Troubleshooting Wireless Clients

Version 1.1

Basic Connectivity

Troubleshooting information in this section covers problems with basic wireless connectivity, such as inability to associate or inability to communicate after association.

General

The Wi-Fi Alliance has made great strides in testing interoperability between 802.11 devices from many different manufacturers. Despite these efforts, however, client incompatibility remains the primary complaint from network managers deploying wireless LANs. A wide range of wireless hardware and software is in use, with a corresponding wide range of quality – a given client adapter card may work fine with one revision of driver software, but experience numerous problems with another. A given operating system may perform poorly on a wireless network until specific vendor patches are applied. For this reason, Aruba recommends that enterprise network managers develop standard supported configurations for their deployment. This configuration should consist of:

- Device type and model (laptops, PDAs, handheld devices, voice handsets, etc.)
- Operating system (Windows 2000, Windows XP, MacOS X, Linux, etc.)
- Wireless NIC hardware manufacturer and model
- Wireless NIC software driver
- Wireless NIC firmware revision, if required
- Wireless NIC client utility or radio manager, if needed
- Authentication and encryption software (VPN client, 802.1x supplicant, etc.)

Spending the time up front to develop and test such configurations will greatly reduce troubleshooting time and effort after the network is deployed and operational. A table of configurations tested by Aruba appears in the Design Guide, but this testing cannot take into account all possibilities. Network managers can use these recommendations but should always perform testing in their own environments with their own applications.

Client cannot find AP

Before a wireless client can associate to a network, it must locate at least one Access Point. Most wireless clients locate available network by broadcasting a series of 802.11 *probe-request* frames on multiple channels. APs hearing these probe-request frames should answer with *probe-response* frames containing the AP's ESSID and various other capability parameters. Two types of probe-request frames are possible:

> **Broadcast Probe Request** – In a broadcast probe request, a client looks for any available ESSID. It does so by leaving the ESSID field empty in the probe-request frame. Normally, all AP's receiving the probe-request, regardless of ESSID, will answer. This is how Windows XP, for example, populates the list of available wireless networks.
>
> **Specific Probe Request** – In this type of probe-request, the client is only interested in one particular ESSID. It will include this ESSID in the request, and only APs supporting this ESSID will respond.

It is possible in an Aruba deployment to disable responses to broadcast probe-requests, and require a specific probe-request with the correct ESSID before an AP will answer. If a client does not find an AP to associate with, there are a number of possible causes.

A packet capture of a normal probe-request/probe-response sequence is shown in the figure below. Detailed packet capture data can be found in Appendix A.

Source	Destination	Protocol	BSSID
SMC Net:64:BE:08	Ethernet Broadcast	802.11 Probe Req	FF:FF:FF:FF:FF:FF
SMC Net:64:BE:08	Ethernet Broadcast	802.11 Probe Req	FF:FF:FF:FF:FF:FF
Cisco:4F:75:9C	SMC Net:64:BE:08	802.11 Probe Rsp	00:0C:30:4F:75:9C
Aruba Net:9D:65:E0	SMC Net:64:BE:08	802.11 Probe Rsp	00:0B:86:9D:65:E0
Cisco:4F:75:9C	SMC Net:64:BE:08	802.11 Probe Rsp	00:0C:30:4F:75:9C
Aruba Net:80:A6:00	SMC Net:64:BE:08	802.11 Probe Rsp	00:0B:86:80:A6:00
Aruba Net:9D:65:E0	SMC Net:64:BE:08	802.11 Probe Rsp	00:0B:86:9D:65:E0
Netgear:85:DF:38	SMC Net:64:BE:08	802.11 Probe Rsp	00:09:5B:85:DF:38
Linksys Group:0F:6...	SMC Net:64:BE:08	802.11 Probe Rsp	00:06:25:0F:6E:1F
Cisco:4F:75:9C	SMC Net:64:BE:08	802.11 Probe Rsp	00:0C:30:4F:75:9C
Cisco:4F:75:9C	SMC Net:64:BE:08	802.11 Probe Rsp	00:0C:30:4F:75:9C
The Linksys Group:...	SMC Net:64:BE:08	802.11 Probe Rsp	00:0C:41:8F:9E:D8

