MA1 Access control and monitoring for campus computer labs

MA-BPD-5 Monitoring activities at campus computer labs

+

MA-BPD-6 Profile and role-based firewall control for campus classrooms labs

Vangel V. Ajanovski <vangel.ajanovski@finki.ukim.mk>
Faculty of Computer Science and Engineering
Ss. Cyril and Methodius University in Skopje

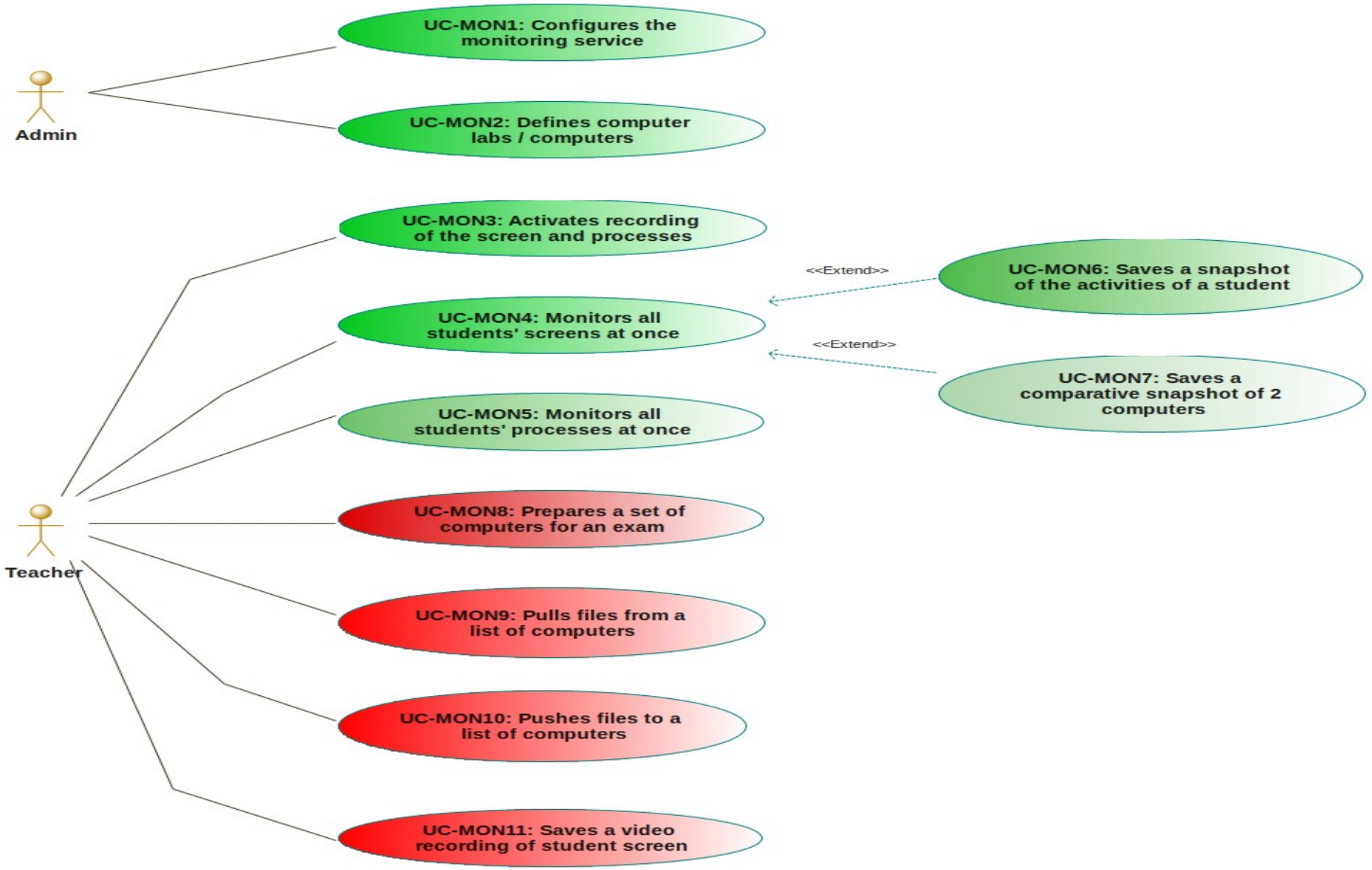
Introduction to MA-BPD-5

- Computer-based teaching laboratories at the universities in Macedonia are used in three general situations: practical demonstrations as part of the teaching process, individual work by students on their assignments, projects, and as an environment for conducting exams.
- There are several different stakeholders in this process, requiring various level of monitoring as a way to check the status of the process in real-time and retrospectively.
  - Administrators wish to know the status of the computing resources, whether they are used by students, installed and working properly.
  - Teachers are obliged by law and academic ethics and conduct to give professional classes to the students, setup and demonstrate in-lab activities and then check the status and results of the students' works.
  - Students are directly using the resources so for them it is crucial to have the right access to the relevant tools. The evaluation of their work is largely based on monitoring of relevant activities in the computer classrooms.
- This document discusses the processes and stakeholder needs, and details some possible solutions - with description of the environment and the proposed systems in use and the needed network architecture. Software tools are pointed out that enable easier monitoring - when needed and as needed by the different stakeholders.
- *This document should be considered as a reference and guide, based on many years of trials at computing departments within the Ss. Cyril and Methodius University, Skopje, Macedonia.*

Problem statement for MA-BPD-5

- **The problem of not being able to monitor/observe/oversee the activities of the students, during the classes and exams,**
  - affects mainly teachers that work with larger groups of students in computer labs,
  - the impact of which is increased physical effort required from the teacher, forced to literally run around the classroom, and peep into one or other students' desktop screens.
  - a successful solution would be a system that enables the teacher to closely and easily monitor students' online activities both as a group, and person by person.
- **Problem statement regarding academic and ethical misconduct**
  - The problem of growing frequency and span of academic and ethical misconduct among students, especially while doing online assessments and exams, confirmed by the existence on numerous online chats, forums, social networks and other systems and online places where plagiarism is increasingly offered as a business, or is requested as a service
  - affects the teachers that are obliged by laws and academic standards to discover such cases and report them, and affects the students that are unknowingly victims of their plagiarising peers
  - the impact of which is increased unproductive effort required by teachers, to search and investigate possible plagiarism, and gather documents and proofs to initiate a disciplinary process, instead of focusing their attention on the real quality work required to run a succesful class
  - a successful solution would be a system that enable the students to work online, but helps to prevent and eliminate academic and ethical misconduct as early as possible, and a system that helps with gathering of the required documents and logs when proofs of misconduct are needed.

