

# DATA Corp S.A.

## 1. Description

### 1.1. Introduction

Just in time for the end of the Corona pandemic, the company "DataCorp S.A." has completed its new office building and eagerly awaits the return of its employees from the home office. Finally, the annoying online meetings can be replaced again by proper team meetings, which can be held in the more than fifty conference rooms of the new office building.

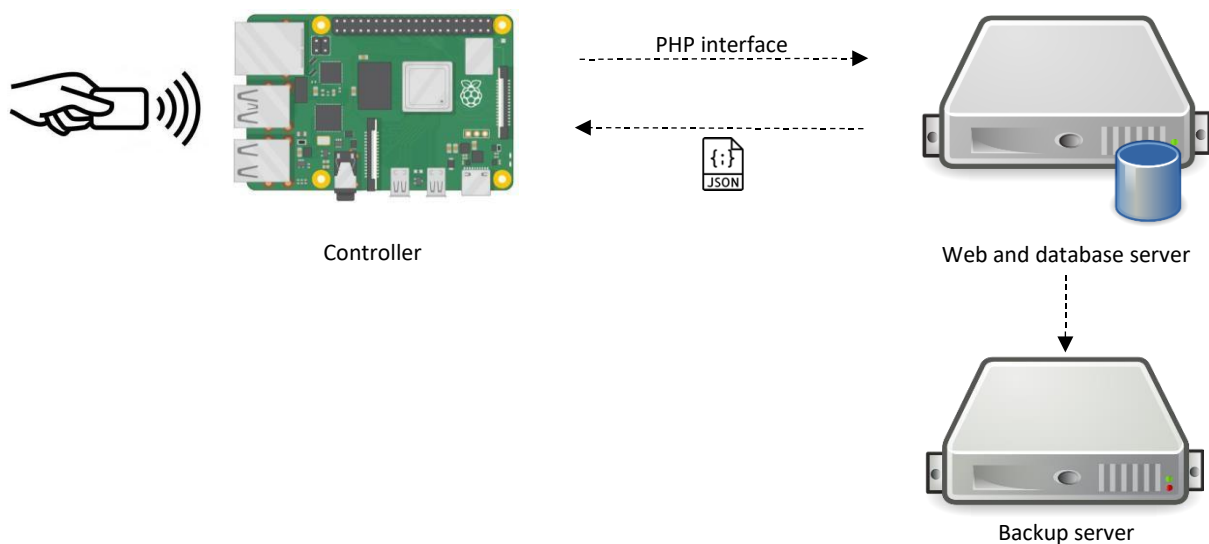
However, in order for the conference rooms to be used efficiently and flexibly by the many employees, a **reservation system** and a **digital locking system** are missing. The reservation system would in fact allow employees to book free conference rooms and allow the company to completely dispense with metal keys, because employees can unlock the reserved conference room completely unproblematically with their RFID batch.



Since the company attaches great importance to security, the entire system must be separated from the internet and hosted only on the company's intranet. Furthermore, backups of all relevant data must be created regularly and stored on a separate server.

As a DataCorp S.A. technician, it now falls to you to plan and implement such a system so that in future all the company's conference rooms can be reserved and unlocked with it. For demonstration purposes, you first have to show your boss your solution using a simple model.

### 1.2. General structure



- The model to be made in the workshop consists of various materials and is used to hold the system components as well as to represent the various functions of the locking system. All details can be found in the chapter *General workshop section*
- .
- The website allows staff to reserve free conference rooms. In addition, an interface informs controllers whether doors may be unlocked by a staff member or not. All details can be found in the chapter *Website*.
- The database stores the data of the reservations of the employees. All details can be found in the chapter *Database*.
- The web and database server hosts the website and the database. You can find all the details in the chapter *Web and database server*.
- The controller reads the RFID batches of the employees and uses the interface of the website to unlock or allow the door. All details can be found in the chapter *Controller*.
- The backup server automatically creates backups of the database and makes them available via FTP. All details can be found in the chapter *Backup server*.
- The integration of the digital locking system into the company network is simulated in Cisco Packet Tracer. You can find all the details in the chapter *Network*.