Figure 1 - Network Discovery

Client's list of available networks is empty

- Ensure that the user is physically located in an area with AP coverage. Sometimes wireless LANs are deployed only in certain parts of a building. The user may not be aware of this fact, and may be reporting a problem when there is none.
- Make sure the client's wireless adapter is enabled. Some newer laptops with built-in wireless hardware have a physical switch that enables and disables the radio. NIC client utilities often contain similar software switches. Finally, the adapter may be disabled by the operating system.
- If responses to broadcast probe-requests have been disabled in the Aruba network, ensure that the client has been configured with the proper ESSID. If the ESSID is incorrect, the client will not be able to locate any APs.
- Ensure that the wireless network is operational and that no APs or switches have failed. If part of the network has failed, it is likely that multiple users will report problems. Note that in a standard dense-mode Aruba deployment, multiple APs will normally be able to provide service to one user, so the failure of one AP is unlikely to cause this symptom.
- Enable client debugging for the client device in question. From the Aruba CLI, use the command "aaa user debug mac <MAC address of client>". Log output from the debug process can be viewed by issuing the command "show log intuser 30" (to display the last 30 lines of the log file). Verify that the switch is receiving probe requests from the client.
- Perform a wireless packet capture through the Aruba system for the appropriate area where the user is located. Filter the capture for the user's MAC address. A packet capture is a sure way to find out if the client is transmitting probe-requests, if the probe-requests contain the correct ESSID, and if an AP is answering probe-requests.
- Reset the client NIC or operating system. In the case of malfunctioning client software, this does not fix the underlying problem but is often the fastest way to get the user back on the network.
- Replace the client NIC. If a packet capture appears normal and client mis-configuration has been ruled out, it is possible that the client NIC has failed.

Client's list of available networks contains some entries, but not the correct ESSID

- If responses to broadcast probe-requests have been disabled in the Aruba network, ensure that the client has been configured with the proper ESSID. If the ESSID is incorrect, the client will not be able to locate any APs.
- Ensure that the wireless network is operational and that no APs or switches have failed. If part of the network has failed, it is likely that multiple users will report problems. Note that in a standard dense-mode Aruba deployment, multiple APs will normally be able to provide service to one user, so the failure of one AP is unlikely to cause this symptom.
- Perform a wireless packet capture through the Aruba system for the appropriate area where the user is located. Filter the capture for the user's MAC address. A packet capture is a sure way to find out if the client is transmitting probe-requests, if the probe-requests contain the correct ESSID, and if an AP is answering probe-requests.
- Reset the client NIC. In the case of malfunctioning client software, this does not fix the underlying problem but is often the fastest way to get the user back on the network.

Client finds AP, but cannot associate

After a client has located one or more APs supporting the desired ESSID, it must associate to that AP. Association is a four-step process consisting first of 802.11 authentication (not to be confused with 802.1x or VPN authentication) followed by association. Four frames are exchanged on the wireless network during association, as shown in the figure below.

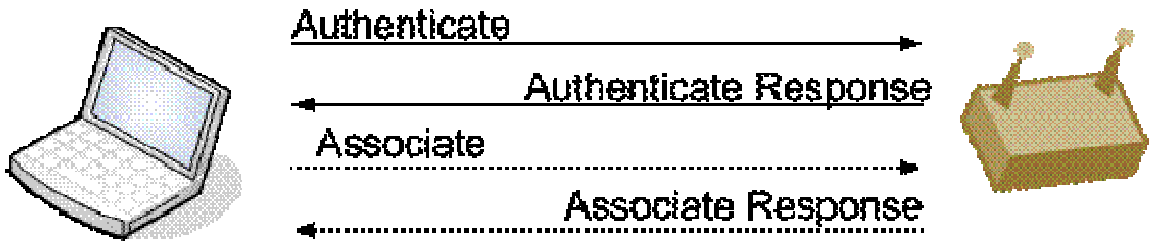

Figure 2 - Association Process

The figure below shows a packet capture of a normal authenticate/associate sequence. Detailed packet capture data can be found in Appendix A.

Source	Destination	Protocol	BSSID
SMC Net:64:BE:08	Aruba Net:80:18:00	802.11 Auth	00:0B:86:80:18:00
Aruba Net:80:18:00	SMC Net:64:BE:08	802.11 Ack	
Aruba Net:80:18:00	SMC Net:64:BE:08	802.11 Auth	00:0B:86:80:18:00
SMC Net:64:BE:08	Aruba Net:80:18:00	802.11 Assoc Req	00:0B:86:80:18:00
Aruba Net:80:18:00	SMC Net:64:BE:08	802.11 Ack	
Aruba Net:80:18:00	SMC Net:64:BE:08	802.11 Assoc Rsp	00:0B:86:80:18:00

Figure 3 - Association Process Packet Capture

If the client and AP are configured differently, association will typically fail. Very little information is given to the user when an association fails, so most troubleshooting must be done from the network side. The most likely cause for an authentication or association failure is client misconfiguration.

802.11 Authentication Fails

The 802.11 *authenticate* exchange is a primitive form of authentication specified by the original 802.11 standard, and is not related to secure authentication such as 802.1x or VPN. This authentication exchange must still take place before an association exchange, but no useful information is exchanged.

