

## CCNA 2: SRWE Practice PT Skills Assessment (PTSA) – Part 2 Answers

---

 [itexamanswers.net/ccna-2-srwe-practice-pt-skills-assessment-ptsa-part-2-answers.html](http://itexamanswers.net/ccna-2-srwe-practice-pt-skills-assessment-ptsa-part-2-answers.html)

December 21, 2019

### CCNA 2 v7 – SRWE Practice PT Skills Assessment (PTSA) – Part 2 Answers

---

[Updated on Sep 2021 – 100% Scored]

---

CCNAv7: Switching, Routing, and Wireless Essentials v7.0 (SRWE)

---

- [ID 1](#)
- [ID 0](#)
- [ID 2](#)



SRWE Practice PT Skills Assessment (PTSA) - Part 2 ID 1

## Final Packet Tracer Skills Assessment - Part 2

---

### Addressing Table

---

<b>Device</b>	<b>Interface</b>	<b>Address and Prefix</b>
Central	G0/0/0	192.168.1.1/24
		2001:db8:acad:1::1/64
		fe80::1
	G0/0/1	192.168.2.1/24
		2001:db8:acad:2::1/64
		fe80::1
	G0/0/2	10.1.0.1/30
		2001:db8:acad:a::1/64
		fe80::2
	S0/1/0	10.2.0.1/30
		2001:db8:acad:b::1/64
		fe80::2
	S0/1/1	10.4.0.1/30
		2001:db8:acad:d::1/64
Office-1	S0/1/1	10.4.0.2/30
		2001:db8:acad:d::2/64
		fe80::2
	G0/0/0	192.168.3.1/24
		2001:db8:acad:3::1/64
		fe80::1
Branch-101	G0/0/0.10	192.168.10.1/24
	G0/0/0.100	192.168.100.1/24
	G0/0/0.172	172.16.1.1/24
	G0/0/1	DHCP
		2001:db8:acad:c::2/64
	S0/1/0	10.2.0.2/30
		2001:db8:acad:b::2/64
ISP Router	G0/0/0	10.1.0.2/24
		2001:DB8:ACAD:A::2/64
	G0/0/1	10.3.0.1/24
		2001:DB8:ACAD:C::1/64
WLC-10	management	192.168.100.254
	WLAN 10	192.168.10.254/24
Server-O1	NIC	192.168.3.122
		2001:db8:acad:3::122

Internet Server	NIC	203.0.113.25 2001:db8:acad:cafe:25
DNS Server	NIC	198.51.100.163 2001:DB8:face::163
Management Host	NIC	192.168.100.23
Wireless Host	NIC	DHCP
RADIUS server	NIC	172.16.1.100/24
PC-A	NIC	192.168.1.10/24 2001:db8:acad:1::10/64
PC-B	NIC	192.168.1.11/24 2001:db8:acad:1::11/64
PC-C	NIC	192.168.2.20/24 2001:db8:acad:2::20/64
PC-D	NIC	192.168.2.11/24 2001:db8:acad:2::21/64
PC-E	NIC	192.168.3.30/24 2001:db8:acad:3::30/64

## Objectives

---

In this assessment, you will configure the following:

- Floating static and default routes in IPv4 and IPv6.
- Host routes in IPv4 and IPv6.
- DHCP pools and scopes.
- Switch security including port security.
- Enhanced LAN security with DHCP snooping, dynamic ARP inspection, PortFast, and BPDU guard.
- Wireless LAN Controller-based wireless LAN with enterprise authentication.

**You will only configure the Central and Branch-101 routers, the S1-1 switch, and the WLC-10 wireless LAN controller. Access to other devices is not available.**

## Background / Scenario

---

Netacad PLC is reworking their network. You have been asked to prototype the network in Packet Tracer for evaluation by senior network staff.

## Instructions

---

### Part 1: Configure Switch Security

---

In this part of the assessment you will configure switch **S1-1** with switch security features. Switch ports FastEtherneto/1 to FastEtherneto/5 are the active switch ports. Port GigabitEtherneto/1 is a dedicated link to router Central. All other ports should be secured.

#### Step 1: Configure VLANs

---

- a. Configure VLAN 10 with name **users**.
- b. Configure VLAN 999 with the name **unused**.

#### S1-1 Switch

```
S1-1(config)#vlan 10
S1-1(config-vlan)#name users
S1-1(config-vlan)#vlan 999
S1-1(config-vlan)#name unused
```

## Step 2: Configure active switch ports.

---

On the active switch ports configure the following:

- Configure FastEthernet 0/1 through 0/5 and GigabitEthernet 0/1 as static access ports in VLAN 10.

```
S1-1(config)#interface range f0/1-5, g0/1
S1-1(config-if-range)#switchport mode access
S1-1(config-if-range)#switchport access vlan 10
```

- Activate port security on the ports.

- Configure the active ports to accept a maximum of **4** MAC addresses.
- If a violation occurs, configure the ports to drop frames from the unauthorized MAC address, log it, and send an alert.
- MAC addresses should be present in the MAC address table for a maximum of 10 minutes before they are removed.
- Ports should add the learned MAC addresses to the running configuration.
- Configure the MAC address of PC-A as a static address on port FastEthernet0/1.

```
S1-1(config)#interface range f0/1-5
S1-1(config-if-range)#switchport port-security
S1-1(config-if-range)#switchport port-security maximum 4
S1-1(config-if-range)#switchport port-security violation restrict
S1-1(config-if-range)#switchport port-security aging time 10
S1-1(config-if-range)#switchport port-security mac-address sticky
S1-1(config-if-range)#exit

S1-1(config)#interface f0/1
S1-1(config-if)#switchport port-security mac-address 00D0.D3DC.2825
S1-1(config-if)#exit
```

- Protect against DHCP snooping.

**Note:** In this simulated network, DHCP snooping may not operate correctly in Packet Tracer. Configure it as you would normally. You will receive full credit for a configuration that meets the requirements below.

- Activate DHCP snooping globally.
- Activate DHCP snooping for the two VLANs that you configured.
- Configure the ports to limit the rate to 5 DHCP packets per second.
- Configure the port that links to the router as trusted.

```
S1-1(config)#ip dhcp snooping
S1-1(config)#ip dhcp snooping vlan 10,999
S1-1(config)#interface range f0/1-5, g0/1
S1-1(config-if-range)#ip dhcp snooping limit rate 5
S1-1(config-if-range)#exit
S1-1(config)#interface g0/1
S1-1(config-if)#ip dhcp snooping trust
S1-1(config-if)#exit
```

- Guard against ARP attacks by implementing DAI.

- Activate DAI globally.
- Activate DAI on the two VLANs.
- Configure the port that links to the router as trusted.

```
S1-1(config)#ip arp inspection vlan 10,999
S1-1(config)#interface g0/1
S1-1(config-if)#ip arp inspection trust
S1-1(config-if)#exit
```

- Mitigate STP attacks by configuring BPDUguard and PortFast on the active ports.

```
S1-1(config)#interface range f0/1-5
S1-1(config-if-range)#spanning-tree portfast
S1-1(config-if-range)#spanning-tree bpduguard enable
```

## Step 3: Secure unused switch ports.

---

- Move all unused switch ports to VLAN 999.

b. Configure all unused switch ports as static access ports.

c. Deactivate all unused switch ports.

```
S1-1(config)#interface range f0/6-24, g0/2
S1-1(config-if-range)#switchport mode access
S1-1(config-if-range)#switchport access vlan 999
S1-1(config-if-range)#shutdown
```

## Part 2: Configure Addressing and DHCP

You will configure DHCP and interface addressing on router **Branch-101** to prepare for implementing the wireless LAN controller network.

### Step 1: Configure and address a subinterface for the WLAN user network.

a. Configure subinterface 10 on the router interface that is connected to the switch S4-1.

b. The router should provide router-on-a-stick routing to VLAN 10.

c. Configure the subinterface with the address from the Addressing Table.

#### Brand-101 Router

```
Branch-101(config)#interface g0/0/0.10
Branch-101(config-subif)#description WLAN users
Branch-101(config-subif)#encapsulation dot1q 10
Branch-101(config-subif)#ip address 192.168.10.1 255.255.255.0
```

### Step 2: Configure a DHCP pool for WLAN user network.

a. Exclude the router interface address and the management address of the WLC.

```
Branch-101(config)#ip dhcp excluded-address 192.168.10.1
Branch-101(config)#ip dhcp excluded-address 192.168.10.254
```

b. Configure a DHCP pool that will be used by hosts that are connecting to the WLAN.

1. Name the pool WLAN-hosts.
2. Configure the pool to use addresses in the 192.168.10.0/24 network.
3. The pool should also provide the default gateway and DNS server addresses.

```
Branch-101(config)#ip dhcp pool WLAN-hosts
Branch-101(dhcp-config)#network 192.168.10.0 255.255.255.0
Branch-101(dhcp-config)#default-router 192.168.10.1
Branch-101(dhcp-config)#dns-server 198.51.100.163
```

### Step 3: Configure an interface as a DHCP client.

On Branch-101, configure the interface that is connected to ISP Router to receive its address over DHCP.

```
Branch-101(config)#interface g0/0/1
Branch-101(config-if)#ip address dhcp
Branch-101(config-if)#exit
```

## Part 3: Configure Static Routes

In this part of the assessment you will configure static, default, floating static, and host routes in both IPv4 and IPv6. You will configure the Central and Branch-101 routers. Netacad PLC has decided that it wants to use static routing between all its networks. In addition, the company wants to use the Ethernet links between routers for most data traffic and reserve serial link between Central and Branch-101 for backup purposes in case one of the Ethernet links becomes unavailable. You will be configuring floating static and default routes.

### Step 1: Configure static routes on Central.

a. Configure IPv4 default routes to the cloud using the Ethernet link as the preferred link and the serial link as the floating backup. Use an administrative distance of **10** for the backup route. These routes should be configured as directly connected routes.

**Note:** Ethernet interfaces will give a warning when configured without a next-hop address. In this configuration, the interface is point-to-point, so the warning can be ignored.

```
Central(config)#ip route 0.0.0.0 0.0.0.0 g0/0/2
Central(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0 10
```

b. Configure IPv4 static routes to the Remote Branch LAN WLAN user network following the same guidelines as above for type of route and administrative distance.

```
Central(config)#ip route 192.168.10.0 255.255.255.0 g0/0/2  
Central(config)#ip route 192.168.10.0 255.255.255.0 s0/1/0 10
```

c. Configure an IPv4 host route on Central to the Server-O1 on the Remote Office LAN. Create a directly connected route.

```
Central(config)#ip route 192.168.3.122 255.255.255.255 s0/1/1
```

**Note:** For the purpose of this assessment, please enter the IPv4 static routes in the following order:

- 1) IPv4 default route
- 2) IPv4 floating default route
- 3) IPv4 host route
- 4) IPv4 static route to Remote Branch LAN
- 5) IPv4 floating static route to Remote Branch LAN

d. Ensure that the device is configured to route IPv6.

e. Configure IPv6 default routes to the cloud. Use the Ethernet link as the primary route, and the serial link as the floating backup. Use an administrative distance of **10** for the backup route. These routes should specify the next hop interface address.

```
Central(config)#ipv6 unicast-routing  
Central(config)#ipv6 route ::/0 2001:DB8:ACAD:A::2  
Central(config)#ipv6 route ::/0 2001:db8:acad:b::2 10
```

f. Configure an IPv6 host route on Central to the Server-O1 on the Remote Office LAN It should be a next-hop route.

```
Central(config)#ipv6 route 2001:db8:acad:3::122/128 2001:db8:acad:d::2
```

**Note:** For the purpose of this assessment, please enter the IPv6 static routes in the following order:

- 1) IPv6 default route
- 2) IPv6 floating default route
- 3) IPv6 host route

## Step 2: Configure static routes on Branch-101.

---

Branch-101 must also be configured with static routes to the other three networks in the Netacad PLC network. It will require floating static and default routes in IPv4 and IPv6 following the same guidelines as were used for the Central static routes.

- IPv6 routes use next-hop address arguments.
- IPv4 routes use exit interface arguments.
- All routes should prefer the Ethernet links over the serial link.
- Backup floating routes use an administrative distance of **10**.

a. Configure IPv4 default routes to the cloud using the Ethernet link as the preferred link and the serial link as the backup.

**Note:** For the purpose of this assessment, please enter the IPv4 static routes in the following order:

- 1) IPv4 default route
- 2) IPv4 floating default route

```
Branch-101(config)#ip route 0.0.0.0 0.0.0.0 g0/0/1  
Branch-101(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0 10
```

b. Ensure that the device is configured to route IPv6.

c. Configure IPv6 default routes to the cloud. Use the Ethernet link as the primary route, and the serial link as backup. Use an administrative distance of **10** for the backup route. These routes should specify the next hop interface address.

```
Branch-101(config)#ipv6 unicast-routing  
Branch-101(config)#ipv6 route ::/0 2001:DB8:ACAD:C::1  
Branch-101(config)#ipv6 route ::/0 2001:DB8:ACAD:B::1 10
```

**Note:** For the purpose of this assessment, please enter the IPv6 static routes in the following order:

- 1) IPv6 default route
- 2) IPv6 floating default route

## Part 4: Configure a Wireless LAN using a Wireless LAN Controller

---

In this part of the assessment, you will configure the wireless LAN controller to provide access wireless access to the network. Username and password are the default **admin/admin**. Connect to the WLC over HTTPS to the management interface.

