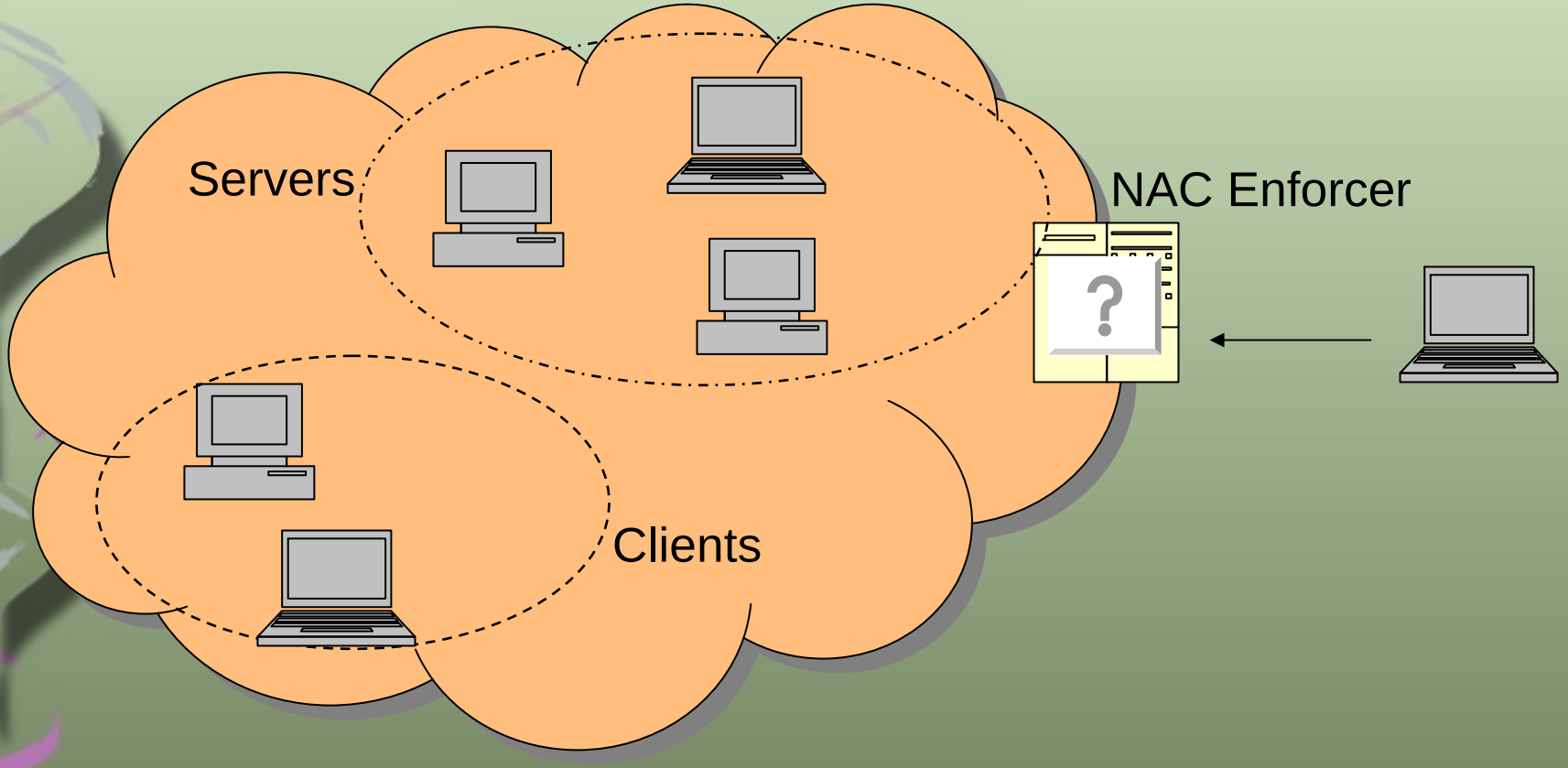
BEHAVIOR-BASED NETWORK ACCESS CONTROL: A PROOF-OF-CONCEPT

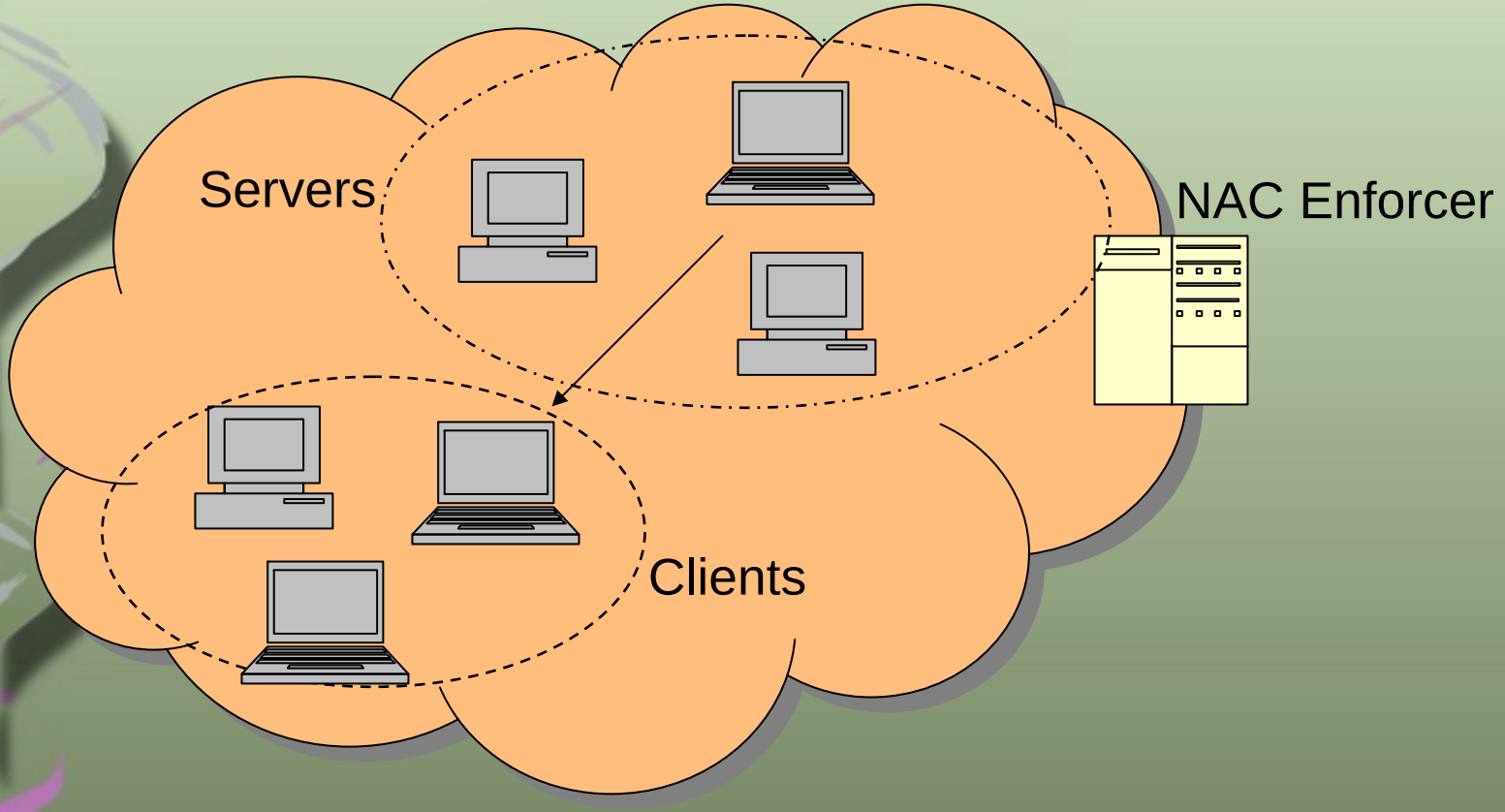
Intrusion Detection Systems Lab
Columbia University

