



Configuration Guide

vWLAN AP Discovery

This configuration guide provides an in-depth look at access point (AP) discovery in ADTRAN Bluesocket virtual wireless local area network (vWLAN) products. Included in this guide are an overview of AP discovery, configuration of AP discovery methods, and general troubleshooting information.

This guide consists of the following sections:

- *AP Discovery Overview on page 2*
- *Hardware and Software Requirements and Limitations on page 2*
- *AP Discovery Method Configuration on page 5*
- *Verifying BSAP Discovery on page 19*
- *Troubleshooting on page 20*

AP Discovery Overview

The cloud-based approach of the ADTRAN Bluesocket vWLAN distributed architecture allows vWLAN components (primary and secondary vWLAN appliances and Bluesocket APs) to be deployed anywhere. This type of flexibility supports several different deployment scenarios:

- Primary and secondary vWLAN systems deployed centrally at corporate headquarters or data centers in a private-cloud network,
- Secondary vWLAN systems deployed at remote disaster recovery sites or data centers,
- Both vWLAN systems deployed in a hosted public-cloud model,
- The primary system deployed at a corporate headquarters while the secondary system is deployed in a hosted model,
- Or a mixture of deployments.

Bluesocket APs (BSAPs) can be deployed locally to the vWLAN system or at remote sites, or behind network address translation (NAT) devices such as routers or firewalls.

Whatever deployment scenario is used, the BSAPs must be configured with a method to discover the primary and secondary vWLAN. AP discovery is based on an algorithm that attempts various discovery methods in a specific order. Discovery methods, in order of precedence, include: statically configuring the BSAP using the command line interface (CLI), configuring Dynamic Host Control Protocol (DHCP) Option 43 in your organization's DHCP server, your organization's domain naming system (DNS) server, or caching a previously discovered vWLAN system. If one discovery method fails, then the next method is attempted (unless the BSAP is statically configured).

This document describes the AP discovery methods, ports and protocols, and sample AP discovery configurations for AOS DHCP servers, Microsoft Windows Server 2008 R2 Enterprise DHCP and DNS servers, Internet Systems Consortium (ISC) DHCP servers, and Cisco Internetwork Operating System (IOS) DHCP servers.

Hardware and Software Requirements and Limitations

This document describes AP discovery configurations for vWLAN hardware and virtual appliances (VMware) and BSAPs running vWLAN software versions 2.2.1 and later.

The following requirements must be met before attempting to configure AP discovery:

- General knowledge of ADTRAN Bluesocket vWLAN and BSAPs
- General knowledge of AOS (if applicable)
- General knowledge of Microsoft Windows Server 2008 R2 Enterprise DHCP and DNS servers (if applicable)
- General knowledge of ISC DHCP servers (if applicable)
- General knowledge of Cisco IOS DHCP servers (if applicable)
- General knowledge of DHCP

Components Used in AP Discovery Configurations

The information in this document was created in a specific lab environment. All of the devices used had a default configuration. The configurations presented in this guide have been tested and found to function as expected. The following components were used in testing:

- vWLAN appliance (hardware) and virtual appliance (VMware) running vWLAN software 2.2.1 and later
- BSAPs 1800 and 1900 Series
- AOS DHCP server
- Microsoft Windows Server 2008 R2 Enterprise DHCP and DNS server
- ISC DHCP server
- Cisco IOS DHCP server



If your network is active, make sure you understand the potential impact of any command issued on these devices. If you experience difficulty configuring the Microsoft Windows Server R2 Enterprise DHCP and DNS server, ISC DHCP server, or Cisco IOS DHCP server, contact Microsoft, ISC, or Cisco respectively for assistance. ADTRAN does not provide support for Microsoft Server R2 Enterprise, ISC DHCP servers, or Cisco IOS.

Required Ports and Protocols

The following ports and protocols are required to be open as necessary between the vWLAN and BSAPs, between primary and secondary vWLAN systems when using high availability, between the vWLAN and authentication servers when using various methods of authentication, between BSAPs when using Layer 3 mobility (tunneling), and between BSAPs and authentication when using external Remote Authentication Dial-In User Service (RADIUS) 802.1x authentication. Ensure that any firewalls or access control lists (ACLs) allow the ports and protocols outlined in [Table 1](#) as applicable.



The ports and protocols described in [Table 1](#) are a comprehensive list of ports and protocols that must be open as necessary. These ports and protocols are not limited to AP discovery.

Table 1. Required Ports and Protocols

Port Type and Number	Port Protocol	Purpose
User Datagram Protocol (UDP) port 53	DNS	AP discovery communication between vWLAN and BSAPs (1800 Series BSAPs only).
Transmission Control Protocol (TCP) port 33333	Transport Layer Security (TLS)	Secure control/management channel between vWLAN and BSAPs.
UDP port 69	Trivial File Transfer Protocol (TFTP)	Used on the BSAP 1800 Series to transfer firmware between vWLAN and the BSAP or between BSAPs and a third-party TFTP server. Also used for AP traffic capture file transfer between vWLAN and the BSAP.

Table 1. Required Ports and Protocols (Continued)

Port Type and Number	Port Protocol	Purpose
TCP port 33334	Secure Copy Protocol (SCP)	Used on the BSAP 1900 Series to transfer firmware between vWLAN and the BSAP or between BSAPs and a third-party SCP server. Also used for AP traffic capture file transfer between vWLAN and the BSAP.
TCP port 28000	Transport Layer Security (TLS)	Used to secure wireless Internet distribution systems (IDS) channels between vWLAN and BSAPs.
TCP port 2335	TLS	Used for communication between primary and secondary vWLAN systems for high availability.
TCP port 3000	Hypertext Transfer Protocol Secure (HTTPS)	Used for communication between primary and secondary vWLAN systems for high availability and access to the vWLAN web-based graphical user interface (GUI).
TCP port 80	Hypertext Transfer Protocol (HTTP)	Required for captive portals between vWLAN and the BSAPs in vWLAN releases prior to 2.2.1.
TCP port 443	HTTPS	Required for captive portals between vWLAN and the BSAPs.
UDP port 1812 or 1645	RADIUS	Required for RADIUS web-based authentication and RADIUS administrative authentication between the BSAP and the authentication server. Also required for RADIUS external 802.1x authentication between the BSAP and the authentication server.
UDP port 1813 or 1646	RADIUS	Required when using RADIUS accounting between vWLAN and an accounting server.
TCP port 389	Lightweight Directory Access Protocol (LDAP)	Required for LDAP or Microsoft Active Directory (AD) authentication between vWLAN and an authentication server.
UDP port 636	LDAP over Secure Socket Layer (SSL)	Required for LDAP or AD authentication between vWLAN and an authentication server.
TCP port 6001	Standard Interchange Protocol (SIP2)	Required for SIP2 authentication between vWLAN and the library authentication server.
	IP protocol 97	Required for Layer 3 roaming between BSAPs.