Open the browser from the desktop of **W-Admin Host (or Management Host/Admin)**. Connect to the IP address of the WLC over HTTPS: <https://192.168.100.254>

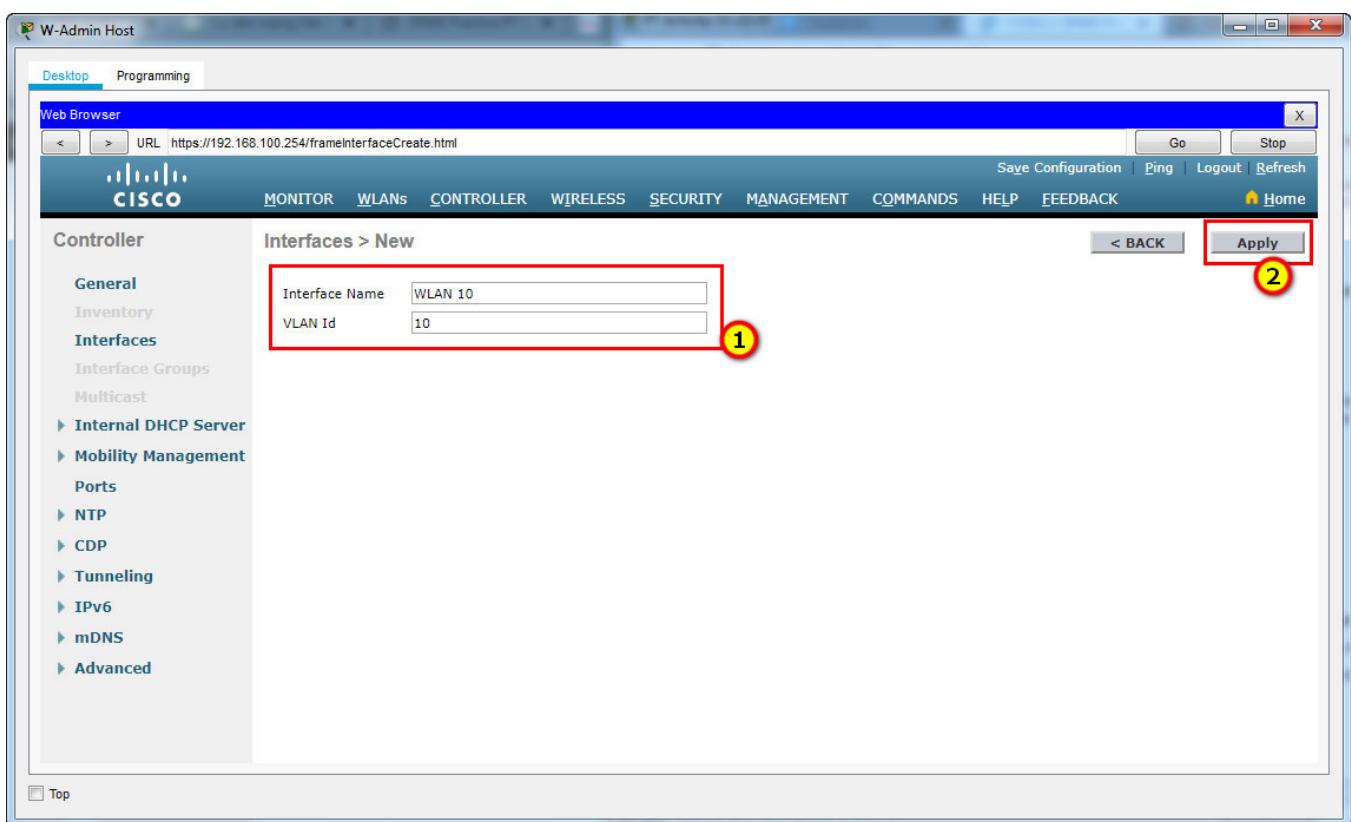
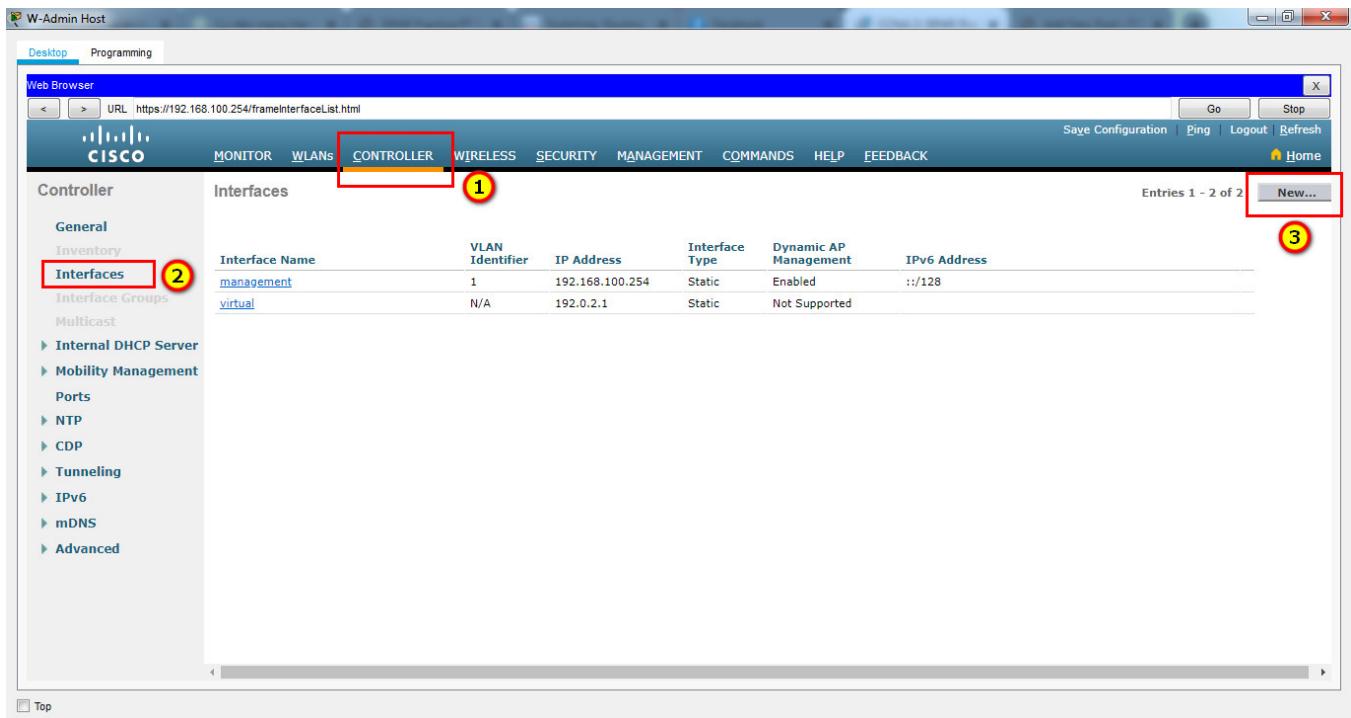


Login with the username **admin** and password **admin**

---

**Step 1: Configure a VLAN interface.**

- a. Create a new interface and name it **WLAN 10**. The interface should use VLAN **10** and physical port **1**.



b. Use the information in the addressing table to configure the addressing settings for the interface. The interface will be using a DHCP pool that is configured on the subinterface that is assigned to **VLAN 10** on router **Branch-101 (or RTR-Branch/R-B-10)**.

The screenshot shows the Cisco W-Admin Host web interface. The left sidebar under 'Controller' has 'Interfaces' selected, indicated by a red circle with the number '1'. The main content area displays a table of interfaces. The first row, 'WLAN 10', is highlighted with a red circle and a red arrow pointing to it, indicating the target for configuration. The table columns are: Interface Name, VLAN Identifier, IP Address, Interface Type, Dynamic AP Management, and IPv6 Address.

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
WLAN 10	10	0.0.0.0	Dynamic	Disabled	
management	1	192.168.100.254	Static	Enabled	::/128
virtual	N/A	192.0.2.1	Static	Not Supported	

