ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Informatik & Security

fh st.pölten

Assignment 3:
WLAN / 802.1X

Lecture:
Building Computer Networks (BCN)

Study Program:
Bachelor **IT Security (BIS)**

Lecturers:

Gabor Österreicher
gabor.oesterreicher@fhstp.ac.at

Manfred Wirlach
lbwirlach@fhstp.ac.at

Stefan Machherndl
stefan.machherndl@fhstp.ac.at

As of: 17. May 2024

Table of Contents

1 General Information 3

2 Infrastructure Requirements 4
2.1 Server infrastructure 4
2.2 Layer 2/3 infrastructure 4
2.3 WLAN Infrastructure 4
2.4 Network setup (physical connections) 5

3 LAN Authentication 6
3.1 Via Certificate (802.1X Machine Auth): 6
3.2 Via MAC Address (MAB) 6

4 WLAN Authentication 7
4.1 Via AD Account (802.1X User Auth / WPA2-Enterprise) 7
4.2 Via PSK (Guest Auth / WPA2-Personal) 8

5 Administrative Access to Network Components *(optional)* 8

6 Cleanup (after the assignment is finished) 8

7 Appendix 9
7.1 802.1X Config Mode 9
7.2 Save and Reload Configuration from/to Custom File 9
7.3 WLC Software Version 9

1 General Information

Assignment Contents:

- Building a network infrastructure using AAA (switches/routers/WLC/APs/servers) for NAC
- Controller-based WLAN solutions
- Wired & Wireless 802.1X authentication using Microsoft Network Policy Server (NPS)

Equipment required per group:

- 1 WLAN controller (2504 or 3504)
- 2 access points (preferably 2800 or 1800 series, 2700 also possible) + power supplies/PoE-injectors
- 1 L3 switch
- Windows Server (VM)
  - Active Directory (AD)
  - DNS
  - DHCP
  - Certificate Authority (CA)
  - Network Policy Server (NPS)
- Windows 11 Client (VM)
  - Needs to join your Active Directory.
- Internal / DMZ Web Server (VM)
  - Any machine running a web service is sufficient, does not need to be authenticated.
- Non-802.1X Client (VM or personal device)
  - Mimicking a coffee machine (IoT device with restricted MAB access)
  - Needs to be authenticated using MAB.
- Any WLAN device for testing
  - e.g., personal smartphones or laptops

Requirements:

- Be sure to use a **clear documentation style**. Document **all steps and commands** that were necessary to perform the tasks and **include outputs** of those commands as well. **Never use screenshots for commands or CLI output!** Always document those in a textual from using **a monospace font.**
- For all tasks**, document successful configurations** with screenshots, log files, debug output, etc. **and explain** the information shown. (e.g., “show authentication session int gi0/x detail” on the switch, etc.) The `documentation notes` are meant as a bare minimum and should help you with this.
- Include the **final configuration** of your switch as an appendix in your documentation.
- Rule of thumb: Screenshot/Debug/Show command/Logfile … or it didn’t happen! :)
- Make sure that all constraints, installation steps, settings (which are made by your team or deviate from systems default settings) and test scenarios are well documented. Each task/point should lead to a specific configuration that is tested and documented. Screenshots must be readable!
- After completing the assignment (interview), be sure to reset all network components to default configurations and reboot them! **Never (!)** leave switches or routers with configured passwords for console access in the labs.
- Please refer to the Appendix of this document before starting your configuration!

