DEMO – Device configurations

Contents

[Introduction 2](#_Toc153466341)

[Scenario 1 2](#_Toc153466342)

[MikroTik 3](#_Toc153466343)

[3COM 4500G 3](#_Toc153466344)

[Corporate WEB and DNS Server 4](#_Toc153466345)

[Cisco 3560 4](#_Toc153466346)

[Ruckus Wireless AP 5](#_Toc153466347)

[Scenario 2 6](#_Toc153466348)

[MikroTik 7](#_Toc153466349)

[Corporate WEB, DNS and DHCP Server 8](#_Toc153466350)

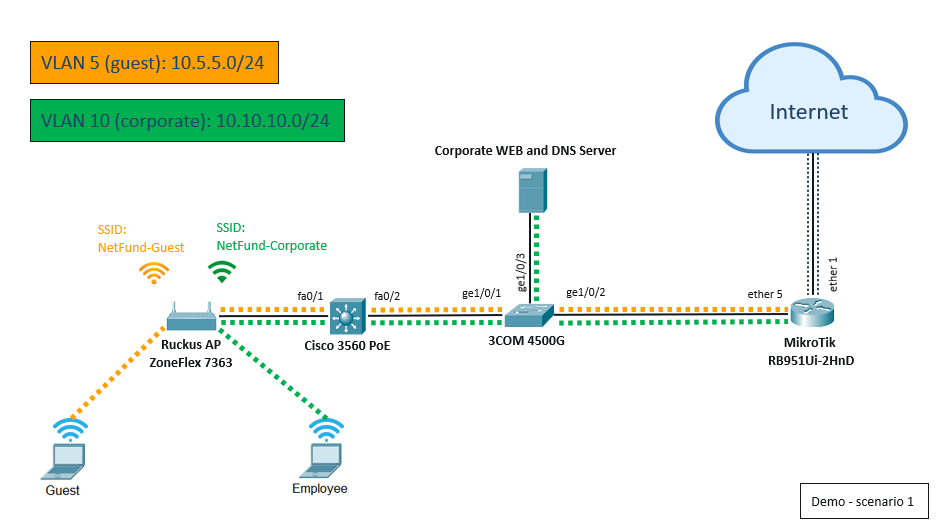
[Cisco 3560 8](#_Toc153466351)

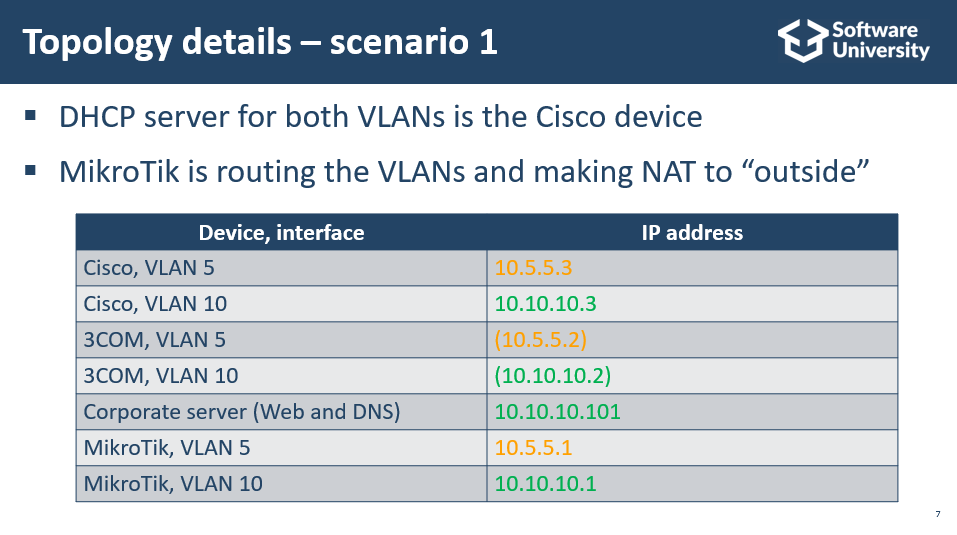
[Ruckus Wireless AP 9](#_Toc153466352)

# Introduction

This document provides a very high-level explanation of the device configurations used in the demonstration in Lecture 9. It does not provide step by step details and can be used just as a reference. The topologies and the detailed configurations are explained in the lecture. For the details, please have a look at the video for Lecture 9.

