Ascertaining the Reality of Network Neutrality Violation in Backbone ISPs

Z. Morley Mao

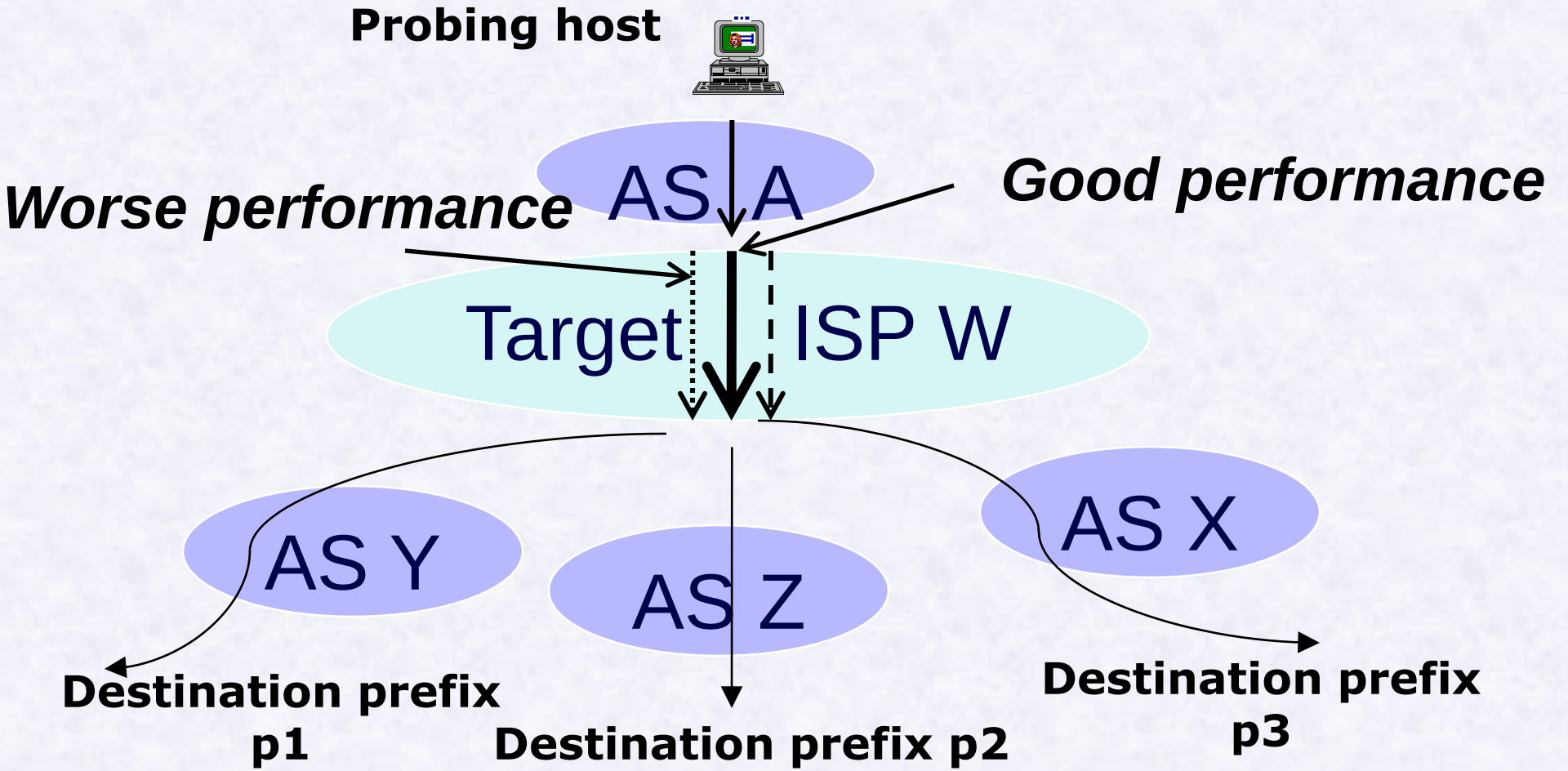
Joint work with Ying Zhang and Ming Zhang

