

Hierarchical Policies for Software Defined Networks

Andrew Ferguson, Arjun Guha, Chen Liang,
Rodrigo Fonseca, and Shriram Krishnamurthi



BROWN

Participatory Networking



NETFLIX

89%

Buffering

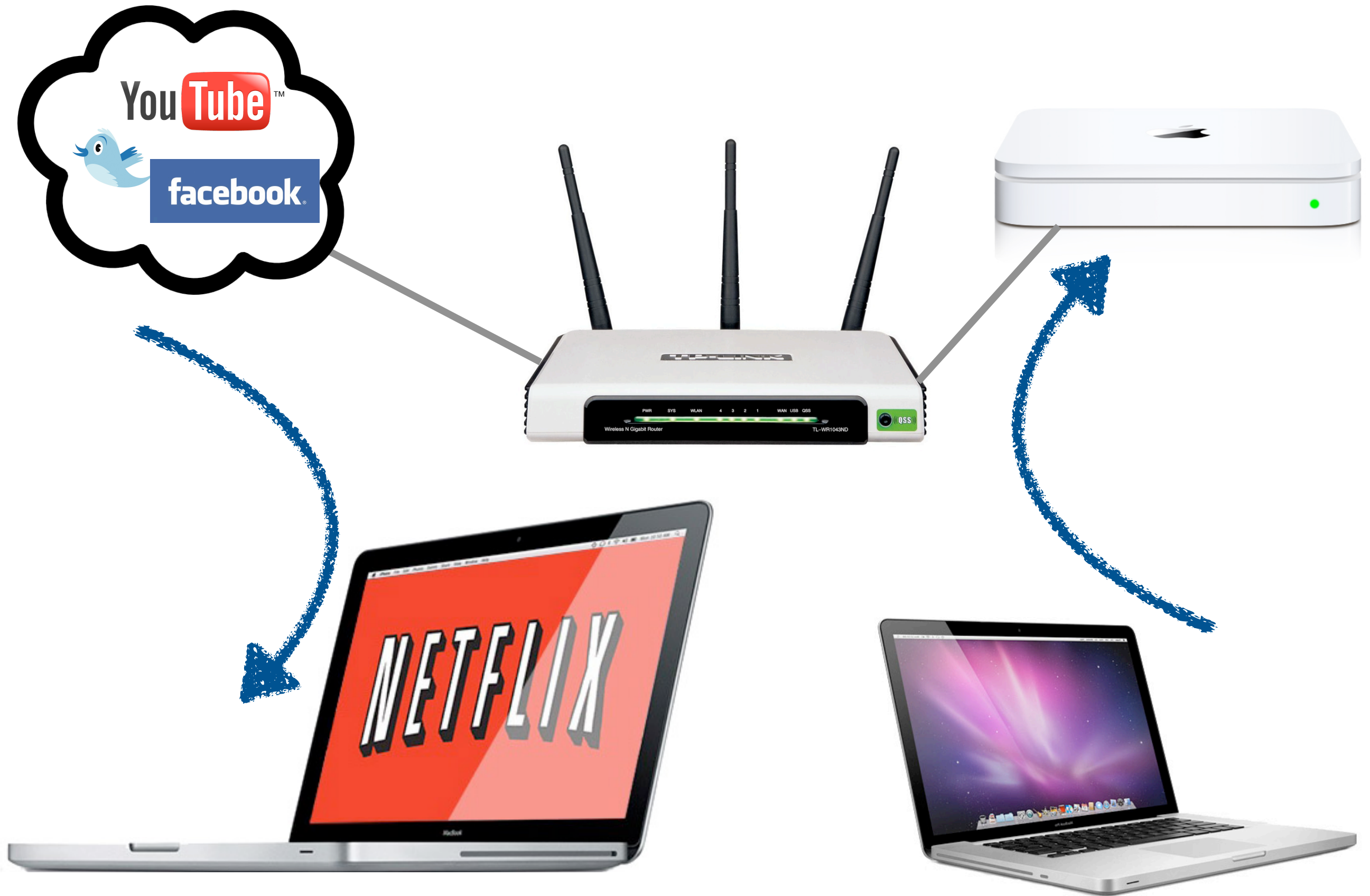


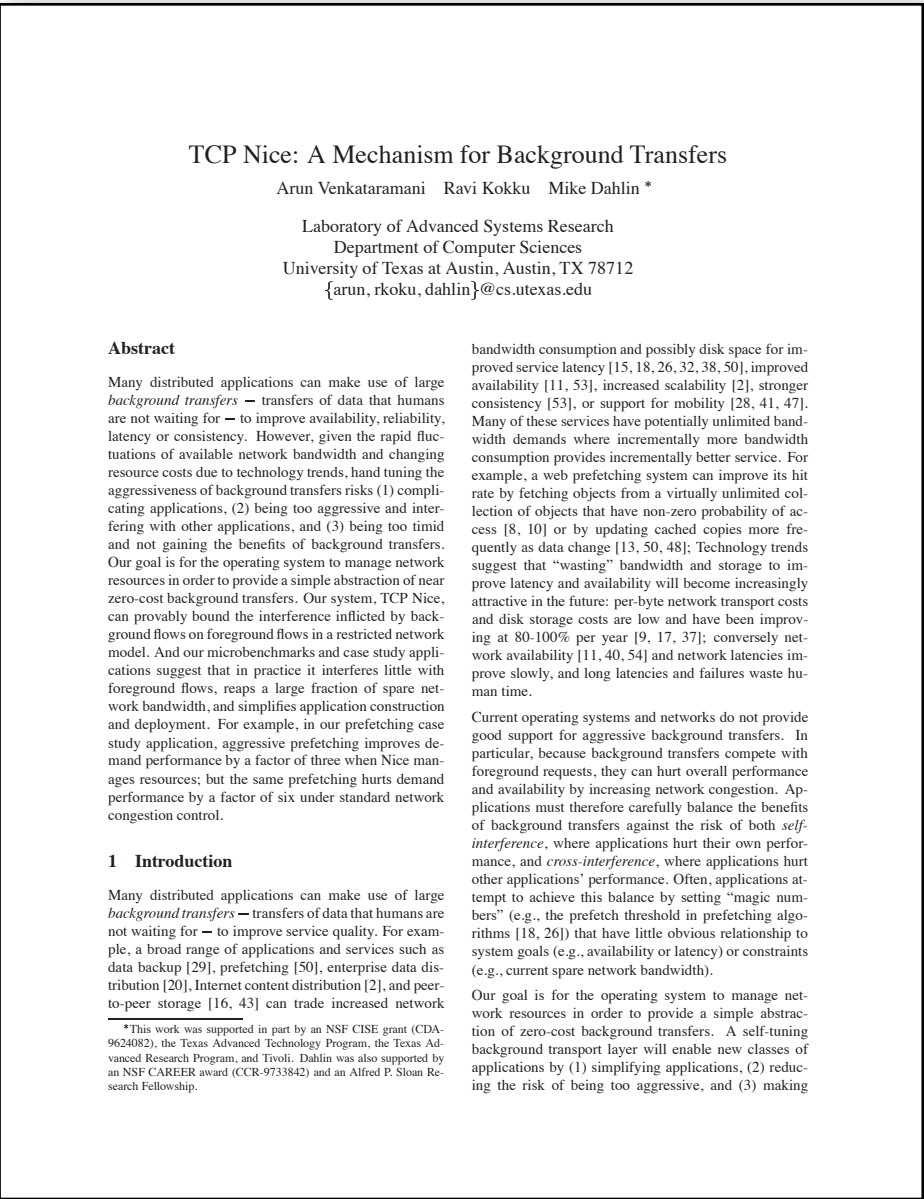
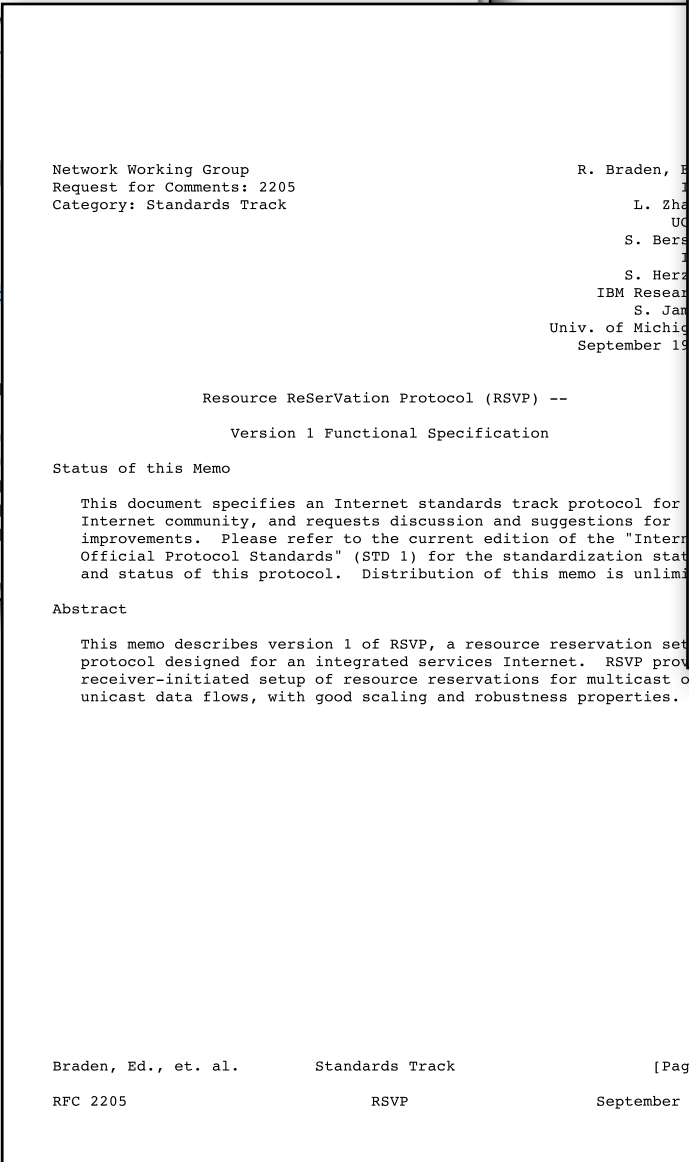
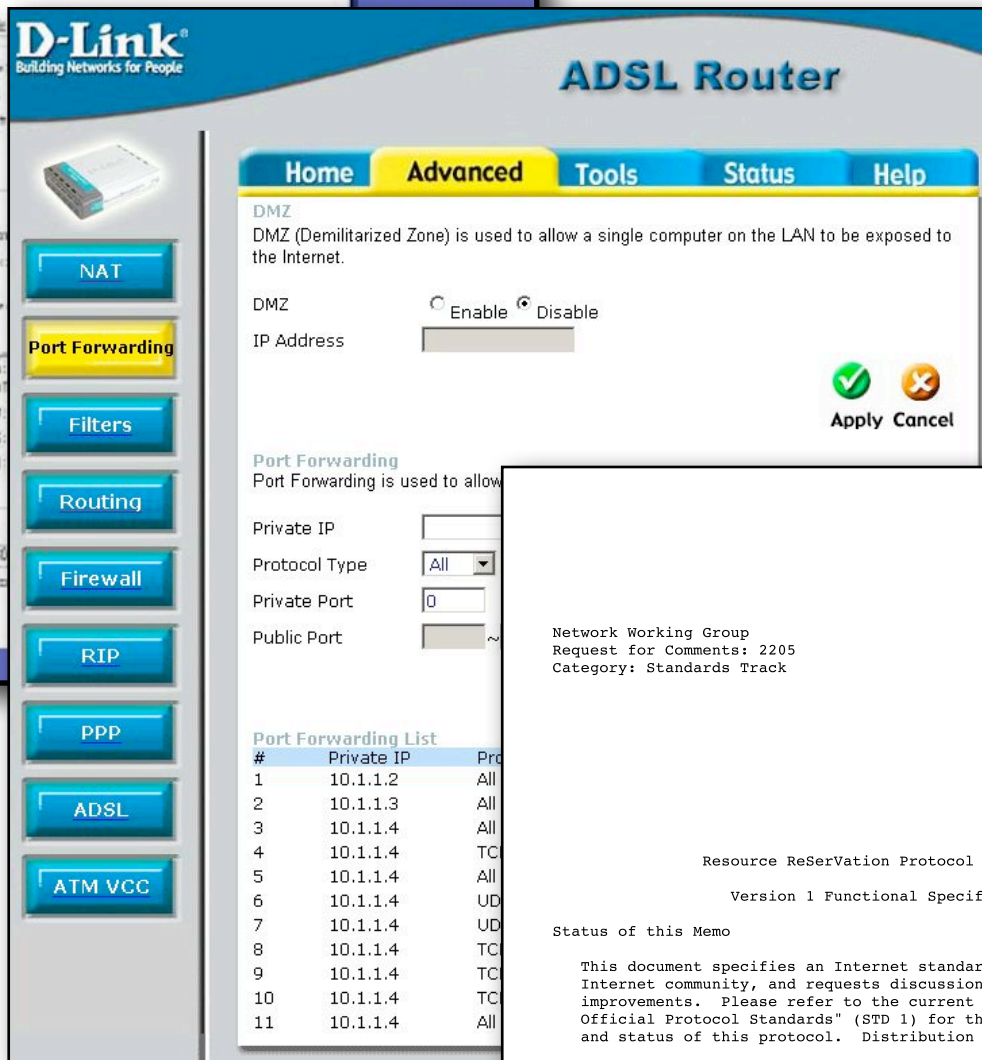
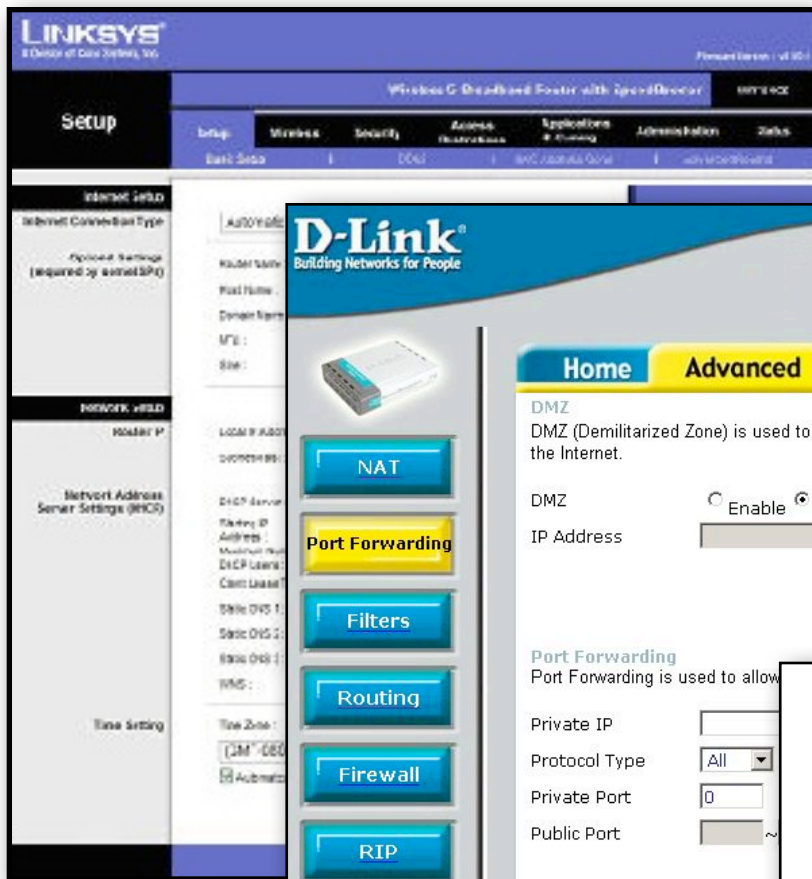
Full Screen