In vWLAN firmware versions previous to 2.6, APs were required to use DNS to communicate with vWLAN and determine if the vWLAN was active. In vWLAN release 2.6, this requirement has been removed so that the AP discovery process is not interrupted when APs are not configured for outbound DNS access because of firewall policies. DNS is still required, however, for BSAP 1800 Series upgrades.

AP Discovery Method Configuration

The following sections describe how to configure the four types of AP discovery methods. These methods are:

- *Statically Configuring BSAPs Using the CLI on page 5*
- *Configuring DHCP Option 43 in Your Organization's DHCP Server on page 8*
- *Configuring an Entry for AP Discovery in Your Organization's DNS Server on page 17*
- *Caching a Previously Discovered vWLAN IP Address for AP Discovery on page 18*



*If a vWLAN is not discovered, the AP attempts to connect to a server at the following IP address: **76.164.174.46**. This server is for future use. If you are attempting to connect to a different vWLAN, refer to [Troubleshooting on page 20](#) to determine why the AP did not connect.*

Statically Configuring BSAPs Using the CLI

You can configure each BSAP for static discovery mode and populate the vWLAN public network interface IP address using the CLI (console port or secure shell (SSH)). It is only necessary to populate the primary vWLAN public network interface IP address. If high availability is enabled, the secondary vWLAN public network interface IP address is automatically configured.



Configuring BSAPs using the CLI is not recommended for large scale deployments because each BSAP must be configured individually.

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

1. Connect to the console port of the BSAP. You can use a DB-9 female to RJ-45 rollover cable and open a VT100 terminal session with the following settings: **115200** baud, **8** data bits, no parity, and **1** stop bit (no flow control).

Alternatively, you can connect to the BSAP using SSH on port 2335. The default management IP address of the BSAP is **192.168.190.1**. Connect your computer directly to the network port of the BSAP and then configure the computer with an IP address in the same subnet (for example, **192.168.190.2**). You can also 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. BSAPs 1800v1, 1920, 1925, and 1940 do not have console ports so SSH is required.

- Once connected to the BSAP, you must log in to access the CLI. Enter the default user name of **admin** and the default password of **blue1socket**.



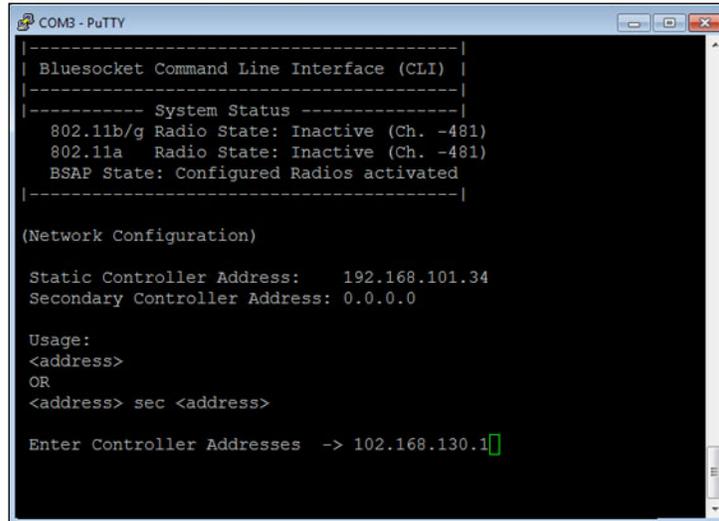
Passwords are configurable on a per-AP template basis using the GUI. Refer to the [vWLAN Administrator Guide](https://supportforums.adtran.com) (available online at <https://supportforums.adtran.com>) for more information. If the BSAP has not yet discovered the vWLAN and automatically downloaded a configuration, use the default password.

- In the BSAP CLI, select option **1** in the **Main Menu** for network configuration.
- In the **Network Configuration** menu, select option **5** to set the controller mode.
- At the prompt, enter **1** to configure a static controller. After entering this value you will be returned to the main menu.

```
COM3 - PuTTY
-----|
| 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 |
```

- In the main menu, select option **6** to set the controller address.
- Enter the primary vWLAN public network interface IP address at the prompt. It is only necessary to specify the primary vWLAN system public network interface IP address. If high availability is enabled,

the secondary vWLAN system's public network interface IP address is automatically configured. After entering this value you will return to the **Network Configuration** menu.



```

COM3 - PuTTY
|-----|
| Bluesocket Command Line Interface (CLI) |
|-----|
|----- System Status -----|
| 802.11b/g Radio State: Inactive (Ch. -481)|
| 802.11a Radio State: Inactive (Ch. -481)|
| BSAP State: Configured Radios activated |
|-----|

(Network Configuration)

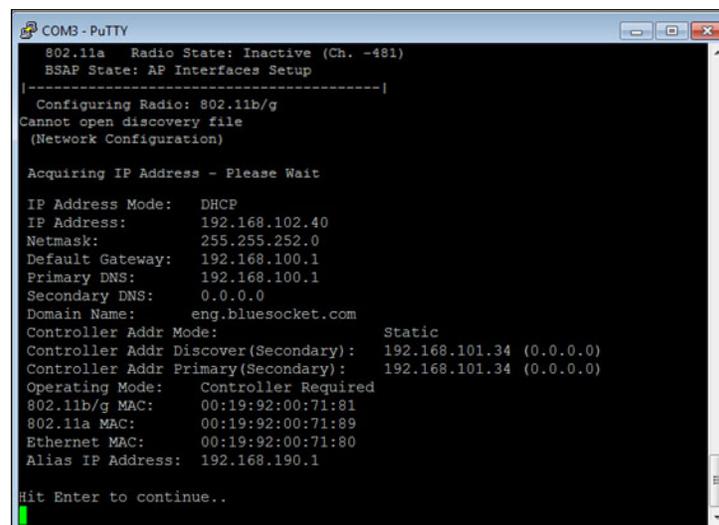
Static Controller Address: 192.168.101.34
Secondary Controller Address: 0.0.0.0

Usage:
<address>
OR
<address> sec <address>

Enter Controller Addresses -> 102.168.130.1