# Scenario 1





## MikroTik

1. Bridges and interfaces

|  |  |  |  |
| --- | --- | --- | --- |
| Bridge name | Member interfaces | IP address | Details |
| Bridge | ether2, ether3, ether4 | 192.168.99.1 | DHCP server |
| Bridge-WiFi | wlan1 | Automatic (DHCP client) | SNAT (masquerading) has to be configured |
| N/A | ether1 | Automatic (DHCP client) | Default SNAT (masquerading) |
| Bridge-Port5 | ether5 | 10.5.5.1/24  10.10.10.1/24 | VLAN 5  VLAN 10 |

1. Source NAT (masquerading)
   1. From “any” to “Out interface: Bridge-WiFi”, action: “masquerade”
   2. From “any” to “Out interface List: WAN” (default rule), action: “masquerade”
2. Configuration of wlan1 as wireless client
   1. Create a new security profile in Wireless Tables -> Security Profiles and configure it with a name, authentication type and password
   2. Configure wlan1 in wireless mode: “station”, associate it with the security profile created before and scan for WiFi networks
3. [Optional] Create ACL to block the routing between VLAN 5 and VLAN 10

Note: The steps in green are only used when the MikroTik requires wireless connection to the main home router (access point) and because of this acts as a wireless client. This is normally used only during the lab/demo preparation and not used in the actual demonstration. Instead, a wired/cable connection is normally used as it requires less configuration steps and is more reliable.

## 3COM 4500G

1. Baud rate is 19200 (needed for the console connection)
2. G1/0/1 and G1/0/2 should be trunks (do not forget to include all VLANs)
3. G1/0/3 should be access port in VLAN 10
4. IP addresses and default gateway are optional, but useful for testing
5. DNS – entirely for testing purposes (“dns server 8.8.8.8” and “dns resolve”)