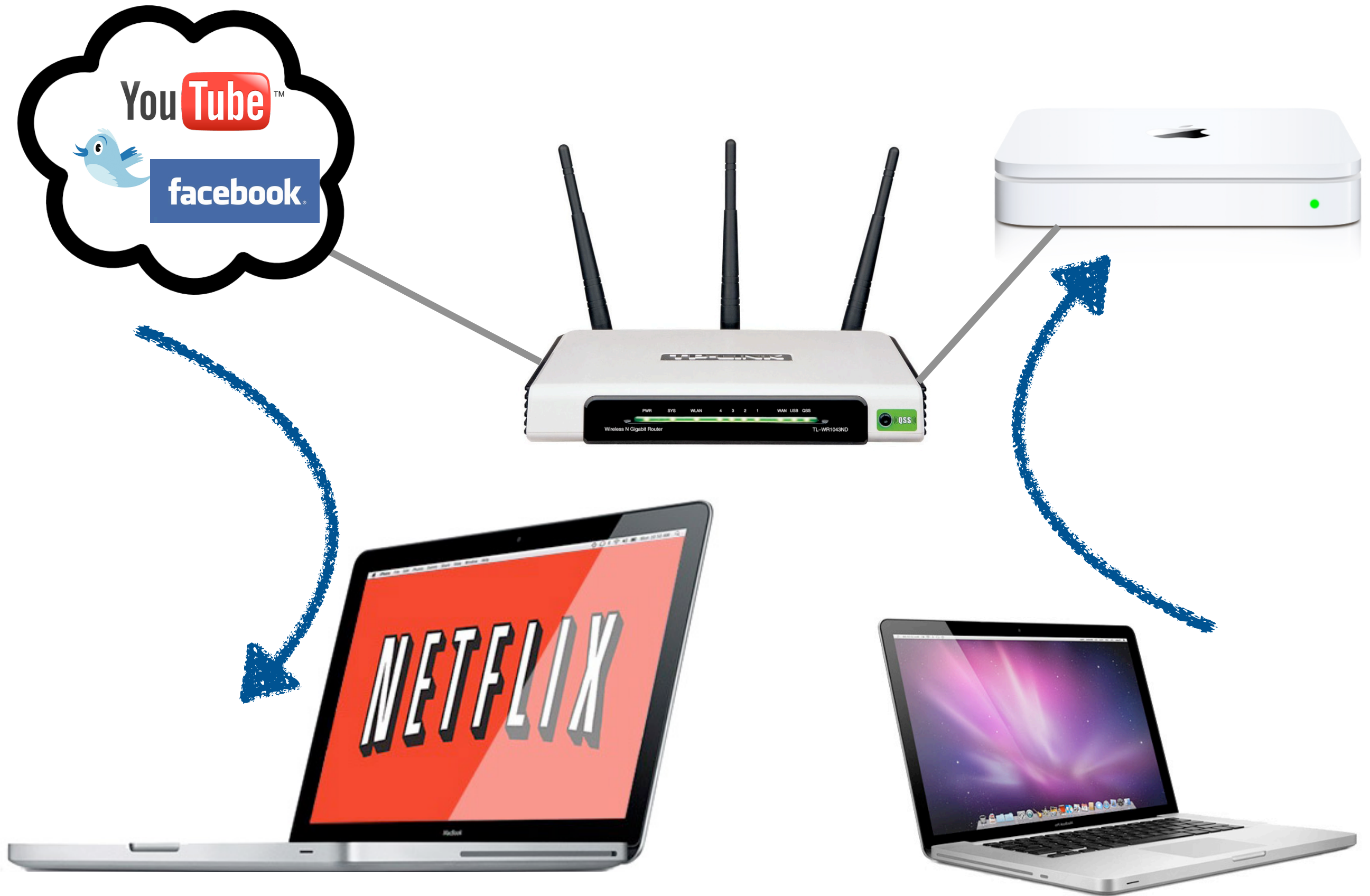


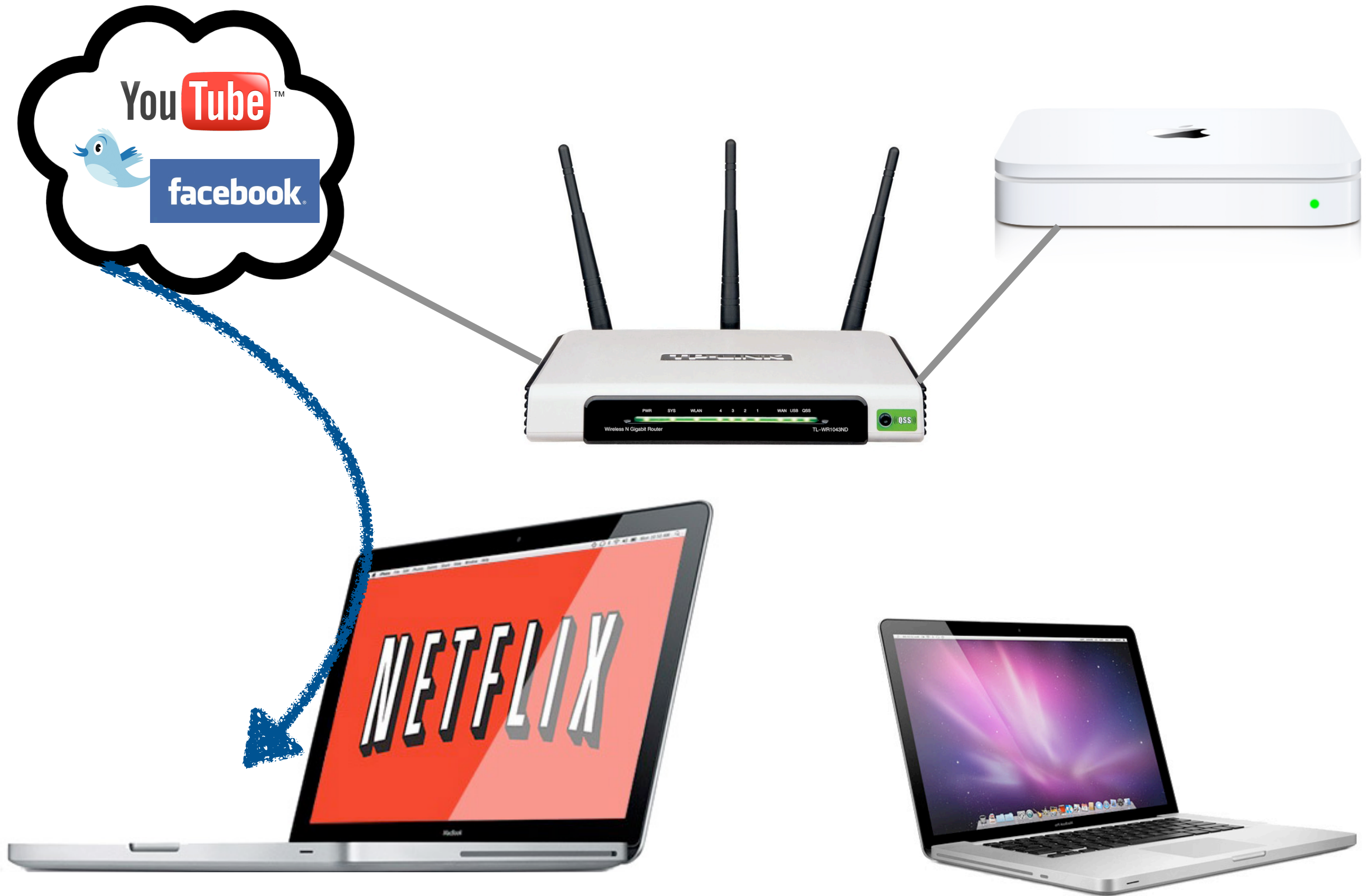
More Episodes

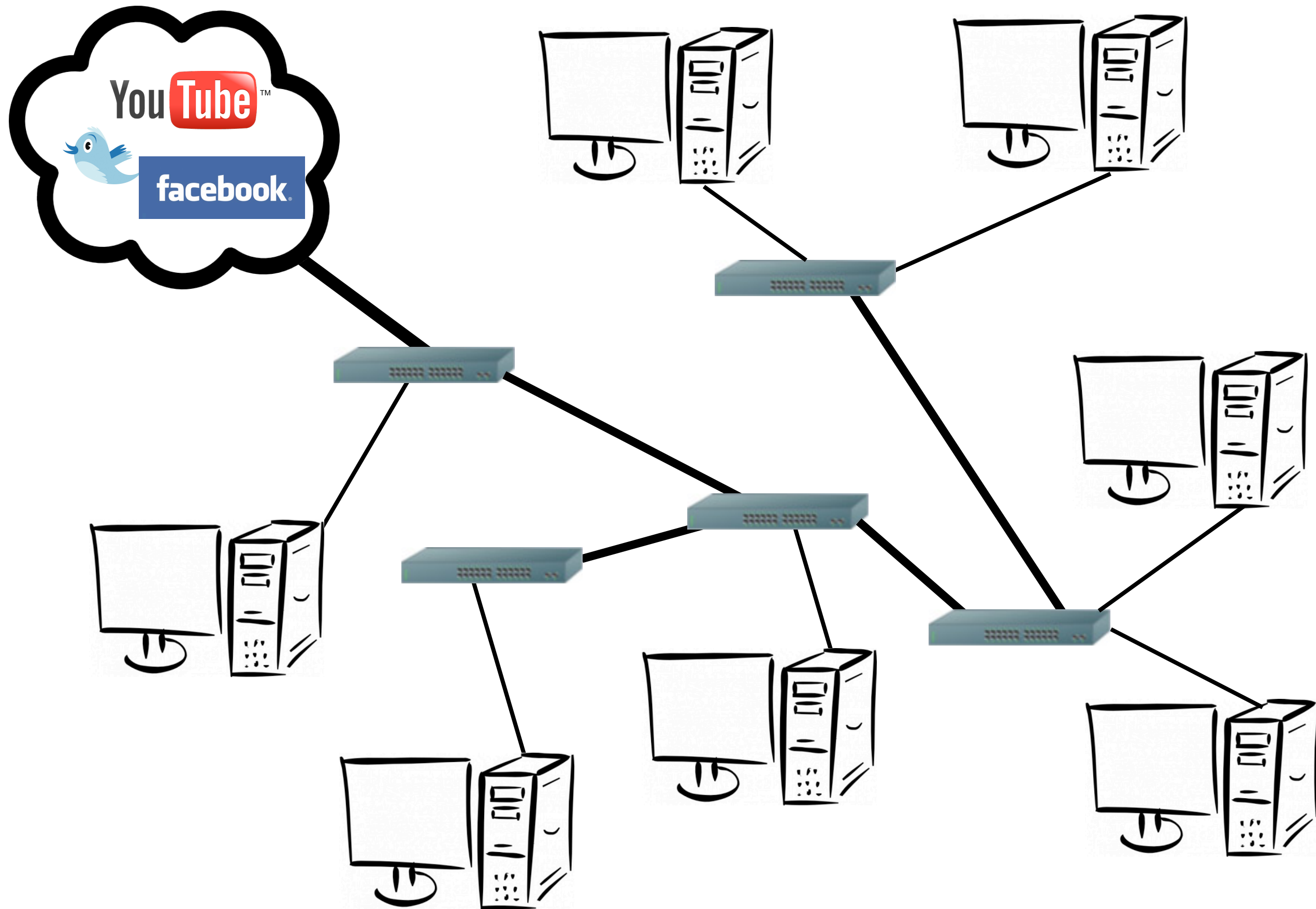
Back to Browsing

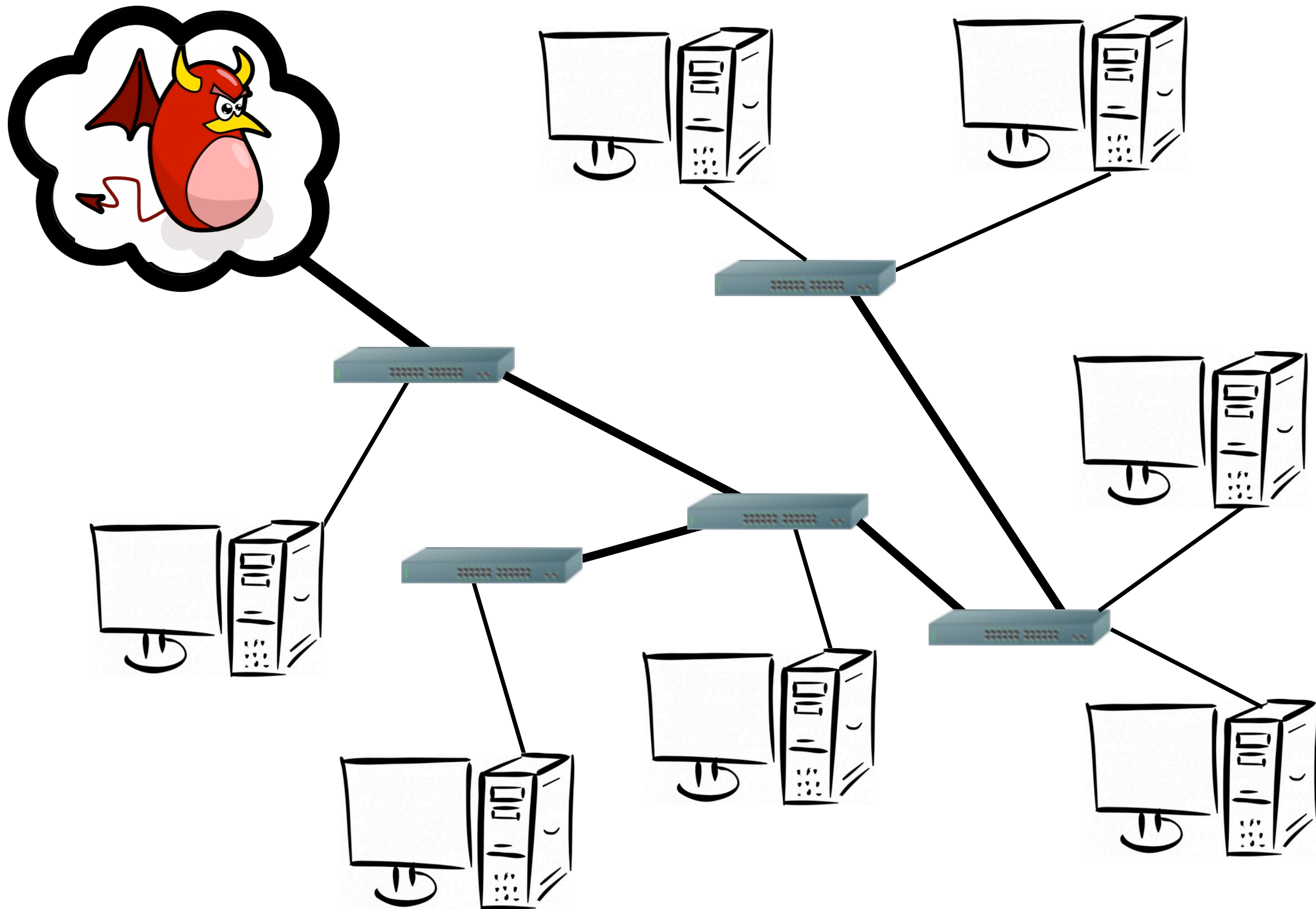


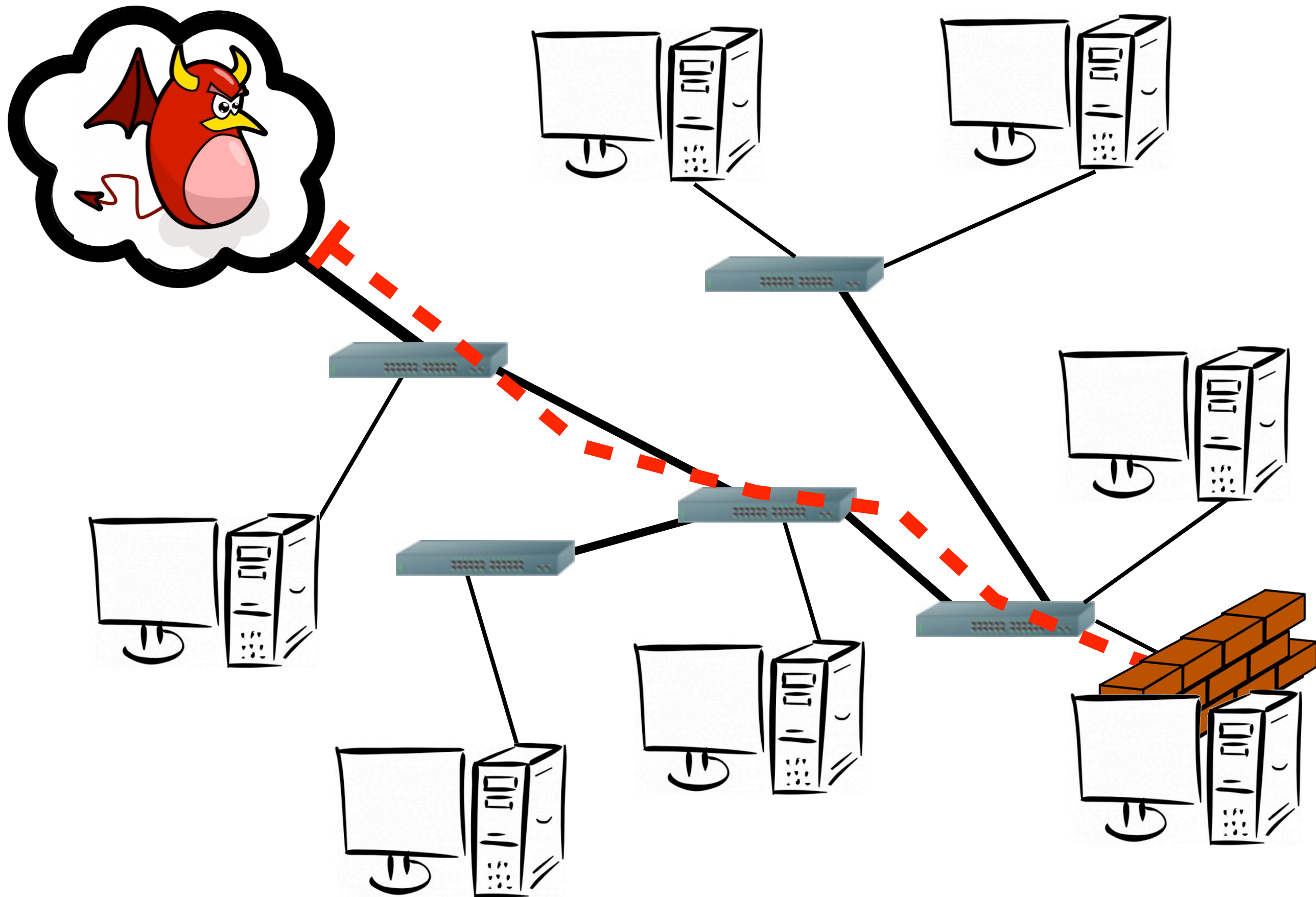


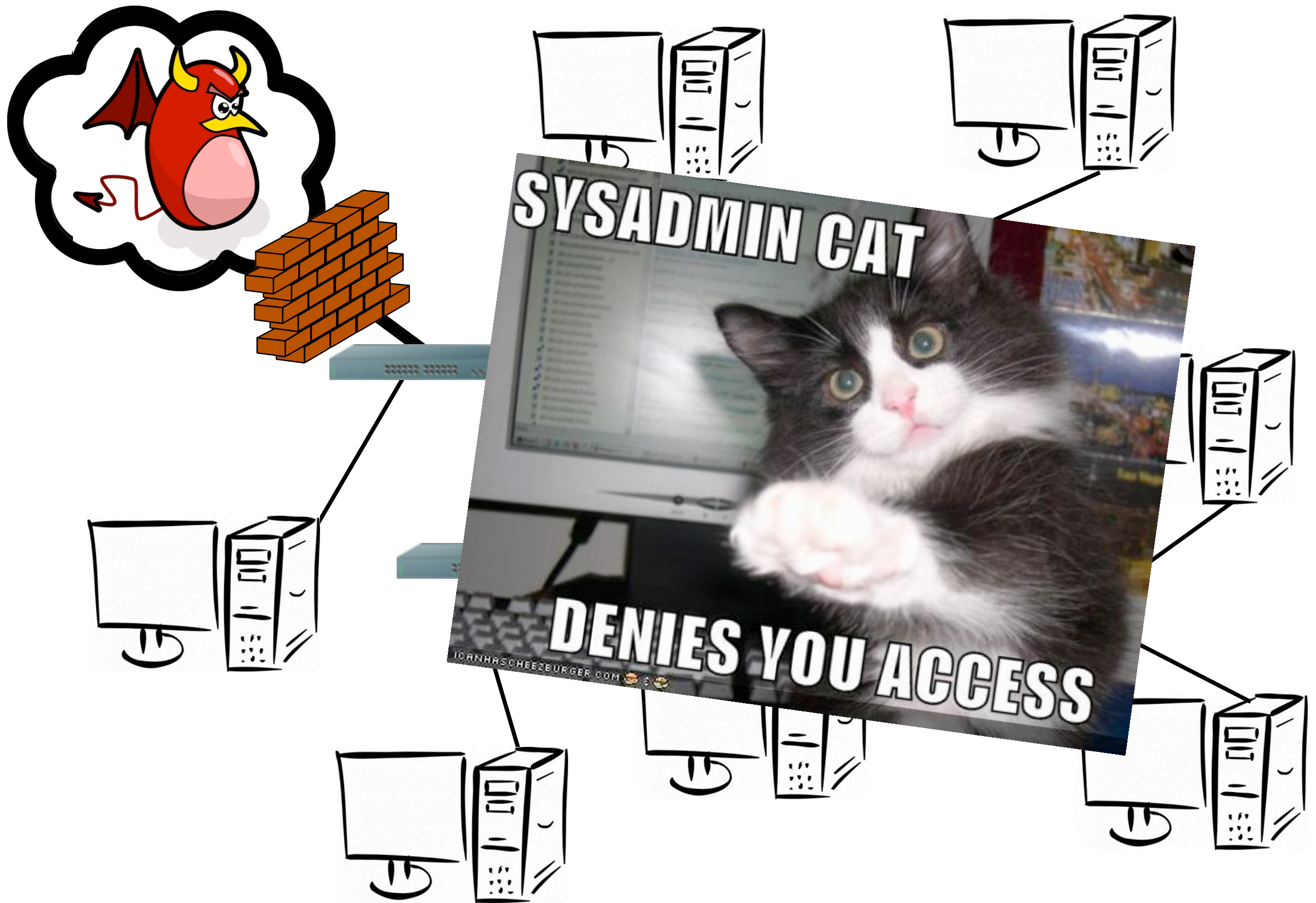


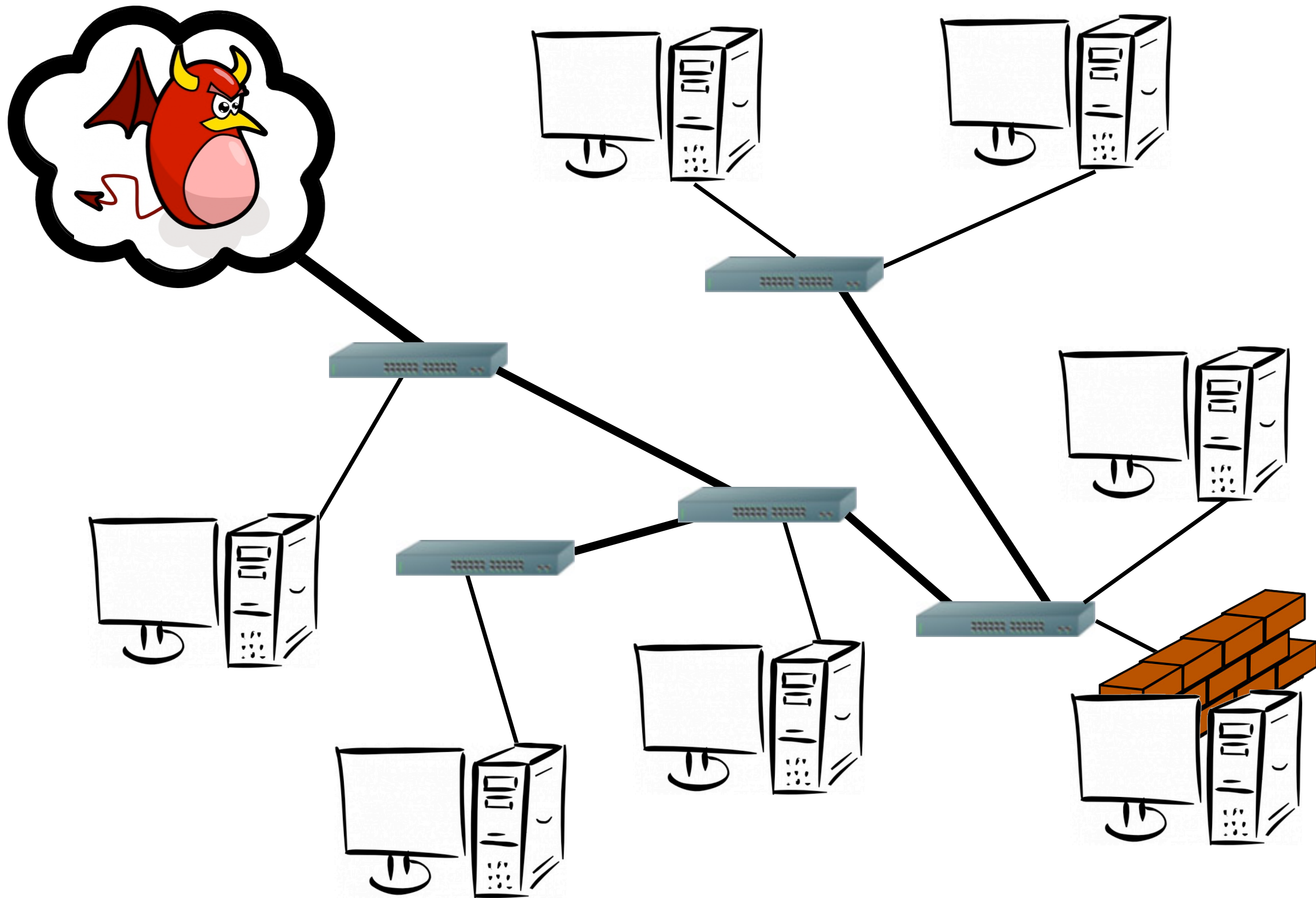


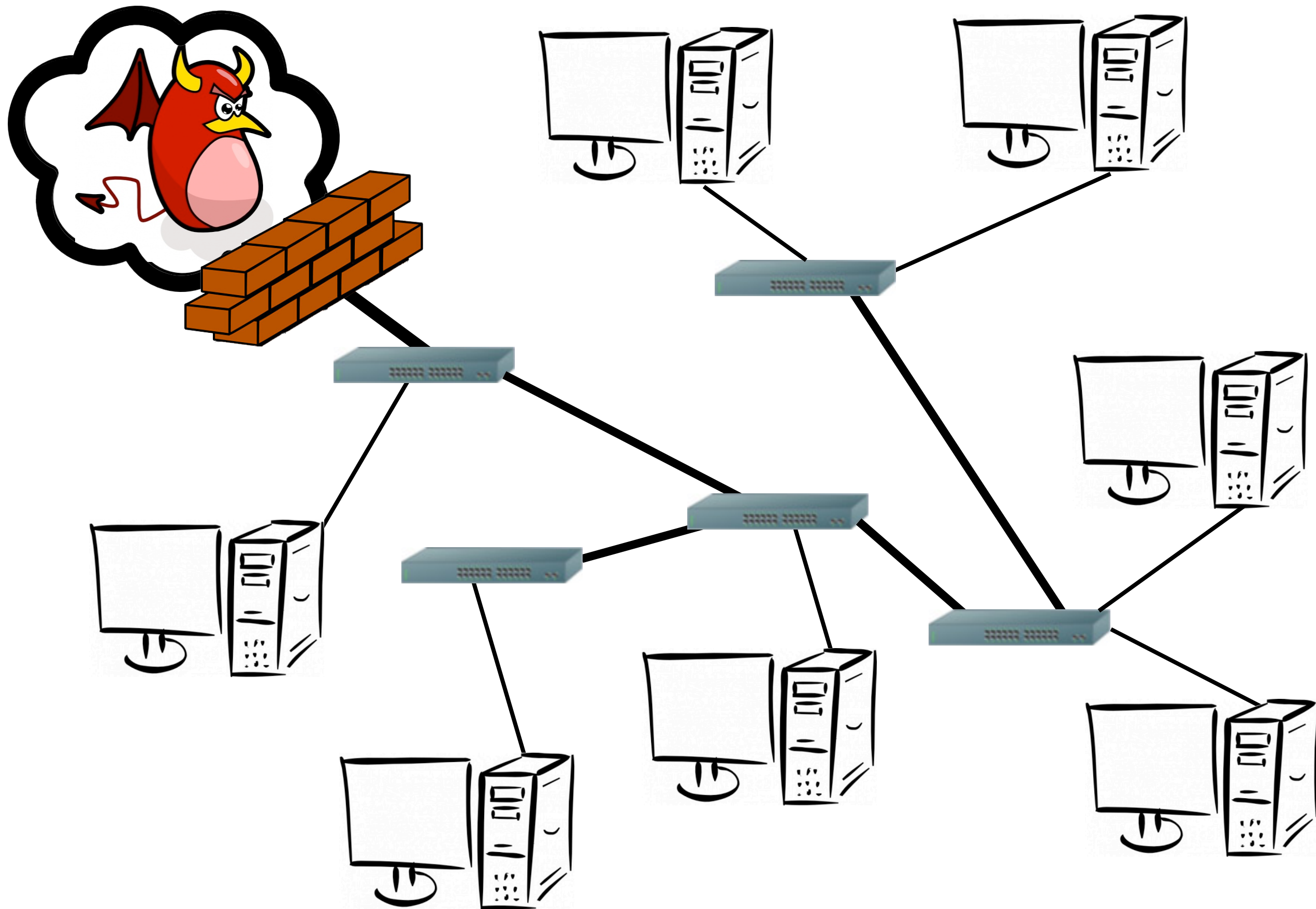




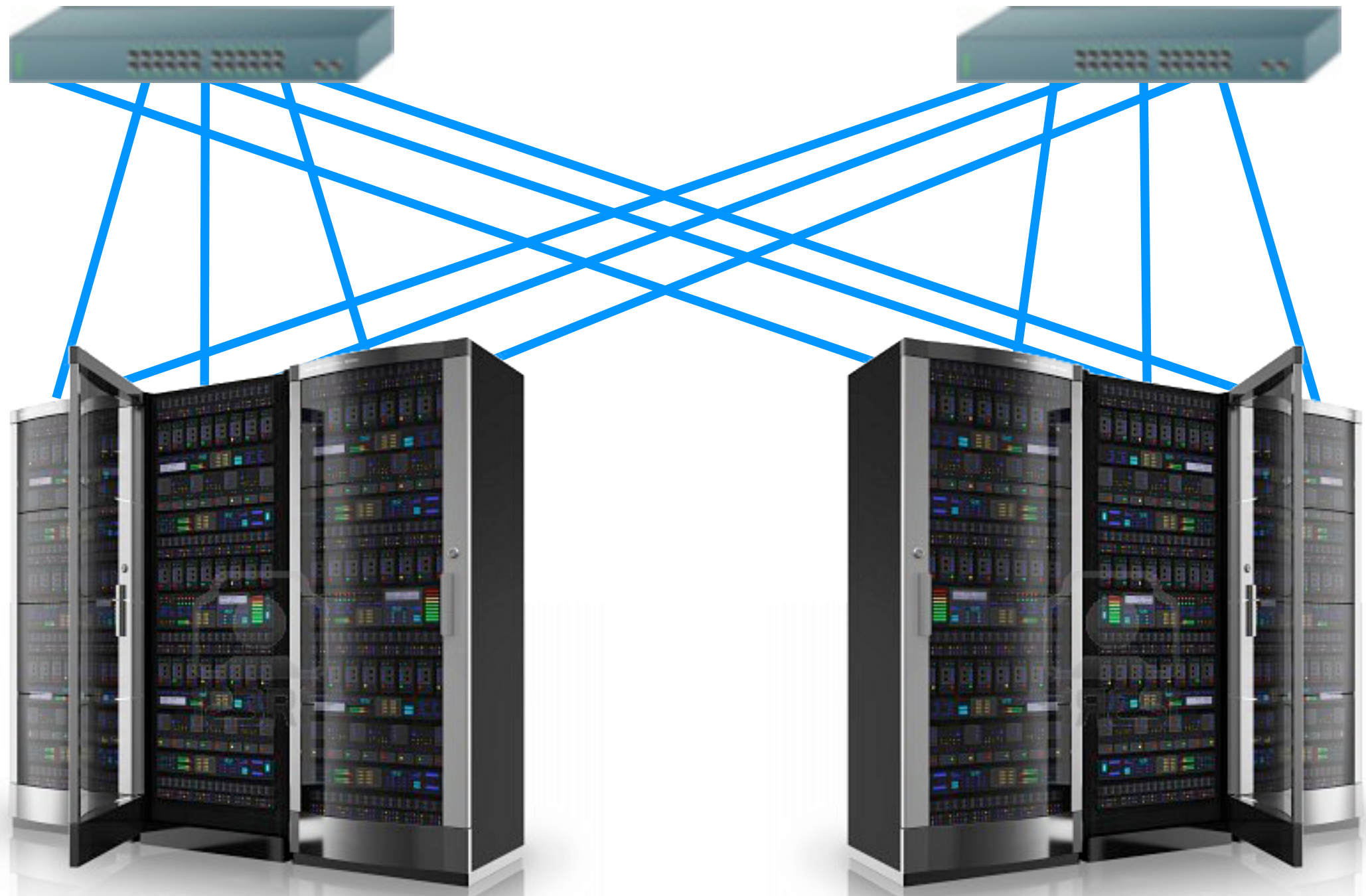


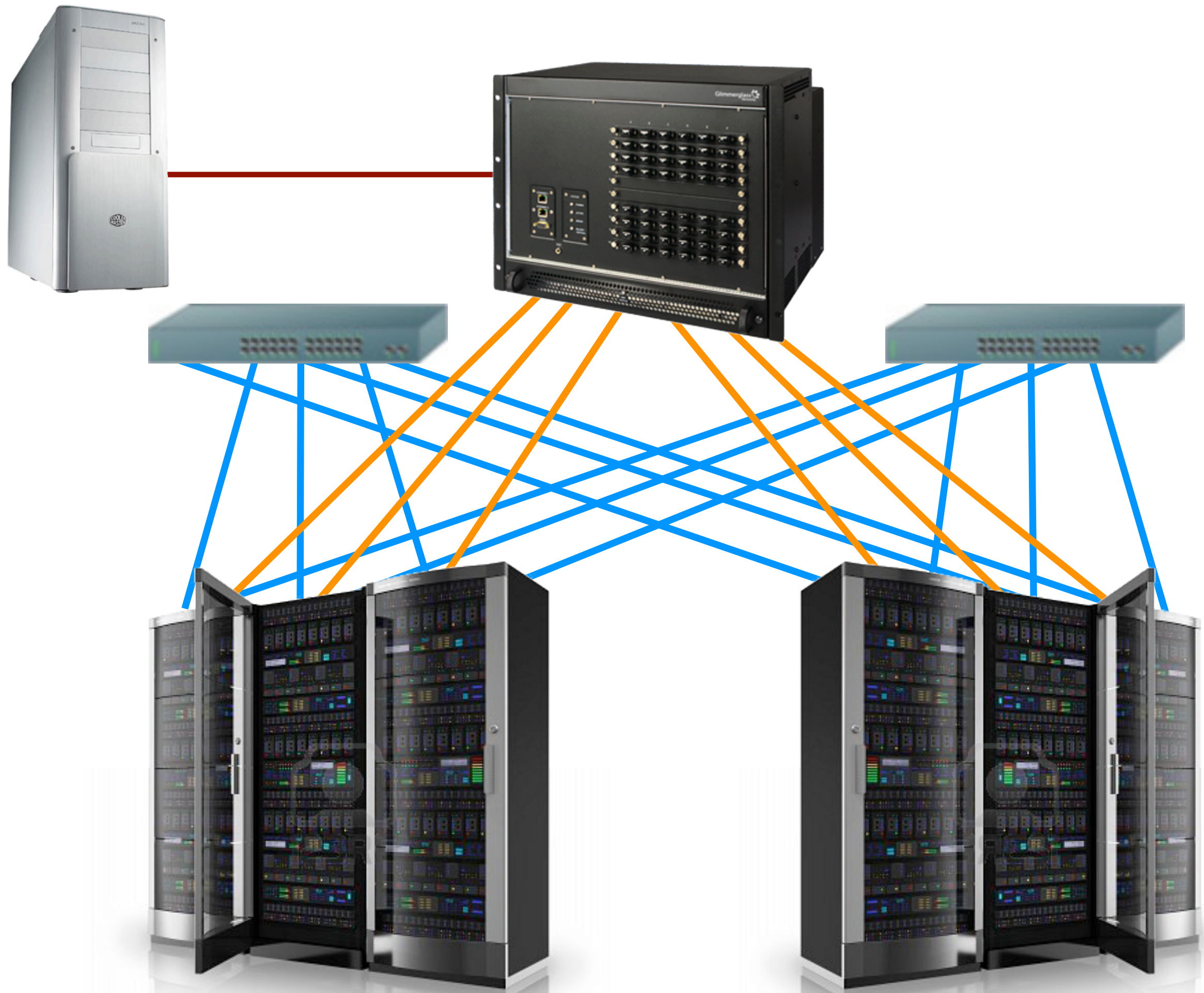


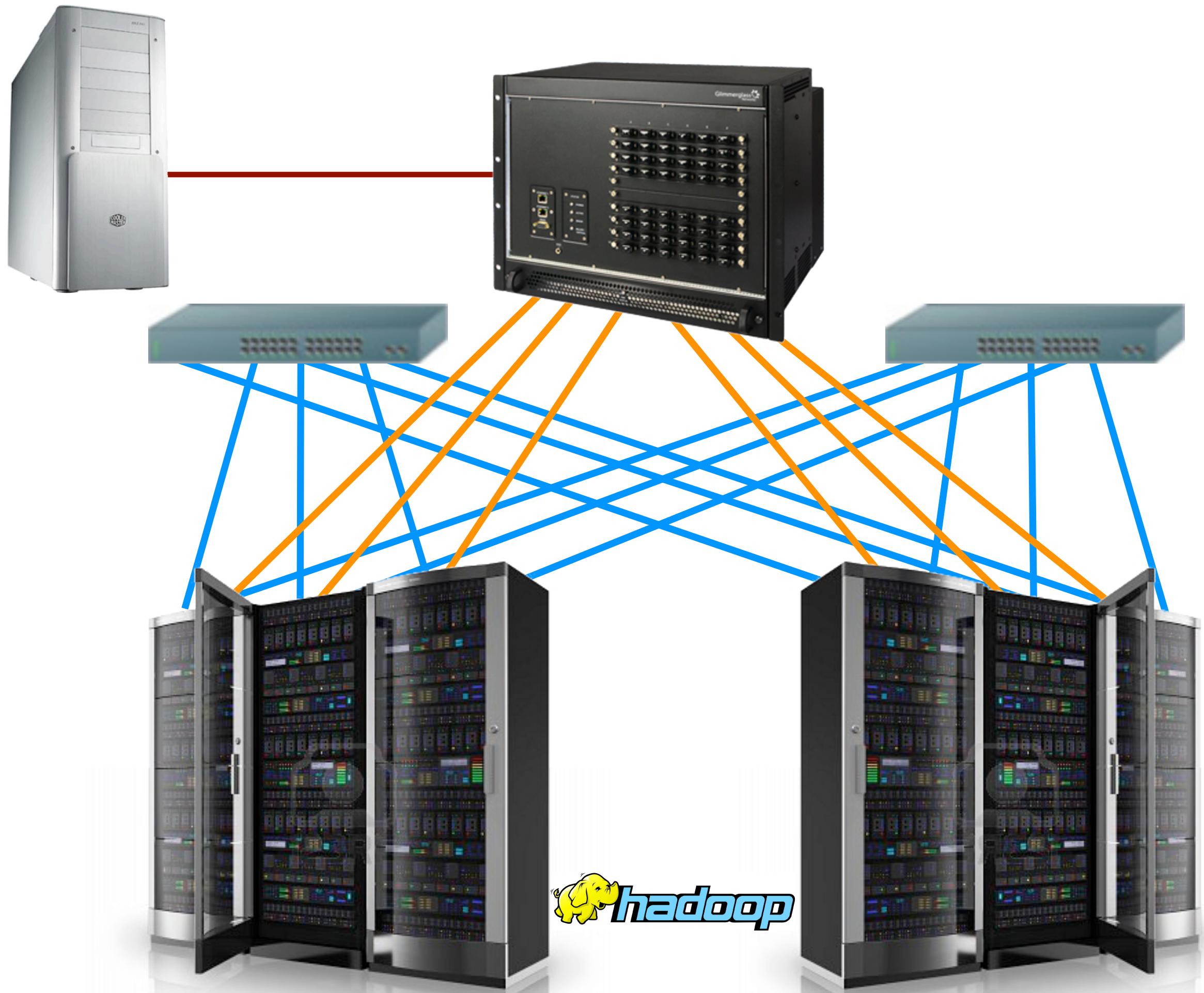


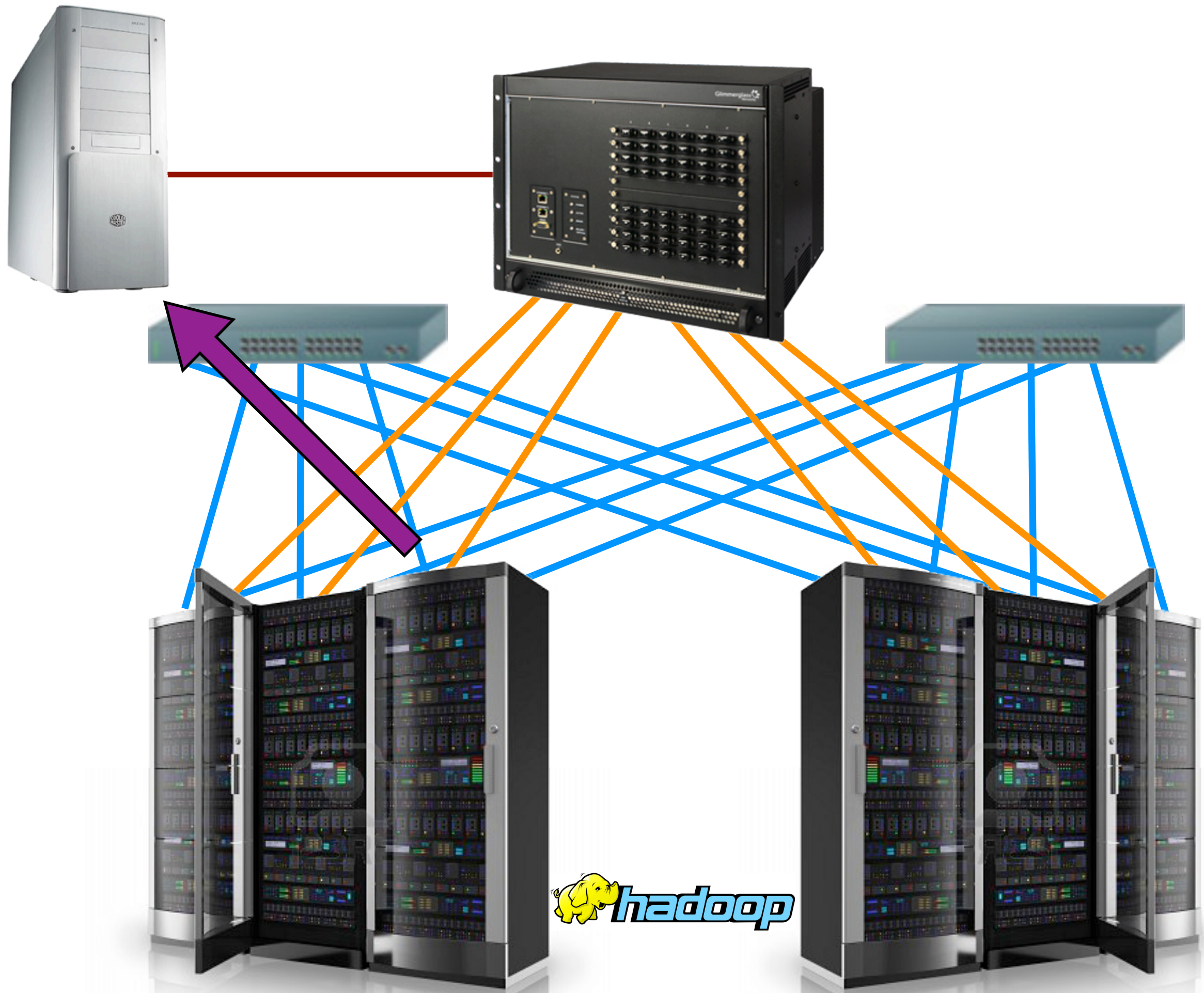


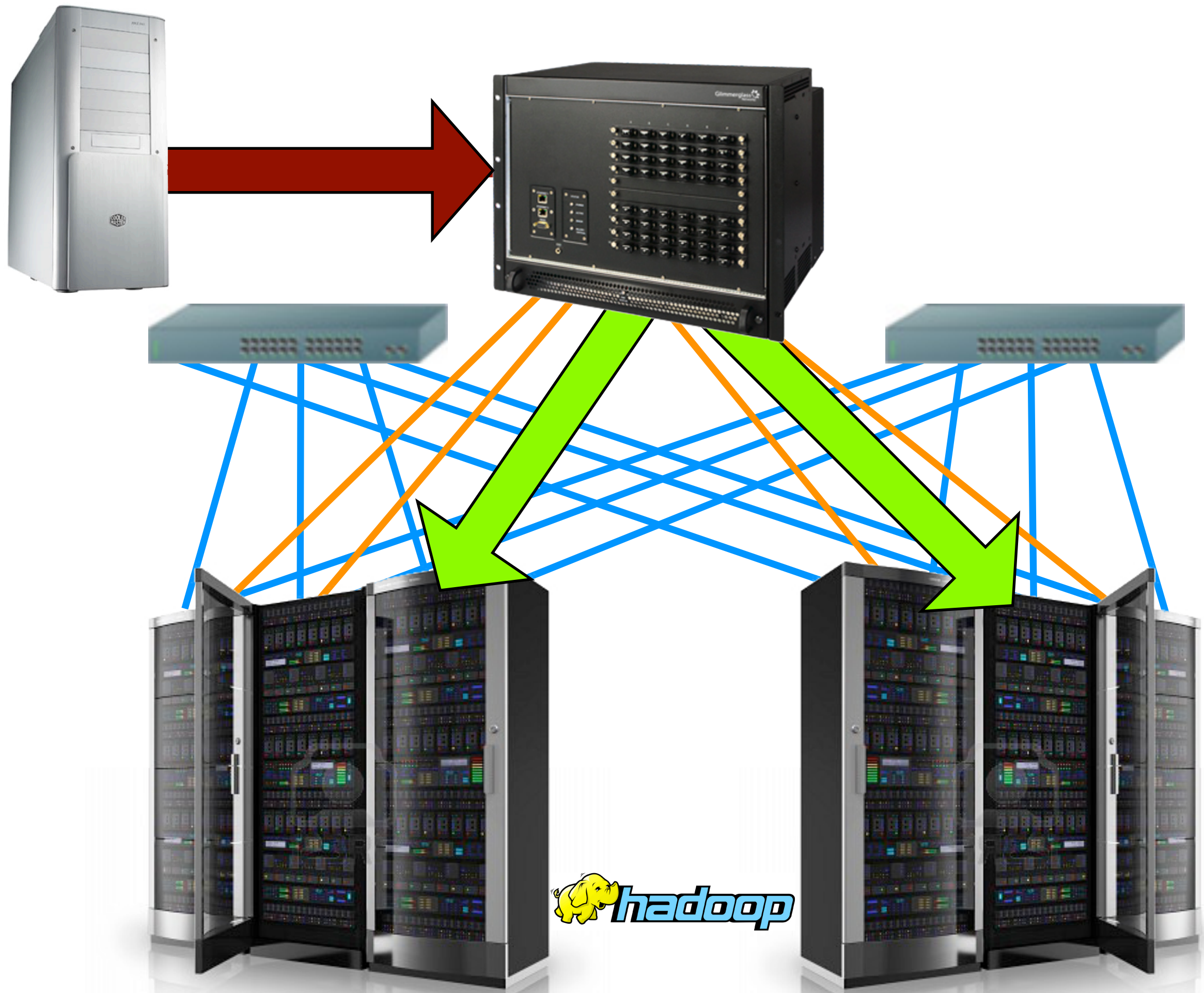






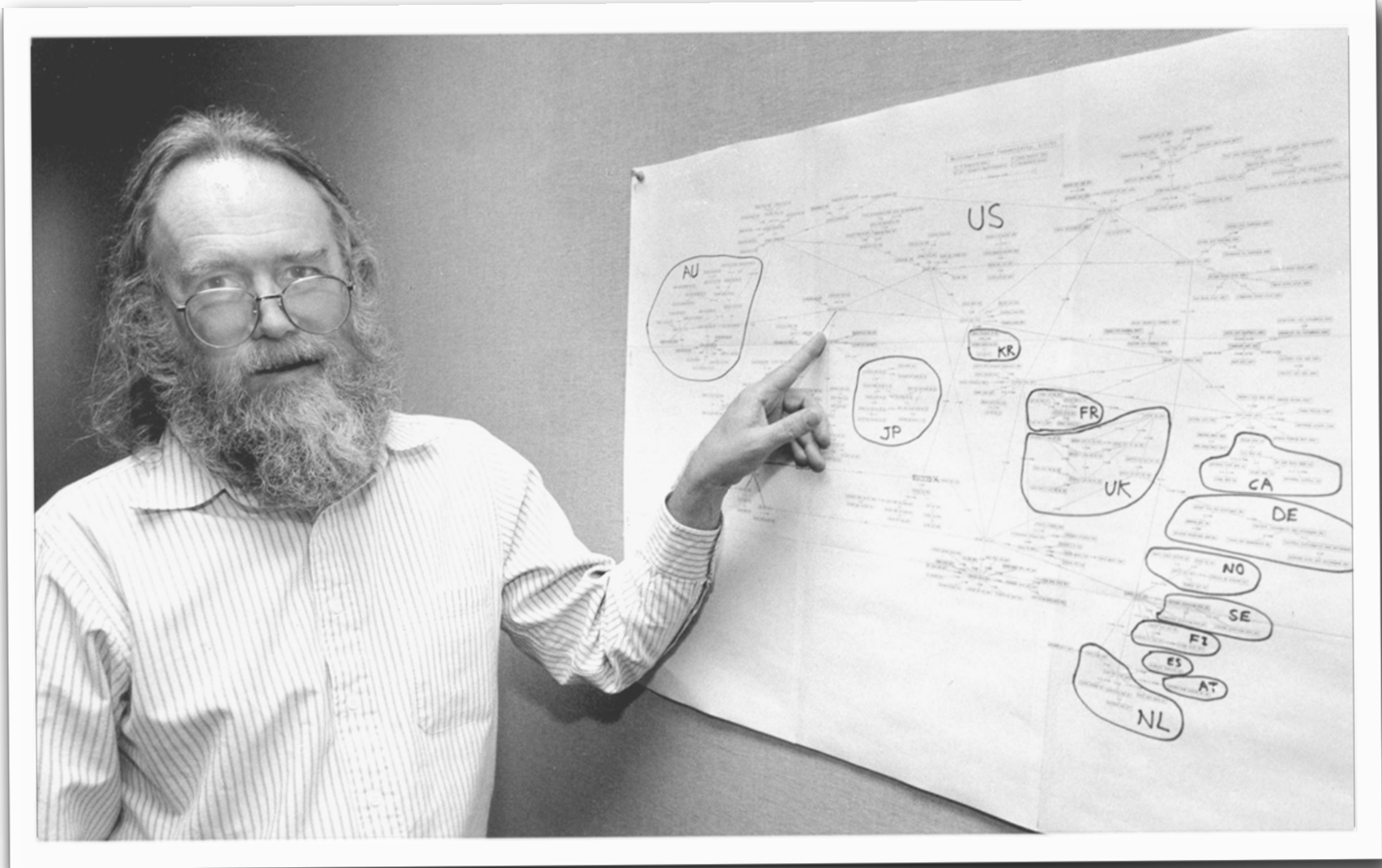