Vanessa Frias-Martinez, vf2001@cs.columbia.edu
Salvatore J. Stolfo, sal@cs.columbia.edu
Angelos D. Keromytis, angelos@cs.columbia.edu

Motivation: Pre-connect Phase



Motivation: Post-connect Phase



Problem Statement

How to automate the creation and update of pre-connect and post-connect policies in a NAC environment?

- Derive pre- and post-connect policies by ***profiling the behavior of network devices***

Outline

- BB-NAC Mechanism
  - Initial Setup
  - Pre-connect Phase
  - Post-connect Phase
- Experimental Evaluation
- Concept Drift in Behavior Profiles
- BB-NAC latency analysis
- Conclusions and Future Work

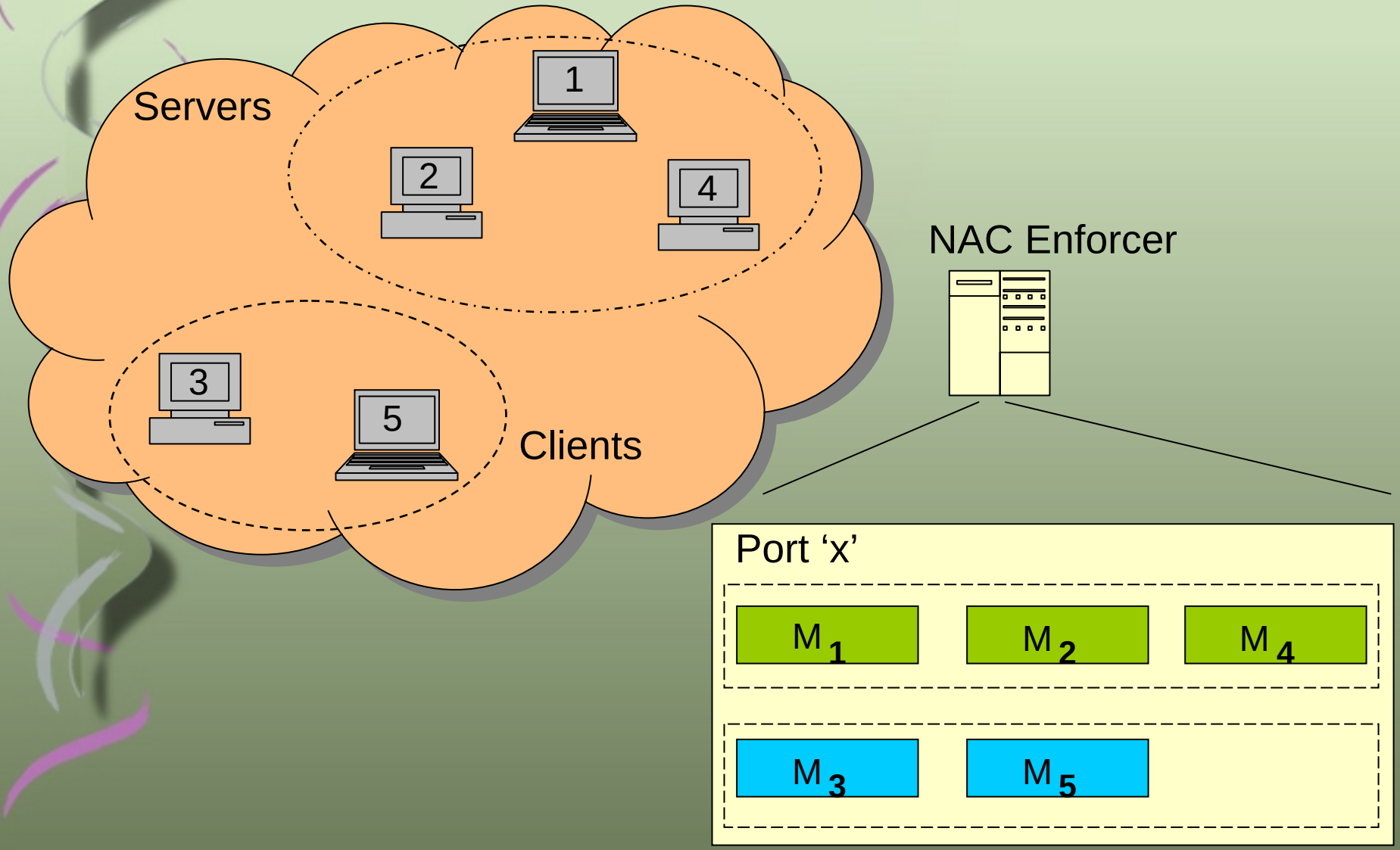
BB-NAC: Initial Setup

- Each device is represented by $M_i = \{P_i, B_i\}$
  - Behavior profile modeled by an AD sensor
  - Bad profile: malware knowledge
  - All are automatically updated by the AD sensor
  - Behavior characterizes payload or volumetric features of the network traffic exchanged

- Devices are grouped in pre-determined clusters of behavior:
  - Clients and servers (per port and direction)
  - Each cluster of behavior profiles represents a valid behavior for the network

- NAC enforcer and high-ranked monitors responsible for the execution of the pre- and post-connect phases, not the members themselves

BB-NAC: Initial Setup



BB-NAC: Pre-connect Phase

- New device with behavior profile P_{new} and bad profile B_{new} solicits admission to network declaring its behavior type
- Behavior Profile Check
  - Does the device's self-declared behavior exist in the set of accepted behaviors in the network?
- Bad Profile Check
  - Does it have enough malware knowledge?

