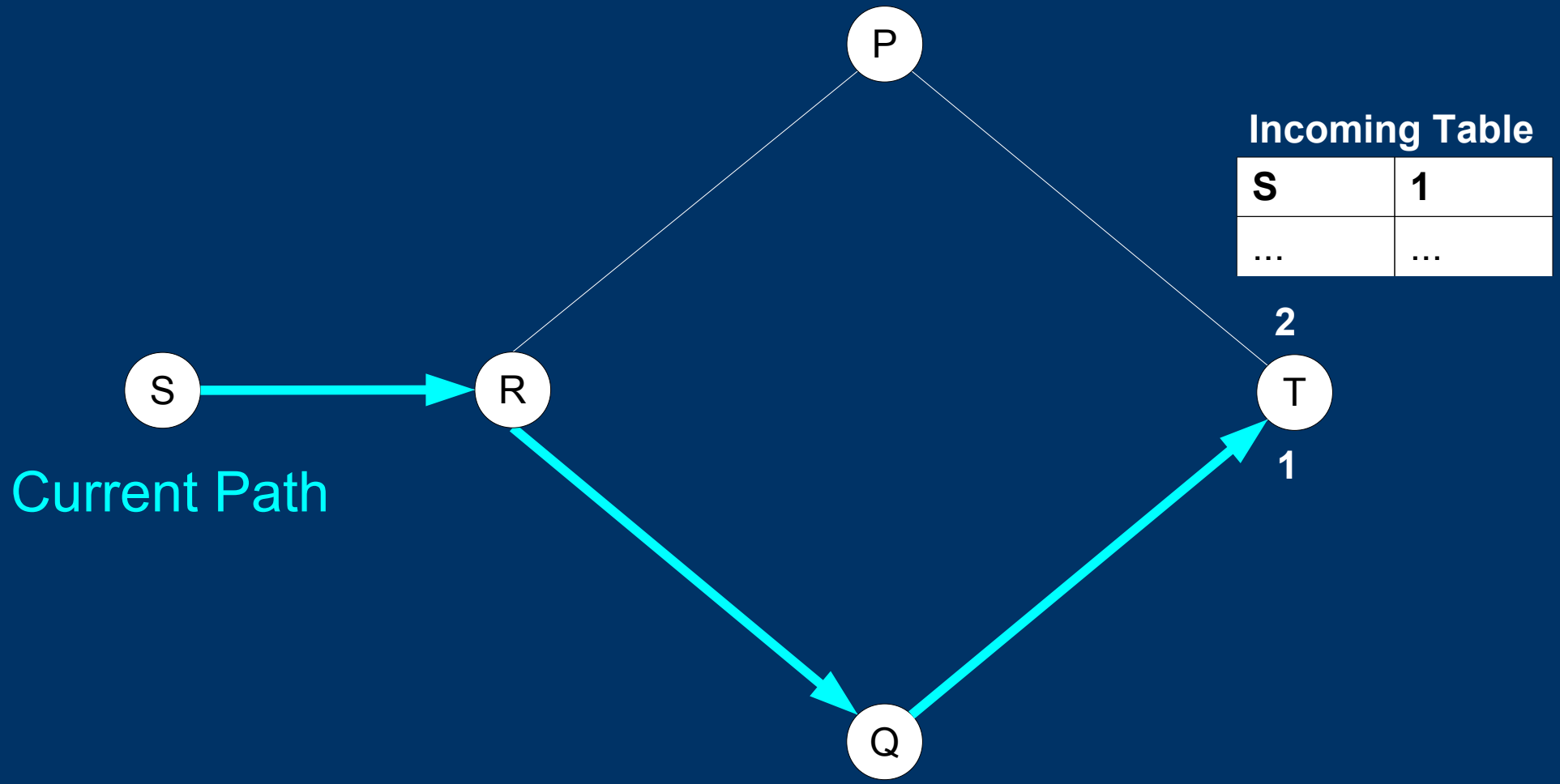
Jun Li, Jelena Mirkovic, Toby Ehrenkranz, Mengqiu Wang, Peter Reiher, and Lixia Zhang, "Learning the valid incoming direction of IP packets," Computer Networks, vol. 52, no. 2, February 2008, pp. 399-417.

Jun Li, Jelena Mirkovic, Mengqiu Wang, Peter L. Reiher, and Lixia Zhang, "SAVE: Source address validity enforcement protocol," in IEEE INFOCOM, June 2002, pp. 1557-66