```

8. In the **Network Configuration** menu, select option **P** to return to the previous menu.
9. In the main menu, select option **2** to save and apply the configuration.
10. You will be prompted to save and reboot. Enter **y** for yes.
11. To verify the configuration, log back into the BSAP.
12. In the main menu, select option **1** to enter the **Network Configuration** menu.
13. In the **Network Configuration** menu, select option **8** to view the network summary.
14. Verify that the **Controller Address Mode** is set to **Static** and the **Controller Address** is the appropriate public network interface IP address for the primary vWLAN system.



```

COM3 - PuTTY
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: 192.168.102.40
Netmask: 255.255.252.0
Default Gateway: 192.168.100.1
Primary DNS: 192.168.100.1
Secondary DNS: 0.0.0.0
Domain Name: eng.bluesocket.com
Controller Addr Mode: Static
Controller Addr Discover(Secondary): 192.168.101.34 (0.0.0.0)
Controller Addr Primary(Secondary): 192.168.101.34 (0.0.0.0)
Operating Mode: Controller Required
802.11b/g MAC: 00:19:92:00:71:81
802.11a MAC: 00:19:92:00:71:89
Ethernet MAC: 00:19:92:00:71:80
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 discovery message 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. The VCI used by all BSAPs regardless of model is **BlueSecure.AP1500**.

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 discovery message 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 pool that offers IP addresses to the BSAPs.

RFC 2132 states 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, and value within Option 43. The definition of encapsulated vendor-specific options is specific to the vendor.

When DHCP servers are programmed to offer vWLAN public network interface IP addresses as Option 43 for BSAPs, the encapsulated vendor-specific options are defined in the following manner:

Code: 127 (in decimal format)

Length: A count of the characters of the ASCII string in the **Value** field (in decimal format)

Value: ASCII string that is a comma separated list of primary vWLAN public network interface IP addresses followed by secondary vWLAN public network interface IP addresses. Secondary vWLAN public network interface IP addresses start with **F**, denoting failover. No spaces should be embedded in the list.

Example DHCP Option 43 Code, Length, and Value

The following is sample information for the code, length, and value of DHCP Option 43:

Primary vWLAN public network interface IP address: 192.168.130.1

Secondary vWLAN public network interface IP address: 192.168.130.2

Code: 127

Length: 28

Value: 192.168.130.1,F192.168.130.2

 **NOTE**

The secondary vWLAN public network interface IP address starts with F, denoting failover. When high availability is enabled, the secondary vWLAN public network interface IP address is 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 system.

Converting DHCP Values to Hexadecimal Values

Depending on the DHCP server, it might be necessary to convert DHCP values to hexadecimal values. For example, the Microsoft DHCP server allows you to enter the code value in decimal format, and the value in ASCII characters, and the length is calculated automatically. The ISC DHCP server and the Cisco IOS server, however, require the values to be converted to hexadecimal format. In addition, values converted to hexadecimal format can be beneficial in troubleshooting.

The following is an example of DHCP code and length values from the previous example converted from decimal format to hexadecimal format:

127=7f (Code value)

28=1c (Length value)

The following is an example of DHCP values converted from ASCII to hexadecimal format using the conversions described in Table 2:

192.168.130.1 is converted as 1=31, 9=39, 2=32, .=2e, 1=31, 6=36, 8=38, .=2e, 1=31, 3=33, 0=30, .=2e, 1=31, resulting in 3139322e3136382e3136382e3133302e31.

F192.168.130.2 is converted as 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, resulting in 463139322e3136382e3133302e32.

Table 2. ASCII to Hexadecimal Conversion

ASCII Value	Hexadecimal Value
0	30
1	31
2	32
3	33
4	34
5	35
6	36
7	37
8	38
9	39
.	2e
,	2c
F	46

The DHCP Option 43 from the previous example appears as follows when converted to hexadecimal format:

7f1c3139322e3136382e3133302e312c463139322e3136382e3133302e32

In order for the BSAP to discover the vWLAN, the DHCP server must be programmed to return the primary and secondary vWLAN public network interface IP addresses based on the VCI of the BSAP. You must program the DHCP server to recognize the VCI for the BSAP and then define the vendor-specific information. The semantics of DHCP server configuration vary based on the DHCP server vendor. Steps for configuring the various DHCP servers tested for this document are outlined in the following sections:

- *AOS DHCP Option 43 Configuration on page 10*
- *Microsoft Windows Server 2008 R2 DHCP Option 43 Configuration on page 12*
- *ISC DHCP Option 43 Configuration on page 17*

- [Cisco IOS DHCP Option 43 Configuration on page 17](#)

AOS DHCP Option 43 Configuration

The AOS DHCP server can be configured using the CLI or the GUI. To configure the AOS DHCP server using the CLI, follow these steps:

1. Access the AOS server's CLI and enter the Global Configuration mode.
2. Create a DHCPv4 pool, specifying the network, DNS server, and default router. Use the commands outlined in [Table 3](#) to configure the DHCPv4 pool.

Table 3. AOS DHCPv4 Pool Configuration Commands

Prompt	Command	Description
(config)#	ip dhcp-server pool <name>	Creates a DHCPv4 server pool and enters the pool's configuration mode.
(config-dhcp)#	network <ipv4 address> <subnet mask>	Specifies the subnet number and mask for the DHCPv4 pool.
(config-dhcp)#	dns-server <ipv4 address>	Specifies the default DNS server to use for the DHCPv4 client.
(config-dhcp)#	default-router <ipv4 address>	Specifies the default primary router to use for the DHCPv4 client.

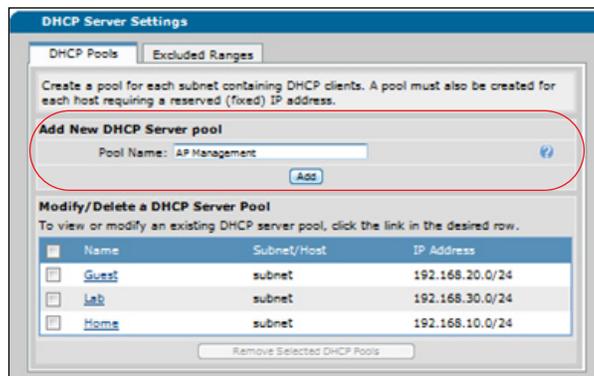
3. Add Option 43 to the DHCPv4 server pool using the **option** <number> **ascii** <string> command. Enter the command as follows:

```
(config-dhcp)#option 43 ascii 192.168.130.1,F192.168.130.2
```

4. The CLI configuration of the AOS DHCPv4 server pool is complete. Enter the **do write** command to save the configuration.

To configure the AOS DHCPv4 server pool using the AOS GUI, follow these steps:

1. Access the AOS server's GUI and navigate to **System > DHCP Server**. Select the **DHCP Pools** tab and enter the server pool's name in the **Pool Name** field. Select **Add**.



- In the **DHCP Server Pool** configuration menu, select the **Required Configuration** tab and enter the subnet address, subnet mask, and default gateway in the appropriate fields.

DHCP Server Pool "AP Management"

Required Configuration Optional Configuration Numbered Options

Create a pool for each subnet containing DHCP clients. A pool must also be created for each host requiring a reserved (fixed) IP address.

IP Addresses

Assign IP addresses to all DHCP clients on a subnet.
 Subnet Address: 192 . 168 . 130 . 0
 Subnet Mask: 255 . 255 . 255 . 0

Reserve a fixed IP address for a single host.
 MAC Address:
 IP Address:
 Subnet Mask:

DHCP Options

Default Gateway: 192 . 168 . 130 . 254
 Lease Time: 1 days 0 hours 0 min.

Cancel Apply

- Select the **Optional Configuration** tab and enter the DNS servers in the appropriate fields.

DHCP Server Pool "AP Management"

Required Configuration Optional Configuration Numbered Options

Use this tab to configure values for DHCP named options.

Domain Name:

Primary DNS: 4 . 2 . 2 . 1

Second DNS: 4 . 2 . 2 . 1

Third DNS:

Fourth DNS:

Primary WINS:

Secondary WINS:

TFTP Server:

NTP Server:

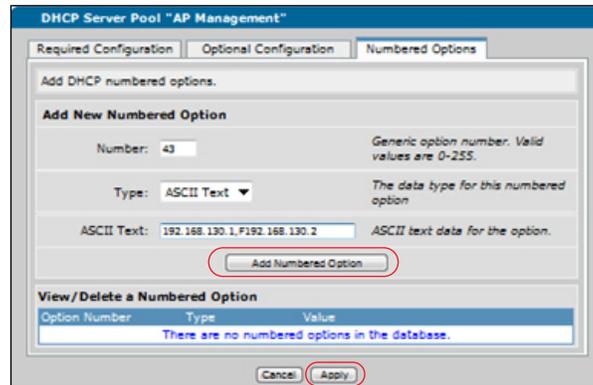
Timezone offset: 0

NAP:

Cancel Apply

- Select the **Numbered Options** tab and enter **43** in the **Number** field. Select **ASCII Text** from the **Type** drop-down menu, and enter the vWLAN public network IP addresses in the **ASCII Text** field. Each address should be separated by a comma (with no spaces between addresses), and the secondary address

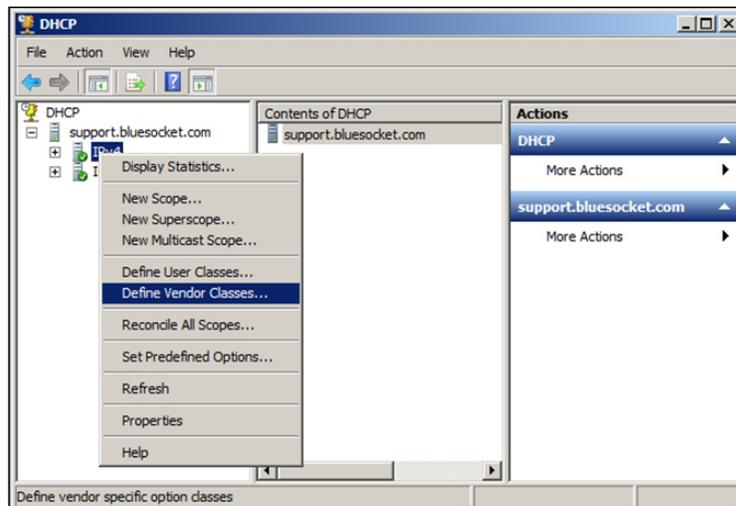
should begin with **F**. Select **Add Numbered Option** and then select **Apply**. The AOS DHCPv4 server pool configuration is complete.



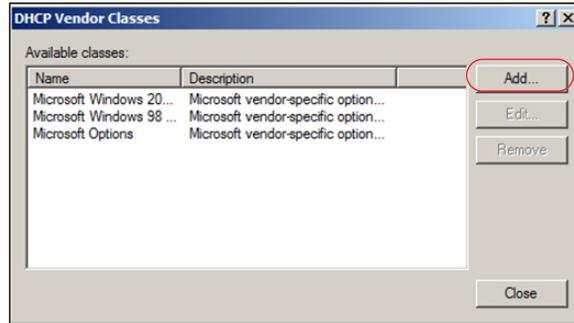
Microsoft Windows Server 2008 R2 DHCP Option 43 Configuration

Configure the DHCP Option 43 on the Microsoft Windows Server R2 Enterprise DHCP server by defining the vendor class, configuring the predefined Option 43, and configuring the option for the BSAP DHCP scope. To complete this configuration, follow these steps:

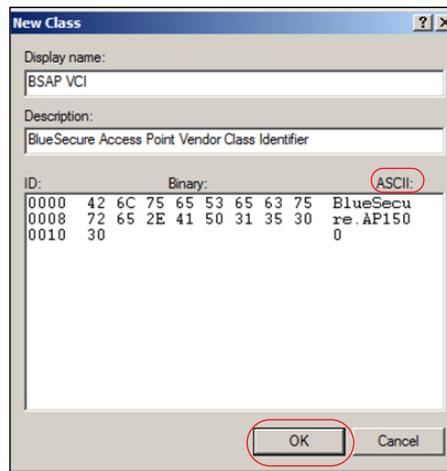
1. Access the Microsoft Windows Server 2008 R2 and navigate to **Start > Administrative Tools > DHCP**.
2. In the left pane of the **DHCP** menu, right-click **IPv4** and select **Define Vendor Classes**.



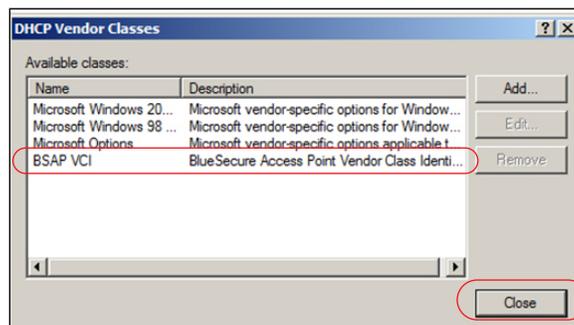
- In the **DHCP Vendor Classes** menu, select **Add**.



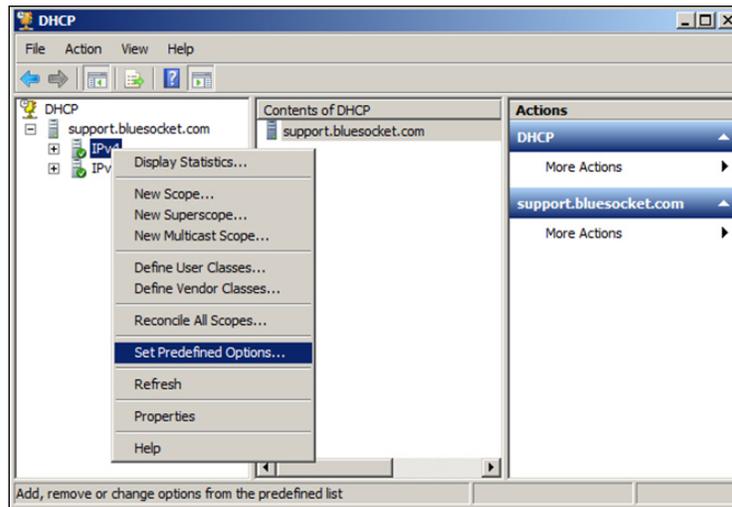
- In the **New Class** menu, enter the display name and description of the vendor class in the appropriate fields. Select the **ASCII** field, enter **BlueSecure.AP1500**, then select **OK**.



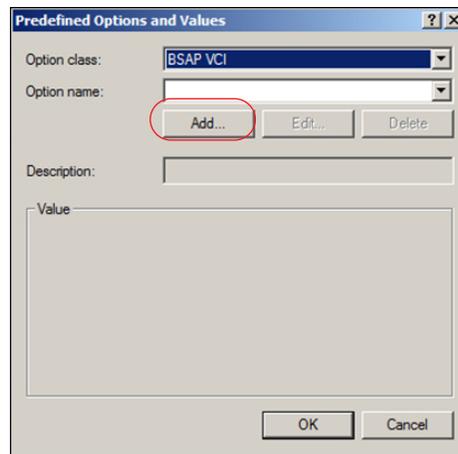