Bad Profile Check

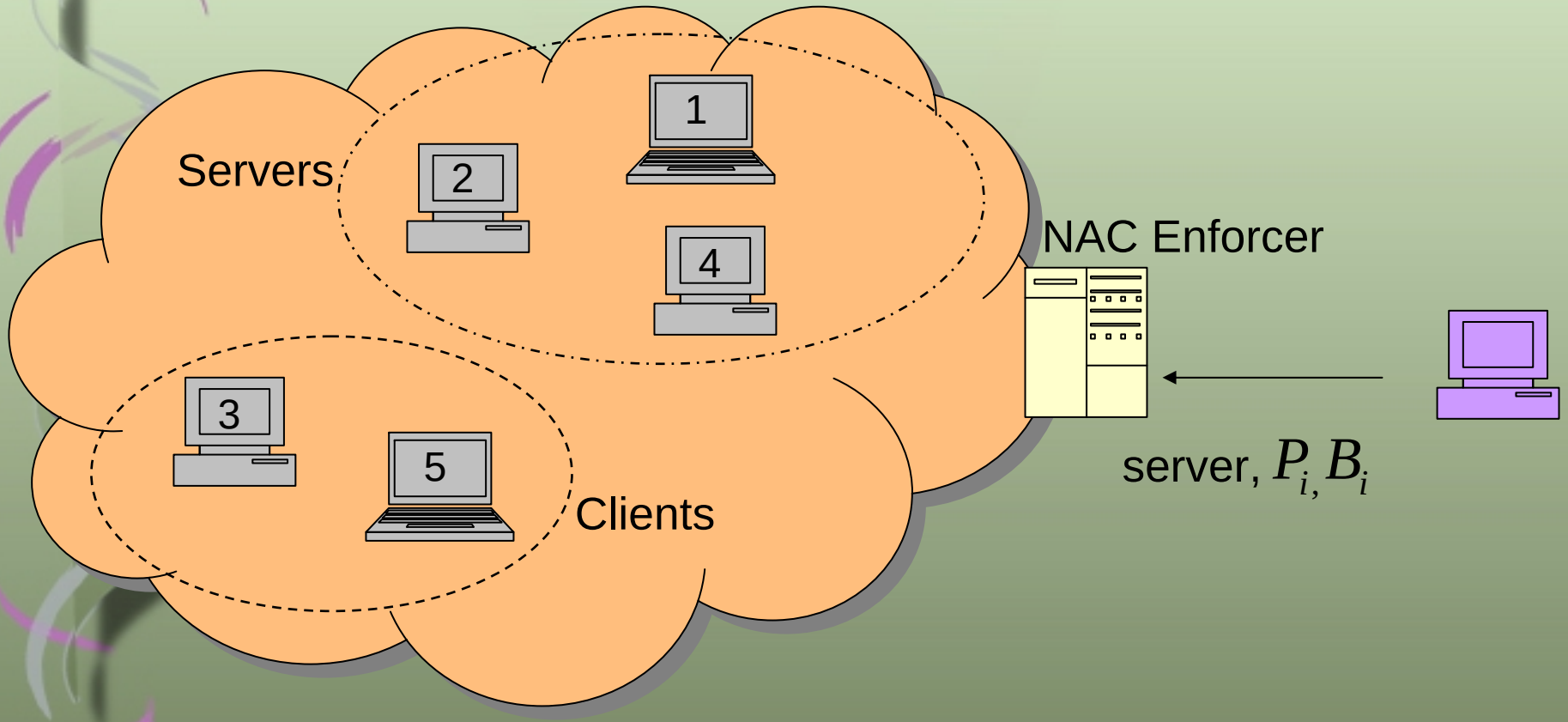
- Group decision based on the sum of individual decisions from each member of its cluster (percentage of agreement, ε)
- Individual decisions evaluate the difference between their local malware knowledge and the newcomer's malware knowledge
  - Individual decision:

$$v_i = 1 \text{ if } B_i \subset \mathrm{B}_{\text{new}} \text{ where } B_i \in cluster$$

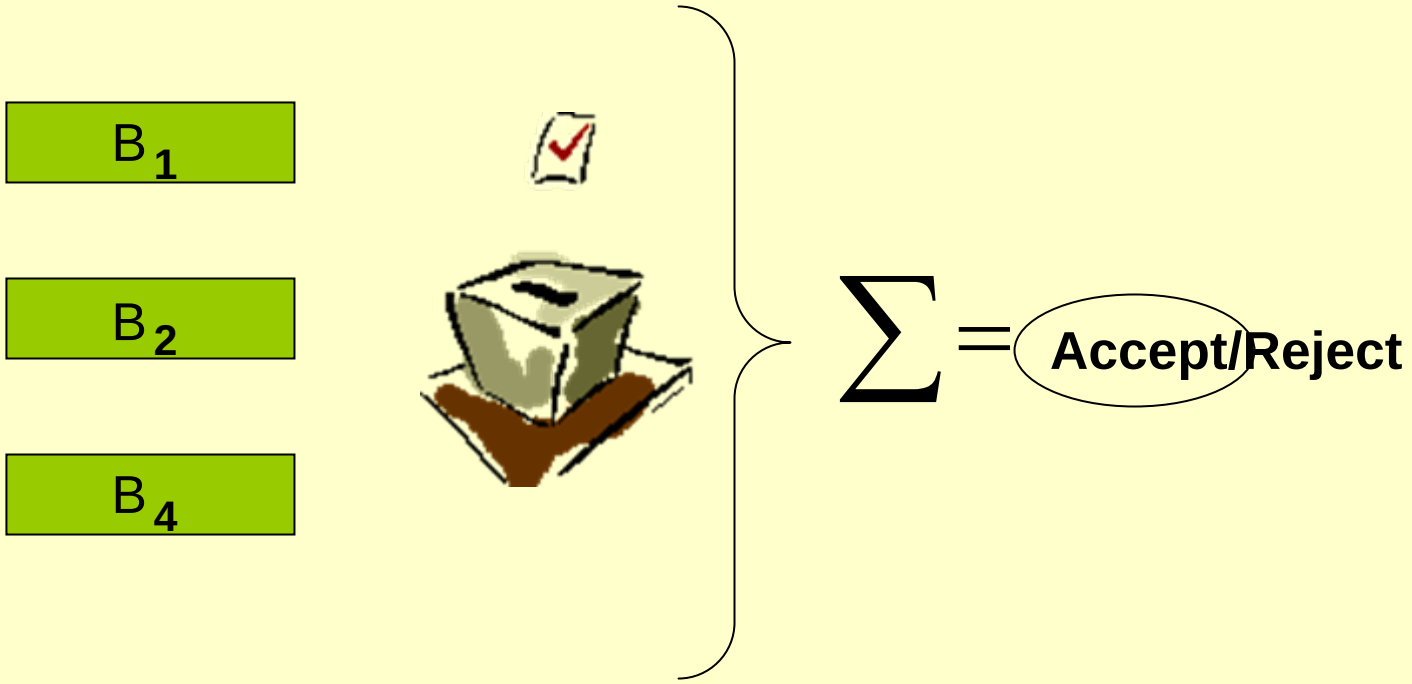
  - Final Group Decision:

