SWITCH - 2960

```
> en
# conf t
(config)# hostname SwNetworkName
(config)# no ip domain-lookup
(config)# no cdp run
(config)# service password-encryption
(config)# enable secret ciscosecpa55
(config)# enable password ciscoenapa55
(config)# spanning-tree mode rapid-pvst
(config)# banner motd "Vineri la ora 14 serverul va intra in mentenata!"
(config)# ip domain name sal.ro
(config)# username Admin01 privilege 15 secret Admin01pa55
(config)# crypto key generate rsa
2048
(config)# ip ssh version 2
(config)# ip ssh time-out 90
(config)# ip ssh authentication-retries 3
(config)# logging host ServerIp
(config)# service timestamps log datetime msec
(config)# service timestamps debug datetime msec
(config)# line console 0
(config-line)# password ciscoconpa55
(config-line)# login
(config-line)# logging synchronous
(config-line)# exec-timeout 15 20
(config-line)# exit
(config)# line vty 0 15
(config-line)# password ciscovtypa55
(config-line)# login
(config-line)# logging synchronous
(config-line)# exec-timeout 15 20
(config-line)# transport input ssh
(config-line)# login local
(config-line)# exit
(config)# interface vlan 1
(config-if)# description Legatura cu ramura X
(config-if)# ip address SwIpAddress NetworkMask
(config-if)# no sh
(config-if)# exit
(config)# ip default-gateway IpDefaultGateway
(config)# interface range fastEthernet 0/1-24
(config-if-range)# sh
(config-if-range)# exit
(config)# ntp server ServerIp key 1
```

```
(config)# ntp authenticate
(config)# ntp trusted-key 1
(config)# ntp authentication-key 1 md5 NTPpa55
(config)# end
# copy running-config startup-config
```

ROUTER - 2911

```
> en
# conf t
(config)# hostname RNetworkName
(config)# no ip domain-lookup
(config)# no cdp run
(config)# service password-encryption
(config)# security passwords min-length 10
(config)# login block-for 60 attempts 3 within 15
(config)# enable secret ciscosecpa55
(config)# enable password ciscoenapa55
(config)# banner motd "Vineri la ora 14 serverul intra in mentenanta!"
(config)# banner login "Accesul strict interzis persoanelor neautorizate!"
(config)# ip domain name sal.ro
(config)# username Admin01 privilege 15 secret Admin01pa55
(config)# crypto key generate rsa
2048
(config)# ip ssh version 2
(config)# ip ssh time-out 90
(config)# ip ssh authentication-retries 3
(config)# logging host IpDnsServer
(config)# service timestamps log datetime msec
(config)# service timestamps debug datetime msec
(config)# line console 0
(config-line)# password ciscoconpa55
(config-line)# login
(config-line)# logging synchronous
(config-line)# exec-timeout 15 20
(config-line)# exit
(config)# line vty 0 15
(config-line)# password ciscovtypa55
(config-line)# login
(config-line)# logging synchronous
(config-line)# exec-timeout 15 20
(config-line)# transport input ssh
(config-line)# login local
(config-line)# exit
(config)# interface gigabitEthernet 0/0
(config-if)# description Legatura cu SwDaisy
```

```
(config-if)# ip address 192.168.10.1 255.255.255.0
(config-if)# no sh
(config-if)# ip ospf message-digest-key 1 md5 MD5pa55
(config-if)# exit
(config)# interface GigabitEthernet 0/1
(config-if)# description Legatura cu Wi-FiDaisy
(config-if)# ip address 10.10.10.5 255.255.255.252
(config-if)# no sh
(config-if)# ip ospf message-digest-key 1 md5 MD5pa55
(config-if)# exit
(config)# interface Serial 0/0/0
(config-if)# description Legatura cu RDonald
(config-if)# ip address 10.10.10.9 255.255.255.252
(config-if)# no sh
(config-if)# ip ospf message-digest-key 1 md5 MD5pa55
(config-if)# exit
(config)# router ospf 1
(config-router)# network 192.168.10.0 0.0.0.255 area 0
(config-router)# network 10.10.10.4 0.0.0.3 area 0
(config-router)# network 10.10.10.8 0.0.0.3 area 0
(config-router)# passive-interface gigabitEthernet 0/2
(config-router)# passive-interface serial 0/0/1
(config-router)# area 0 authentication message-digest
(config-router)# exit
(config)# ntp server 192.168.20.254 key 1
(config)# ntp authenticate
(config)# ntp trusted-key 1
(config)# ntp authentication-key 1 md5 NTPpa55
(config)# ntp update-calendar
```