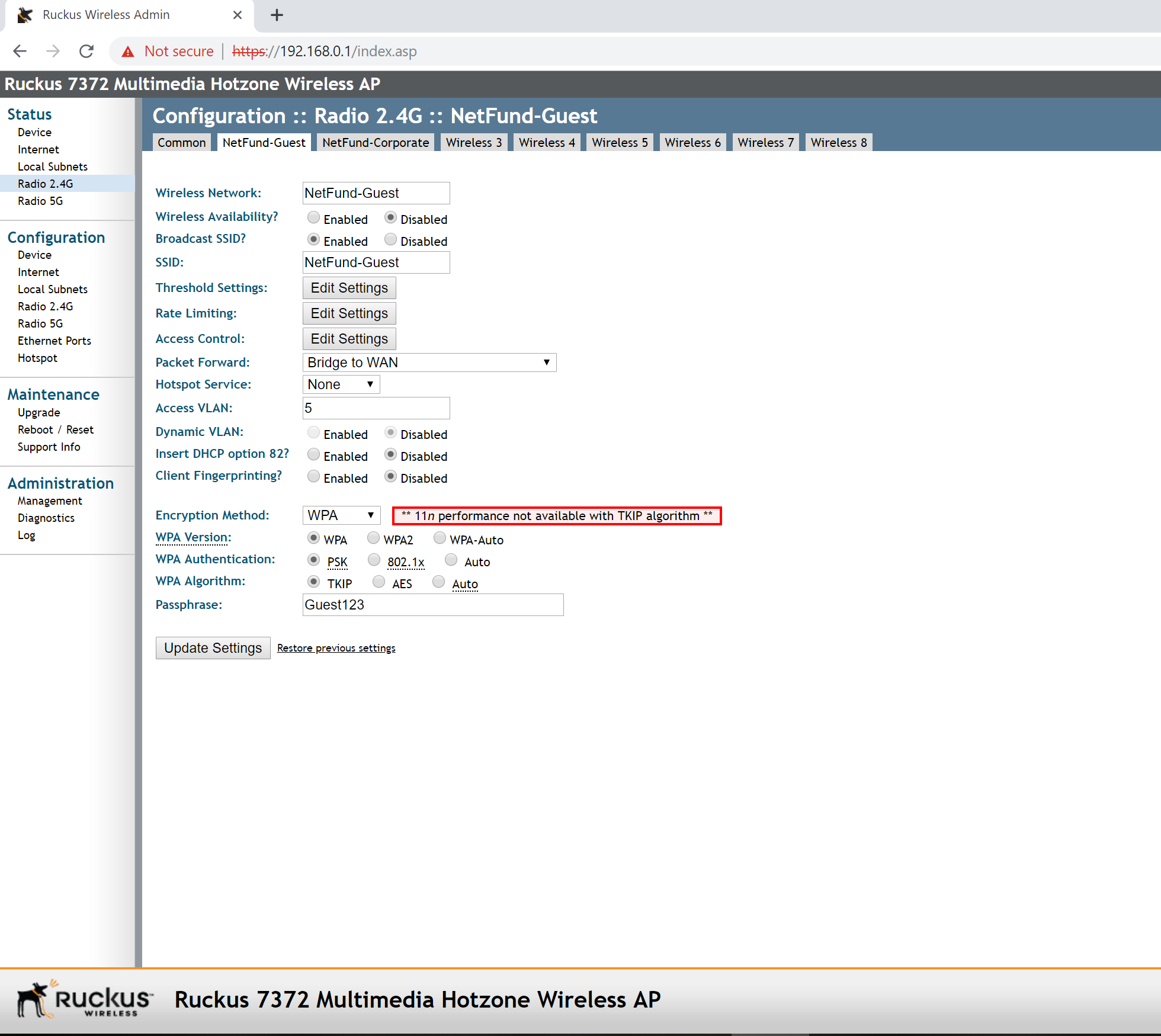
## Corporate WEB and DNS Server

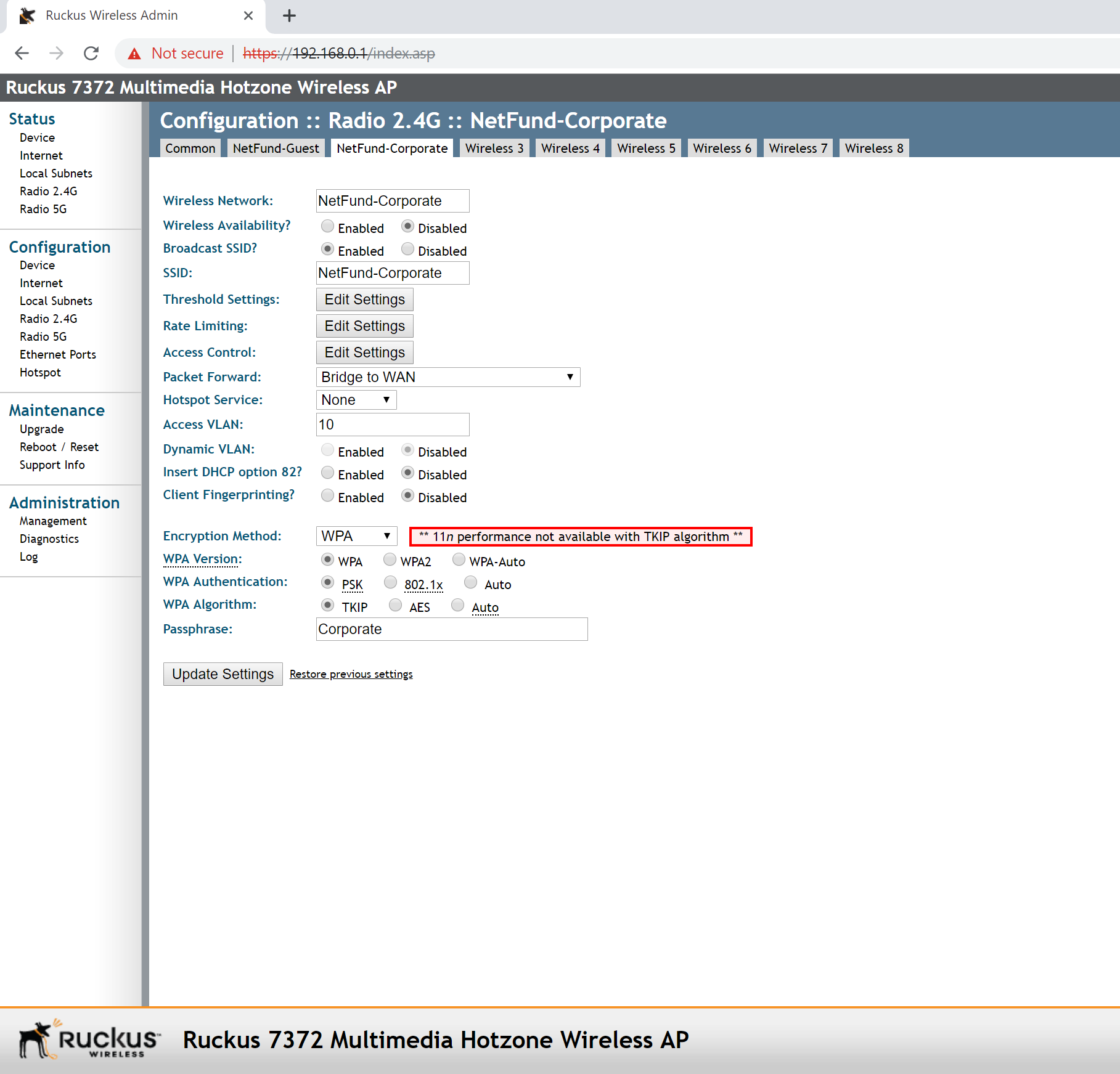
1. The VM inside the laptop uses “External” Hyper-V switch, bridged directly to the LAN card
2. WEB and DNS roles are installed inside the VM
3. The DNS has one zone - “softuni.local” (used only by a corporate/employee network) and has a forwarder to 8.8.8.8 for all other requests
4. The two DNS A records (softuni.local and [www.softuni.local](http://www.softuni.local)) point to 10.10.10.101