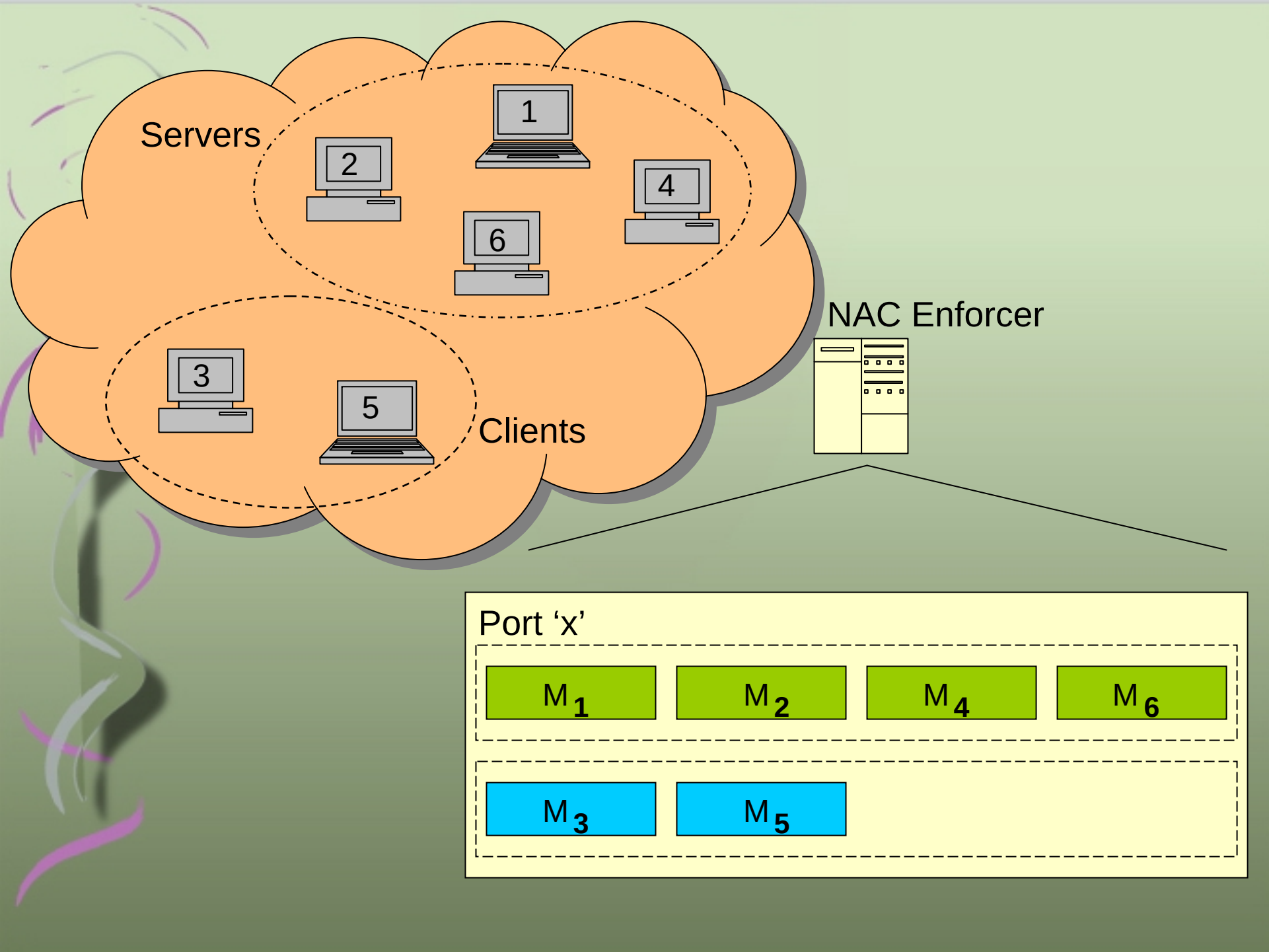
$$v = \frac{1}{n} \sum_{i=0..n} v_i \text{ where } v \geq \varepsilon$$

