vWLAN Access Point Discovery

Date: January 26, 2011
Revision: 1.0

Introduction

The cloud-based approach of the vWLAN distributed architecture means that the Primary and Secondary (Backup) vWLAN Appliance or vWLAN Virtual Appliance (VMware) and BlueSecure Access Points (BSAP) can be deployed anywhere. This flexibility allows several different deployment scenarios. For example the Primary and Secondary vWLAN Appliances could be deployed centrally at the corporate head quarters or data center (Private Cloud), or perhaps the Secondary vWLAN Appliance could be deployed at a remote disaster recovery site or data center. The Primary and Secondary vWLAN Appliances could even be deployed in a hosted model (Public Cloud), or a mix of both; perhaps the Primary vWLAN Appliance could be deployed at the corporate head quarters or data center while the Secondary vWLAN Appliance could be deployed in a hosted model. BSAPs can be deployed local to the vWLAN Appliance or at remote sites. BSAPs can even be deployed behind NAT devices such as routers or firewalls. Whatever deployment scenario you choose, BSAPs must be configured with a method to discover the Primary and Secondary vWLAN Appliances. Those methods include:

1. **Statically Configuring the BSAP via the CLI.**
2. **Configuring DHCP Option 43 in Your Organization's DHCP Server.**
3. **Configuring an Entry for apdiscovery in Your Organization's DNS server.**
4. **Caching a Previously Discovered vWLAN Appliance.**

The above order lists the precedence that is used for AP discovery. The statically configured BSAP takes precedence over DHCP Option 43, over DNS, over caching. If one method fails, then the next is tried. This document describes the AP discovery methods, the TCP/UDP ports required between the BSAP and vWLAN Appliance, and sample configurations including DHCP option 43 for the following DHCP servers:

- **Microsoft Windows Server 2008 R2 Enterprise DHCP Server**
- **ISC DHCP Server**
- **Cisco IOS DHCP Server**

Requirements

Bluesocket recommends that you have knowledge of these topics:

- Basic knowledge on the Bluesocket vWLAN solution
- Basic knowledge of DHCP

Components Used
This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Required TCP/UDP Ports
The following TCP/UDP ports are required to be open between the BSAP and vWLAN Appliance. Please ensure any firewalls or Access Control Lists (ACL) between the BSAP and vWLAN Appliance allow the following TCP/UDP ports as applicable.

1. **UDP port 53 (DNS):** AP discovery communication.
2. **TCP port 33333:** Secure TLS control channel.
3. **UDP port 69 (TFTP):** AP firmware.
4. **TCP port 28000:** Secure TLS RFIDS channel.
5. **TCP port 80 (HTTP):** Only required for captive portal and BlueProtect endpoint scanning.
6. **TCP port 443 (HTTPS):** Only required for captive portal and BlueProtect endpoint scanning.
7. **UDP port 1812 (RADIUS):** Only required for Internal 802.1X authentication. NOT required for External 802.1X authentication however may be required between BSAP and external RADIUS Server.

AP Discovery Methods
Statically Configuring the BSAP via the CLI
You can configure each BSAP for static discovery mode and populate the vWLAN Appliance IP address via the console port or SSH. It is only required to populate the Primary vWLAN Appliance IP address. When High Availability is enabled the Secondary vWLAN Appliance IP address will be automatically configured. This method is typically only recommended for small deployments and or lab testing as you would need to configure each BSAP individually.

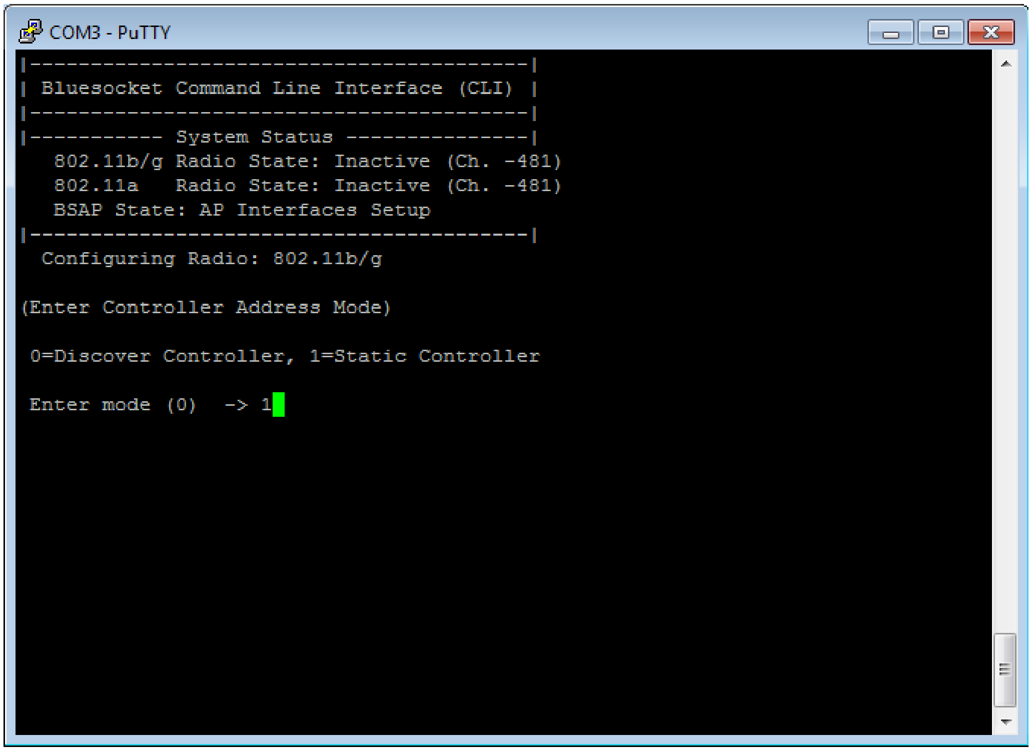
To statically configure the BSAP for AP discovery via the CLI follow these steps:

1. Connect to the console port of the BSAP using a DB9 female to RJ45 rollover cable and a terminal emulation program (115200, 8, none, 1, none).

   Or.

2. SSH to the BSAP using port 2335. The default management IP address of the BSAP is 192.168.190.1. Connect your laptop directly to the network port of the BSAP and then configure your laptop with an IP address in the same subnet, 192.168.190.2 for example. Alternatively connect the BSAP directly to the network, obtain the BSAP’s IP address from the DHCP server, and SSH to the BSAP over the network. The BSAP-1800v1 does not have a console port so you will be required to SSH to the BSAP-1800v1.

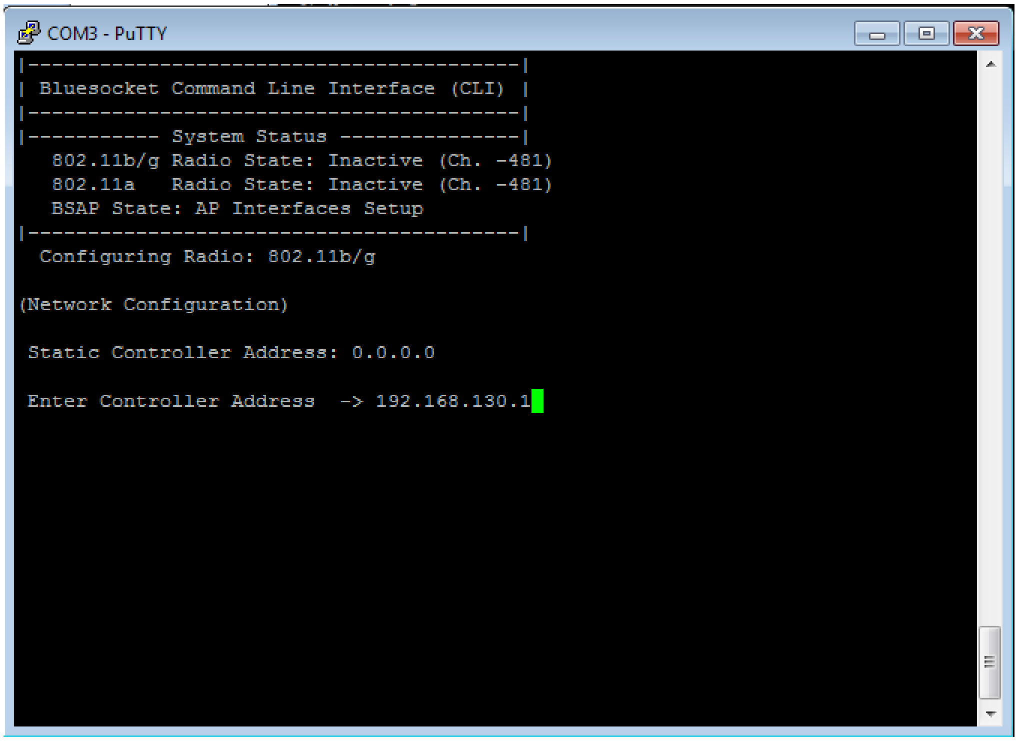
3. Log into the BSAP. The default username/password is adm1n/blue1socket. The password is configurable in the secure web based administrative console of the vWLAN Appliance under Provision>Wireless>global however if the BSAP has not yet discovered the vWLAN Appliance and automatically downloaded a configuration it will still be configured with the default password.
4. Select option 1 for Network Configuration from the Main Menu.
5. Select option 5 for Set Controller Mode from the Network Configuration Menu.
6. Enter 1 for Static Controller. You will be brought back to the Network Configuration Menu.



```
|-----------------------------------------|
| Bluesocket Command Line Interface (CLI) |
|-----------------------------------------|
|----------- System Status ---------------|
   802.11b/g Radio State: Inactive (Ch. -481)
   802.11a   Radio State: Inactive (Ch. -481)
   BSAP State: AP Interfaces Setup
|-----------------------------------------|
  Configuring Radio: 802.11b/g

(Enter Controller Address Mode)

 0=Discover Controller, 1=Static Controller

 Enter mode (0)   -> 1
```