DHCP (closest router to the server)

```
(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.11
(config)# ip dhcp pool NetworkName
(dhcp-config)# network 192.168.10.0 255.255.255.0
(dhcp-config)# default-router 192.168.10.1
(dhcp-config)# dns-server 192.168.20.254
(dhcp-config)# domain-name sal.ro
(dhcp-config)# end
# copy running-config startup-config
```

DHCP (on routers where we want DHCP)

```
(config)# interface GigabitEthernet 0/0
(config-if)# ip helper-address 10.10.10.10
(config-if)# end
# copy running-config startup-config
```

Wi-FiDaisy - WRT300N

Connect Service Laptop (FastEthernet0) to Wi-FiDaisy WRT300N (Ethernet 1). In Service Laptop go to Desktop > Web Browser > 192.168.0.1 and enter:

User Name: admin

Password: admin

Go into Setup > Basic Setup:

Internet Connection Type: Static IP

Internet IP Address: 10.10.10.6

Subnet Mask: 255.255.255.252

Default Gateway: 10.10.10.5

DNS 1: 192.168.20.254

IP Address: 192.168.50.97

Subnet Mask: 255.255.255.224

Start IP Address: 98

Maximum number of Users: 29

Go into Service Laptop > Desktop > IP Configuration:

IPv4 Address: 192.168.50.100

Subnet Mask: 255.255.255.224

Go into Service Laptop > Desktop > Web Browser > 192.168.50.97:

User Name: admin

Password: admin

Go into Wireless > Basic Wireless Settings:

Network Name (SSID): Wi-FiDaisy

Standard Channel: 6 - 2.437GHz / 11 - 2.462GHz

Go into Wireless > Wireless Security:

Security Mode: WPA2 Enterprise

RADIUS Server: 192.168.20.254

Shared Secret: RadiusPa55

Bring 2 laptops into topology (Lap1 and Lap2). Add WPC300N module to them. Do these same steps to each laptop. Go into Desktop > PC Wireless > Profiles > New (Wi-FiDaisy) > Advanced Setup > Next > Next > Security: WPA2-Enterprise > Next:

Login Name: Wi-FiDaisy

Password: RadiusPa55

Next > Save > Connect to Network.

Connect Service Laptop to RDaisy:

```
(config)# interface gigabitEthernet 0/1
(config-if)# description Legatura cu Wi-FiDaisy
(config-if)# ip address 10.10.10.5 255.255.255.252
(config-if)# no sh
```

Connect RDaisy 2911 (GigabitEthernet0/1) to Wi-FiDaisy WRT300N (Internet) with a Copper Cross-Over cable.

SDonald - Server

Go into Services > HTTP and turn off HTTP.
Go into DNS:

    Name: sal.ro
    Address: 192.168.20.254

Go into AAA:

    Service: On
    Client Name: Wi-FiDaisy
    Client IP: 10.10.10.6
    Secret: RadiusPa55
    Username: Wi-FiDaisy
    Password: RadiusPa55

Go into NTP:

    Authentication: Enable
    Key: 1
    Password: NTPpa55

Go into EMAIL:

    Domain Name: sal.ro
    User: SDonald
    Password: 123456
    User: Daisy
    Password: 123456

Go into FTP:

    Username: Daisy
    Password: 123456
    Write, Read, List
    Username: SDonald
    Password: 123456
    Write, Read, List

Check services

HTTP/HTTPS/DNS, SSH, FTP, DHCP, SYSLOG, NTP, EMAIL, AAA

Access-control list

RDaisy:

```
(config)# ip access-list standard 77
(config-std-nacl)# permit 192.168.10.12
(config-std-nacl)# exit
(config)# line vty 0 15
(config-line)# access-class 77 in
(config-line)# exit
```

```
(config)# ip access-list extended ACL
(config-ext-nacl)# deny tcp host 192.168.10.13 host 192.168.20.254 eq www
(config-ext-nacl)# deny tcp host 192.168.10.13 host 192.168.20.254 eq 443
(config-ext-nacl)# deny tcp host 192.168.10.12 host 192.168.20.254 eq ftp
(config-ext-nacl)# deny icmp host 192.168.10.12 host 192.168.20.254
(config-ext-nacl)# permit ip any any
(config-ext-nacl)# exit
(config)# interface gigabitEthernet 0/0
(config-if)# ip access-group ACL in
```