Participatory Networking

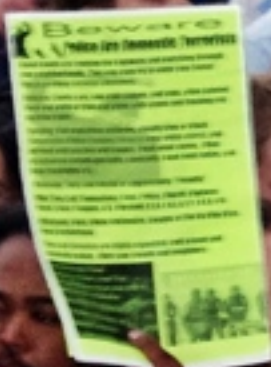




OCCUPY EVERYTHING

#OCCUPYWALLST

WE ALREADY KNOW THAT WE OWN EVERYTHING--THE TASK IS TO EXCLUDE THE INTRUSIONS OF CAPITAL AND POWER



BANKS
BAILED
OUT
WE
G

Participatory Networking

Safe?

Secure?

Fair?

Loop freedom?

Black holes?

Participatory Networking

1. semantics + protocol (Hot-ICE '12)

Participatory Networking

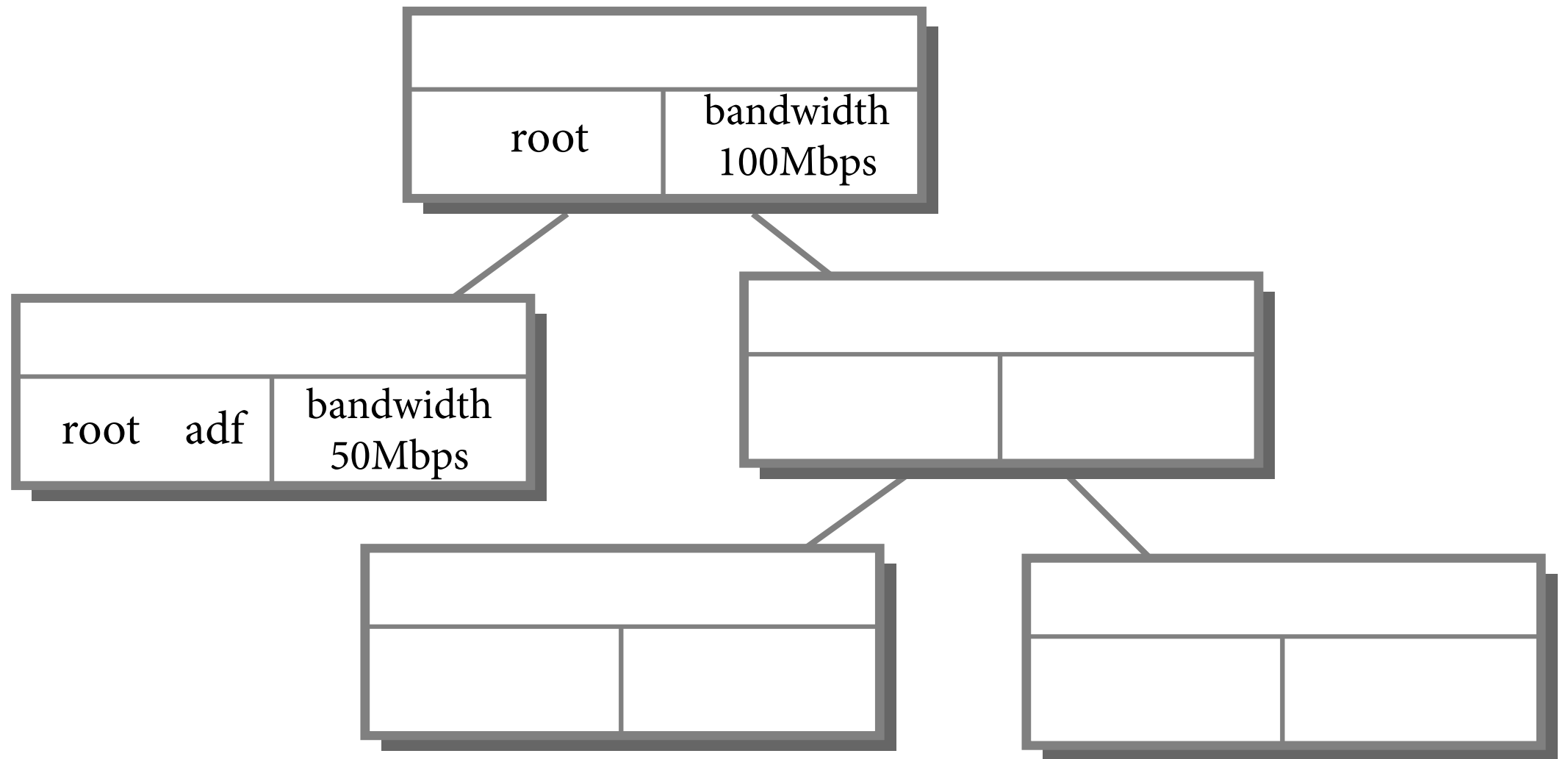
1. semantics + protocol (Hot-ICE '12)
- 2. implementation (this talk)**

Participatory Networking

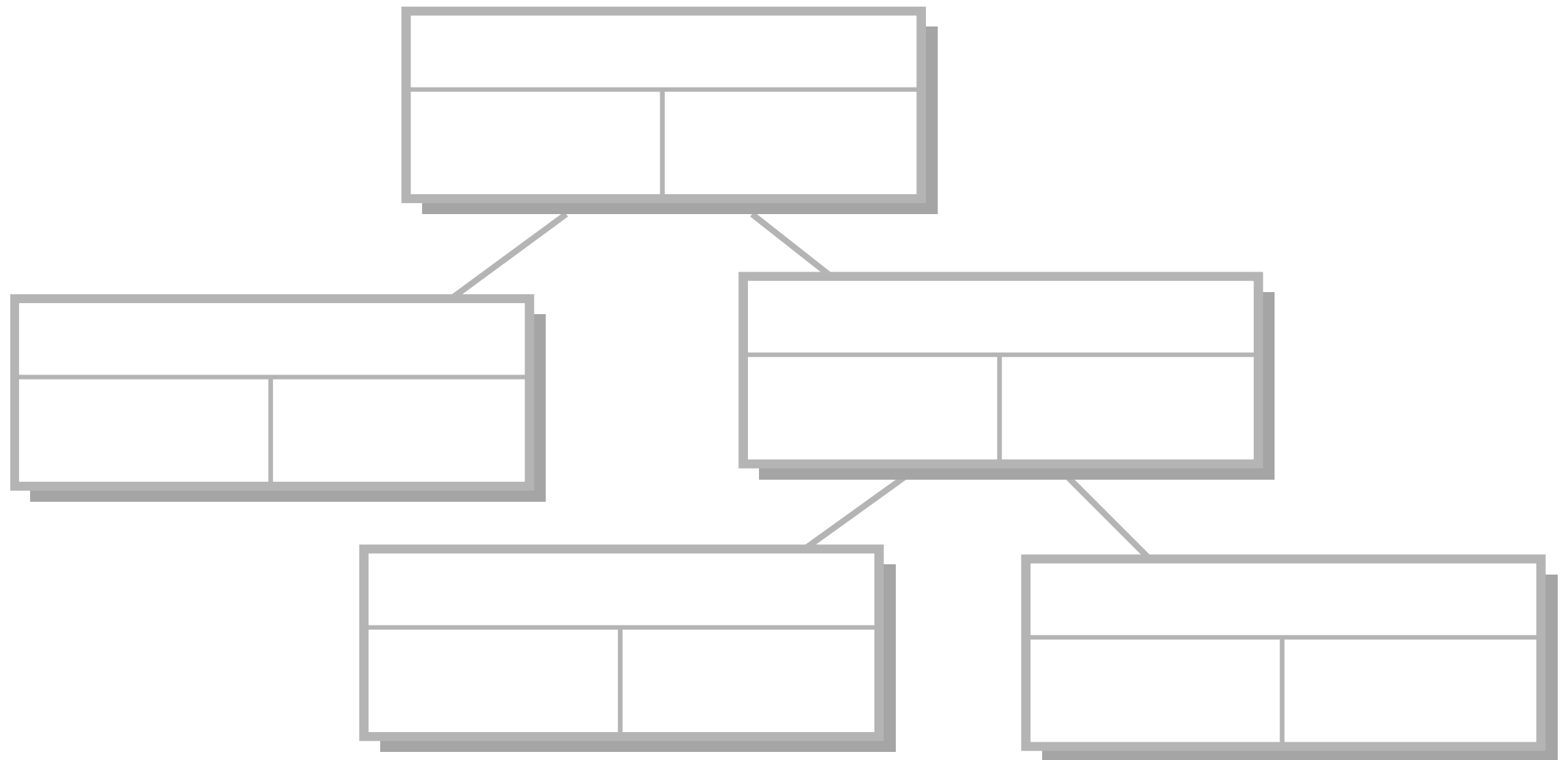
1. semantics + protocol (Hot-ICE '12)
2. implementation (this talk) **PANE**

