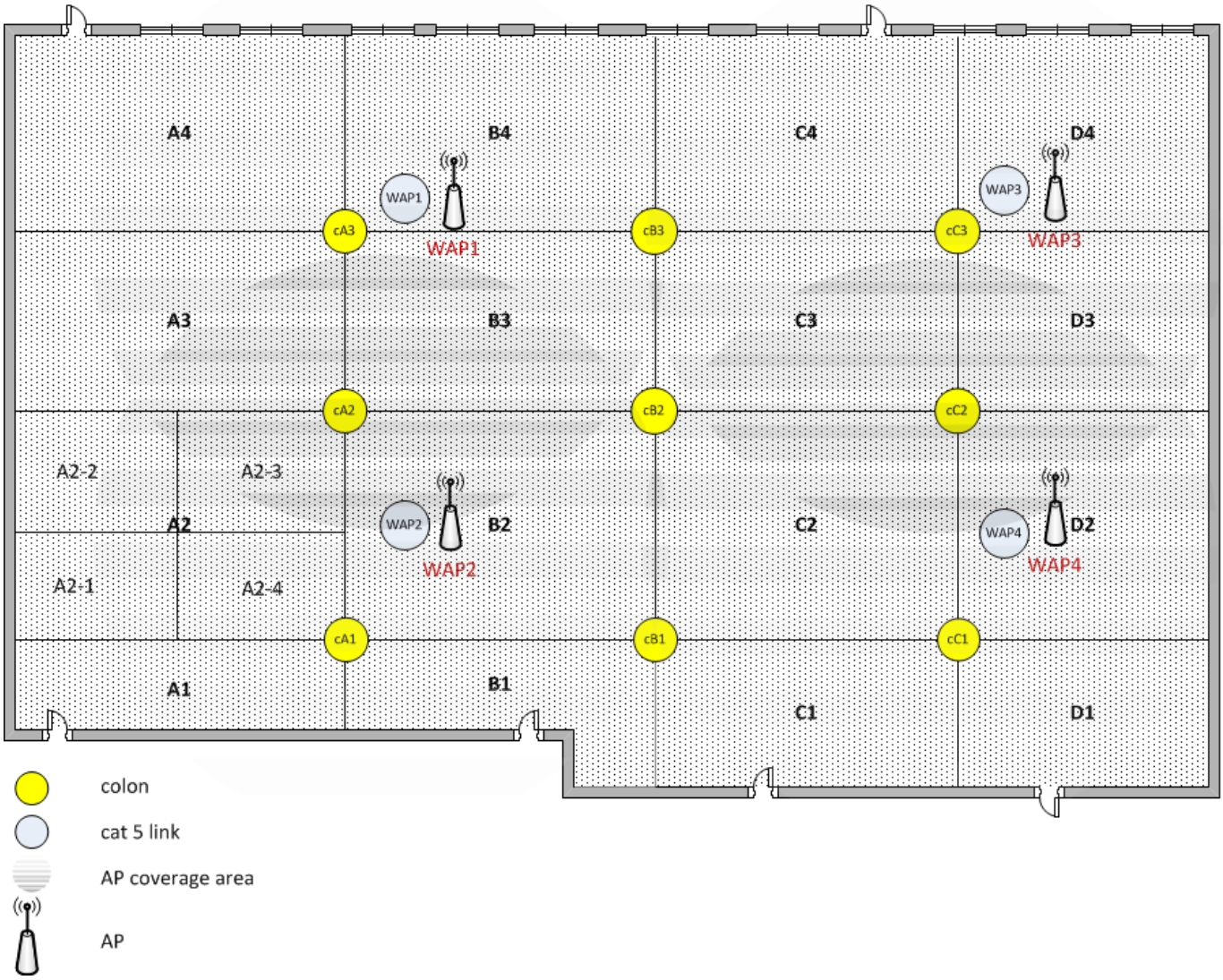
Wireless network based on Mikrotik Mesh

Pros of this kind of configuration: One single SSID for clients and seamless roaming.