- Enable client debugging for the client device in question. From the Aruba CLI, use the command "aaa user debug mac <MAC address of client>". Log output from the debug process can be viewed by issuing the command "show log intuser 30" (to display the last 30 lines of the log file). The log file should indicate the reason for a failed authentication or association. Often the cause is a capability mismatch between the client and AP.
- If the authenticate process fails, it is likely because the client has been configured for *shared-key authentication*. Shared-key authentication opens a security vulnerability and should never be used - the Aruba system does not support shared-key authentication. The client should be configured for either "open system" or "WPA" authentication, but never shared-key.
- Ensure that the user is physically located in an area with AP coverage. If signal strength is too low, radio transmission may be garbled to the point that authentication or association is impossible. The Station Manager log will indicate with which AP the client is attempting to associate – ensure that this AP is near the user's physical location.
- Perform a wireless packet capture. If the Station Manager log provides no useful information or is inaccessible, a packet capture will always show the reason for a failed association.
- Reset the client NIC. In the case of malfunctioning client software, this does not fix the underlying problem but is often the fastest way to get the user back on the network.

Association Fails

During the association request/response exchange, a number of capabilities are exchanged. If there is a mismatch between the client and network configuration, the association will often be rejected by the AP. On the client, there is often no indication that an association has failed other than a lack of association. For example, under Windows XP using the built-in "Zero Configuration" service, Windows will continually display "One or more wireless networks are available…"

- Enable client debugging for the client device in question. From the Aruba CLI, use the command "aaa user debug mac <MAC address of client>". Log output from the debug process can be viewed by issuing the command "show log intuser 30" (to display the last 30 lines of the log file). The log should indicate the reason for a failed authentication or association. Often the cause is a capability mismatch between the client and AP.
- Verify that the AP has not reached the maximum number of users. If the system has been configured to allow only 20 associations per AP, the 21st client will be rejected. A simple way to do this is using the "show ap-leds" command to view the status of AP LEDs on the switch. An AP that is full will indicate such via the AP LEDs.
- If the client fails association, the likely cause is a client misconfiguration. If the network has been configured for WPA and TKIP encryption, and the client has been configured for open system and WEP encryption, association will fail.
- Ensure that the user is physically located in an area with AP coverage. If signal strength is too low, radio transmission may be garbled to the point that authentication or association is impossible. The Station Manager log will indicate with which AP the client is attempting to associate – ensure that this AP is near the user's physical location.
- In a dense-mode AP deployment, the AP's minimum rate may have been adjusted to a higher value. If the client cannot support this higher value because of signal impediments or configuration, association will fail.
- Perform a wireless packet capture. If the Station Manager log provides no useful information or is inaccessible, a packet capture will always show the reason for a failed association.
- Reset the client NIC. In the case of malfunctioning client software, this does not fix the underlying problem but is often the fastest way to get the user back on the network.
- If "Authentication Failure Auto-Blacklisting" has been enabled on the Aruba switch, multiple authentication failures will cause a client to be denied association. If this feature has been enabled, check the current "Black List" in the management GUI by navigating to

Monitoring▫Client▫Client Blacklist. Ensure that the authentication problem has been fixed before re-attempting association.

- Verify that no denial of service attack is underway. From the client perspective, a successful association followed by an immediate disassociation will appear the same as an unsuccessful association. Examine the Wireless Management System (WMS) log files on the Aruba switch by navigating in the management GUI to the Events tab. A packet capture will also reveal the presence of a denial of service attack.

Client associates to AP, but higher-layer authentication fails

Problems with higher-layer authentication such as 802.1x are normally not related to basic connectivity, but can disguise themselves as such. If association to an AP is successful, basic connectivity problems are likely ruled out.

- Reset the client NIC. If association is successful a second or third time but authentication continues to fail, it is unlikely that a basic connectivity problem is causing the issue. See the "Authentication" section of this guide for more details on troubleshooting higher-layer authentication problems.
- Perform a wireless packet capture. If authentication problems are being caused by a busy network or a denial of service attack, a packet capture will make this clear.

Client associates / authenticates, but no network connectivity

In this scenario, a client has successfully associated to an AP and, if configured, has successfully gone through higher-layer authentication. However, the client has no access to network services.