Use-cases for MA-BPD-5



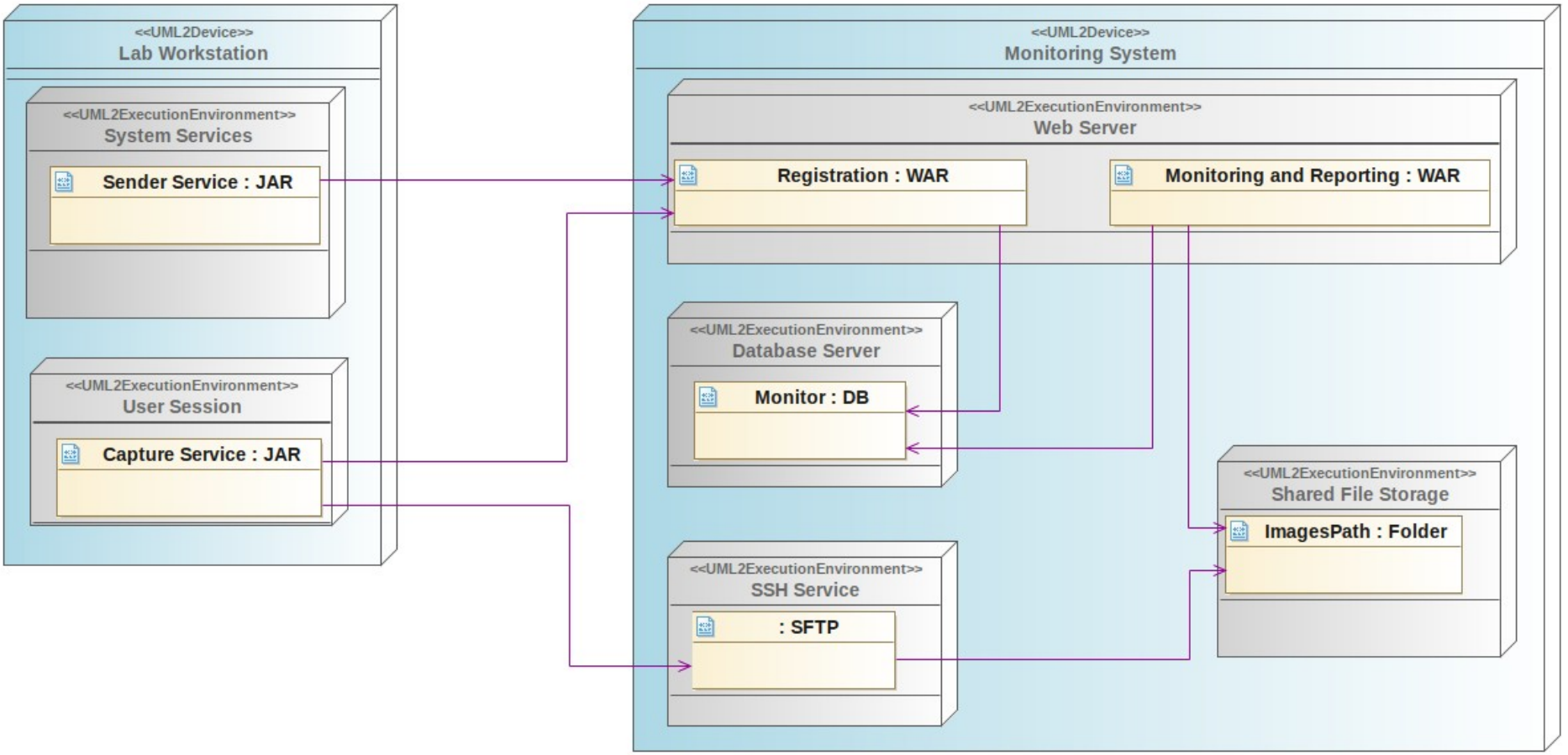
Monitoring lab activities

- There are two services that have to be installed
  - Screenshot service
  - Info sending service
- Screenshot service
  - http://develop.finki.ukim.mk/projects/fccapps
  - It is a simple service, that when run by a desktop user, executes every 10 seconds and takes a screenshot and some general process and computer information and stores it to a file in a pre-configured location.