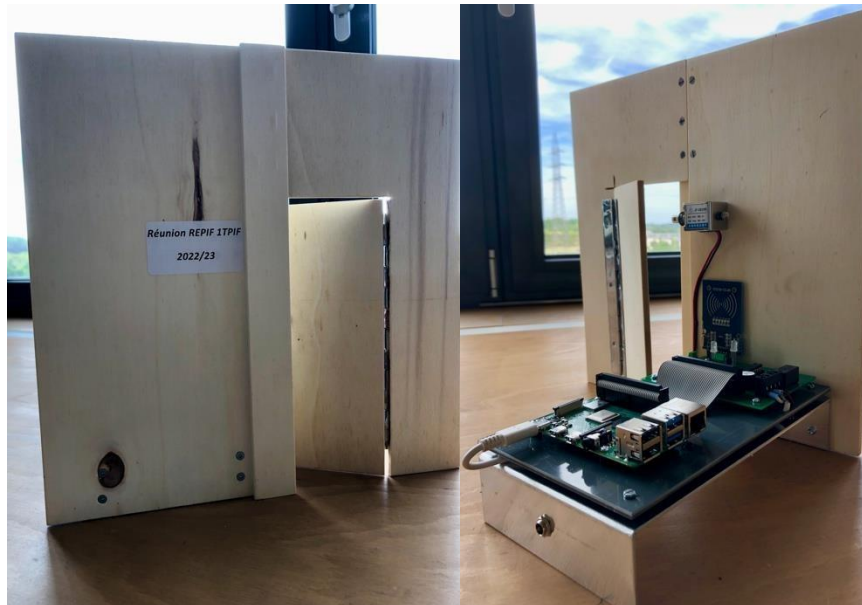
## 2. Timeline

KW	Labo	Studio (2h. each)	Special
38			Stage
39			
40			
41			
42			
43			
44	Congé de la Toussaint		
45	Database	Hand over components and material according to the material list.	Read competences, programme and assignment
46	Database		
47	Website	Printed circuit board & ribbon cable	User story "website" must be planned
48	Website		
49	Website	PVC sheet	
50	Website		
51	Website	Sheet metal holder for PVC panel	
52	Vacances de Noël		
1			
2	Website		Interim presentation 1
3	Website	Sheet metal holder for PVC panel	
4	Packet Tracer		
5	Packet Tracer	Door with frame	
6	Packet Tracer		
7	Congé de Carnaval		
8	Controller	Door with frame	Possibly swap the user story "Controller" with "Webserver" if RPi is not yet available.
9	Controller		
10	Web server	Final assembly, wiring & testing	User story "Web server" must be planned
11	Web server		
12	Backup server	Commissioning	User story "Commissioning" must be planned
13	Backup server		
14	Vacances de Pâques		
15			
16			Last Sprint & Interim Presentation 2
17			
18			
19			
20			
21			Final levy
22	Congé de la Pentecôte		
23			

### 3. Implementation

#### 3.1. General workshop section

In order to test and demonstrate the functions of the reservation system and the locking system of the company "DataCorp S. A.", a corresponding model is to be produced. The complete device should be clearly laid out and all components should be easily accessible. However, live elements must be fused.



All system components are to be mounted in the demonstration unit and connected to each other:

- Raspberry Pi
- Assembled printed circuit board
- Sensors & Pushbuttons
- Actuators
- Connecting conductor
- Connection to power supply

The power supply is provided by an external power supply unit.

The production of the demonstration unit is divided into individual user stories. Missing information must be determined and documented yourself. All practical work is to be produced cleanly, professionally and on time.

#### 3.2. Listing of the workshop user stories

##### 3.2.1. Userstory 1 Workshop: Making a printed circuit board & ribbon cable

The kit-type circuit board must be correctly assembled and soldered. The ribbon cable to connect the board to the Raspberry Pi must be made and tested. All information obtained by the students themselves must be documented.