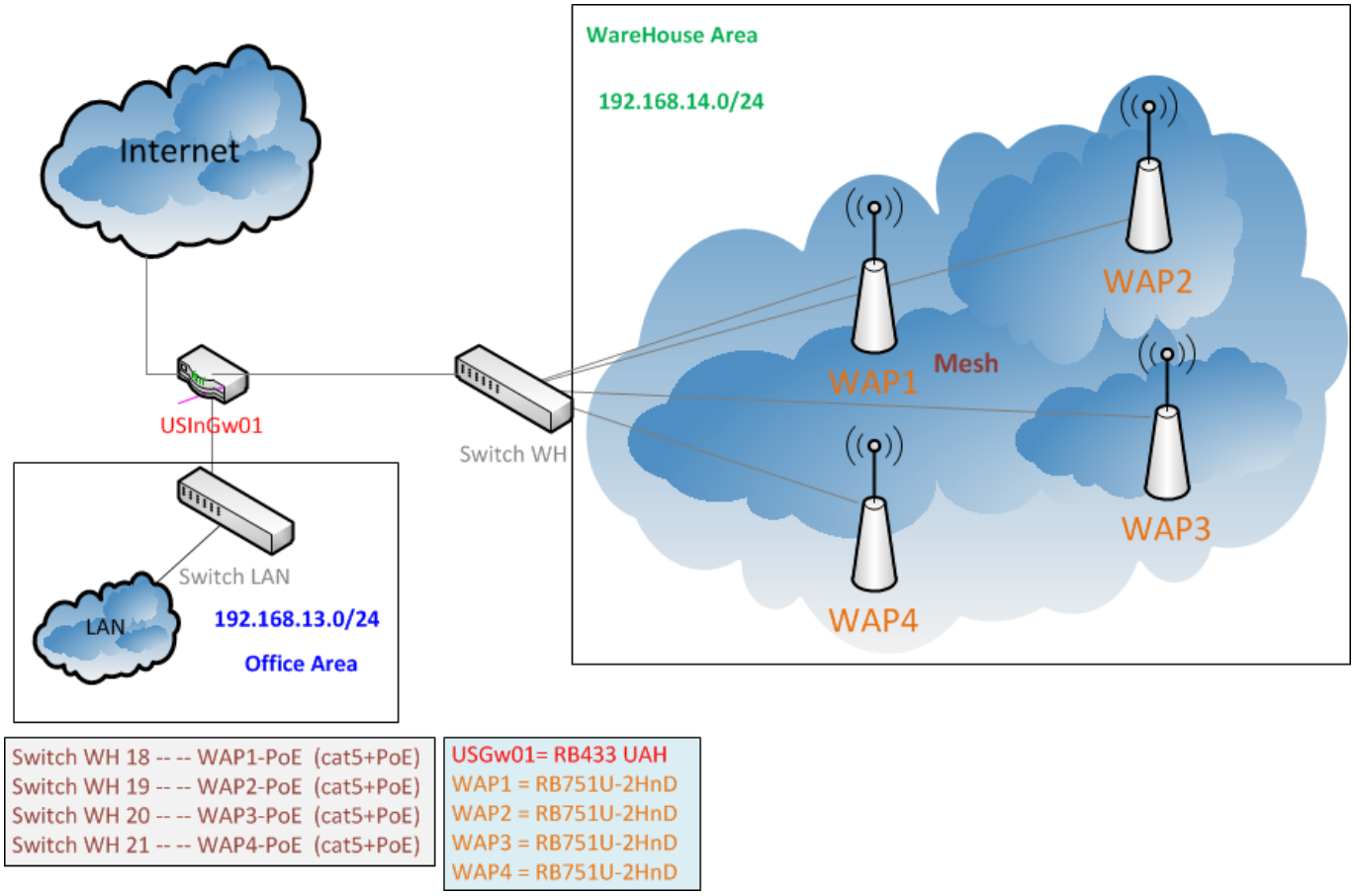
Here is the complete configuration example of a wireless network based on Mikrotik mesh with all Router OS code ready to copy/paste into terminal.