2 Infrastructure Requirements

2.1 Server infrastructure

1. The Windows Server handles the DC (Domain Controller), DNS, DHCP and PKI services**. The domain name (= DNS name) must be "grp*Y*.bcn", where *Y* is your group number** (as found on eCampus). Create all users and groups in the OU "Grp*Y*" and use self-explanatory names for them.
2. You must set and sync the current time on all core network components and servers. Use NTP (Network Time Protocol, time zone: CET) and the L3 switch as NTP server for this.

```
Output of time and NTP status of all network components
Documentation of all clock and NTP settings
```

2.2 Layer 2/3 infrastructure

1. Create a VLAN for each client use case and your infrastructure/backend systems (SSIDs, management, APs, servers, DMZ, clients, etc.)
    a. Use a dedicated management VLAN in which the management IP addresses of the network components (but not those of the servers) are located.

```
Detailed network plan and address plan for the final setup
```

2. Hosts are only allowed to use IP addresses from the VLAN they should be in.
3. DHCP pools are only needed for clients and the AP subnets. Server and management subnets use static IP addressing.
4. Use ACLs to implement various access restrictions.
    a. Implement **all ACLs centrally on the switch** (not on the WLC!) according to the respective subnet's access restrictions.
5. No interface in the entire network should transmit frames from VLANs that are not explicitly required.
6. Protect your network from unexpected BPDUs wherever possible.
7. All links should go to "Forwarding" as quickly as possible, if technically feasible.
8. Simulate "the Internet" by a dedicated loopback interface on the central router. Create the "Internet" loopback interface on the router and assign it the IP address: 13.13.13.13

2.3 WLAN Infrastructure

1. All SSIDs must be optimized for the highest possible data throughput in the 5 GHz frequency band.
2. Activate "Fast SSID Change" on the WLC (best practice setting, and not only useful in the lab)
3. Use a separate VLAN for each use case / each SSID and use dynamic VLAN assignment for this.