7. Select option 6 for Set Controller Address from the Network Configuration Menu.

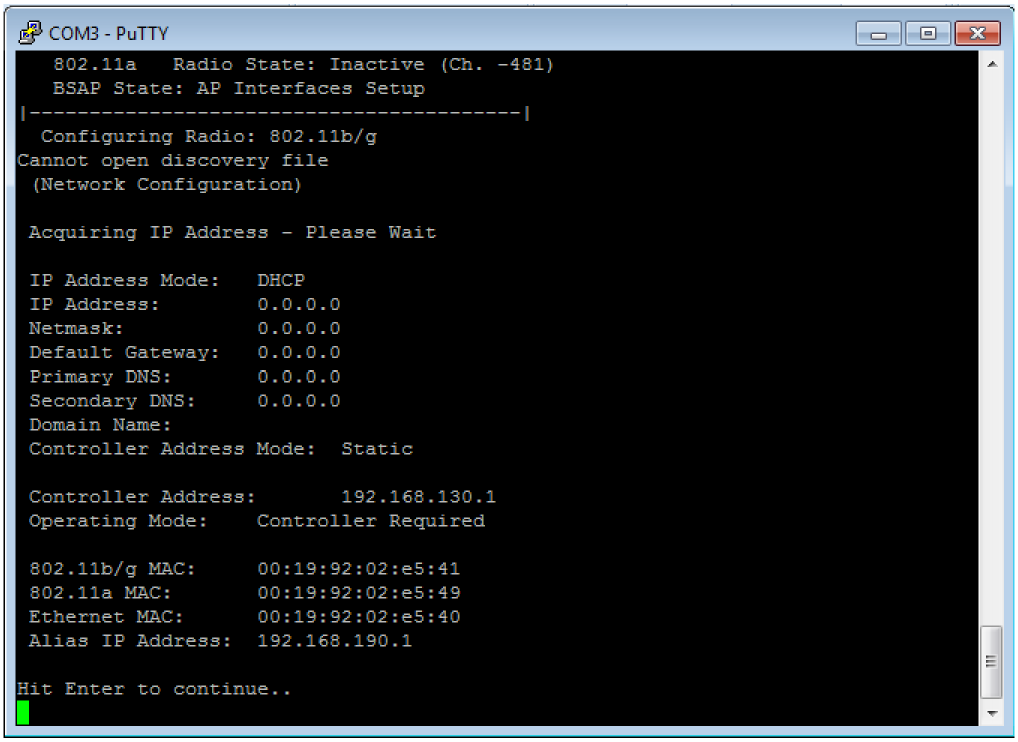
8. Enter the Primary vWLAN Appliance IP address. You will be brought back to the Network Configuration Menu. It is only required to populate the Primary vWLAN Appliance IP address. When High Availability is enabled the Secondary vWLAN Appliance IP address will be automatically configured.



```
|-----------------------------------------|
| Bluesocket Command Line Interface (CLI) |
|-----------------------------------------|
|----------- System Status ---------------|
   802.11b/g Radio State: Inactive (Ch. -481)
   802.11a   Radio State: Inactive (Ch. -481)
   BSAP State: AP Interfaces Setup
|-----------------------------------------|
  Configuring Radio: 802.11b/g

(Network Configuration)

 Static Controller Address: 0.0.0.0

 Enter Controller Address  -> 192.168.130.1
```

9. Select option P for Previous Menu from the Network Configuration Menu.
10. Select option 2 for Save/Apply Configuration from the Main Menu.
11. You will be prompted to save and reboot. Enter y for yes.
12. To verify log back into the BSAP.
13. Select option 1 for Network Configuration from the Main Menu.
14. Select option 8 for Network Summary from the Network Configuration Menu.

15. Verify the Controller Address Mode is set to Static and the Controller Address is populated with the appropriate IP address for the Primary vWLAN Appliance.



```
   802.11a   Radio State: Inactive (Ch. -481)
   BSAP State: AP Interfaces Setup
|-----------------------------------------|
  Configuring Radio: 802.11b/g
Cannot open discovery file
 (Network Configuration)

 Acquiring IP Address - Please Wait

 IP Address Mode:   DHCP
 IP Address:        0.0.0.0
 Netmask:           0.0.0.0
 Default Gateway:   0.0.0.0
 Primary DNS:       0.0.0.0
 Secondary DNS:     0.0.0.0
 Domain Name:
 Controller Address Mode:  Static

 Controller Address:       192.168.130.1
 Operating Mode:    Controller Required

 802.11b/g MAC:     00:19:92:02:e5:41
 802.11a MAC:       00:19:92:02:e5:49
 Ethernet MAC:      00:19:92:02:e5:40
 Alias IP Address:  192.168.190.1

Hit Enter to continue..
```

Configuring DHCP Option 43 in Your Organization's DHCP Server

When a BSAP sends a DHCP discover to obtain an IP address it includes DHCP Option 60. DHCP Option 60 is the Vendor Class Identifier (VCI). The VCI is a string that identifies the BSAP to the DHCP server. Below is the VCI used by all BSAPs regardless of model:

Vendor Class Identifier (VCI)

BlueSecure.AP1500

In order for the BSAP to discover the vWLAN Appliances, the DHCP server must be programmed to return the Primary and Secondary vWLAN Appliance IP addresses based on the VCI of the BSAP. To do this you need to program the DHCP server to recognize the VCI for the BSAP, and then define vendor specific information.

Vendor Specific Information

On the DHCP server, the vendor specific information is mapped to the VCI string. When the DHCP server sees a recognizable VCI in a DHCP discover from a BSAP, it returns the mapped vendor specific information in its DHCP offer to the BSAP as DHCP Option 43. On the DHCP server, Option 43 is defined in each DHCP scope (pool) that offers IP addresses to the BSAPs.

RFC 2132 defines that DHCP servers must return vendor specific information as DHCP Option 43. The RFC allows vendors to define encapsulated vendor-specific options. The Encapsulated vendor specific options are all included in the DHCP offer encoded as a sequence of Code/Length/Value within Option 43. The definition of encapsulated vendor-specific options is vendor specific.

When DHCP servers are programmed to offer vWLAN Appliance IP addresses as Option 43 for BSAPs, the encapsulated vendor-specific options are defined in this way:

- **Code:** 127 (in decimal).
- **Length**: A count of the characters of the ASCII string in the Value field (in decimal).
- **Value:** ASCII string that is a comma-separated list of Primary vWLAN Appliance IP address followed by Secondary vWLAN IP address. Secondary vWLAN IP address should start with F denoting failover. No spaces should be embedded in the list.

Example DHCP Option 43 Code/Length/Value
Primary vWLAN Appliance IP Address: 192.168.130.1
Secondary vWLAN Appliance IP Address: 192.168.130.2

- **Code:** 127
- **Length:** 28
- **Value**: 192.168.130.1,F192.168.130.2

Note: The Secondary vWLAN Appliance IP Address starts with F denoting failover. When High Availability is enabled the Secondary vWLAN Appliance IP address will be automatically configured however it is best practice to include the Secondary vWLAN IP address in DHCP Option 43 in case the BSAP is unable to obtain a configuration from the Primary vWLAN Appliance.

Converting Values to Hex
Depending on the DHCP Server it may be necessary to convert these values to hex. For example the Microsoft DHCP Server allows you to enter the Code in decimal, and the Value in ASCII characters; the Length is calculated for you automatically. The ISC DHCP Server and Cisco IOS DHCP Server however, require the values be converted to hex. Converting to hex may also be beneficial for troubleshooting purposes.

Code and Length Converted from Decimal to Hex
127=7f
28=1c

Value Converted from ASCII to Hex Using Conversion Table Below
1=31, 9=39, 2=32, .=2e, 1=31, 6=36, 8=38, .=2e, 1=31, 3=33, 0=30, .=2e, 1=31, F=46, 1=31, 9=39, 2=32, .=2e, 1=31, 6=36, 8=38, .=2e, 1=31, 3=33, 0=30, .=2e, 1=32,

3139322e3136382e3133302e312c463139322e3136382e3133302e32

ASCII to Hex Conversion Table	
ASCII	**Hex**
0	30
1	31
2	32
3	33
4	34
5	35
6	36
7	37
8	38
9	39
.	2e
,	2c
F	46

Complete Example DHCP Option 43 Code/Length/Value Converted to Hex
7f1c3139322e3136382e3133302e312c463139322e3136382e3133302e32

The semantics of DHCP server configurations vary based on the DHCP server vendor. This document contains specific instructions on the Microsoft Windows Server 2008 R2 Enterprise DHCP server, ISC DHCP Server, and Cisco IOS DHCP server. For other DHCP server products, consult the vendor documentation for instructions on vendor specific options.

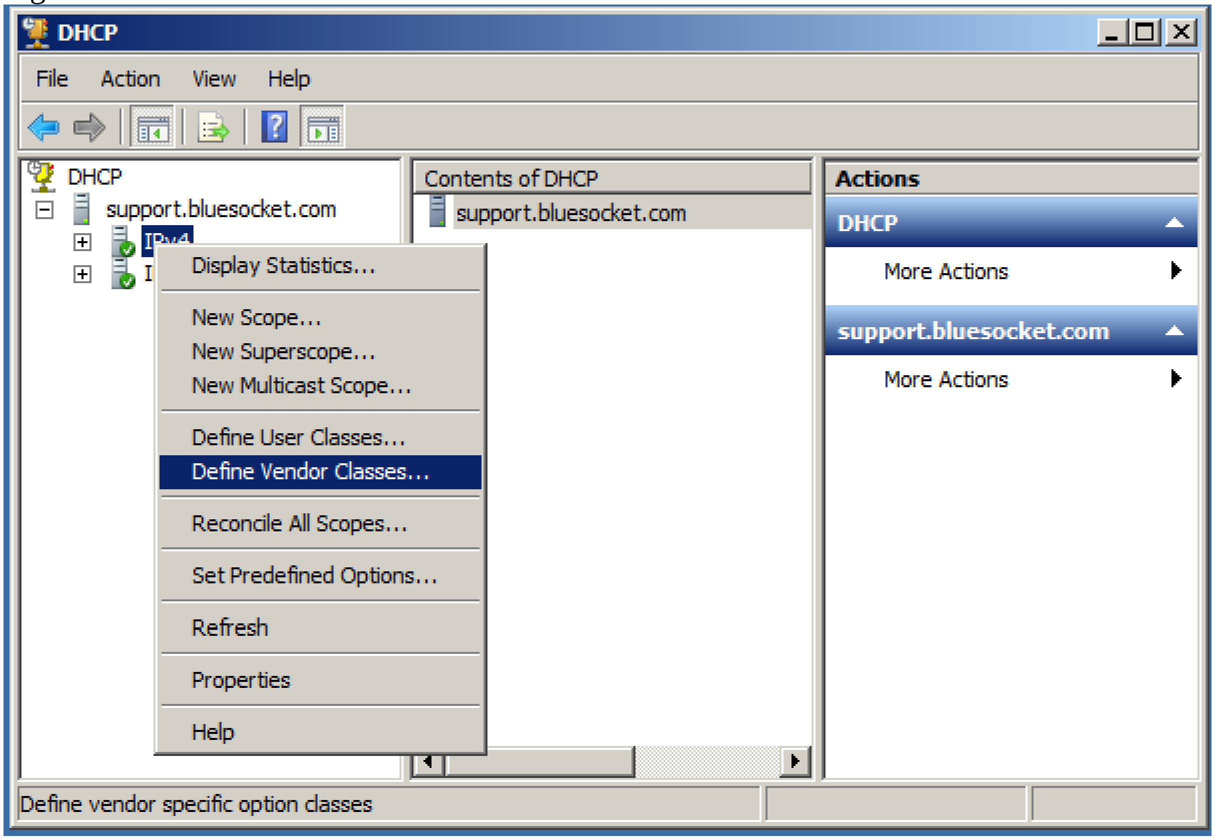
Microsoft Windows Server 2008 R2 DHCP Server

Follow these steps in order to configure DHCP Option 43 for AP discovery on the Microsoft Windows Server 2008 R2 Enterprise DHCP Server:

- Define the Vendor Class.
- Set the predefined Option 43.
- Configure the option for the BSAP DHCP scope.