Port Number: 1

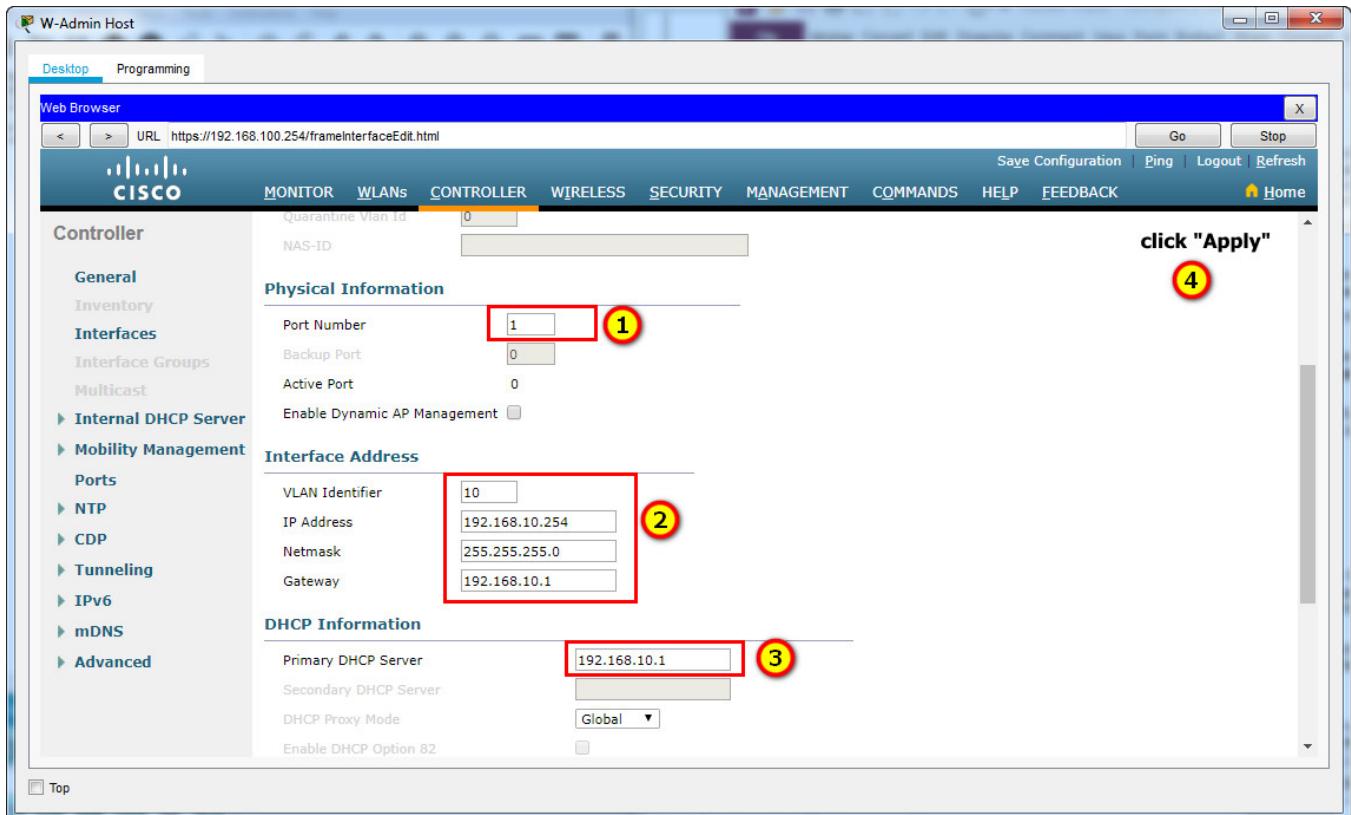
VLAN Identifier: 10

IP Address: 192.168.10.254

Netmask: 255.255.255.0

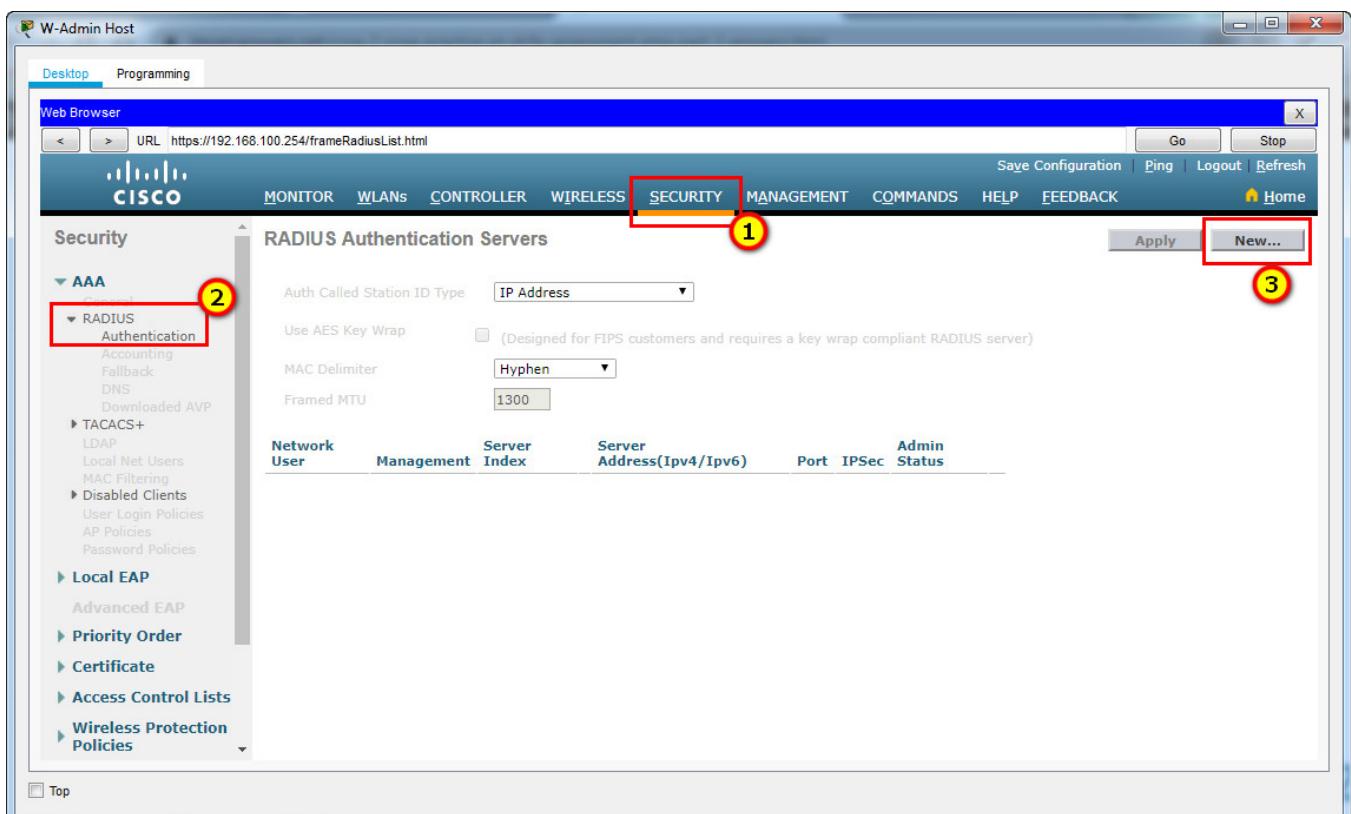
Gateway: 192.168.10.1

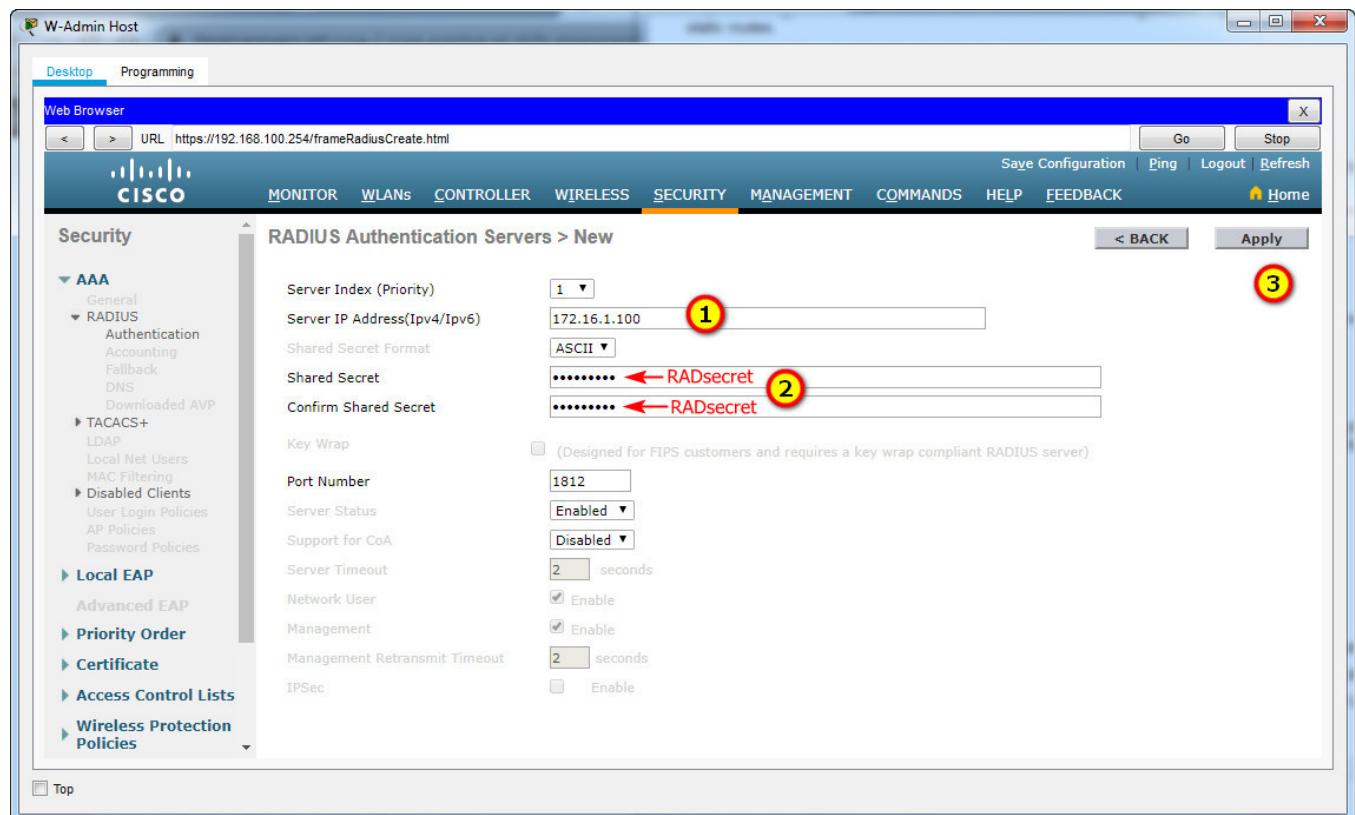
Primary DHCP Server: 192.168.10.1



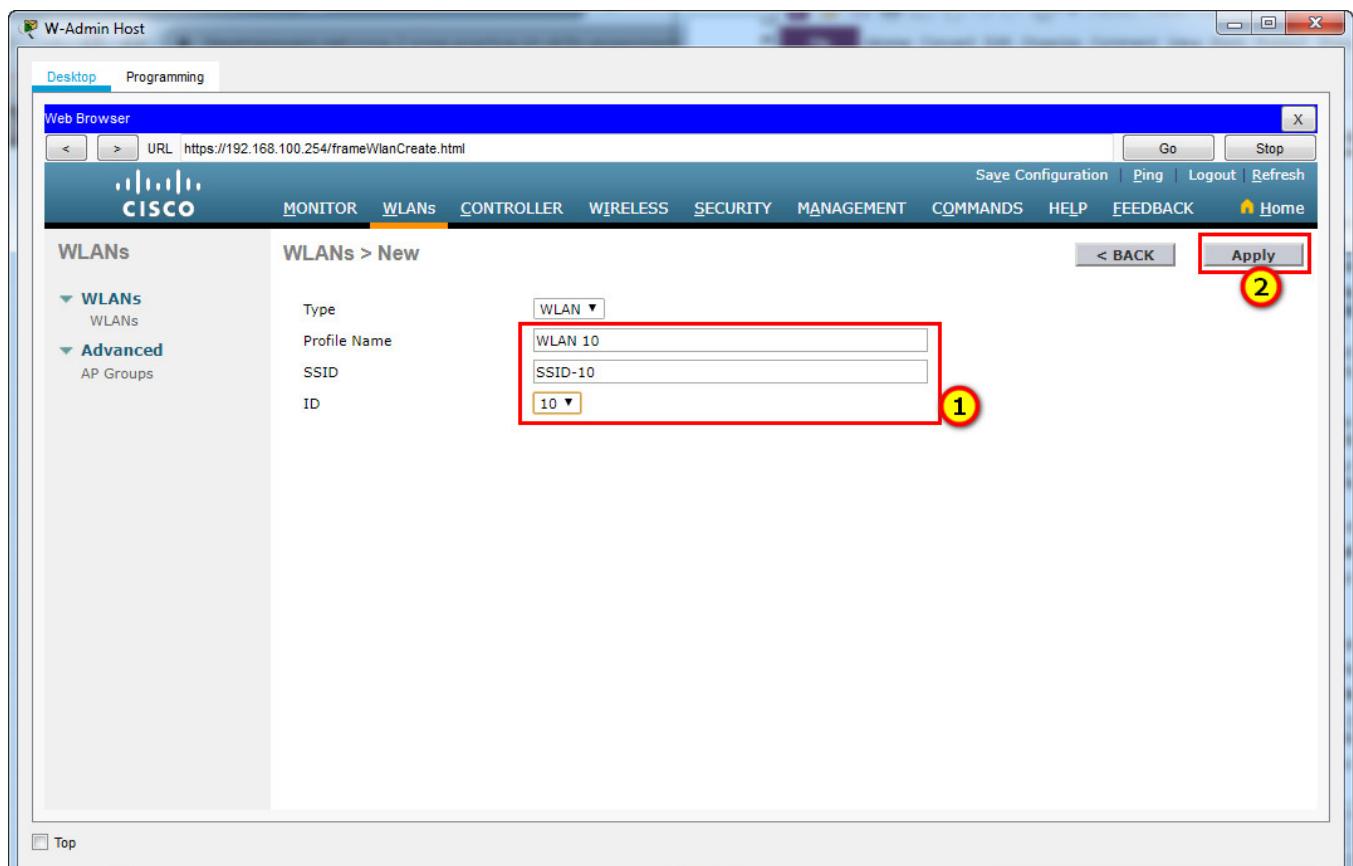
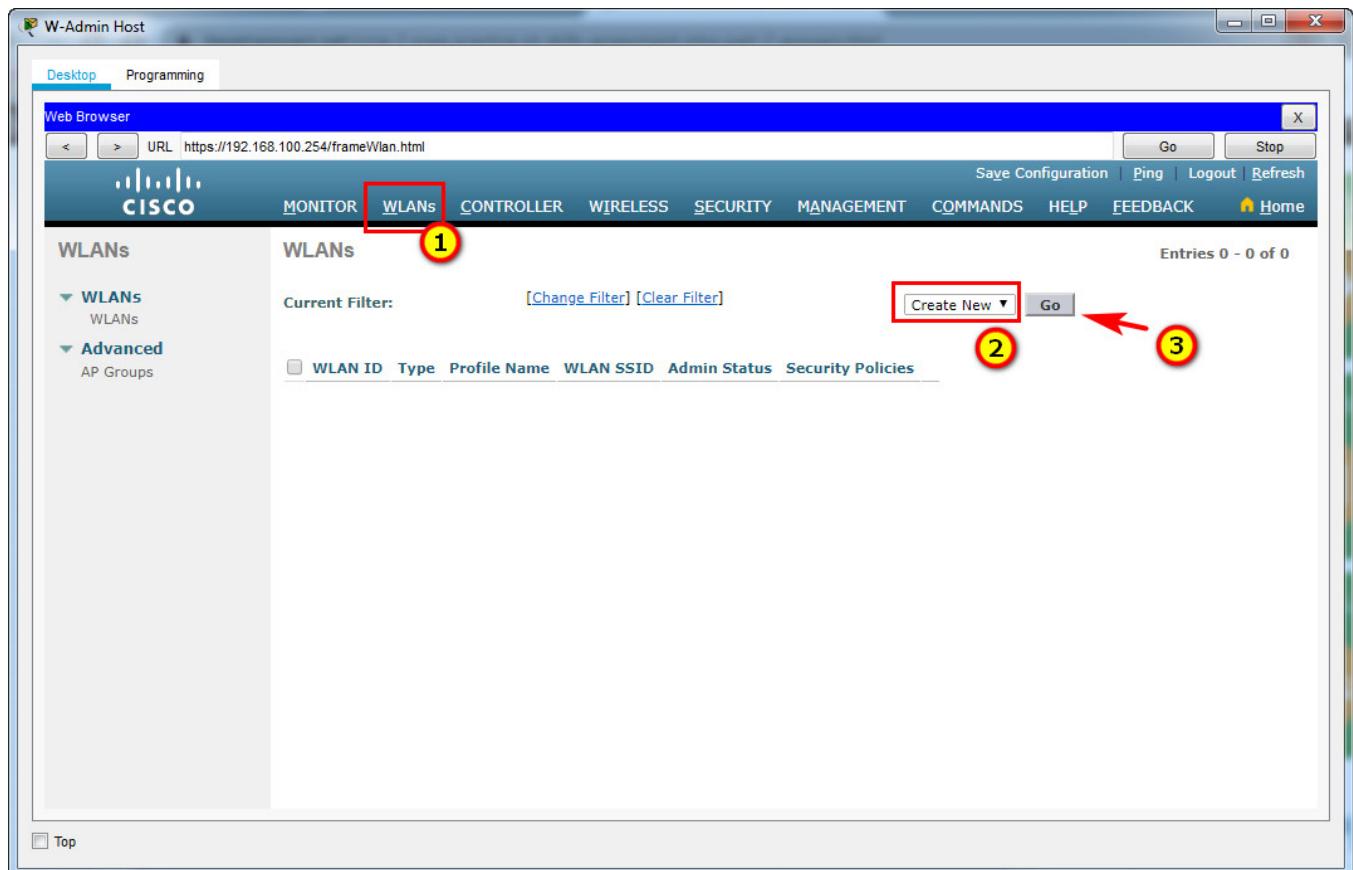
## Step 2: Configure a RADIUS server.

- Configure the WLC with the RADIUS server IPv4 address.
- Use a shared secret of **RADsecret**.