...

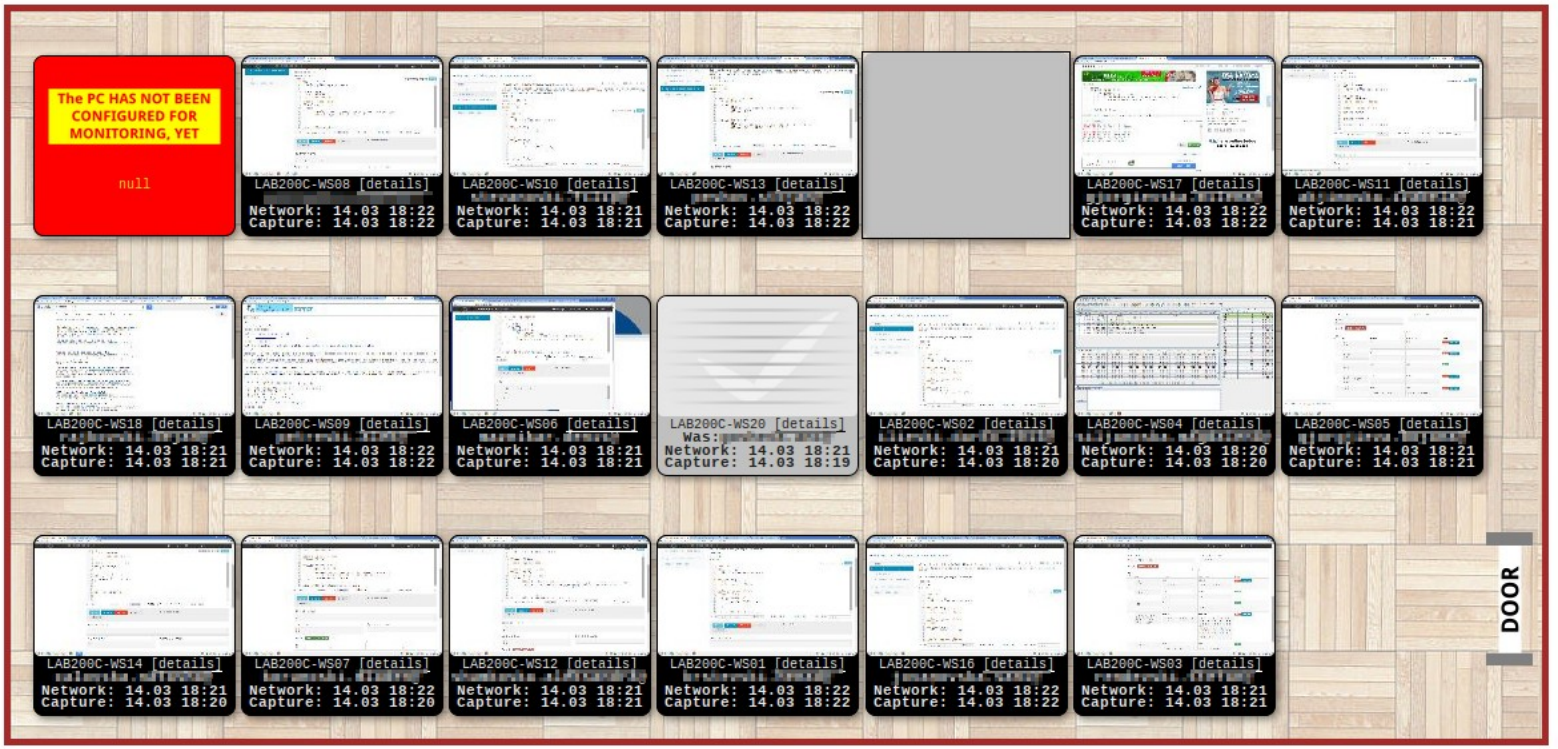
- Info sending service
  - http://evelop.finki.ukim.mk/projects/fccapps
  - It runs every 10 seconds, records data about some system information (for example: logged-in username, cpu usage, temperature, list of processes) to a local file and uploads this file via SFTP to a configured location.
- If the screen shot service is running it can also
  - upload the file with the current screenshot via SFTP