Example shown here is purposed for wireless scanners inside a warehouse.

Warehouse map:



Network map:



General Description

1. We use USGw01(RB433UAH) for Internet access of entire office(Office Area).
2. USGw01 also used for Mesh Setup as DHCP Server and Firewall.
3. On warehouse we use Wireless Barcode Scanners - Symbol MC3090 as wireless clients.
4. They are working only with server in LAN(Office Area).
5. Scanners should have access only for DNS server(for name resolving) and for WarehouseServer.
6. All WAP have Static IP.
7. All Scanners have Dynamic IP obtained from DHCP Server(USGw01).
8. In this setup Wireless security settings are not described. And you will get network secured only by MAC. If you want to secure your WAP by authentication you should create an appropriate security profile and assign it to your WAP interface - on all WAP.

RB433UAH

```
# add mesh interface
interface mesh add name=mesh-interface
# assign ports to the mesh interface
interface mesh port add interface=ether2-warehouse mesh=mesh-interface
# add ip to the mesh interface
ip address add address=192.168.14.1/24 interface=mesh-interface
```

```
ip pool add name=warehouse-dhcp-ip-pool ranges=192.168.14.230-192.168.14.253
ip dhcp-server add name=warehouse-dhcp-server interface=mesh-interface
lease-time=12:00:00 address-pool=warehouse-dhcp-ip-pool always-broadcast=yes
disabled=no
ip dhcp-server network add address=192.168.14.0/24 gateway=192.168.14.1
```

```
netmask=24 dns-server=192.168.13.1
```

```
# T001
ip dhcp-server lease add address=192.168.14.231 mac-
address=00:00:00:00:00:01 server=warehouse-dhcp-server lease-time=0 address-
list=US-WH-Scanners disabled=no comment="Scanner T001"
# T002
ip dhcp-server lease add address=192.168.14.232 mac-
address=00:00:00:00:00:02 server=warehouse-dhcp-server lease-time=0 address-
list=US-WH-Scanners disabled=no comment="Scanner T002"
```

```
system ntp client set enabled=yes mode=unicast primary-ntp=64.73.32.134
secondary-ntp=38.229.71.1
```

```
system ntp server set broadcast=no broadcast-addresses="" enabled=yes
manycast=no multicast=no
```

```
ip firewall address-list add address=192.168.13.1 comment="admin01"
disabled=no list=Gw-admins
ip firewall address-list add address=192.168.13.2 comment="linux for backups
to SVN" disabled=no list=Gw-admins
ip firewall address-list add address=192.168.13.1 disabled=no list=US-Srv-
DNS
ip firewall address-list add address=192.168.13.1 disabled=no list=US-Srv-
WareHouseServer
ip firewall address-list add address=192.168.14.201 comment=WAP1 disabled=no
list=US-WH-WAP
ip firewall address-list add address=192.168.14.202 comment=WAP2 disabled=no
list=US-WH-WAP
ip firewall address-list add address=192.168.14.203 comment=WAP3 disabled=no
list=US-WH-WAP
ip firewall address-list add address=192.168.14.204 comment=WAP4 disabled=no
list=US-WH-WAP
# US-WH-Scanners - dynamic via DHCP
```

```
# Input chain
ip firewall filter add action=accept chain=input comment="Drop invalid
connections" connection-state=invalid disabled=no
ip firewall filter add action=accept chain=input comment="Allow Established