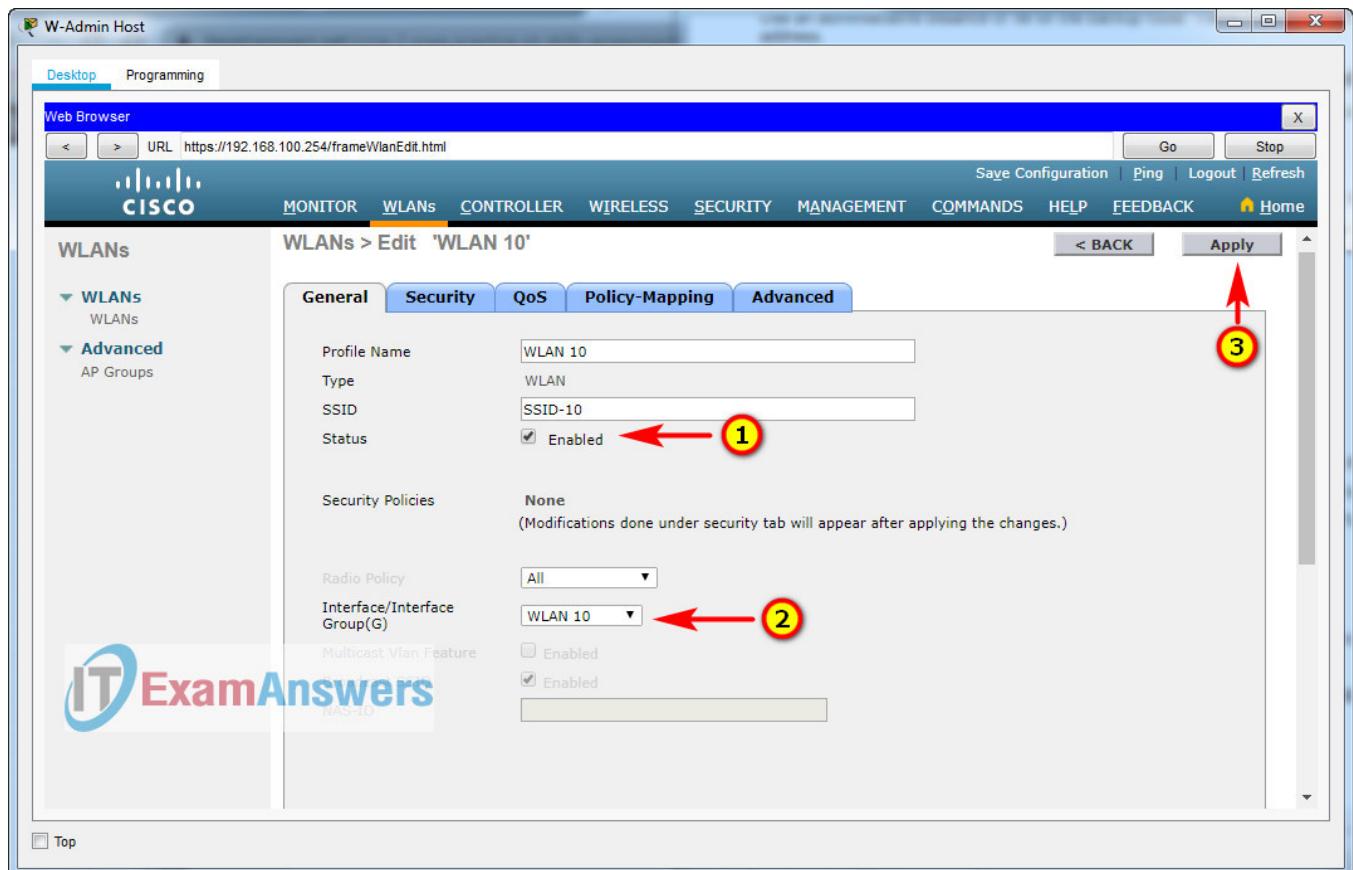


**RADIUS Server:**Server IP Address: **172.16.1.100**Shared Secret: **RADsecret****Step 3: Configure a Wireless LAN.**

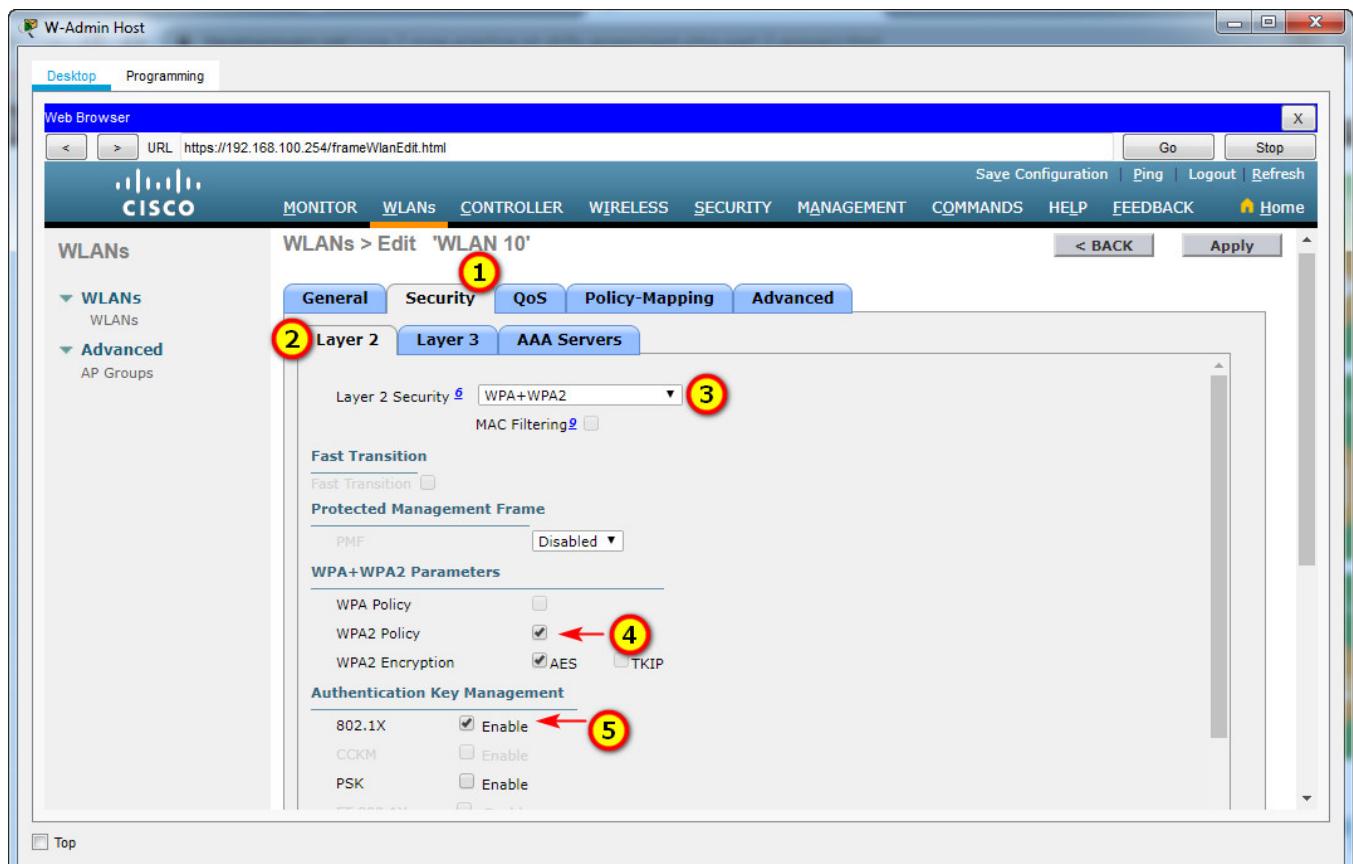
- Create a new WLAN. Name it **WLAN 10** and configure the SSID as **SSID-10**.



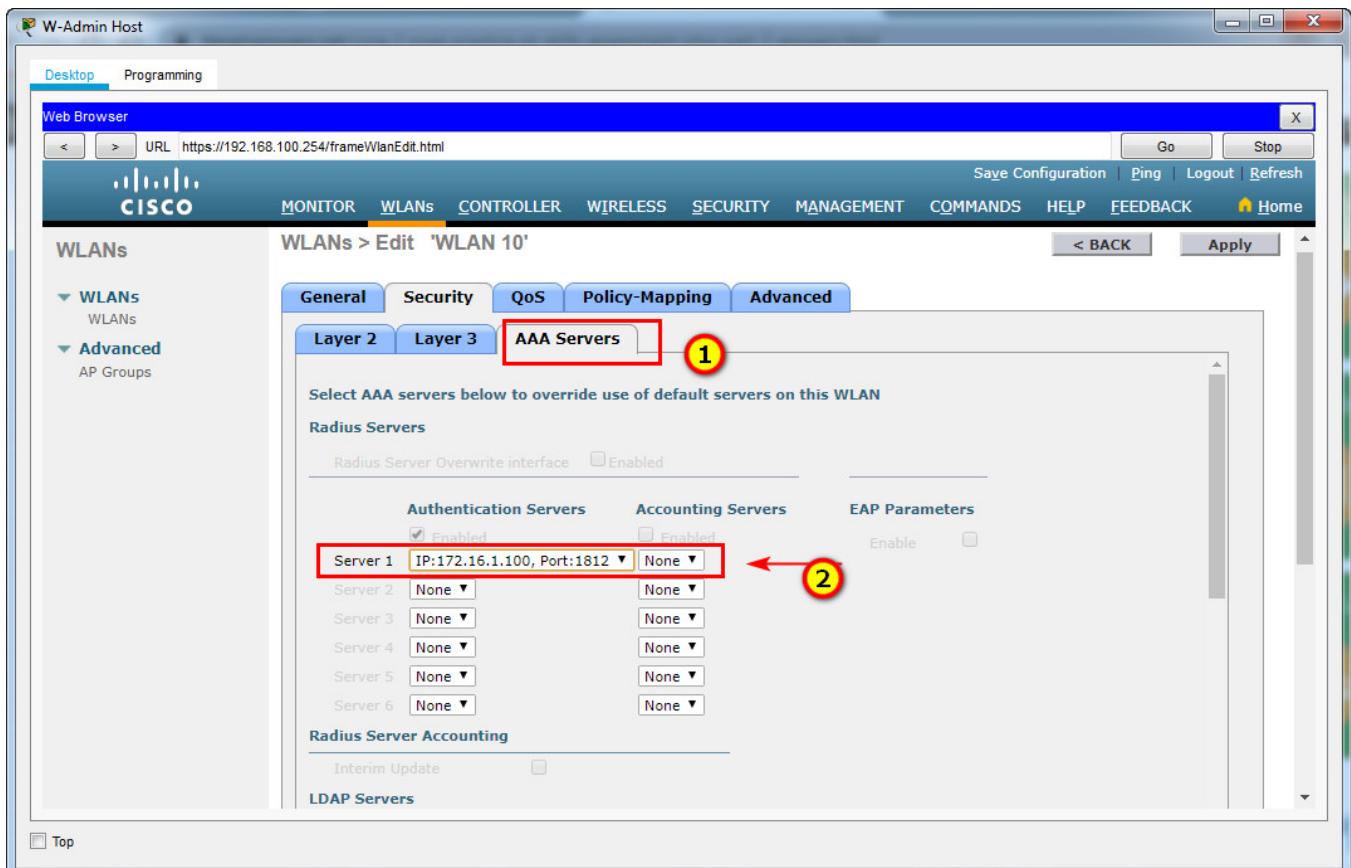
b. The wireless LAN should use the VLAN interface that was previously configured.



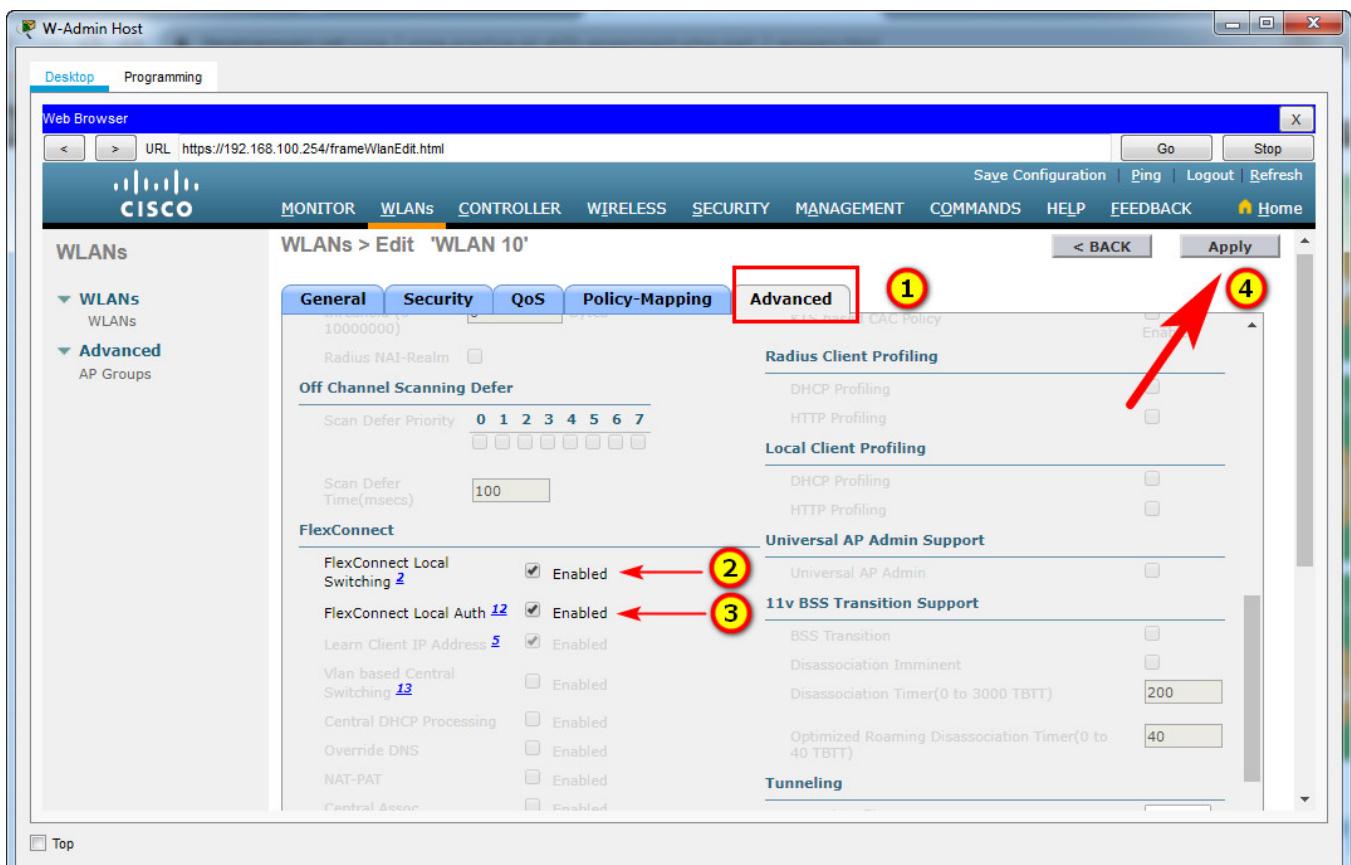
c. Configure the WLAN to use the WPA2 security policy and dot1x Authentication Key Management.



d. Configure the WLAN to use the RADIUS server that was previously configured to authenticate wireless users.