Deployment


<<UML2Device>>
Lab Workstation
<<UML2ExecutionEnvironment>>
System Services
Sender Service : JAR
<<UML2ExecutionEnvironment>>
User Session
Capture Service : JAR
<<UML2Device>>
Monitoring System
<<UML2ExecutionEnvironment>>
Web Server
Registration : WAR
Monitoring and Reporting : WAR
<<UML2ExecutionEnvironment>>
Database Server
Monitor : DB
<<UML2ExecutionEnvironment>>
SSH Service
: SFTP
<<UML2ExecutionEnvironment>>
Shared File Storage
ImagesPath : Folder

...

Monitoring Lab [redacted]



...

lab[redacted]

Screenshot: 2016.03.09 19:28
Sent: 2016.03.10 03:55
Logged on: [redacted]

Hover over image to grow, click to show fully.

User Processes

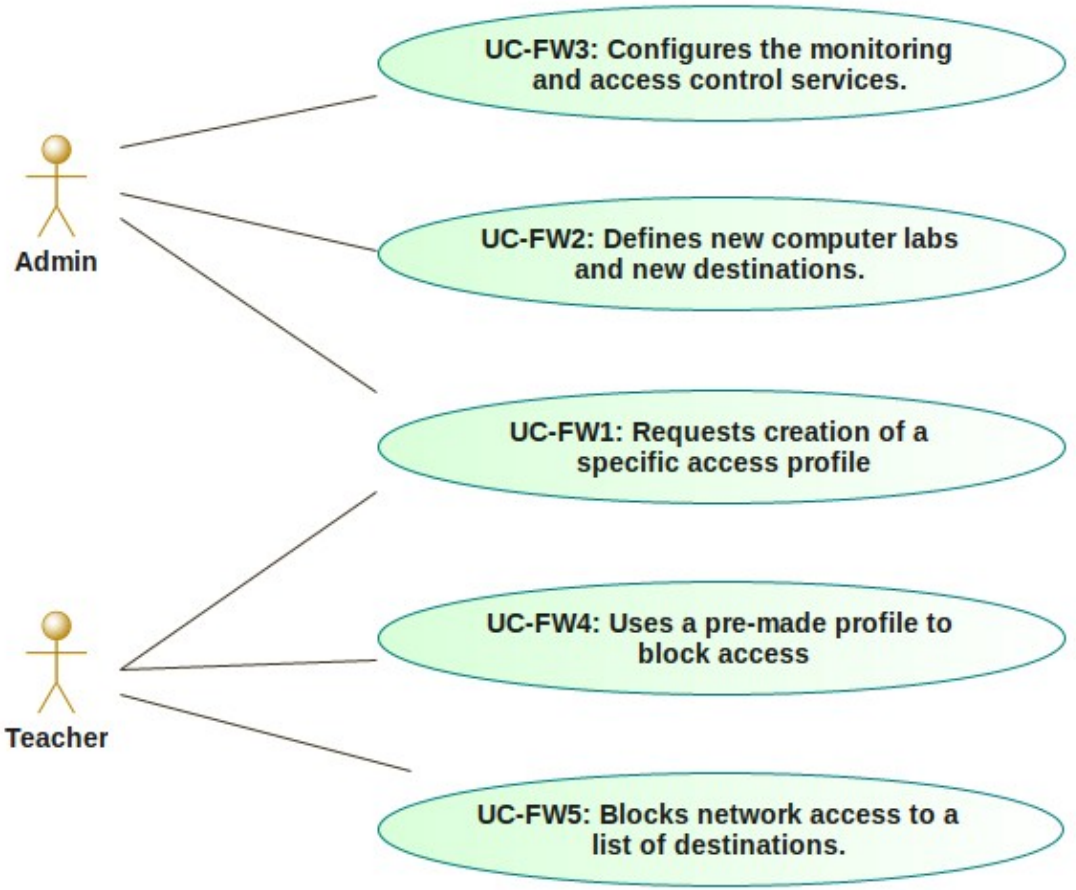
Process Name	Time	User	Virtual Memory	Physical Memory	CPU	Command
System Idle Process	00:00:00	null	0	24	null	
cmd.exe	00:00:00	null	18932	2832	null	[redacted]
conhost.exe	00:00:00	null	22328	2860	null	[redacted]

Back

Introduction to MA-BPD-6

- Computer-based teaching laboratories at the universities in Macedonia are used in three general situations:
  - practical demonstrations of various technologies as part of the teaching process,
  - individual work by students on their assignments, projects, and
  - as an environment for conducting exams of many different types.
- Depending on the special use-cases for each situation, different access permissions are required, different network setup is required, access to online resources should be permitted/denied, and in most situations such adjustments should be performed by the teacher, without any network administration knowledge and direct access to the networking equipment. In this document the design and organizational process of the deployment of such a system is presented together with the tools that enable and ease the implementation and customization based on the needs stemming from the real environment.
- *This document should be considered as a reference and guide to possible simple solutions, based on many years of trials at computing departments within the Ss. Cyril and Methodius University, Skopje, Macedonia.*

Use-cases for MA-BPD-6



FINKI-Firewall control application

- FINKI-Firewall is a Java based web application
  - created initially by the author Dragan Sahpaski
  - for use at the FCSE, but later was shared
- https://github.com/dragansah/finki-firewall
- To be used by teachers
  - enabling them to control and block network traffic in the computer labs.

Customization

Network access profiles in JSON files

```
{
"name" : "Profile",
"description" : "Access to SITE only",
"iptables" : [
  "iptables -I FORWARD -s ${ipClass} -j DROP",
  "iptables -I FORWARD -s ${ipClass} -d SITE.ADDRESS -j ACCEPT",
  "iptables -I FORWARD -s ${ipClass} -d DOMAIN.CONTROLLER.INTERNAL.ADDR  -j ACCEPT",
  "iptables -I FORWARD -s ${ipClass} -d MONITORING.SERVER.INTERNAL.ADDR -j ACCEPT",
  "iptables -I FORWARD -s ${ipClass} -d FW.INTERNAL ADDR -j ACCEPT"
]},
```

Computer labs

No.	Code	Lab Name	Active profile
1	Lab-200		
2	Lab-118		
3	Lab-3		
4	Lab-26		
5	Lab-215		Moodle