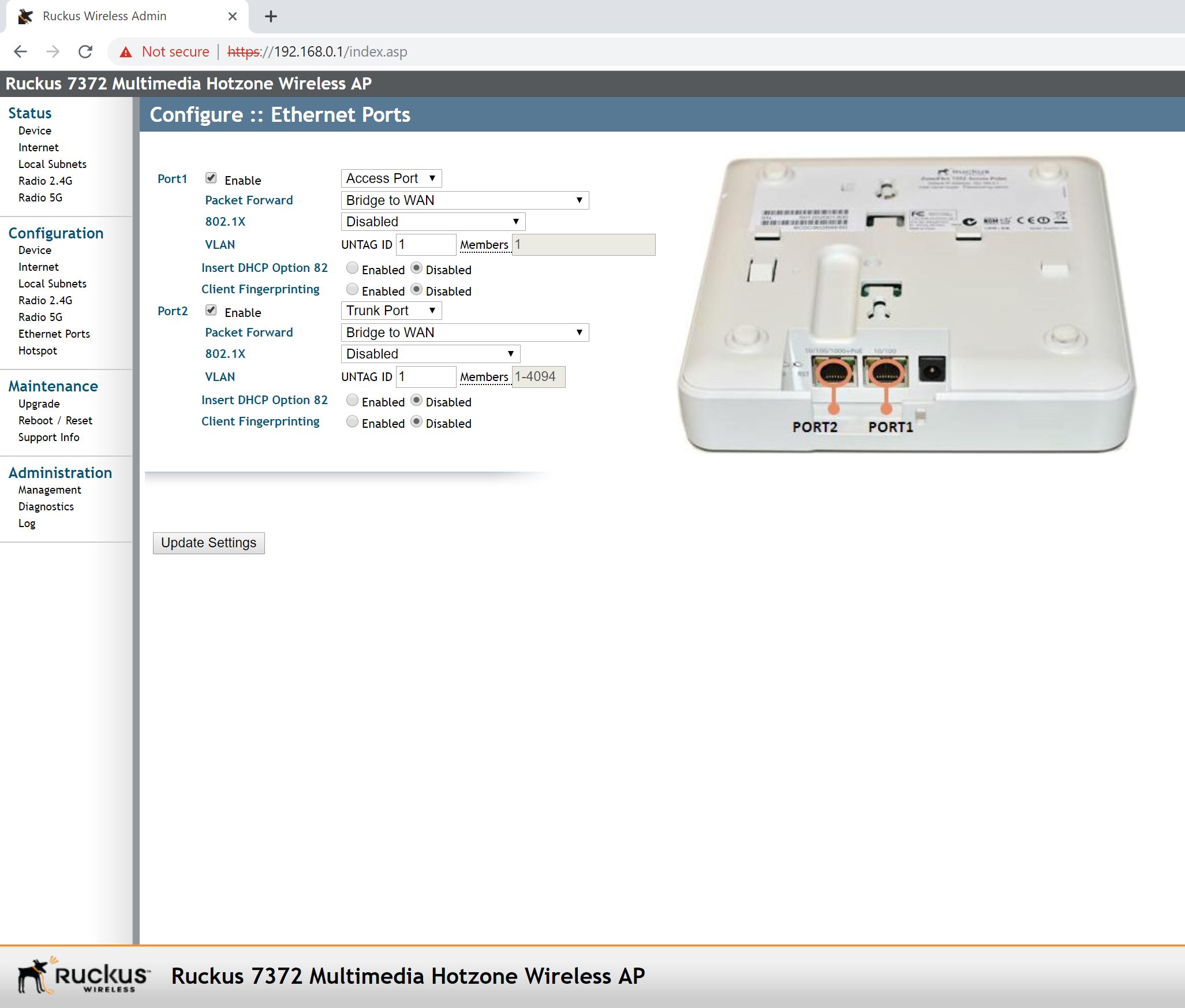
## Cisco 3560

1. VLANs, trunk ports and IP addresses should be created
2. Default gateway is not required but useful for testing. Note the L2/L3 mode of the device
3. DNS – entirely for testing purposes (“ip domain-lookup” and “ip name-server 8.8.8.8”)
4. DHCP scopes and exclusions:
   1. VLAN5 (ip dhcp pool VLAN5; network 10.5.5.0 /24; default-router 10.5.5.1; dns-server 8.8.8.8)
   2. VLAN10 (ip dhcp pool VLAN10; network 10.10.10.0 /24; default-router 10.10.10.1; dns-server 10.10.10.101)
   3. Ip dhcp excluded-address 10.5.5.1, 10.5.5.2, 10.10.10.1, 10.10.10.2, 10.10.10.101