- e. Open the Advanced tab and scroll down to the Flexconnect sections. Activate **FlexConnect Local Switching** and **FlexConnect Local Auth**.



f. Verify that the WLAN is configured and operational.

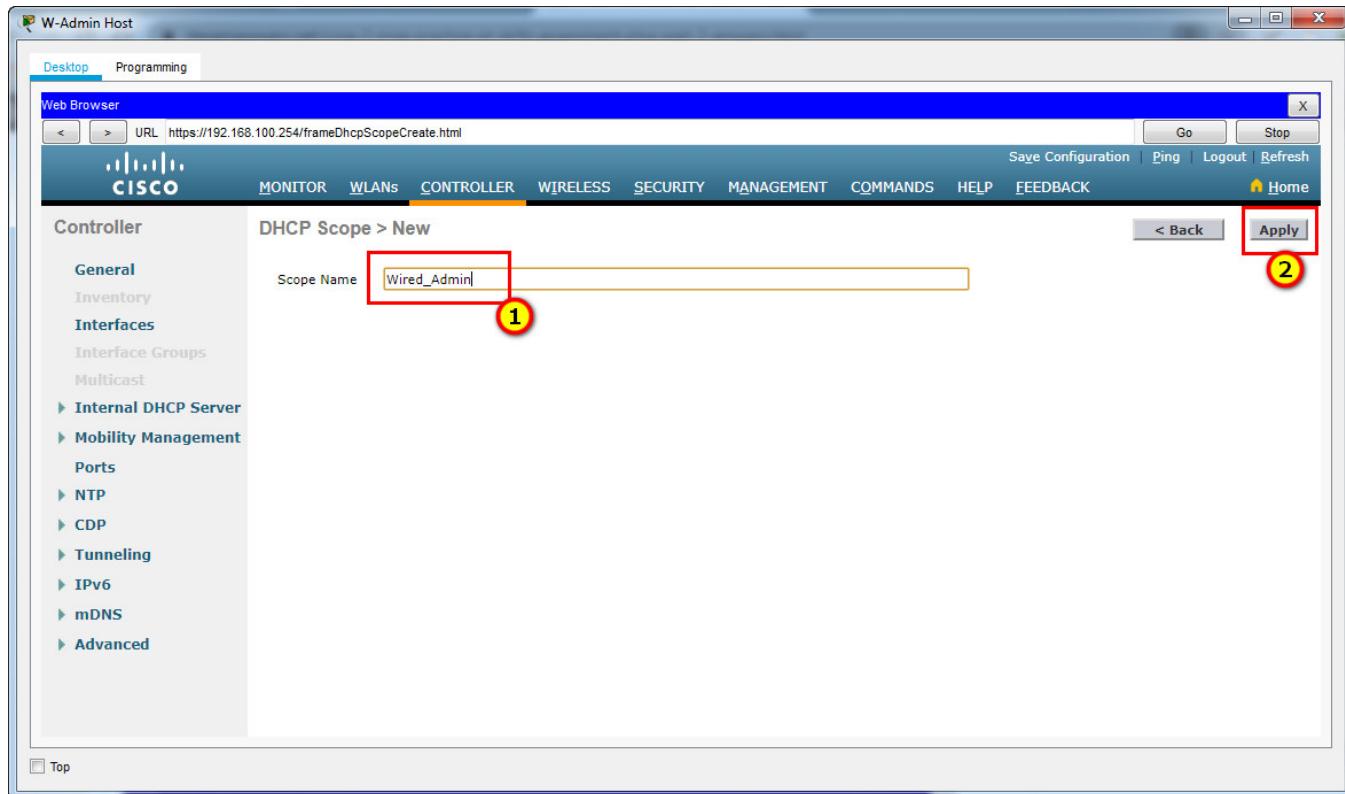
The screenshot shows the W-Admin Host web-based management interface for a Cisco device. The URL in the browser is <https://192.168.100.254/frameWlan.html>. The main menu at the top includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The WLANs tab is selected, showing a table of configured WLANs. The table has columns for WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. One entry is visible: WLAN ID 10, Type WLAN, Profile Name WLAN 10, WLAN SSID SSID-10, Admin Status Enabled, and Security Policies [WPA2][Auth(802.1X)]. A red arrow points from the left towards this row. The left sidebar shows navigation options like WLANS and Advanced.

#### Step 4: Configure a DHCP scope for the management network.

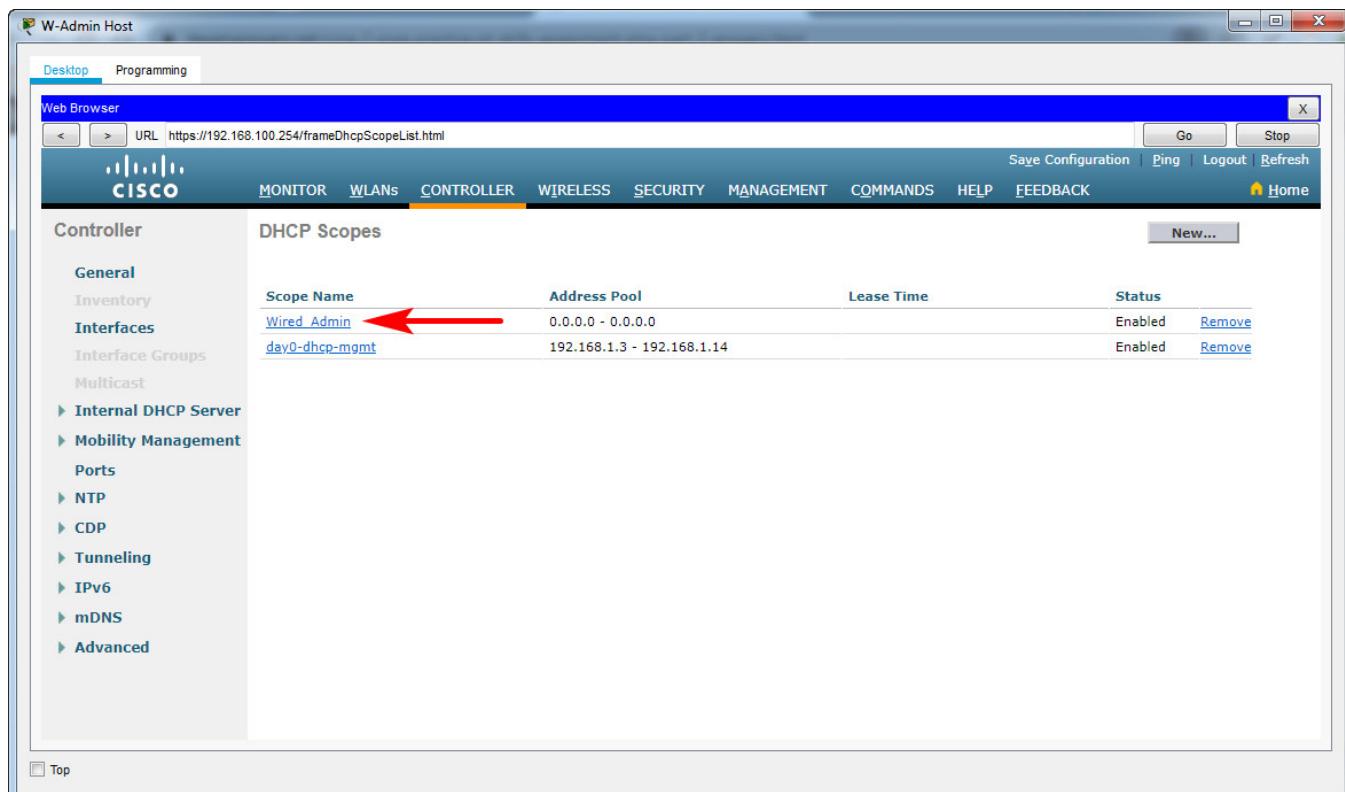
Configure a new DHCP scope to be used by the LAPs and other management devices on the network.

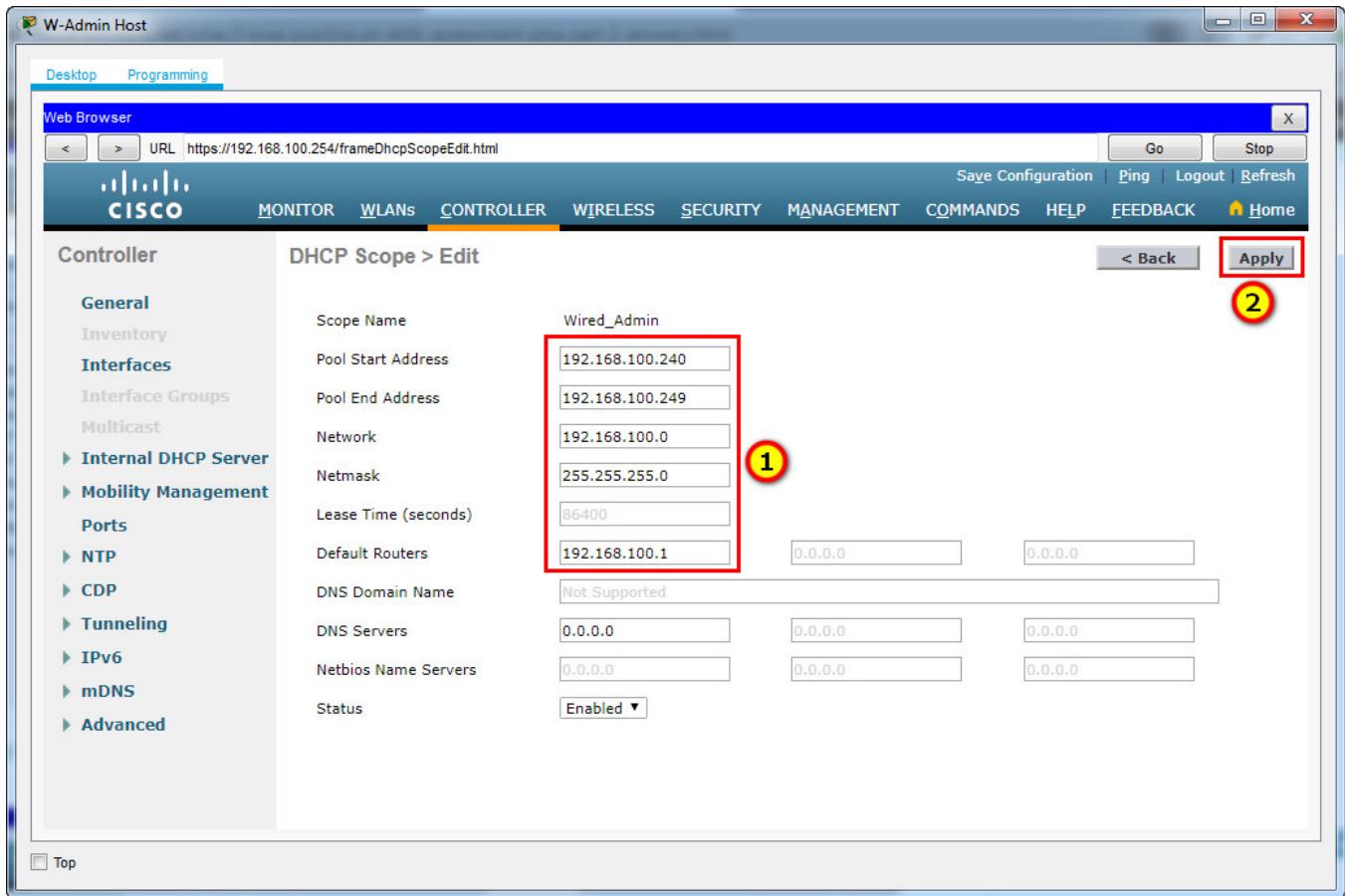
- Name the DHCP scope **Wired\_Admin**.