Network neutrality debate

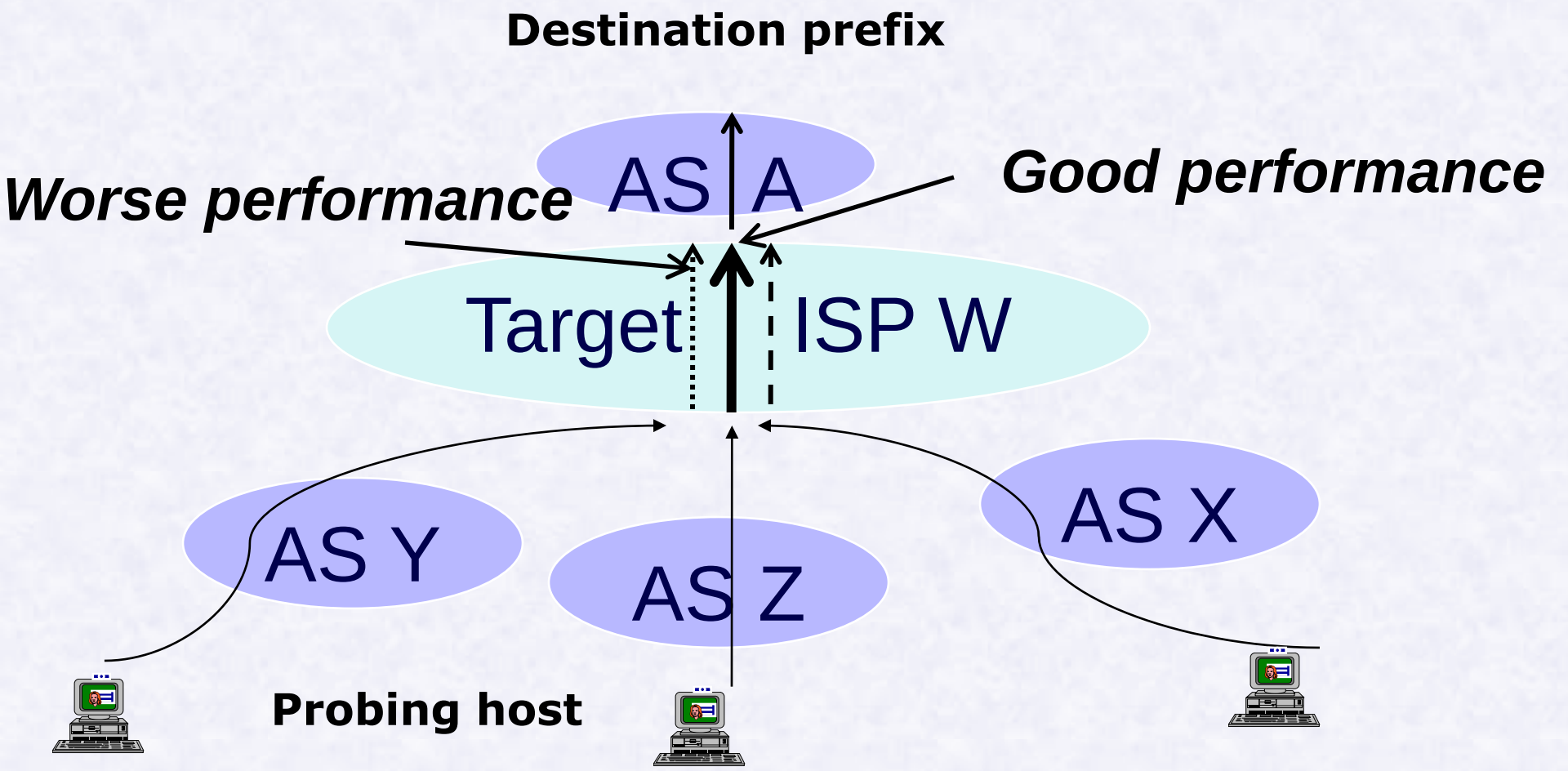
Definition of network neutrality

- ISPs should be neutral to any traffic
  - No different treatment to packets of different types
- Violation of network neutrality exists
  - Traffic properties are used to perform discrimination
    - Application types, traffic source network, destination network, previous/next hop network
    - A well-known example: Comcast slows down Peer-to-Peer traffic