connections to Gateway" connection-state=established disabled=no
ip firewall filter add action=accept chain=input comment="Allow Related
connections to Gateway" connection-state=related disabled=no
ip firewall filter add action=accept chain=input comment="Allow SG Network
Core: NTP on LAN" disabled=no dst-port=123 in-interface=!ether1-wan-primary
protocol=udp
# Forward chain
#
# General rules
ip firewall filter add action=accept chain=forward comment="Drop invalid
connections" connection-state=invalid disabled=no
ip firewall filter add action=accept chain=forward comment="Allow
```

```
Established connections to Any" connection-state=established disabled=no
ip firewall filter add action=accept chain=forward comment="Allow Related
connections to Any" connection-state=related disabled=no
# From Mesh to LAN
ip firewall filter add action=accept chain=forward comment="Allow Network
Core: ICMP from Mesh" disabled=no in-interface=mesh-wap out-
interface=bridge-lan protocol=icmp
ip firewall filter add action=accept chain=forward comment="Allow Scanners
to DNS - US-WH-Scanners" disabled=no dst-address-list=US-Srv-DNS dst-port=53
in-interface=mesh-wap out-interface=bridge-lan protocol=udp src-address-
list=US-WH-Scanners
ip firewall filter add action=accept chain=forward comment="Allow Scanners
to WareHouseServer - US-WH-Scanners" disabled=no dst-address-list=US-Srv-
WareHouseServer dst-port=80 in-interface=mesh-wap out-interface=bridge-lan
protocol=tcp src-address-list=US-WH-Scanners
ip firewall filter add action=log chain=forward comment="Log any other from
scanners" disabled=yes in-interface=mesh-wap
ip firewall filter add action=drop chain=forward comment="Drop any other
from scanners" disabled=no in-interface=mesh-wap
# From LAN to Mesh
ip firewall filter add action=accept chain=forward comment="Allow SG Network
Core: ICMP to WAP" disabled=no dst-address-list=US-WH-WAP in-
interface=!ether1-wan-primary out-interface=mesh-wap protocol=icmp
ip firewall filter add action=accept chain=forward comment="Allow SG Network
Core: ICMP to Scanners" disabled=no dst-address-list=US-WH-Scanners in-
interface=!ether1-wan-primary out-interface=mesh-wap protocol=icmp
ip firewall filter add action=accept chain=forward comment="Allow SG Remote
Access: Winbox for admins on WAP" disabled=no dst-port=8291 in-
interface=!ether1-wan-primary out-interface=mesh-wap protocol=tcp src-
address-list=Gw-admins
ip firewall filter add action=accept chain=forward comment="Allow SG Remote
Access: SSH for backup WAP" disabled=no dst-port=22 in-interface=!ether1-
wan-primary out-interface=mesh-wap protocol=tcp src-address-list=Gw-admins
ip firewall filter add action=accept chain=forward comment="Allow SG
Monitoring: SNMP on WAP segment" disabled=no dst-port=161 in-
interface=bridge-lan out-interface=mesh-wap protocol=udp
ip firewall filter add action=log chain=forward comment="Log any other to
scanners" disabled=yes out-interface=mesh-wap
ip firewall filter add action=drop chain=forward comment="Drop any other to
scanners" disabled=no out-interface=mesh-wap
```

