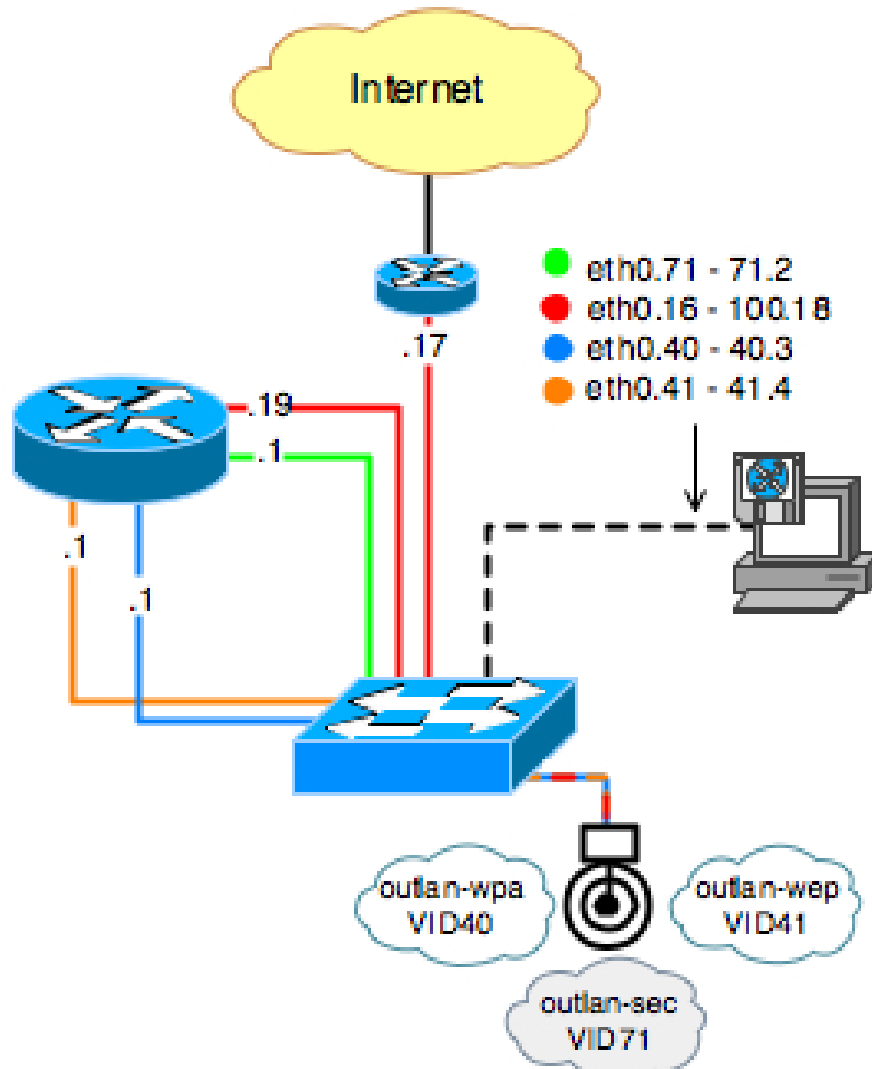


# Initial Configuration of a Cisco 1200 802.11g WLAN Access Point

Michael J. Martin

Our router expert continues his series on building a secure wireless LAN with a Linux base. We've already covered network segmenting with virtual LANs (VLANs) and the 802.1Q standard, as well as supporting 802.1Q interfaces on Linux and Cisco IOS. Today we will show how to utilize a single Cisco 1200 series access point (AP) to provide access to three different IP network segments using VLANs and multiple service set identifiers (MSSIDs).