##### 3.2.2. Userstory 2 Workshop: Making the PVC plate for mounting the circuit boards

A PVC plate for mounting and wiring the circuit boards and all other required components must be made according to the plan. The drill holes for mounting the PCBs and for pulling through the

connecting wires must be determined by yourself (assembled PCB as well as the Raspberry Pi). The completed PVC board is then to be mounted on the holder in Userstory 3. Evaluate your work yourself and document what you did well and what you did less well. Briefly explain what you can do better next time.

### 3.2.3. Userstory 3 Workshop: Sheet metal holder for PVC plate

A bracket to hold the PVC panel and to stabilise the door with frame (Userstory 4) is to be made of aluminium according to the plan. Attention: The drill holes for fixing the PVC panel are only shown as a guide in the plan! The PVC panel is to be mounted provisionally with spacers and must not protrude! All work steps must be fully documented.

### 3.2.4. Userstory 4 Workshop: Making a door with a frame

The individual prefabricated components of the door frame are to be assembled together. The bracket from Userstory 3 is to be mounted on the door frame construction so that the door with frame is set up vertically. The arrangement of the magnetic door lock, the LED and the RFID sensor must be determined and mounted. Any adjustments to the door frame are to be carried out independently. Evaluate your work yourself and document what you did well and what you did less well. Briefly explain what you can do better next time.

### 3.2.5. Userstory 5 Workshop: Wiring & testing the model

All components must be wired together correctly and professionally. Care must be taken to arrange the components correctly. Missing information is to be determined by yourself.

### 3.2.6. Userstory 6 Workshop: Commissioning of the model

The completed model is to be put into operation and all functions are to be recorded in a test report. Any faults must be rectified.

## 3.3. Website

### 3.3.1. Description

The website allows DataCorp S.A. employees to reserve conference rooms for meetings or important appointments, and then unlock them at the right time with their RFID batch. Since the company puts a lot of emphasis on its appearance, the website has to be graphically appealing. In order to be ready for launch as soon as possible, only a desktop version of the website is planned in the first phase, but many employees would like to see a mobile version.

### 3.3.2. Registration

The website can only be used by registered employees. As the website is only accessible on the intranet, the company has not planned any validation of user accounts, i.e. anyone can register and is immediately unlocked.

To register, a staff member must complete the following fields, which are validated on the server side:

Field	Requirements
E-mail	valid format, unique
Name	must not be empty
First name	must not be empty
RFID batch	must not be empty, unique
Password	must not be empty

### 3.3.3. Log in

To log in, a staff member must provide their email and password.

### 3.3.4. Change user profile

In his user profile, a logged-in employee may edit his first name and surname, his RFID batch and his password. The same server-side validations apply as for registration.

### 3.3.5. Select conference room

On an overview page, the logged-in employee sees all conference rooms that exist in the office building and are known to the website. There are no restrictions on who can reserve which room. For each room, one sees the name of the room with a small description (such as special features of the room).

### 3.3.6. Select day

After the employee has selected a room, the employee now selects a date on which he or she would like to reserve the room. Although the office building is not available to employees on weekends, such control is not planned in a first phase.

### 3.3.7. Daily overview

For the selected room and the selected day, the employee sees a daily overview of the room utilisation here. The following points simplify the system:

- A reservation always lasts one or more whole hours
- A room can only be reserved from 08:00 to 17:00, i.e. there are only 9 "slots" where a reservation can take place
- If the space is free, this slot should be displayed in green
- If the room is occupied, this slot is to be displayed in red
- For each occupied slot, one should be able to see the first name and name of the employee who made the reservation, as well as the purpose of the reservation

If you want to reserve a slot, you simply click on a free slot (link, button or other usage elements are allowed).

### 3.3.8. Make a reservation

Finally, a staff member can make a reservation. To avoid mistakes, all important information is displayed again: room, date and start time of the slot.

The employee must now select the duration of the reservation (in hours) from a selection list. The values of this selection list are determined intelligently by the system, i.e. only sensible numbers may be in this selection list:

- A reservation takes at least 1 hour
- A reservation cannot last longer than the day allows, i.e. up to a maximum of 17:00. If, for example, you select 14:00 as the slot and there are no other reservations later on that day, the list will contain the values 1, 2 and 3.
- A reservation can last at most until the next reservation. For example, if you select 14:00 as the slot and there is a next reservation at 16:00, then the list only contains the values 1 and 2.