Hierarchical Flow Tables

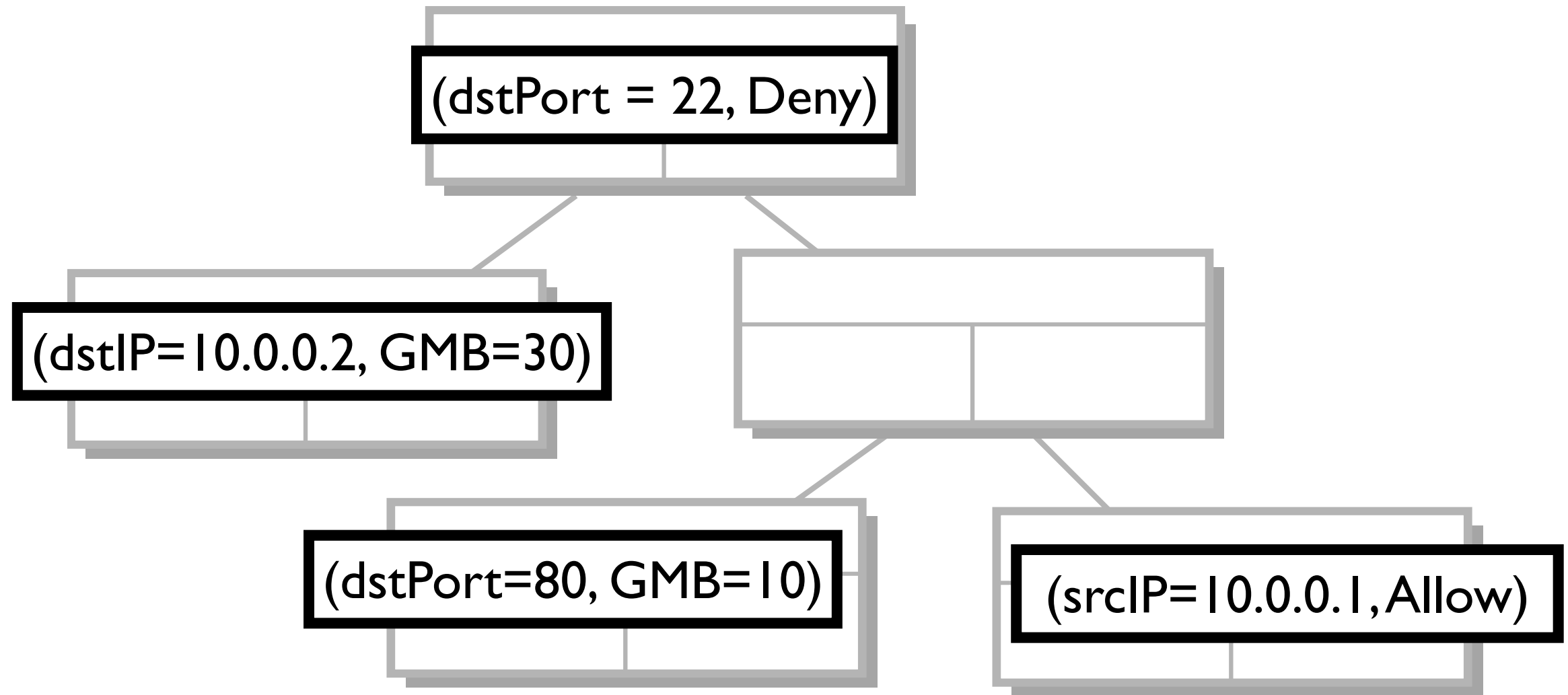




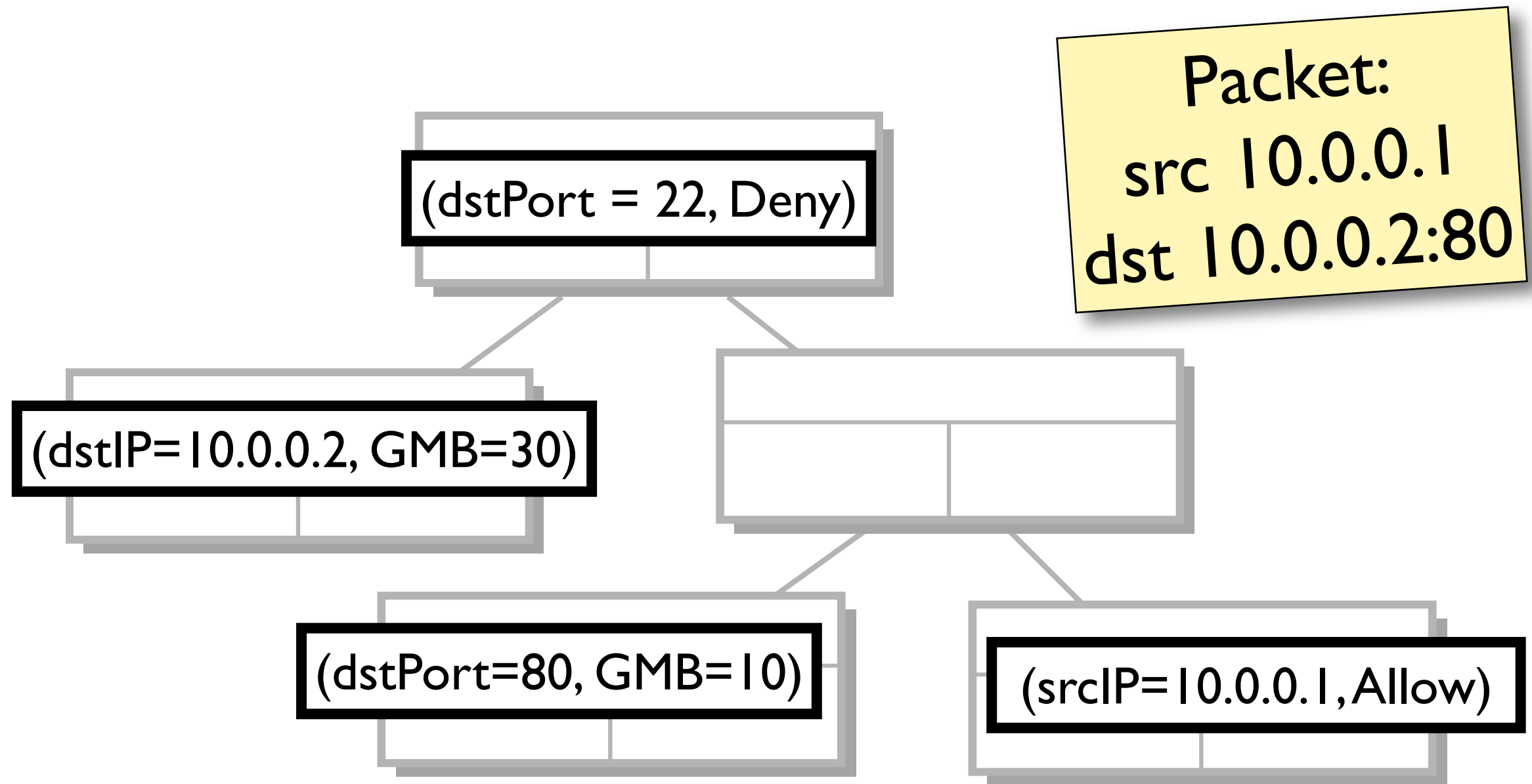
Hierarchy of Privileges



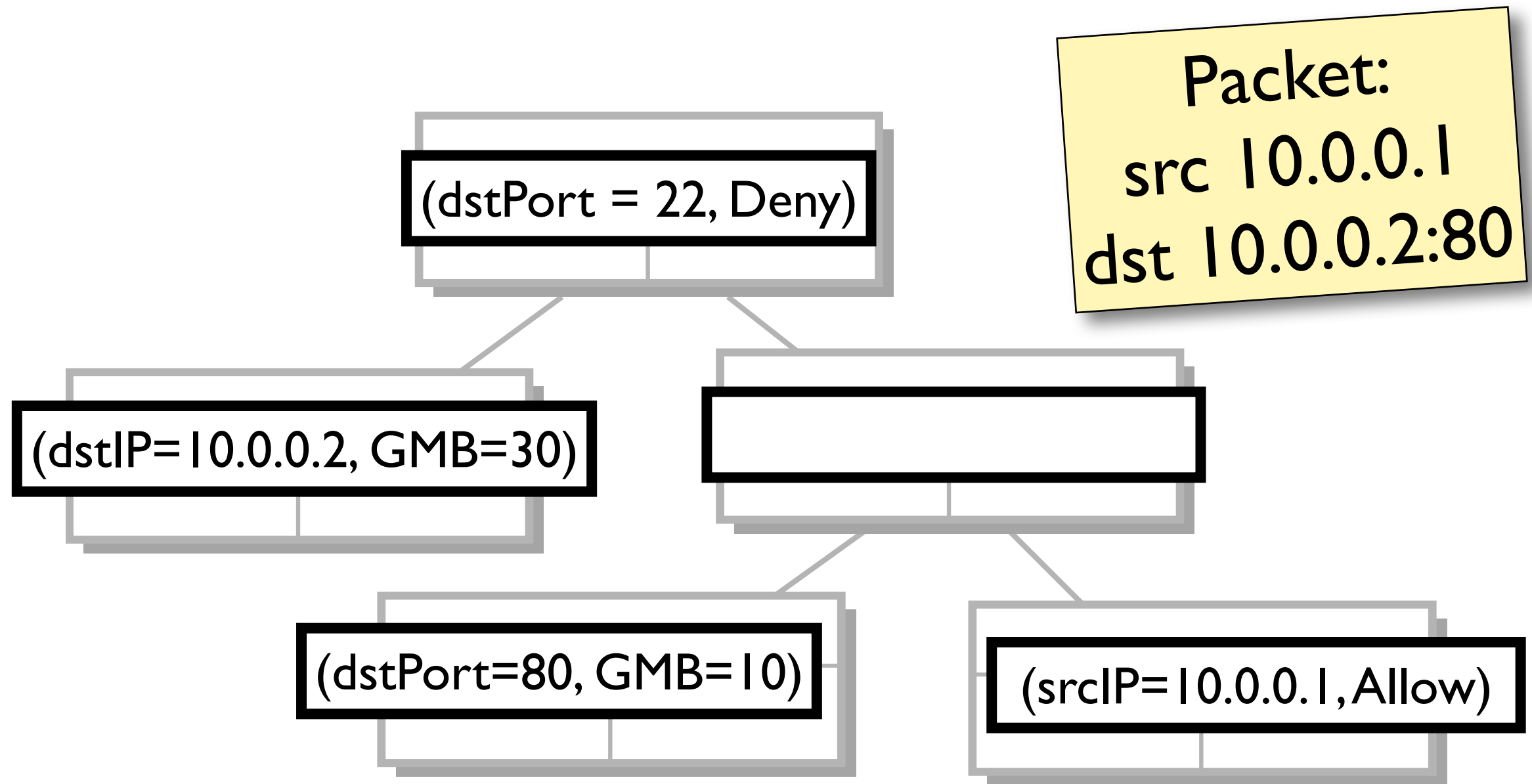
Hierarchy of Policies



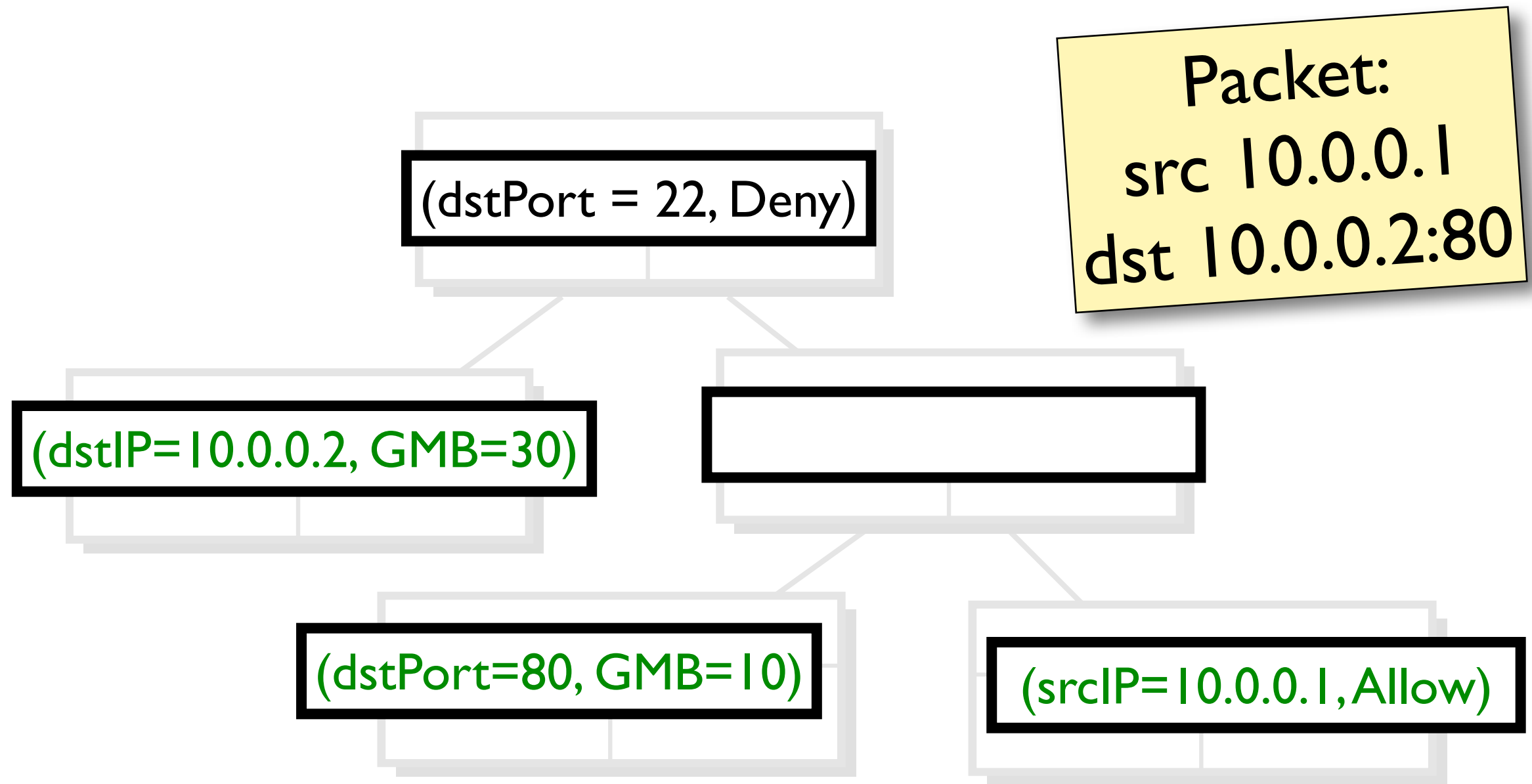
Hierarchy of Policies



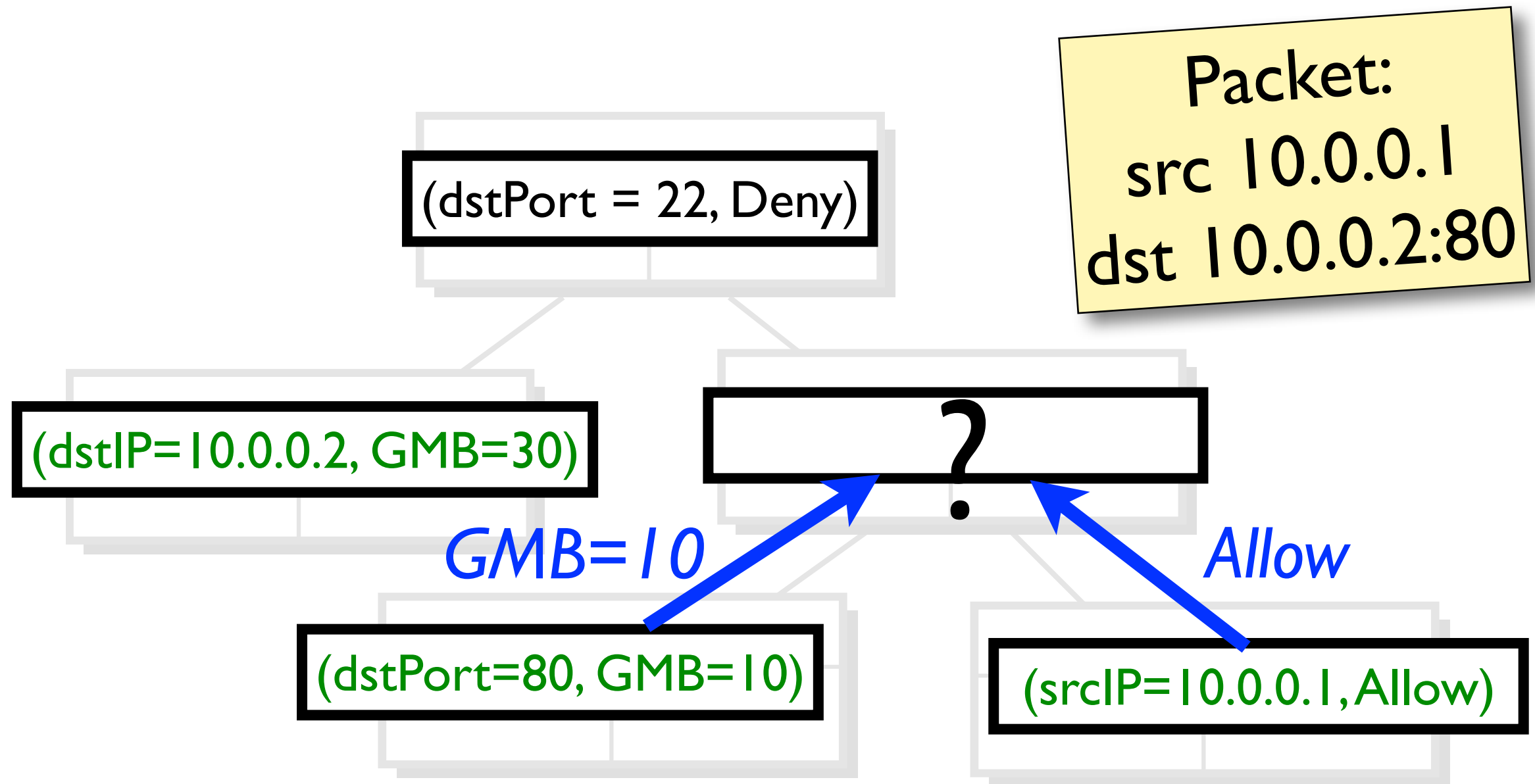
Hierarchy of Policies



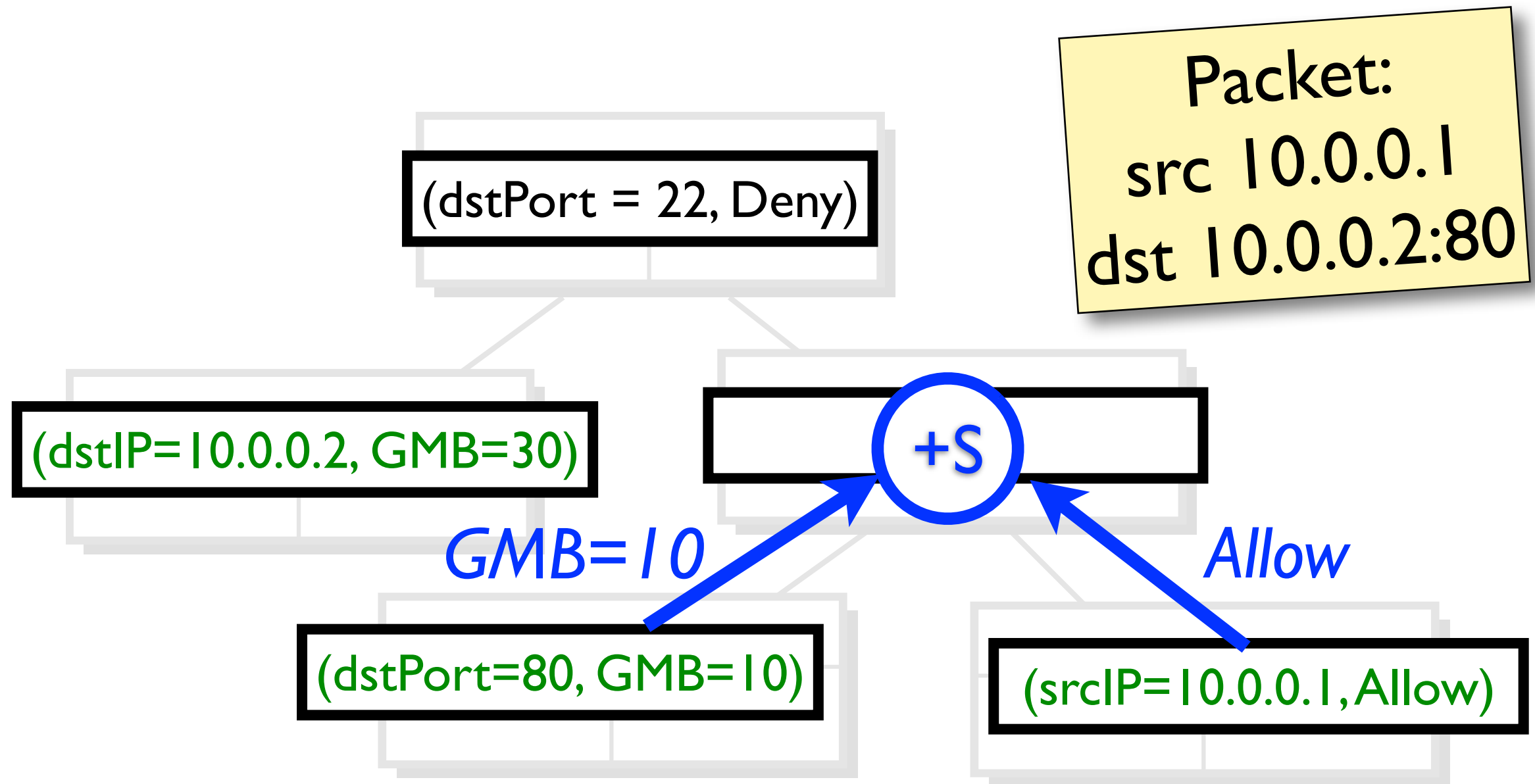
Hierarchical Flow Table



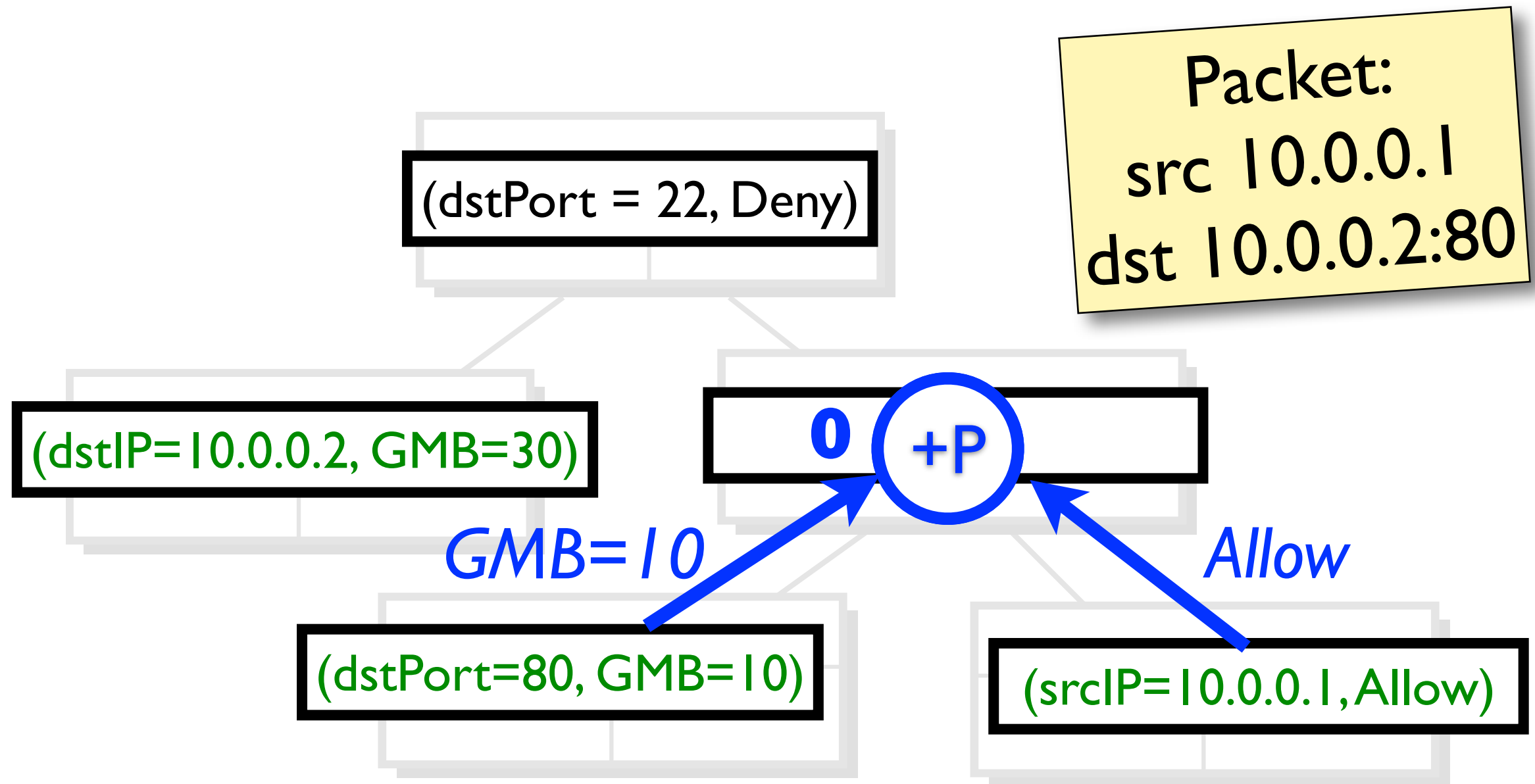
Hierarchical Flow Table



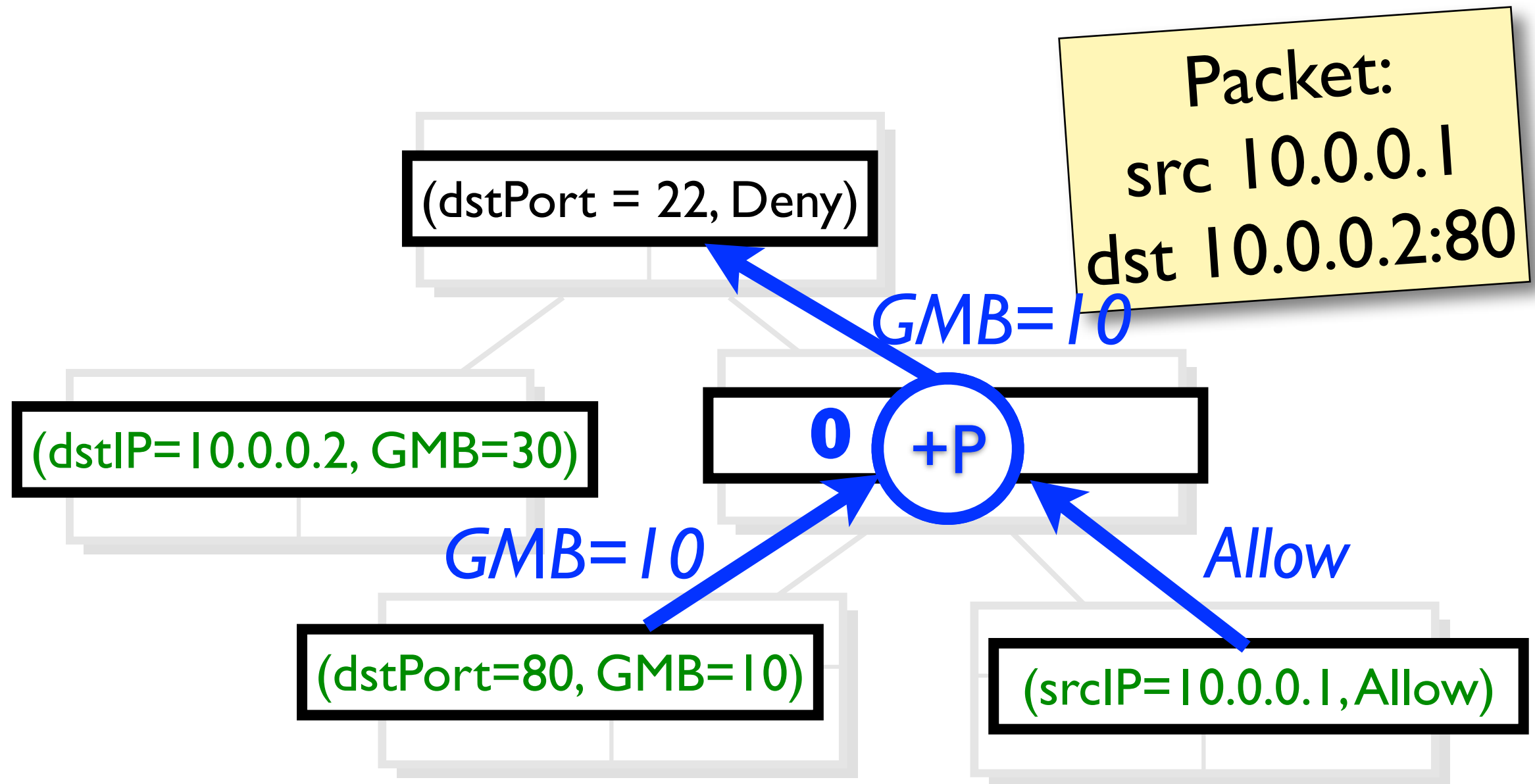
Hierarchical Flow Table



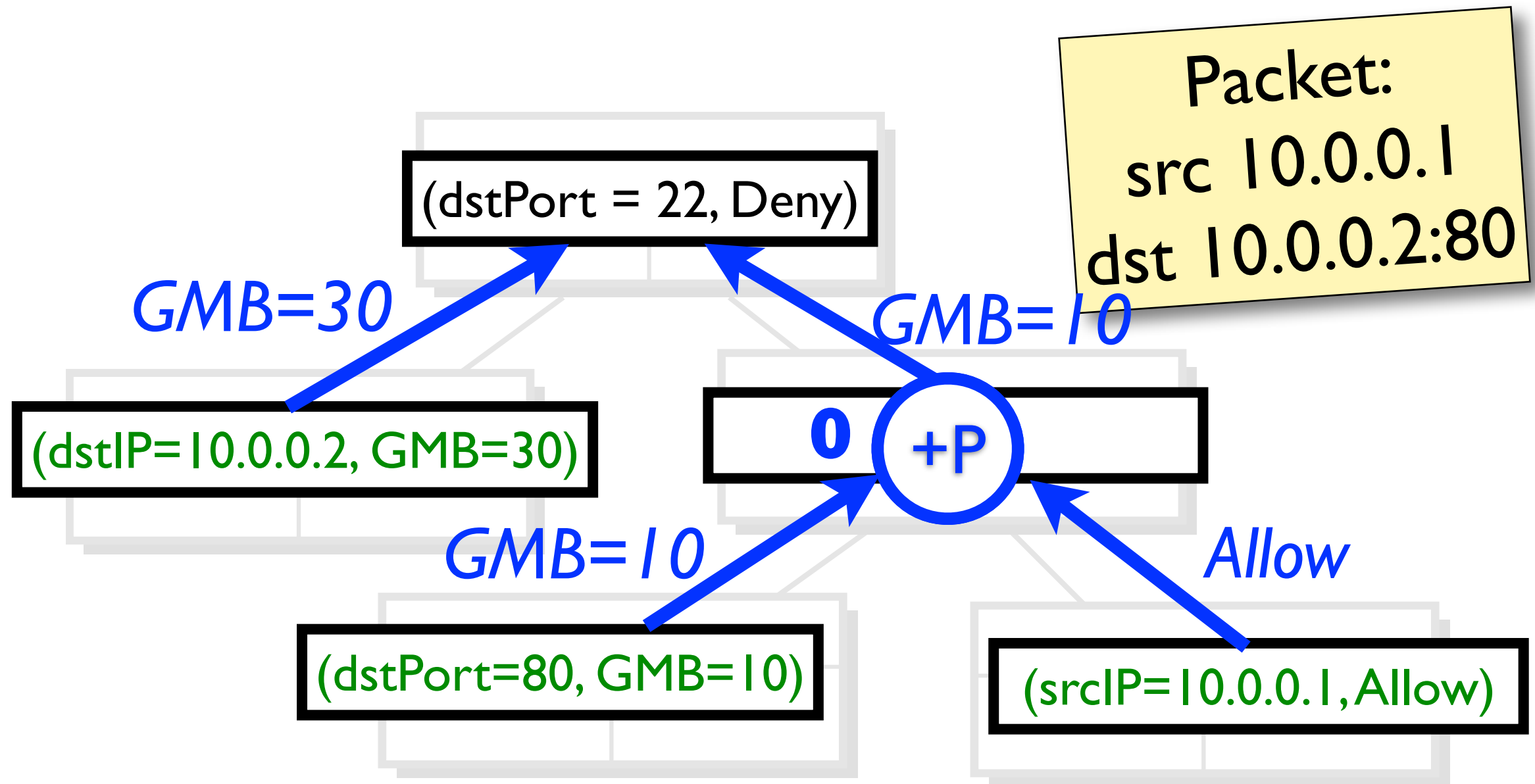
Hierarchical Flow Table



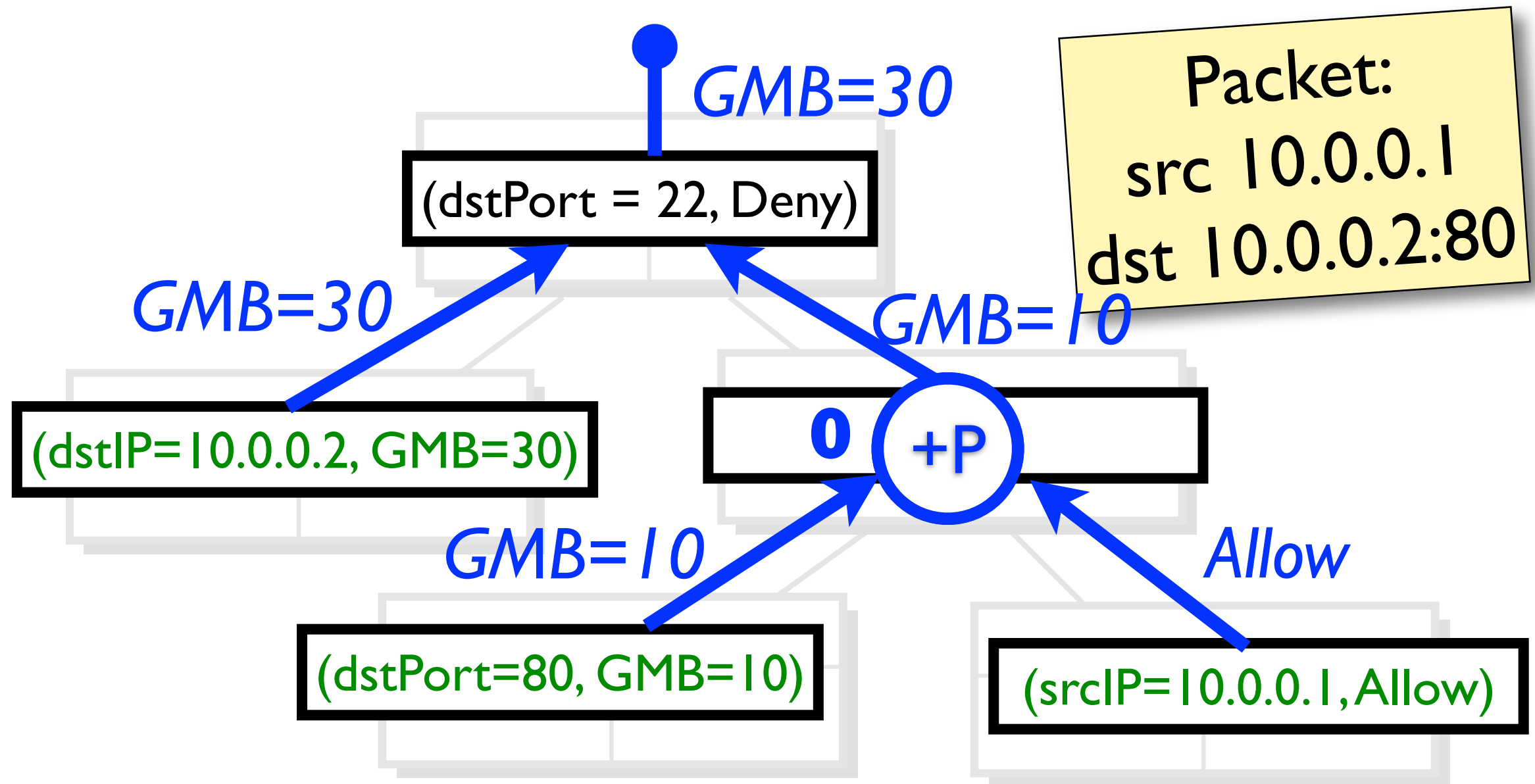
Hierarchical Flow Table



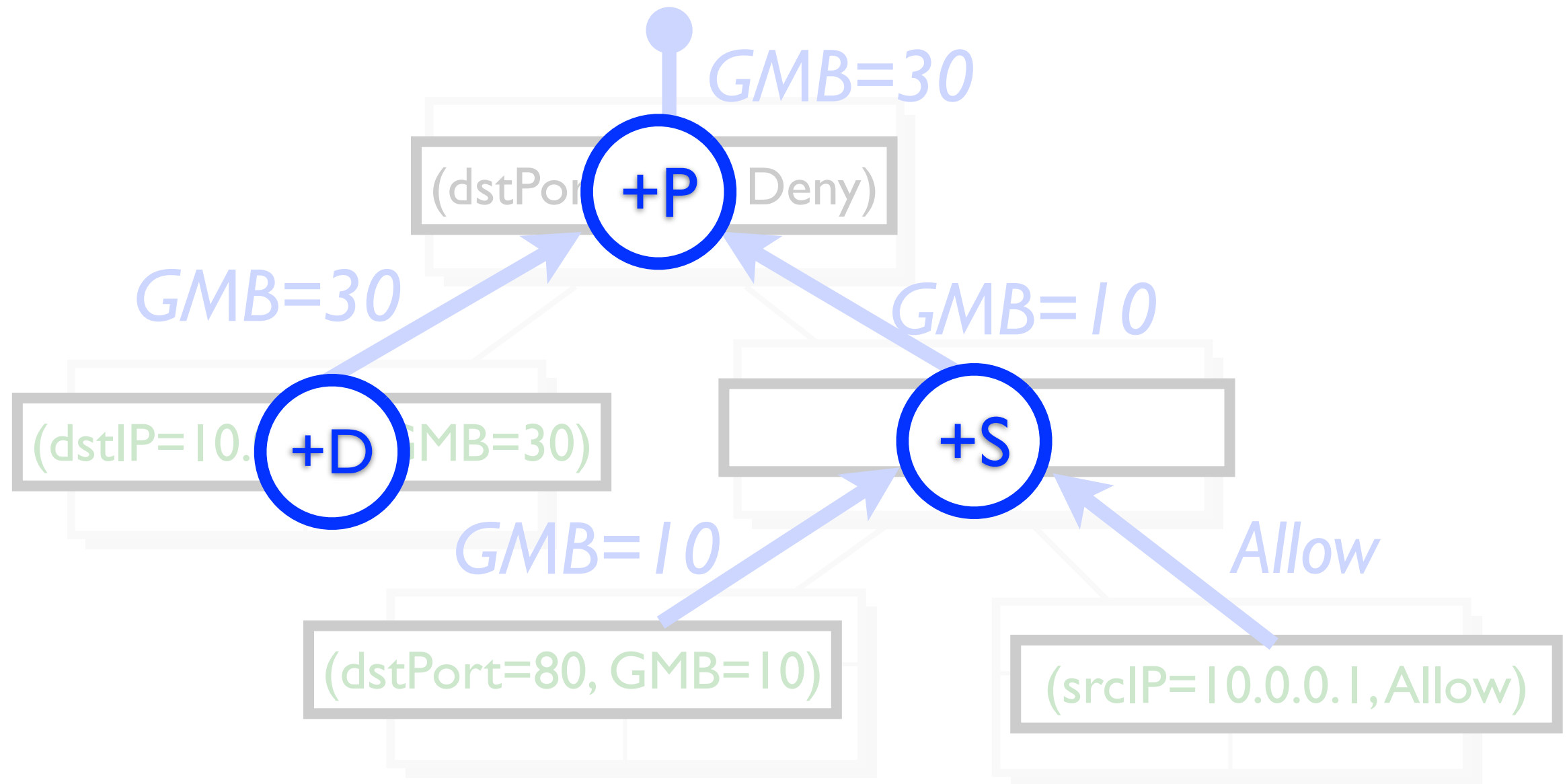
Hierarchical Flow Table



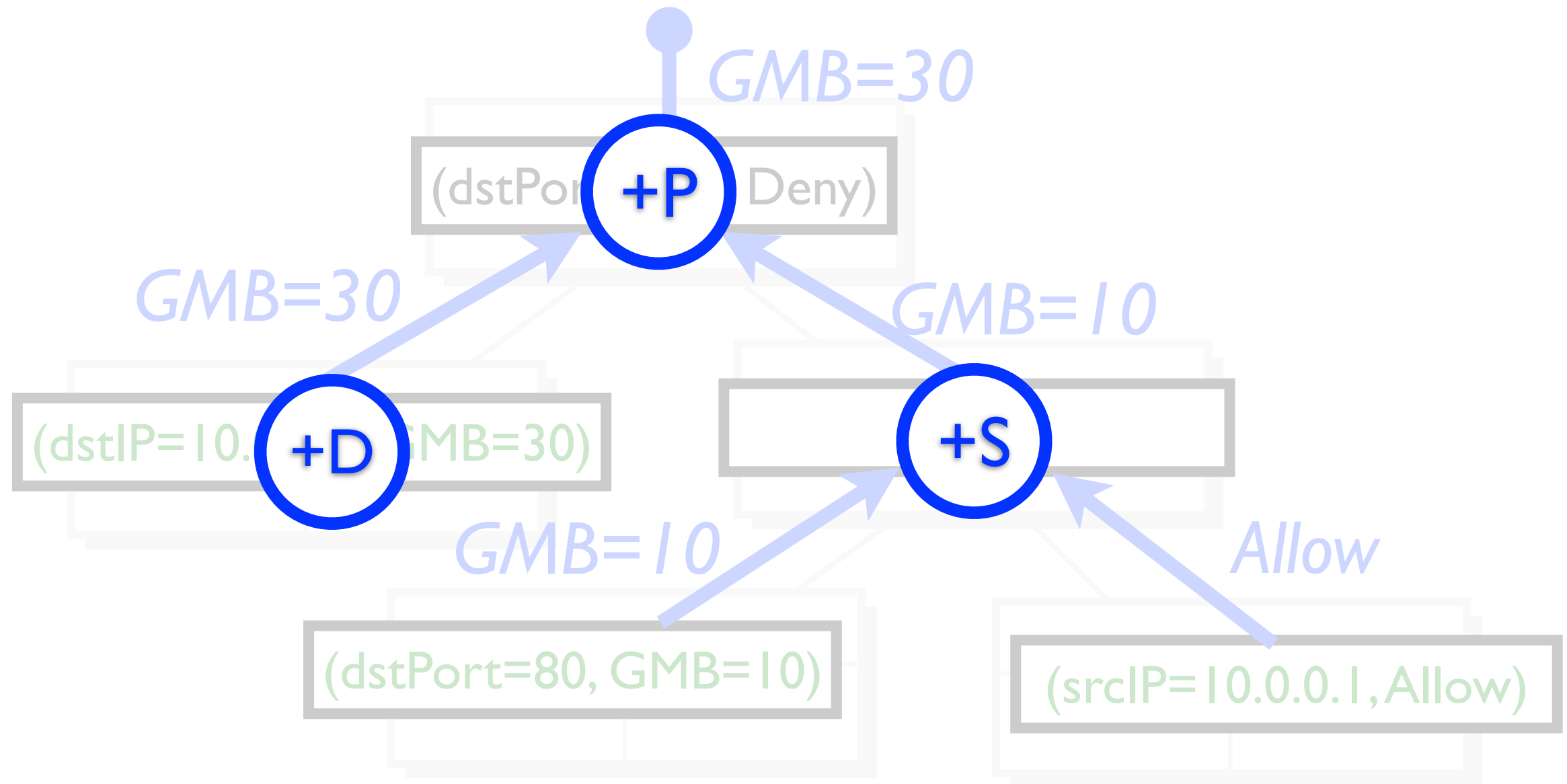
Hierarchical Flow Table



Hierarchical Flow Table

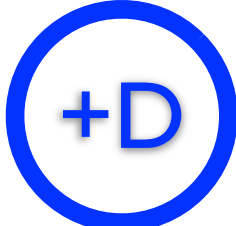


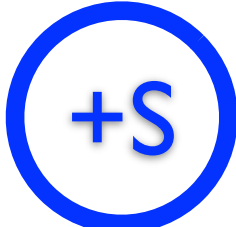
Hierarchical Flow Table



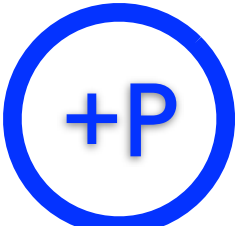
*Only Requirements: Associative, **0**-identity*