The above diagram illustrates the VLAN/MSSID configuration we will cover in this article. In this configuration we'll provide access to three IP network segments, supporting three different security policies:

- WiFi-Protected Access (WPA)
- Wireless Equivalency Protocol (WEP), the original admission control and data security standard developed for wireless access
- OPEN/IP security (IPsec) which leaves the wireless segment open to any client, but requires the use of an IPsec client to access any real data

# Initial Configuration of a Cisco 1200 802.11g WLAN Access Point

Michael J. Martin

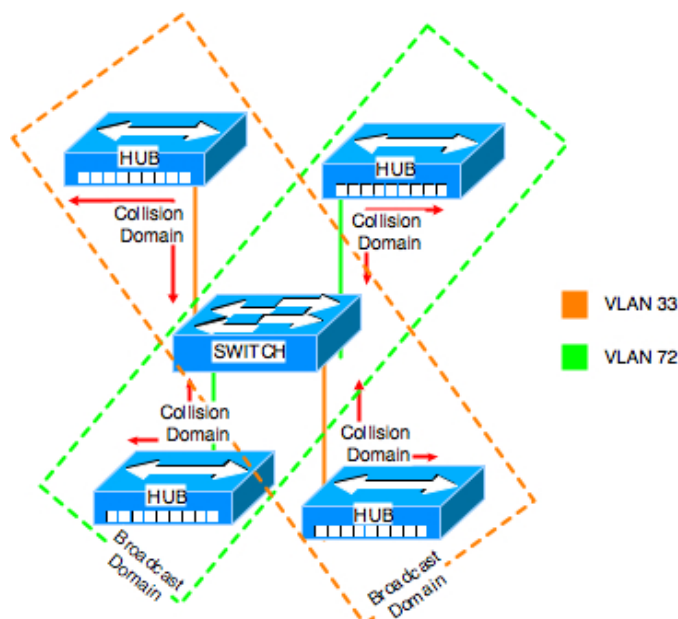
The configuration of these security policies is the subject of future articles. VLAN and MSSID support is required for this network access model. It will enable the network partitioning needed to provide unique Layer 3 network access and discreet WLAN client authentication policies. Without VLAN/MSSID support, a Cisco AP can only support access to a single Layer 3 network segment and a single client authentication policy such as WEP or WPA.

A wireless AP configured to provide access to single SSID and LAN segment operates more or less like an Ethernet hub. Wireless Ethernet uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to manage client access to the radio frequency to transmit and receive data. Wired Ethernet devices utilize Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to regulate client access to the wire to transmit and receive data.

The way something appears to be is not always the way it really is. In reality, a wireless AP is a network bridge. In the context of Ethernet, a network bridge is any device that is used to interconnect two (or more) Ethernet media collision domains in the overall formation of a broadcast domain. An Ethernet collision domain is the physical transmission medium shared by nodes to transmit and receive Ethernet frames; its access is governed by CSMA/CD or CSMA/CA. A broadcast domain is a number of collision domains interconnected using Ethernet bridges or switches.

A VLANs is the logical, rather than physical, manifestation of an Ethernet broadcast domain. Using VLAN tagging, multiple Ethernet broadcast domains can utilize the same physical link between two bridges or switches. Using VLANs on an Ethernet switch (which is just a large multi-port bridge with each port a single collision domain) makes it possible to carve up the switch's port density to support multiple broadcast domains, each operating independently of the other.