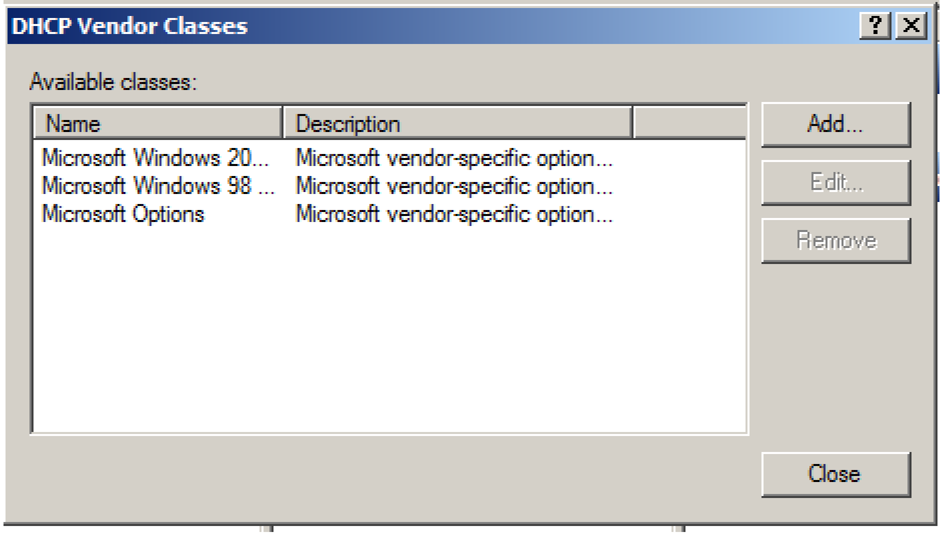
1. Go to Start>Administrative Tools>DHCP.

2. Right click IPv4 and select Define Vendor Classes.



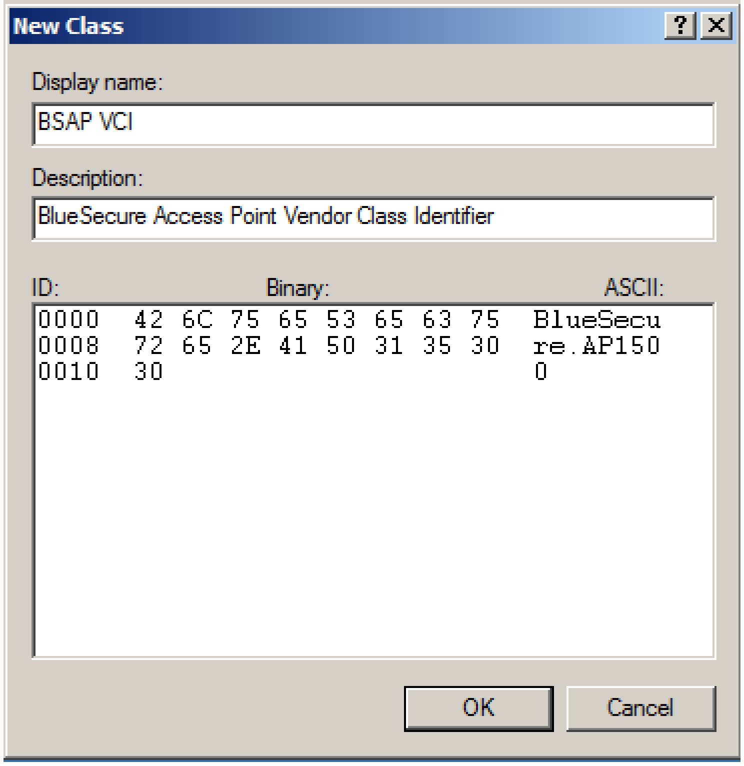
Define vendor specific option classes

3. The DHCP Vendor Classes dialogue box will appear. Click Add.



Name	Description
Microsoft Windows 20...	Microsoft vendor-specific option...
Microsoft Windows 98 ...	Microsoft vendor-specific option...
Microsoft Options	Microsoft vendor-specific option...

4. The New Class dialogue box will appear. Populate the Display Name and Description fields with a meaningful Display Name and Description. For example a Display Name of BSAP VCI and a Description of BlueSecure Access Point Vendor Class Identifier. Click in the ASCII field and populate it with BlueSecure.AP1500. Click OK.

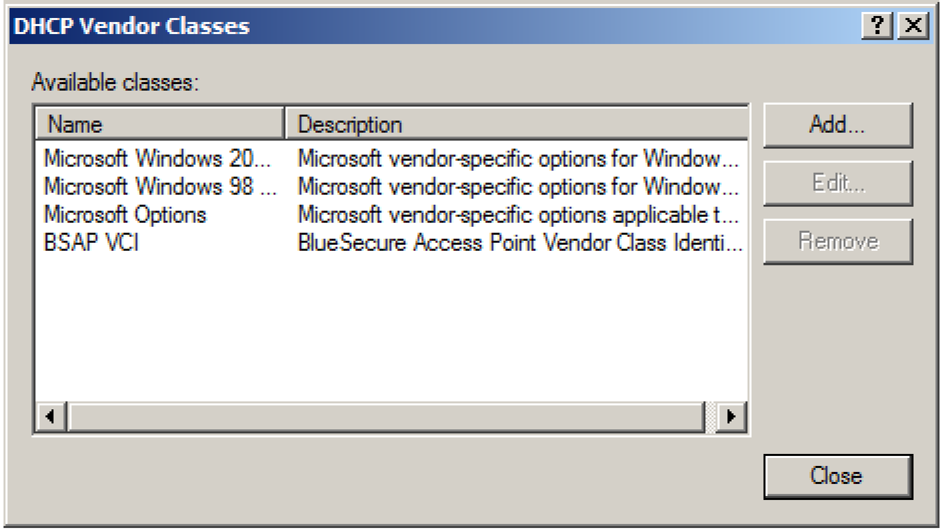


Display name: BSAP VCI

Description: BlueSecure Access Point Vendor Class Identifier

```
ID:               Binary:                    ASCII:
0000   42 6C 75 65 53 65 63 75   BlueSecu
0008   72 65 2E 41 50 31 35 30   re.AP150
0010   30                        0
```

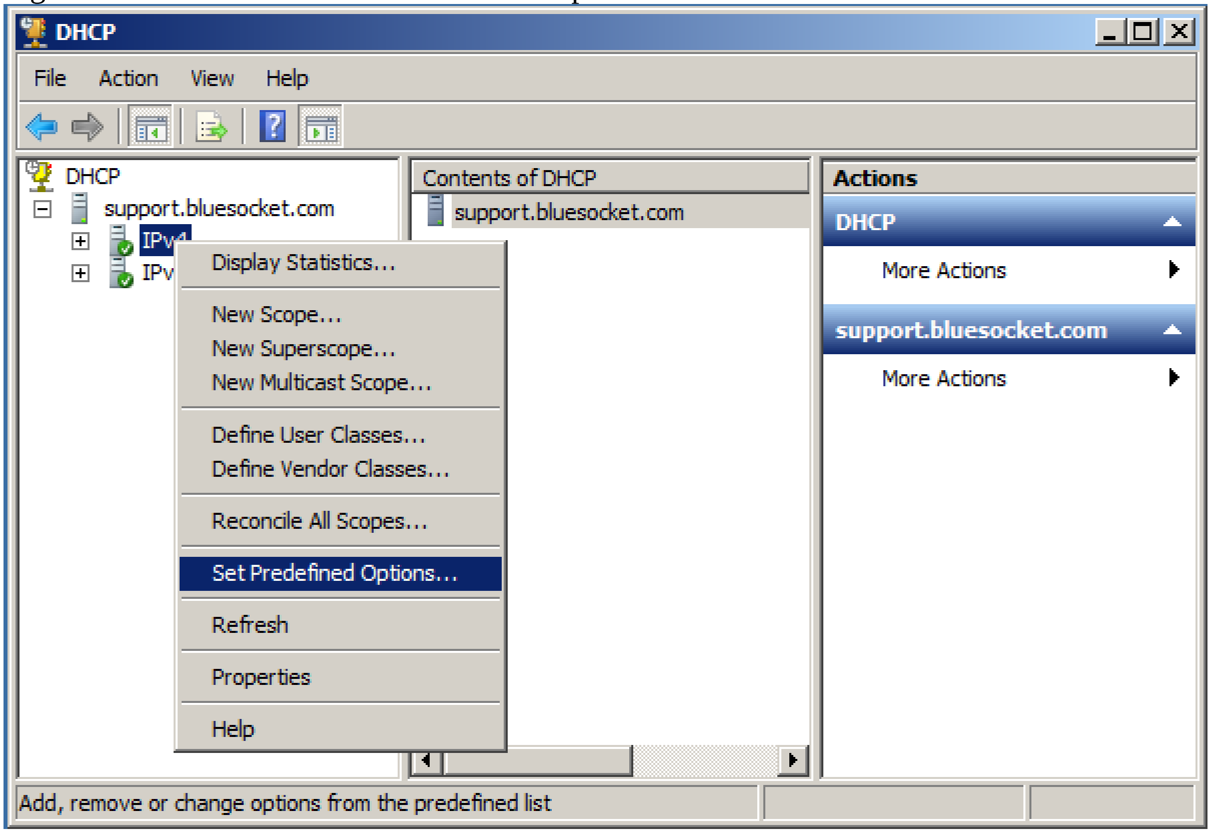
5. You will be brought back to the DHCP Vendor Classes dialogue box where you will see the name and description of the class you just created. Click Close.