The screenshot shows the W-Admin Host interface again, this time under the CONTROLLER tab. The URL is <https://192.168.100.254/frameDhcpScopeList.html>. The CONTROLLER tab is highlighted with a red box and a yellow circle labeled '1'. On the left sidebar, the Internal DHCP Server section is expanded, with a yellow circle labeled '2' next to it. In the main pane, the 'DHCP Scopes' section is shown with one entry: Scope Name dav0-dhcp-mgmt, Address Pool 192.168.1.3 - 192.168.1.14, Lease Time, and Status Enabled. A red box surrounds the 'New...' button, which has a yellow circle labeled '3' over it. The rest of the interface is similar to the previous WLAN configuration screen.



b. Start the scope at address **192.168.100.240**. End the scope at address **192.168.100.249**.





Pool Start Address: 192.168.100.240

Pool End Address: 192.168.100.249

Network: 192.168.100.0

Netmask: 255.255.255.0

Default Routers: 192.168.100.1

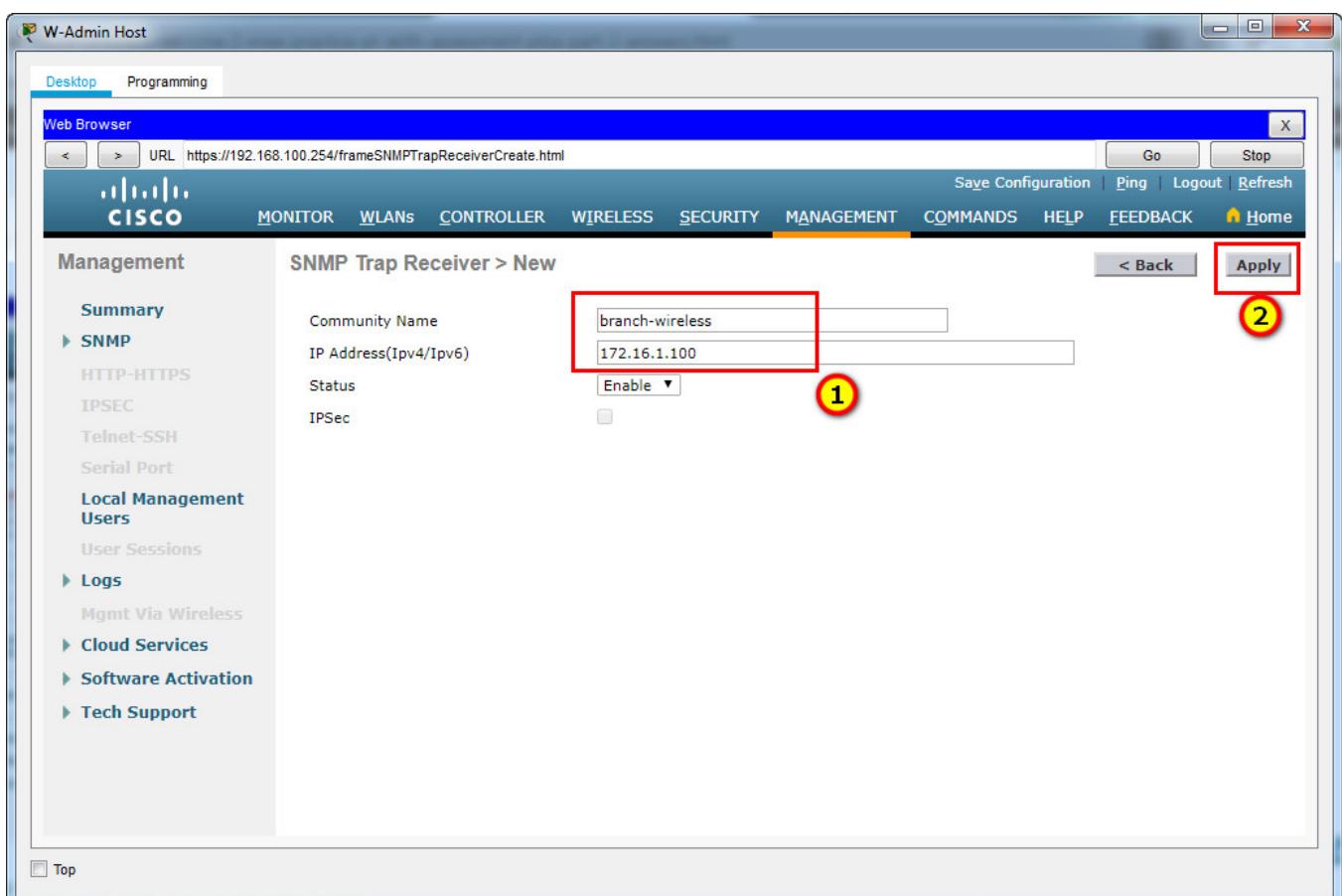
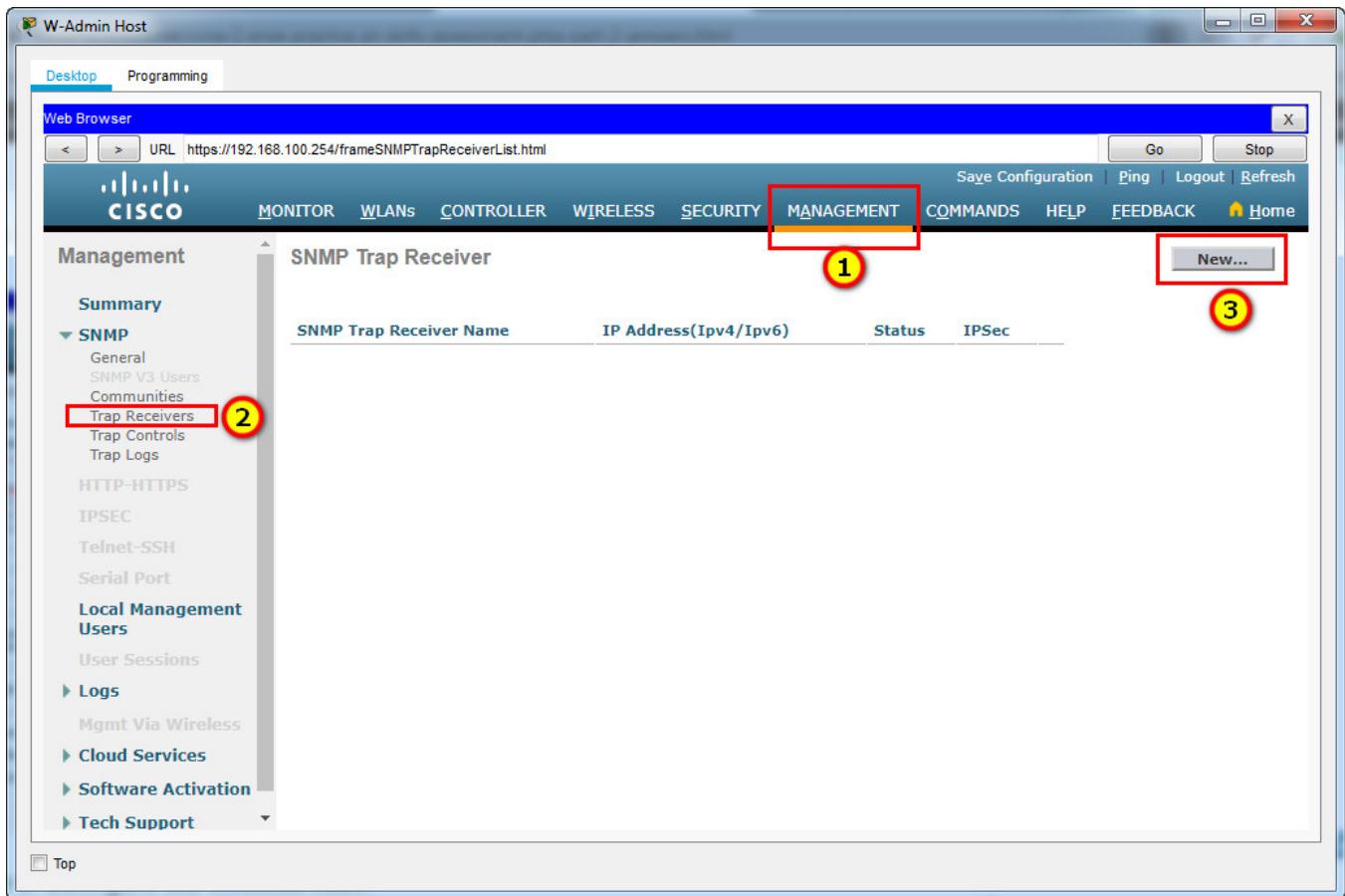
c. Other information that is required can be found in the Addressing Table.

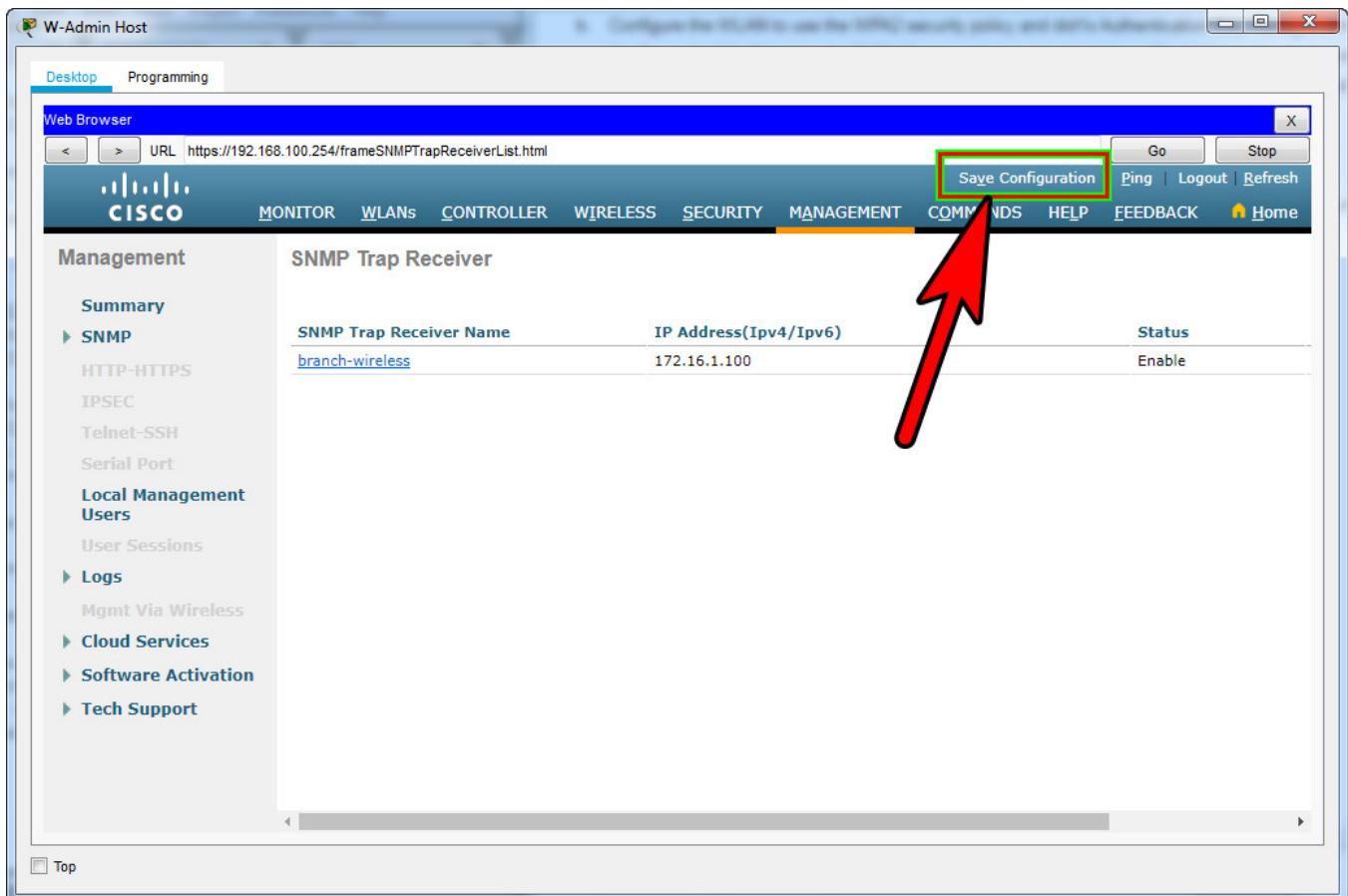
#### Step 5: Configure an SNMP server.

Configure an SNMP server to receive traps from the WLC.

a. Use the community name **branch-wireless**.

b. Use **172.16.1.100** as the server address.