2.4 Network setup (physical connections)

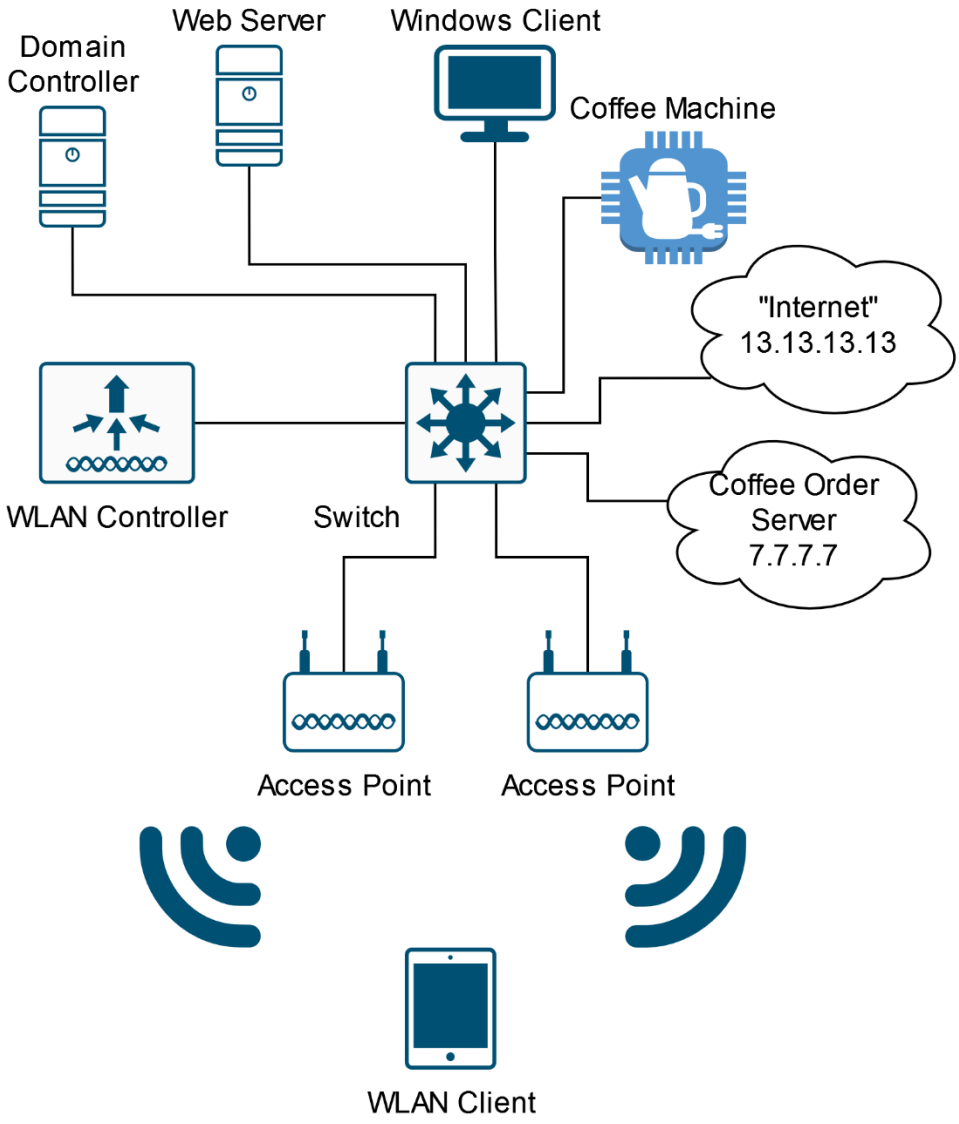

Figure 1: Network Setup

Make sure to first define and document your network plan, including chosen IP addresses, subnets, involved interfaces, VLANs, etc. Discuss your design choice with the lab instructor before you start configuring your network components!

3 LAN Authentication

Note: If problems occur due to the use of VMs as 802.1X clients, set the 802.1X host mode to "multi-auth"!

3.1 Via Certificate (802.1X Machine Auth):

1. Implement LAN EAP-TLS authentication for a Windows 11 client (VM).
    a. Configure the EAP-LAN settings for your Domain clients via Windows Group Policy
2. For LAN access to the network, the client must have a computer account in the domain and a valid certificate from the internal PKI.
    a. Distribute the certificates for the clients automatically via Windows Group Policy
3. Under no circumstances may the clients attempt to authenticate themselves with RADIUS servers outside the company!

```
Documentation of all necessary NPS settings
Documentation of NPS policy set for LAN 802.1X
Documentation of the GPO settings
Documentation of successful distribution of client certificates
Documentation of the successful NPS Authentication Log
Documentation of global switch settings
show run interface <<client interface>>
show authentication session int <<client interface>> details
show mac address-table interface <<client interface>>
```

4. Make sure that (by using ACLs):
    a. Clients with valid certificates have full access to the DMZ and server subnets.
    b. Clients with valid certificates have access to "the internet" via HTTP/HTTPS.
    c. No AD client has access to the management and AP subnets.

```
Documentation of necessary ACLs and interface assignments
```

5. Extend your configuration so that - in contrast to common AD clients - computers in the AD group "Admin PCs" automatically join a VLAN from which full access to the network is permitted.

Note: Test and document the functionality by using the Windows 11 VM!

3.2 Via MAC Address (MAB)

The new coffee machines in the office support automatic ordering of coffee but therefore need network access. According to the manufacturer, the devices do not support 802.1X. The coffee machines use DHCP and must establish connections to an order server (simulated by a dedicated loopback interface on the central router).

1. Ensure that an **additional** check is made for the existence of a known MAC address on each switch port with 802.1X authentication.
2. If the MAC address is known, network access should be granted to the Coffee Machines VLAN.
3. The known MAC addresses are managed centrally at the NPS in a connection request policy.
    a. Cf. https://www.reddit.com/r/sysadmin/comments/dwei0n/comment/f7iynre/

4. Create the order server loopback interface on the router and assign it the IP address: 7.7.7.7

```
Documentation of all necessary NPS settings
Documentation of NPS policy set for LAN MAB
Documentation of the successful NPS Authentication Log
Documentation of global switch settings
show run interface <<client interface>>
show authentication session int <<client interface>> details
show mac address-table interface <<client interface>>
```

5. Make sure that (by using ACLs):
    a. MAB Clients only have access to the order server IP via port 1337/tcp.
    b. No MAB Client should have access to any other subnet.

```
Documentation of necessary ACLs and interface assignments
```

Note: Test and document the functionality on a representative basis with a VM with deactivated 802.1X authentication or a personal computer!

