NETGEAR® ProSAFE® WC7520 Wireless Controller

Configuring Office and Guest SSIDs Using a Layer 3 Switch on Separate Layer 3 Subnets
INTRODUCTION

Business environments are dynamic in nature, with many different types of users, each with a wide range of networking needs. Employees and contractors require Internet connectivity and access to printers, files, and other shared resources through the wireless network. The organization may also want to enable Internet access for visitors, without allowing them to see the other users or access any corporate resources. This paper will discuss how to use the NETGEAR® ProSAFE® wireless system to provide an appropriate level of access to multiple groups of users while maintaining the highest level of security.

OVERVIEW

There are two ways to go about resolving this challenge. One way is to use two access points – one for employees and contractors, and one for the guest users. However, this strategy requires twice the amount of equipment to be purchased, configured, and managed long-term, thereby increasing capital and operating expenses.

A superior solution is to use access points that support multiple SSIDs, such as NETGEAR ProSAFE access points. Then, using the NETGEAR ProSAFE WC7520 Wireless Controller, the organization can easily configure and maintain two separate SSIDs on one access point – one for employees and the other for guests. A single ProSafe WC7520 can manage up to 50 access points from a single interface, blending extraordinary flexibility with robust security administration.

CONFIGURATION

The first thing that needs to be done is to separate the guests from the employees using VLANs on the wired network. To do this, we’ll create an Office VLAN and a Guest VLAN. Then, we’ll enable routing on that VLAN and provide Guests with their own subnet.
Here’s the address scheme we’ll use:

**Switch**
- VLAN1 (Management and internet)
  - 192.168.1.2
- VLAN10 (Office)
  - 192.168.10.1
- VLAN20 (Guest)
  - 192.168.20.1

**WC7520**
- 192.168.1.250

**PC**
- 192.168.1.3

In this scenario we’re assuming that there is already a wired network set up on VLAN 1, 192.168.1.0/24, with a router with a DHCP server and internet access on 192.168.1.1.

**Internet/Corporate Router**
- 192.168.1.1

**CONFIGURATION**

**M4100 Switch**

**Step 1 – Add VLAN 10 and 20 for Wireless**

Select **Routing – VLAN – VLAN Routing Wizard** for each VLAN to add the VLAN, IP address and enable routing.
You only need to tag the ports that have the access points in them. Since the actual traffic will go through the switch, it doesn't go through the WC7520 itself. After, make sure that the ports for the APs and WC7520 have VLAN1 Untagged and PVID 1 set, for discovery of the access points later.
Step 2 – Configure the DHCP pools
Select System – Services – DHCP Server. Select DHCP Pool Configuration and add 2 pools, one for each VLAN. Making sure you pick the correct subnet, assign default gateway matching the switch VLAN IP address created earlier in the wizard, and assign a DNS server. Don’t forget to turn on the server under System – Services – DHCP Server – DHCP Server Configuration.
Step 3 – Add ACLs to deny Guests from reaching the Office LAN and WLAN

Add ACLs like in the screenshots below, making sure that there is a Permit – Match Every at the end, and above that, rules to deny traffic to the Office LAN and Office WLAN, but allowing access to the router for DNS. After creating the ACLs, you have to bind them to the Guest VLAN.
WC7520

Step 1 – Configure the IP settings
Log in to the WC7520 and select Configuration – System – IP/VLAN.

Connect to the default IP of the WC7520, 192.168.0.250. Change the IP address; we’ll use 192.168.1.250/24. The default gateway and the DNS server will be the router on 192.168.1.1. You’ll have to change IP now, and reconnect to the WC7520 on its new IP address.
Step 2 – Configure the Office SSIDs

Select Configuration – Profile – Basic – Radio. We will call the first wireless network Office; we won’t use any encryption for now. We will call the second wireless network Guests. We’ll enable client separation to prevent wireless guests from seeing each other.
Step 3 – Plug in your Access Points to port 3 and 4
Make sure the Access Point is on Factory Defaults, and wait until it’s fully booted up.
Step 4 – Discover and add your AP
Select Access Point – Discovery Wizard. Choose Factory Default state and Same L2 network. You should find the Access Point on its default IP address. Select it, and select Add. Leave the password field blank and select Add. Wait until you see Connected in the status column. This will take a few minutes.

Router

Step 1 – Add static routes to new Wireless LANs
The router needs to know about these new IP subnets. So we need to add two static routes. One for 192.168.10.0/255.255.255.0 and one for 192.168.20.0/255.255.255.0, through the gateway, which is the switch on 192.168.1.2.

NOTES
This guide is based on a factory default WC7520, running firmware 2.5.0.5_3215.