Network Access Profiles

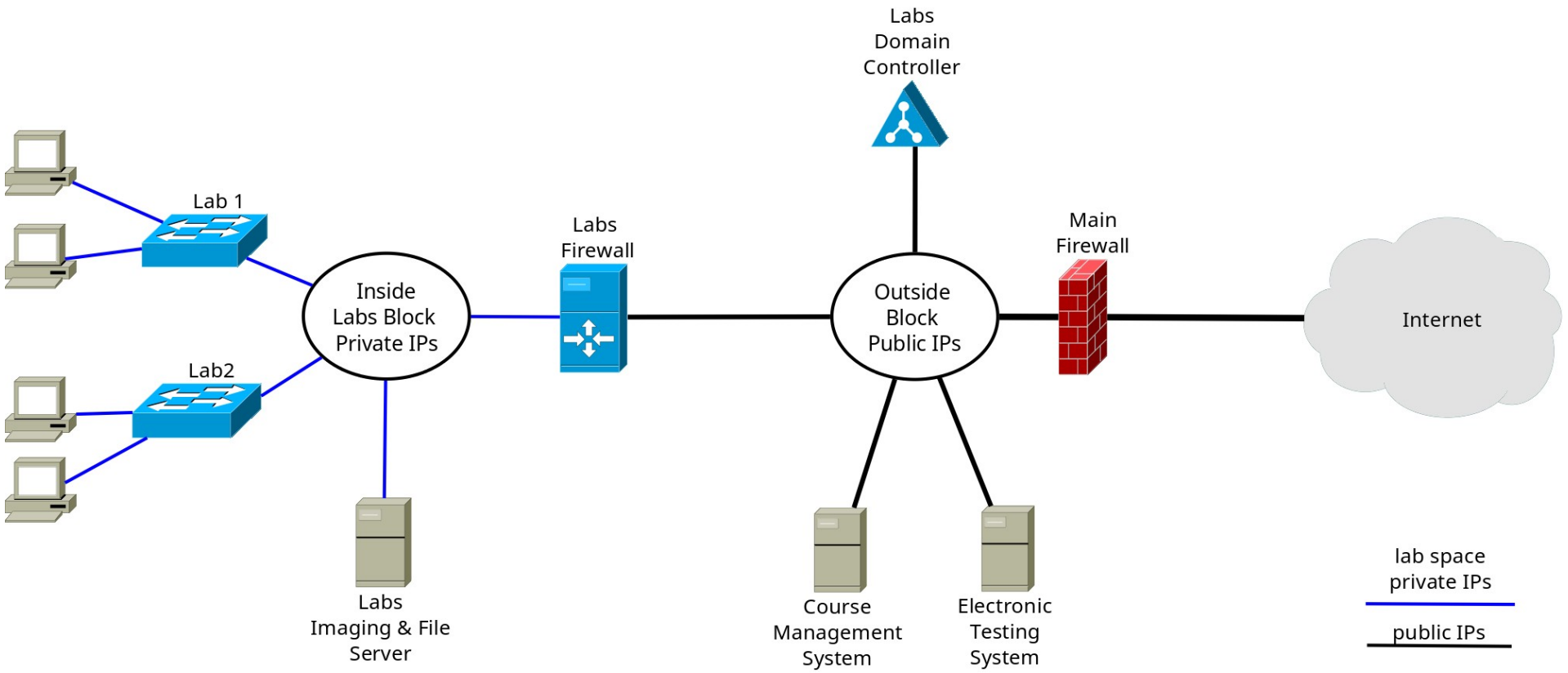
No.	Profile	Description	
1	Moodle	Access to local Moodle server	Lab 215
2	Oracle	Access to local Oracle server	
3	Home Network	Access restricted to local network services	
4	Internet	Unrestricted Internet Access	