4 WLAN Authentication

4.1 Via AD Account (802.1X User Auth / WPA2-Enterprise)

1. Employees are allowed to connect their smartphones and other private devices to the corporate WLAN with the SSID “Staff-Grp*Y*”. This is achieved by using 802.1X authentication with their AD account.
2. The SSID should be accessible regardless of which frequency bands the connecting devices support.
3. Employees have different permissions in and access to the network, based on their work position:
    a. Create two new groups in your Active Directory, one for Users and one for Admins.
    b. Create at least one user account in each of the 2 groups.
    c. Based on the group membership, the user must be assigned to the correct VLAN automatically

```
Documentation NPS settings for WLAN 802.1X
Documentation global WLC settings
Documentation WLC SSID Settings
Documentation WLAN Client Settings
Documentation Switchport Settings of WLAN components
Documentation ISE Authentication Report
Documentation WLC Client Status (Monitor - Clients) -> IP, VLAN, Security, etc.
Documentation Switch MAC Address Table (Switchports of APs and WLC)
```

4. Make sure that (by using ACLs):
    a. Admins have:
        - access to all subnets

- (Note: This is not a very secure way to authenticate Admins! We use it as a demonstration example to assign multiple VLANs via only one SSID. Consider TEAP or EAP-TLS for admin access in productive environments!)

b. Users have:
   - https access to the DMZ web server
   - http/https access to the “Internet”
   - no access to any other subnet.

```
Documentation of necessary ACLs and interface assignments
```

Note: Test and document the functionality using a Wi-Fi capable device, such as a personal smart phone or notebook

4.2 Via PSK (Guest Auth / WPA2-Personal)

1. Configure a custom SSID “Guest-Grp*Y*” for your guests.
2. The guest WLAN is secured using a WPA2-AES PSK.
3. All guests should only use 2.4 GHz as the common frequency band.
4. Guests should not be able to reach each other.

```
Documentation WLC SSID Settings
Documentation WLC Client Status (Monitor - Clients) -> IP, VLAN, Security, etc.
```

5. Make sure that (by using ACLs):
   a. Guests have http/https access to “the Internet”.
   b. No Guest has access to any other subnet.

```
Documentation of necessary ACLs and interface assignments
```

Note: Test and document the functionality using a Wi-Fi capable device, such as a personal smart phone or notebook

5 Administrative Access to Network Components *(optional)*

1. Administrative access via SSH to the switch should be secured via central AAA.
2. All administrators should be in “Enable Mode” immediately after logging in.
3. Ensure that you are able to log in with a local fallback user in case the RADIUS server is down!

6 Cleanup (after the assignment is finished)

- Reset your WLC to default settings.
- Remove your configurations on the switch.
- Remove and restore all cabling you did/changed in the labs (including the workplace and server room!)
- Return all the used hardware (WLC, APs, power adapters, cables, etc.)

7 Appendix

7.1 802.1X Config Mode

Before you start the configuration, check whether the switches used are operating in 802.1X “Legacy Config Mode”:

```
Switch# authentication display config-mode
Current configuration mode is legacy
```

If a Switch is operating in “new-style” mode (= IBNS 2.0 Mode), then proceed as follows:

1. `Switch#write erase` *or* `erase startup-config`
2. `Switch#reload` (don’t save the config!)
3. `Switch#authentication display legacy`

More Information:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ibns/configuration/15-e/ibns-15-e-book/ibns-cntrl-pol.html

7.2 Save and Reload Configuration from/to Custom File

If needed, preserve your current configuration on the flash memory of network devices for later reuse:

1. `Switch#copy running-config flash:/<grpY-timestamp>.txt`

Reload configuration from custom file to be used by network device during next startup:

1. `Switch#copy flash:/<grpY-timestamp>.txt startup-config`
2. `Switch#reload`

7.3 WLC Software Version

Please check if your WLC is operating on software version 8.5.182.0 or higher:

Figure 2: WLC Software Version

If your WLC is not running the required software version, please notify the lab instructors.