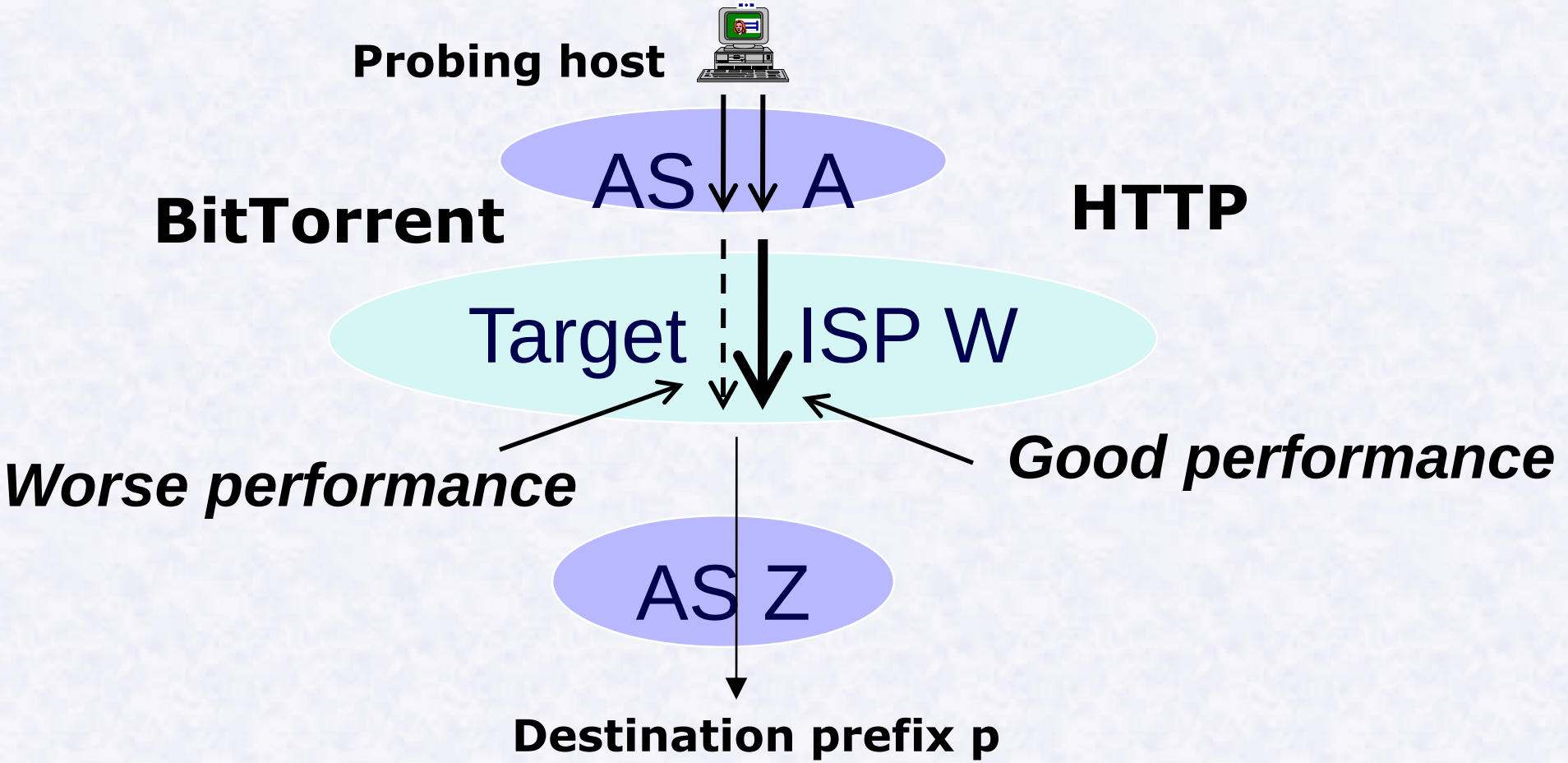
Discrimination type I: Next-hop AS based discrimination