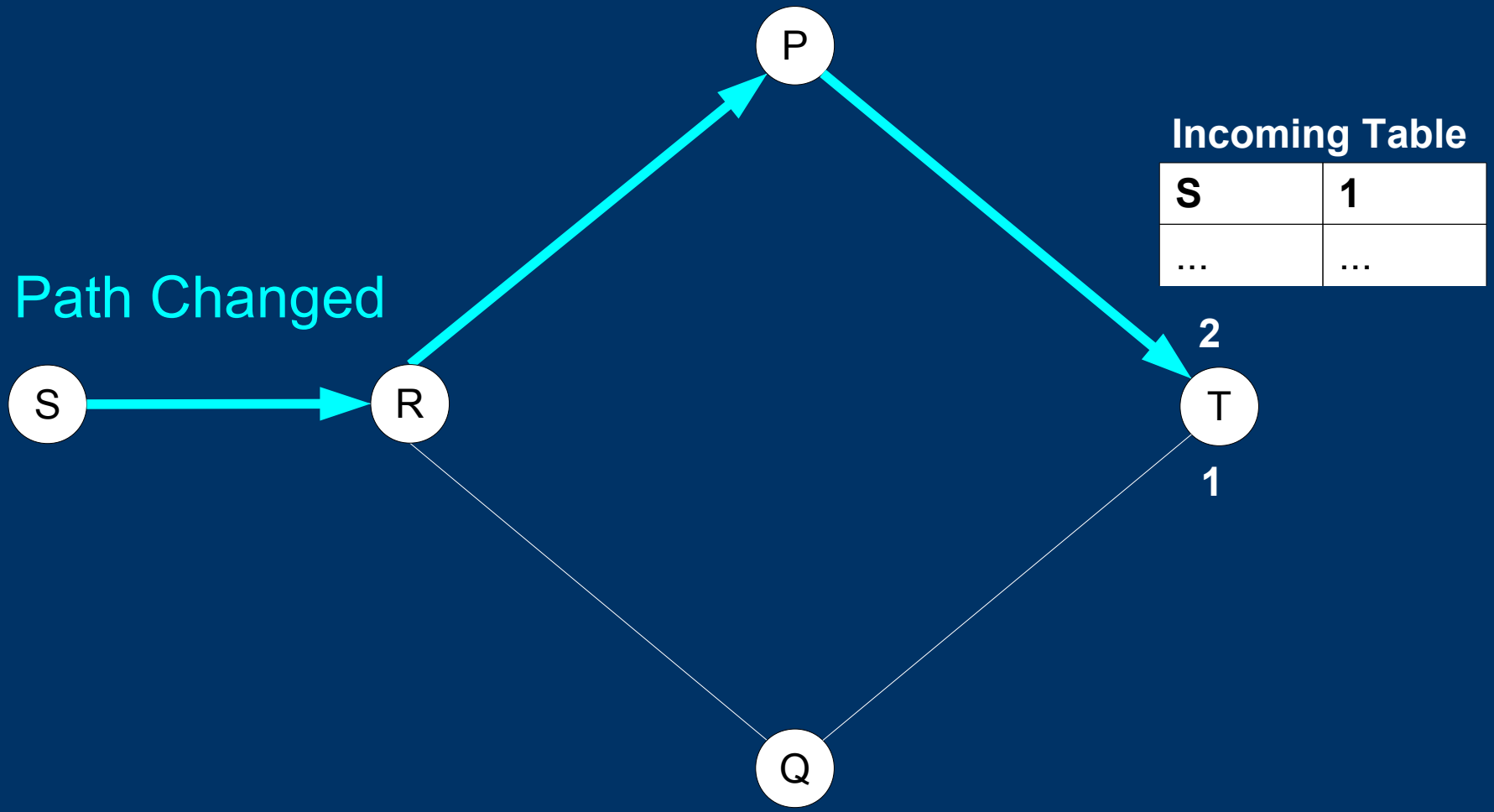
SAVE Update Initiation



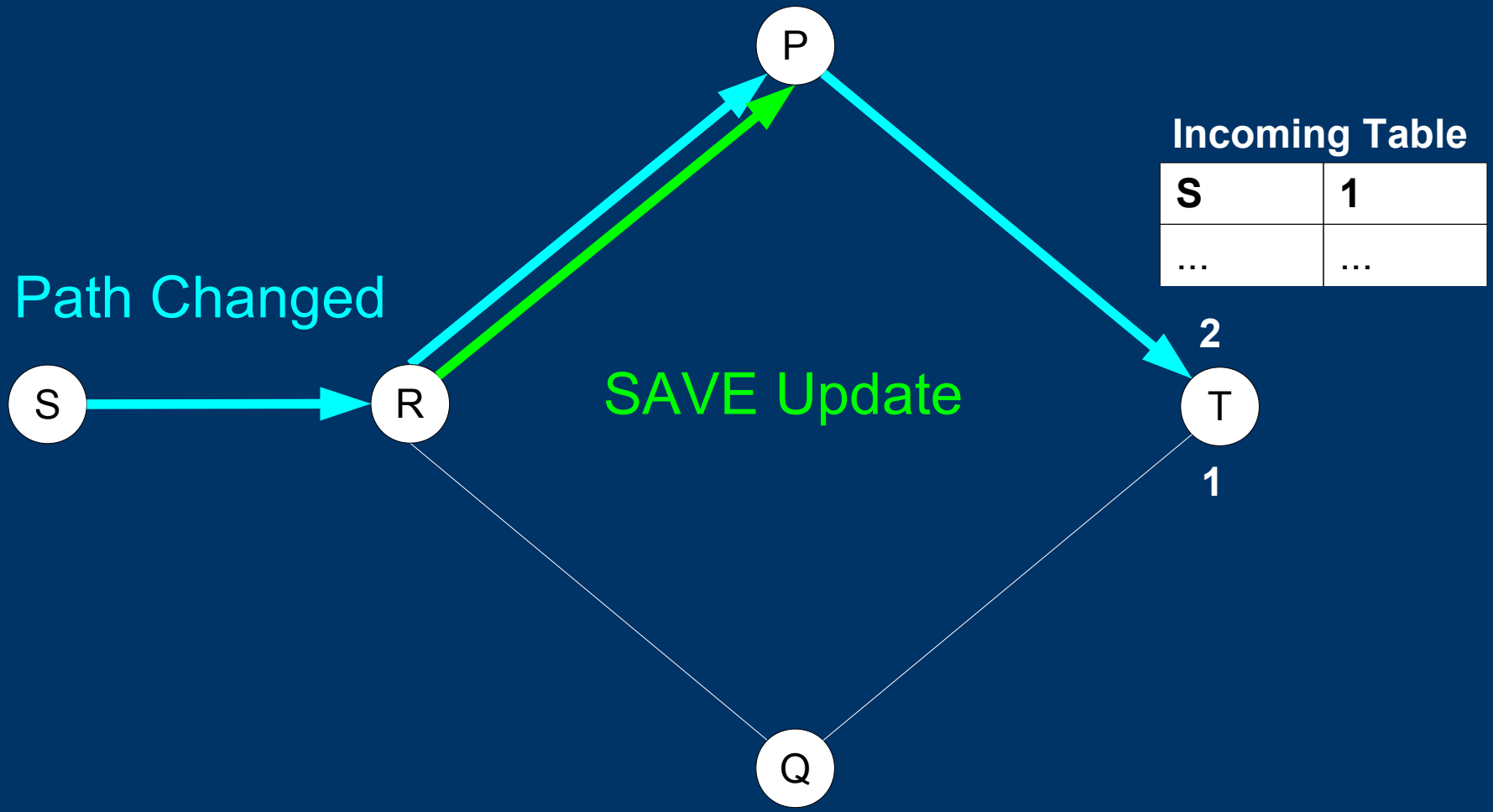
SAVE Update Initiation



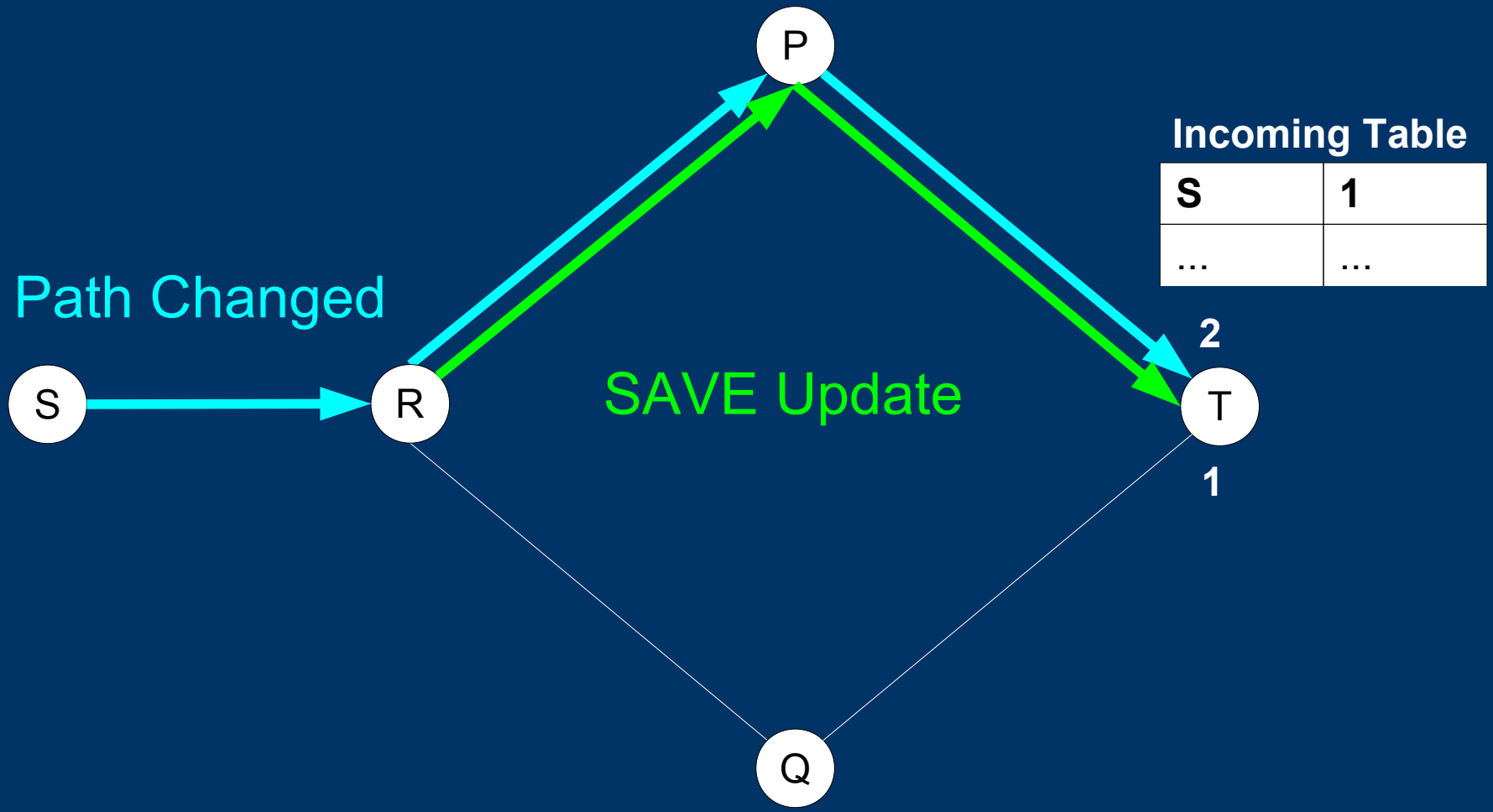
SAVE Update Initiation



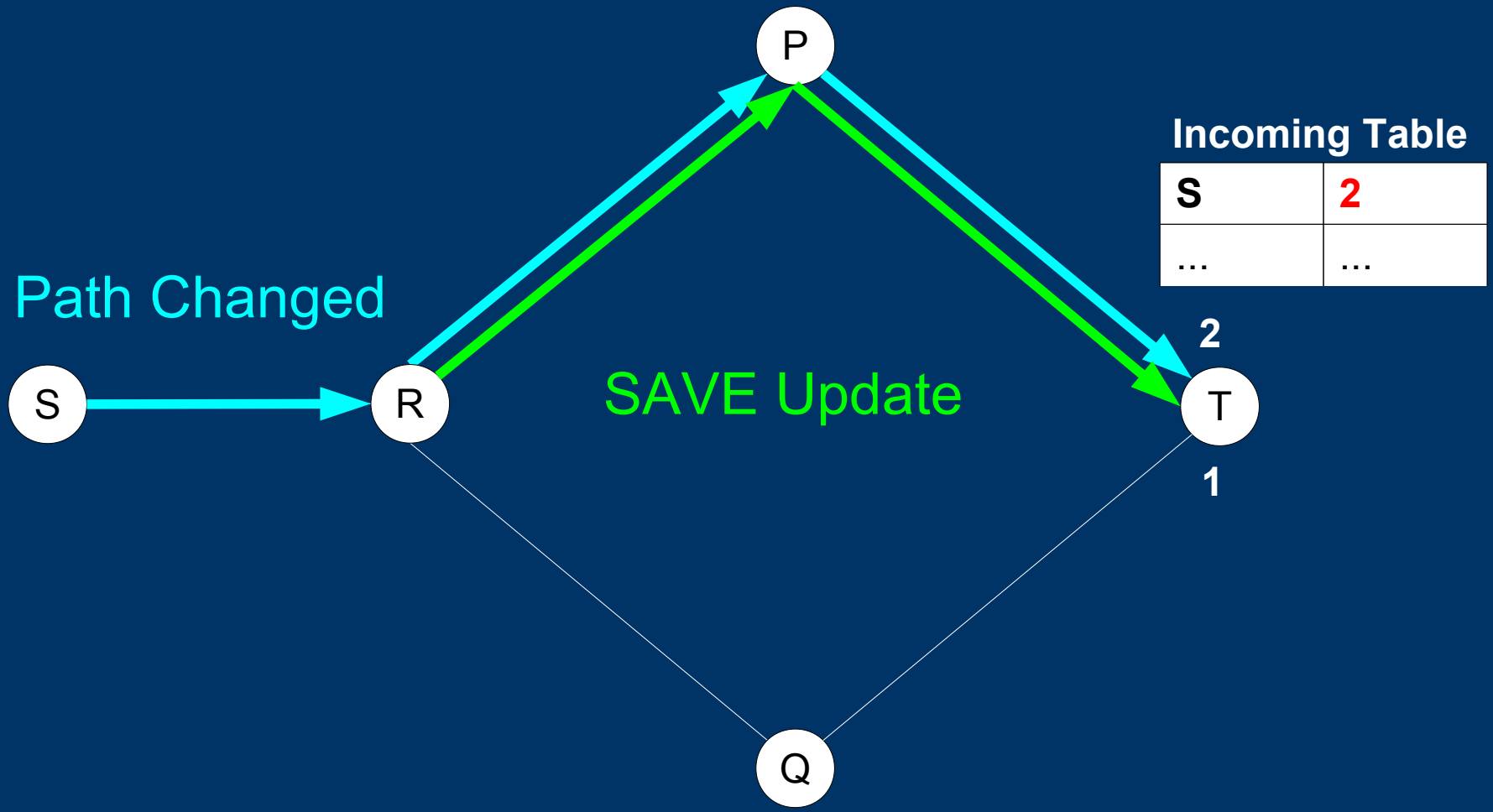
SAVE Update Initiation



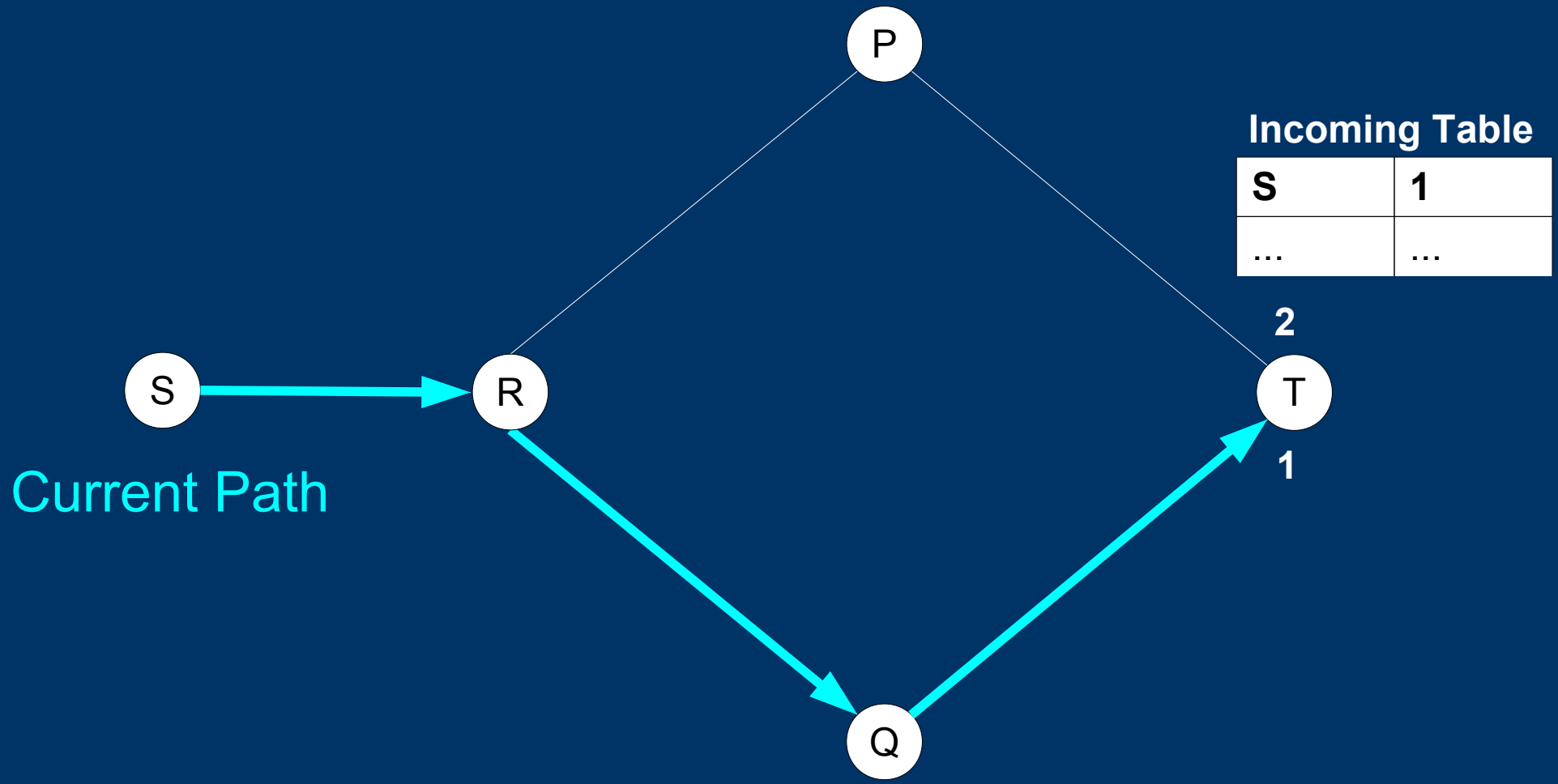
SAVE Update Initiation



SAVE Update Initiation

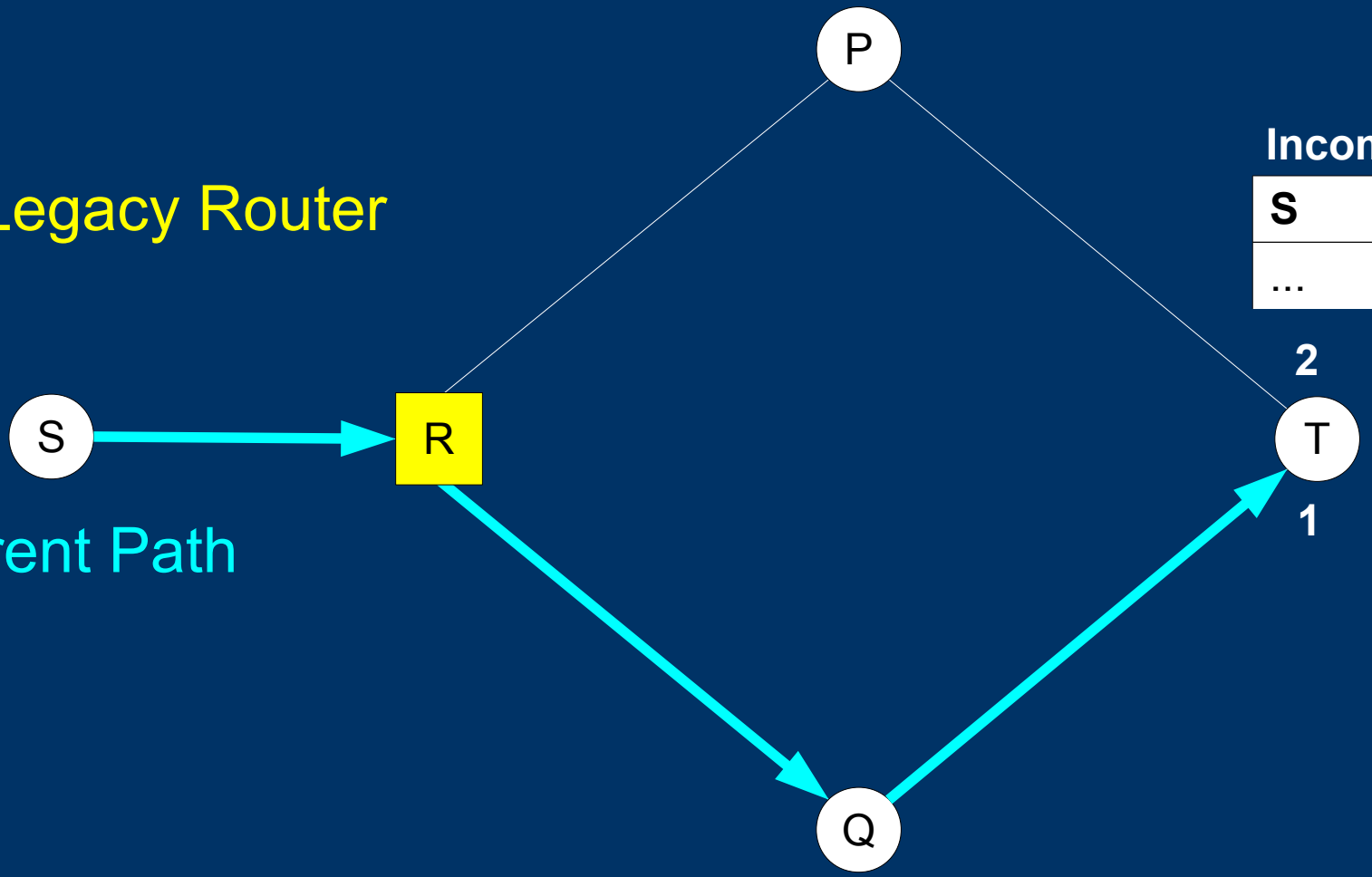


SAVE Update Initiation And Legacy Routers



SAVE Update Initiation And Legacy Routers

R is a Legacy Router



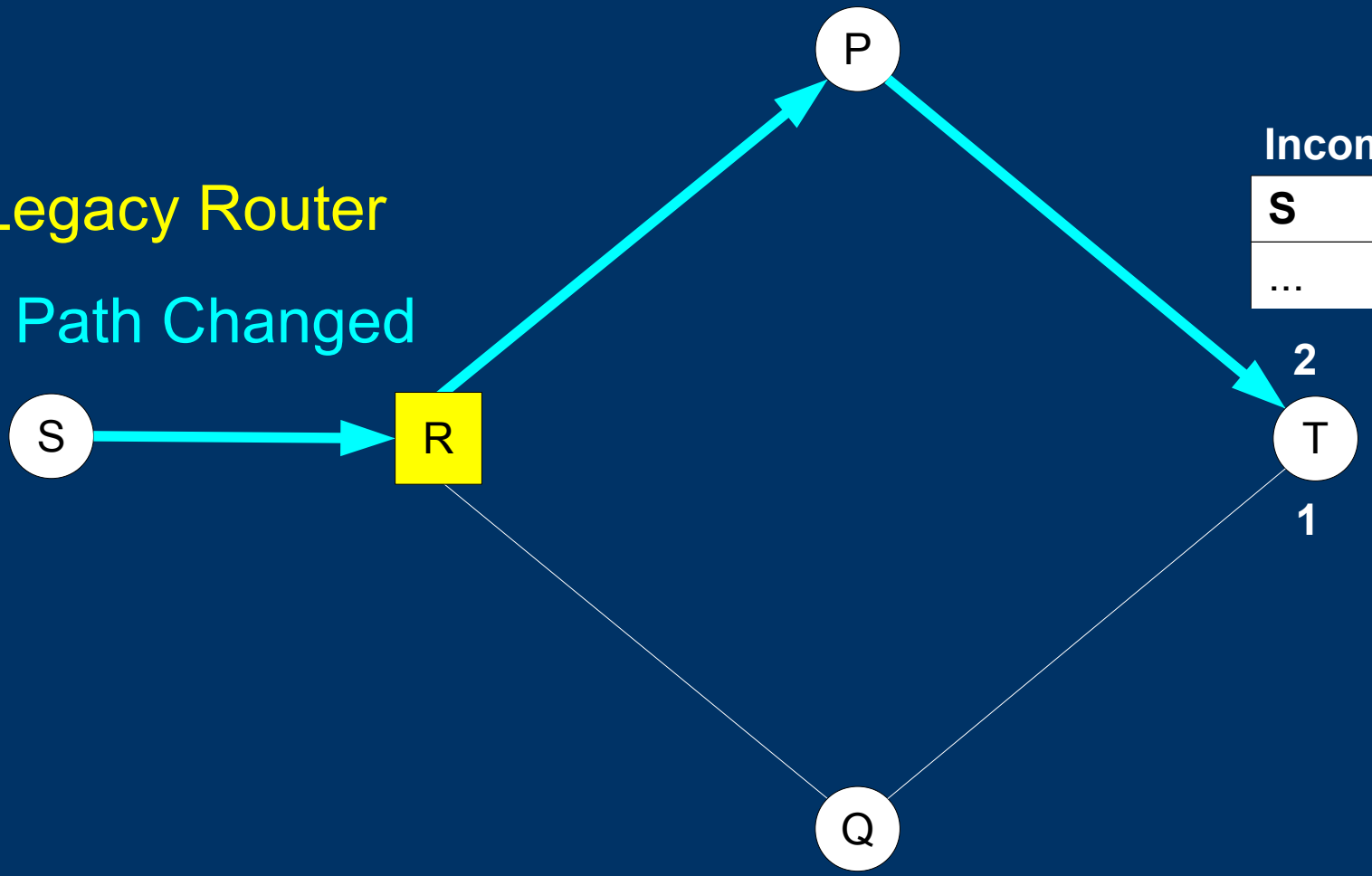
Incoming Table

S	**1**
...	...

SAVE Update Initiation And Legacy Routers

R is a Legacy Router

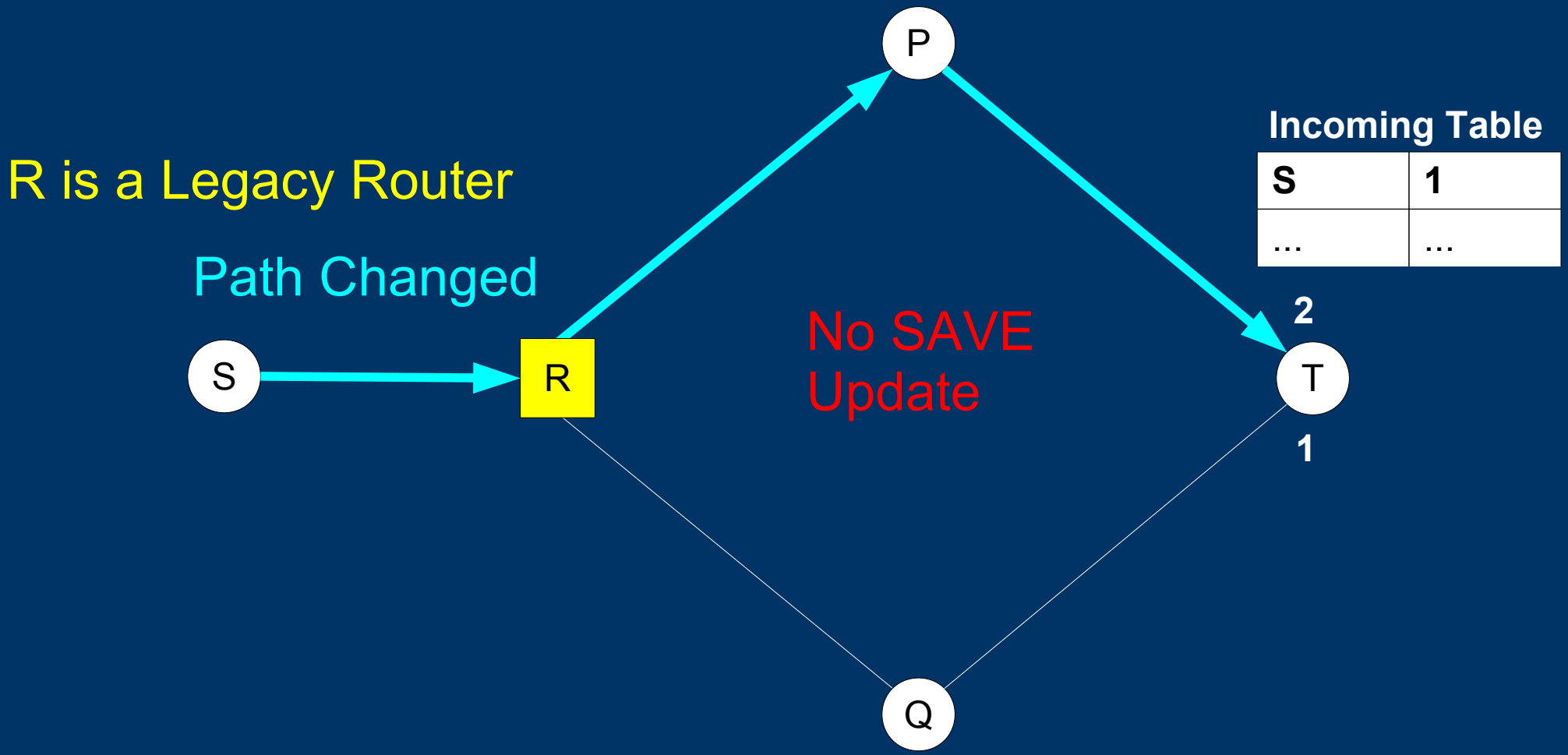
Path Changed



Incoming Table

S	1
...	...