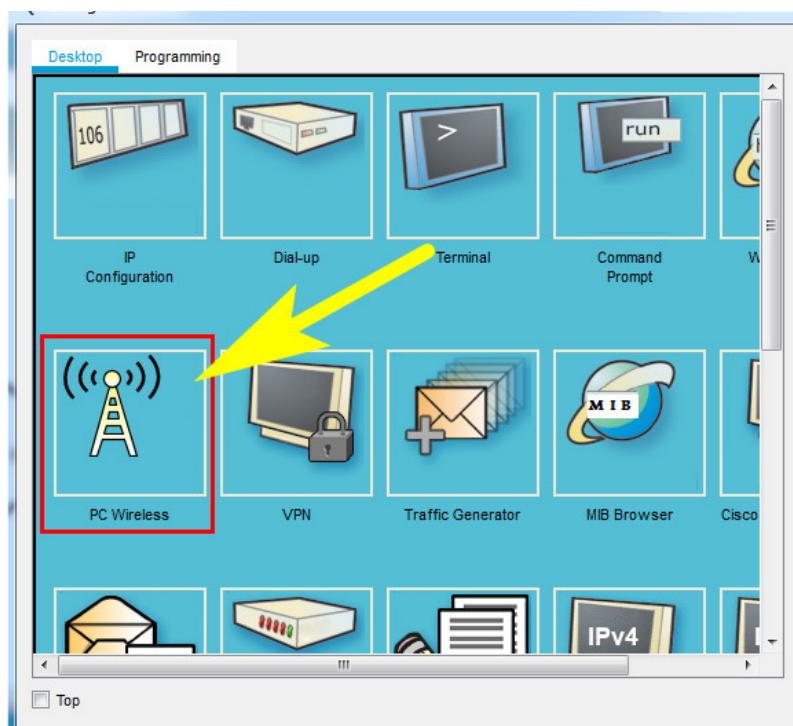


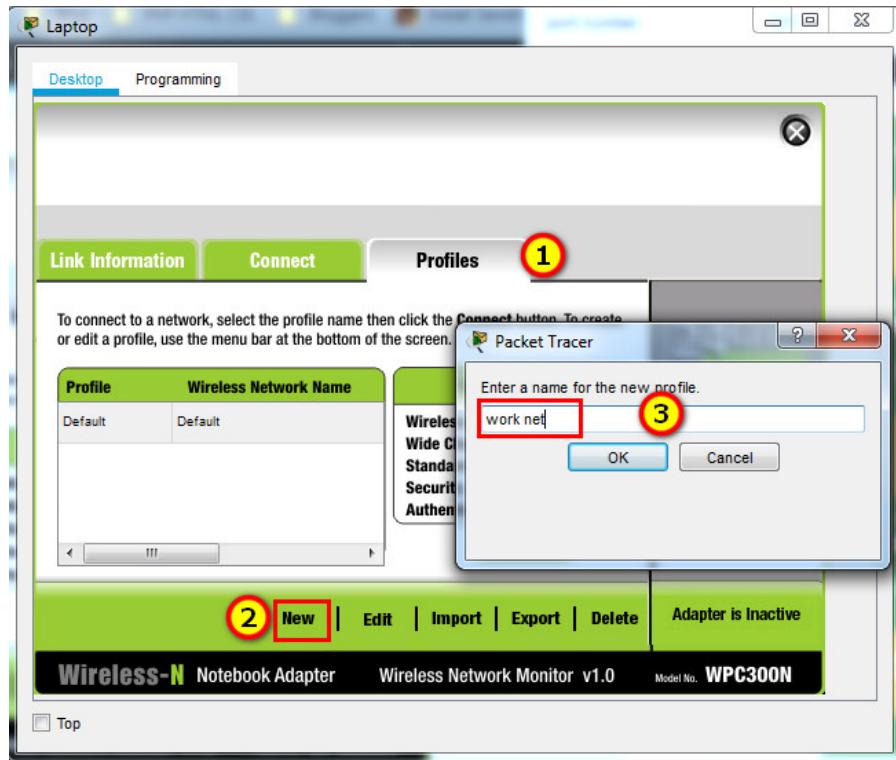
#### Step 6: Configure the wireless host.

Configure the Laptop (or Wireless Host/LT-1 laptop) to connect to the WLAN.

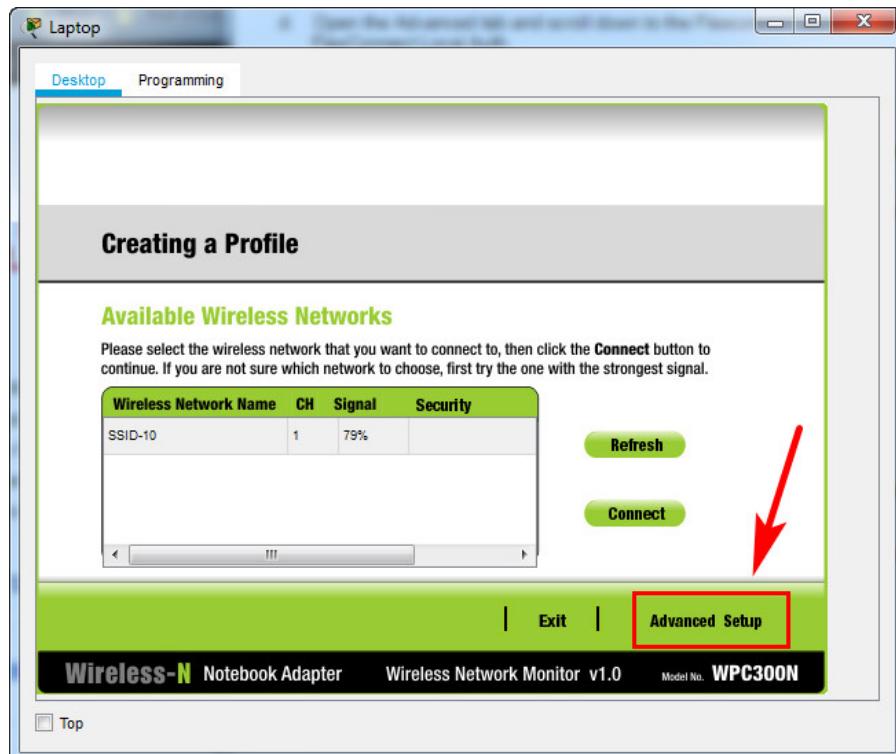
- Create a new wireless profile on the host. Use the name **work net** for the profile.

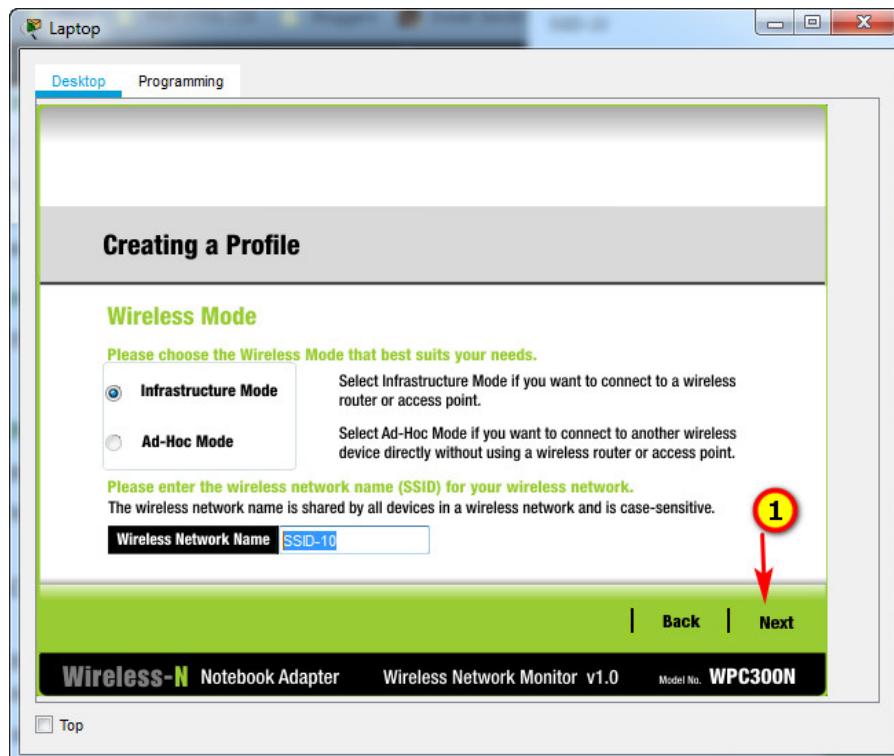
Click **Wireless Host** Laptop and open the **PC Wireless** app

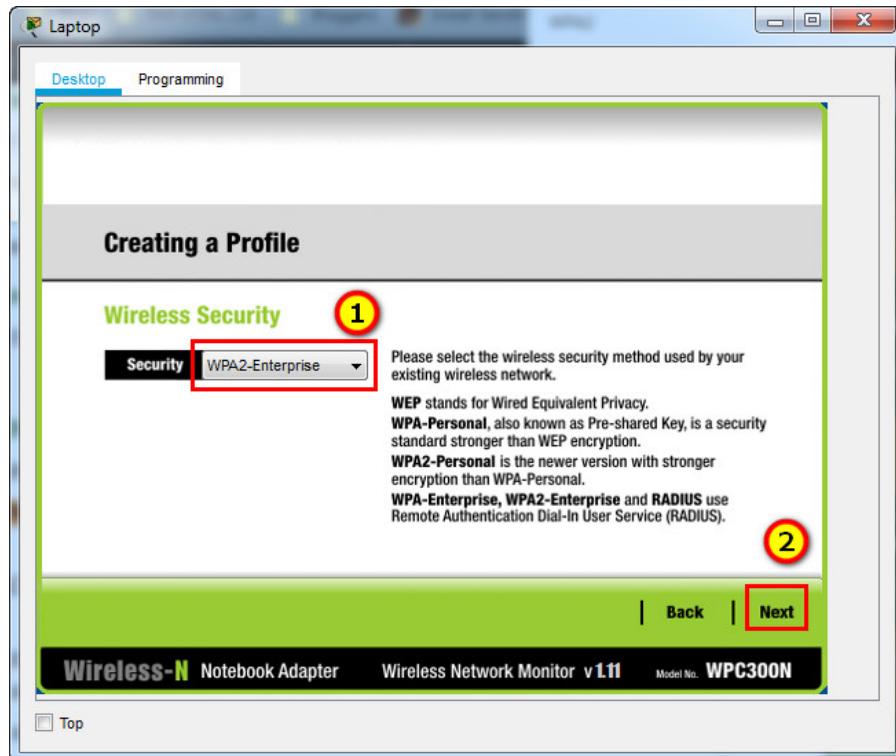




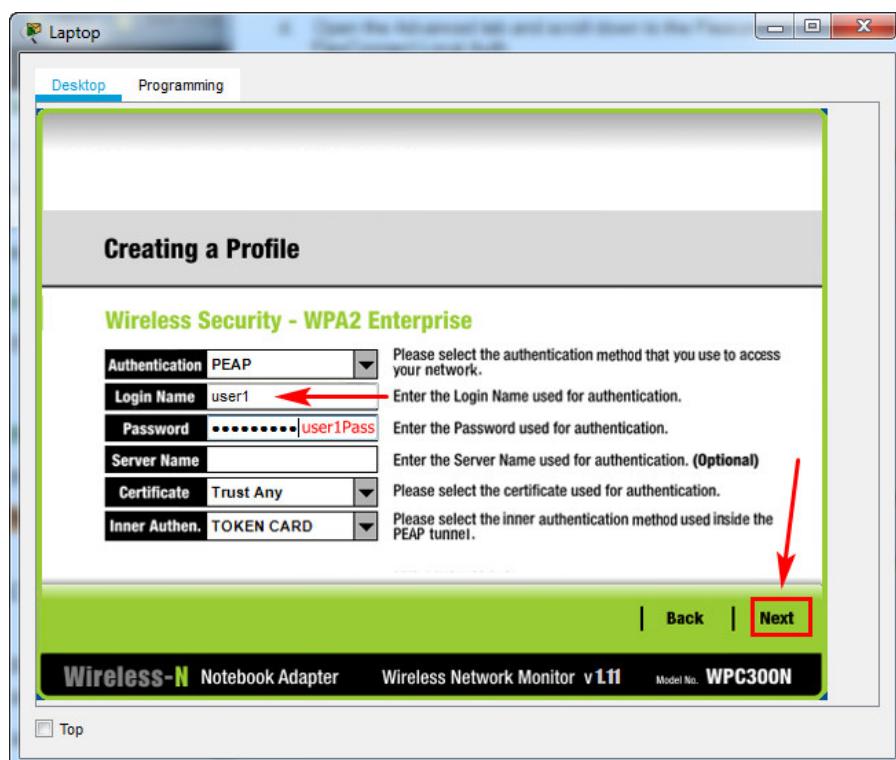
b. Configure the profile for the SSID of the WLAN.