RB751U-2HnD

```
# WAP1/WAP2/WAP3/WAP4
system
routerboard
dhcp
wireless
security
advanced-tools
```

```
# WAP1/WAP2/WAP3/WAP4
interface mesh add name=mesh-interface
interface mesh port add interface=ether1 mesh=mesh-interface
interface mesh port add interface=wlan1 mesh=mesh-interface
```

```
# WAP1
ip address add address=192.168.14.201/24 interface=mesh-interface
# WAP2
ip address add address=192.168.14.202/24 interface=mesh-interface
# WAP3
ip address add address=192.168.14.203/24 interface=mesh-interface
# WAP4
ip address add address=192.168.14.204/24 interface=mesh-interface
```

```
# WAP1/WAP2/WAP3/WAP4
interface wireless set wlan1 disabled=no mode=ap-bridge band=2ghz-b/g/n
frequency=2452 ssid=Mikrotik-Mesh default-authentication=no default-
forwarding=no
```

```
# WAP1/WAP2/WAP3/WAP4
#
# ban Scanners with low signal strength
interface wireless access-list add interface=wlan1 mac-
address=00:00:00:00:00:00 signal-range=-80 authentication=no forwarding=no
```

```
# WAP1/WAP2/WAP3/WAP4
#
# T001
interface wireless access-list add disabled=no authentication=yes
forwarding=no interface=wlan1 mac-address=00:00:00:00:00:01 comment="Scanner
T001"
# T002
interface wireless access-list add disabled=no authentication=yes
forwarding=no interface=wlan1 mac-address=00:00:00:00:00:02 comment="Scanner
T002"
```

```
# WAP1/WAP2/WAP3/WAP4
ip route add dst-address=0.0.0.0/0 gateway=192.168.14.1
```

```
# WAP1/WAP2/WAP3/WAP4
ip service set ssh port=22
```

```
# WAP1/WAP2/WAP3/WAP4
system clock set time-zone-name=America/Detroit
system ntp client set enabled=yes mode=unicast primary-ntp=192.168.14.1
```

```
# WAP1/WAP2/WAP3/WAP4
ip service disable ftp
ip service disable telnet
ip service disable www
```

```
ip service disable www-ssl
```

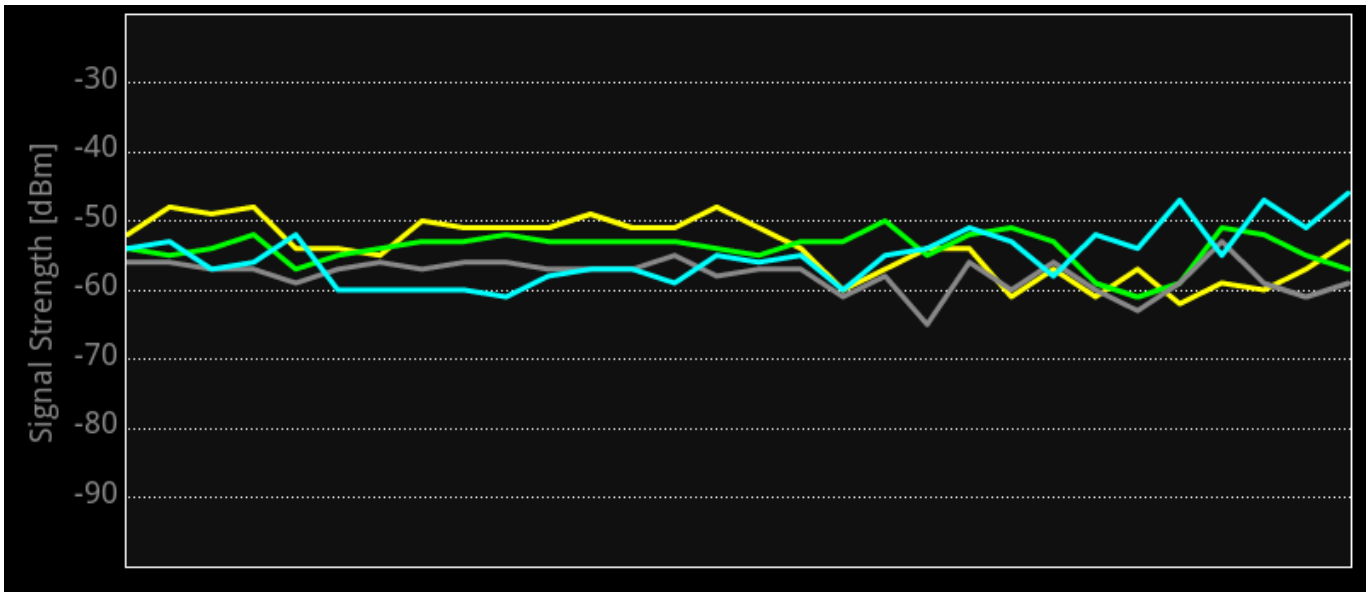
```
# WAP1/WAP2/WAP3/WAP4
/user group add name=monitoring policy=winbox,read comment="Group for
monitoring purpose"
/user add name=dude password="********" group=monitoring
address=192.168.13.1/32 comment="User for Dude monitoring"
```