Discrimination type II: Previous-hop AS based discrimination



Discrimination type III: Application based discrimination

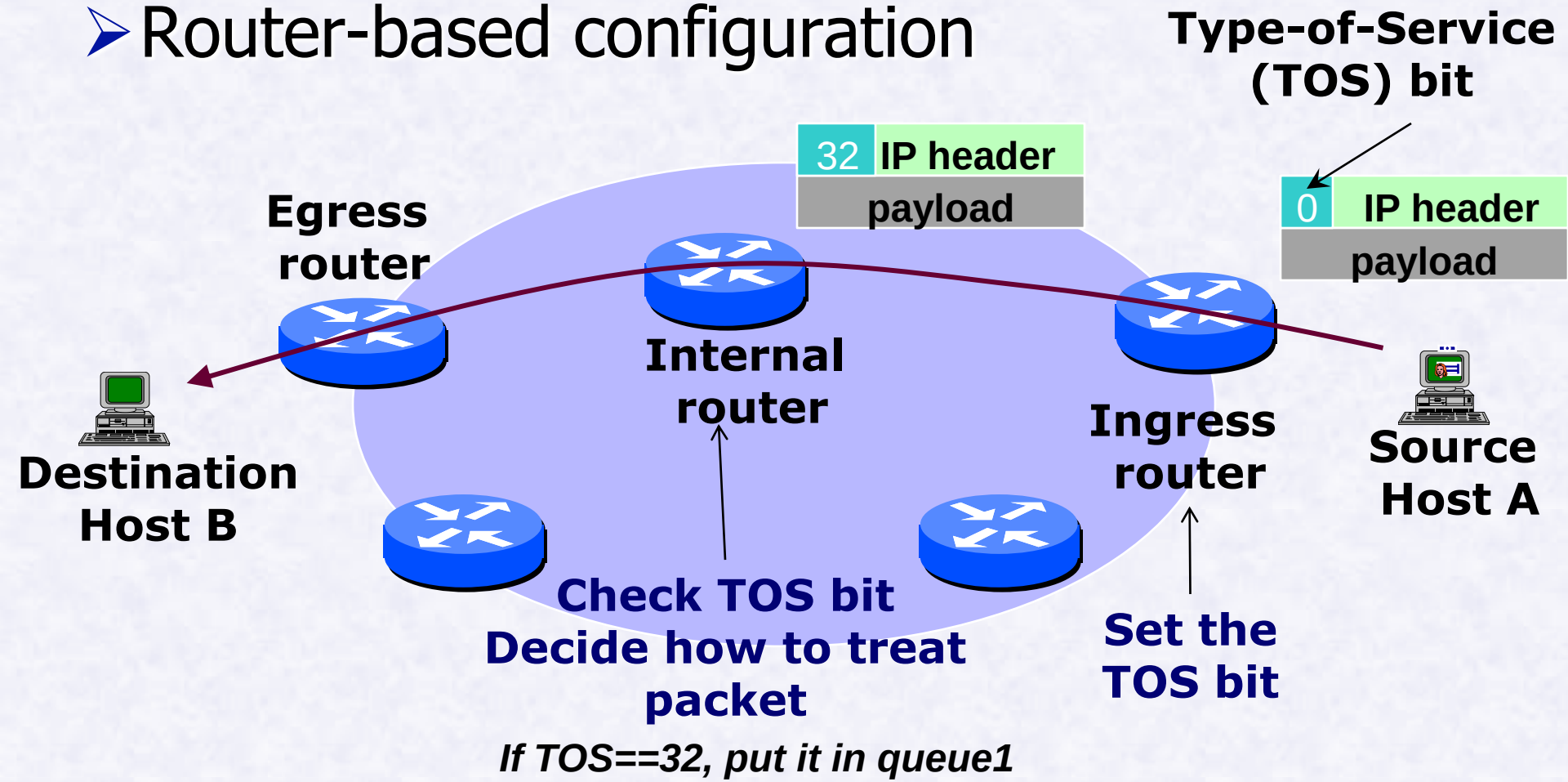


Information used for discrimination

- IP/TCP/UDP packet header fields
  - Src/dst port numbers, protocol types
- Application payload
  - Application protocol header, data content
- Network policies
  - Previous-hop, next-hop AS, source/destination
- Traffic behavior
  - Flow rate, packet size, flow duration
- Available resources
  - Router state (memory, load)

How to implement discrimination?