Pre-connect Phase: Example



Profiles in cluster of servers vote for new profile



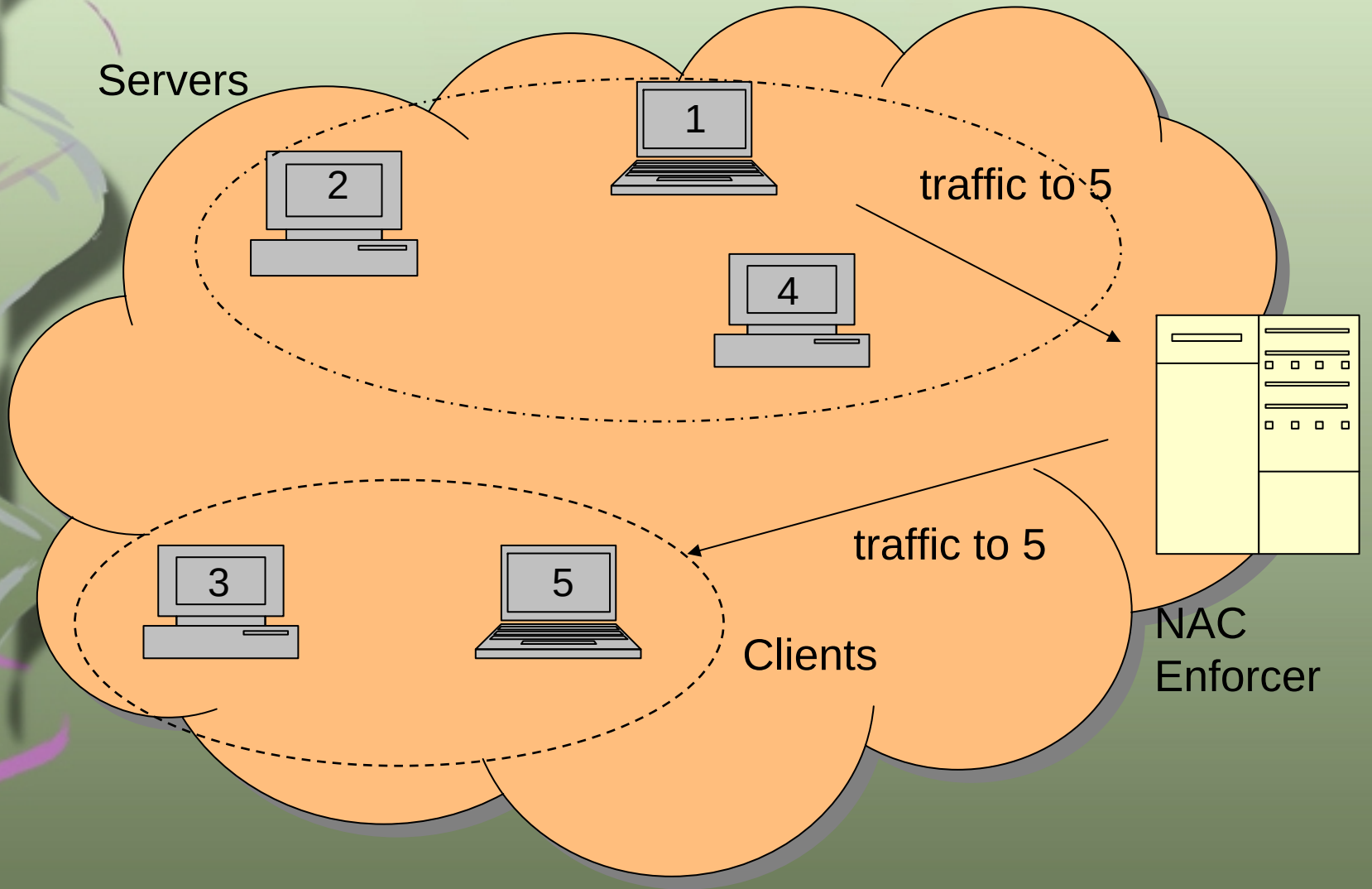

Servers
1
2
4
6
3
5
Clients
NAC Enforcer
Port ‘x’
M 1
M 2
M 4
M 6
M 3
M 5

BB-NAC Post-connect Phase

- Traffic is deemed normal or anomalous based on a group-profile decision
- All members in a cluster vote, not only the ones exchanging traffic: group knowledge

$$v = \frac{1}{n}\sum_{k=1}^{n} P_{k,d}(t) \text{ where } \mathrm{v} \geq \varepsilon \text{ and } P_{k,d} \text{ is the behavior profile of } k$$