Hierarchical Flow Table

 *In node*

 *Sibling*

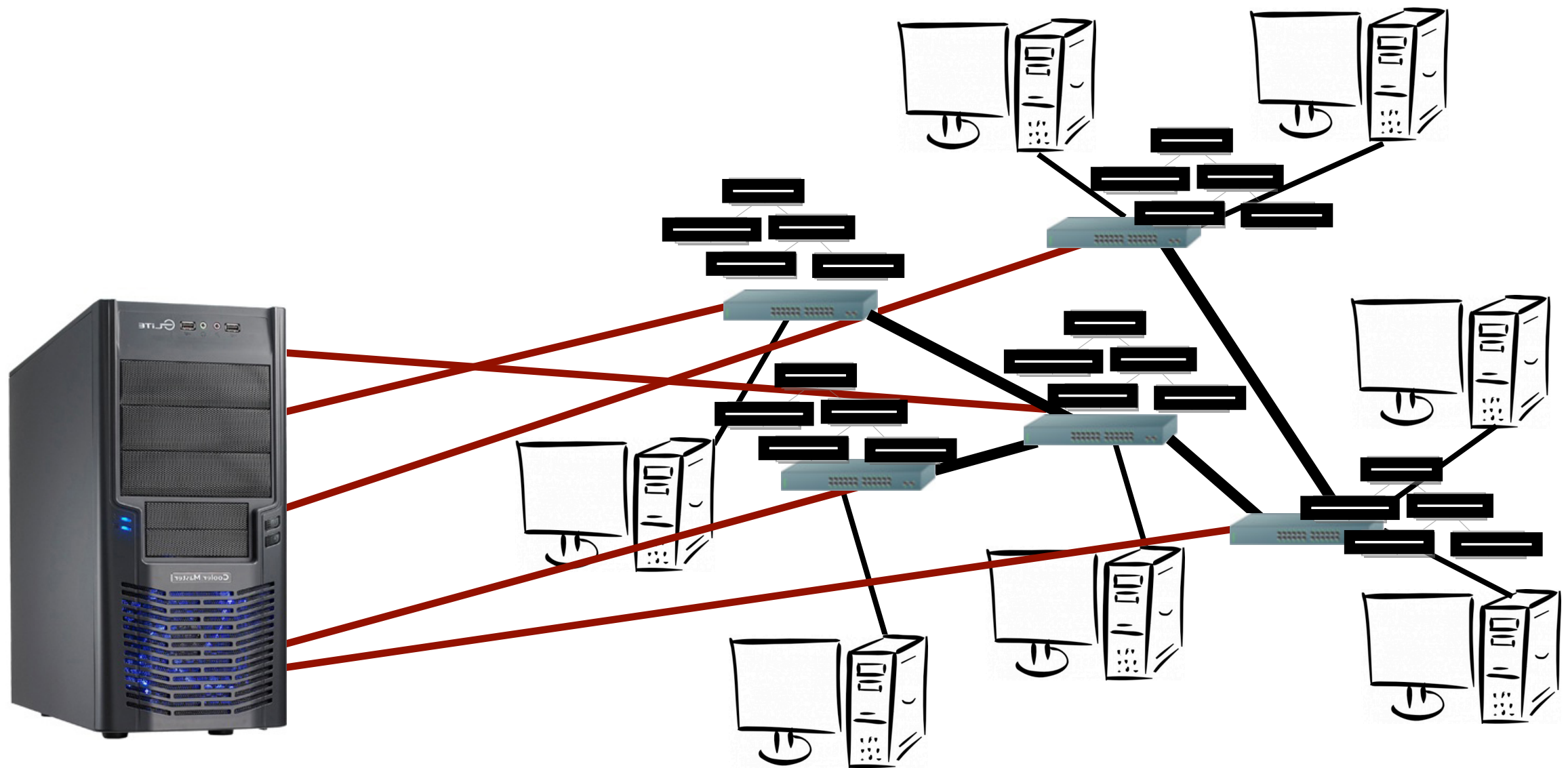
D and S identical.
Deny overrides Allow.
GMB combines as **max**

 *Parent-Sibling*

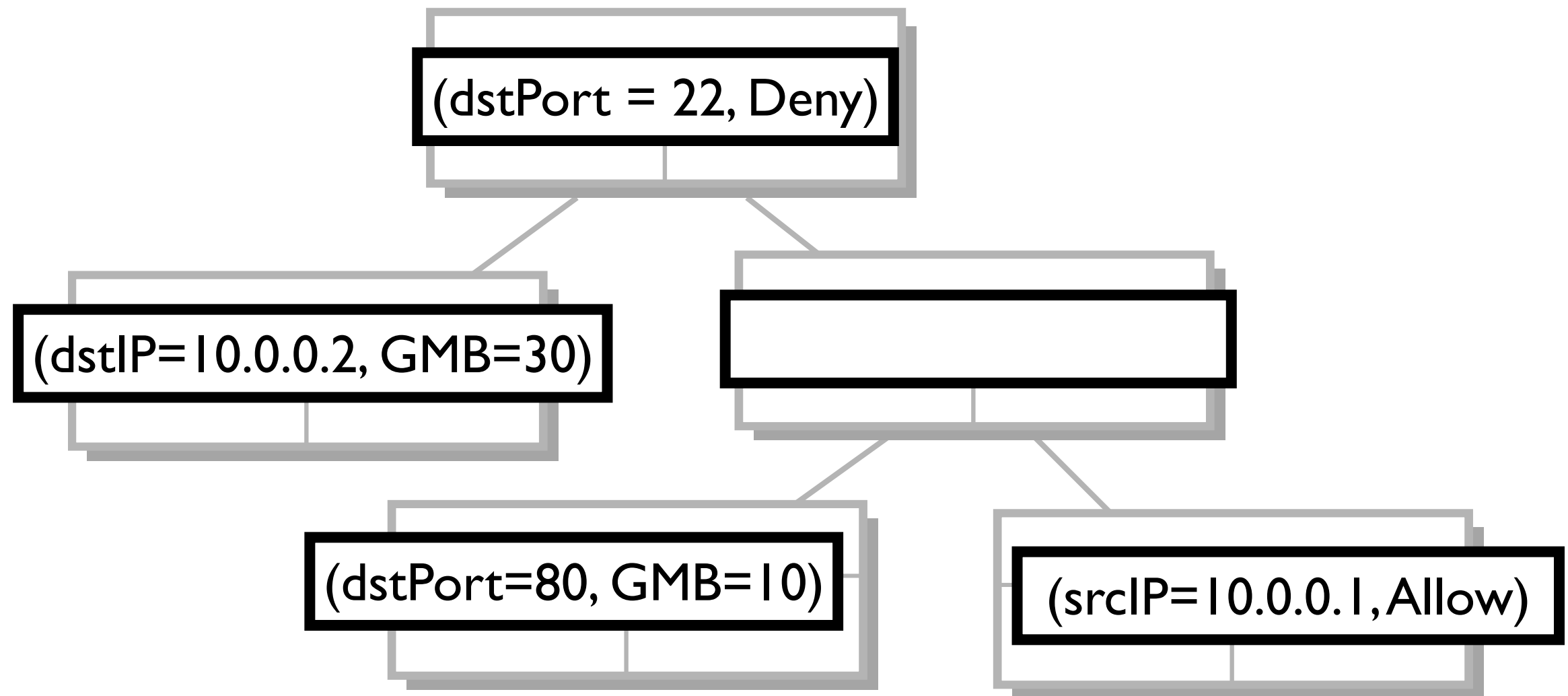
Child overrides Parent
for Access Control
GMB combines as **max**

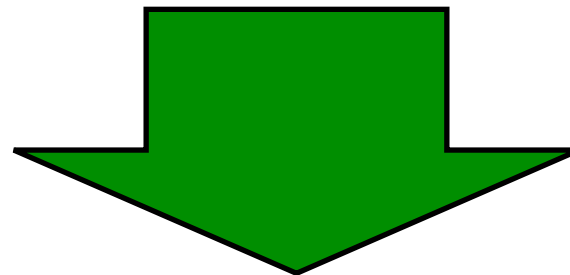
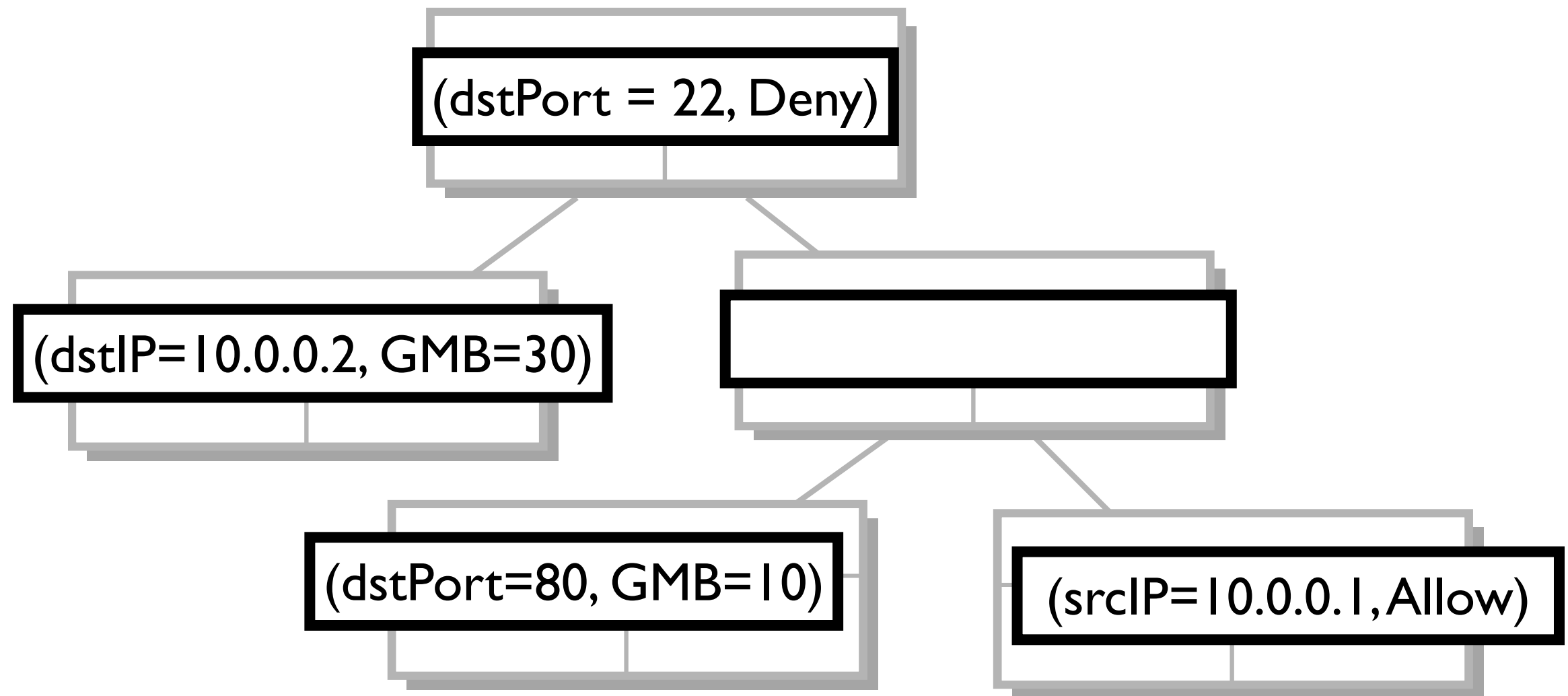
PANE's HFT Operators

Implementation



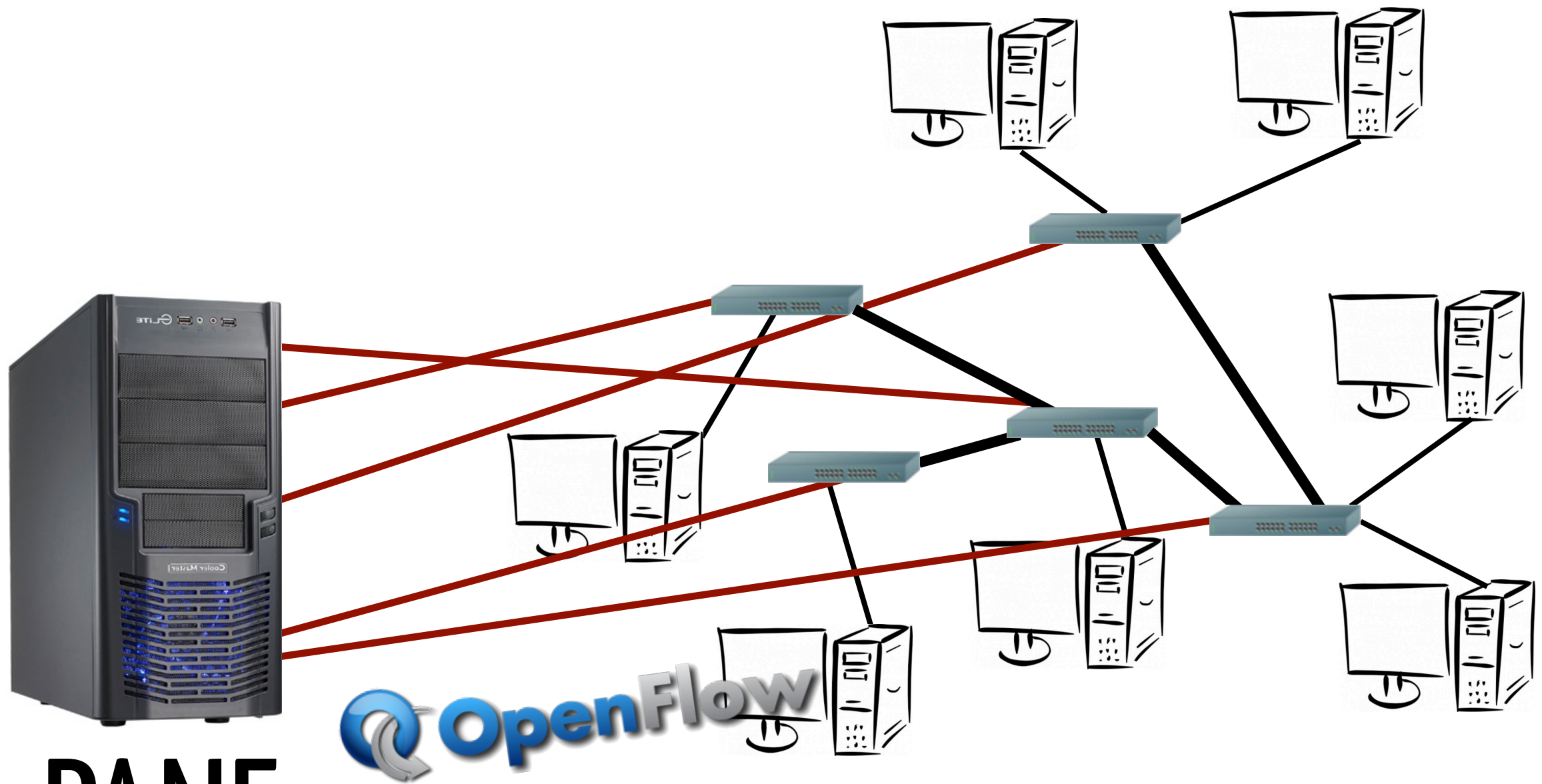
PANE



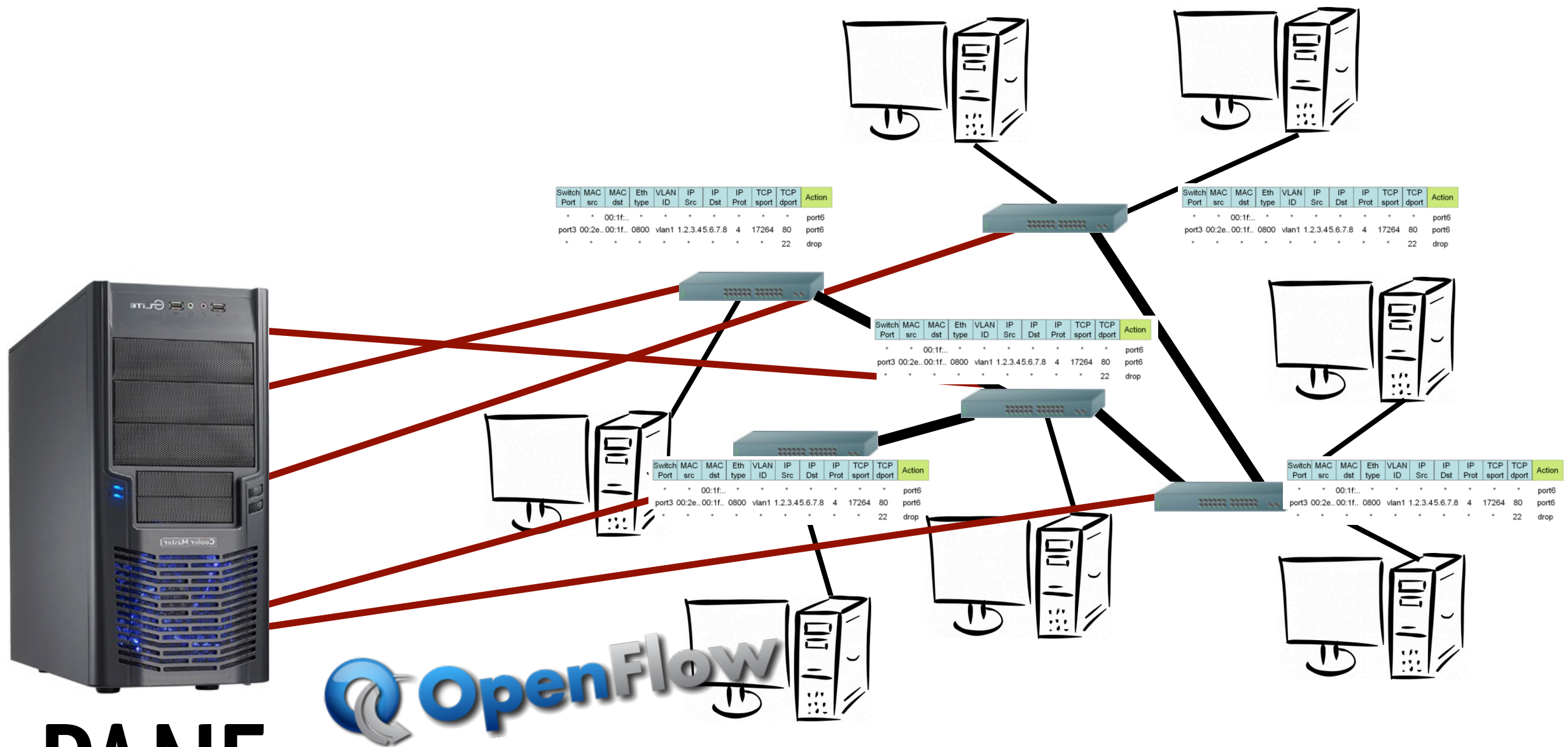


Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	00:1f:...	*	*	*	*	*	*	*	port6
port3	00:2e:..	00:1f:..	0800	vlan1	1.2.3.4	5.6.7.8	4	17264	80	port6
*	*	*	*	*	*	*	*	*	22	drop