- In the **DHCP Vendor Classes** menu, verify the name and description of the newly created class. Once the class is verified, select **Close**.



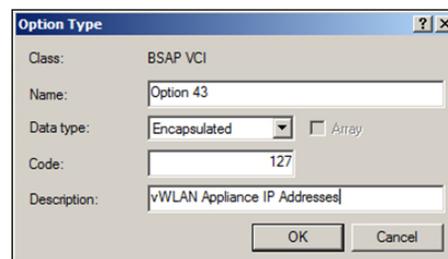
6. In the left pane of the **DHCP** menu, right-click **IPv4** and select **Set Predefined Options**.



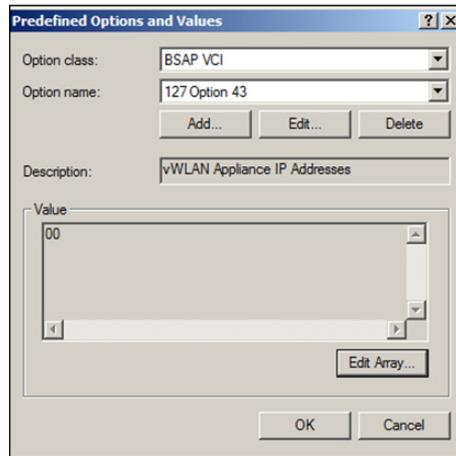
7. In the **Predefined Options and Values** menu, select the newly created option class from the **Option class** drop-down menu (created in Step 4 on [page 13](#)). Select **Add**.



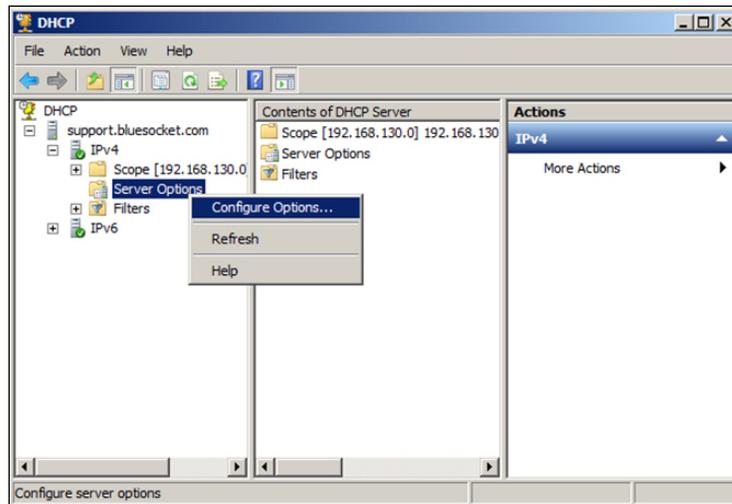
8. In the **Option Type** menu, enter the name and description of the option in the appropriate fields. Select **Encapsulated** from the **Data type** drop-down menu and enter **127** in the **Code** field. Select **OK**.



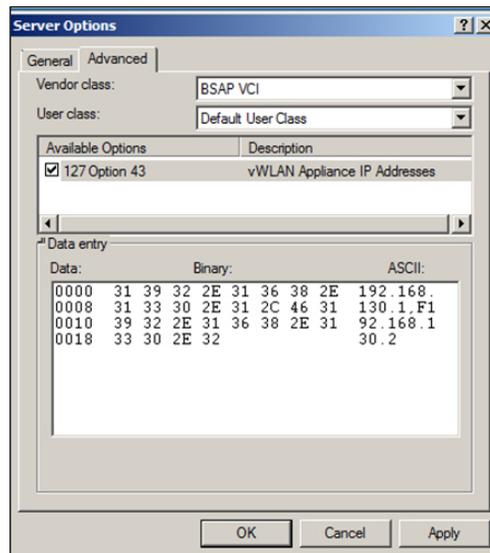
9. In the **Predefined Options and Values** menu, verify the name and description of the newly created option. Select **OK**.



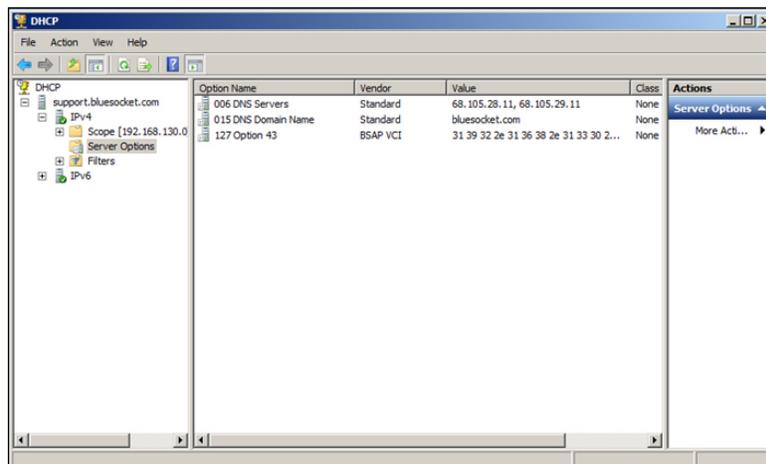
10. In the left pane of the **DHCP** menu, expand the **IPv4** menu and right-click **Server Options** under the scope that will service the BSAPs (**Scope 192.168.130.0** in the example below). Select **Configure Options**.



11. In the **Server Options** menu, select the **Advanced** tab. Select the vendor class created in Step 4 (on [page 13](#)) from the **Vendor class** drop-down menu. Select the check box next to the option created in Step 8 (on [page 14](#)) in the **Available Options** pane. Then, select **ASCII** in the **Data Entry** pane and enter the vWLAN public network interface IP addresses. The addresses should be separated by a comma (with no spaces between the addresses), and the secondary address should begin with **F**. You must delete the . that is preinserted into the field. After entering the appropriate information, select **Apply** and then select **OK**.



12. In the **DHCP** menu, navigate to **IPv4 > Scope > Server Options** and verify that the displayed option name, vendor, and value are correct. If so, configuration of the Microsoft Windows Server 2008 R2 DHCP server is complete.



ISC DHCP Option 43 Configuration

To configure the DHCP Option 43 for AP discovery in the ISC DHCP server, follow these steps:

1. Access the ISC DHCP server and add the **Option 60** VCI.
2. Add the vendor-encapsulated options (Option 43) using the following settings:
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 this step is assembled as a sequence of code/length/value settings converted to hexadecimal format and separated by colons. For information about these values and their conversion, refer to *Vendor-Specific Information on page 8*.

Cisco IOS DHCP Option 43 Configuration

To configure the DHCP Option 43 for AP discovery in the Cisco IOS DHCP server, follow these steps:

1. Access the Cisco IOS DHCP server and enter the configuration mode in the CLI.
2. Create a DHCP pool and configure the necessary parameters, including the default router and DNS server. Use the following commands:

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

3. Add Option 60 using the following command:

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

4. Add Option 43 using the following command:

```
option 43 hex 7f1c3139322e3136382e3133302e312c463139322e3136382e3133302e32
```

The hexadecimal string in this step is assembled as a sequence of code/length/value settings converted to hexadecimal format and separated by colons. For information about these values and their conversion, refer to *Vendor-Specific Information on page 8*.

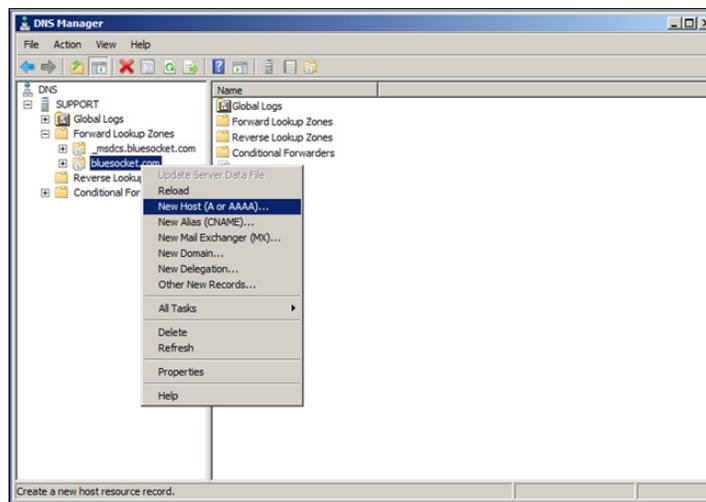
Configuring an Entry for AP Discovery in Your Organization's DNS Server

You can configure a host (A) record in your organization's DNS server to facilitate AP discovery using the name **apdiscovery** and the public network interface IP address of the primary vWLAN system. When high availability is enabled, the secondary vWLAN system IP address is automatically configured; however, it is best practice to also configure an A record with the public network interface IP address of the secondary vWLAN system in case the BSAP is unable to obtain a configuration from the primary vWLAN. An associated pointer record (PTR) is not required for AP discovery.

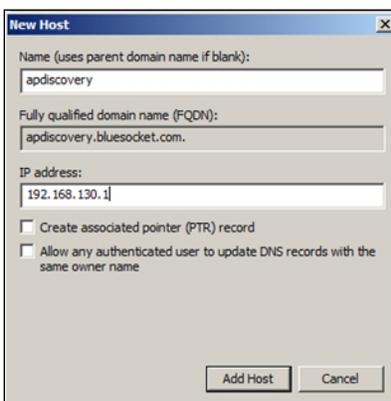
To configure the DNS entry for AP discovery on the Microsoft Windows Server 2008 R2 Enterprise DNS server, follow these steps:

1. In the Windows server, navigate to **Start > Administrative Tools > DNS**.

- In the left pane of the **DNS Manager** menu, expand the **Forward Lookup Zones** menu, and right-click the appropriate zone. Select **New Host (A or AAAA)**.



- In the **New Host** menu, specify **apdiscovery** in the **Name** field, and enter the public network interface IP address of the primary vWLAN system. Select **Add Host**.



- Repeat Steps 2 and 3 to configure the secondary vWLAN system public network interface IP address. The Windows Server 2008 R2 Enterprise is now configured with DNS entries for AP discovery.

Caching a Previously Discovered vWLAN IP Address for AP Discovery

The BSAP remembers (or caches) the vWLAN public network interface IP address from the last successful AP discovery. It is recommended that one of the previous methods for AP discovery is permanently configured in the BSAP when used in production. If the BSAP is reset to factory default settings, it will not remember the last discovered vWLAN address. Without one of the previous methods for AP discovery configured, the BSAP will not discover the vWLAN.

You can verify that the BSAP has successfully discovered the vWLAN using the GUI or CLI of the BSAP. To verify that the BSAP has successfully discovered the vWLAN using the GUI, follow these steps:

- Connect to the BSAP GUI and navigate to **Configuration > AP licenses > Platform** (you must have administrative access). The BSAP is automatically displayed in this menu in preparation for licensing, and it will display an associated domain when it has successfully discovered vWLAN. If the AP is

licensed and assigned a domain, it is also displayed in the GUI under **Configuration > Wireless > Access Points** and **Status > Access Points**.

2. If you do not have platform administrative privileges for the vWLAN, but instead have domain administrative access, the AP will not be displayed in any of the previously mentioned menus until a license is uploaded in the **Configuration > Wireless > AP licenses > Domain** menu. Proceed to license the AP and then navigate to **Configuration > Wireless > Access Points** or **Status > Access Points** to verify the AP has discovered the vWLAN.

Verifying BSAP Discovery

To verify that the BSAP has successfully discovered vWLAN using the BSAP CLI, follow these steps:

1. Connect to the console port of the BSAP. You can use a DB-9 female to RJ-45 rollover cable and open a VT100 terminal session with the following settings: **115200** baud, **8** data bits, no parity, and **1** stop bit (no flow control).

Alternatively, you can connect to the BSAP using SSH on port 2335. 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. BSAPs 1800v1, 1920, 1925, and 1940 do not have console ports so SSH is required.

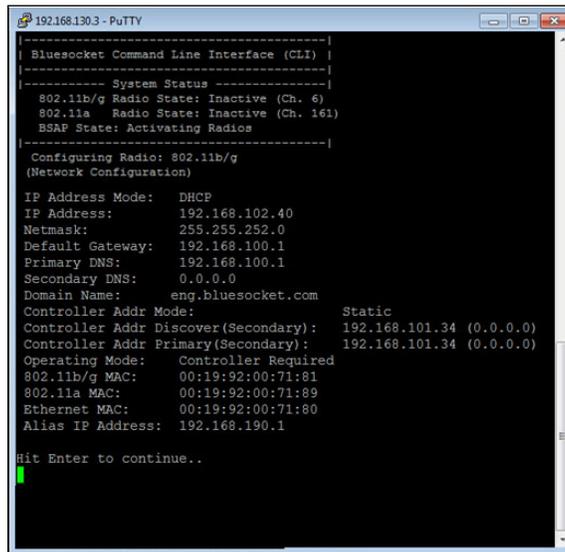
2. Once connected to the BSAP, you must log in to access the CLI. Enter the default user name of **admin** and the default password of **blue1socket**.



Passwords are configurable on a per-AP template basis using the GUI. Refer to the [vWLAN Administrator Guide](https://supportforums.adtran.com) (available online at <https://supportforums.adtran.com>) for more information. If the BSAP has not yet discovered the vWLAN and automatically downloaded a configuration, use the default password.

3. In the BSAP CLI, select option **1** in the **Main Menu** for network configuration.
4. In the **Network Configuration Menu**, select option **8** for network summary information.

5. Verify the vWLAN's public network interface IP address is populated under **Controller Address**.