SAVE Update Initiation And Legacy Routers



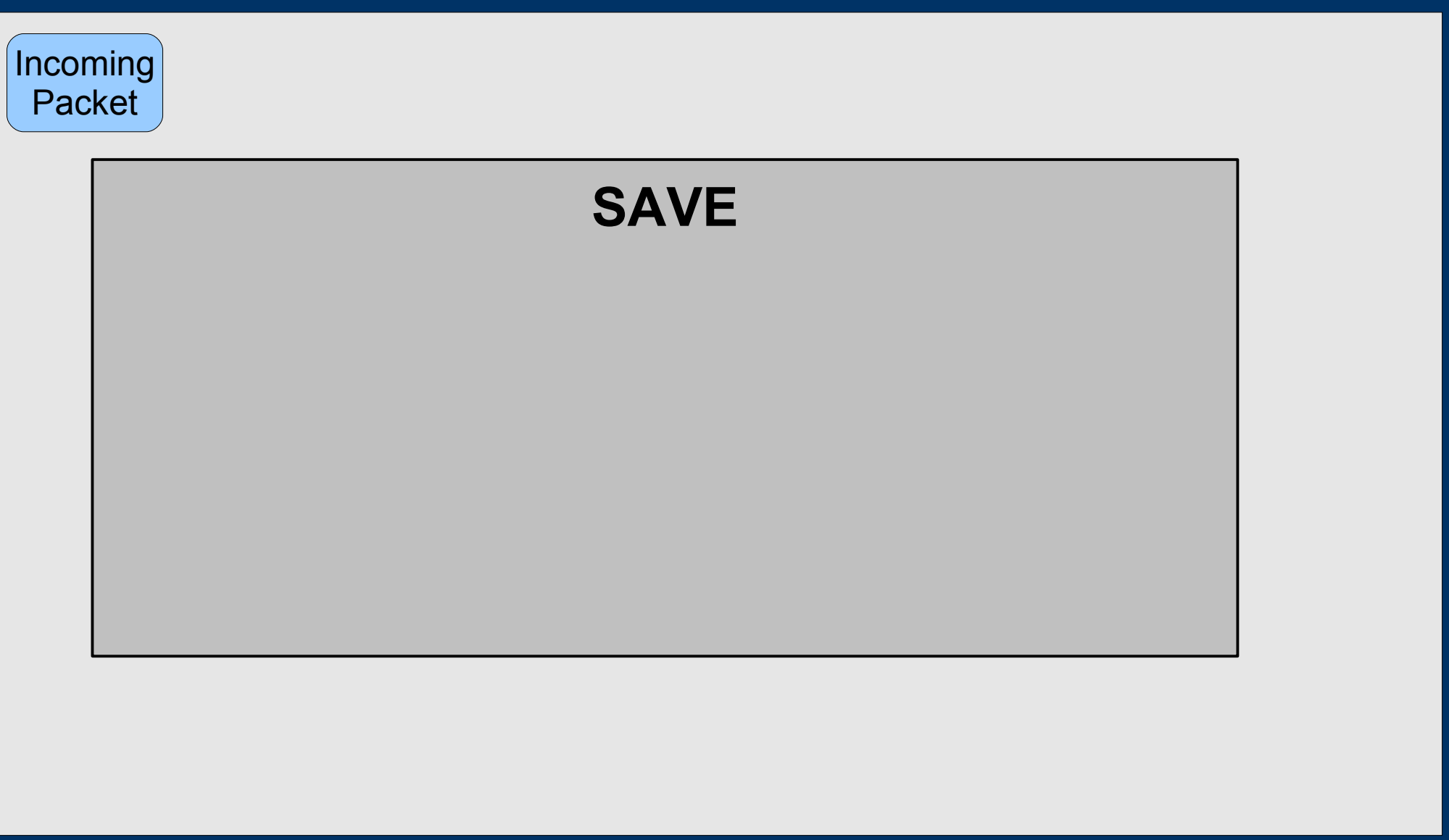
Outline

- Introduction
- Related/Existing Work
- New Mechanisms of SAVE
- Evaluation
- Conclusion

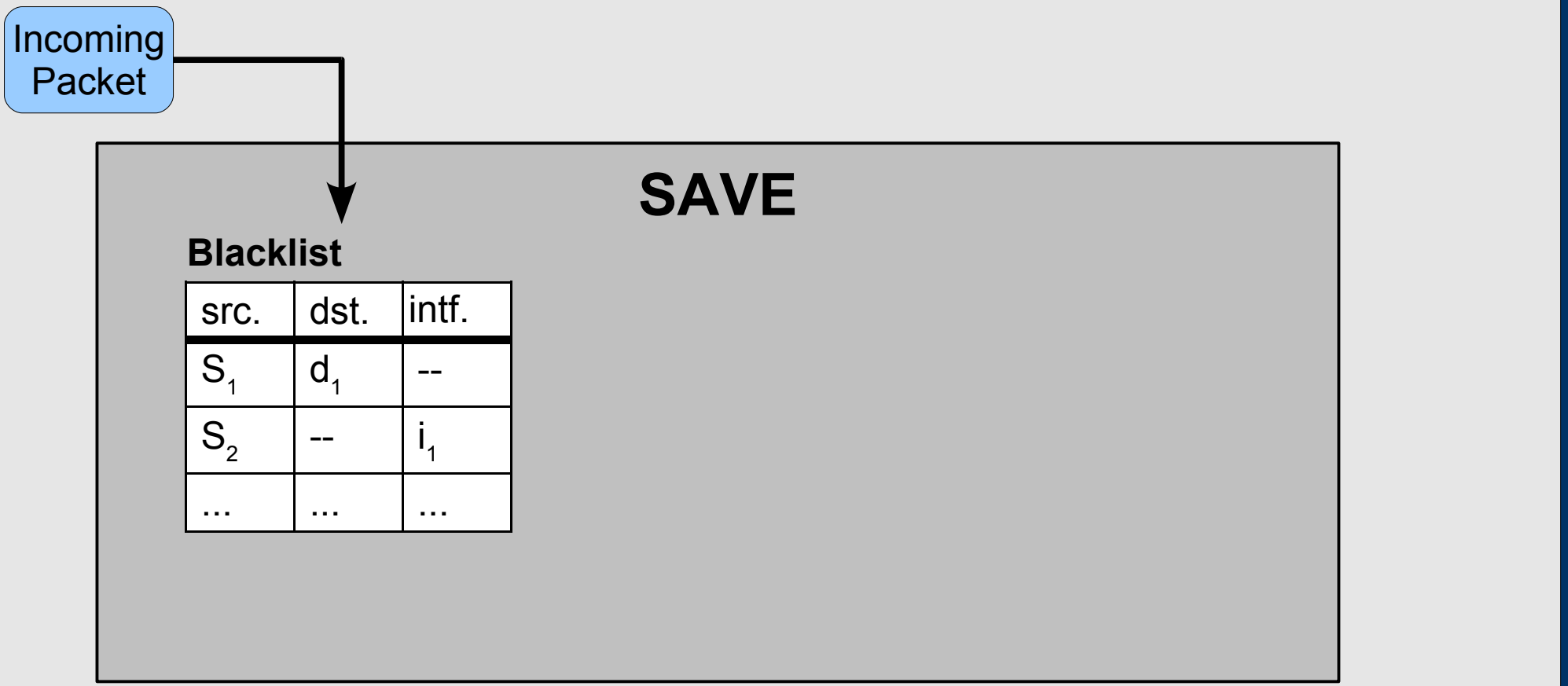
New Mechanisms of SAVE

- On-demand update: verifies incoming direction information
- Blacklist: keeps track of traits seen in packets spoofing protected networks
- Pushback: filters packets as close as possible to the attacker