Add new scanner to Warehouse wireless network

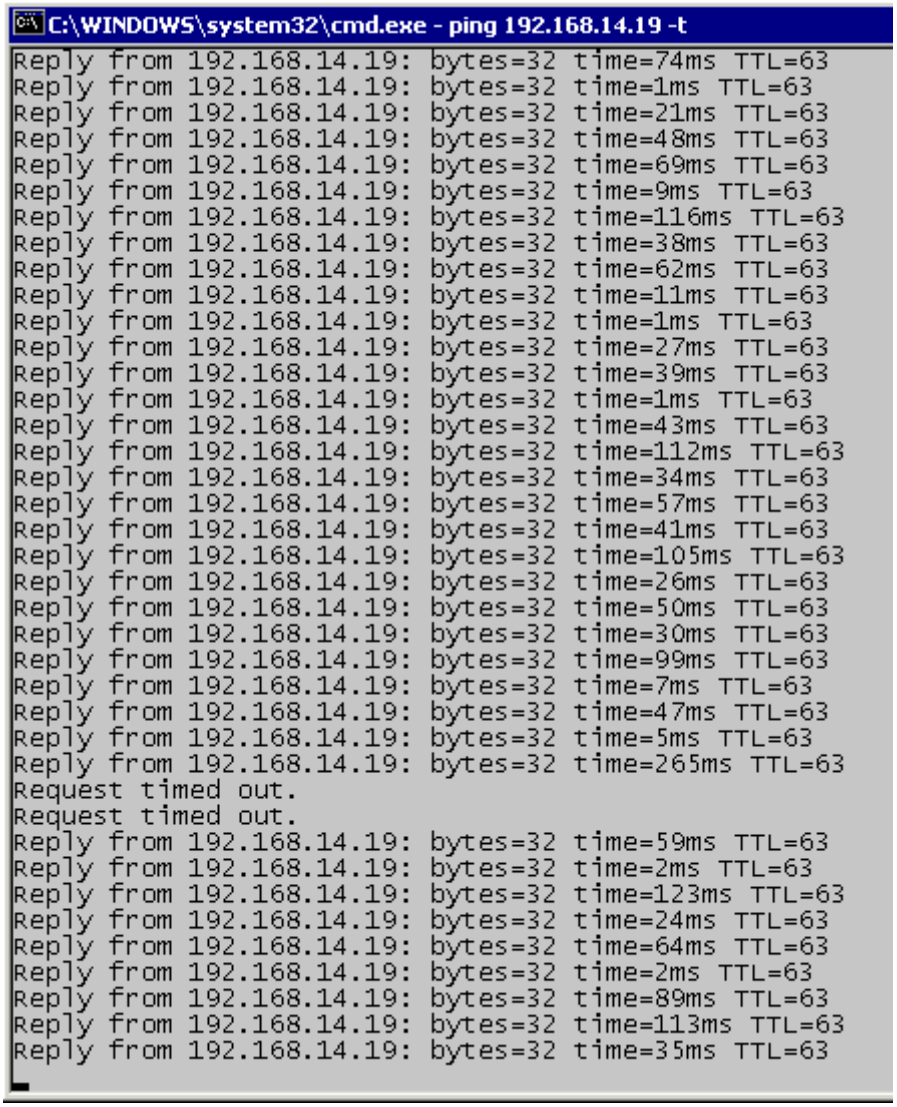
```
# This must be done on all AP in Mesh
# T0XY
interface wireless access-list add disabled=no authentication=yes
forwarding=no interface=wlan1 mac-address=00:00:00:00:00:03 comment="Scanner
T0XY"
```

```
# T0XY
ip dhcp-server lease add address=192.168.14.2zz mac-
address=00:00:00:00:00:03 server=warehouse-dhcp-server lease-time=0 address-
list=US-WH-Scanners disabled=no comment="Scanner T0XY"
```