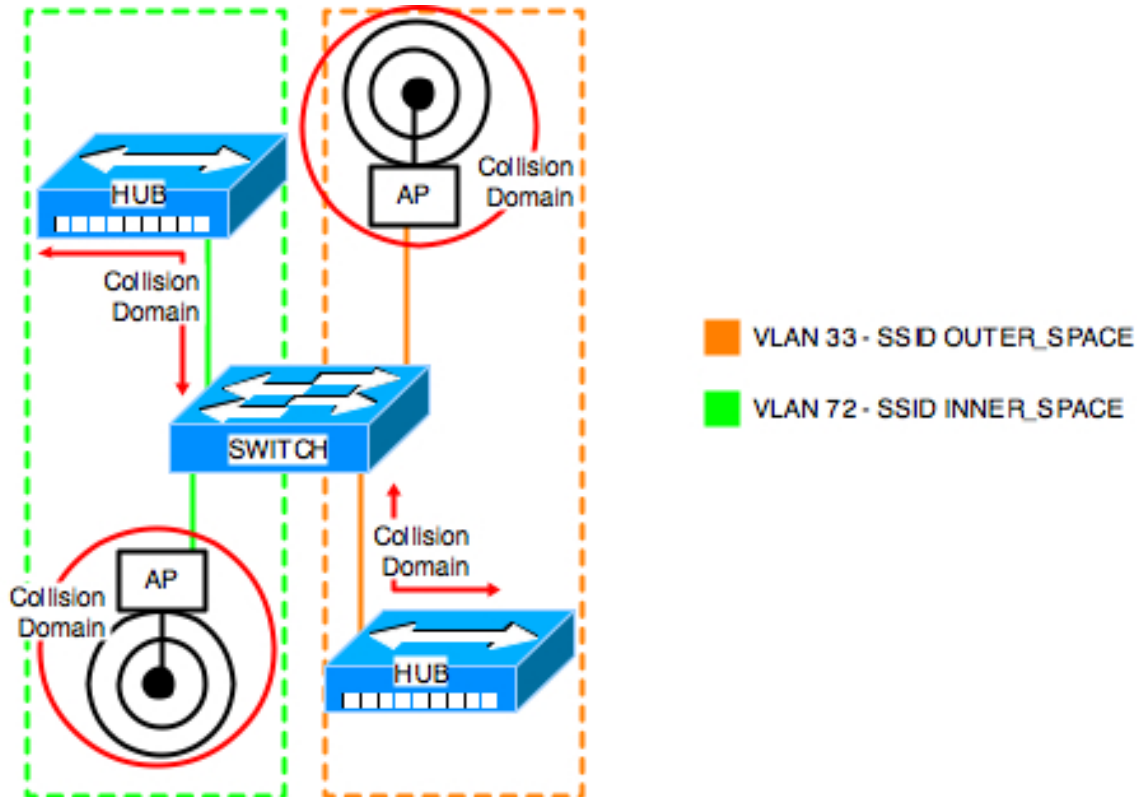
What makes the broadcast domain so important is that each of the nodes connected to the Ethernet broadcast domain is considered to be "local" to the others (even when they exist across multiple switches). That means that all of the nodes connected to the broadcast domain can know how to directly exchange Ethernet frames with each other. Typically, a single IP network subnet is mapped to a single Ethernet broadcast domain. So the logical partitioning of Ethernet broadcast domains by extension partitions Layer 3 subnets.



# Initial Configuration of a Cisco 1200 802.11g WLAN Access Point

Michael J. Martin

The illustration above depicts the standard implementation of Ethernet hubs and an Ethernet switch using VLANs to support two Layer 2/3 network segments. Each segment at the Layer 2 level operates independently; a router or routing switch could be used to interconnect the two segments and enable the exchange of data at Layer 3. This exact same configuration can be supported using wireless APs:



Each AP and each hub operates as a collision domain and the Ethernet switch "bridges" them together. Data can be exchanged between the two broadcast domains at Layer 3 using a router or routing switch.

Here is where it gets a little messy: When you implement VLANs and MSSID support on the Cisco 1200 AP, you effectively convert the AP from a standard two-port bridge into a multi-port bridge. Now, today the term "multi-port bridge" is almost synonymous with "switch." The AP, however, does not become a wireless switch. In fact, quite the contrary happens. So while MSSIDs do provide the ability to create unique SSIDs in terms of client association limits and authentication schemes and operate as a "bridged" collision domain, there is still only one radio that utilizes one frequency with the available bandwidth shared between each of the SSIDs. The MSSID virtualizes the radio in much the same fashion that an 802.1Q trunk port operates. There are a number of different networks laying claim to the port, but in the end each packet is forwarded one at a time.