```

192.168.130.3 - PuTTY
-----|
| 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: 192.168.102.40 |
| Netmask: 255.255.252.0 |
| Default Gateway: 192.168.100.1 |
| Primary DNS: 192.168.100.1 |
| Secondary DNS: 0.0.0.0 |
| Domain Name: eng.bluesocket.com |
| Controller Addr Mode: Static |
| Controller Addr Discover(Secondary): 192.168.101.34 (0.0.0.0) |
| Controller Addr Primary(Secondary): 192.168.101.34 (0.0.0.0) |
| Operating Mode: Controller Required |
| 802.11b/g MAC: 00:19:92:00:71:81 |
| 802.11a MAC: 00:19:92:00:71:89 |
| Ethernet MAC: 00:19:92:00:71:80 |
| Alias IP Address: 192.168.190.1 |
|
| Hit Enter to continue..

```



*If a vWLAN is not discovered, the AP attempts to connect to a server at the following IP address: **76.164.174.46**. This server is for future use. If you are attempting to connect to a different vWLAN, refer to [Troubleshooting on page 20](#) to determine why the AP did not connect.*

Troubleshooting

Troubleshooting the BSAP discovery functionality relies upon verifying the ports and protocols allowed between the vWLAN and the BSAPs, the static AP discovery configuration, the DHCP Option 43 configuration, and the DNS configuration. These troubleshooting methods are described in the following sections.

Troubleshooting Required TCP/UDP Ports and Protocols

Verify that you are allowing the appropriate ports and protocols in any firewall or ACL between the vWLAN and BSAPs, between the primary and secondary vWLAN systems (when using high availability), between the vWLAN and any authentication servers, between BSAPs when using Layer 3 mobility (tunnelling), and between BSAPs and any authentication servers when using external RADIUS 802.1x authentication. You can configure the firewall or ACL to log dropped packets to verify that all ports or protocols are allowed. If the BSAP is unable to establish a control channel (TCP port 33333) to the vWLAN, it will automatically reboot every 3 minutes until a control channel is established.

Troubleshooting Static AP Discovery

To troubleshoot static AP discovery, log into the BSAP using the CLI and verify that it has been configured appropriately for static discovery. Refer to [Statically Configuring BSAPs Using the CLI on page 5](#) for specific information. Verify that the **Controller Address Mode** is set to **Static** and the

Controller Address is the appropriate vWLAN public network interface IP address.