To complete the reservation, the employee must still enter the reservation purpose and send the reservation (without additional confirmation).

### 3.3.9. Controller interface

If an employee wants to unlock a room with his RFID batch, the controller must ask the web server whether this RFID batch is authorised to unlock the door for this room and for this time. This communication takes place via HTTP. The website must therefore provide a PHP interface that receives the scanned RFID batch of the employee and the host name of the controller via GET parameter. The interface responds with a JSON-encoded data structure that tells the controller whether the door may be unlocked or not. This data structure must be an object with a single attribute "allowed" whose value is either *true* or *false*. Example when access is allowed:

```
{
  "allowed": true
}
```

### 3.3.10. Optional elements

DataCorp S.A. wants the website to be operational as soon as possible and is therefore prepared to sacrifice important functionalities in an initial phase. There is therefore no mobile version, no administration of rooms or staff accounts and no possibility to edit or manage reservations. All these interactions should initially only be possible through direct administration of the database.

Furthermore, the company would like to have a functionality as soon as possible that would allow the cleaning staff, for example, to see when rooms are free/occupied, but without having sensitive data displayed (names of employees or reservation purpose) and without being able to make reservations. This functionality would also be ideally expandable, so that cleaning staff could always unlock free rooms with their RFID batch without having to reserve this room first.

## 3.4. Database

The database is used to store all the data necessary for the correct functioning of the basic functionalities of the website. The following information is important to design the database correctly:

1. The conference rooms in the office building always have only one access door. So there is no bookable room that would have two or more doors.
2. Each conference room has only one door, therefore only one controller. This controller is identifiable by its unique host name.
3. Each employee has a unique RFID batch<sup>1</sup>. A history of which employee had which batch for how long is not provided.

Since the company wants to expand the website with additional functionalities as soon as possible, the database must already take some of these additions into account.

Thus, there must already be a possibility in the database to define user groups and to assign users to these user groups. A user must always belong to a user group and can only belong to a maximum of one such group.

---

<sup>1</sup> An RFID batch has an ID defined during production and can additionally be written with data by an RFID reader. The controller firmware provided only uses the ID. The ID is usually a very large number whose size, however, depends on the manufacturer.

Furthermore, it must be possible to define special rights (such as "can reserve room", "can view reservation purpose", "can administer user"). These rights can then be assigned to user groups and the date on which this right was granted to a user group should also be able to be saved.

With this rights system, it will be possible in future to flexibly define new user groups and give them the associated rights on the website. The website could then use these rights to specifically switch features on or off when logging in.

Example: the user group "cleaning staff" would have the right "can view daily overview" but not the rights "can reserve room", "can view reservation purpose" or "can administer user"

### 3.5. Web and database server

A virtual machine is to serve as a web and database server. The latest Ubuntu Server LTS version, an Apache, MySQL and PHP stack and the OpenSSH server are to be installed on this server.

- The host name, Mac address and static IP address should be configured according to the instructions. The time zone must be configured correctly.
- MySQL:
  - The use of *mysql\_secure\_installation* is not recommended.
  - The MySQL *root* user must still use the authentication method *unix\_socket*.
  - A MySQL user with your IAM code as the user name must be created. This user must have the privilege *ALL PRIVILEGES* and the authentication method *mysql\_native\_password* configured.
- PHP must be configured to display PHP error messages on the web page.

In order to save time, DataCorp S.A. decided that the website should already be developed locally and only migrated to the server later, once it had been set up. In order to facilitate the migration, phpMyAdmin should also be installed and configured on the web server.

### 3.6. Controller

Each door of a conference room has a controller on which special software decides when the door can be unlocked, when the individual LEDs turn on, etc. The controller is then used to control the door. As a controller for your model, you use a Raspberry Pi with ready-made Python firmware that only needs to be adapted.