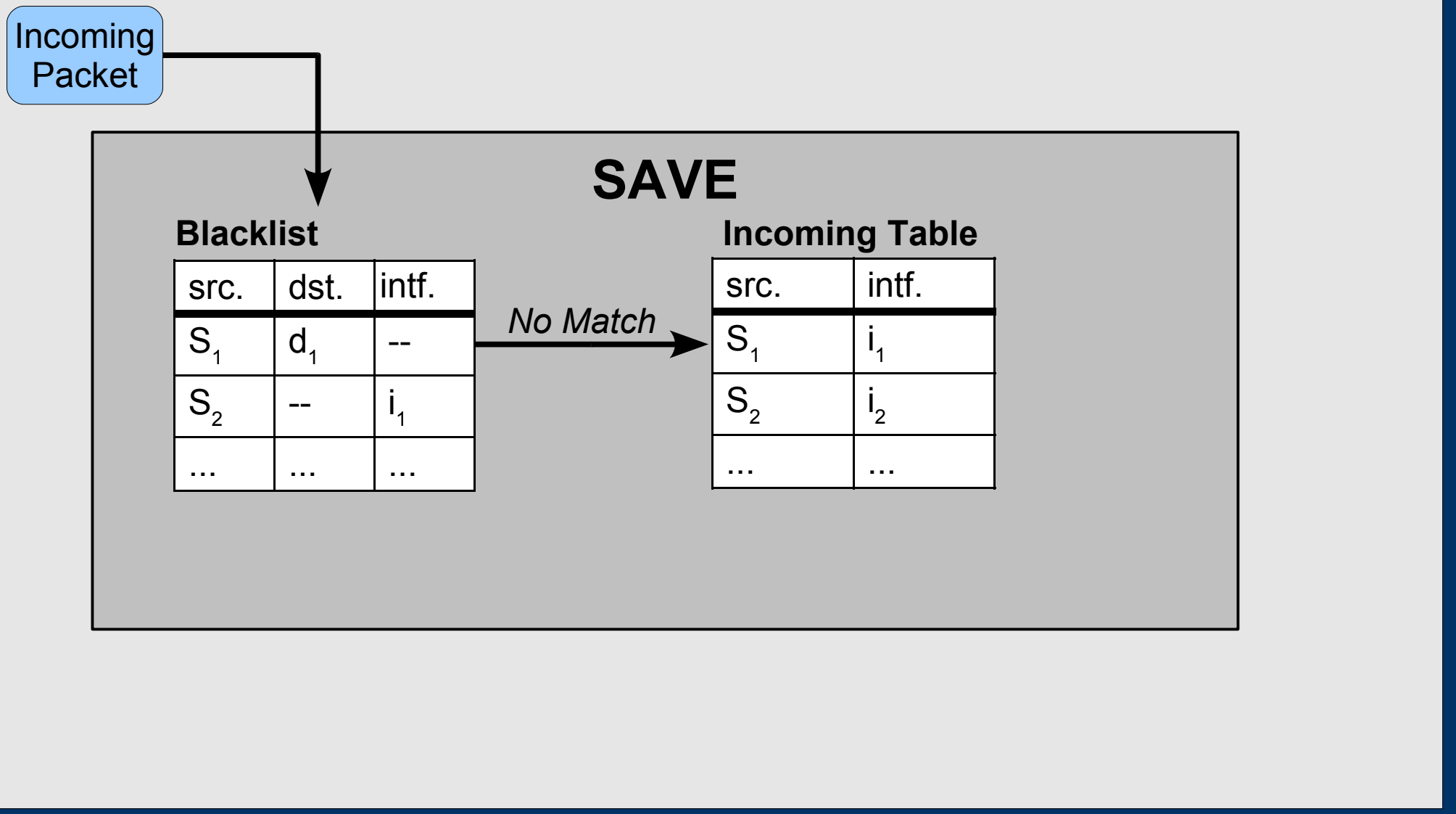
Packet Classification



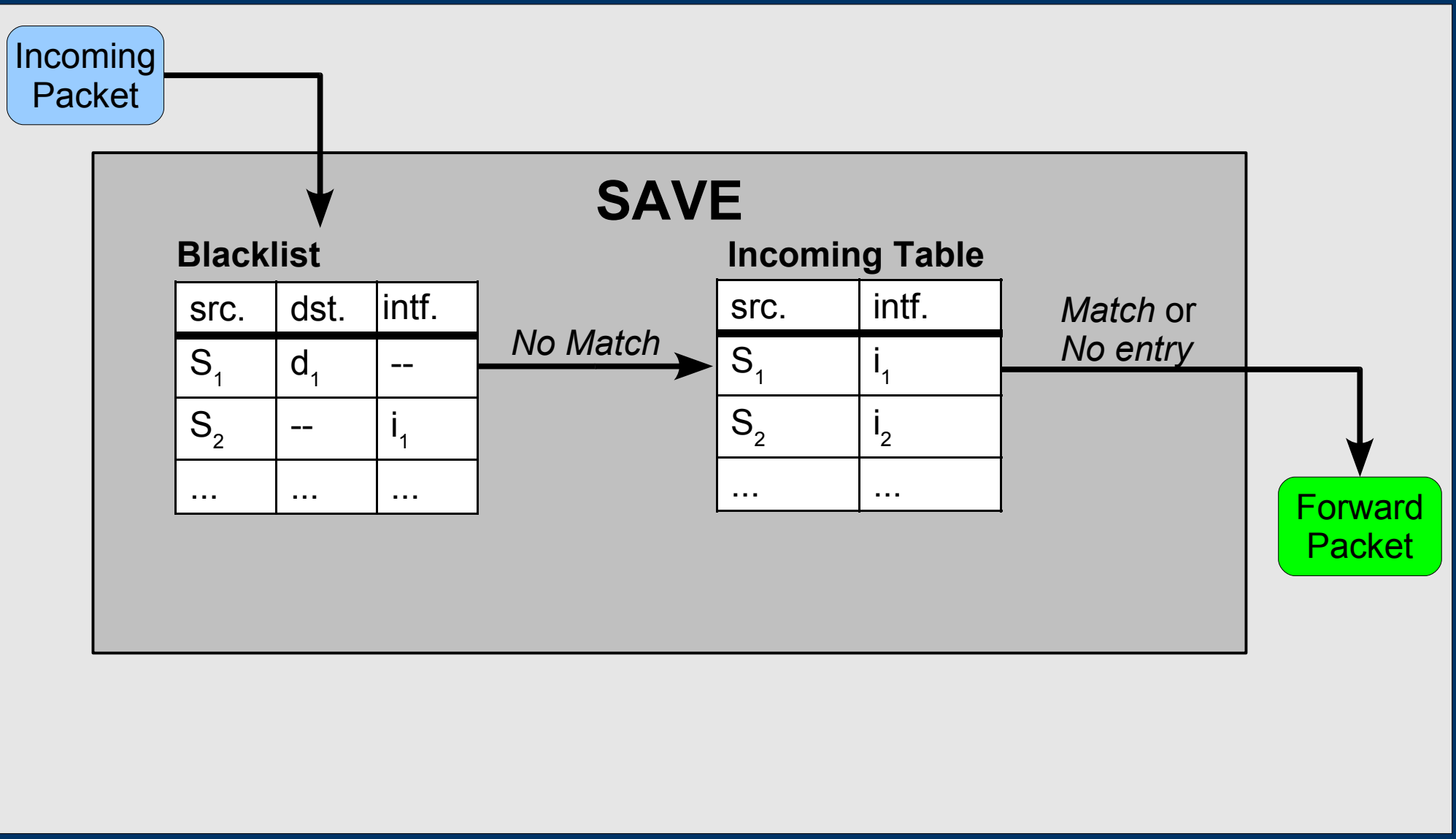
Packet Classification



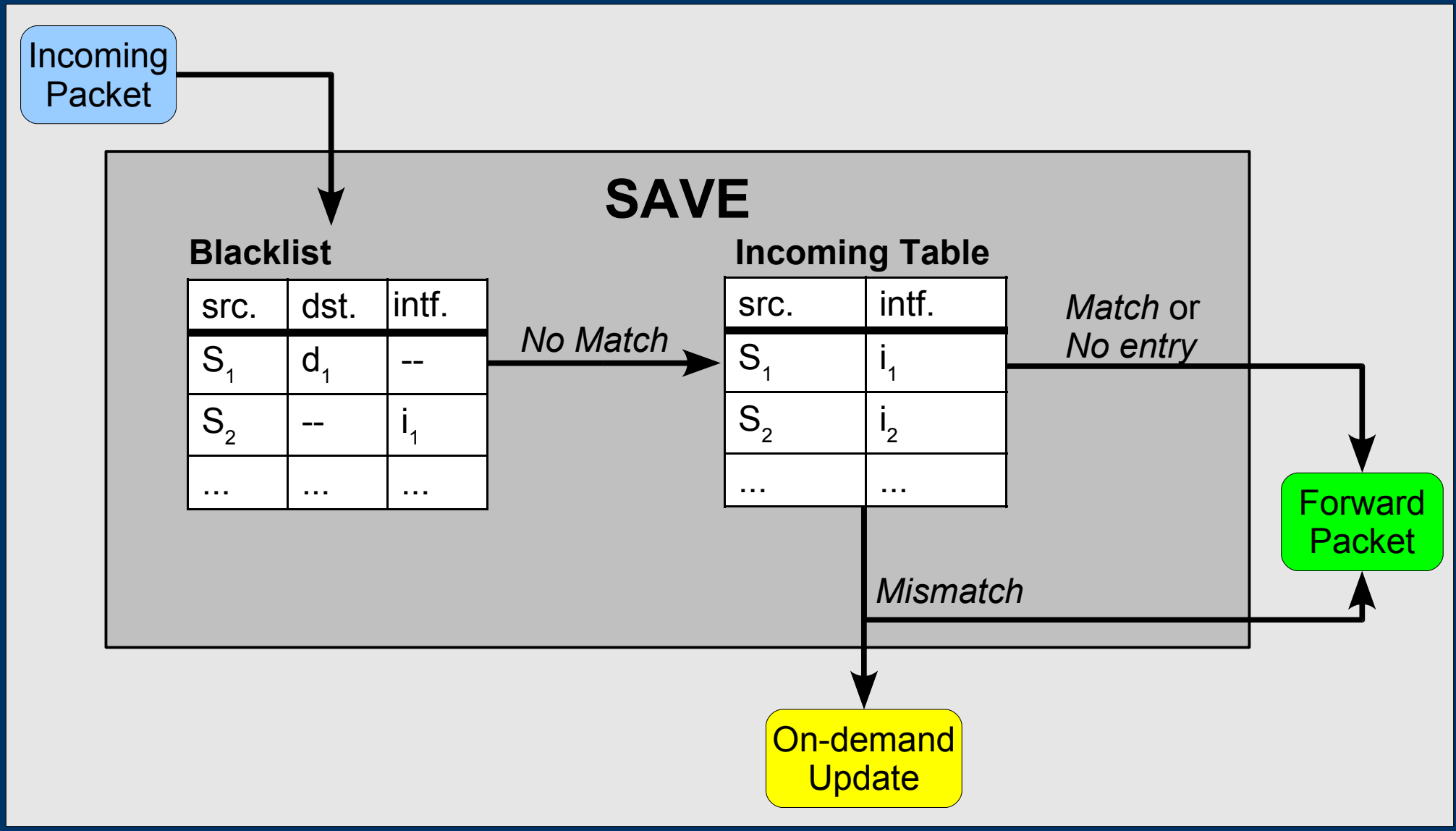
Packet Classification



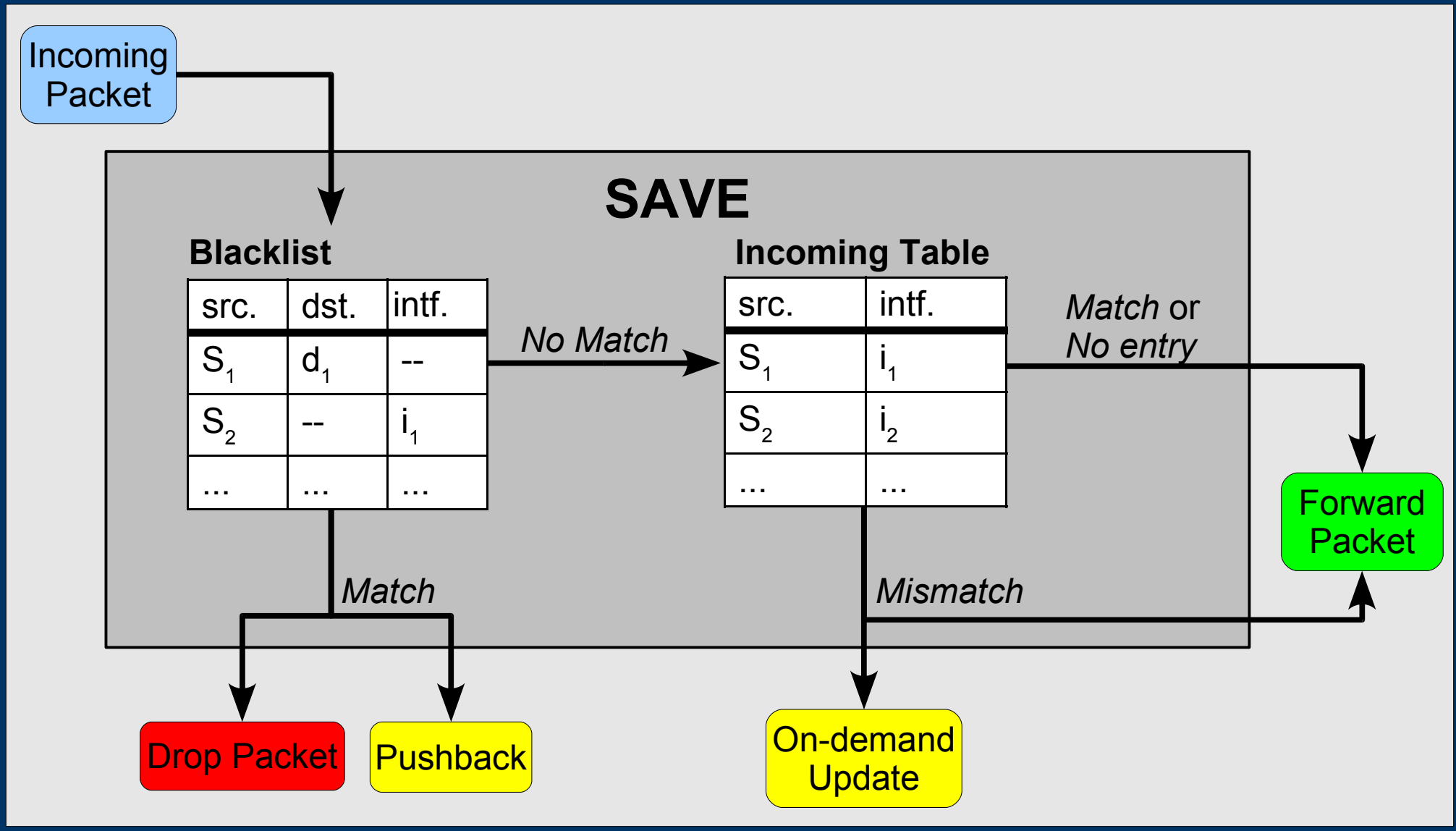
Packet Classification



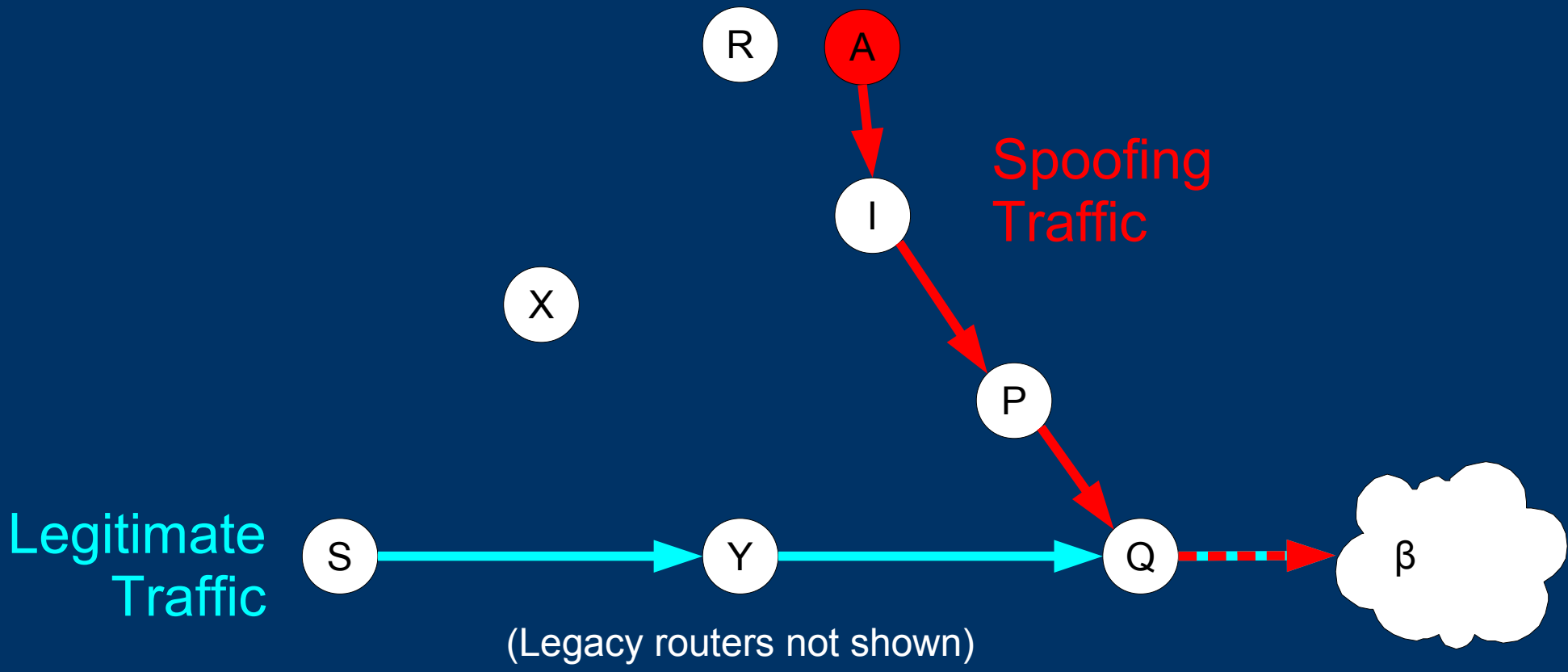
Packet Classification



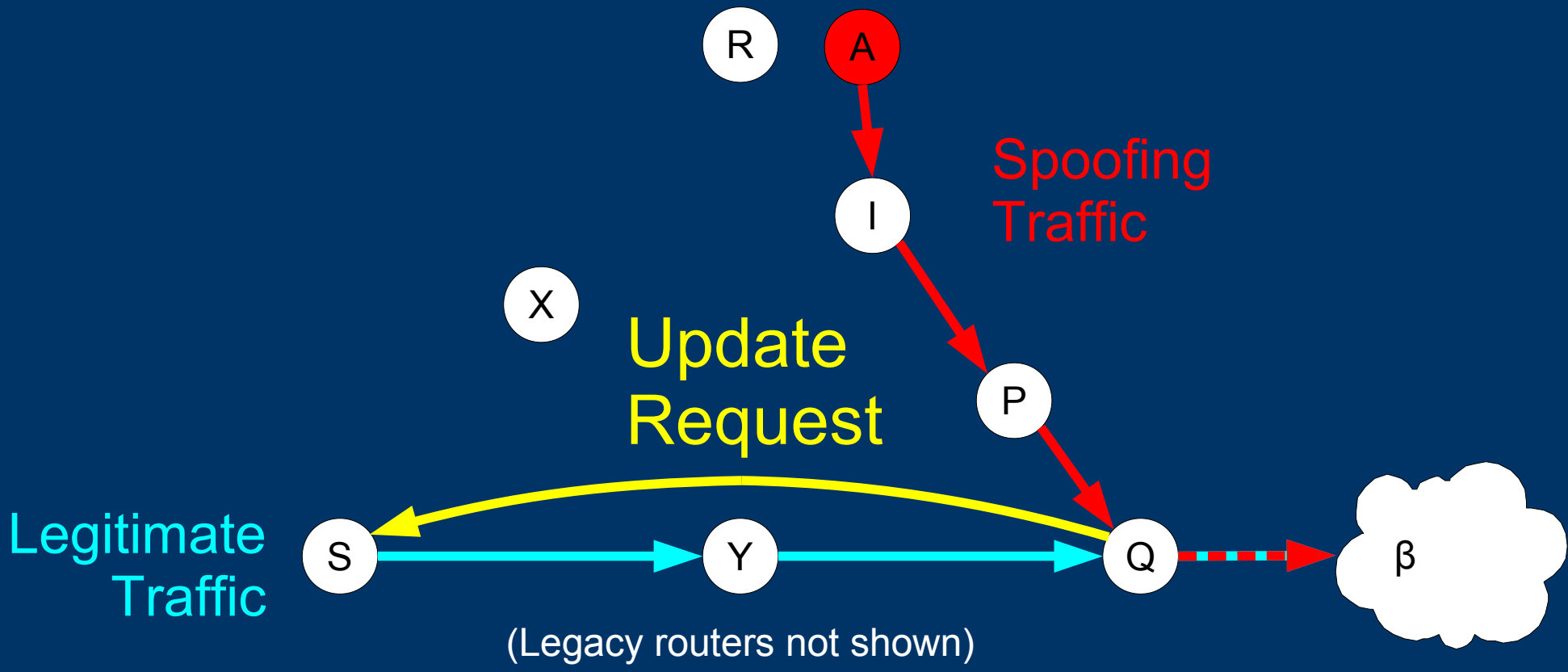
Packet Classification



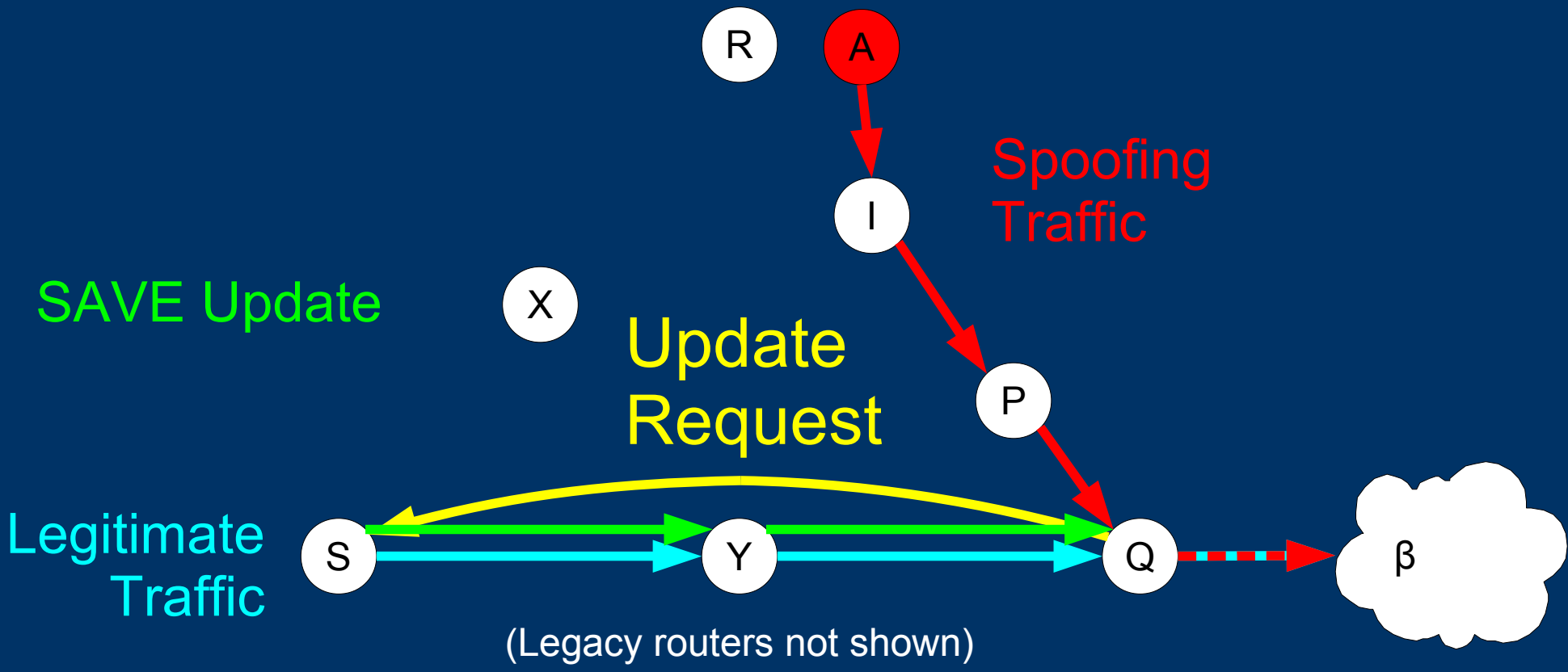
On-Demand Update



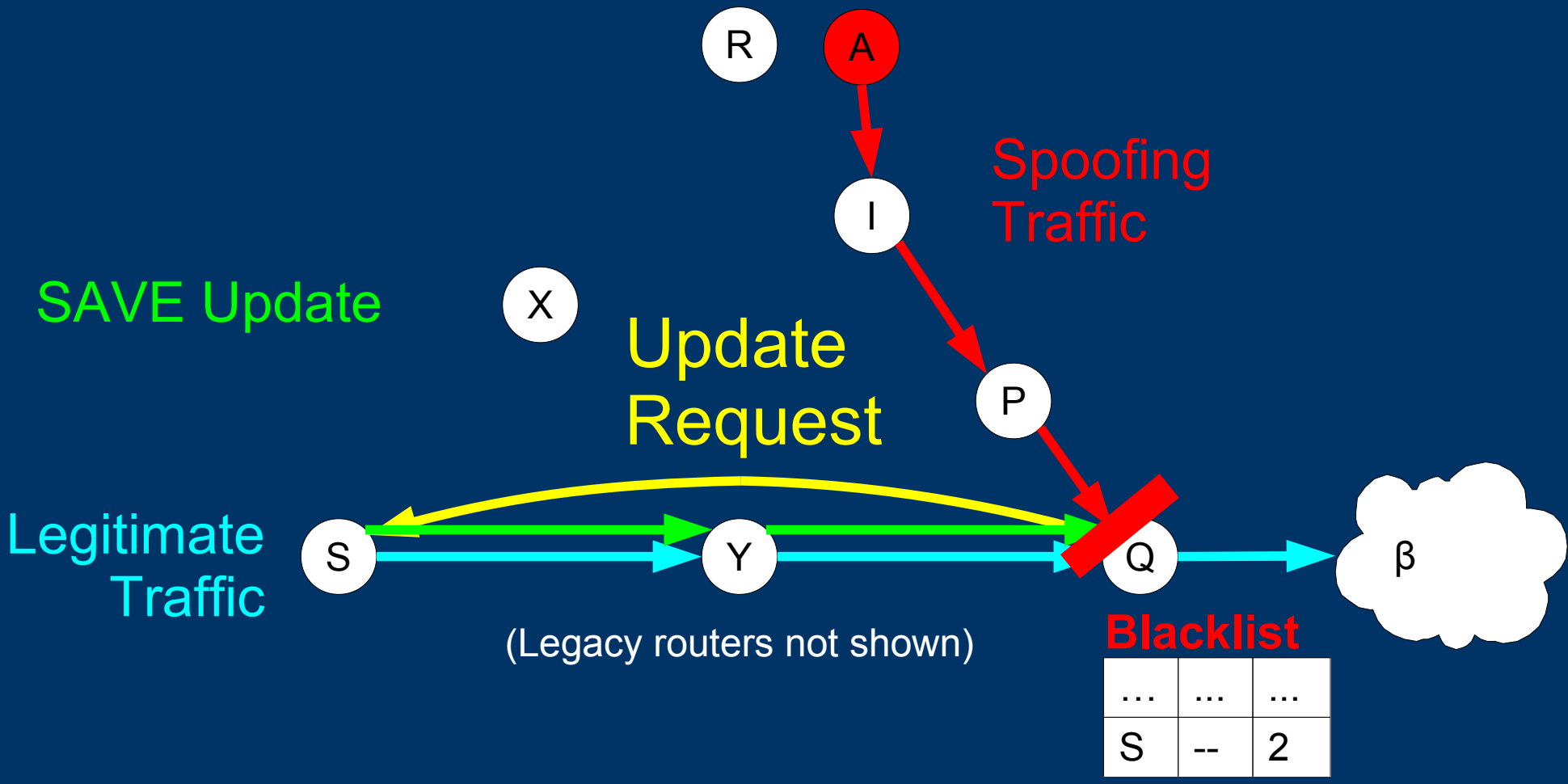
On-Demand Update



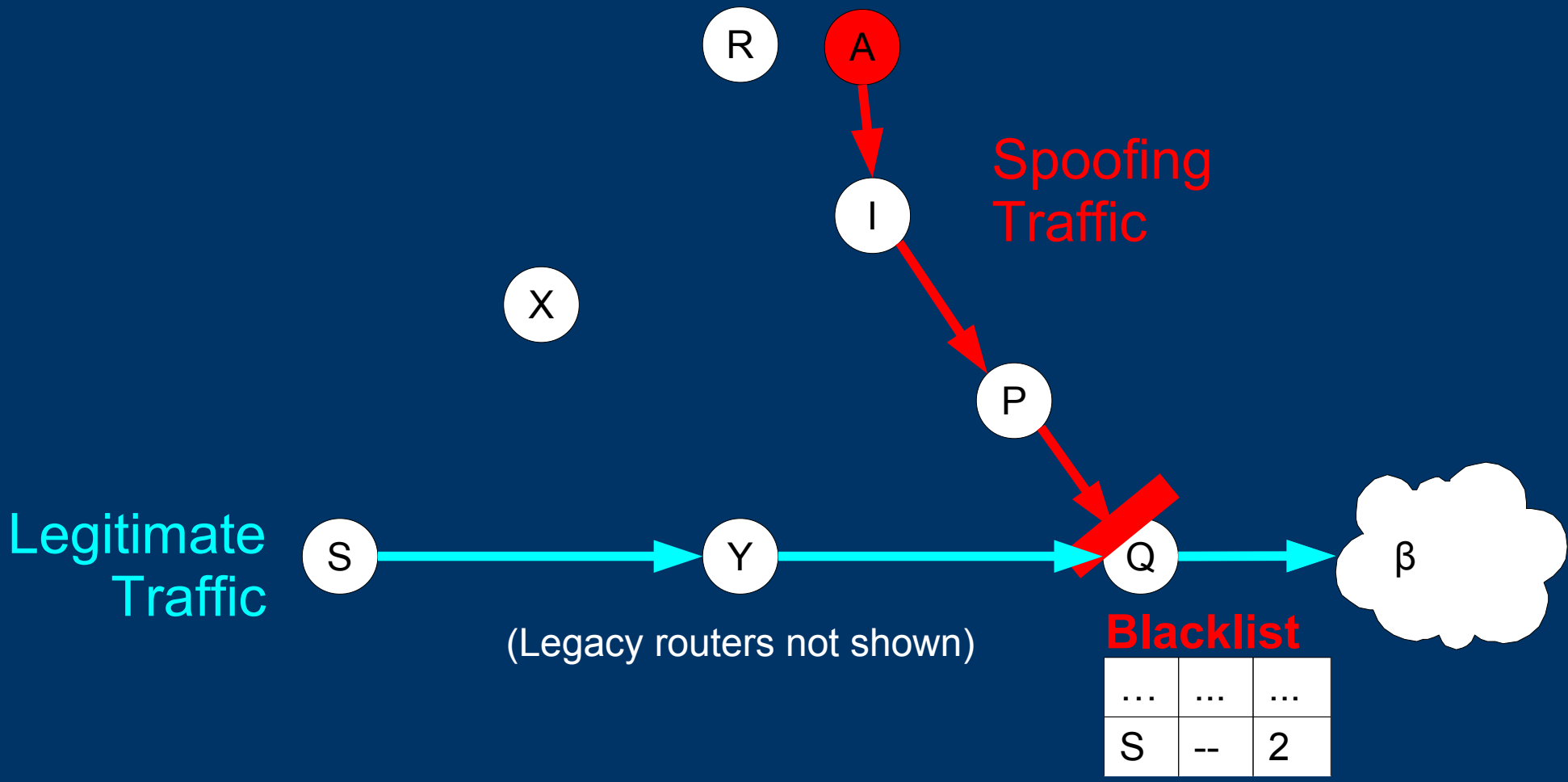
On-Demand Update



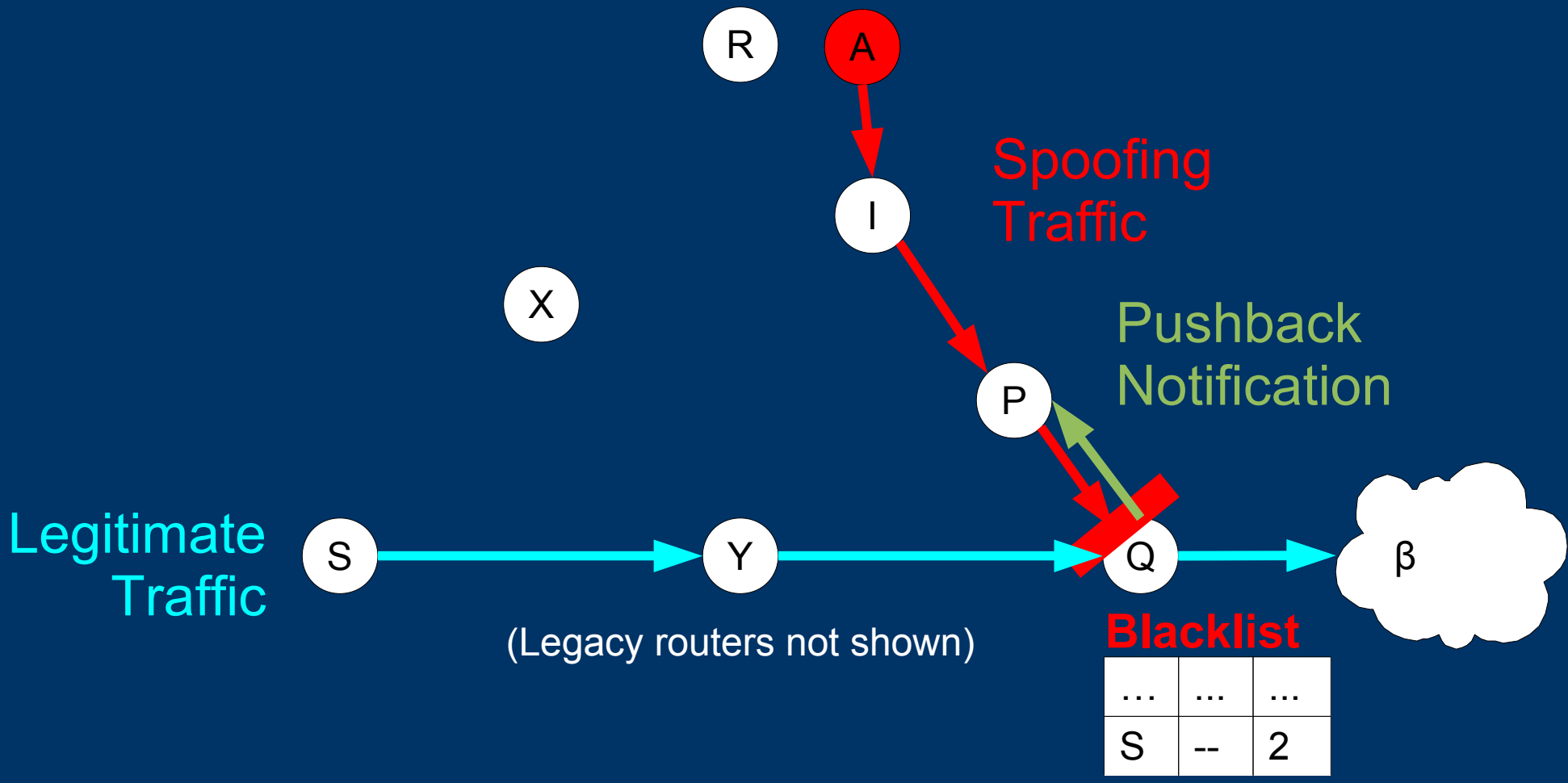