Available classes:

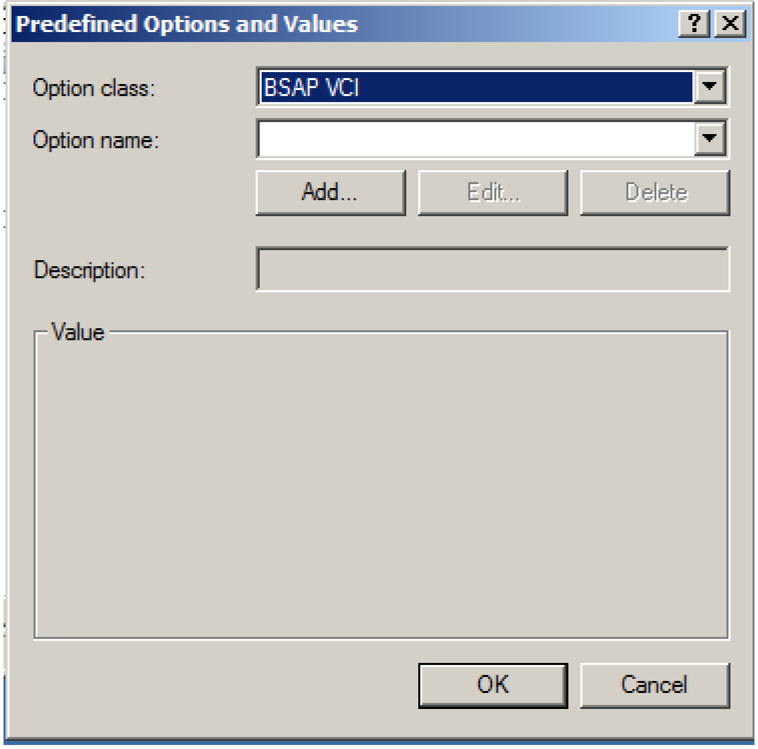
Name	Description
Microsoft Windows 20...	Microsoft vendor-specific options for Window...
Microsoft Windows 98 ...	Microsoft vendor-specific options for Window...
Microsoft Options	Microsoft vendor-specific options applicable t...
BSAP VCI	BlueSecure Access Point Vendor Class Identi...

6. Right click IPv4 and select Set Predefined Options.



Add, remove or change options from the predefined list

7. The Predefined Options and Values dialogue box will appear. Click the drop down arrow in the Option Class field and select the class created in step 4. Click Add.

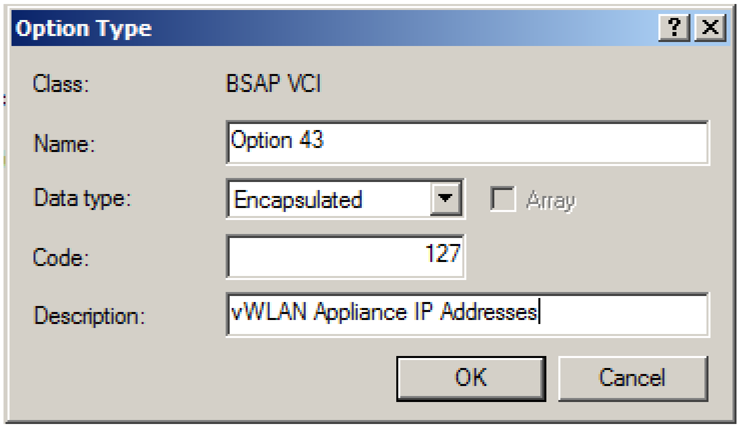


Option class: BSAP VCI

Option name:

Description:

8. The Option Type dialogue box will appear. Populate the Name and Description fields with a meaningful name and description. For example a Name of Option 43 and a Description of vWLAN Appliance IP Addresses. Click the drop down arrow in the Data Type field and Select Encapsulated. Populate the Code field with 127. Click OK.



Option Type

Class: BSAP VCI

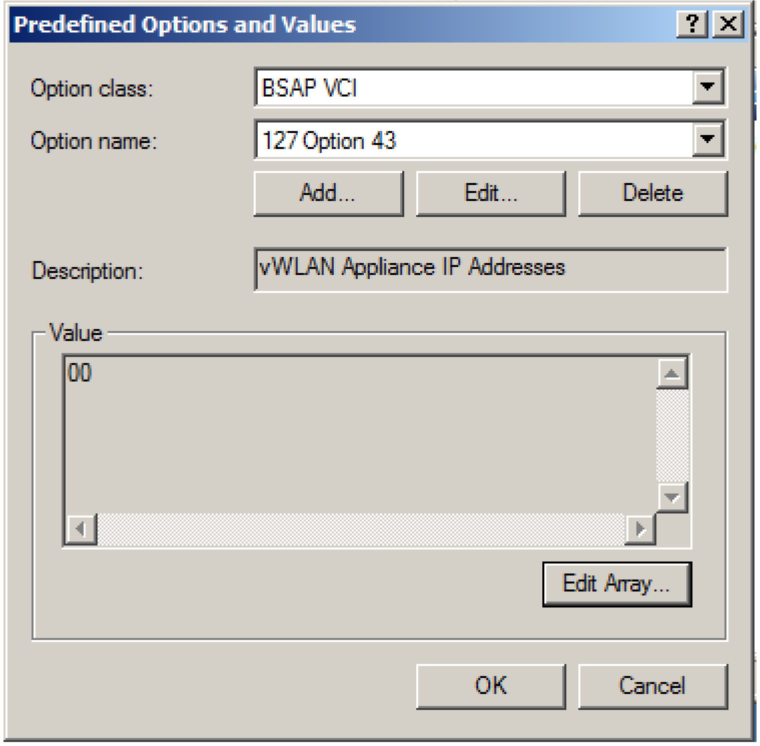
Name: Option 43

Data type: Encapsulated ☐ Array

Code: 127

Description: vWLAN Appliance IP Addresses

9. You will be brought back to the Predefined Options and Values dialogue box where you will see the name and description of the option you just created. Click OK.



Predefined Options and Values

Option class: BSAP VCI

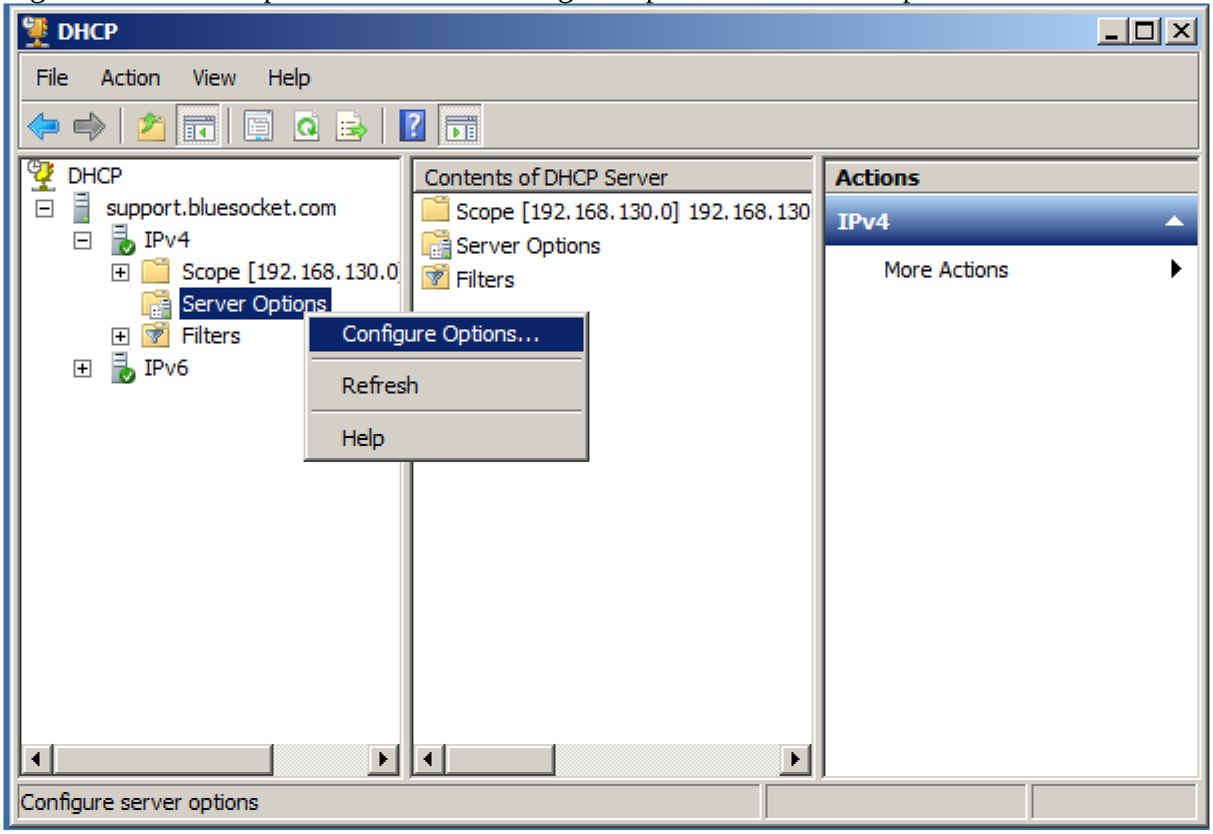
Option name: 127 Option 43

Description: vWLAN Appliance IP Addresses

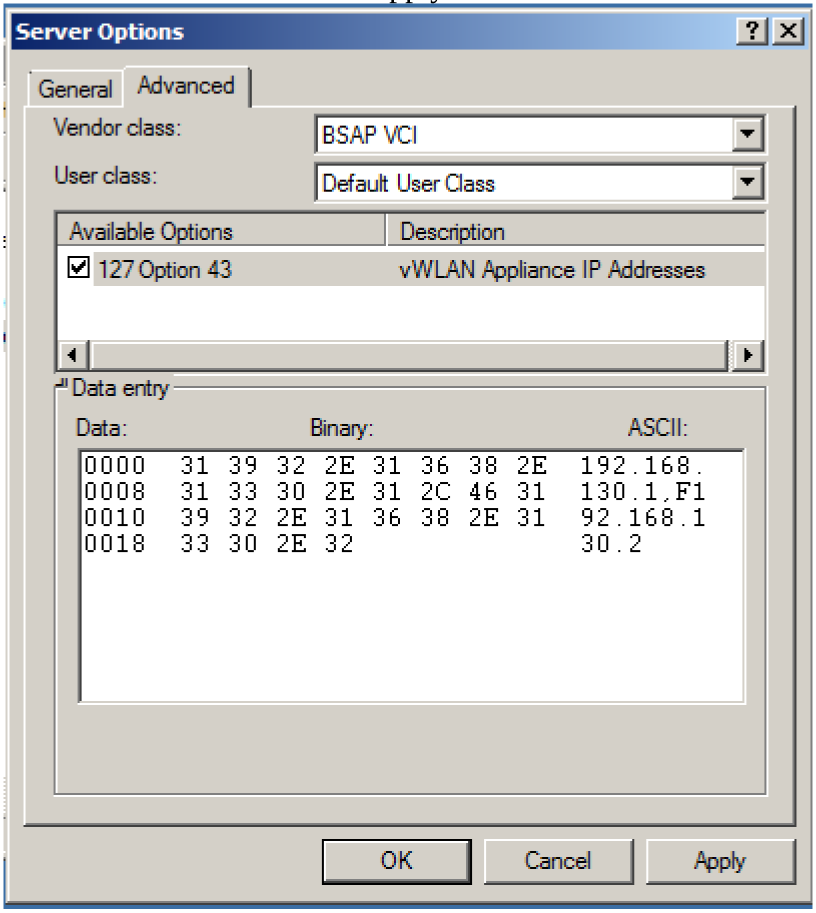
Value

00

10. Right click Server Options and select Configure Options under the scope that will service the BSAPs.



11. The Server Options dialogue box will appear. Click the advanced tab. Click the drop down arrow in the Vendor Class field and select the class created in step 4. The option created in step 8 will be listed under Available Options. Select the check box for the option created in step 8. Click in the ASCII field and populate it with a comma separated list of the vWLAN Appliance IP addresses. The Secondary vWLAN Appliance IP address should start with F denoting failover. Be sure to delete the period that is pre-inserted into the field. Click Apply and then OK.