- Router-based configuration

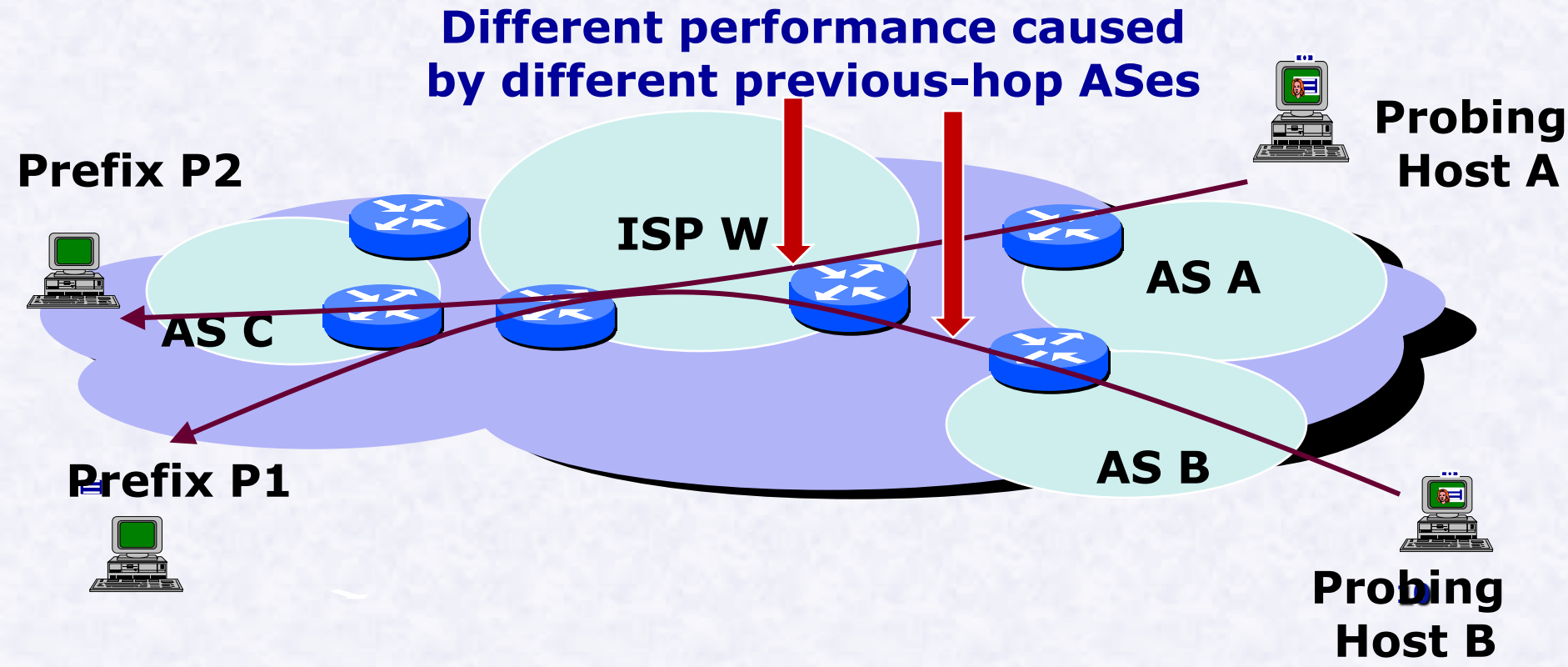


Other implementation methods

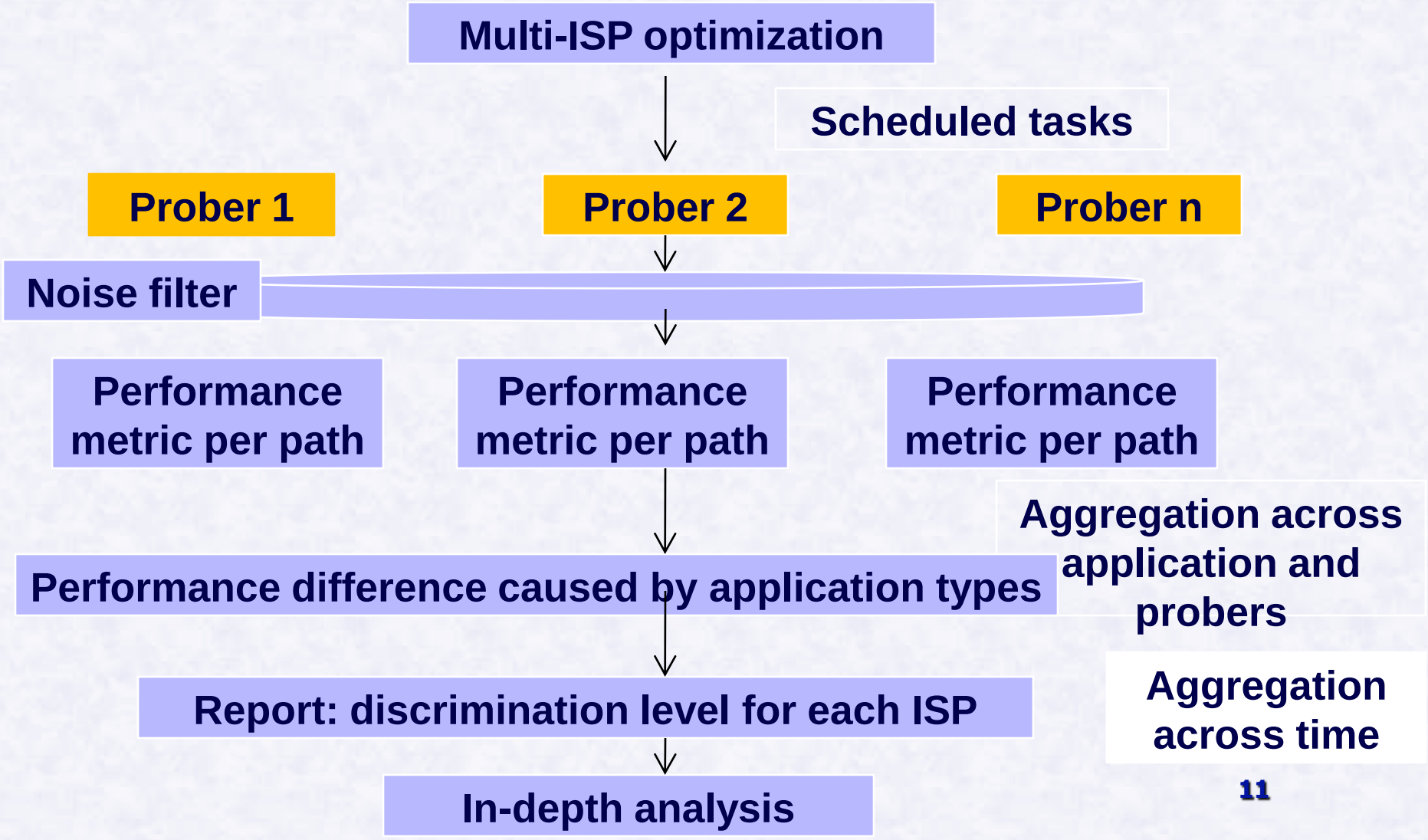
- Deep packet inspection (DPI) support
  - Packet classification on line speed
    - 10 to even 100 Gbps
  - Several commercial products exist
    - E.g. Arbor Ellacoya e100, CPacket Networks' Complete Packet Inspection on a Chip