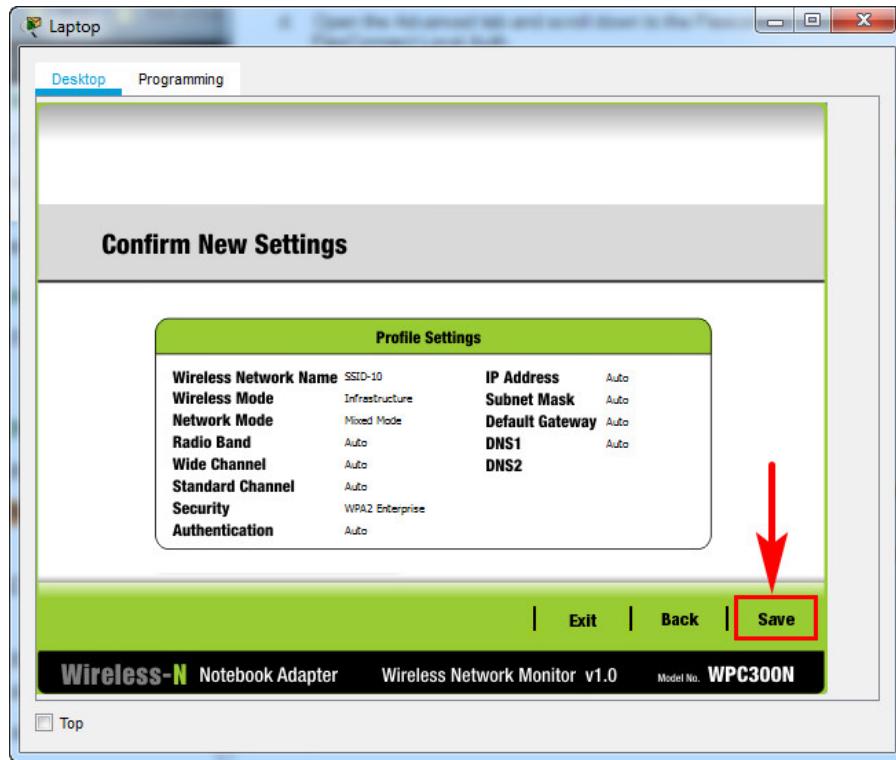






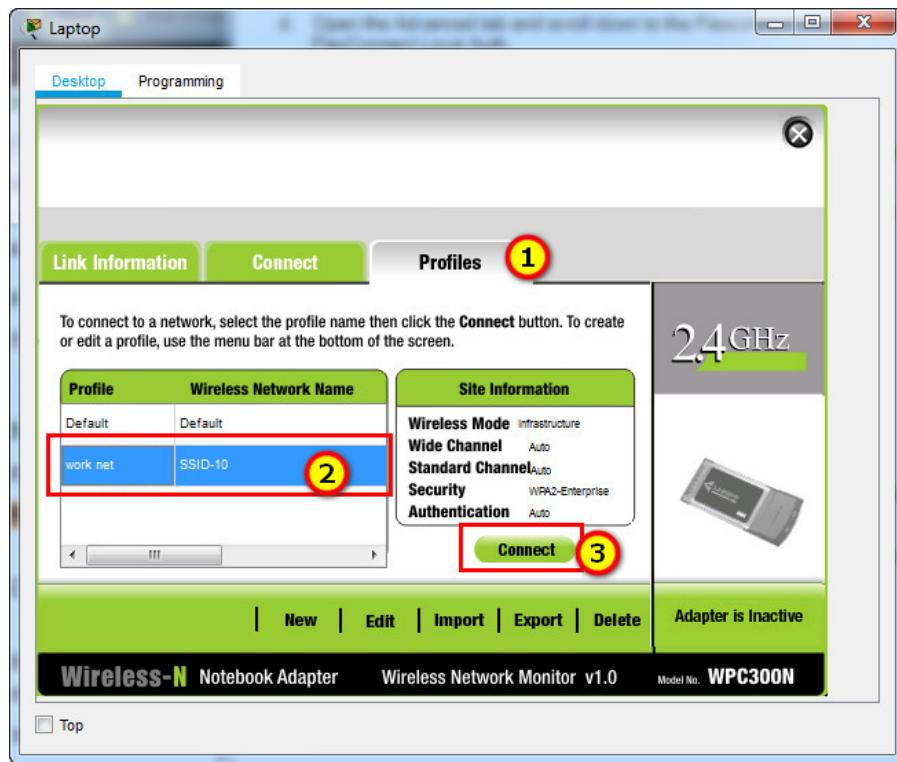
c. Use enterprise authentication with a username of **user1** and password of **user1Pass**.



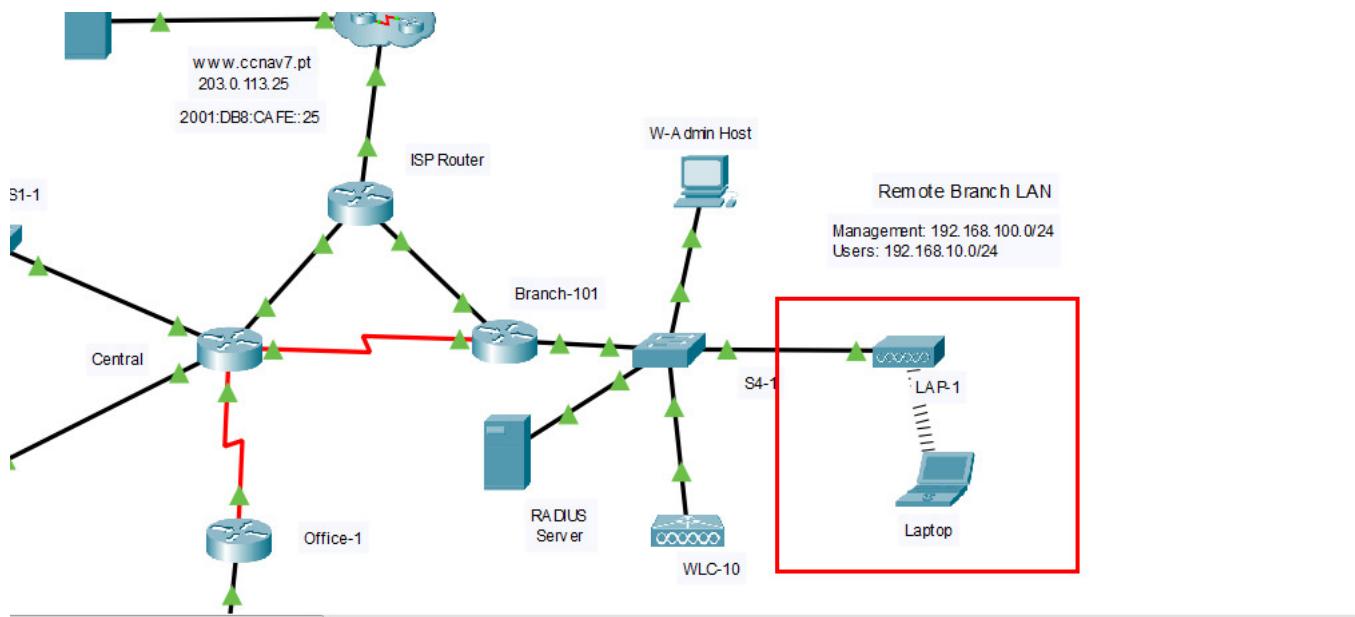


d. When you are finished, click **Connect to Network**. It will take time for the connection to be established.

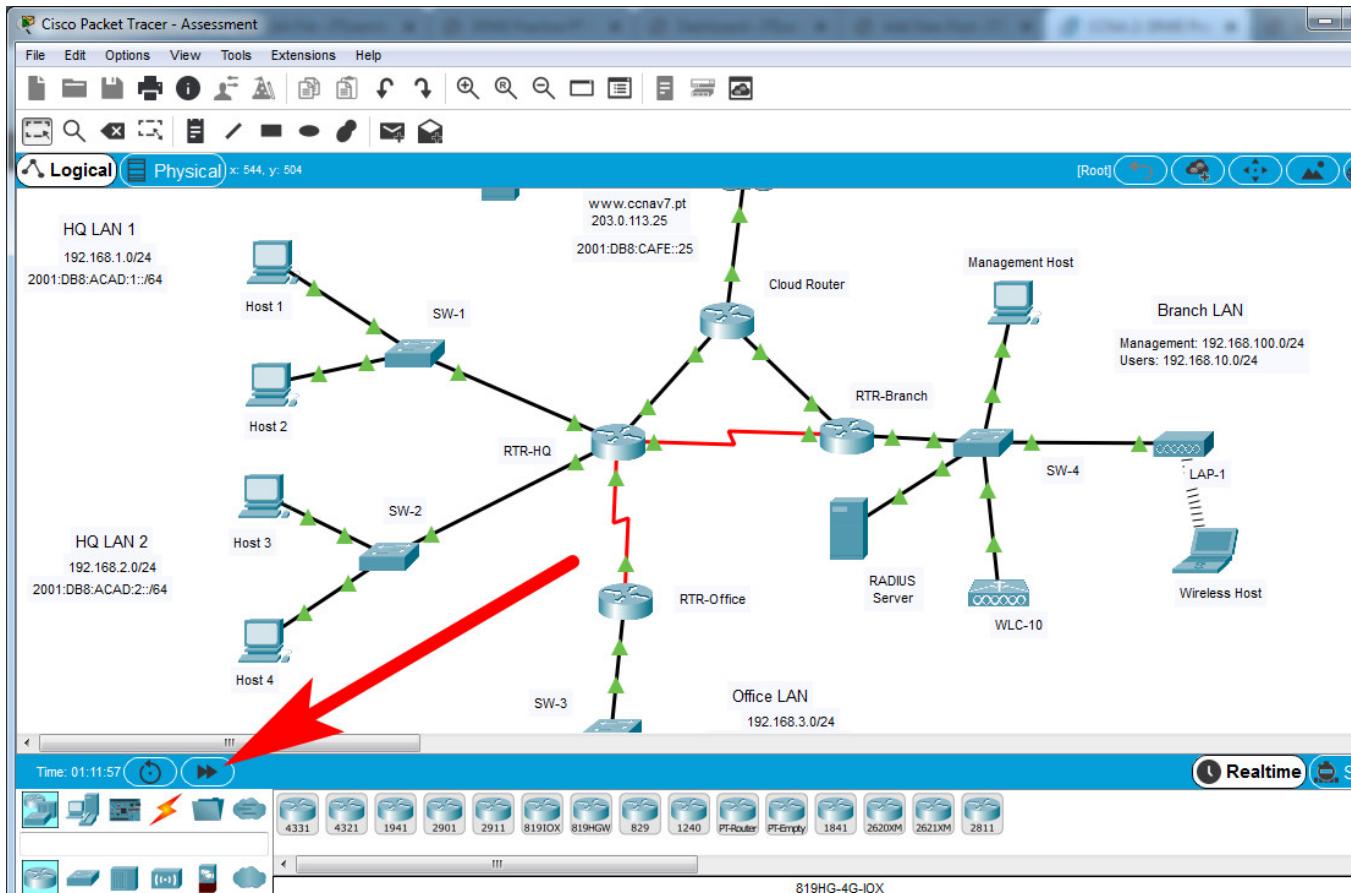




### Result



You can click the **Fast Forward Time** button speed up the process.



## Fast script – Answers

Assessment Results
Switching, Routing, and Wireless Essentials (Version 7.00) - SRWE Practice Skills Assessment - PT Part 2
 Date Assessment was taken: 10/10/2023 Time Assessment was taken: 00:00:00
<b>Domain Knowledge - Standard Score</b>
Max Points: 110
Earned Points: 110
Percentage: 100%
<b>PASSED</b>

## Part 1 + 2 + 3

## S1-1 Switch (or SW-1/Sw-A)

```

en
config t
vlan 10
name users
vlan 999
name unused
exit

interface range f0/1-5, g0/1
switchport mode access
switchport access vlan 10

interface range f0/1-5
switchport port-security
switchport port-security maximum 4
switchport port-security violation restrict
switchport port-security aging time 10
switchport port-security mac-address sticky
exit

interface f0/1
switchport port-security mac-address 00D0.D3DC.2825
exit

ip dhcp snooping
ip dhcp snooping vlan 10,999
interface range f0/1-5, g0/1
ip dhcp snooping limit rate 5
exit
interface g0/1
ip dhcp snooping trust
exit

ip arp inspection vlan 10,999
interface g0/1
ip arp inspection trust
exit

interface range f0/1-5
spanning-tree portfast
spanning-tree bpduguard enable

interface range f0/6-24, g0/2
switchport mode access
switchport access vlan 999
shutdown

```

#### **Branch-101 Router (or RTR-Branch/R-B-10)**

---

```

en
config t
interface g0/0/0.10
description WLAN users
encapsulation dot1q 10
ip address 192.168.10.1 255.255.255.0
exit

ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.10.254
ip dhcp pool WLAN-hosts
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 198.51.100.163
exit

interface g0/0/1
ip address dhcp

end
exit

```

#### **Central Router (or RTR-HQ/R-1-A)**

---

```
enable
conf t
ip route 0.0.0.0 0.0.0.0 g0/0/2
ip route 0.0.0.0 0.0.0.0 s0/1/0 10
ip route 192.168.10.0 255.255.255.0 g0/0/2
ip route 192.168.10.0 255.255.255.0 s0/1/0 10
ip route 192.168.3.122 255.255.255.255 s0/1/1
ipv6 unicast-routing
ipv6 route ::/0 2001:DB8:ACAD:A::2
ipv6 route ::/0 2001:db8:acad:b::2 10
ipv6 route 2001:db8:acad:3::122/128 2001:db8:acad:d::2
```

---

**Branch-101 Router (or RTR-Branch/R-B-10)**

---

```
enable
configure terminal
ip route 0.0.0.0 0.0.0.0 g0/0/1
ip route 0.0.0.0 0.0.0.0 s0/1/0 10
ipv6 unicast-routing
ipv6 route ::/0 2001:DB8:ACAD:C::1
ipv6 route ::/0 2001:DB8:ACAD:B::1 10
```

---

**Download PDF and Packet Tracer files:**

---

[sociallocker id="54558"]



[\*\*Packet Tracer File – SRWE Practice PT Skills Assessment \(PTSA\) – Part 2\*\*](#)    201.26 KB    8732 downloads

---

...

[Download](#)

[/sociallocker]