Vendor class: BSAP VCI

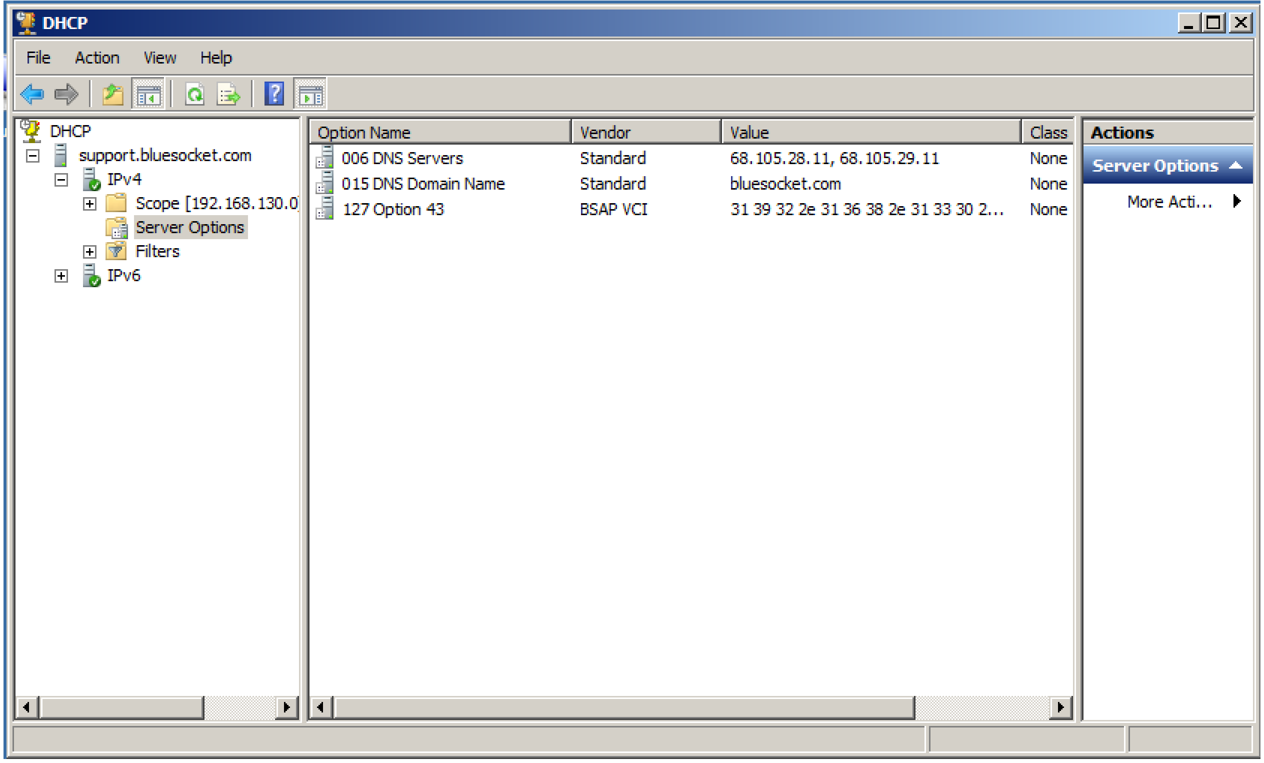
User class: Default User Class

Available Options	Description
☑ 127 Option 43	vWLAN Appliance IP Addresses

Data entry

```
Data:                 Binary:                   ASCII:
0000   31 39 32 2E 31 36 38 2E   192.168.
0008   31 33 30 2E 31 2C 46 31   130.1,F1
0010   39 32 2E 31 36 38 2E 31   92.168.1
0018   33 30 2E 32               30.2
```

12. You will be brought back to the server options for the scope that will service the BSAPs where you will see the option name, vendor, and value.



Option Name	Vendor	Value	Class
006 DNS Servers	Standard	68.105.28.11, 68.105.29.11	None
015 DNS Domain Name	Standard	bluesocket.com	None
127 Option 43	BSAP VCI	31 39 32 2e 31 36 38 2e 31 33 30 2...	None

ISC DHCP Server

Follow these steps in order to configure DHCP Option 43 for AP discovery on the ISC DHCP server:

1. Add the vendor-class-identifier (Option 60).
2. Then add the vendor-encapsulated-options (Option 43) with the following syntax:

```
if option vendor-class-identifier = "BlueSecure.AP1500" {
option vendor-encapsulated-options 7f:1c:31:39:32:2e`:33:30:2e:31:2c:46:31:39:32:2e:
31:36:38:2e:31:33:30:2e:32;
}
```

The hexadecimal string in step 2 is assembled as a sequence of Code/Length/Value converted to hex and separated by colons.

- **Code:** 127 (in decimal). Convert to hex and separate by colons for ISC DHCP Server.
- **Length**: A count of the characters of the ASCII string in the Value field. (in decimal). Convert to hex and separate by colons for ISC DHCP Server.
- **Value:** ASCII string that is a comma-separated list of Primary vWLAN Appliance IP address followed by Secondary vWLAN IP address. Secondary vWLAN IP address should start with F denoting failover. No spaces should be embedded in the list. Convert to hex and separate by colons for ISC DHCP

See **Vendor Specific Information**, **Example DHCP Option 43 Code/Length/Value**, and **Converting Values to Hex** sections above. For the given example above of a Primary vWLAN Appliance IP address of 192.168.130.1 and a Secondary vWLAN appliance IP Address of 192.168.130.2, the ISC command that is added is shown in step 2.

Cisco IOS DHCP Server

Follow these steps in order to configure DHCP Option 43 for AP discovery on the Cisco IOS DHCP server:

1. Enter configuration mode at the Cisco IOS CLI.
2. Create the DHCP pool, which includes the necessary parameters, such as the default router and DNS server. This is an example DHCP scope:

```
ip dhcp pool <pool name>
network <ip network> <netmask>
default-router <default-router IP address>
dns-server <dns server IP address>
```

3. Add the Option 60 line with this syntax:

```
option 60 ascii "BlueSecure.AP1500"
```

4. Add the Option 43 line with this syntax:

```
option 43 hex 7f1c3139322e3136382e3133302e312c463139322e3136382e3133302e32
```

The hexadecimal string in step 4 is assembled as a sequence of Code/Length/Value converted to hex.

- **Code:** 127 (in decimal). Convert to hex for Cisco IOS DHCP Server.
- **Length**: A count of the characters of the ASCII string in the Value field. (in decimal). Convert to hex for Cisco IOS DHCP Server.
- **Value:** ASCII string that is a comma-separated list of Primary vWLAN Appliance IP address followed by Secondary vWLAN IP address. Secondary vWLAN IP address should start with F denoting failover. No spaces should be embedded in the list. Convert to hex for Cisco IOS DHCP

See **Vendor Specific Information**, **Example DHCP Option 43 Code/Length/Value**, and **Converting Values to Hex** sections above. For the given example above of a Primary vWLAN Appliance IP address of 192.168.130.1 and a Secondary vWLAN Appliance IP address of 192.168.130.2, the Cisco IOS command that is added is shown in step 4.

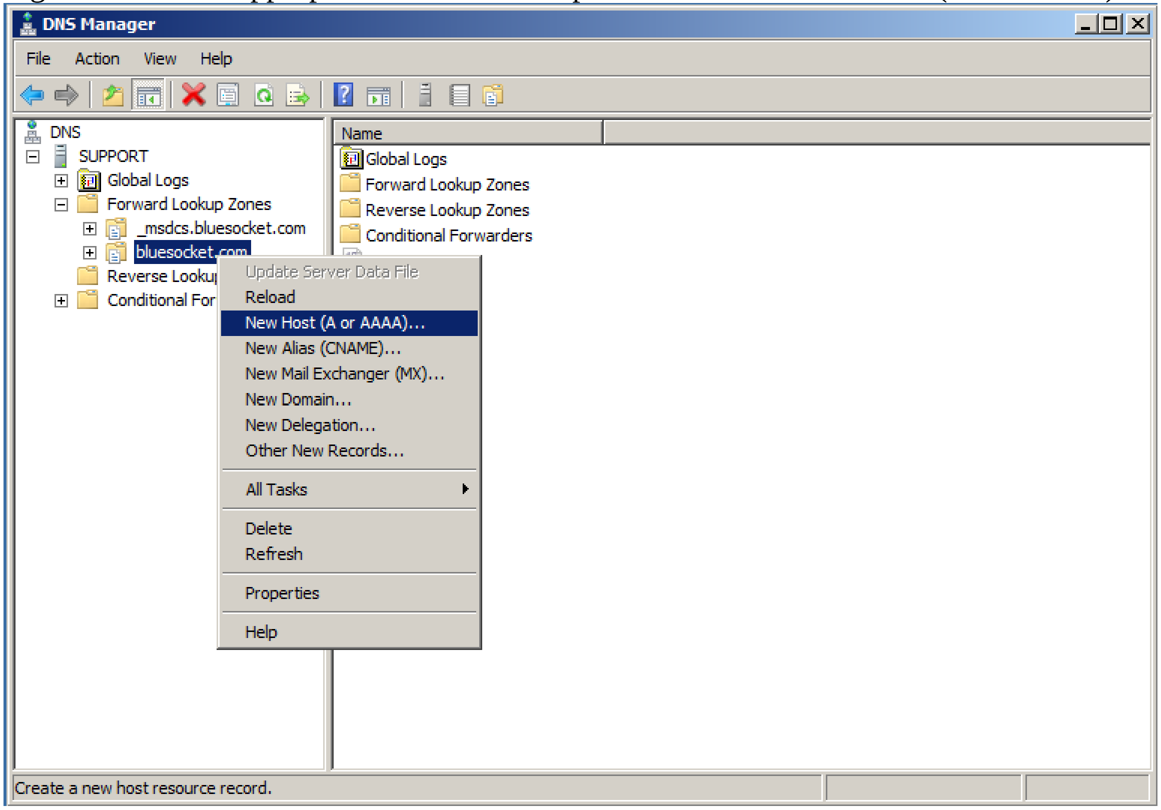
Configuring an Entry for apdiscovery in Your Organizations DNS Server

You can configure a host (A) record in your organizations DNS Server with a Name of apdiscovery and the IP address of the Primary vWLAN Appliance to facilitate AP discovery. When High Availability is enabled the Secondary vWLAN Appliance IP address will be automatically configured however it is best practice to also configure a host (A) record with the IP address of the Secondary vWLAN appliance in case the BSAP is unable to obtain a configuration from the Primary vWLAN Appliance. An associated PTR record is not required for AP discovery.