Our approach: Neutrality Violation Lens (NVLens)

- Develop a distributed measurement system to monitor packet loss and delay inside ISPs
  - To detect potential violations



System architecture



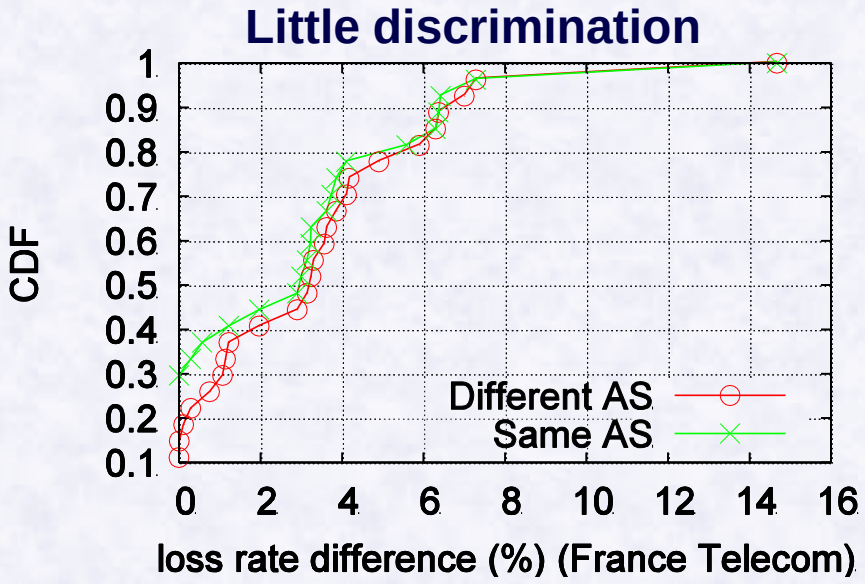
Multi-ISP probing optimization

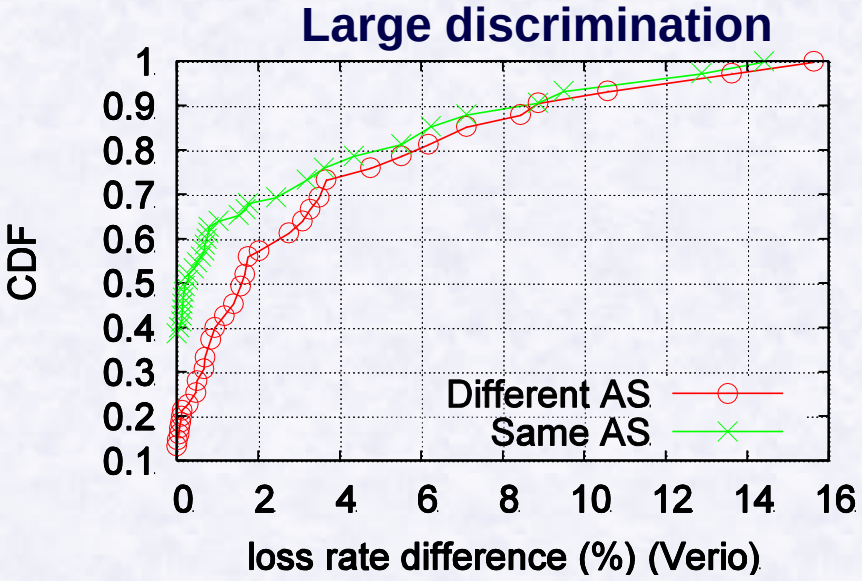
- Path selection problem
  - Each ISP's internal path (ingress-egress pair) is traversed at least n times
    - Monitor path performance
  - Each three-tuple path (src, ingress, egress) is traversed at least n times to different destinations
    - To detect next-hop AS based discrimination
  - Each three-tuple path (ingress, egress, dst) is traversed at least n times by different probers
    - To detect previous-hop AS based discrimination
  - A prober conducts fewer than m probes
    - To ensure the load on each prober is within the limit

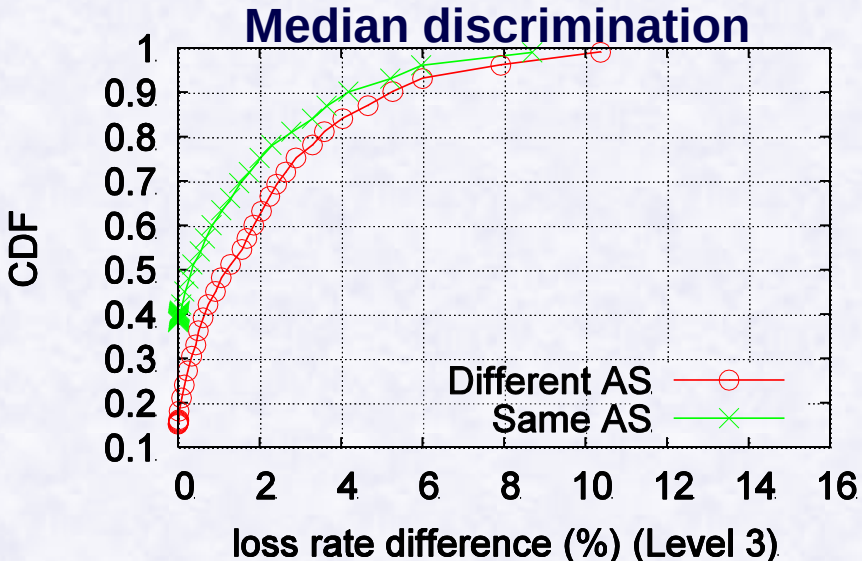
Data collection

- Implemented NVLens in 750 PlanetLab nodes covering about 300 distinct sites
- Collected data for 24 days covering 19 ISPs