Post-Connect Phase: Example



Profiles vote for traffic_unit

P_1

P_2

P_4

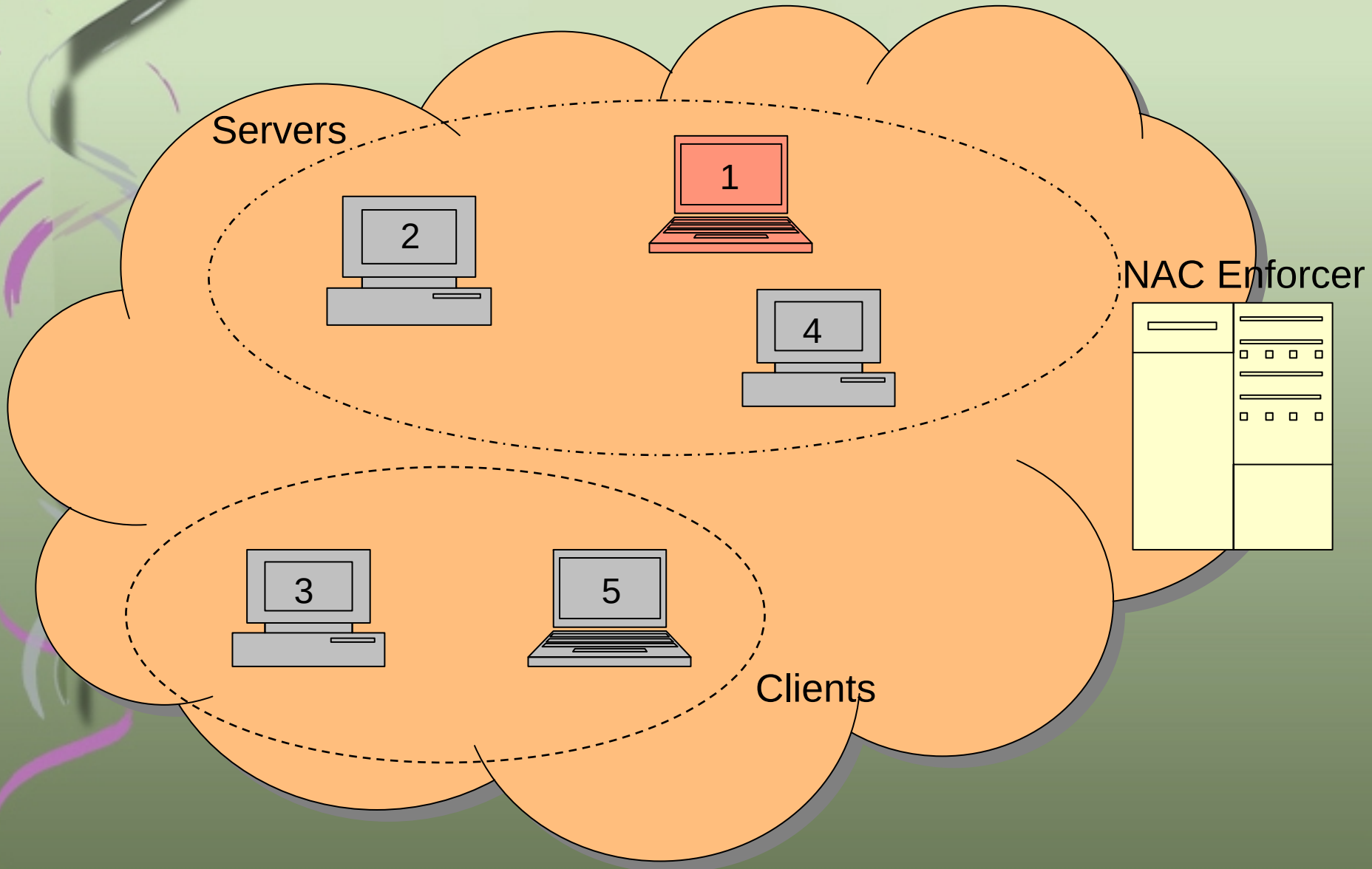
$\sum =$ Normal/Attack

P_3

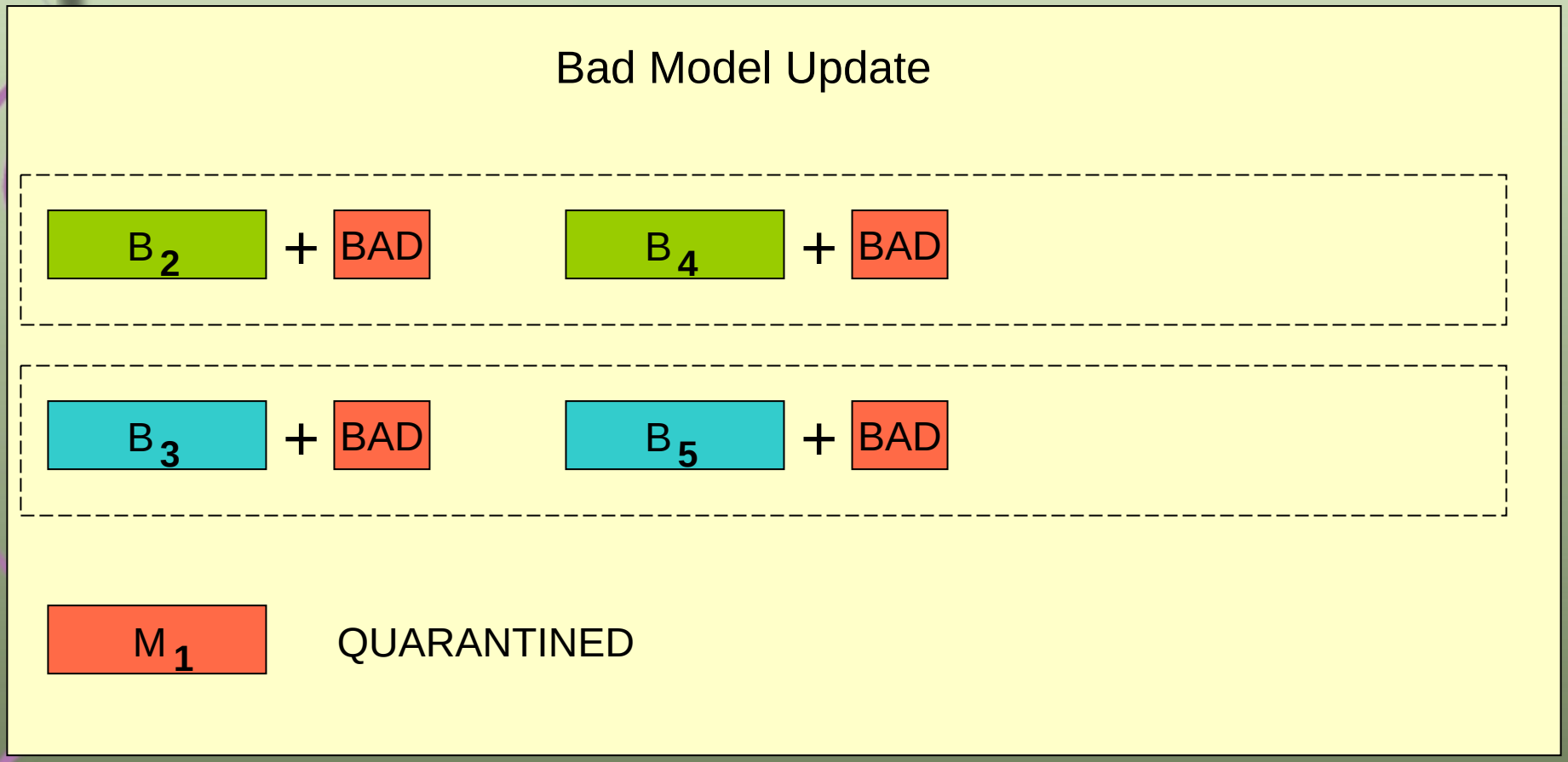
P_5

$\sum =$ Normal/Attack

Profile Quarantine



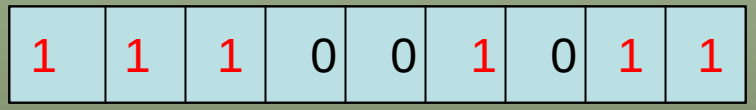
NAC enforcer update



Proof-of-concept Experiments

- Four CS webservers (servers cluster)
- ANAGRAM AD Sensor
  - Modeled input content profiles (4-grams)
  - Saved as BFs for privacy preservation

- Behavior Profile: Bloom Filter with 3 hash functions



Proof-of-concept Experiments

- Behavior Profiles
  - Stable profiles computed for two weeks of traffic (370~700K clean packets)
- Bad Profiles
  - Signature contents from Snort rules and 600 virus samples from *vxheavens*

Pre-connect Results

- Each bad profile contains 10% less than previous bad profile
- Assume three webservers are members and the fourth attempts to enter the network
- Voting with BF:

Scenario	server4_in	server3_in	server2_in	server1_in
(i) 33%	REJ	ACC	ACC	ACC
(ii)66%	REJ	REJ	ACC	ACC
(iii) 100%	REJ	REJ	REJ	ACC

Post-connect Results

- Evaluate in terms of FP/DR
- Clean and poisoned traffic with different CodeRed versions, WebDAV, Mirela and buffer overflows vulnerabilities
- Explore differ

Best Collaborative Solution $\mathcal{E}$ = 75%

Percentage	DR	FP
(i) 25%	100%	0.032%
(ii) 50%	99%	0.02%
(iii) 75%	99%	0.005%
(iv) 100%	83%	0.001%

Group Rates

Server	DR	FP
server1	100%	0.02%
server2	83%	0.009%
server3	99%	0.015%
server4	99%	0.01%