Microsoft Windows Server 2008 R2 DNS Server

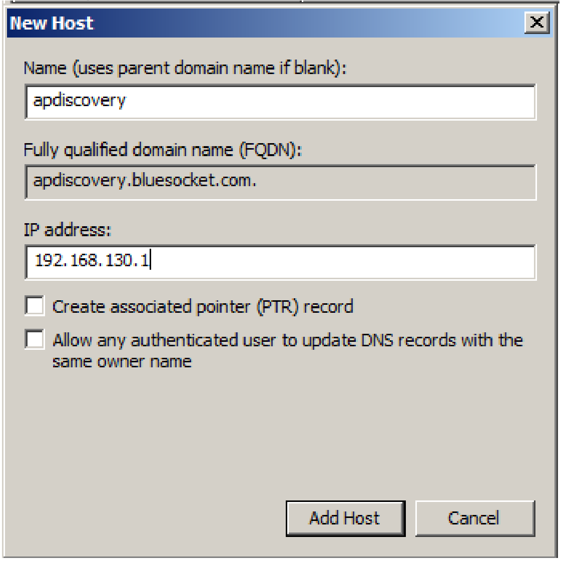
Follow these steps in order to configure a DNS entry for AP discovery on the Microsoft Windows Server 2008 R2 Enterprise DNS Server:

1. Got to Start>Administrative Tools>DNS.
2. Right click on the appropriate forward lookup zone and select New Host (A or AAAA).



Create a new host resource record.

3. Populate the Name field with apdiscovery. Populate the IP Address field with the IP address of the Primary vWLAN Appliance.



Name (uses parent domain name if blank):
apdiscovery

Fully qualified domain name (FQDN):
apdiscovery.bluesocket.com.

IP address:
192.168.130.1

☐ Create associated pointer (PTR) record

☐ Allow any authenticated user to update DNS records with the same owner name

4. Repeat this process for the Secondary vWLAN Appliance IP address.

Caching a Previously Discovered vWLAN Appliance

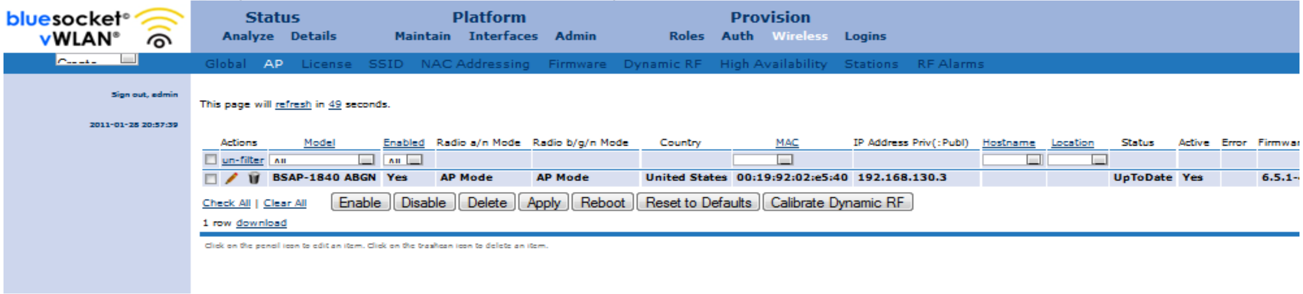
The BSAP will remember or cache the vWLAN Appliance IP Address from the last successful discovery. You could potentially stage the BSAP in a staging facility using DHCP Option 43 or DNS and then move the BSAP into production however it is recommended that one of the above methods for AP discovery be permanently configured in production. If the BSAP were to be reset to factory defaults, it would no longer remember the last discovered address. Without one of the above methods configured, the BSAP would not be able to discover the vWLAN Appliance.

Verify

You can verify the BSAP has successfully discovered the vWLAN Appliance via the vWLAN Appliance's secure web based administrative console or via the CLI of the BSAP.

To verify the BSAP has successfully discovered the vWLAN Appliance via the vWLAN Appliance's secure web based administrative console follow these steps:

1. Go to Provision>Wireless>AP. The BSAP will automatically be displayed under Wireless>AP when it successfully discovers the vWLAN Appliance. The BSAP will be displayed in bold print and the Active column will display Yes if the BSAP is currently active.



2011-01-28 20:57:39

This page will refresh in 49 seconds.

	Actions	Model	Enabled	Radio a/n Mode	Radio b/g/n Mode	Country	MAC	IP Address Priv(:Publ)	Hostname	Location	Status	Active	Error	Firmwar
☐	un-filter	All	All											
☐		BSAP-1840 ABGN	Yes	AP Mode	AP Mode	United States	00:19:92:02:e5:40	192.168.130.3			UpToDate	Yes		6.5.1-

Check All | Clear All Enable Disable Delete Apply Reboot Reset to Defaults Calibrate Dynamic RF

1 row download

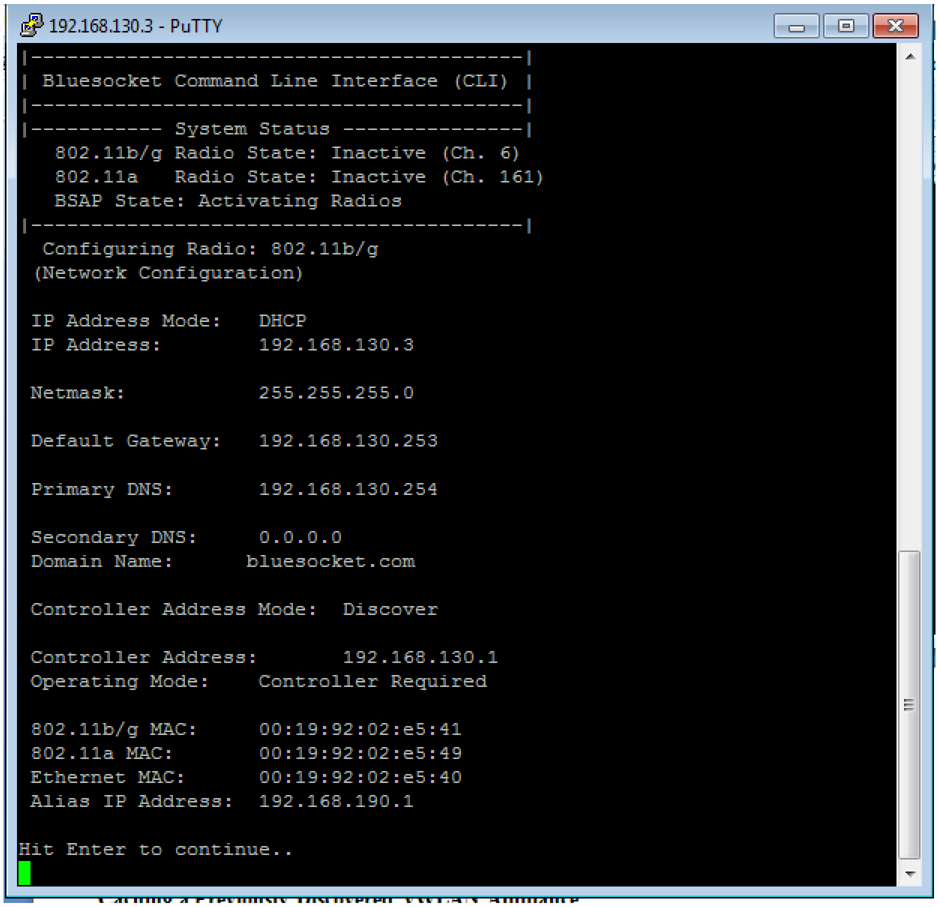
Click on the pencil icon to edit an item. Click on the trashcan icon to delete an item.

To verify the BSAP has successfully discovered the vWLAN Appliance via the CLI of the BSAP follow these steps:

1. Connect to the console port of the BSAP using a DB9 female to RJ45 rollover cable and a terminal emulation program (115200, 8, none, 1, none).

   Or.

2. SSH to the BSAP using port 2335. Obtain the BSAP's IP address from the DHCP server and SSH to the BSAP over the network. The BSAP-1800v1 does not have a console port so you will be required to SSH to the BSAP-1800v1.
3. Log into the BSAP. The default username/password is adm1n/blue1socket. The password is configurable in the secure web based administrative console of the vWLAN Appliance under Provision>Wireless>global however if the BSAP has not yet discovered the vWLAN Appliance and automatically downloaded a configuration it will still be configured with the default password.
4. Select option 1 for Network Configuration from the Main Menu.
5. Select option 8 for Network Summary from the Network Configuration Menu.
6. Verify the vWLAN Appliance IP Address is populated under Controller Address. The CLI will only display one IP address, the vWLAN Appliance the BSAP is currently connected to.



```
|----------------------------------------|
| Bluesocket Command Line Interface (CLI) |
|----------------------------------------|
|----------- System Status ---------------|
   802.11b/g Radio State: Inactive (Ch. 6)
   802.11a   Radio State: Inactive (Ch. 161)
   BSAP State: Activating Radios
|----------------------------------------|
  Configuring Radio: 802.11b/g
 (Network Configuration)

 IP Address Mode:   DHCP
 IP Address:        192.168.130.3

 Netmask:           255.255.255.0

 Default Gateway:   192.168.130.253

 Primary DNS:       192.168.130.254

 Secondary DNS:     0.0.0.0
 Domain Name:      bluesocket.com

 Controller Address Mode:  Discover

 Controller Address:       192.168.130.1
 Operating Mode:    Controller Required

 802.11b/g MAC:     00:19:92:02:e5:41
 802.11a MAC:       00:19:92:02:e5:49
 Ethernet MAC:      00:19:92:02:e5:40
 Alias IP Address:  192.168.190.1

Hit Enter to continue..
```