On-Demand Update



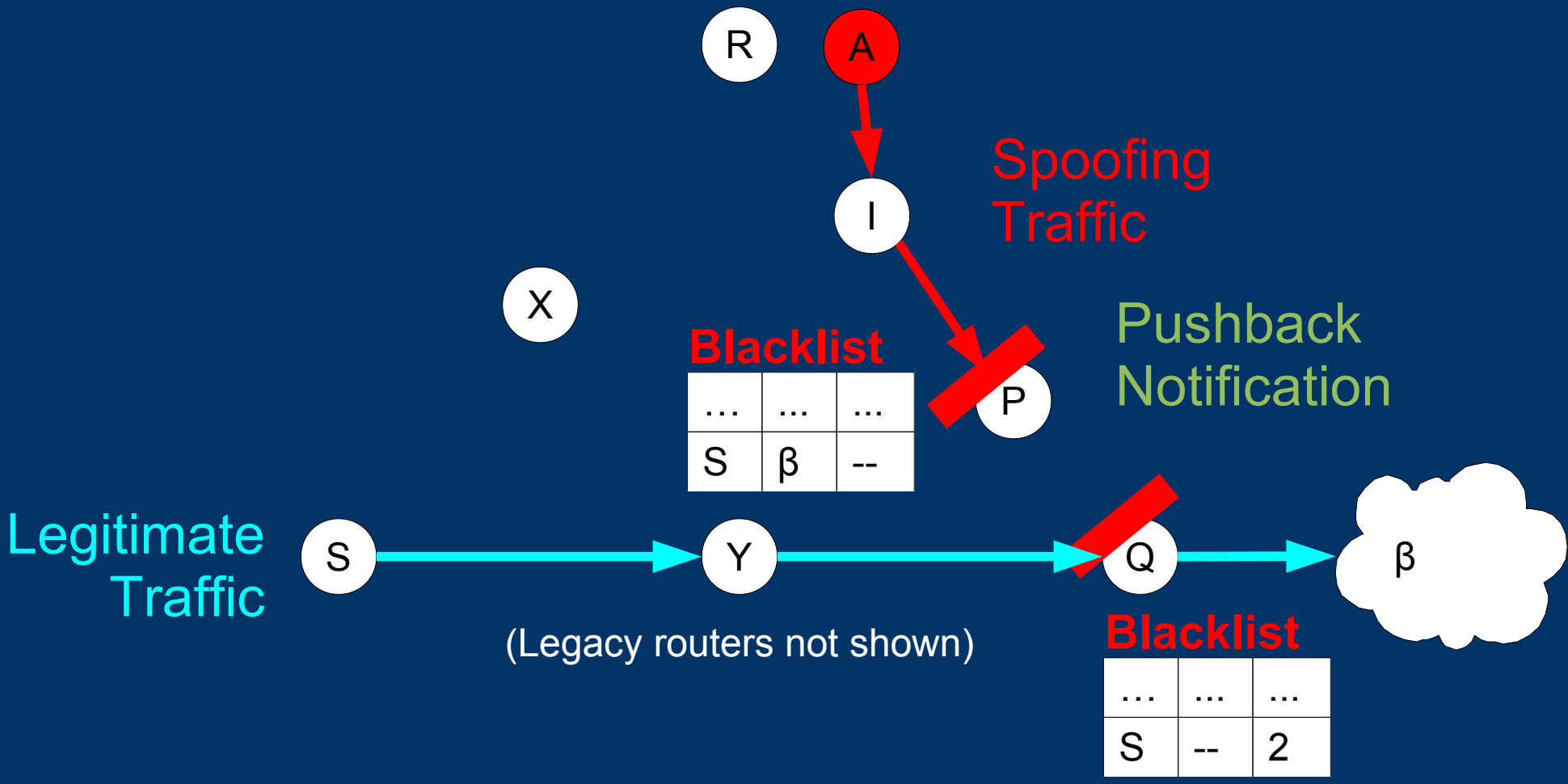
Packet-Driven Pushback



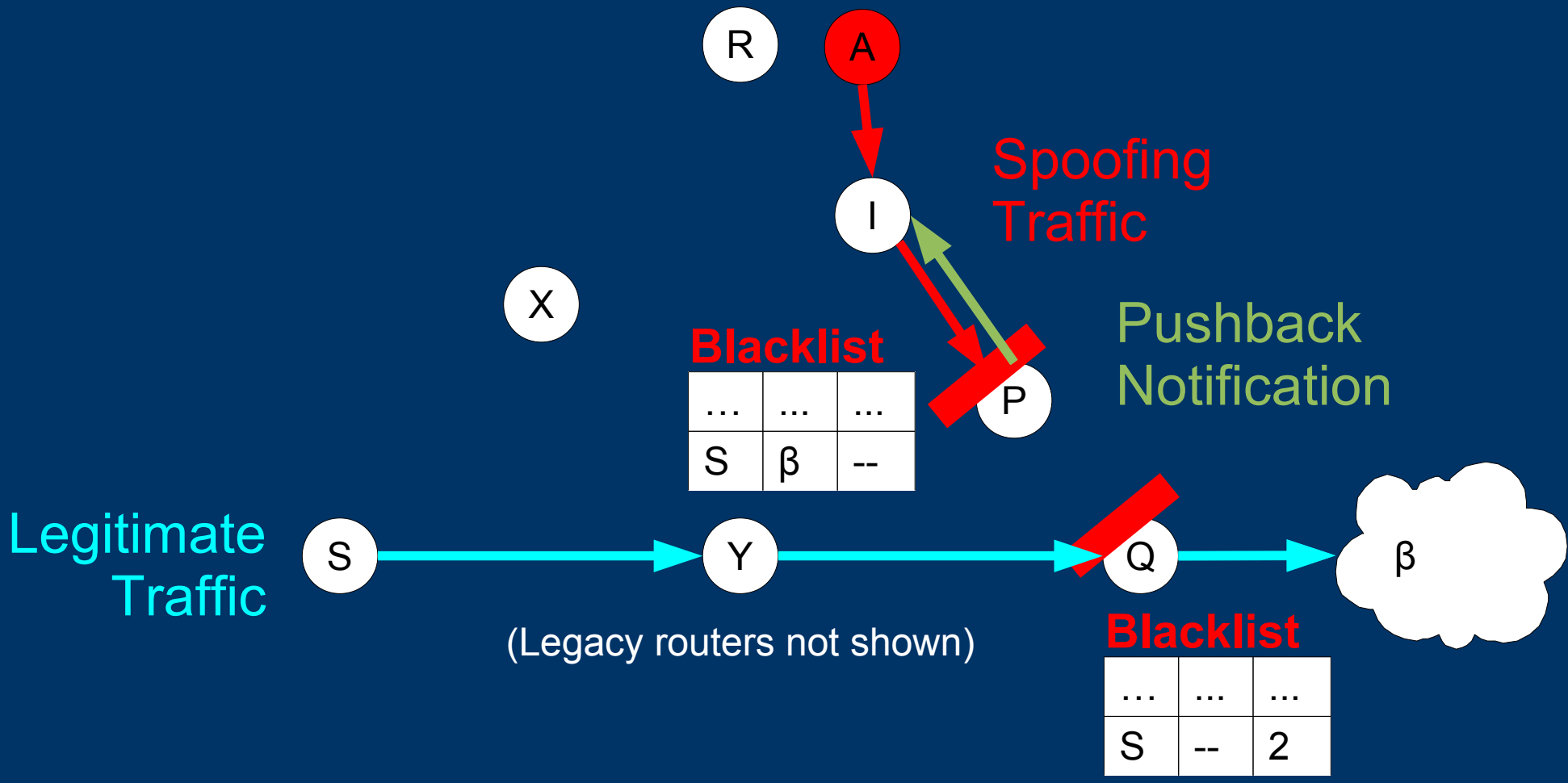
Packet-Driven Pushback



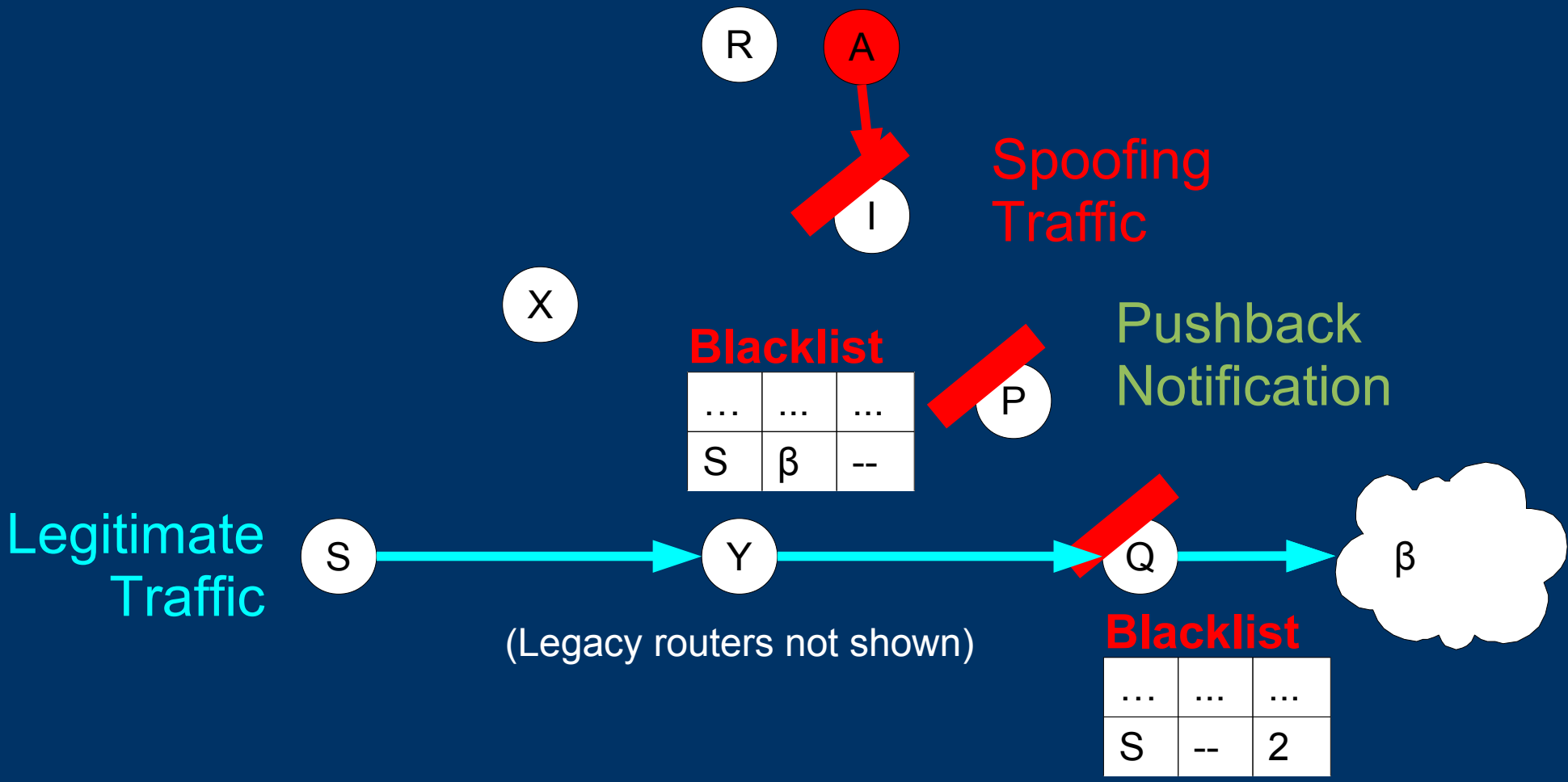
Packet-Driven Pushback



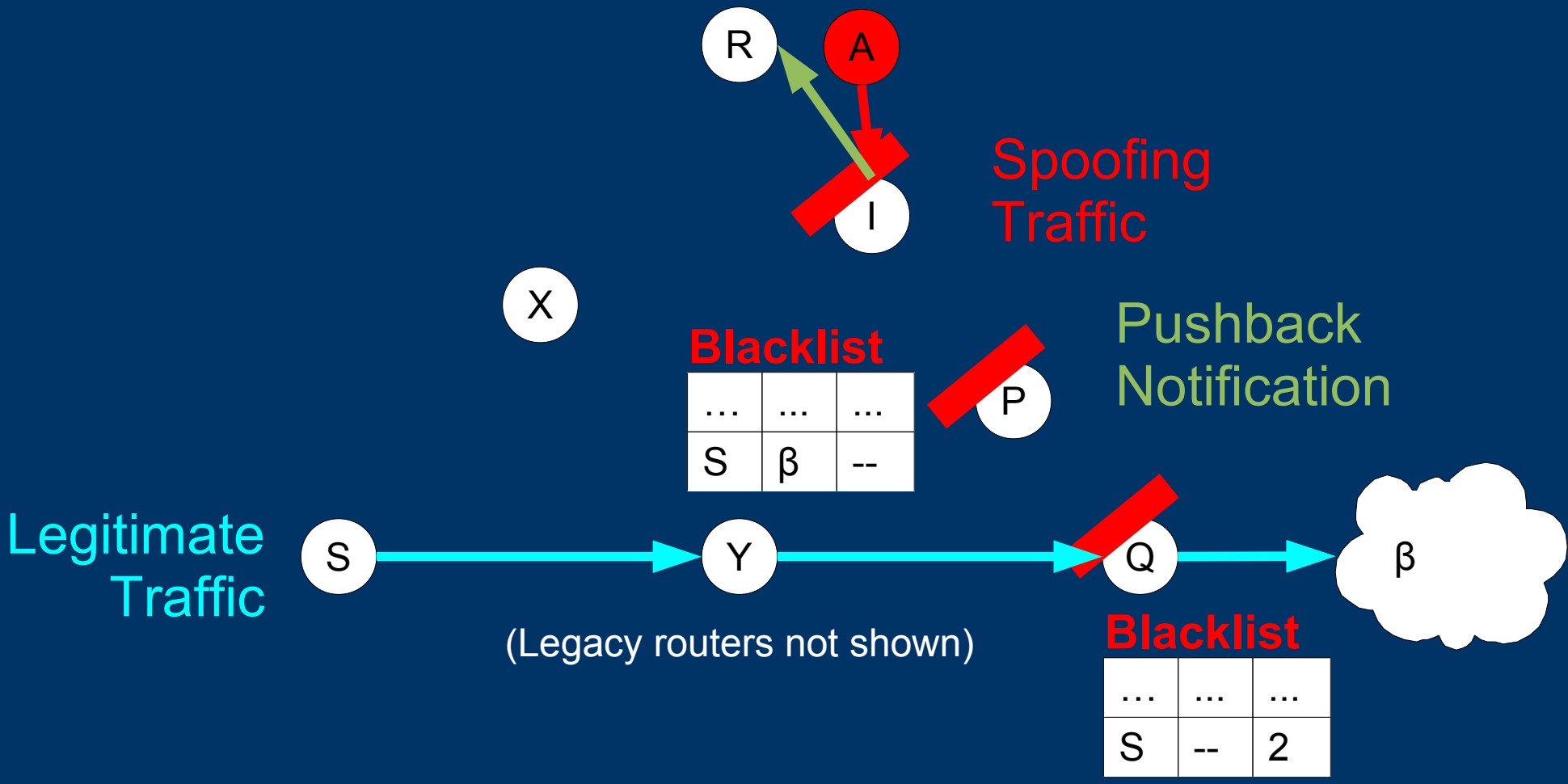
Packet-Driven Pushback



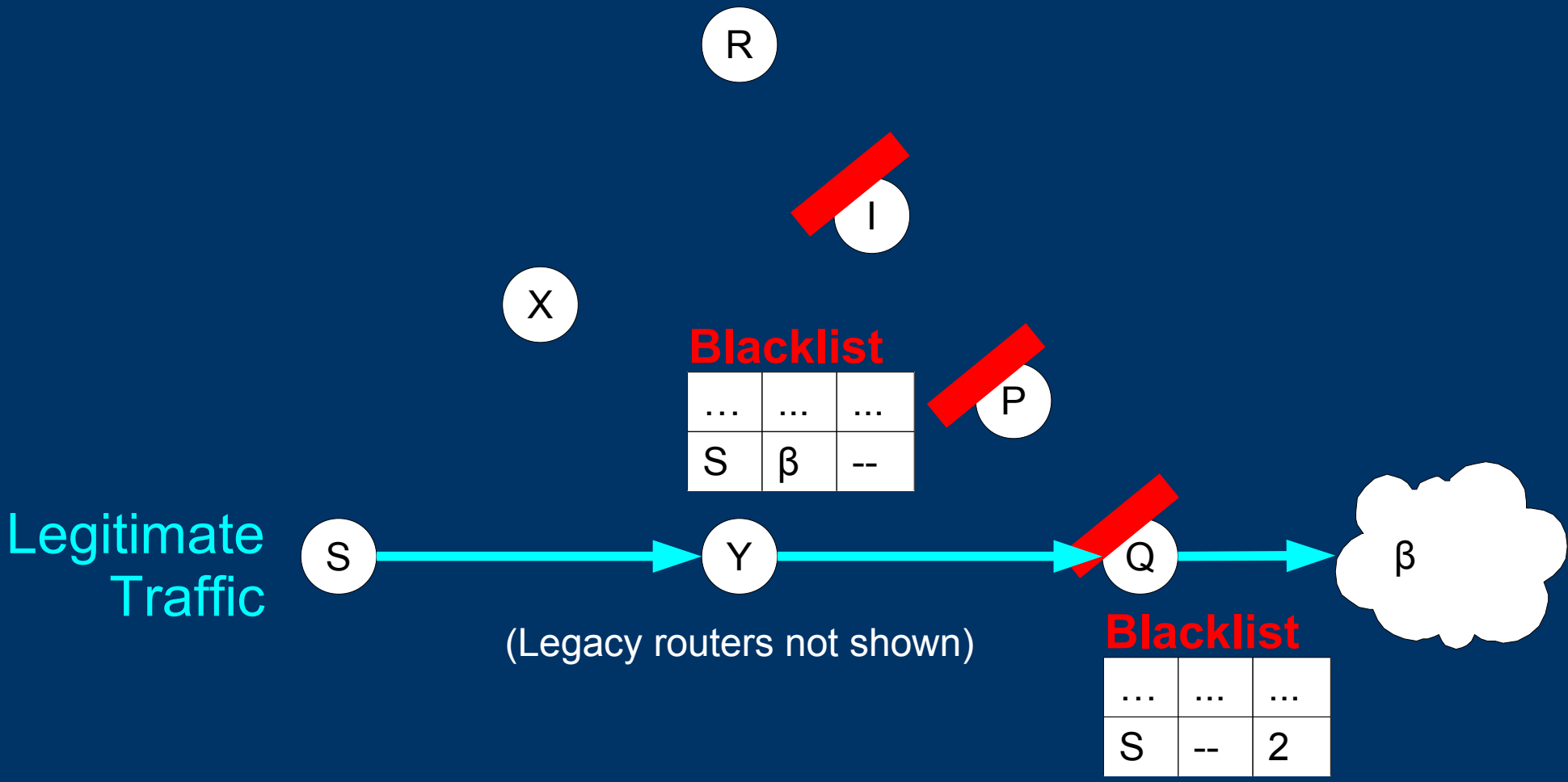
Packet-Driven Pushback



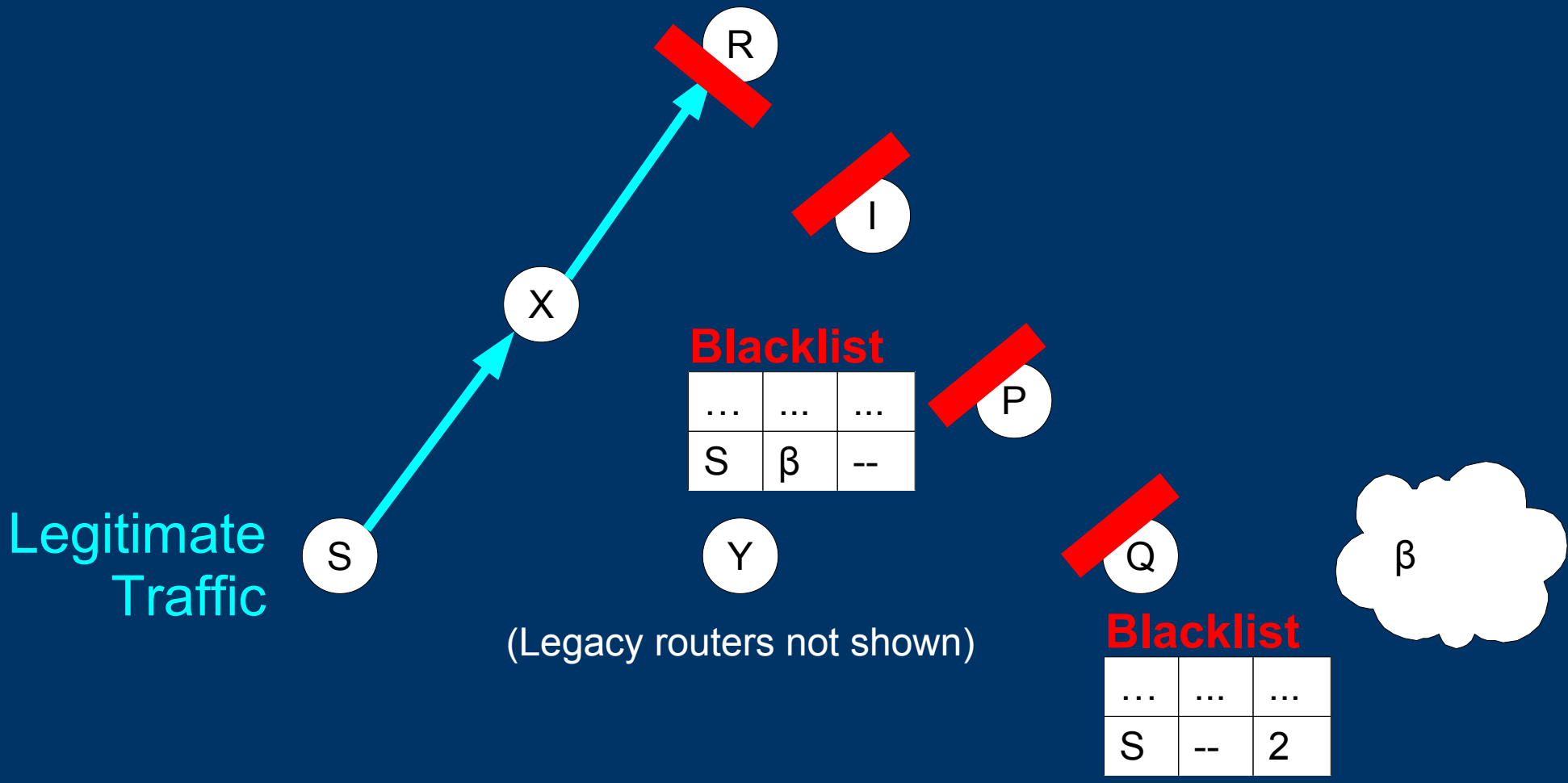
Packet-Driven Pushback



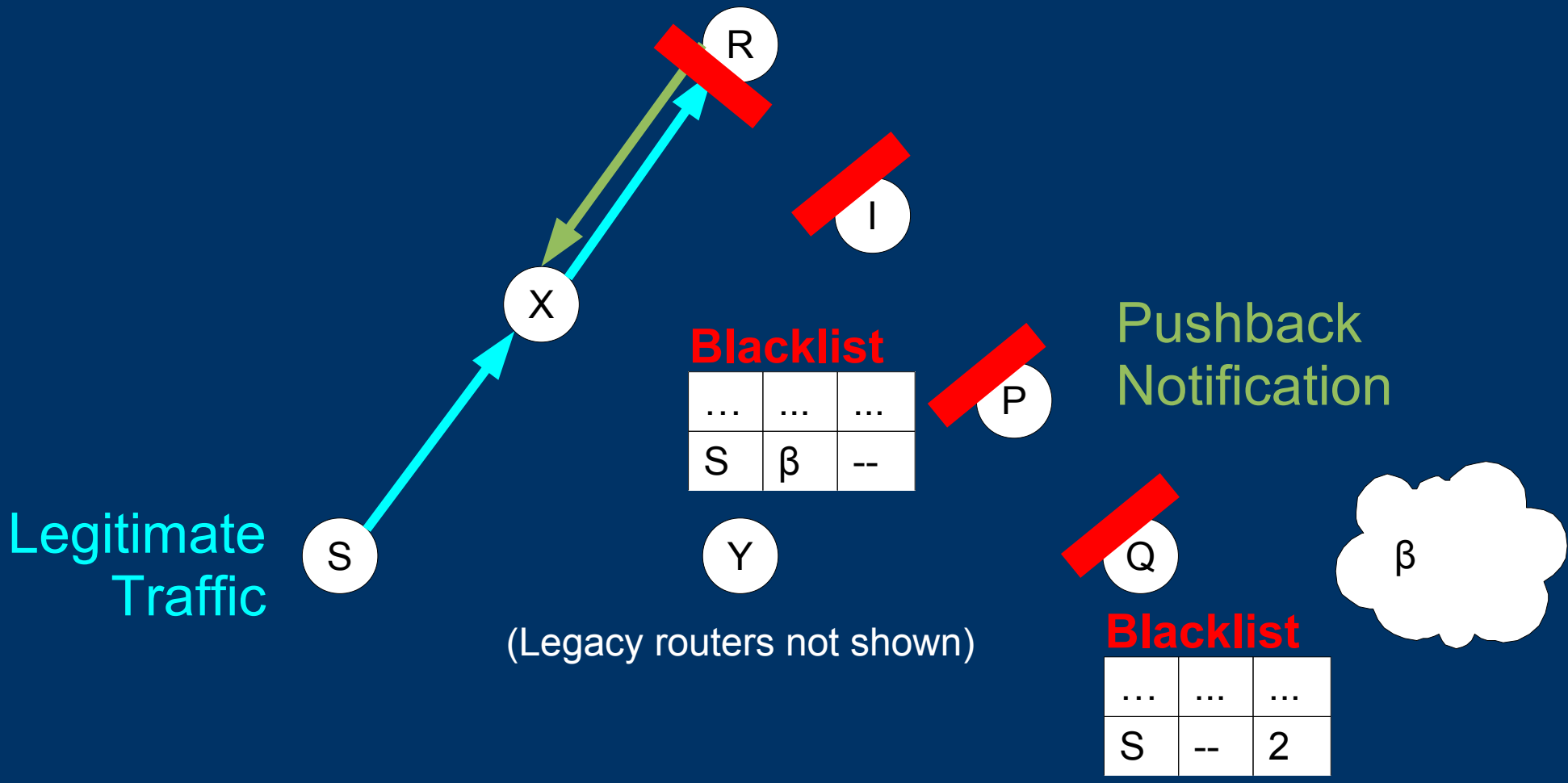
Pushback and Routing Changes



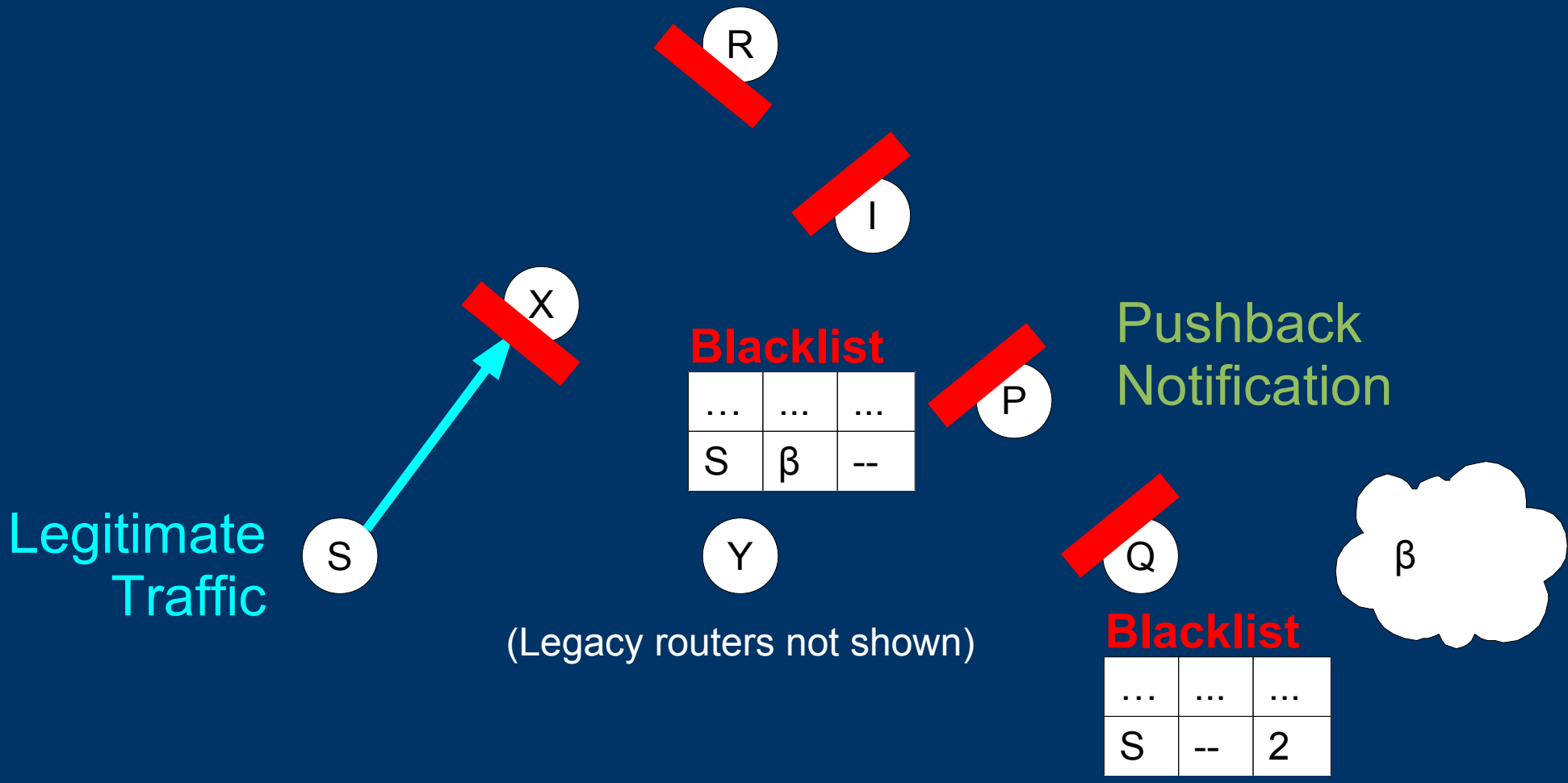
Pushback and Routing Changes