Customizing the application

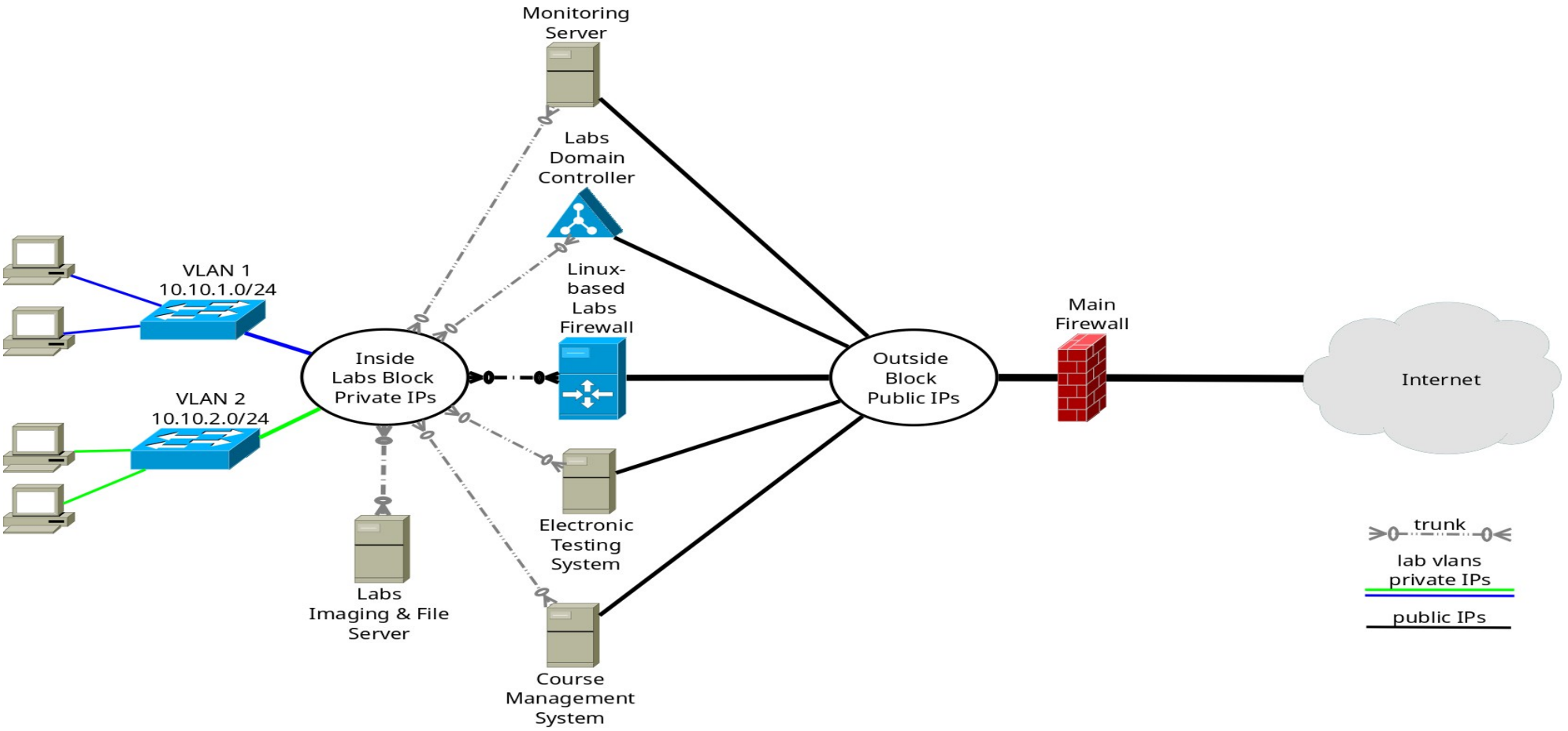
```
<table>
  <tr>
    <td><%=wks("ComputerName1")%></td>
    <td><%=wks("ComputerName2")%></td>
    <td><%=wks("ComputerName3")%></td>
  </tr>
  <tr>
    <td><%=wks("ComputerName4")%></td>
    <td><%=wks("ComputerName5")%></td>
    <td><%=wks("ComputerName6")%></td>
  </tr>
</table>
```

- The sources are given as templates, and being JSP files, they can be easily modified and this can be done live in production
  - This requires very basic HTML knowledge.
  - For advanced customization, basic Java knowledge is required

Architecture Before
(or usual situation in campuses)



Architecture After
(Proposed Solution)



The idea behind this architecture

- Network split in two blocks
  - Inside privately-addressed labs block, a separate VLAN and IP for each lab
  - Outside publicly-addressed server block
- Labs firewall that is based on linux does the following:
  - static router among parts of the labs block + NAT/PAT
  - custom software for switching on/off access to network destinations
  - DNS server for resolving the server names present in the inside block
- Computer labs have presence only in the inside block, each lab in a separate vlan
- Some servers can have presence in both blocks, the reason is
  - computers in the labs should be able to access such servers
    - even if the internet access is disabled completely
  - the servers should know the address of each lab computer that is accessing it
- Access from the inside block to the outside block is only via the labs firewall

Questions?