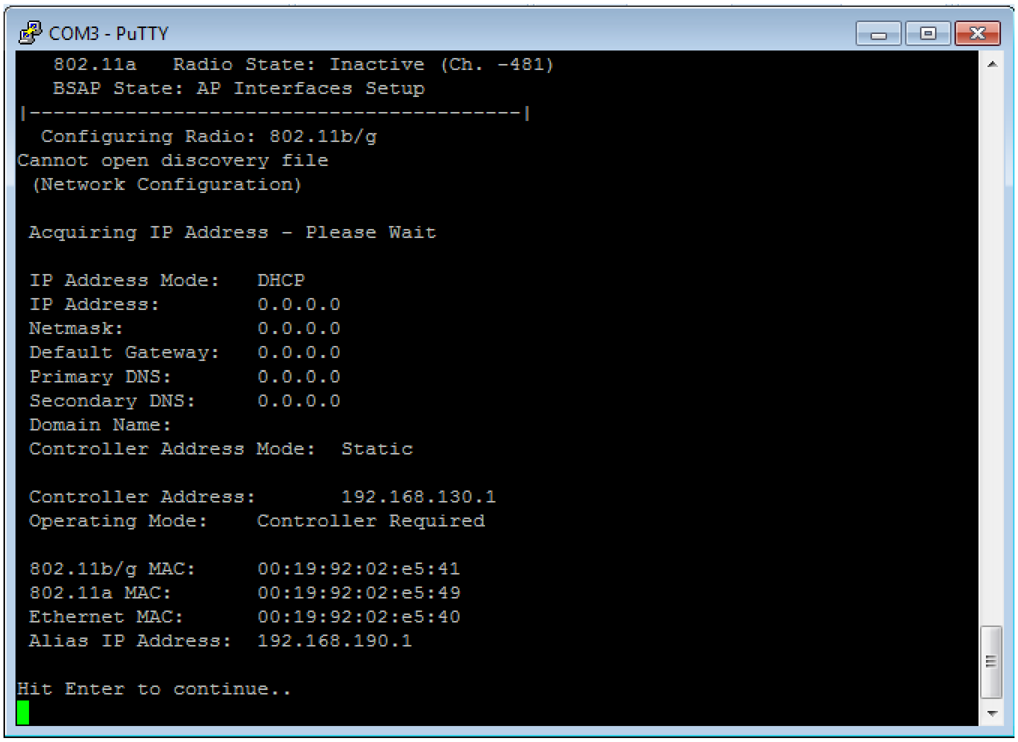
Troubleshooting

Required TCP/UDP Ports

Make sure you are allowing the appropriate TCP/UDP ports in any firewall or ACL between the BSAP and vWLAN appliance. You could log dropped packets in the firewall or ACL to see if one of the appropriate TCP/UDP ports is not being allowed. If the BSAP is unable to establish a control channel (TCP port 33333) to the vWLAN Appliance it will automatically reboot every 3 minutes until a control channel is established. A traffic capture could be performed on the network interface of the vWLAN Appliance to see what traffic on what TCP/UDP ports is being received from the BSAP. To start the traffic capture in the secure web based administration console of the vWLAN Appliance go to Status>Details>Diagnostics>Traffic Capture. You can use Wireshark (wireshark.org) to open and analyze the traffic capture file.

Static AP Discovery

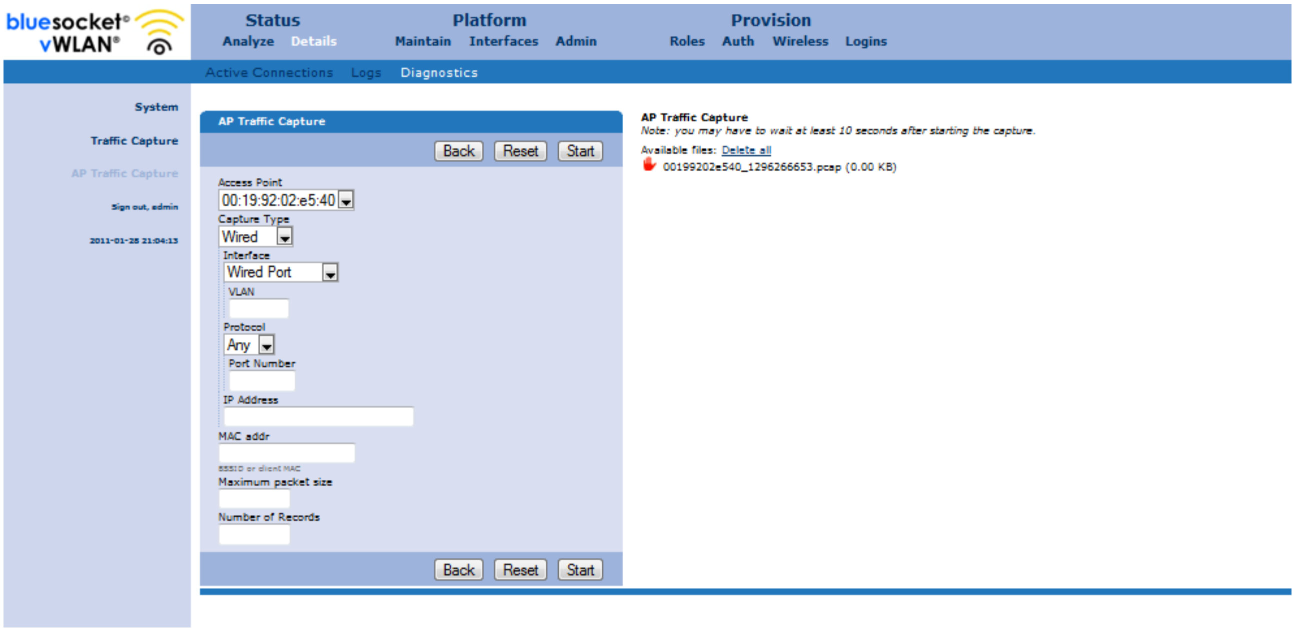
Log into the BSAP via the CLI to verify it has been configured appropriately for static discovery. Follow steps 12-15 of the **Statically Configuring the BSAP via the CLI** section above. The controller Address Mode should be set to static and the Controller Address should be populated with the appropriate vWLAN Appliance IP address.



```
   802.11a   Radio State: Inactive (Ch. -481)
   BSAP State: AP Interfaces Setup
|-----------------------------------------|
  Configuring Radio: 802.11b/g
Cannot open discovery file
 (Network Configuration)

 Acquiring IP Address - Please Wait

 IP Address Mode:    DHCP
 IP Address:         0.0.0.0
 Netmask:            0.0.0.0
 Default Gateway:    0.0.0.0
 Primary DNS:        0.0.0.0
 Secondary DNS:      0.0.0.0
 Domain Name:
 Controller Address Mode:  Static

 Controller Address:       192.168.130.1
 Operating Mode:     Controller Required

 802.11b/g MAC:      00:19:92:02:e5:41
 802.11a MAC:        00:19:92:02:e5:49
 Ethernet MAC:       00:19:92:02:e5:40
 Alias IP Address:   192.168.190.1

Hit Enter to continue..
```

DHCP Option 43 AP Discovery

To troubleshoot DHCP Option 43 a traffic capture could be performed on the network interface of the vWLAN Appliance if it is in the same subnet of the BSAP. If the BSAP is not in the same subnet of the vWLAN Appliance a traffic capture could be performed on the wired interface of another BSAP that is in the same subnet of the problem BSAP. Start the capture and reboot the problem BSAP to capture the broadcast DHCP traffic while the BSAP attempts to obtain an IP Address during boot up. To start the traffic capture in the secure web based administration console of the vWLAN Appliance go to Status>Details>Diagnostics>Traffic Capture or AP Traffic capture. Below is an example of a traffic capture started on the wired interface of a BSAP that is in the same subnet of the problem BSAP. It will be required to configure the BSAP in the same subnet of the problem BSAP for static discovery so that it can discover the vWLAN Appliance and you can use it to perform a traffic capture. You can use Wireshark (wireshark.org) to open and analyze the traffic capture file. Alternative to performing a traffic capture in the secure web based administration console of the vWLAN Appliance you could mirror the switchport where the BSAP is plugged into and perform a traffic capture there, run a traffic on a wired client in the same subnet, run a traffic capture on the gateway, or perhaps run a traffic capture on the DHCP server.



AP Traffic Capture

Access Point: 00:19:92:02:e5:40

Capture Type: Wired

Interface: Wired Port

VLAN:

Protocol: Any

Port Number:

IP Address:

MAC addr:

BSSID or client MAC

Maximum packet size:

Number of Records:

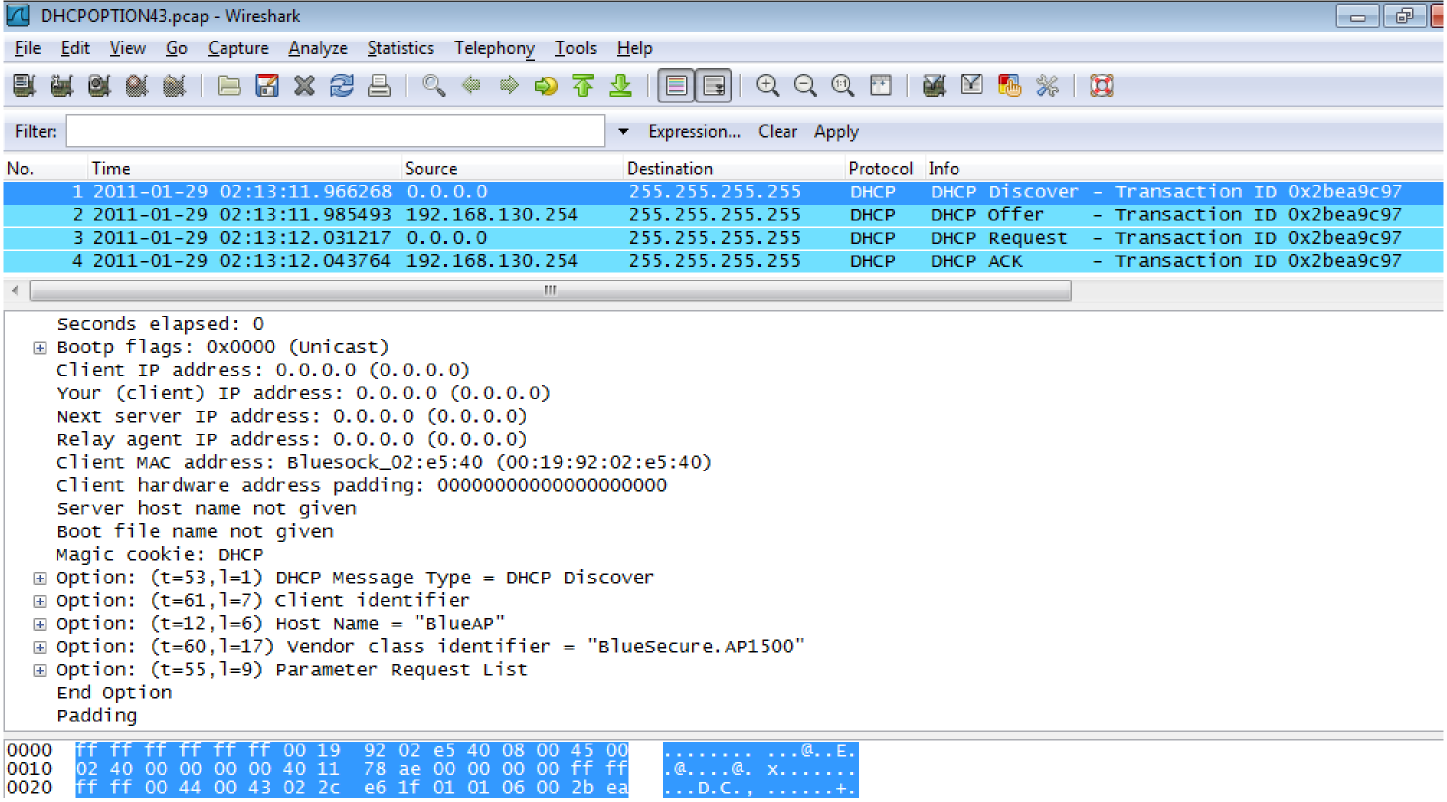
AP Traffic Capture

Note: you may have to wait at least 10 seconds after starting the capture.