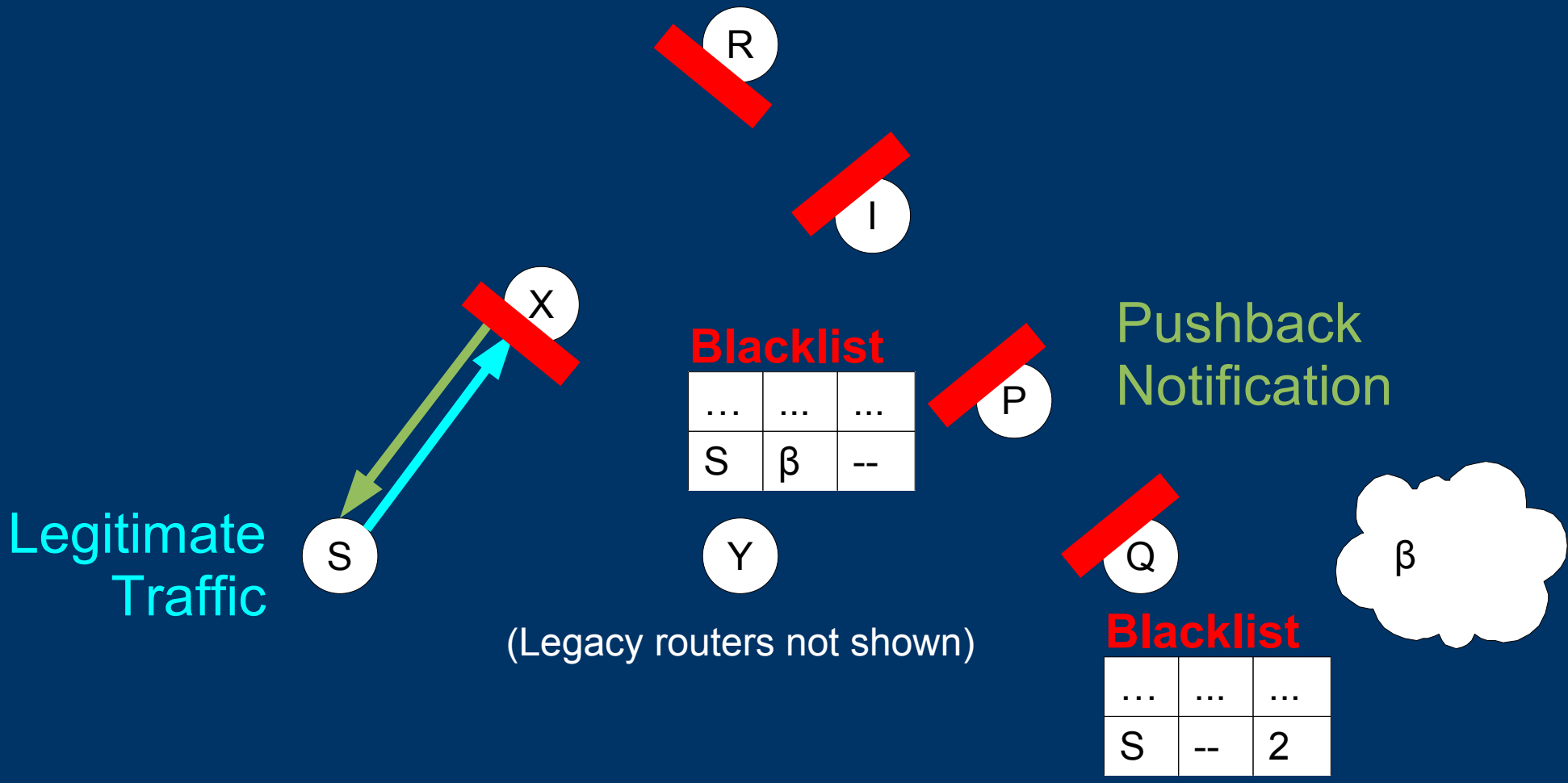
Pushback and Routing Changes



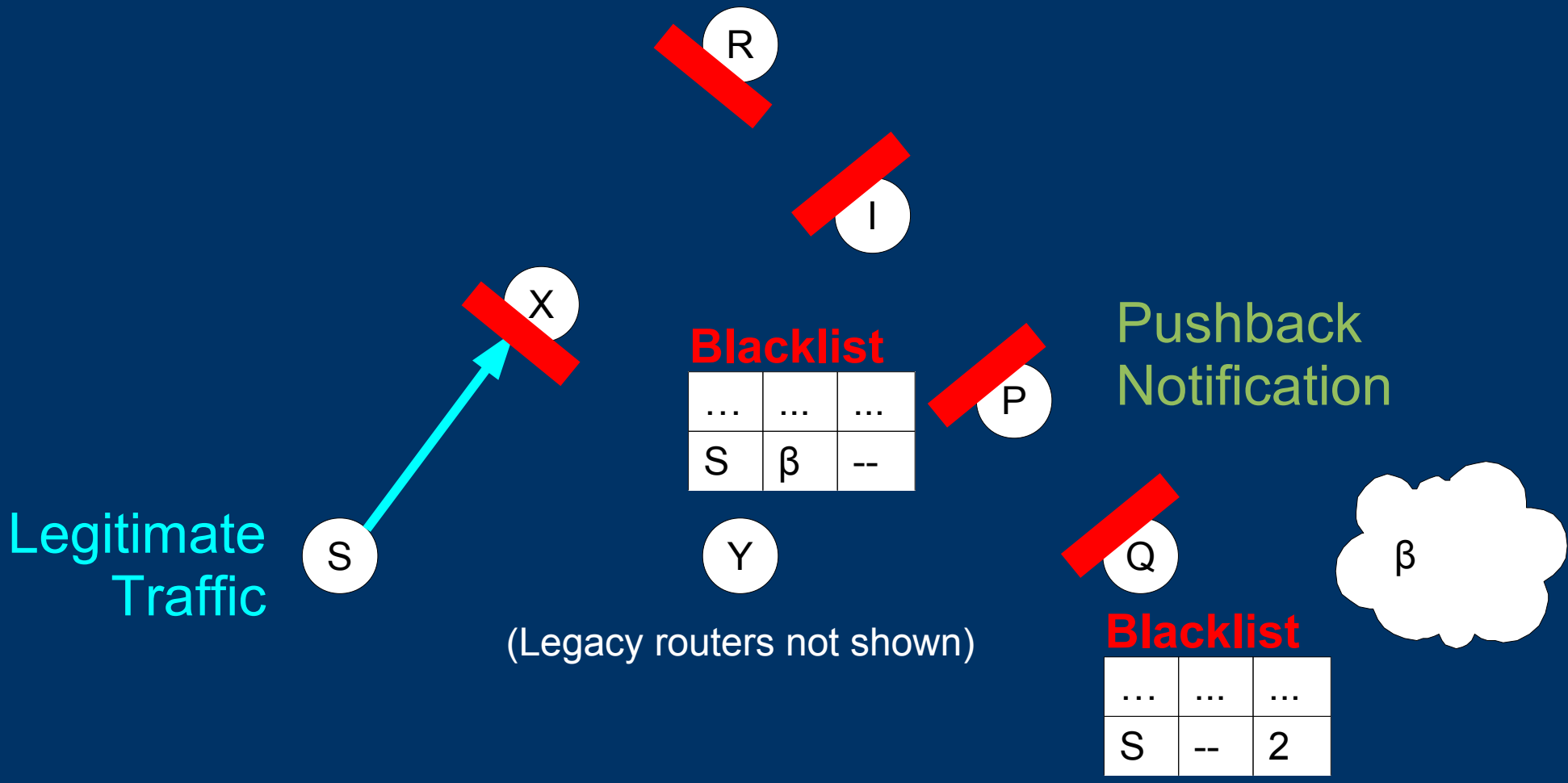
Pushback and Routing Changes



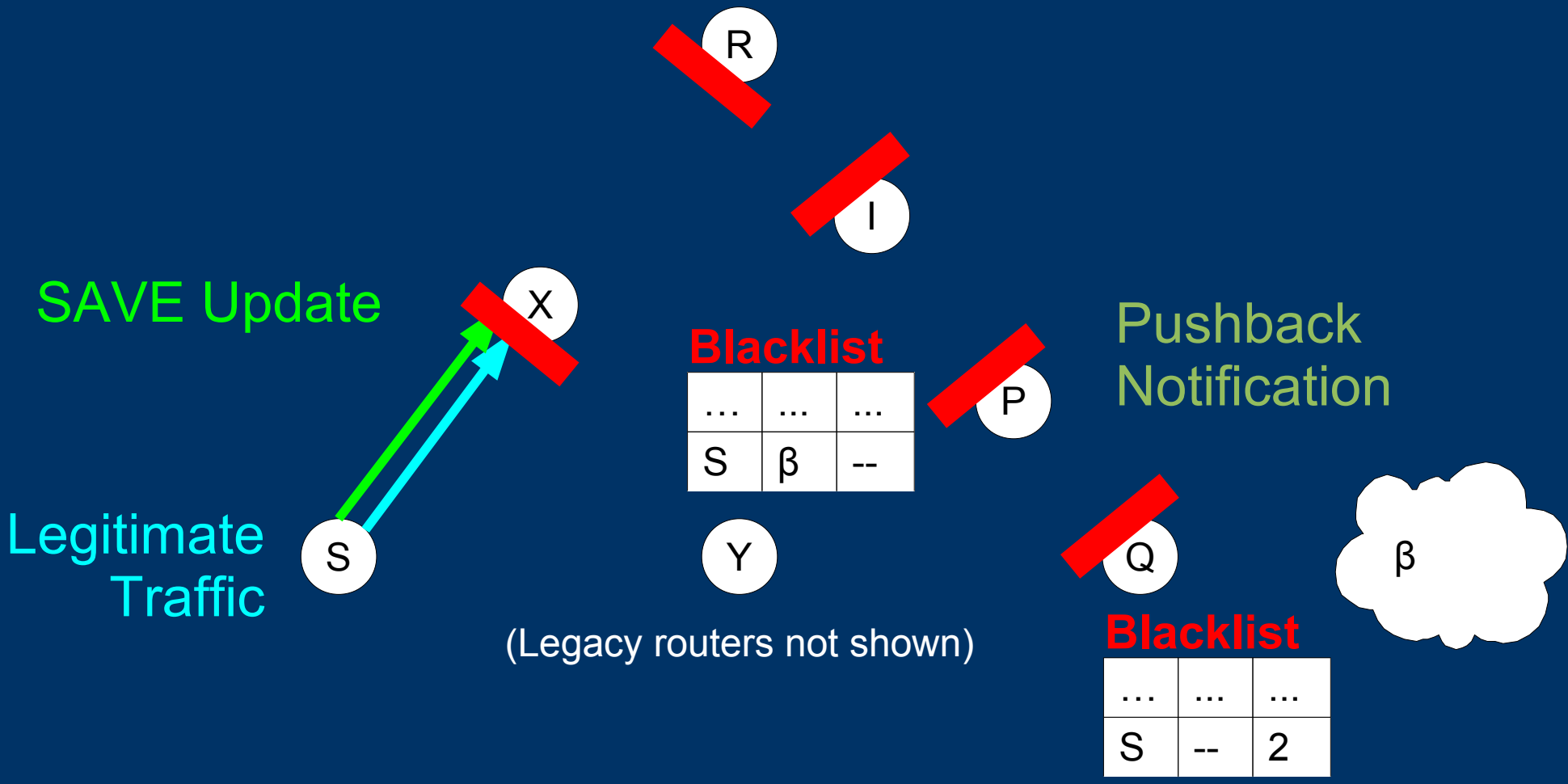
Pushback and Routing Changes



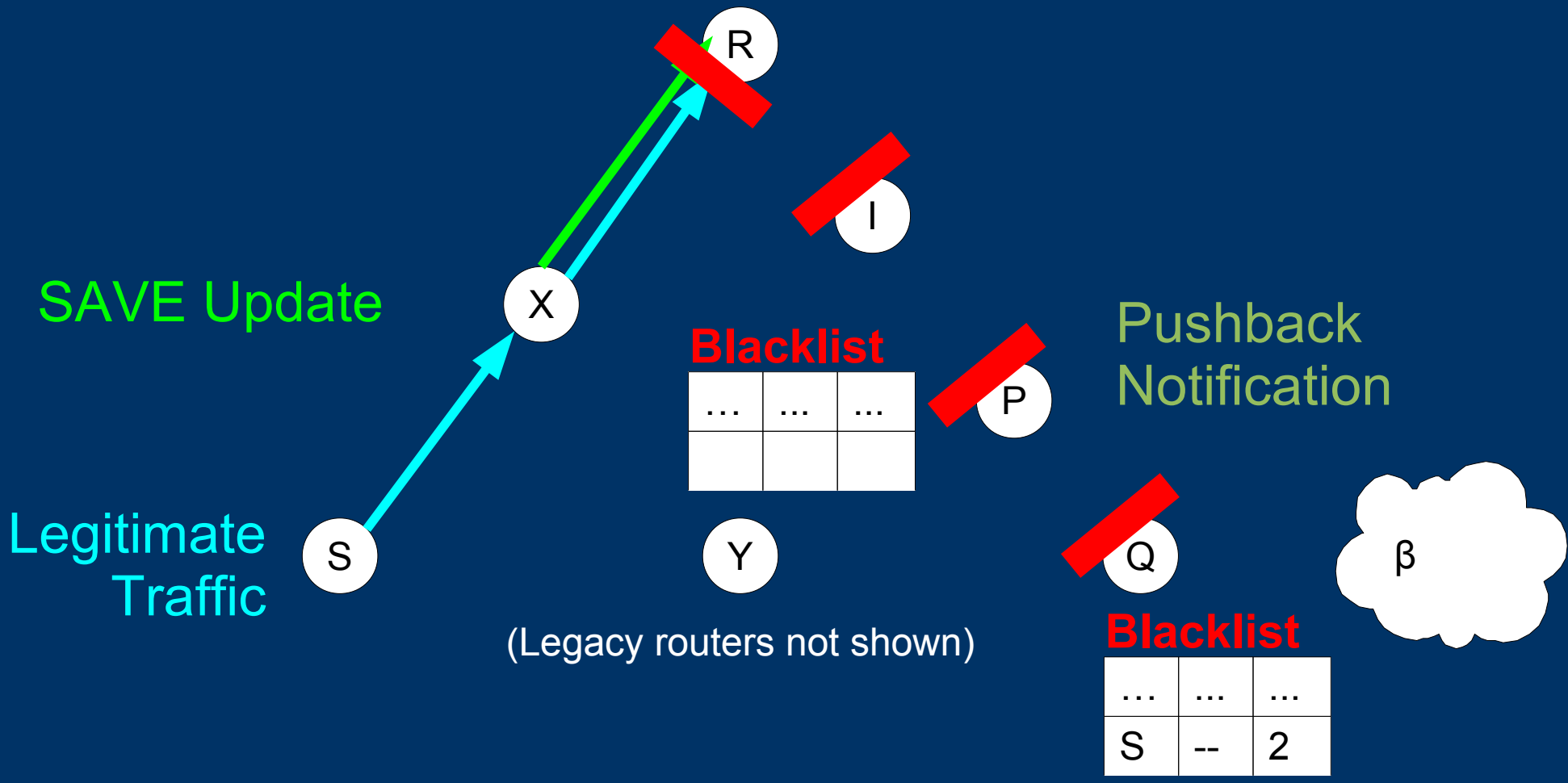
Pushback and Routing Changes



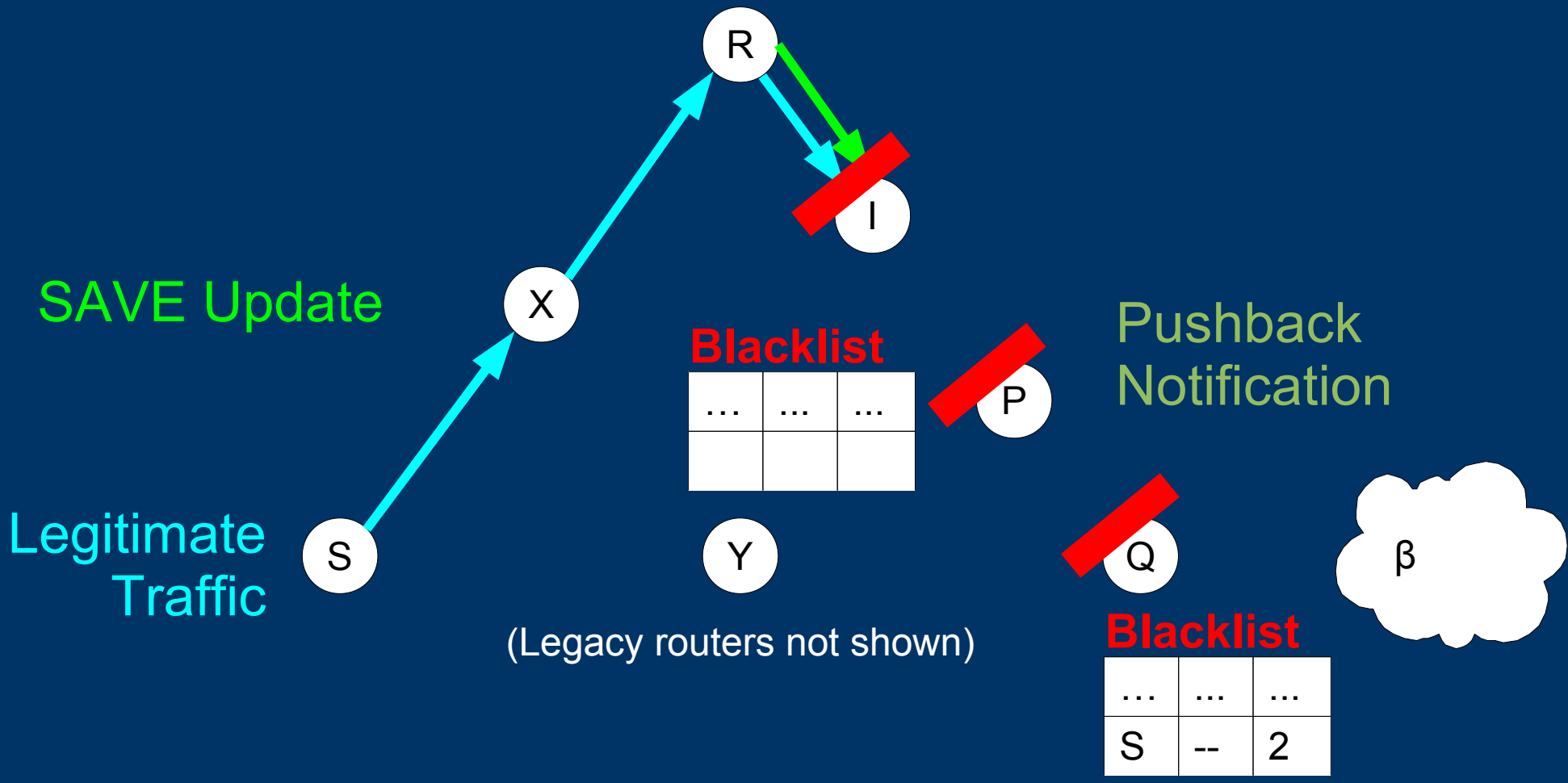
Pushback and Routing Changes



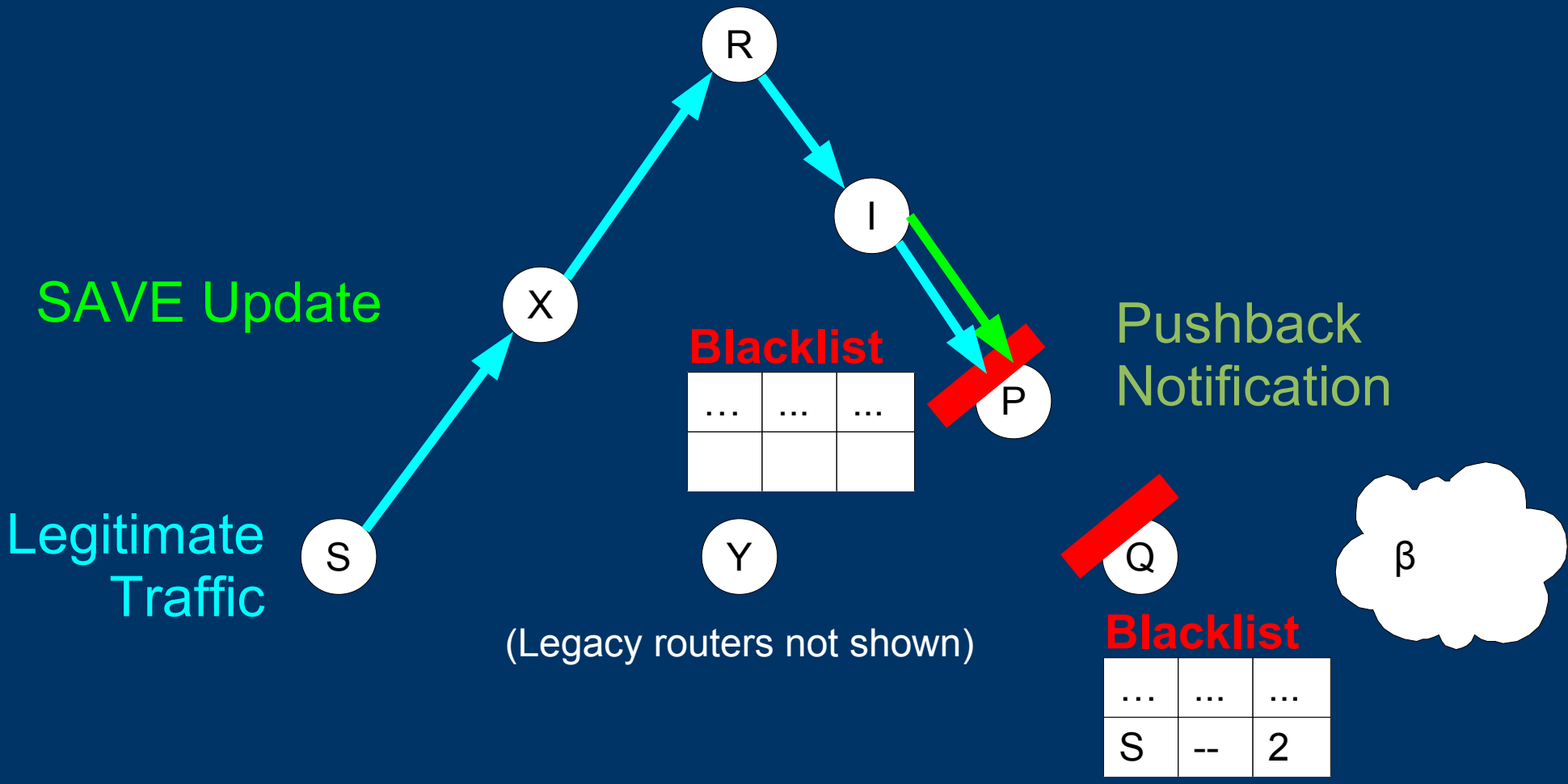
Pushback and Routing Changes



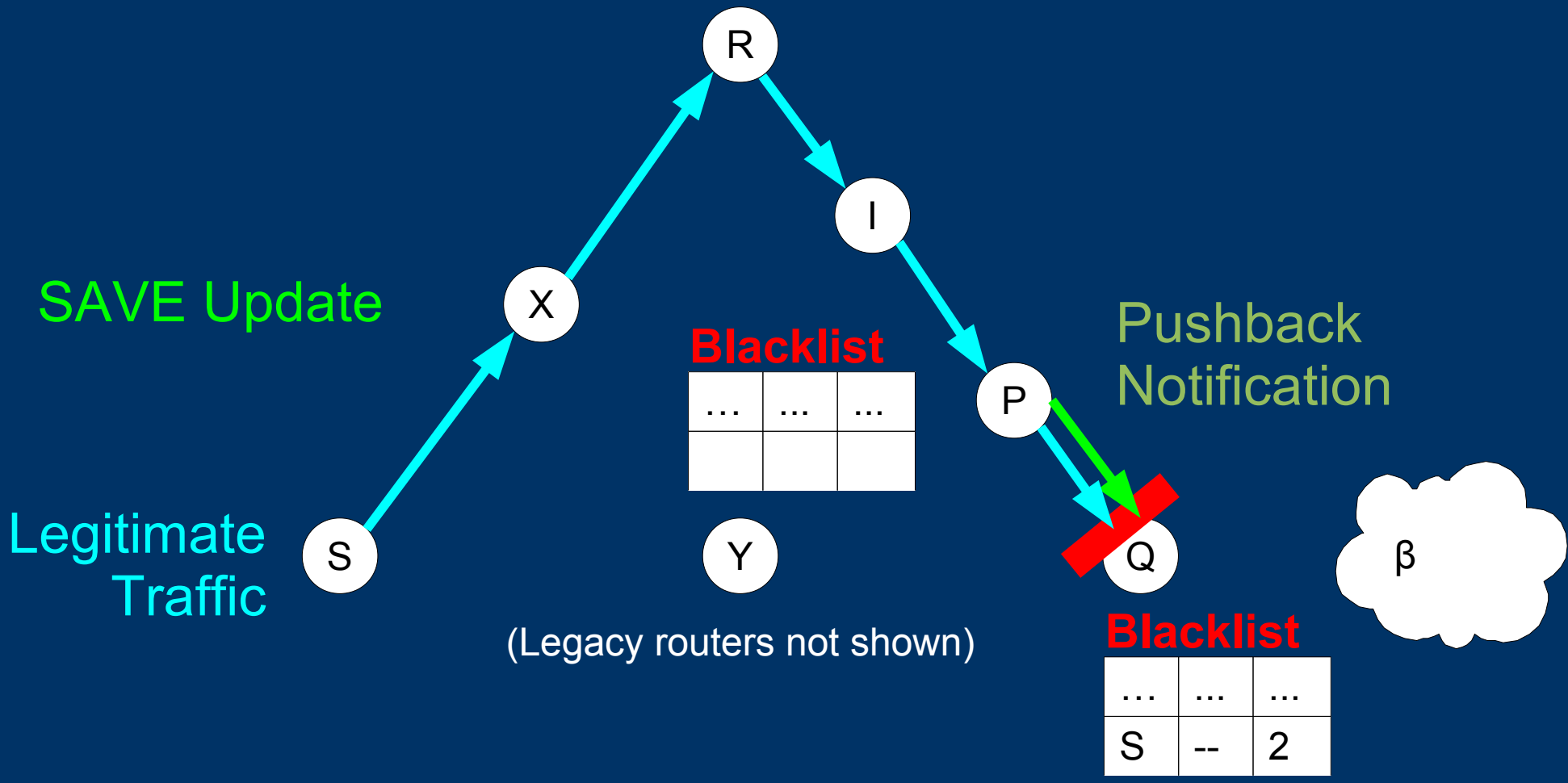
Pushback and Routing Changes



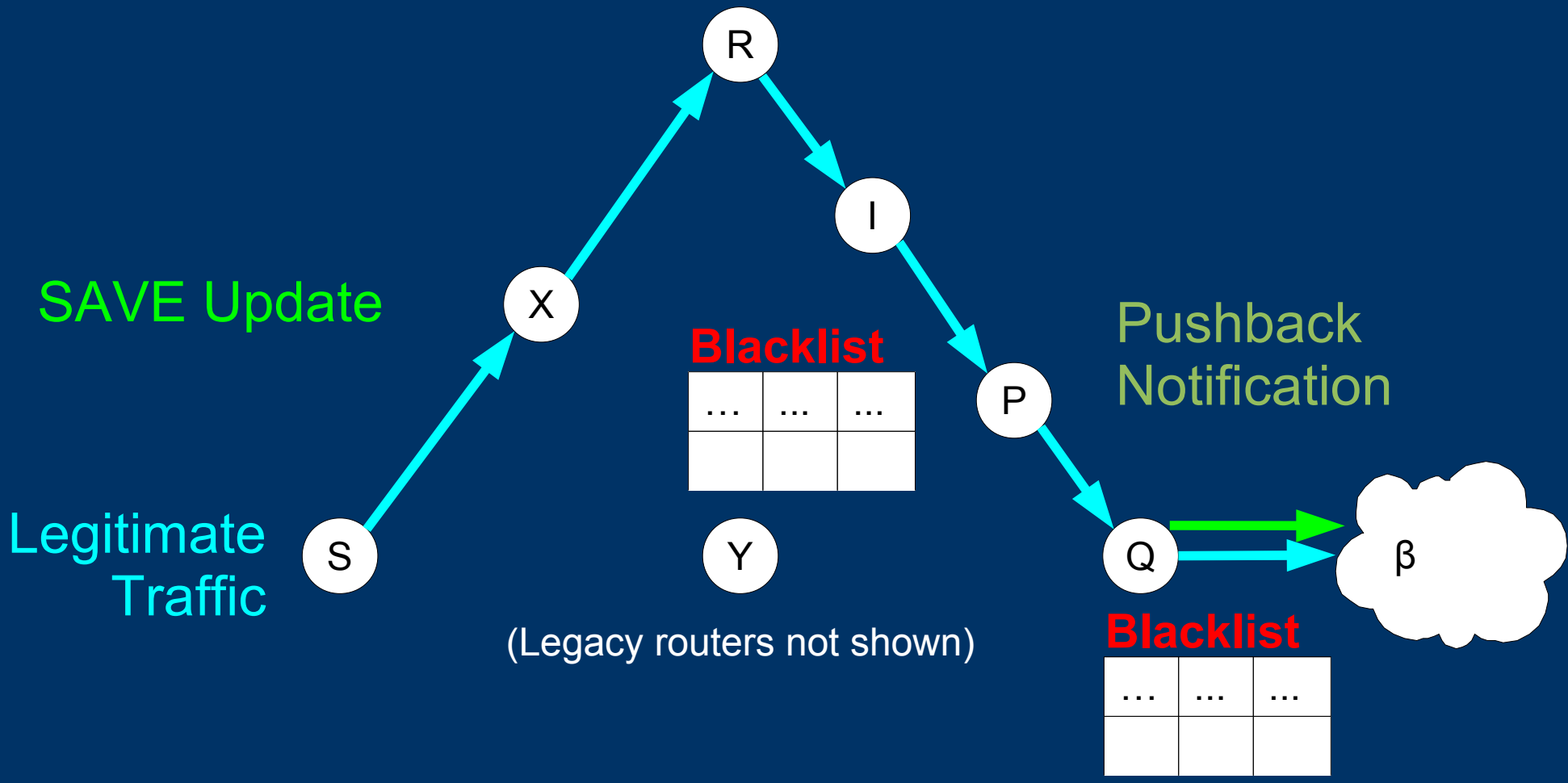
Pushback and Routing Changes



Pushback and Routing Changes