Individual Rates

Concept Drift in Behavior Profiles

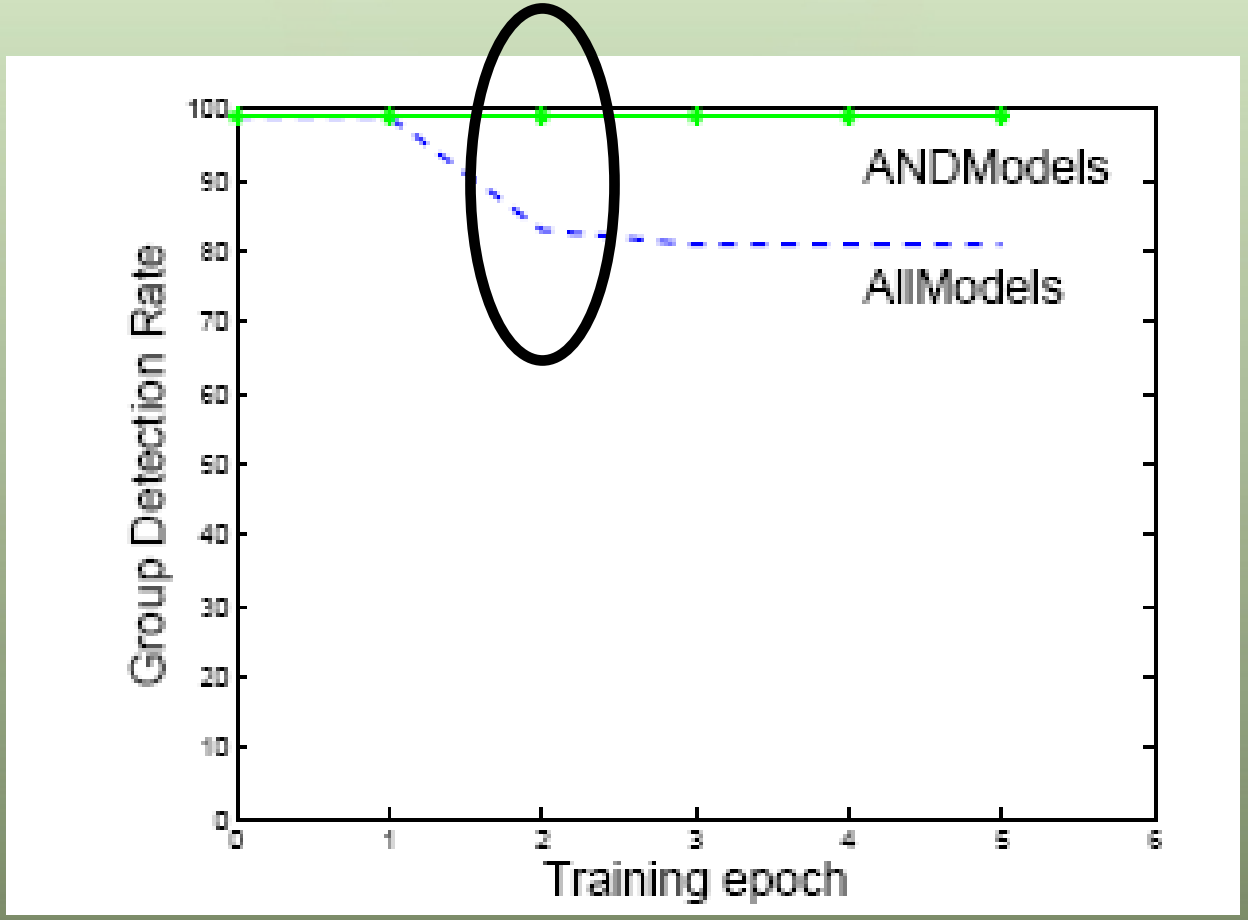
- AllModels: keep all previous knowledge
- ANDModels: keep only common knowledge between models

$$P_i = P_i \wedge P_{i-1} \wedge \ldots \wedge P_{i-q}$$

- Add new behaviors, OR ANDModels:

$$P_i = \vee_{t=0}^{s-1} P_{i-t} \wedge P_{i-1-t} \wedge \ldots \wedge P_{i-q-t}$$

Concept Drift in Behavior Profiles



BB-NAC Latency Analysis

- Pre-connect latency

$$l = l_a + (1 - \rho) \times l_q$$

- Post-connect latency

$$l = (1 - FP) \times l_{BF} + FP \times l_q$$

- BB-NAC values (cluster of 10 devices):
  - Pre-connect: 180~342ms
  - Post-connect (Best collaborative): 5,785~50.56ms

Conclusions

- New mechanism to automatically create and update pre- and post-connect policies
- Novel access control based on a profile-group decision process which may outperform individual decision processes
- New technique to maintain behavior profiles clean over time (resilient to attacks)