When an employee holds his RFID batch to the RFID card reader, the RFID batch number together with the host name of the controller is sent to the web interface on the web server. Based on the database information, the interface decides whether the door may be unlocked or not. This decision is sent back to the controller, which then takes the necessary steps.

### 3.7. Backup server

A loss of the data stored in the project database would lead to considerable problems in the operation of the digital locking system. The database must therefore be backed up to a second storage medium at regular intervals. The backup server is used for this purpose.

The backup server is implemented in the form of a virtual machine. The current LTS version of Ubuntu Server is installed on this server, together with the OpenSSH server.



The backup is carried out with the help of a shell script. The shell script uses the utility `mysqldump`<sup>2</sup>, which directly accesses the MySQL database on the web and database server. For this purpose, a dedicated user is created in the MySQL database who is allowed to access the project database from the backup server. Only the project database is backed up. The backup files are stored in the directory `/backups/mysqldump/webserver/` and the names of the backup files must contain the date on which the backup was made. The backup is performed automatically, daily at 23:00.

FTP access to the directory `/backups/mysqldump/webserver/` is set up on the backup server, which allows a user created for this purpose to transfer a copy of the backup files to a PC. The data is transferred in encrypted form (via FTPS or SFTP).

### 3.7.1. Optional elements

To make the system more secure, the MySQL user's password should not be visible in the shell script<sup>3</sup>. In addition, the MySQL user should only have the minimum rights to perform the backup of the project database with the help of the `mysqldump` utility. To make FTP access more secure, the FTP user should not be allowed to leave the backup directory.

Backup files older than seven days should be deleted automatically. In addition, the head of the IT department wants you to create a procedure that describes how to manually import a backup file into the MySQL database.

In order to monitor the backup of the project database, successful and unsuccessful backups, as well as error messages generated in the shell script, should be logged in a log file.

## 3.8. Network

As a technician, you are assigned by the head of the IT department to simulate the integration of the digital locking system into the company network. The simulation is carried out in Cisco Packet Tracer (version 7.2.2 or higher). The part of the current company network that concerns the simulation is shown in Figure 1 is shown. The move from the old to the new company building is not yet complete and the web and database server is still located in the old company building.

---

<sup>2</sup> <http://manpages.org/mysqldump>

<sup>3</sup> <https://dev.mysql.com/doc/refman/5.7/en/password-security-user.html>