Pushback and Routing Changes



Outline

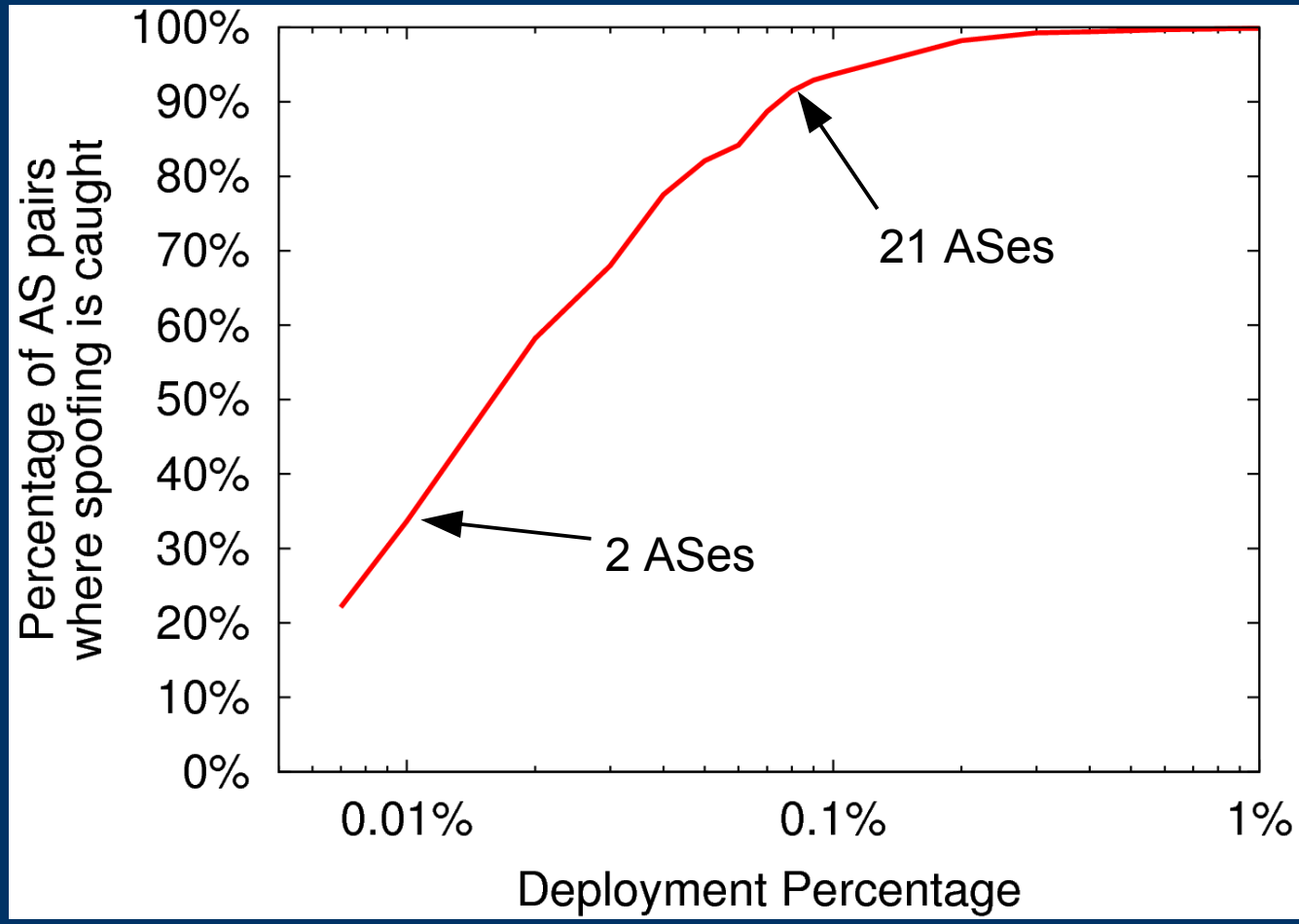
- Introduction
- Related/Existing Work
- New Mechanisms of SAVE
- Evaluation
- Conclusion

Evaluation

- Efficacy
- Overhead
  - Network traffic overhead
  - Storage overhead
  - Computational overhead
- False positives
  - Only for a very short transient period
  - Details in the paper

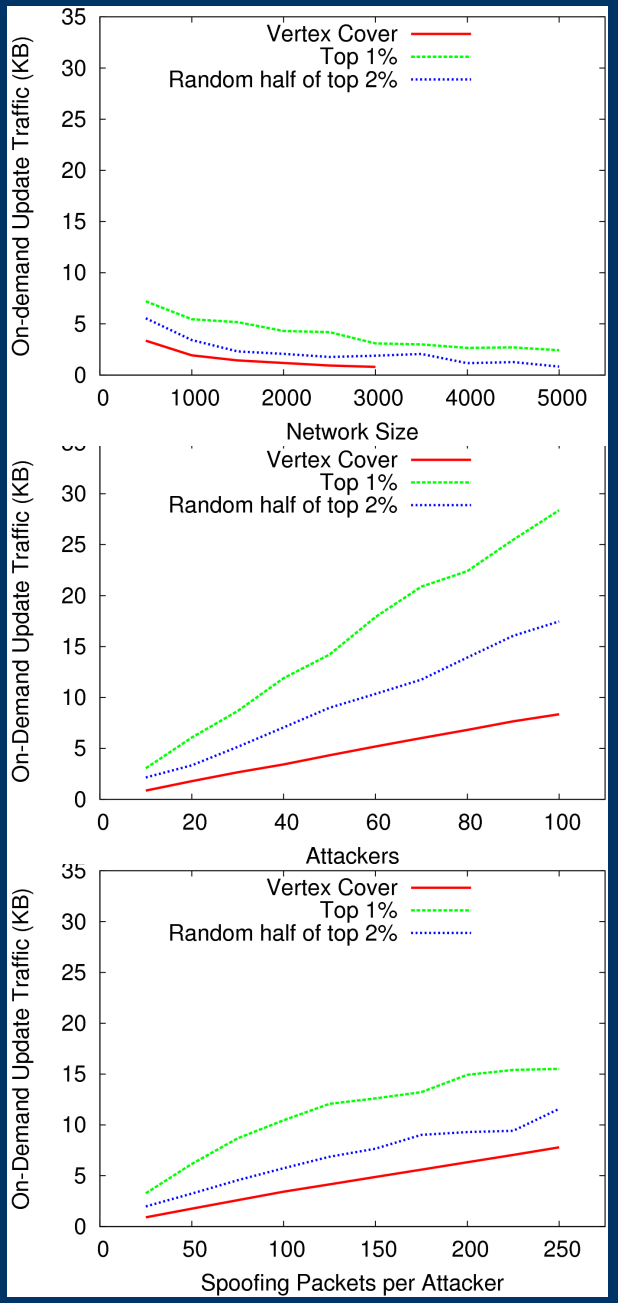
Efficacy

It does not take much to provide great protection!



Overhead

- Per-router network overhead
  - Decreases as network size increases
  - Increases as # of attackers or spoofing packets per attacker increase
- Storage overhead
  - Blacklist is the only new data structure
- Computational overhead
  - Simple table operations
- More details in paper



Conclusion

- Routers lack the information needed to identify spoofing packets
- SAVE – *with newly proposed mechanisms* – solves this deficiency
- Even if only a very small percentage (<0.1%) of ASes deploy SAVE, the Internet will be a better, safer place!

Questions?

- Contact Toby Ehrenkranz for further information
  tehrenkr@cs.uoregon.edu
- Or visit our web site
  http://netsec.cs.uoregon.edu/research/idsave.shtml