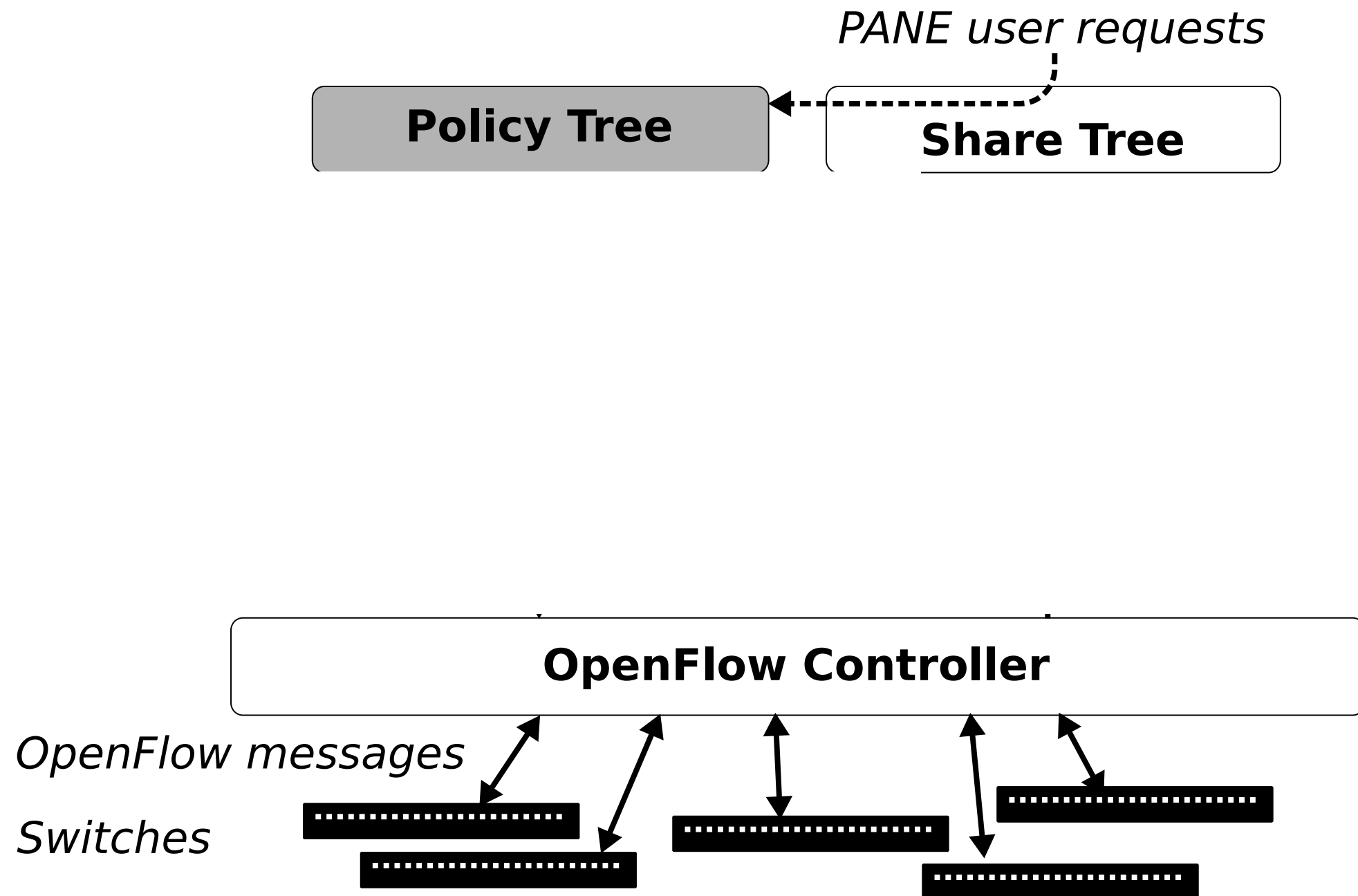


PANE

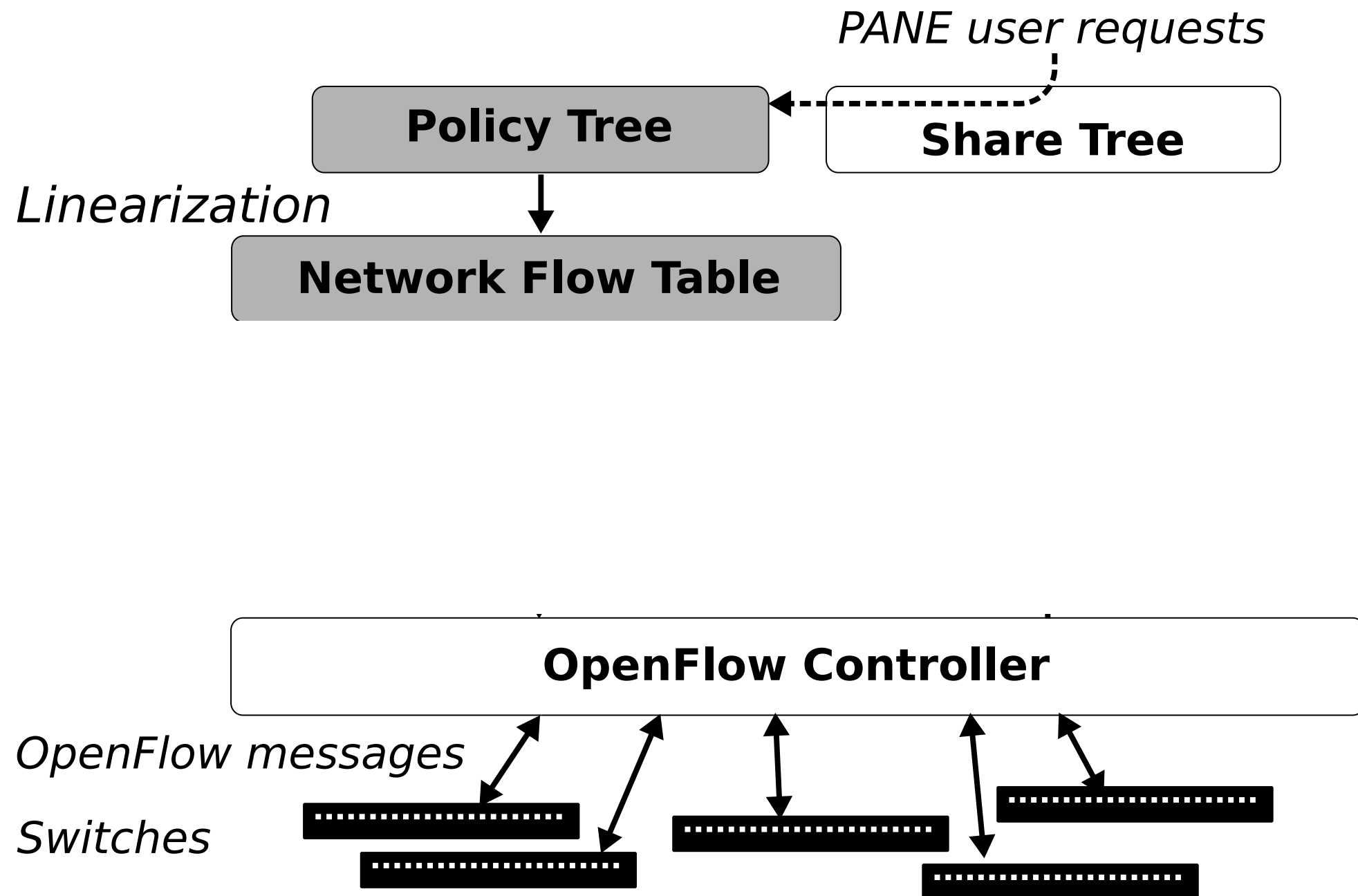


PANE

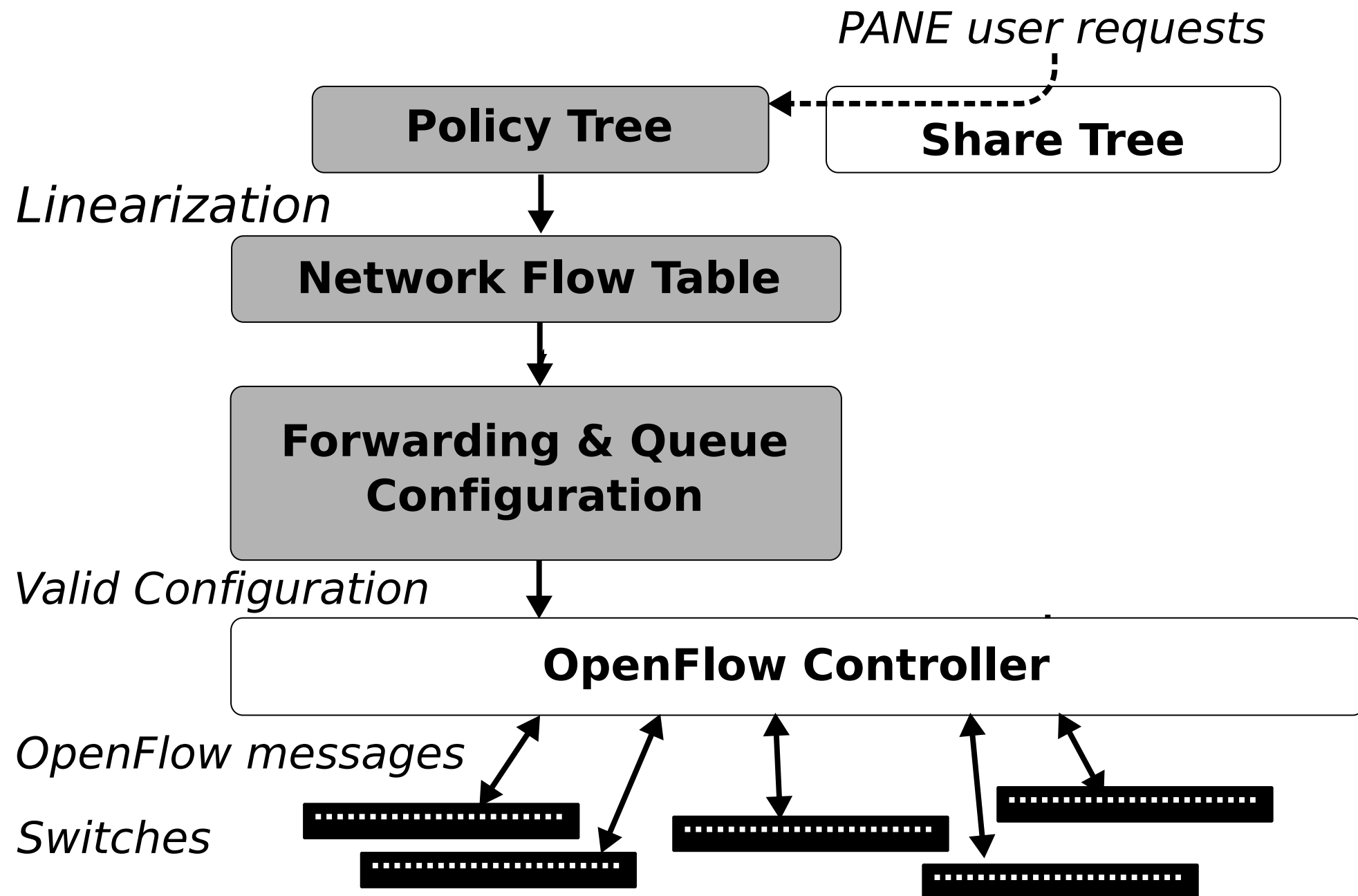
PANE



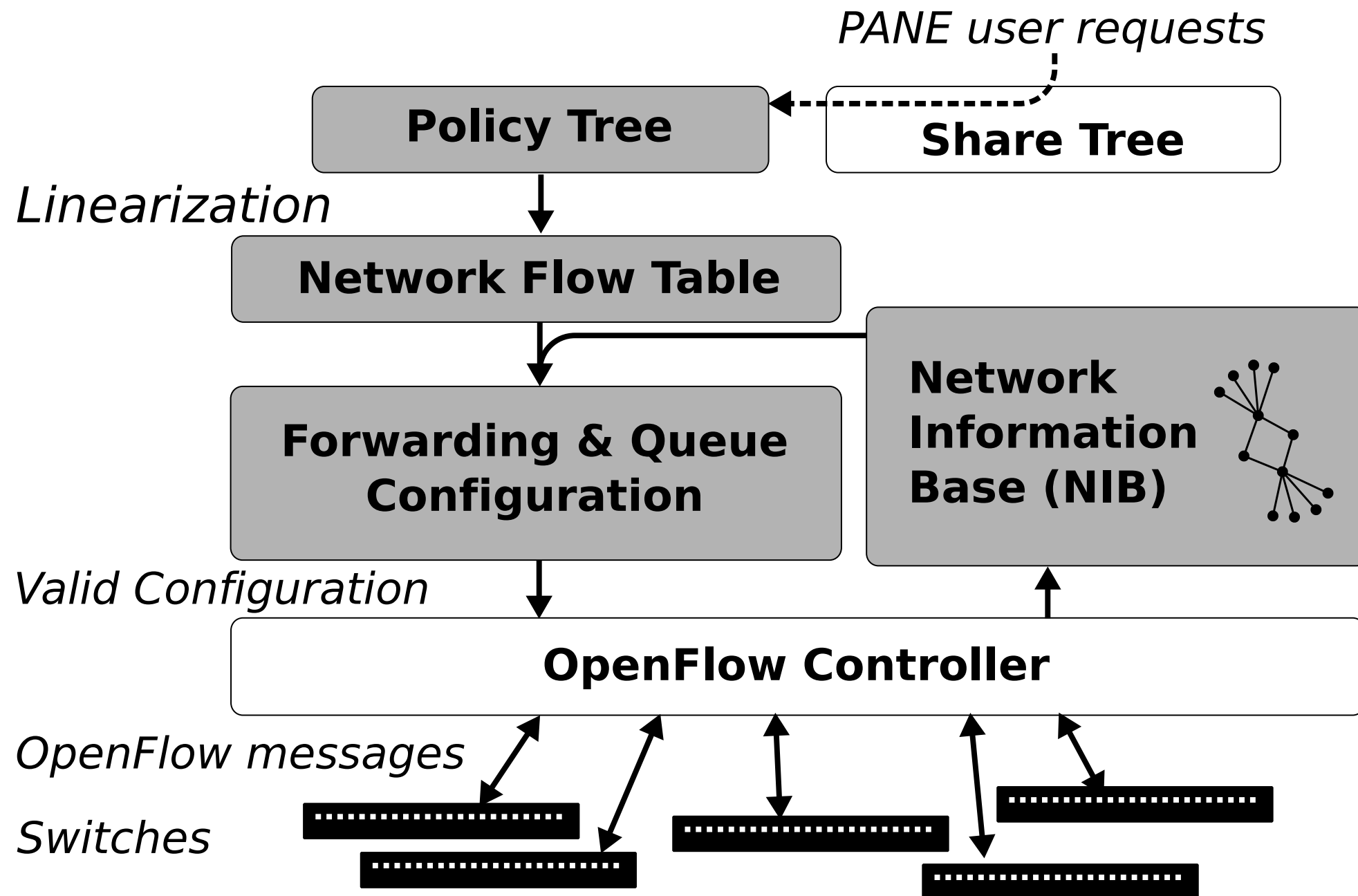
PANE

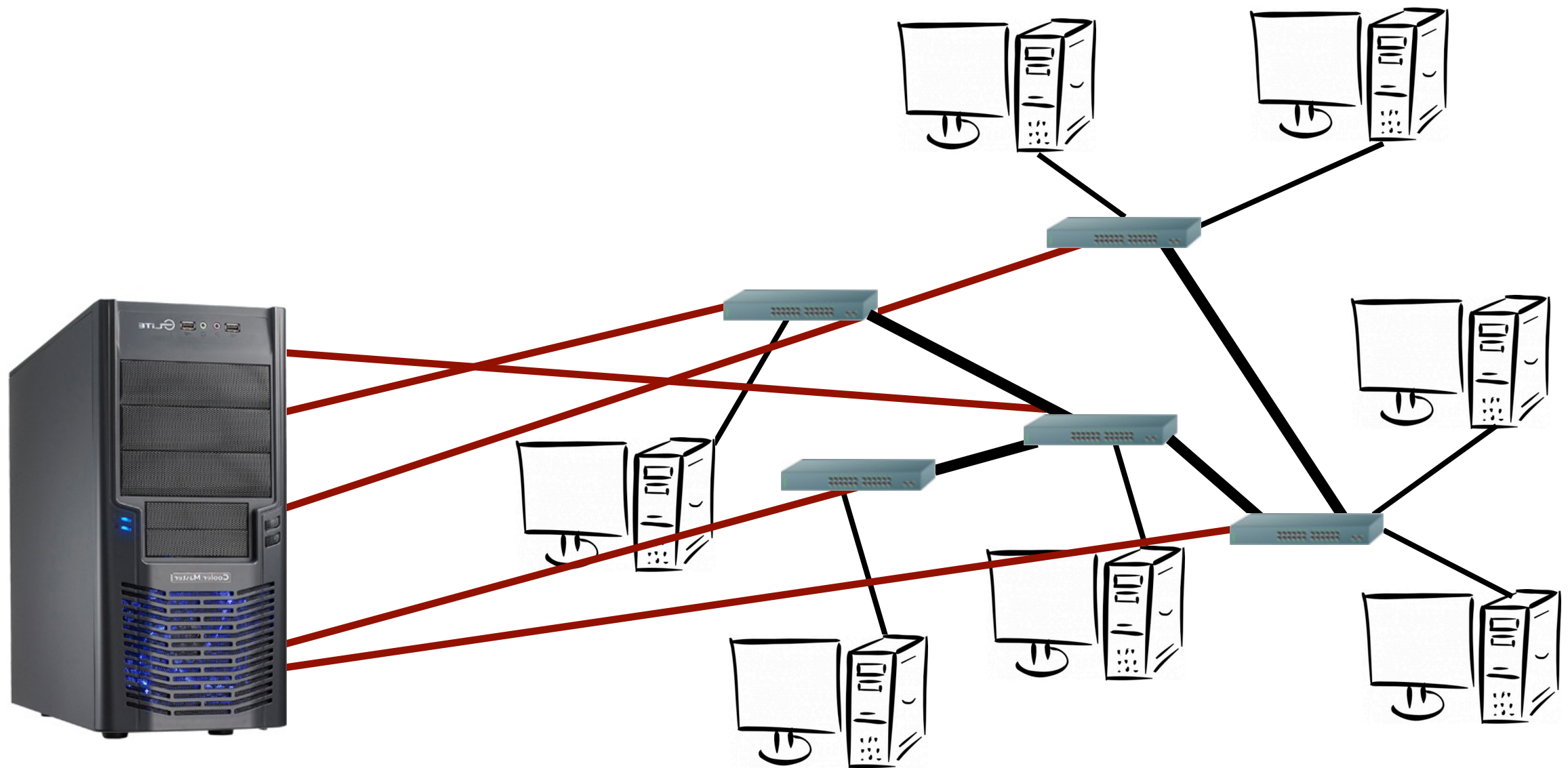


PANE

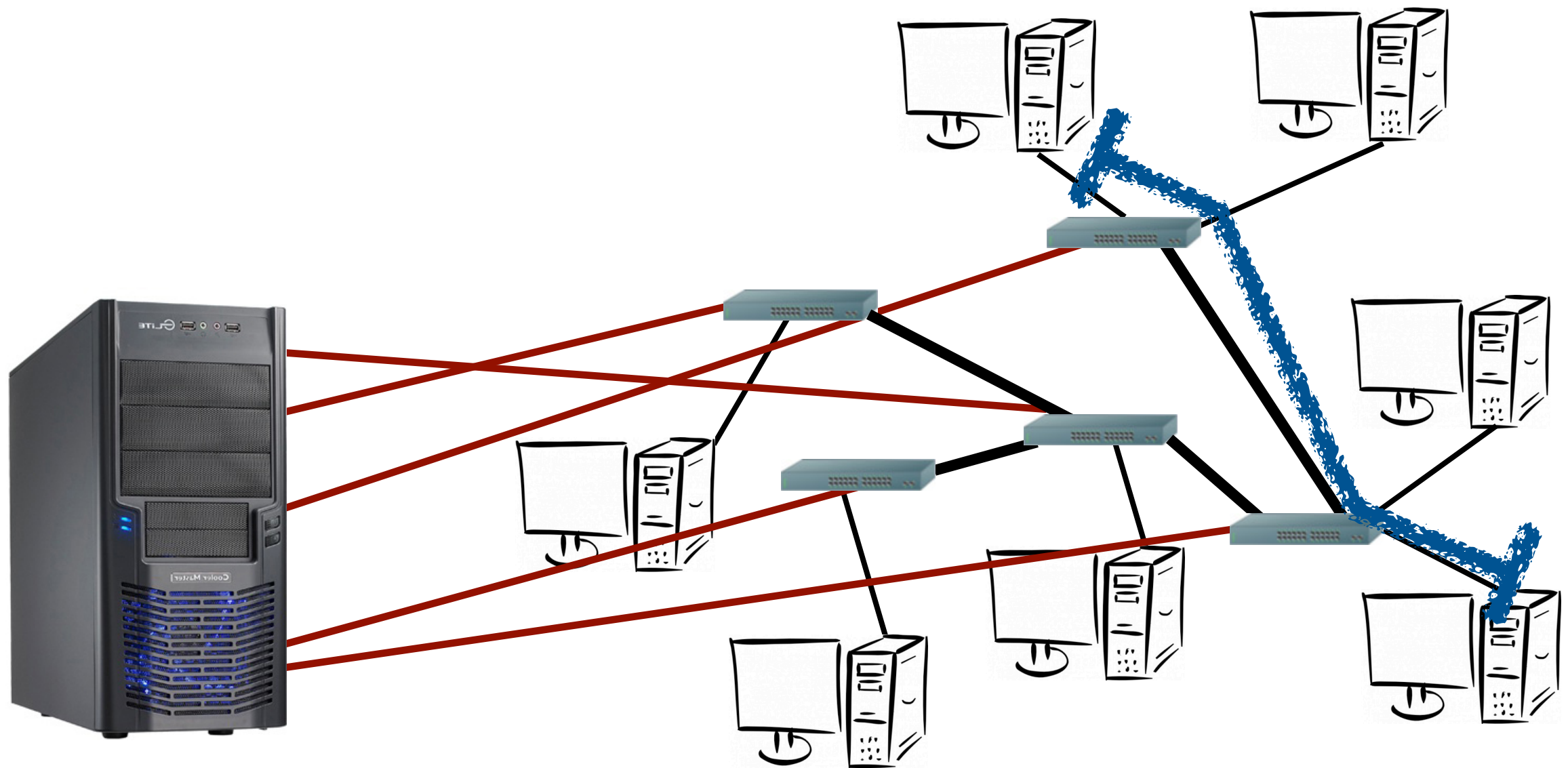


PANE

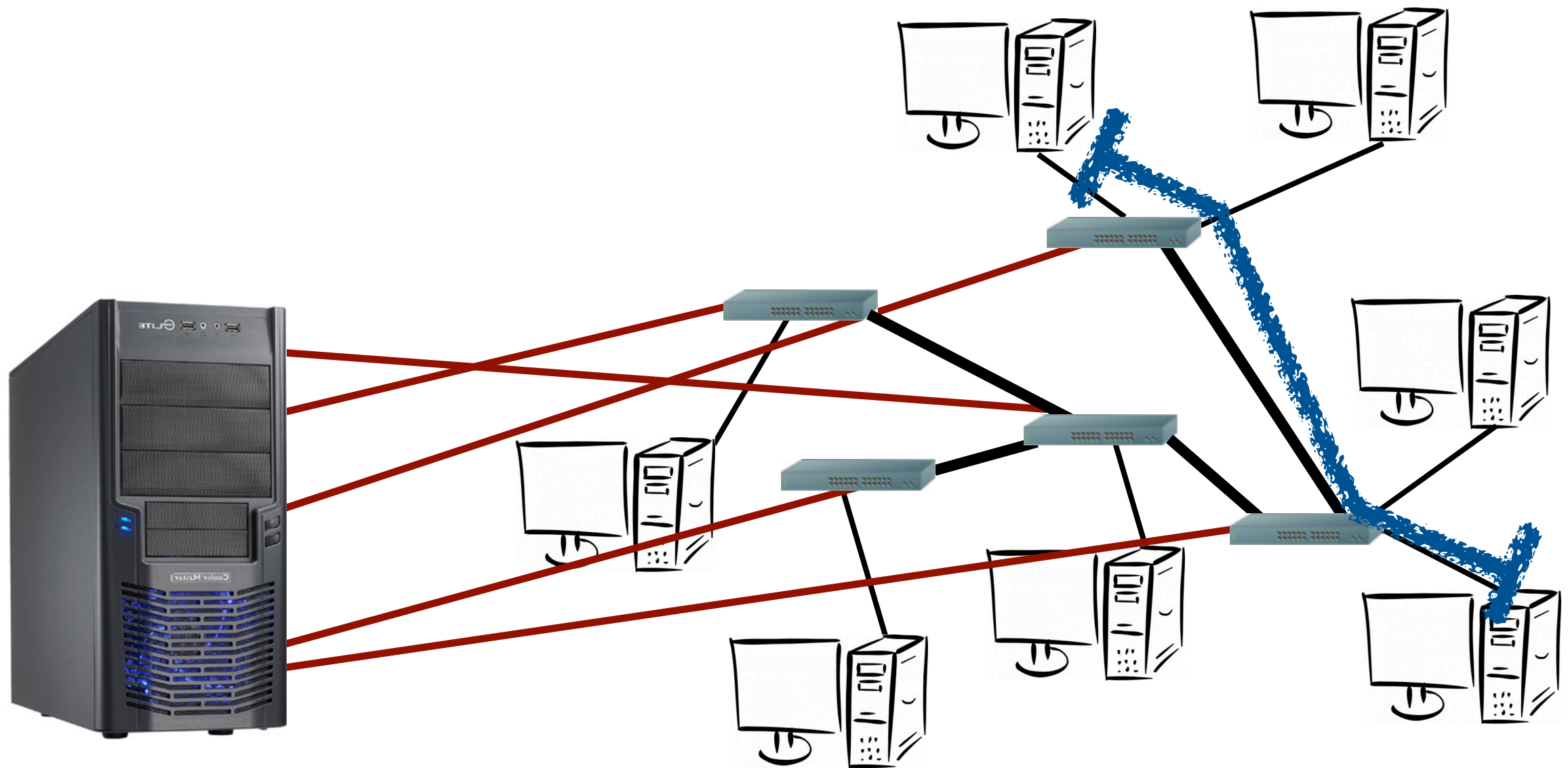




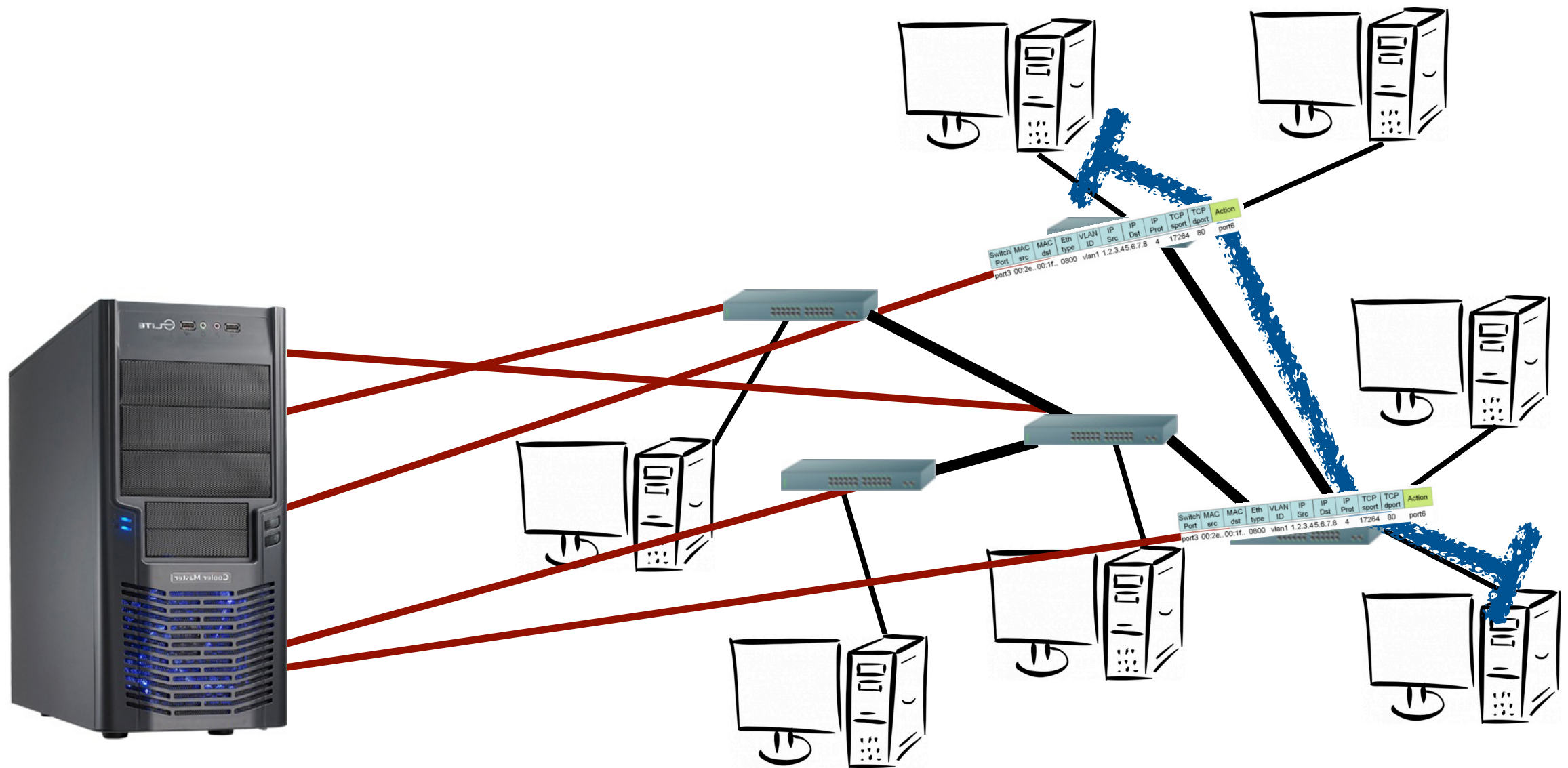
PANE



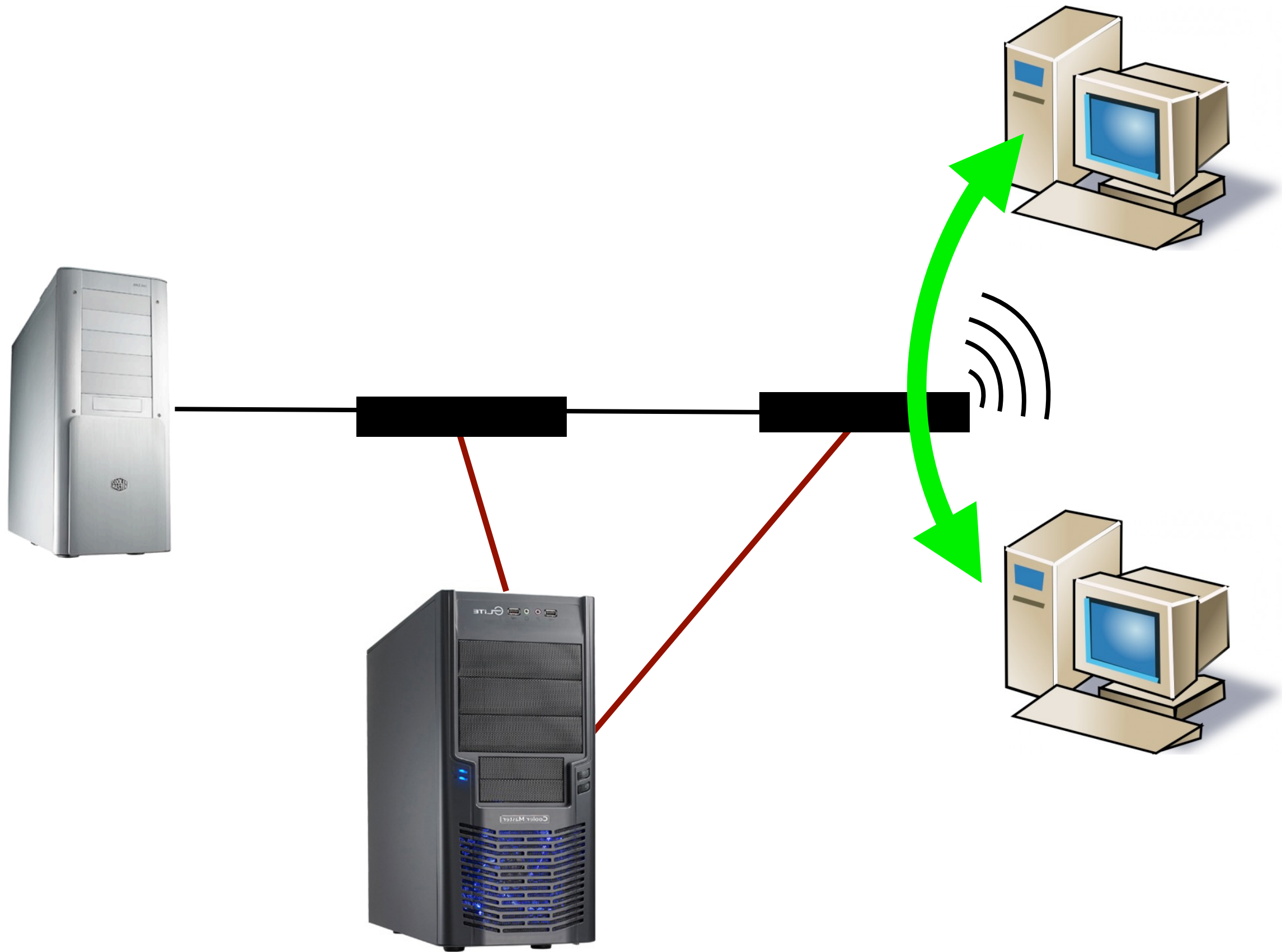
PANE



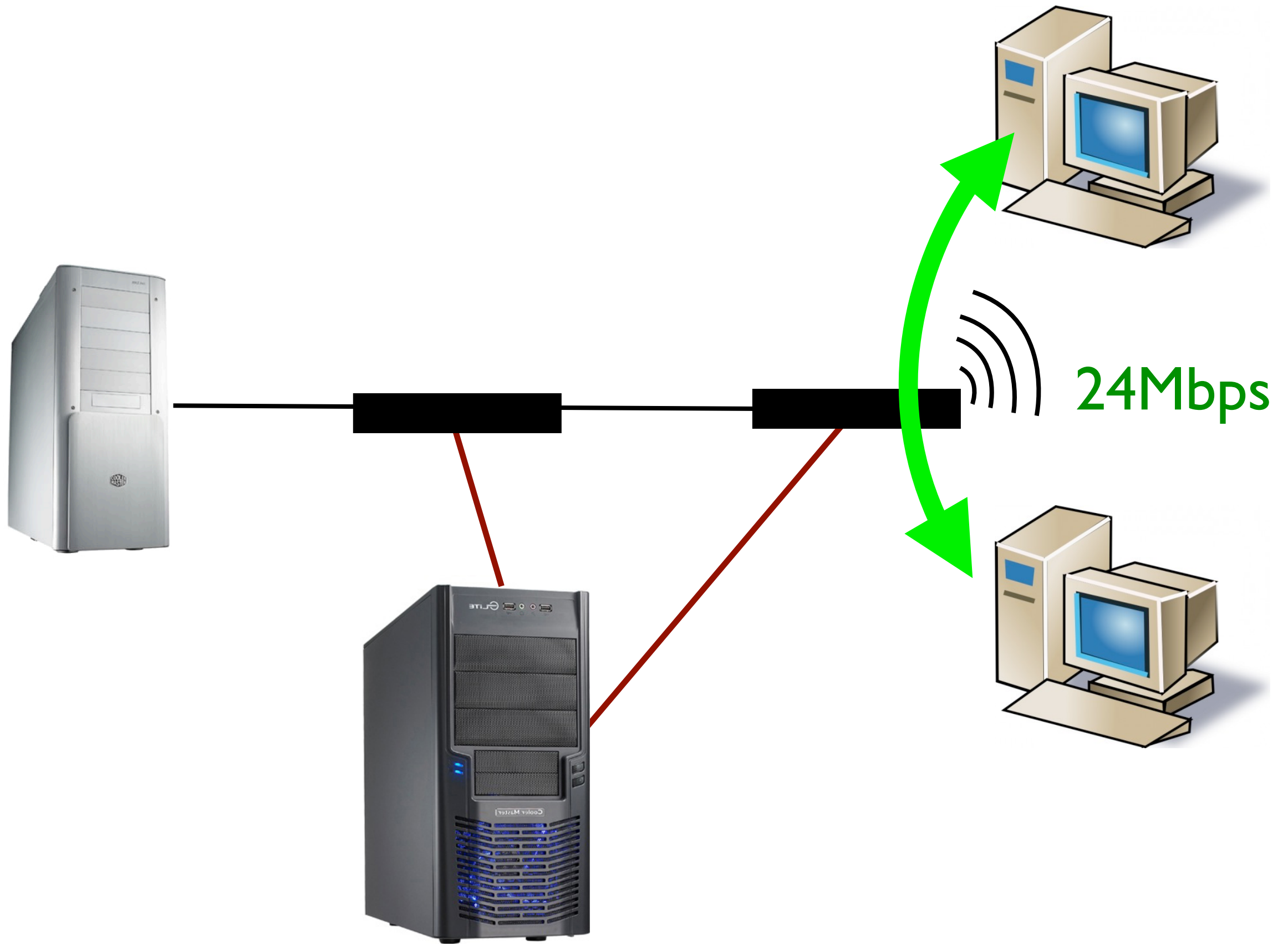
PANE



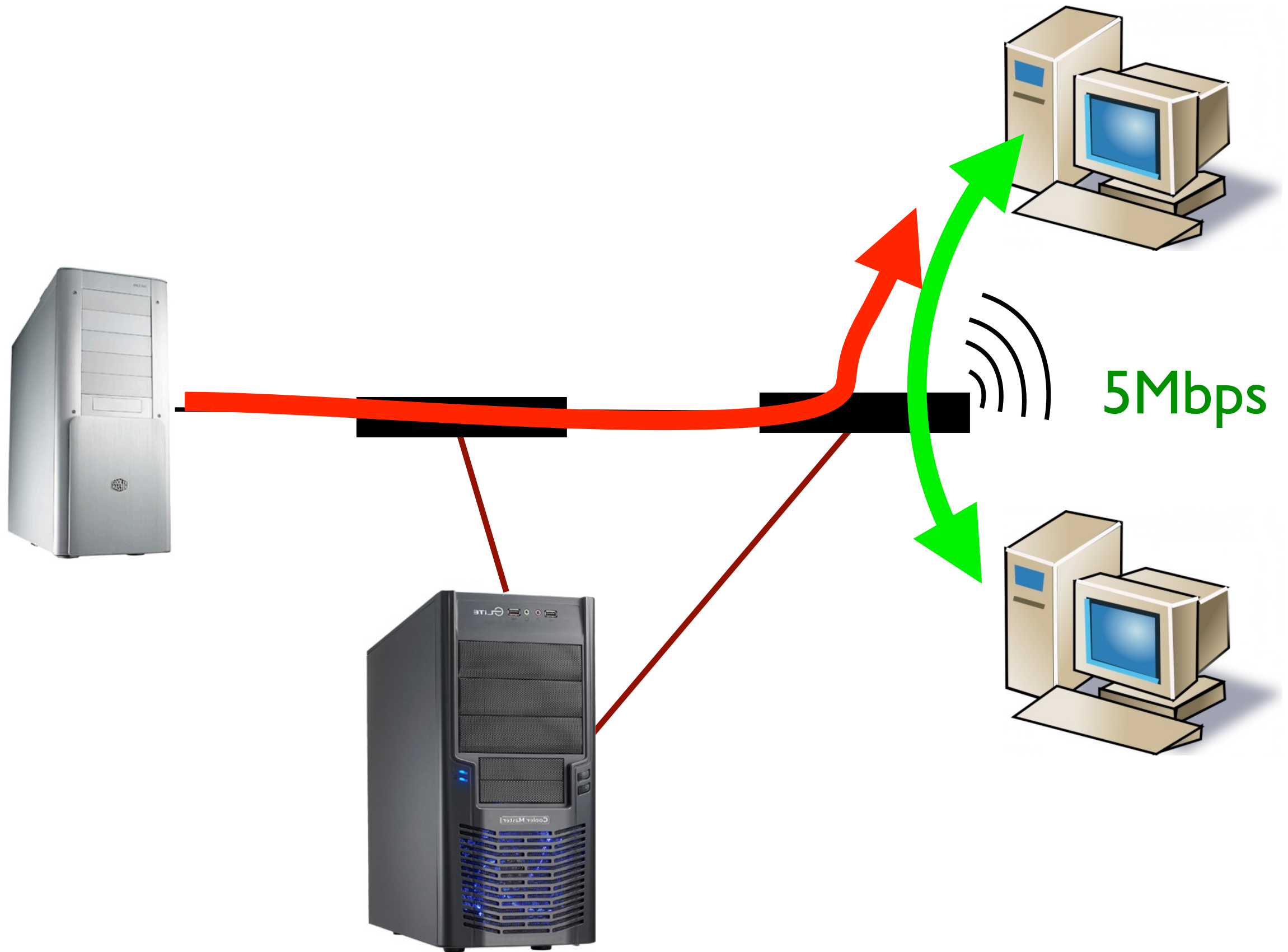
PANE



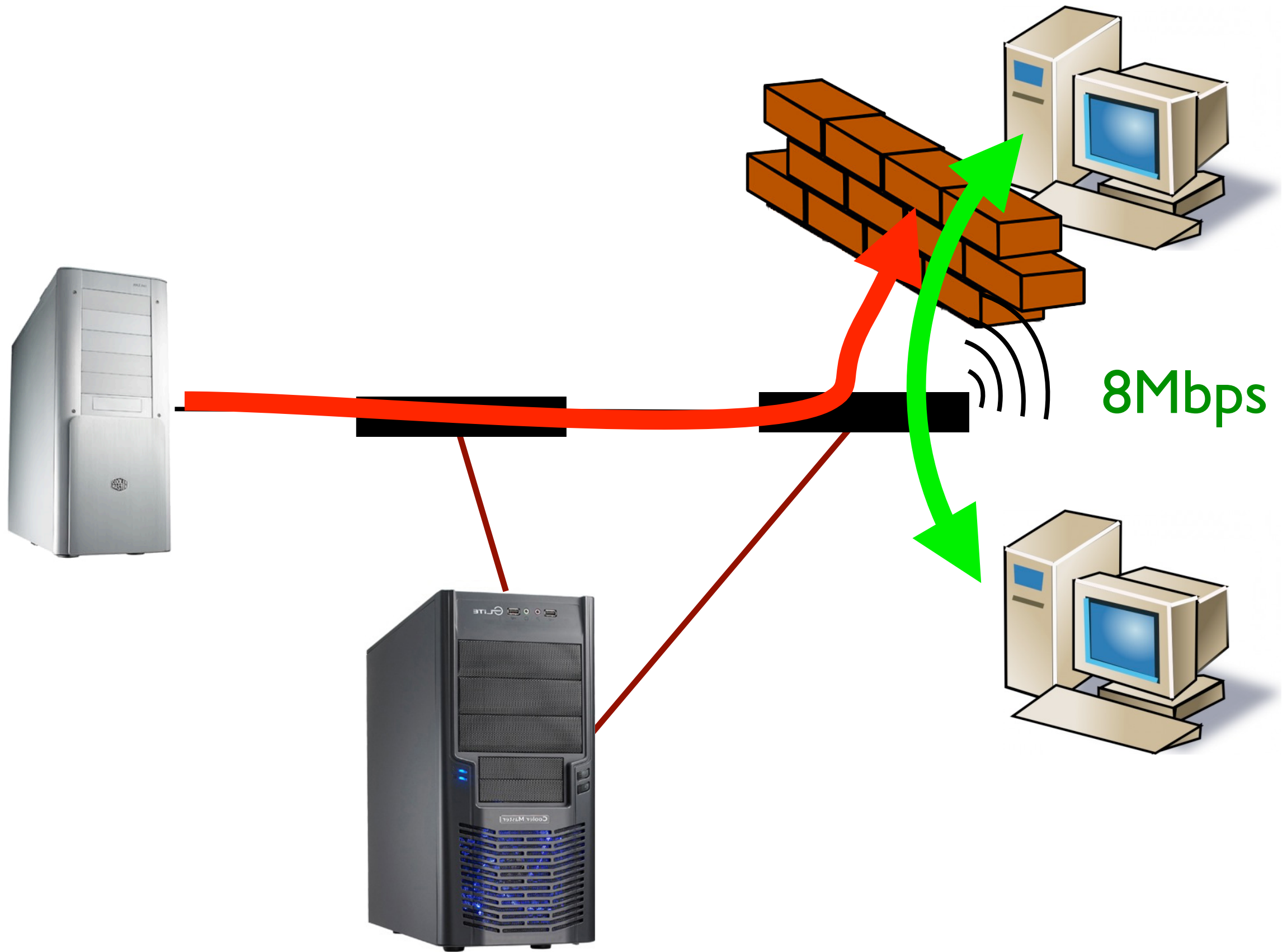
PANE



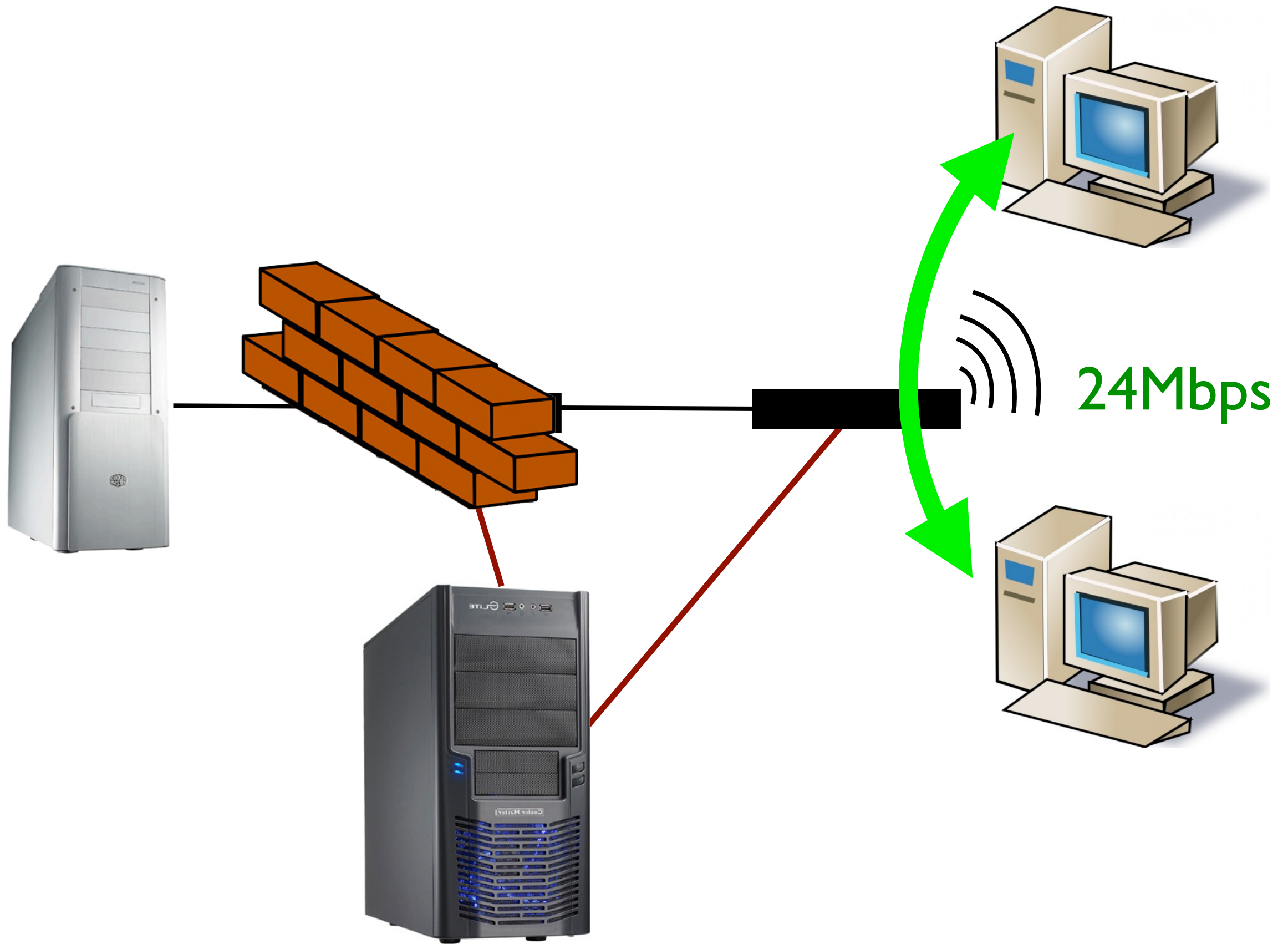
PANE



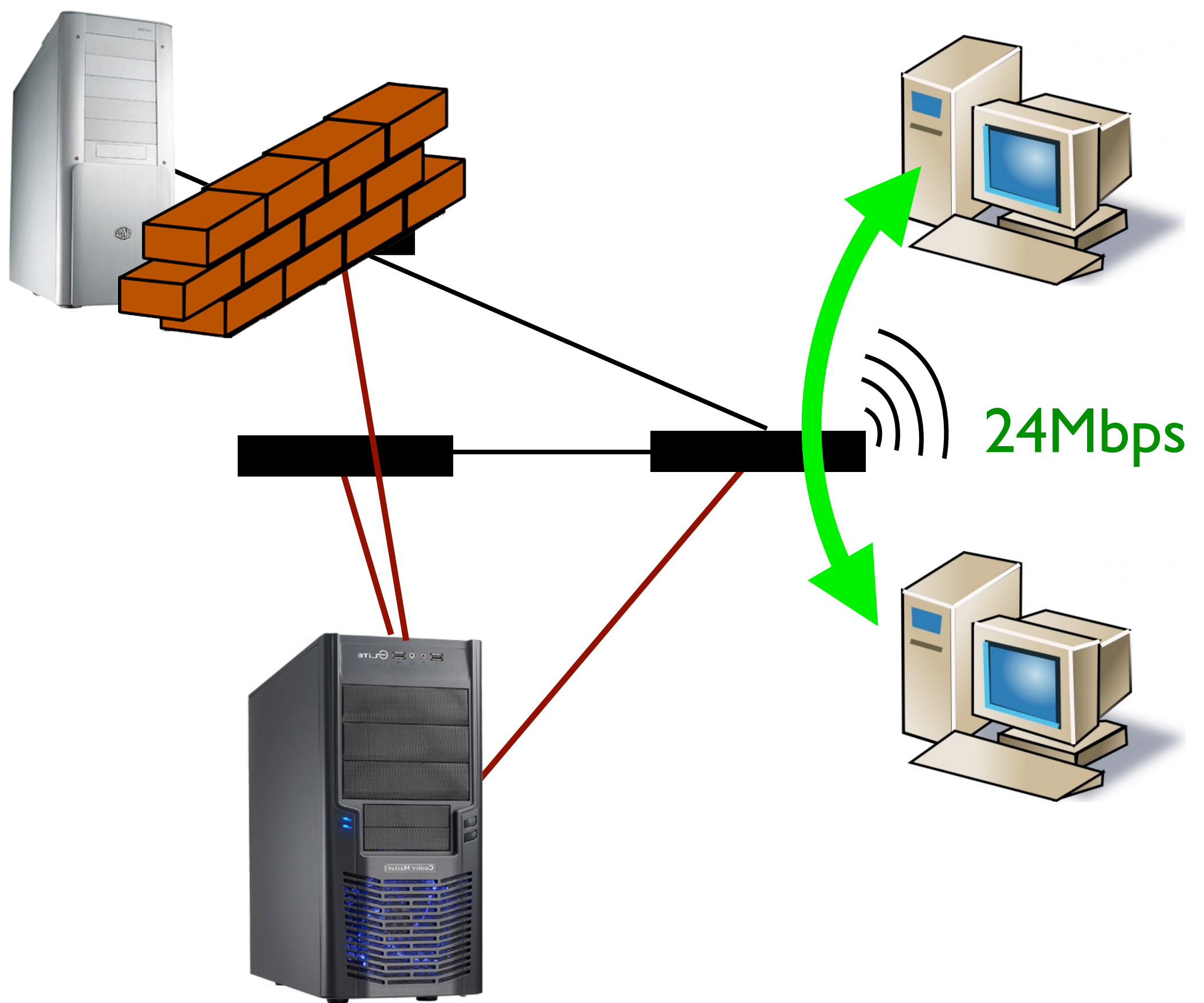
PANE



PANE

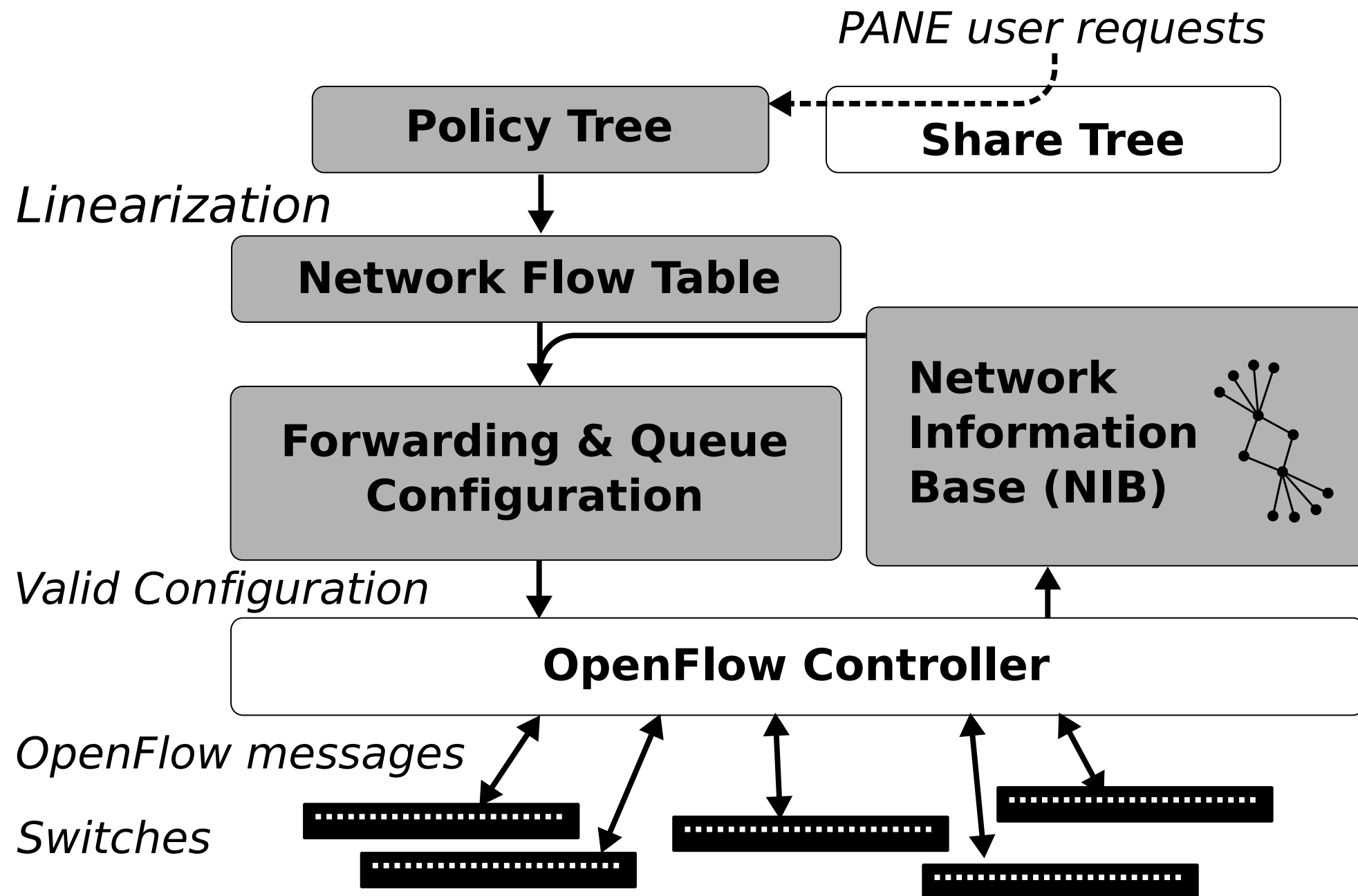


PANE

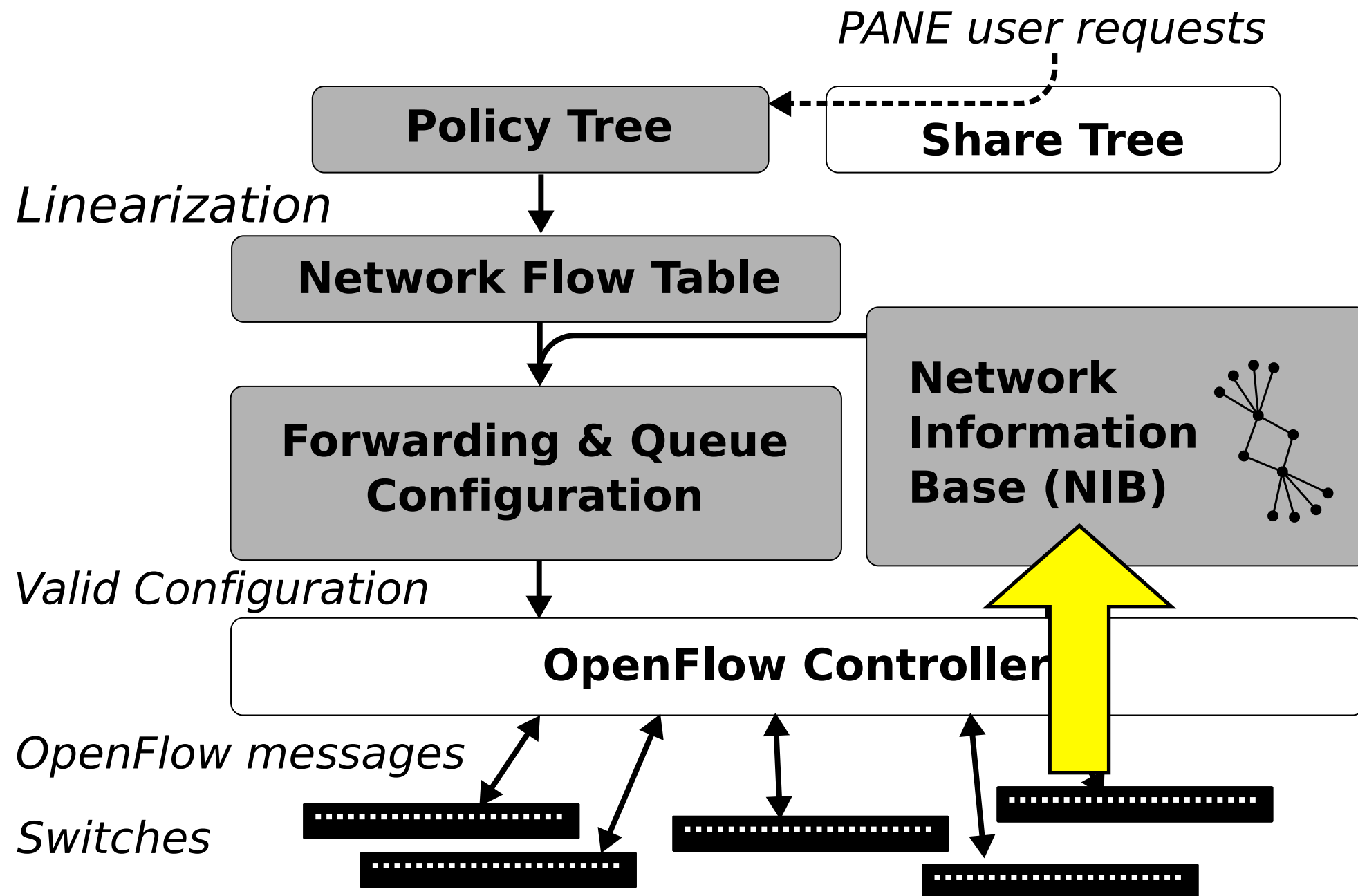


PANE

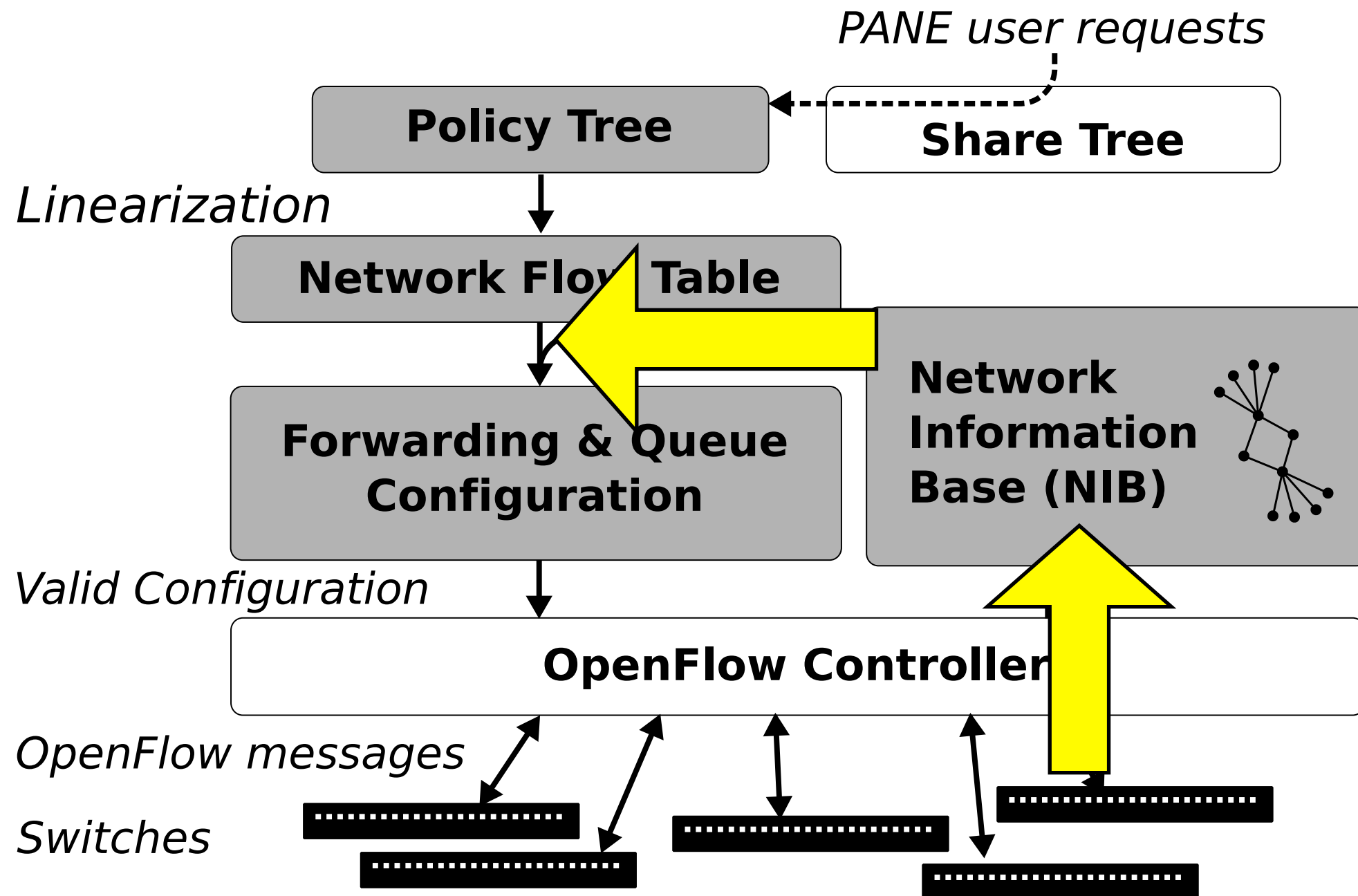
PANE



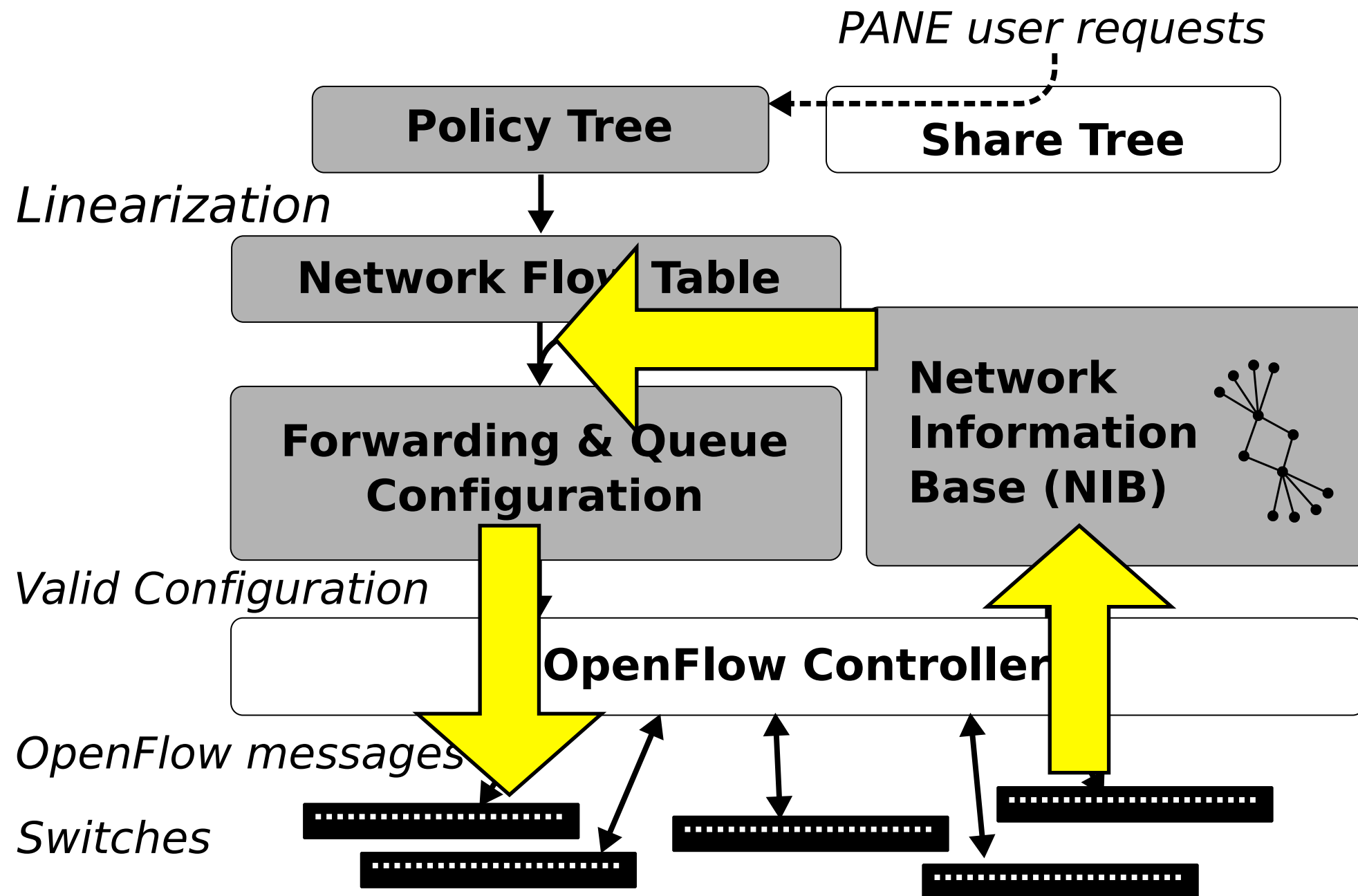
PANE



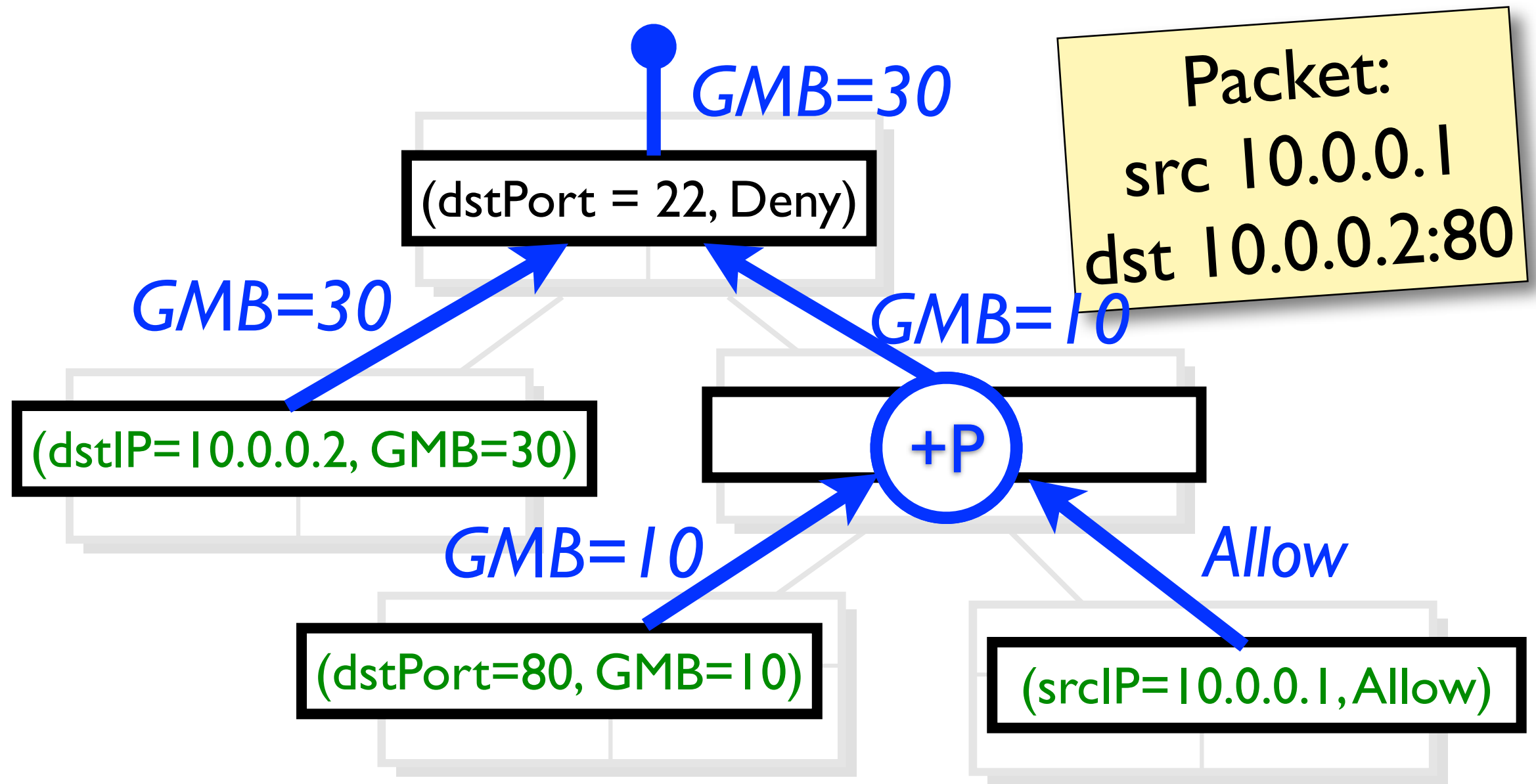
PANE



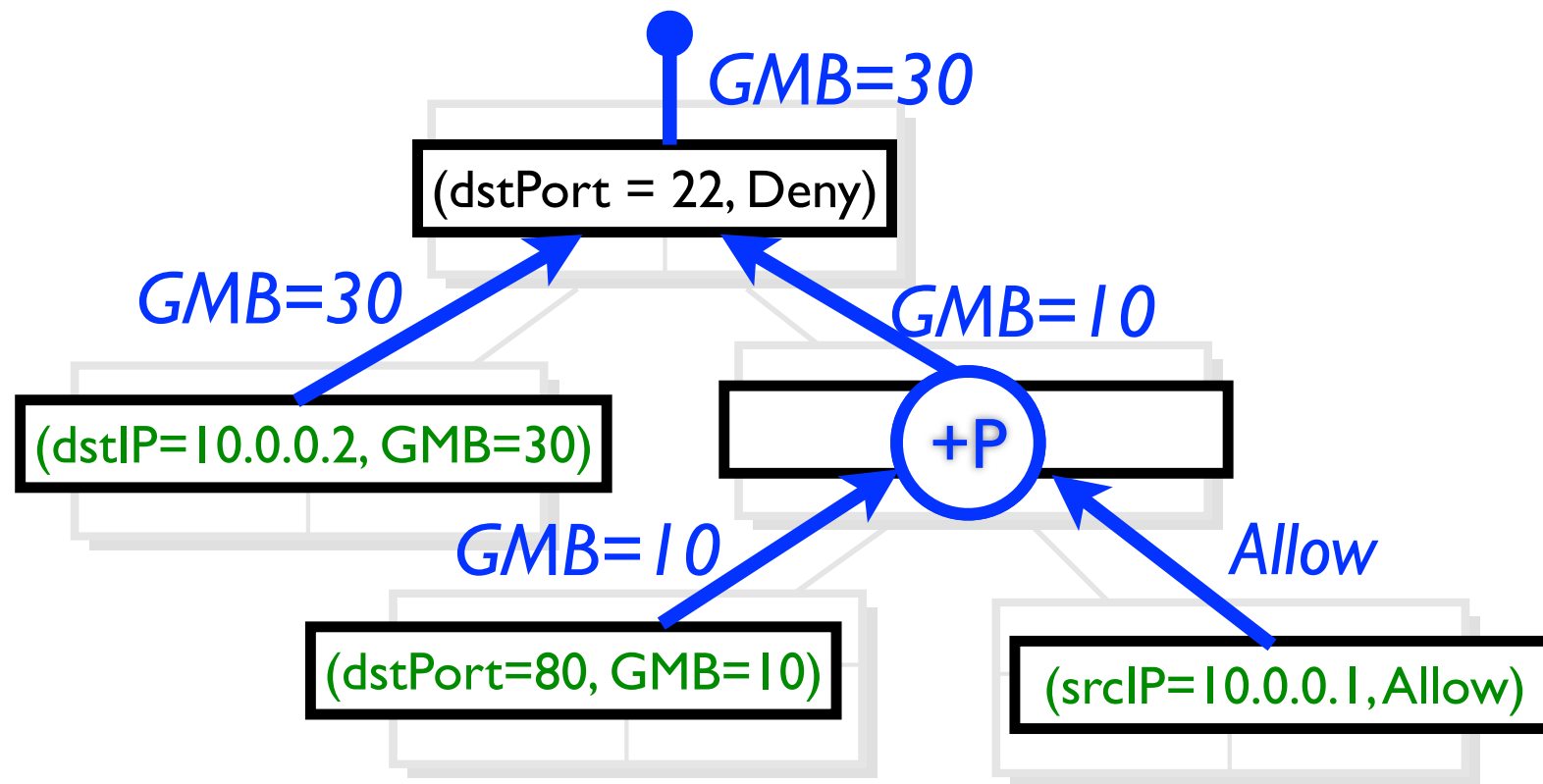
PANE



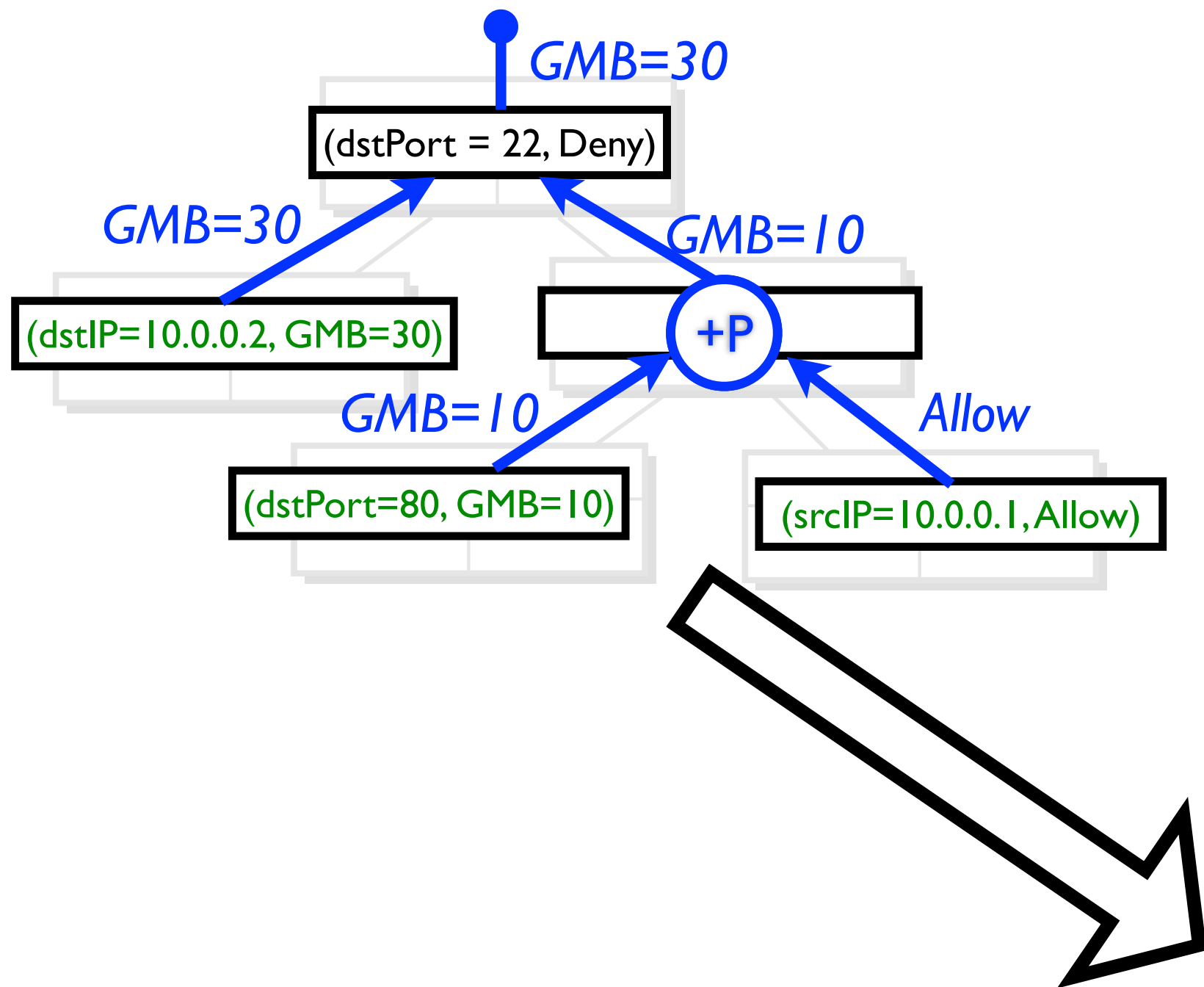