```

COM3 - PuTTY
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: 192.168.190.1
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

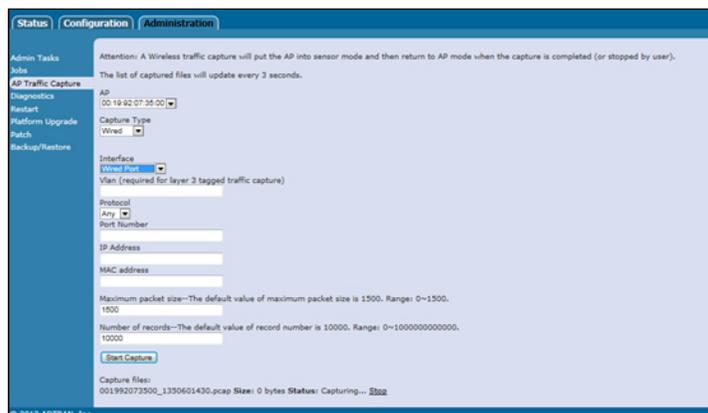
Hit Enter to continue..

```

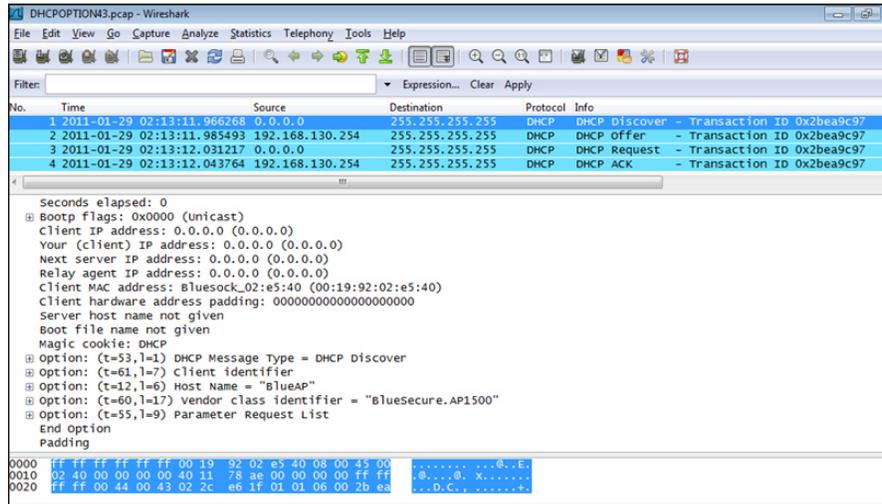
Troubleshooting DHCP Option 43 AP Discovery

To troubleshoot DHCP Option 43 configuration, perform a traffic capture on the wired interface of another BSAP that is in the same subnet of the problem BSAP. Begin the capture and reboot the problem BSAP to capture the broadcast DHCP traffic while the BSAP attempts to obtain an IP address during the boot process. To begin the BSAP traffic capture, connect to the vWLAN GUI and navigate to **Administration > AP Traffic Capture**, or if you are using vWLAN release 2.3 or later, navigate to **Administration > Traffic Capture** for vWLAN system information.

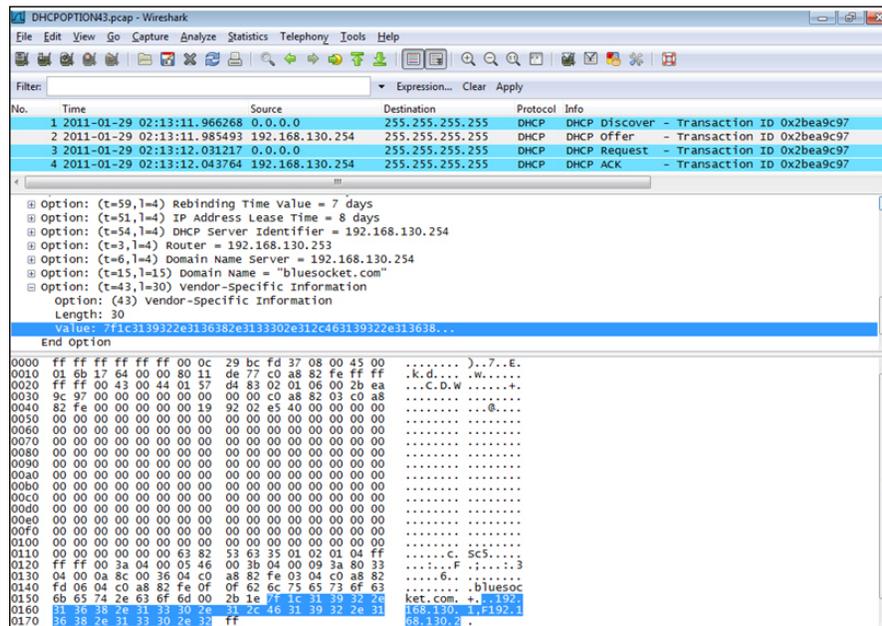
The following is an example of a traffic capture on the wired interface of a BSAP that is in the same subnet of the problem BSAP. For static discovery, it is required to configure the BSAP in the same subnet of the problem BSAP for the vWLAN to be discovered and used to perform a traffic capture. You can use Wireshark (www.wireshark.org) to open and analyze the traffic capture file.



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



Analyze the DHCP Offer from the DHCP server to make sure Option 43 includes the appropriate code/length/value settings. These settings are converted to hexadecimal format. Refer to [Vendor-Specific Information on page 8](#) for more information about hexadecimal format conversion.



If you do not perform a traffic capture using the vWLAN GUI, you have the option to mirror the switchport on which the BSAP is attached and perform a traffic capture there. In addition, you can run a traffic capture on a wired client in the same subnet, run a traffic capture on the gateway, or run a traffic capture on the DHCP server. Verify the Option 60 and Option 43 configurations in all traffic captures.

Troubleshooting DNS AP Discovery

To troubleshoot DNS AP discovery, a traffic capture can be performed; however, because DNS is not broadcast traffic, the traffic capture cannot be performed on another BSAP in the same subnet as the problem BSAP. Instead, you can mirror the switchport on which the problem BSAP is attached and perform a traffic capture there, run a traffic capture on a wired client in the same subnet, run a traffic capture on the gateway, or run a traffic capture on the DNS server. The traffic can then be analyzed to make sure the BSAP sends a DNS request for AP discovery, and that the DNS server replies with the public network interface IP address of the vWLAN.

In addition to the traffic capture, you can troubleshoot DNS configuration using a name server (NS) lookup for AP discovery. Enter the **nslookup** command from the command prompt of a wired client in the same subnet as the problem BSAP to verify that the IP address of vWLAN is returned (assuming the BSAP is configured to use the same DNS servers as the wired client). For example, enter the command as follows at the command prompt:

```
C:\nslookup apdiscovery
```

You should receive the public network interface IP address of the vWLAN once this command is entered.