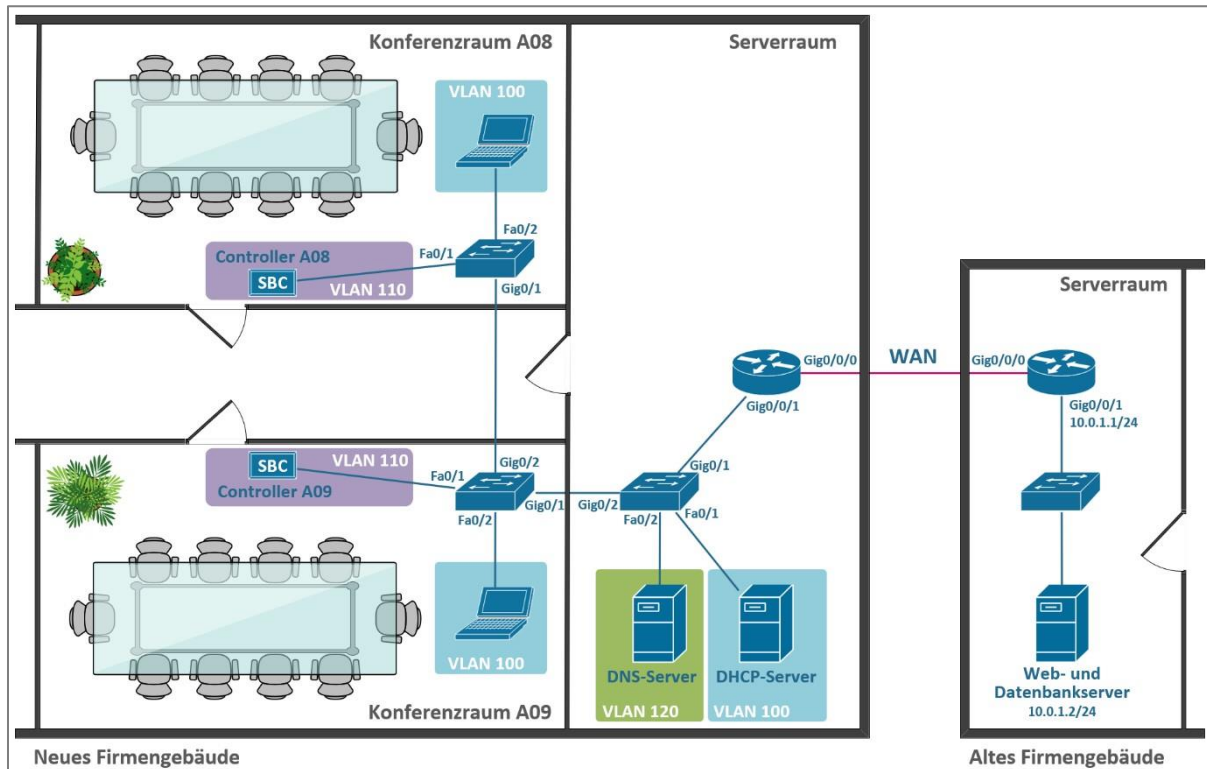


Figure 1

For performance, security and cost reasons, the company network in the new building is divided into individual VLANs. The VLANs relevant for the simulation are listed in Table 1 listed.

VLAN ID	Name	Purpose
100	Laptops	Laptops of the users of the conference rooms
110	Controller	Controller of the locking system
120	Server	Server (currently only the DNS server is in this VLAN)

Table 1

The addresses required for the VLANs and the WAN are listed in Table 2 listed. The IP address range 172.20.22.0/23 is available and must be divided using a VLSM division. The division must be done according to the size of the individual networks (i.e. the first host address of the largest network with 250 addresses is 172.20.22.1). Thus, there is only one possible solution for the division.

IP address range to be divided	Network	Required IP addresses
172.20.22.0/23	VLAN 100	250
	VLAN 110	50
	VLAN 120	8
	WAN	2

Table 2

Note the following guidelines:

- All information contained on the network diagram in Figure 1 must be taken into account (e.g. the interfaces to be used on the network devices for the individual connections and the number of cables). The floor plan Figure 1 is provided to you and you must use it as a background image in Packet Tracer.
- *The SBC boards available* in Packet Tracer are used for the controllers. To connect to the switches, a module with an Ethernet port must be attached to the *SBC boards*.
- The switches are from the manufacturer Cisco (model Catalyst 2960).
- The two routers are also from the manufacturer Cisco (model ISR 4321). They are connected to each other via a fibre optic line (1000BASE-LX/LH). For this purpose, the SFP module GLCLH-SMD is used on both routers. Note: so that the SFP module is used for the Gig0/0/0 interface instead of the permanently installed Ethernet port, the command `media-type sfp` must be entered for this interface.
- The network configuration (IP address, netmask, default gateway, DNS server) of the hosts in VLAN 100 is done via the DHCP server shown in the network diagram. The network configuration of all other hosts and the routers is static.
- In the VLANs, the first host address is assigned to the router.
- The IP addresses of the LAN in the old company building are shown on the network diagram at Figure 1 shown.
- For your simulation, a single record on the company's DNS server is sufficient: a DNS record for the domain raumbuchung.datacorp.lu that points to the web and database server.
- Only the HTTPS service is activated on the web and database server (no HTTP).
- Since the connection to the old company building is only a temporary solution, no dynamic routing is configured on the routers, but static routing. You have to configure the routes necessary to reach the web and database server from the controllers as well as from the laptops in the conference rooms. Since the network on Figure 1 is only a part of the current company network, default routes are not allowed. It is not necessary for the web and database server to be able to access the DNS server.
- For security reasons, it must not be possible to access VLAN 110 from VLAN 100, and vice versa it must also not be possible to access VLAN 100 from VLAN 110 (all packets from VLAN 100 to VLAN 110 and all packets from VLAN 110 to VLAN 100 must be filtered, i.e. deleted). In addition, only data packets sent from or to the web and database server may be allowed through via the fibre optic line between the two routers, namely only ICMP data packets and data packets necessary for the HTTPS service.
- Note: The transfer of data between the controllers and the web and database server cannot be recreated realistically in Packet Tracer. It is sufficient that the controllers can access the HTTP service of the web and database server.