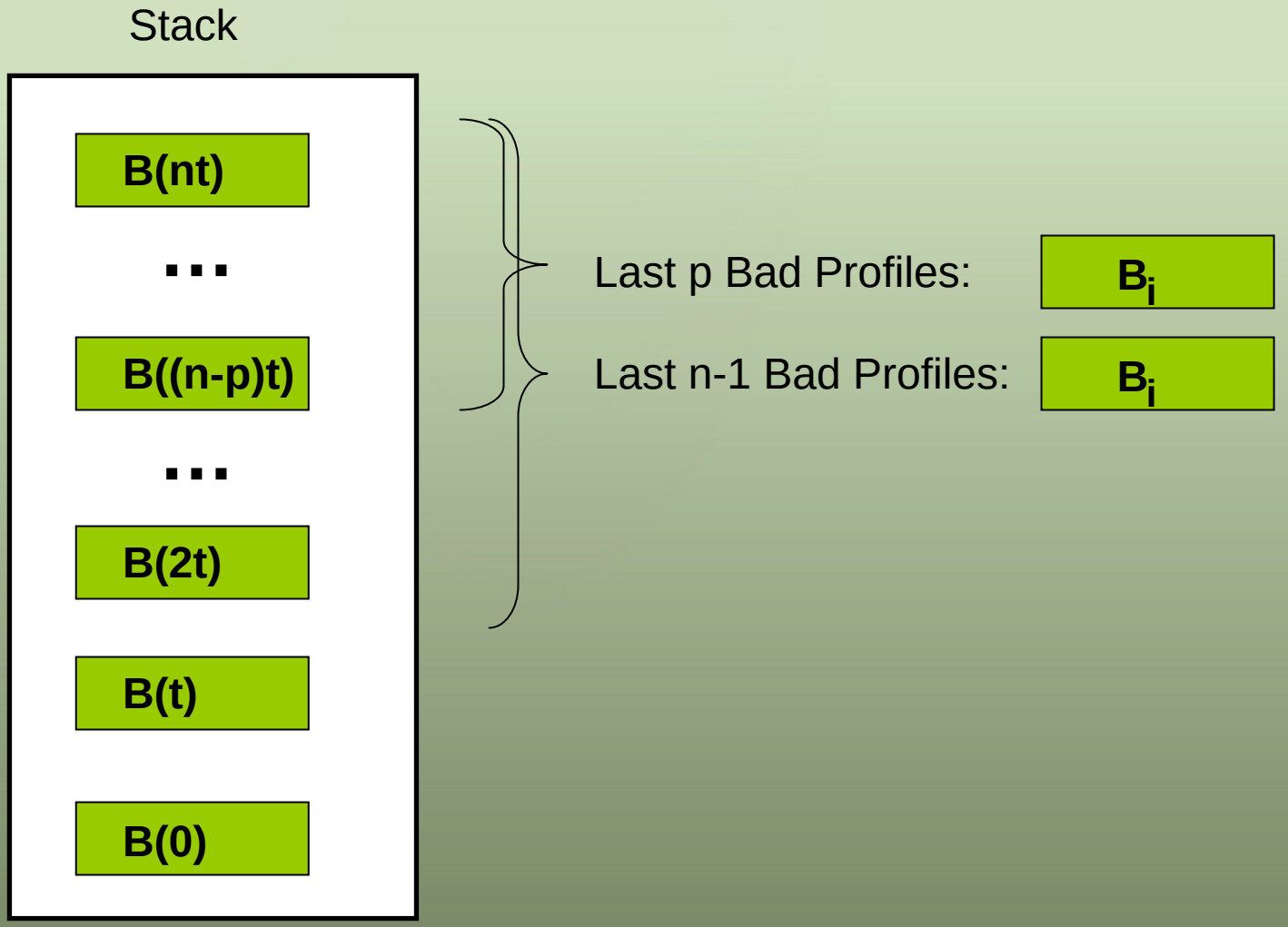
Future Work

- Automatically determine clusters of behavior profiles
  - Additional pre-connect check on the behavior profile
- Automatic detection of malicious behavior profiles trying to manipulate the clusters of behavior defined
- Extensive evaluation of the BB-NAC mechanism with hundreds of behavior profiles modeling content or volumetric behavioral characteristics

THANK YOU!!

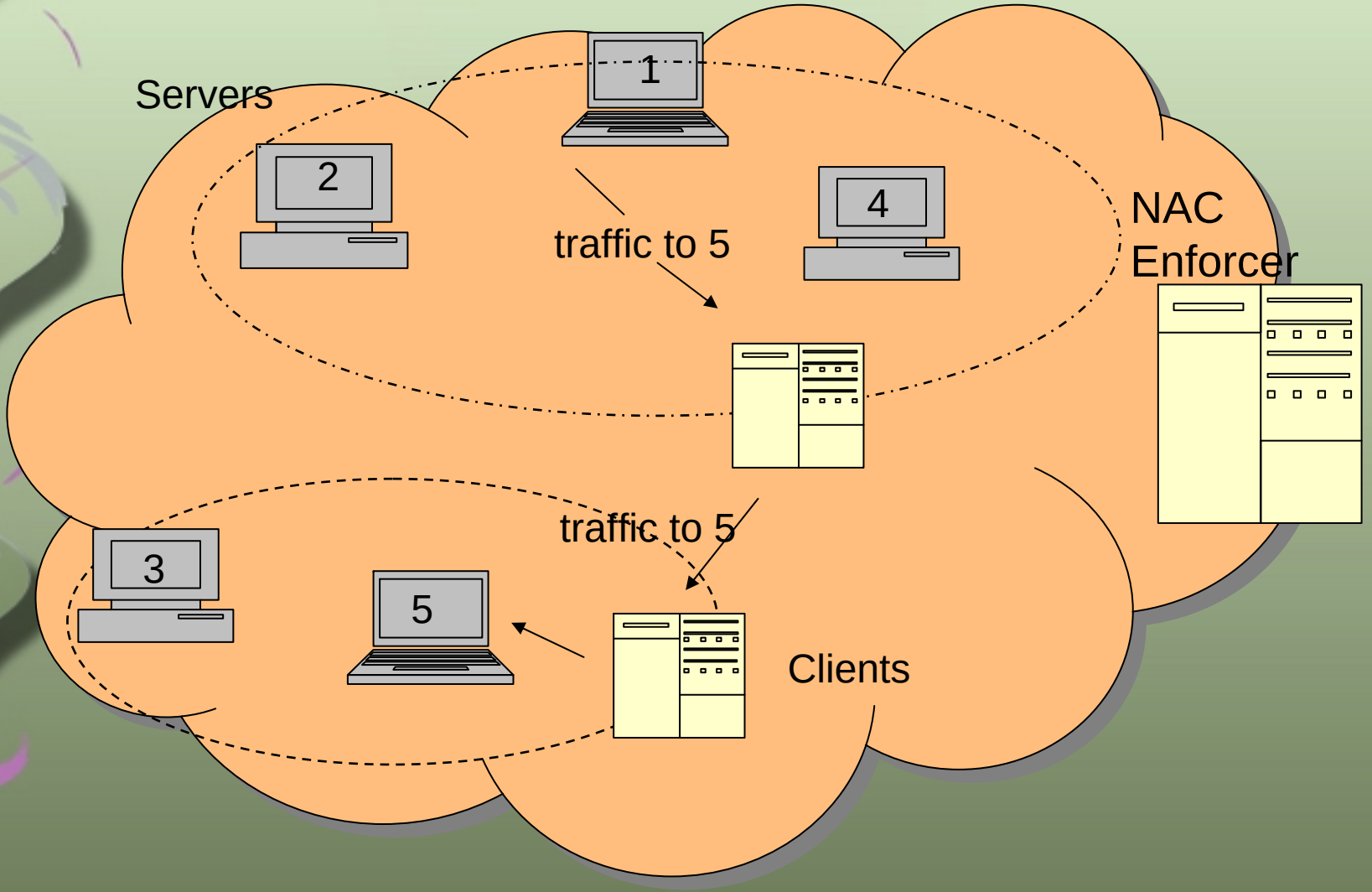
EXTRA SLIDES

Bad Profile History



$$B_i = B_i(nt) \cup B_i((n-1)t) \ldots \cup B_i(n-p)t)$$

Multiple NAC enforcers



Related Work

- Behavior as Security Feature
  - Proof-carrying Code (PCC) (Necula and Lee ’96,’97,’98)
  - Proofs have to be specified by hand
- Collaboration among AD sensors
  - Alert sharing (Parekh et al. ’06, Dressler et al. ’04)
  - Attacks need to be observed by collaborating sites
- Admission and Access control in NAC technologies
  - PacketFence, Cisco NAC Appliance, Microsoft NAP, Symantec
  - All pre- and post-connect policies are manually determined