RDonald:

```
(config)# access-list 20 remark ACL_PING
(config)# access-list 20 permit host 192.168.10.12
(config)# interface gigabitEthernet 0/0
(config-if)# ip access-group 20 out
```

RDuck:

```
(config)# ip access-list extended ACL_MAIL
(config-ext-nacl)# permit tcp host 192.168.30.12 host 192.168.20.254 eq 25
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface gigabitEthernet 0/0
(config-if)# ip access-group ACL_MAIL in
```

Security

RDuck:

```
(config)# license boot module c2900 technology-package securityk9
yes
(config)# exit
# reload
yes
enter
# conf t
(config)# zone security INSIDE
(config-sec-zone)# exit
(config)# zone security CONFROOM
(config-sec-zone)# exit
(config)# zone security INTERNET
(config-sec-zone)# exit
(config)# class-map type inspect match-any INSIDE_PROTOCOLS
(config-cmap)# match protocol tcp
(config-cmap)# match protocol udp
(config-cmap)# match protocol icmp
(config-cmap)# exit
(config)# class-map type inspect match-any CONFROOM_PROTOCOLS
```

```
(config-cmap)# match protocol http
(config-cmap)# match protocol https
(config-cmap)# match protocol dns
(config-cmap)# exit
(config)# policy-map type inspect INSIDE_TO_INTERNET
(config-pmap)# class type inspect INSIDE_PROTOCOLS
(config-pmap-c)# inspect
(config-pmap-c)# exit
(config-pmap)# exit
(config)# policy-map type inspect CONFROOM_TO_INTERNET
(config-pmap)# class type inspect CONFROOM_PROTOCOLS
(config-pmap-c)# inspect
(config-pmap-c)# exit
(config-pmap)# exit
(config)# zone-pair security INSIDE_TO_INTERNET source INSIDE destination
    INTERNET
(config-sec-zone-pair)# service-policy type inspect INSIDE_TO_INTERNET
(config-sec-zone-pair)# exit
(config)# zone-pair security CONFROOM_TO_INTERNET source CONFROOM destination
    INTERNET
(config-sec-zone-pair)# service-policy type inspect CONFROOM_TO_INTERNET
(config-sec-zone-pair)# exit
(config)# exit
# show zone-pair security
# show policy-map type inspect zone-pair sessions
# conf t
(config)# interface gigabitEthernet 0/0
(config-if)# zone-member security INSIDE
(config-if)# exit
(config)# interface gigabitEthernet 0/1
(config-if)# zone-member security CONFROOM
(config-if)# exit
(config)# interface serial 0/0/0
(config-if)# zone-member security INTERNET
(config-if)# exit
```

IPS

RDonald:

```
(config)# license boot module c2900 technology-package securityk9
yes
(config)# exit
# reload
yes
enter
# mkdir ipsdir
```

```
enter
# conf t
(config)# ip ips config location flash:ipsdir
(config)# ip ips name iosips
(config)# ip ips notify log
(config)# ip ips signature-category
(config-ips-category)# category all
(config-ips-category-action)# retired true
(config-ips-category-action)# exit
(config-ips-category)# category ios_ips basic
(config-ips-category-action)# retired false
(config-ips-category-action)# exit
(config-ips-category)# exit
enter
(config)# interface gigabitEthernet 0/0
(config-if)# ip ips iosips out
(config-if)# ip ips signature-definition
(config-sigdef)# signature 2004 0
(config-sigdef-sig)# status
(config-sigdef-sig-status)# retired false
(config-sigdef-sig-status)# enabled true
(config-sigdef-sig-status)# exit
(config-sigdef-sig)# engine
(config-sigdef-sig-engine)# event-action produce-alert
(config-sigdef-sig-engine)# event-action deny-packet-inline
(config-sigdef-sig-engine)# exit
(config-sigdef-sig)# exit
(config-sigdef)# exit
enter
(config)# exit
# sh ip ips all
```