After you have completed your simulation, you must save the current configurations (running-config) of all network devices (switches and routers) on the network devices in Packet Tracer (startup-config) and add them to your documentation.

The Head of IT expects that the created Access Control Lists (ACLs) are tested and that these tests are documented. Note the following requirements:

- The test protocols are documented using a table that corresponds to the example in the appendix of the corresponding user story.
- Test logs must be created regarding all configured ACLs (test logs for the packets allowed through by an ACL, as well as test logs for the packets deleted by an ACL). The tests must be unambiguous and meaningful.
- Test protocols regarding server services (DHCP, DNS, HTTPS), inter-VLAN routing and static routes are assessed as optional elements. Command line tools such as nslookup and traceroute may be used.

### 3.8.1. Optional elements

The management has decided that in a further phase the digital locking system will also be used on doors other than those of the conference rooms. As the cabling of the controllers for some of these doors is very difficult, it should be possible to integrate the controllers into the network via WLAN. Your simulation should therefore include a controller connected via WLAN at the door of the server room. You should consider the following possibilities:

- the controllers connected via WLAN should be in VLAN 110
- the access points should be configured via a WLAN controller
- The access points should not only be used for the controllers, but they should also enable the users of the conference rooms to connect their laptops to the company network (VLAN 100) via WLAN.
- You should consider for which WLAN connections it makes sense that a user name and password are required for logging in.

The web and database server in the old company building can only be used as a temporary solution until the old company building has to be vacated. By then, the new web and database server must be operational in the new company building. This will be integrated into a DMZ as shown in Figure 2 this will be integrated into a DMZ. In order for the backup server to be able to take over the function of the web and database server in an emergency, it makes sense to integrate the backup server into the DMZ as well. The head of the IT department will be impressed if you can simulate the architecture shown according to the following specifications:

- The HTTPS service of the new web and database server is accessible from the company network as well as from the Internet.
- A PAT network address translation is set up on the firewall for the private IP addresses of the company network.
- The IP address 194.154.32.2/30 is available for the connection to the Internet Service Provider. Public IP addresses are also used in the DMZ. The IP address range 194.154.91.184/29 is available for this purpose.
- In order to test the possibility of VPN connections to the company network, the old web and database server is accessible from the Internet via a VPN connection.