Proof of Correctness



Hierarchical Flow Tables

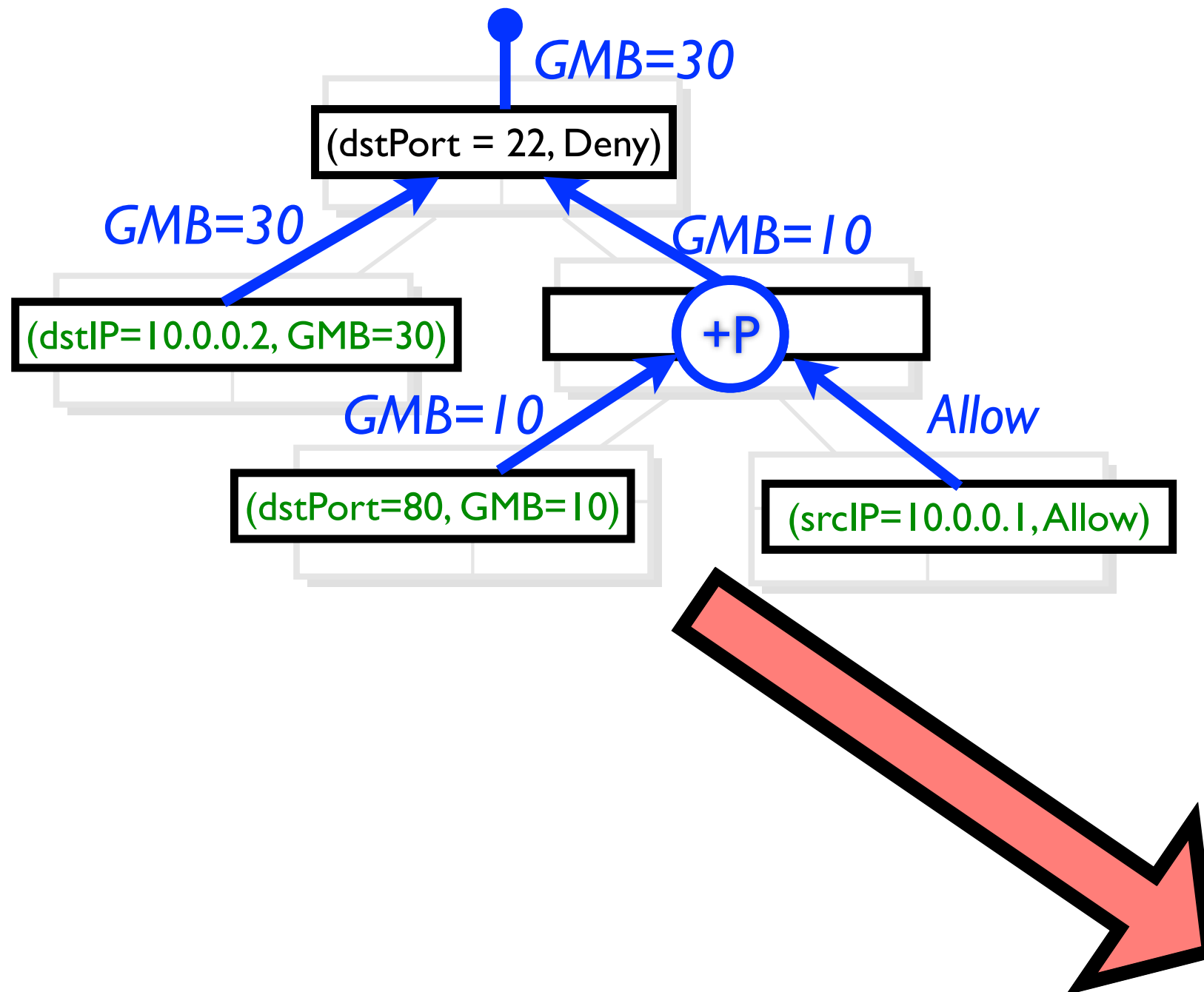


Compiler Correctness



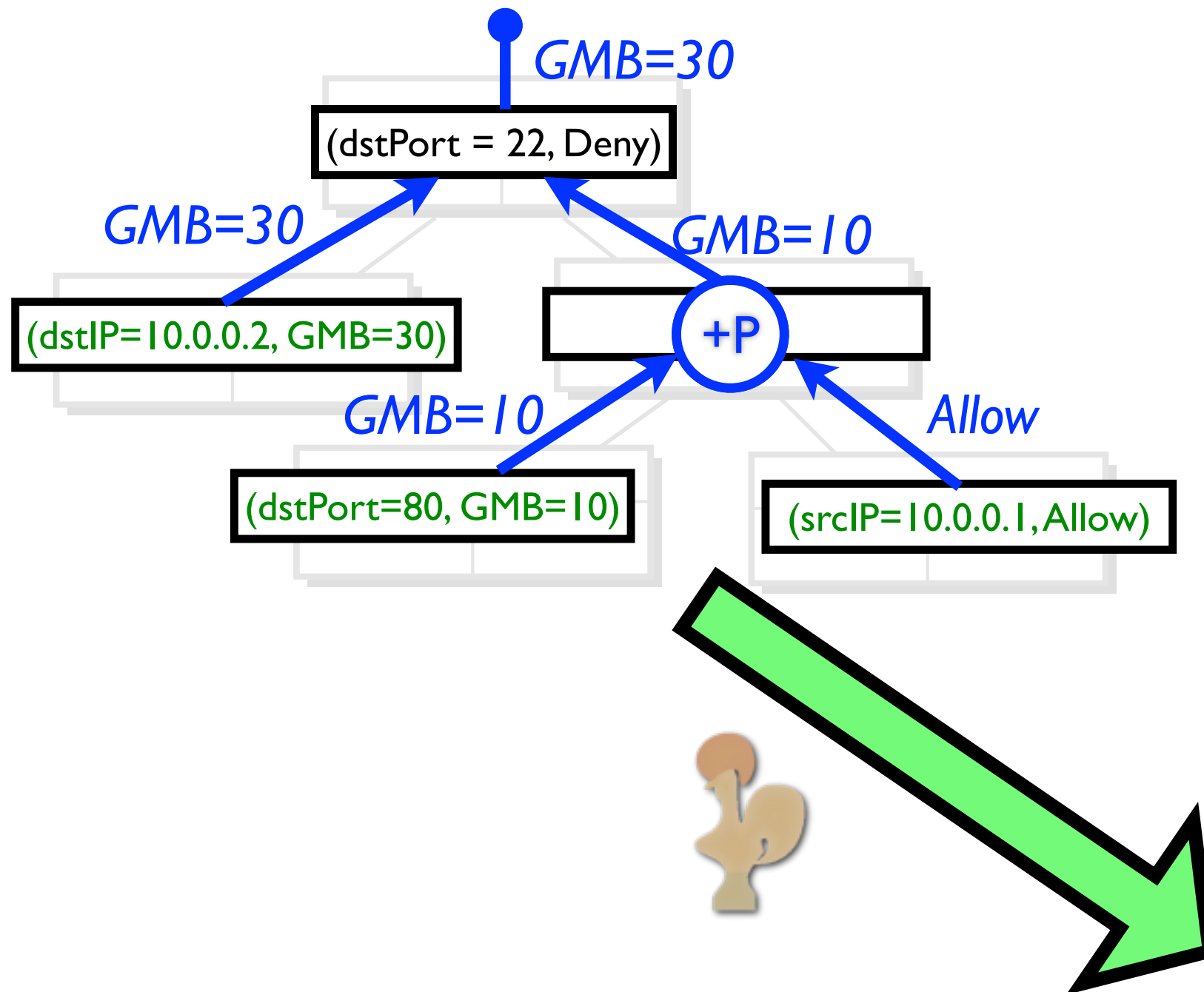
Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	00:1f:...	*	*	*	*	*	*	*	port6
port3	00:2e:..	00:1f:..	0800	vlan1	1.2.3.4	5.6.7.8	4	17264	80	port6
*	*	*	*	*	*	*	*	*	22	drop

Compiler Correctness



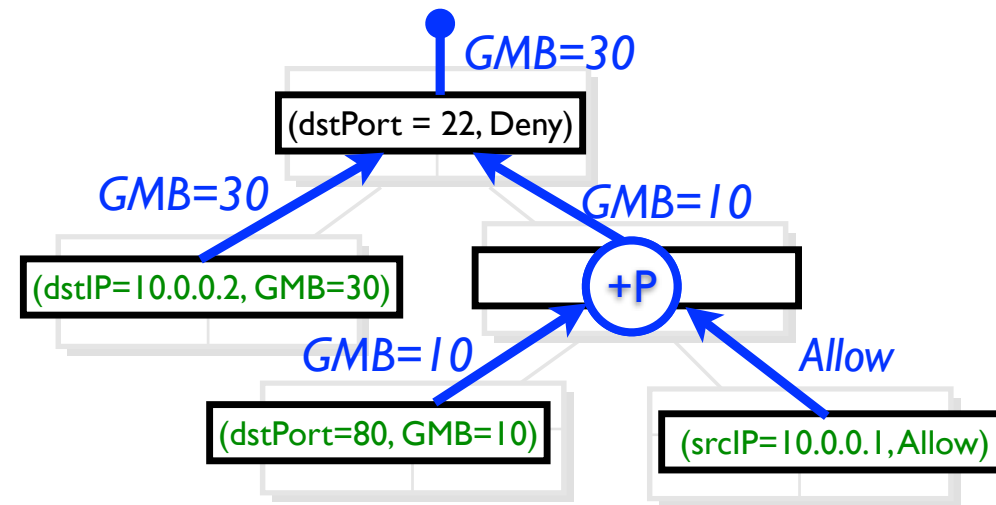
Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	00:1f:...	*	*	*	*	*	*	*	port6
port3	00:2e:..	00:1f:..	0800	vlan1	1.2.3.4	5.6.7.8	4	17264	80	port6
*	*	*	*	*	*	*	*	*	22	drop

Compiler Correctness



Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	00:1f:...	*	*	*	*	*	*	*	port6
port3	00:2e:..	00:1f:..	0800	vlan1	1.2.3.4	5.6.7.8	4	17264	80	port6
*	*	*	*	*	*	*	*	*	22	drop

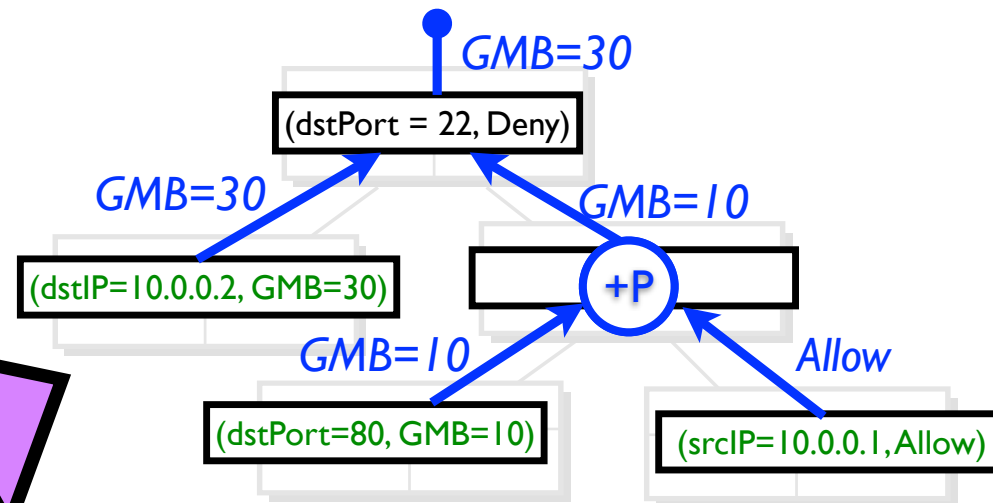
Coq Proof Assistant



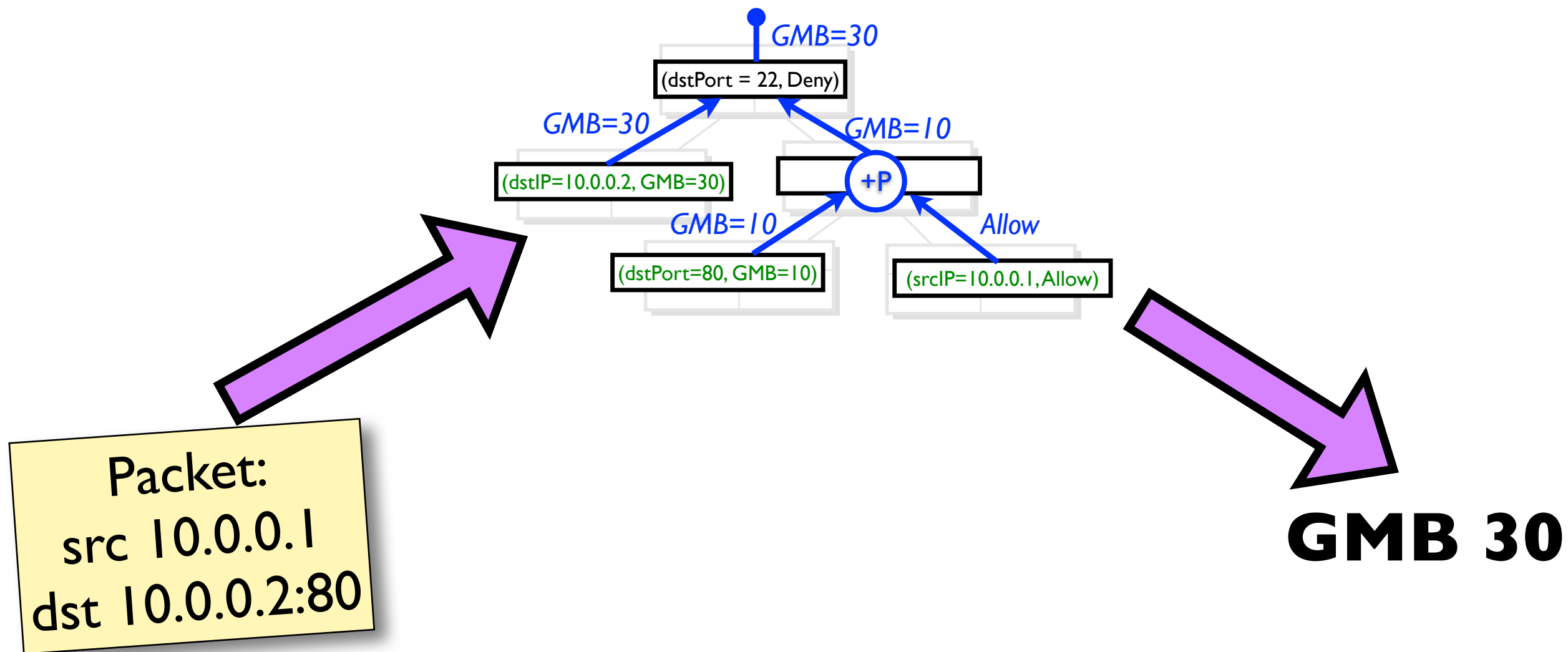
Packet:
src 10.0.0.1
dst 10.0.0.2:80

Theorem

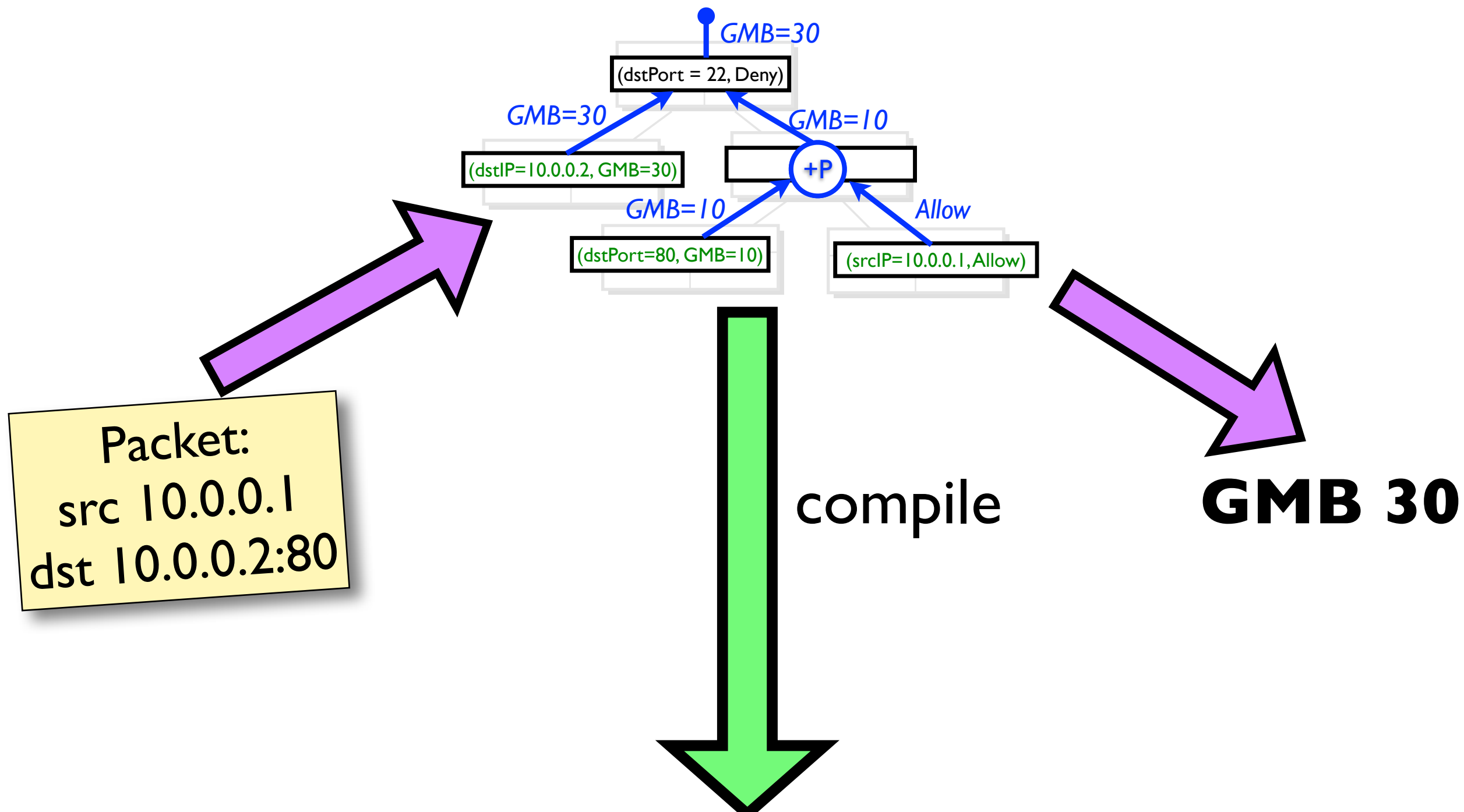
Packet:
src 10.0.0.1
dst 10.0.0.2:80



Theorem

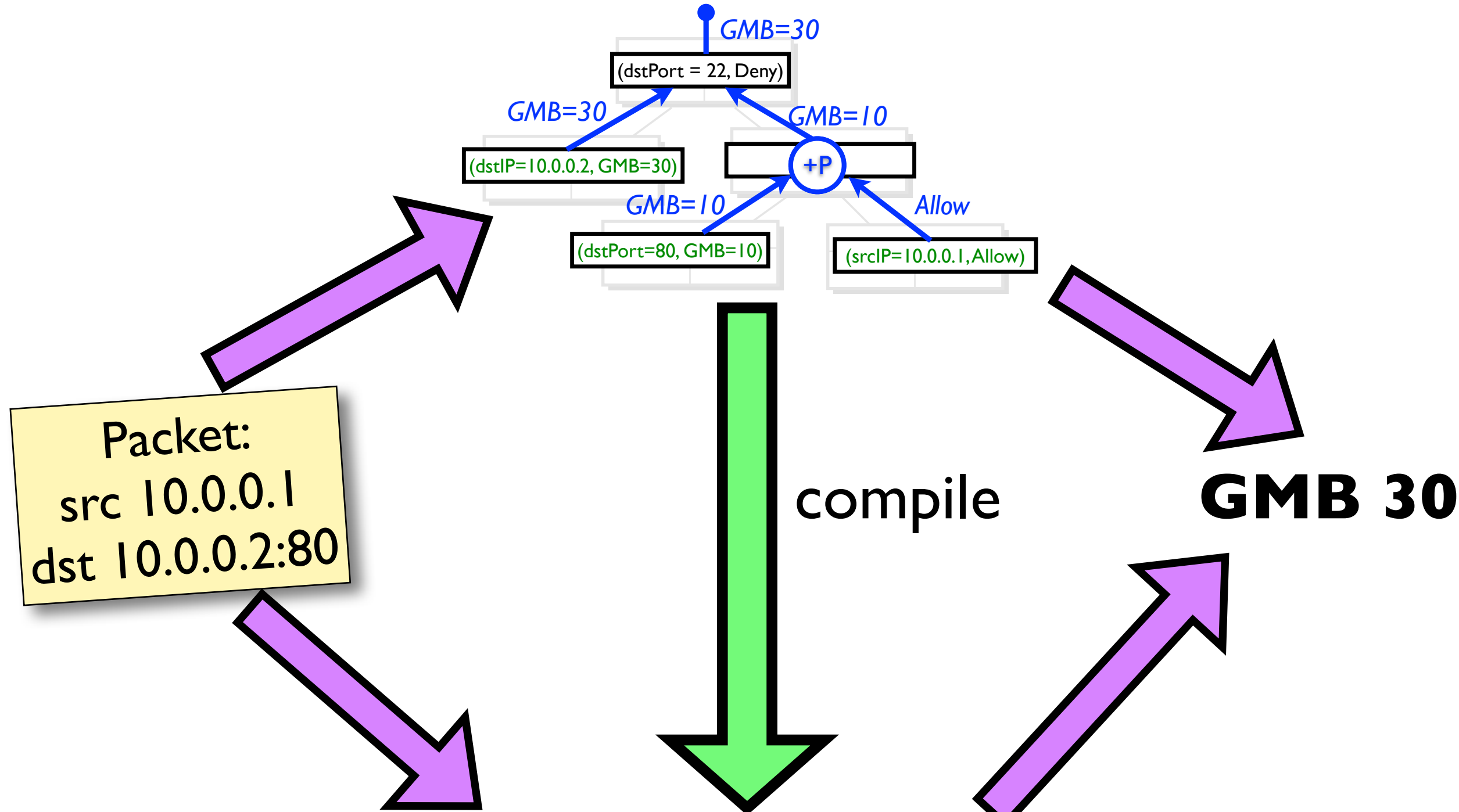


Theorem



Theorem

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	00:1f:..	*	*	*	*	*	*	*	port6
port3	00:2e:..	00:1f:..	0800	vlan1	1.2.3.4	5.6.7.8	4	17264	80	port6
*	*	*	*	*	*	*	*	*	22	drop



Theorem

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	00:1f:..	*	*	*	*	*	*	*	port6
port3	00:2e:..	00:1f:..	0800	vlan1	1.2.3.45.6.7.8	4	17264	80	port6	
*	*	*	*	*	*	*	*	*	22	drop

Current Status



1. working controller

Current Status

1. working controller
2. client libraries

Current Status

1. working controller
2. client libraries
3. pane.cs.brown.edu

Current Status

1. working controller
2. client libraries
3. pane.cs.brown.edu
4. github.com/brownsys/pane

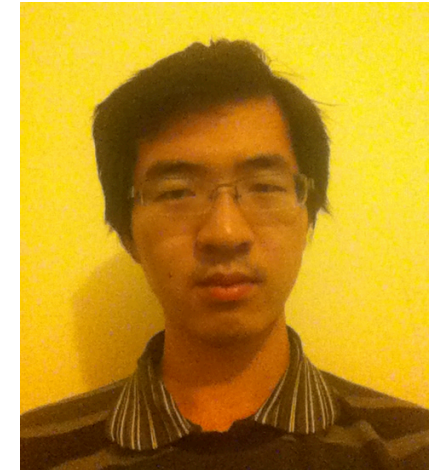
Current Status

Questions?

Andrew Ferguson
adf@cs.brown.edu

Co-authors

- Arjun Guha
- Chen Liang
- Rodrigo Fonseca
- Shriram Krishnamurthi



Questions?

Andrew Ferguson
adf@cs.brown.edu

Backup Slides