Available files: Delete all

00199202e540_1296266653.pcap (0.00 KB)

Analyze the DHCP Discover to make sure Option 60 from the BSAP includes the appropriate VCI (BlueSecure.AP1500):


DHCPOPTION43.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

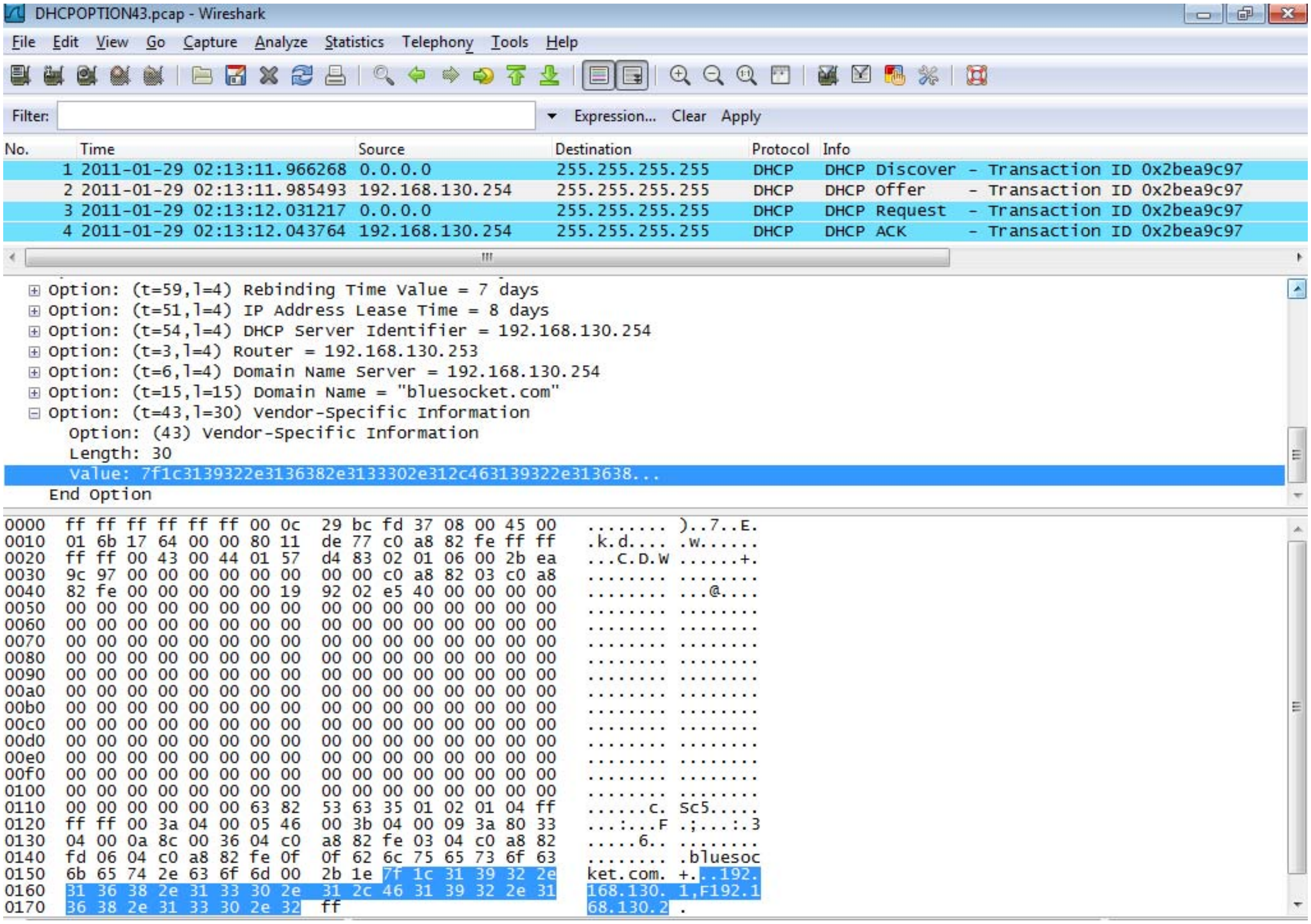
```
No.   Time                        Source           Destination      Protocol Info
    1 2011-01-29 02:13:11.966268 0.0.0.0          255.255.255.255  DHCP     DHCP Discover - Transaction ID 0x2bea9c97
    2 2011-01-29 02:13:11.985493 192.168.130.254  255.255.255.255  DHCP     DHCP Offer    - Transaction ID 0x2bea9c97
    3 2011-01-29 02:13:12.031217 0.0.0.0          255.255.255.255  DHCP     DHCP Request  - Transaction ID 0x2bea9c97
    4 2011-01-29 02:13:12.043764 192.168.130.254  255.255.255.255  DHCP     DHCP ACK      - Transaction ID 0x2bea9c97
```

```
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Bluesock_02:e5:40 (00:19:92:02:e5:40)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
  ⊞ Option: (t=61,l=7) Client identifier
  ⊞ Option: (t=12,l=6) Host Name = "BlueAP"
  ⊞ Option: (t=60,l=17) Vendor class identifier = "BlueSecure.AP1500"
  ⊞ Option: (t=55,l=9) Parameter Request List
    End Option
    Padding
```

```
0000  ff ff ff ff ff ff 00 19  92 02 e5 40 08 00 45 00   ........ ...@..E.
0010  02 40 00 00 00 00 40 11  78 ae 00 00 00 00 ff ff   .@....@. x.......
0020  ff ff 00 44 00 43 02 2c  e6 1f 01 01 06 00 2b ea   ...D.C., ......+.
```

Analyze the DHCP Offer from the DHCP Server to make sure Option 43 includes the appropriate Code/Length/Value. Refer to the **Converting Values to Hex** section above as the Code/Length/Value will be converted to Hex in the traffic capture.

- **Code:** 127 (in decimal). Converted to hex in the traffic capture.
- **Length**: A count of the characters of the ASCII string in the Value field (in decimal). Converted to hex in the traffic capture.
- **Value:** ASCII string that is a comma-separated list of Primary vWLAN Appliance IP address followed by Secondary vWLAN IP address. Secondary vWLAN IP address should start with F denoting failover. No spaces should be embedded in the list. Converted to hex in the traffic capture.


DHCPOPTION43.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No.   Time                        Source            Destination       Protocol  Info
    1 2011-01-29 02:13:11.966268  0.0.0.0           255.255.255.255   DHCP      DHCP Discover  - Transaction ID 0x2bea9c97
    2 2011-01-29 02:13:11.985493  192.168.130.254   255.255.255.255   DHCP      DHCP Offer     - Transaction ID 0x2bea9c97
    3 2011-01-29 02:13:12.031217  0.0.0.0           255.255.255.255   DHCP      DHCP Request   - Transaction ID 0x2bea9c97
    4 2011-01-29 02:13:12.043764  192.168.130.254   255.255.255.255   DHCP      DHCP ACK       - Transaction ID 0x2bea9c97
```

```
⊞ Option: (t=59,l=4) Rebinding Time Value = 7 days
⊞ Option: (t=51,l=4) IP Address Lease Time = 8 days
⊞ Option: (t=54,l=4) DHCP Server Identifier = 192.168.130.254
⊞ Option: (t=3,l=4) Router = 192.168.130.253
⊞ Option: (t=6,l=4) Domain Name Server = 192.168.130.254
⊞ Option: (t=15,l=15) Domain Name = "bluesocket.com"
⊟ Option: (t=43,l=30) Vendor-Specific Information
    Option: (43) Vendor-Specific Information
    Length: 30
    Value: 7f1c3139322e3136382e3133302e312c463139322e313638...
  End Option
```

```
0000  ff ff ff ff ff ff 00 0c  29 bc fd 37 08 00 45 00   ........ )..7..E.
0010  01 6b 17 64 00 00 80 11  de 77 c0 a8 82 fe ff ff   .k.d.... .w......
0020  ff ff 00 43 00 44 01 57  d4 83 02 01 06 00 2b ea   ...C.D.W ......+.
0030  9c 97 00 00 00 00 00 00  00 00 c0 a8 82 03 c0 a8   ........ ........
0040  82 fe 00 00 00 00 00 19  92 02 e5 40 00 00 00 00   ........ ...@....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 63 82  53 63 35 01 02 01 04 ff   ......c. Sc5.....
0120  ff ff 00 3a 04 00 05 46  00 3b 04 00 09 3a 80 33   ...:...F .;...:.3
0130  04 00 0a 8c 00 36 04 c0  a8 82 fe 03 04 c0 a8 82   .....6.. ........
0140  fd 06 04 c0 a8 82 fe 0f  0f 62 6c 75 65 73 6f 63   ........ .bluesoc
0150  6b 65 74 2e 63 6f 6d 00  2b 1e 7f 1c 31 39 32 2e   ket.com. +...192.
0160  31 36 38 2e 31 33 30 2e  31 2c 46 31 39 32 2e 31   168.130. 1,F192.1
0170  36 38 2e 31 33 30 2e 32  ff                        68.130.2 .
```

DNS AP Discovery

To troubleshot DNS AP discovery a traffic capture could also be performed, however because DNS is not broadcast traffic you would not be able perform a traffic capture on the vWLAN Appliance or another BSAP in the same subnet. You could mirror the switchport where the BSAP is plugged into and perform a traffic capture there, run a traffic capture on the gateway, or perhaps run a traffic capture on the DNS Server. You could then analyze the traffic capture to make sure the BSAP sends a DNS request for apdiscovery and to make sure the DNS Server replies with the IP Address of the vWLAN Appliance.

You could also perform an nslookup for apdiscovery from a command prompt of a wired client in the same subnet as the BSAP to make sure the IP address of the vWLAN Appliance is returned. Assuming the BSAP is configured to use the same DNS servers as the wired client. For example:

```
C:\>nslookup  apdiscovery
```

You should be returned the IP address of the vWLAN Appliance.