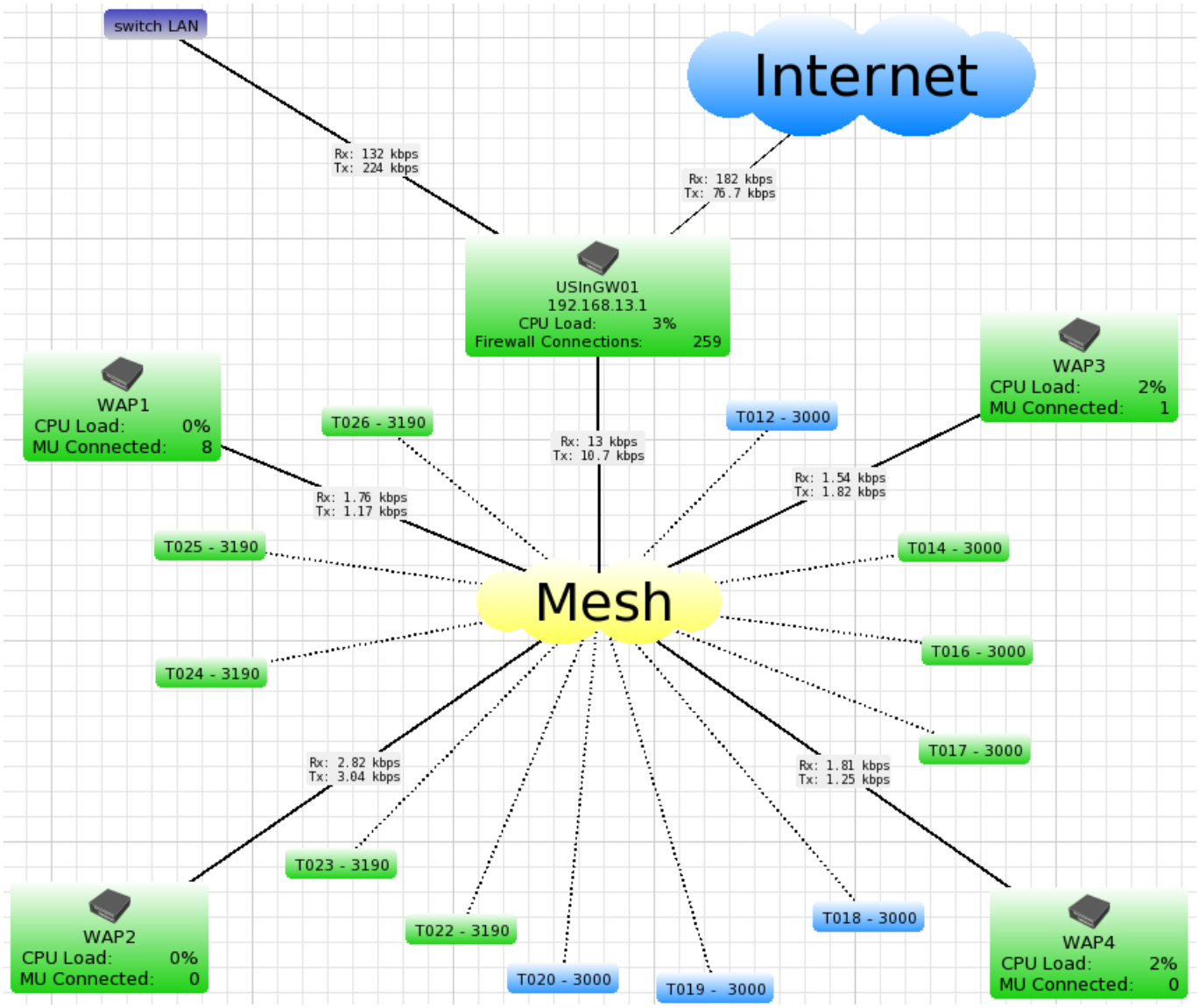
Testing WareHouse perimeter:



Test (Android) when WAP1 goes down, device connect to WAP2


C:\WINDOWS\system32\cmd.exe - ping 192.168.14.19 -t
Reply from 192.168.14.19: bytes=32 time=74ms TTL=63
Reply from 192.168.14.19: bytes=32 time=1ms TTL=63
Reply from 192.168.14.19: bytes=32 time=21ms TTL=63
Reply from 192.168.14.19: bytes=32 time=48ms TTL=63
Reply from 192.168.14.19: bytes=32 time=69ms TTL=63
Reply from 192.168.14.19: bytes=32 time=9ms TTL=63
Reply from 192.168.14.19: bytes=32 time=116ms TTL=63
Reply from 192.168.14.19: bytes=32 time=38ms TTL=63
Reply from 192.168.14.19: bytes=32 time=62ms TTL=63
Reply from 192.168.14.19: bytes=32 time=11ms TTL=63
Reply from 192.168.14.19: bytes=32 time=1ms TTL=63
Reply from 192.168.14.19: bytes=32 time=27ms TTL=63
Reply from 192.168.14.19: bytes=32 time=39ms TTL=63
Reply from 192.168.14.19: bytes=32 time=1ms TTL=63
Reply from 192.168.14.19: bytes=32 time=43ms TTL=63
Reply from 192.168.14.19: bytes=32 time=112ms TTL=63
Reply from 192.168.14.19: bytes=32 time=34ms TTL=63
Reply from 192.168.14.19: bytes=32 time=57ms TTL=63
Reply from 192.168.14.19: bytes=32 time=41ms TTL=63
Reply from 192.168.14.19: bytes=32 time=105ms TTL=63
Reply from 192.168.14.19: bytes=32 time=26ms TTL=63
Reply from 192.168.14.19: bytes=32 time=50ms TTL=63
Reply from 192.168.14.19: bytes=32 time=30ms TTL=63
Reply from 192.168.14.19: bytes=32 time=99ms TTL=63
Reply from 192.168.14.19: bytes=32 time=7ms TTL=63
Reply from 192.168.14.19: bytes=32 time=47ms TTL=63
Reply from 192.168.14.19: bytes=32 time=5ms TTL=63
Reply from 192.168.14.19: bytes=32 time=265ms TTL=63
Request timed out.
Request timed out.
Reply from 192.168.14.19: bytes=32 time=59ms TTL=63
Reply from 192.168.14.19: bytes=32 time=2ms TTL=63
Reply from 192.168.14.19: bytes=32 time=123ms TTL=63
Reply from 192.168.14.19: bytes=32 time=24ms TTL=63
Reply from 192.168.14.19: bytes=32 time=64ms TTL=63
Reply from 192.168.14.19: bytes=32 time=2ms TTL=63
Reply from 192.168.14.19: bytes=32 time=89ms TTL=63
Reply from 192.168.14.19: bytes=32 time=113ms TTL=63
Reply from 192.168.14.19: bytes=32 time=35ms TTL=63

The Dude:



Comments

1. Clients see only one network with SSID Mikrotik-Mesh and they don't know anything about 4 AP.
2. Tested on ROS 5.18.
3. Scanners are Motorola Symbol MC3100.
4. Very low traffic from scanners.
5. Scanners have access only to DNS and Web servers in LAN.

Hopefully this will be useful for someone. Original article on forum here.