## Ruckus Wireless AP

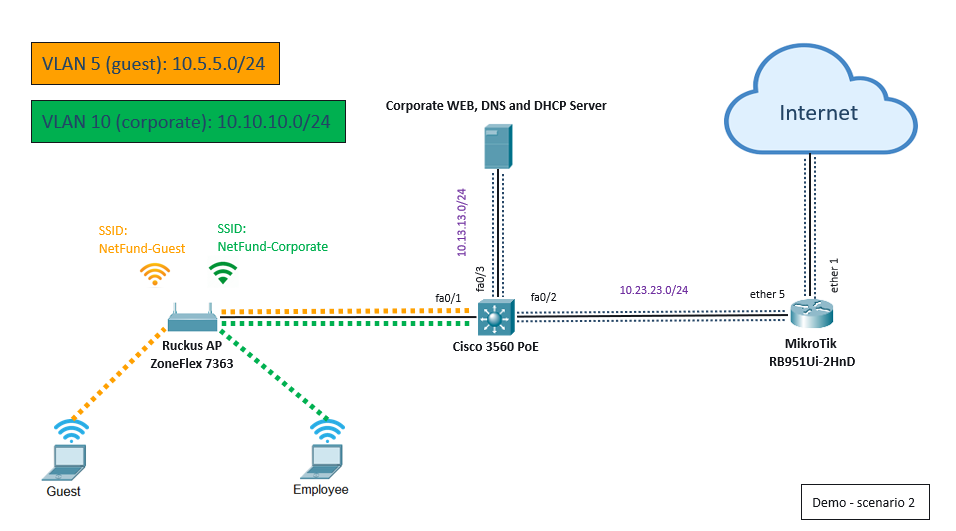


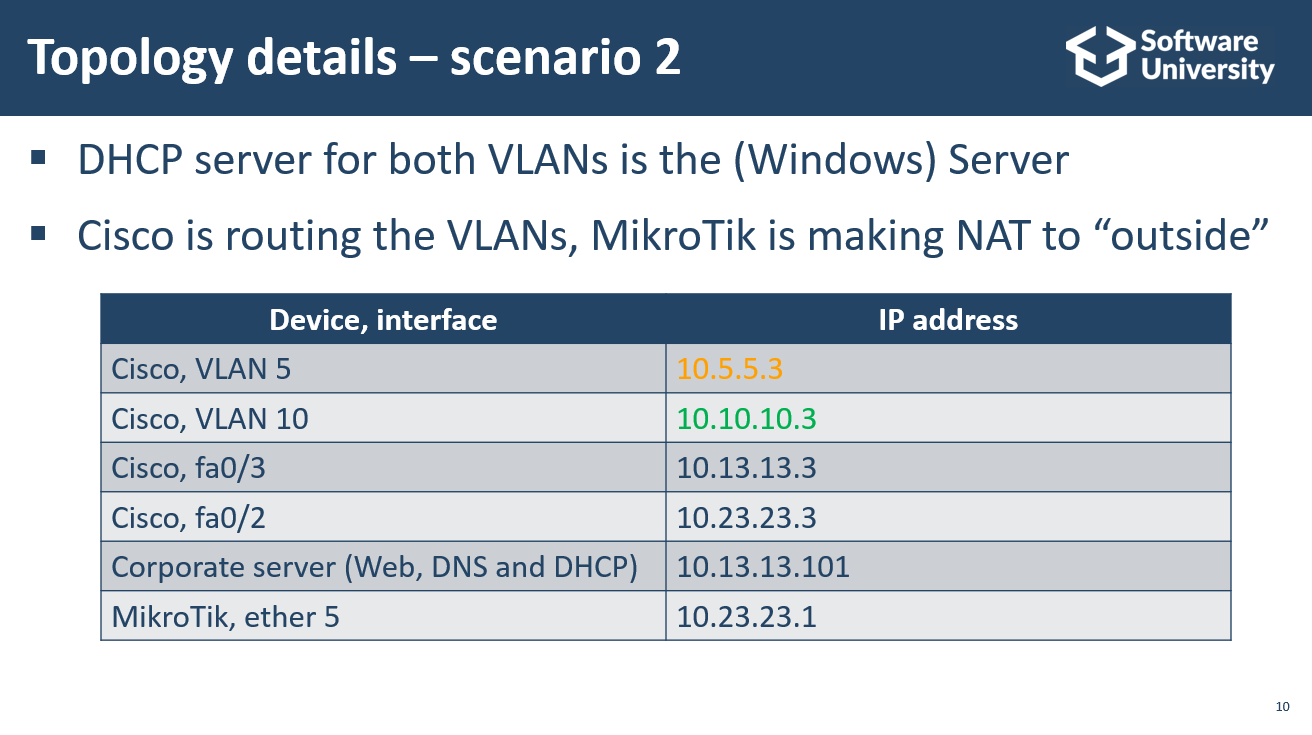






# Scenario 2





## MikroTik

1. Bridges and interfaces

|  |  |  |  |
| --- | --- | --- | --- |
| Bridge name | Member interfaces | IP address | Details |
| Bridge | ether2, ether3, ether4 | 192.168.99.1 | DHCP server |
| Bridge-WiFi | wlan1 | Automatic (DHCP client) | SNAT (masquerading) has to be configured |
| N/A | ether1 | Automatic (DHCP client) | Default SNAT (masquerading) |
| Bridge-Port5 | ether5 | 10.23.23.1 | N/A |

1. Source NAT (masquerading)
   1. From “any” to “Out interface: Bridge-WiFi”, action: “masquerade”
   2. From “any” to “Out interface List: WAN” (default rule), action: “masquerade”
2. Configuration of wlan1 as wireless client
   1. Create a new security profile in Wireless Tables -> Security Profiles and configure it with a name, authentication type and password
   2. Configure wlan1 in wireless mode: “station”, associate it with the security profile created before and scan for WiFi networks
3. Static routing. The device will do NAT to outside, but the Cisco 3560 in the inside network will route from different subnets, that is why a static route to 10.0.0.0/8 is needed (using ether5 or pointing to 10.23.23.3)

Note: Separate routes to 10.5.5.0/24, 10.10.10.0/24 and 10.13.13.0/24 will also work here.

Note: The steps in green are only used when the MikroTik requires wireless connection to the main home router (access point) and because of this acts as a wireless client. This is normally used only during the lab/demo preparation and not used in the actual demonstration. Instead, a wired/cable connection is normally used as it requires less configuration steps and is more reliable.

## Corporate WEB, DNS and DHCP Server

Changes from Scenario 1 include:

1. DHCP role installed and configured with the following scopes:
   1. VLAN5-Guests (Pool: 10.5.5.10-10.5.5.50, Default gateway: 10.5.5.3, DNS: 8.8.8.8)
   2. VLAN10-Corp (Pool: 10.10.10.10-10.10.10.50, Default gateway: 10.10.10.3, DNS: 10.13.13.101)
2. IP address of the VM (hosting the three services) changed to 10.13.13.101
3. Default gateway of the VM changed to 10.13.13.3 (Cisco 3560)
4. The two DNS A records (for softuni.local and www.softuni.local) changed to 10.13.13.101

## Cisco 3560

1. VLANs, trunk ports and IP addresses should be created (use the “no switchport” command to configure IP addresses directly on Fa0/2 and Fa0/3)
2. Default gateway is required. Note the L2/L3 mode of the device (L3 is required in this scenario)
3. DNS – entirely for testing purposes (“ip domain-lookup” and “ip name-server 8.8.8.8”)
4. DHCP relay for VLAN 5 and VLAN 6, pointing to 10.13.13.101

## Ruckus Wireless AP

This device has the same configuration as from Scenario 1.