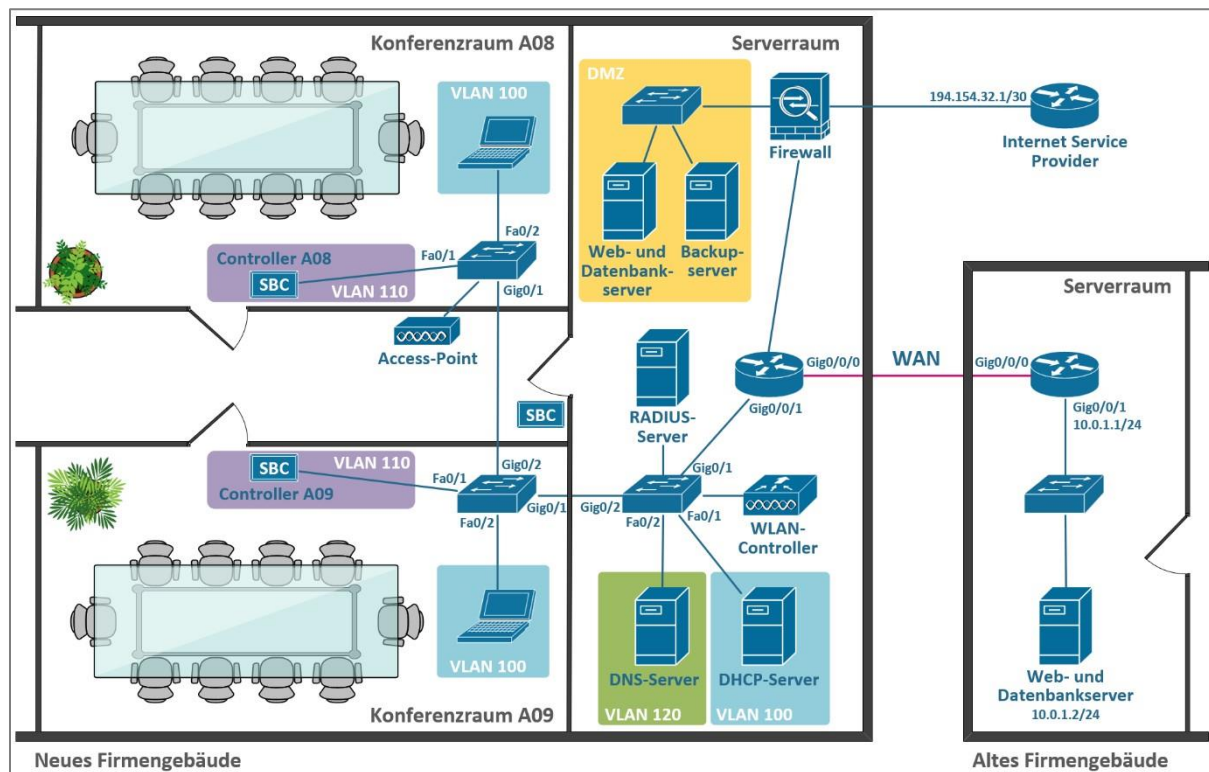


Figure 2

Since IPv6 is becoming increasingly important compared to IPv4, it would be good to extend your simulation so that several network services are available not only via IPv4 but also via IPv6. The choice of IPv6 addresses is up to you.

## 4. Materials list

Number	Designation
1	Raspberry Pi 4
1	Raspberry Pi 15.3W USB-C Power Supply - White
1	16 GB microSD card - Pre-installed NOOBS 3.1
1	Precision mount 18-pin
1	ULN2803 8*Darl-Dr. 50V 0,5A DIP18
1	Omron Relay 2 Form C 5V
2	Post connector 40 pole with strain relief
1	Tub connector 40pin straight
2	RGB LED PL9823
1	Recessed socket for RGB LED PL9823
1	Buzzer 5V - Breadboard friendly
1	Medium Push-Pull Solenoid 5 or 6V
1	Temp. sensor DS18B20+
2	Resistor 18R
1	Resistance 4.7K
1	Resistor 10k
1	Diode 1N4148
1	Contact socket 1*8pin 7mm high
1	DC built-in socket 2.1mm with thread
1	DC-St. 2.1*5.5 long, bend
±11cm	Ribbon cable 40 pin 28AWG grey
12	Spacer roller plastic 5mm

1	Mini Push Button Switch
1	Mifare RC522 IC Card RFID Module Kit
1	1 Printed circuit board according to attached Gerber file
1	Terminal strip RM 5.0 vertical 4-pole
1	Terminal strip RM 2.54 vertical 4-pole
1	Terminal strip RM 2.54 vertical 2-pole
±15cm	Stranded wire red LIYV 0.25 mm
±15cm	Stranded wire black LIYV 0,25mm
2	Wire end ferrules 0,75mm <sup>2</sup>
1	PVC sheet 205*120*3 (mm)
1	Set of multiplex boards (4 pieces according to plan)
1	Aluminium sheet 280*120*2 (mm)
1	Piano tape (175 mm per candidate)
6	Screws 3*8mm wood
-	Adhesive tape for hot glue gun
8	Cylinder head screws M2.5*12
8	Nuts M2.5
4	Cylinder head screws M3*12
8	M3 nuts
4	Countersunk screws M3*10