Discrimination based on the next hop AS



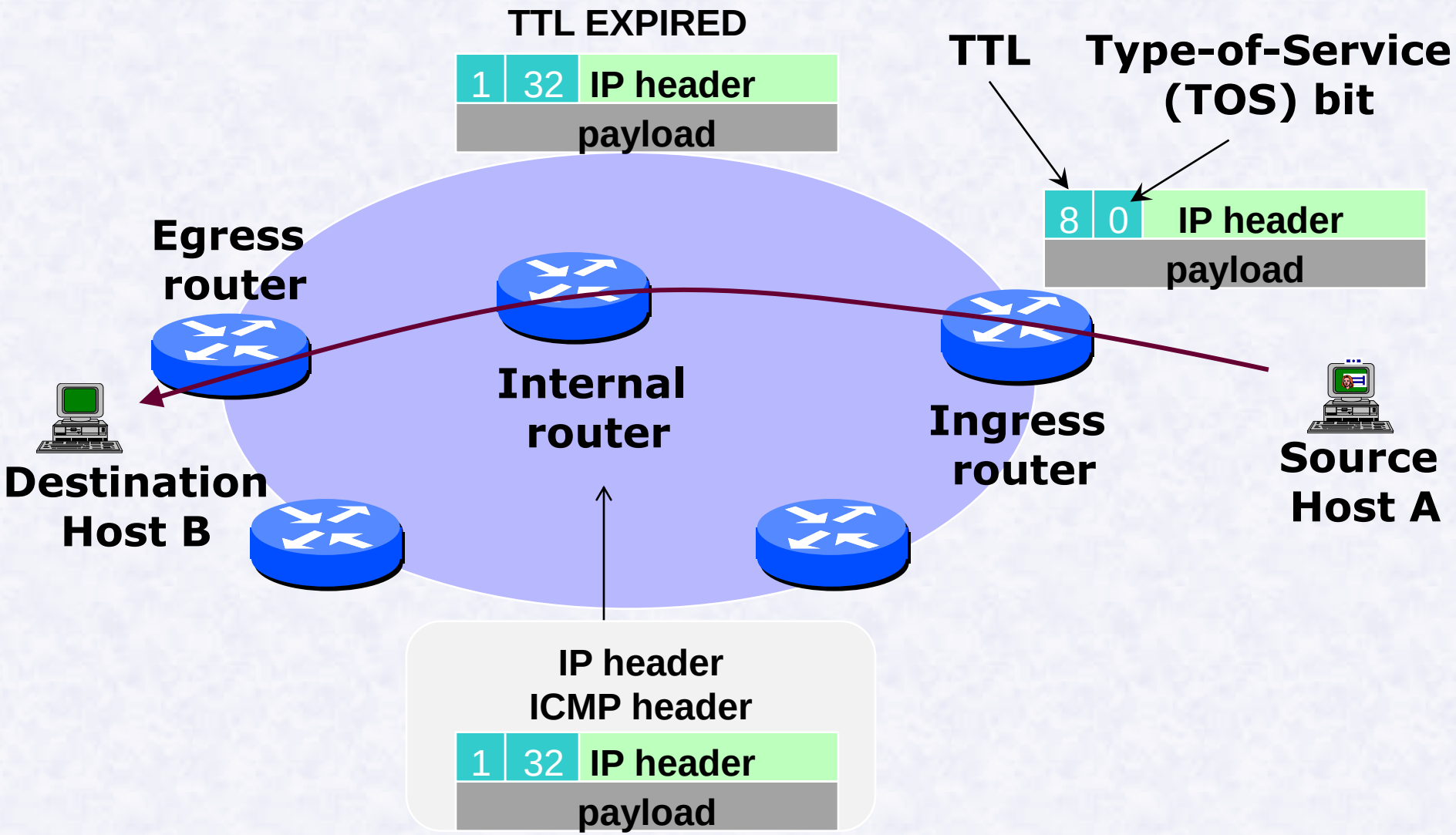




Discrimination inference

- Statistical test
  - Goal: to test whether there is any difference between two sets of data samples
    - No assumption on their distribution properties
    - Applying Wilcoxon test and permutation tests

Validation using ToS bits



Detected discrimination

Discriminated path pairs in absolute number, percentage values

AS name	Application				Previous hop	Next-hop	Same AS path
	BitTorrent	UDP	Skype	Game	PoP-PoP-NextAS	PrevAS-PoP-PoP	PrevAS-PoP-PoP-NextAS
UUNet	20, 0.9%	90,3.6%	0	0	**633, 3.6%**	38, 0.2%	92, 0.5%
Level 3	0	1,0.05%	0	0	**746, 1%**	7, 0.01%	9,0.1%
Tiscali	**221, 8%**	0	17, 1%	0	184, 3%	6, 0.1%	0
AT&T	0	2, 0.1%	0	0	330,1%	0	0

Correlation with TOS bits

AS name	% TOS-marked path pairs with discrimination	% discrimination path pairs matching TOS rules
AT&T	**90%**	**77%**
UUNet	71%	45%
Sprint	16%	11%
AOL	**80%**	**76%**
Verio	**95%**	**89%**
Level3	**92%**	**80%**
Global Crossing	81%	70%
Deutsche Telekom	0	0

In-depth analysis

- Understanding what information is used for discrimination
  - Using different port
  - Zeroing out the payload
  - No control packets

In-depth experiment results

Number of discriminated path pairs identified

	Full	Diff port	Empty payload	No control
# path pairs	221	103	198	221

Conclusion and Discussion

- NVLens can identify discrimination policies
  - Location of enforcement
  - Time-of-day effect
  - Fields used to construct discrimination policy
- It can help end-systems to make more informed selection of routes and ISPs
- It is not trivial for the ISPs to evade detection

Thank you.

- Questions?