This kind of bandwidth sharing does not present a problem in most cases, because most 802.1Q trunk ports are configured using Gigabit Ethernet as the interconnection medium. When you do this with a fixed transmission range radio, you need to keep in mind how radio access works with 802.11. The radio operates at the lowest client supported speed. So, if you have users on the OUTER\_SPACE SSID operating at 54 Mbps and someone joins the INNER\_SPACE SSID at 11 Mbps, everyone will run at 11 Mbps.

# Initial Configuration of a Cisco 1200 802.11g WLAN Access Point

Michael J. Martin

I emphasize this fact because throughout this series on WLAN, part of the emphasis has been the use of inexpensive APs (such as the Linksys WAP54G) because they are inexpensive and they offer the same basic security options (i.e., WPA and WEP) as the Cisco 1100/1200 APs. While wireless client authentication is important, to a large degree the security of our configuration is not dependent on any of the enhanced support options that are part of the 1100/1200 series APs. So why are we talking about the Cisco 1200 today? Well, after some recent client experiences, reader feedback (I love reader feedback) and enhancements to the Cisco 1200's capabilities such as VLAN/MSSID support, I thought some attention was due.

Using a Cisco 1200 AP instead of three Linksys WPA54Gs does provides some advantages in terms of support, manageability (i.e., authentication, authorization and accounting support, command line interface and standard IOS command support) and better utilization of radio spectrum space. I feel that makes it worth the additional cost for some environments.

There are also a few caveats to supporting the following solution. The first is that the unit must be a Cisco 1200 that has an 802.11g radio (model # C1200-K9W7-M or later). The second is that the unit must be running Cisco's Internetwork Operating System (IOS). Now, if your 1200's radio supports only 802.11b and/or is running the VxWorks OS, you do have options. First, you can purchase an 802.11g radio upgrade for around \$100.00. This is a great option for shops that have existing APs. It is also possible to upgrade the OS code from VX to IOS. Cisco has a process to perform this conversion, but it is not reversible. Once you go IOS, you can't go back.

The process for upgrading the IOS code on the AP is the same one followed when upgrading the code on a Cisco IOS-based switch: using the `<archive>` command. IOS-based routers use a single compressed file with a .bin extension. The file is read from the flash file system and uncompressed into memory. Java-based http graphical user interface (GUI) switches and APs boot the core OS using the same process, but rely on html and Java files stored on the device's flash file system. So when you upgrade the IOS code, you need to upgrade the GUI tree as well. Code for switches and APs are stored as tape archive files with a .tar extension. To upgrade the IOS and GUI, use the following command syntax:

```
archive download-sw /overwrite tftp://server_address/tarfile
```

The configurations discussed in this and subsequent articles on the 1200 AP were tested using IOS c1200-k9w7-tar.123-4.JA.tar. There are issues with MBSSID and VLAN support in later code versions, so testing should be performed before upgrading to later code.

With APs it is best to start with the default config. To reset the AP to the factory default, disconnect the power, hold the "mode" button and reconnect the power, and then hold the mode button until the AP's center light turns amber. When the unit completes the boot cycle it will have no SSID information and the LAN interface will support IP assignment via DHCP. (This is also the default on newer APs. Some older units will have tsunami configured as the default SSID and will be active out of the box -- very secure.)

Unlike other Cisco hardware, the AP allows you to open a telnet session (or use the http server, enabled by default as well) to the device in its default state. Once the connection has been established, you will be asked for a username and password, which is the very secure combination of Cisco:Cisco:

```
Trying 172.30.80.48...  
Connected to 172.30.80.48.
```

# Initial Configuration of a Cisco 1200 802.11g WLAN Access Point

Michael J. Martin

Escape character is '^]'.

## User Access Verification

Username: Cisco

Password:

ap&rt;

There is also a default password. I'll give you three guesses...give up? It's "Cisco!" Now the sarcasm you may be sensing is not directed at Cisco. The fact is that Cisco was insightful enough to predict that there would be boneheads in the world that would connect an AP to a live network without ever configuring the unit. These passwords provide a screen door, at best, but at least there is a door. The message here is: Do not connect any AP to a live network. Next month, we will get into the switch and AP configuration.