- Static WEP Key mismatch: If the client and AP are configured for static WEP, it is likely that the WEP keys do not match. This symptom commonly manifests itself when a client configured for DHCP fails to obtain an IP address. Check the client's WEP key and ensure that it matches the WEP key configured in the Aruba system.
- Dynamic WEP Key Exchange Failure: If the network uses 802.1x with automatically-assigned WEP keys (dynamic WEP), it is possible that the key exchange process failed. Because this key exchange is non-standard and does not involve a verified "handshake", the process sometimes fails without an error message being generated. Resetting the client NIC or rebooting the client operating system often restores connectivity in this situation.
- WPA/802.11i Key Exchange Failure: In a WPA or 802.11i network, the dynamic key exchange process may fail. This is an error condition and indicates either a man-in-the-middle attack or a faulty NIC driver. Examine the "Authentication" log file in the Aruba switch for details – because the WPA/802.11i key exchange is a standard and utilizes a four-way verified handshake, error messages will be generated when part of the process fails. To view the Authentication log file in the Aruba management GUI, navigate to Monitoring▫Process Logs and filter on "Authentication." From the CLI, enter the command "show log arubaauth".
- Once association and higher-layer authentication have succeeded, it is analogous to the link light turning on in a wired Ethernet network. Troubleshoot the problem using traditional tools such as "ping" and "traceroute". Problems such as this often indicate faults in the wired network or in client network settings. For example, the client may be configured for a static IP address, the default gateway for the network may be down, or there may be a routing problem.
- If the client is configured for DHCP and does not obtain an IP address, it may indicate a problem with the DHCP server or the uplink network from the Aruba switch. Enable client debugging for the client device in question. From the Aruba CLI, use the command "aaa user debug mac <MAC address of client>". Log output from the debug process can be viewed by issuing the command "show log intuser 30" (to display the last 30 lines of the log file). DHCP activity will appear in the log file.
- If multiple users on the same AP are experiencing problems, examine statistics on the AP. It is possible that the network is extremely busy, is experiencing interference, or is experiencing a denial of service attack. Perform a wireless packet capture when in doubt.

Client initially has network connectivity, then loses connectivity

In this scenario, a client successfully associates to an AP, authenticates, and has network connectivity. At some future time, communication fails.

- Ensure that a higher-layer network failure has not taken place. Use tools such as "ping" and "traceroute" to verify. If an attempt to ping the Aruba switch from the client fails, the problem can be isolated to the wireless network.
- If the failure took place while the user was moving, it is possible that roaming failed. Examine the client's current signal strength and data rate. If they are low, compare the user's physical location with the location of the currently associated AP. This is sometimes caused by an issue known as "client stickiness" – the tendency for a client to maintain an existing association and ignore closer APs even when signal strength has significantly degraded. Ideally, pre-deployment testing will identify client NICs and drivers that exhibit this problem so that they can be excluded from the deployment.
- Dynamic WEP Key Exchange Failure: If the network uses 802.1x with automatically-assigned WEP keys (dynamic WEP), it is possible that the key exchange process failed. Because this key exchange is non-standard and does not involve a verified "handshake", the process sometimes fails without an error message being generated. Resetting the client NIC or rebooting the client operating system often restores connectivity in this situation.
- WPA/802.11i Key Exchange Failure: In a WPA or 802.11i network, the dynamic key exchange process may fail. This is an error condition and indicates either a man-in-the-middle attack or a faulty NIC driver. Examine the "Authentication" log file in the Aruba switch for details – because the WPA/802.11i key exchange is a standard and utilizes a four-way verified handshake, error messages will be generated when part of the process fails. To view the Authentication log file in the Aruba management GUI, navigate to Monitoring▫Process Logs and filter on "Authentication." From the CLI, enter the command "show log arubaauth".
- If multiple users on the same AP are experiencing problems, examine statistics on the AP. It is possible that the network is extremely busy, is experiencing interference, or is experiencing a denial of service attack. Perform a wireless packet capture when in doubt.

Client initially has network connectivity, then wireless association is dropped

In this scenario, a client successfully associates to an AP, authenticates, and has network connectivity. At some future time, the association is dropped.

- If the failure took place while the user was moving, it is possible that the user roamed to an area with no radio coverage and cannot re-associate.
- If the problem repeats often, debug may be enabled for the client experiencing the problem. If the Aruba switch is dropping the association, this will be indicated in the log file. To enable client debug in the Aruba CLI, use the command "aaa user debug mac <MAC address of client>". Log output from the debug process can be viewed by issuing the command "show log intuser 30" (to display the last 30 lines of the log file).
- In a network configured to ignore broadcast probe requests, Windows devices may spend an excessive amount of time transmitting broadcast probe requests before finally transmitting probe requests for a specific ESSID. Under these circumstances, roaming performance between APs may be extremely slow, and may cause the wireless association to be dropped for a long period of time. If this is the cause of the problem, the association will eventually be restored. A wireless packet capture will verify this situation. To resolve, make sure the latest Windows OS patches have been applied. Also consider enabling responses to broadcast probe requests – this feature should be used only as a convenience factor to hide special-purpose ESSIDs from clients and should not be considered a security feature.
- The cause for the dropped association may have been a denial of service attack – specifically a "deauth" or "disconnect station" attack. View the Aruba Wireless Management System log file by navigating in the management GUI to the Events tab to see if this is the case. A wireless packet capture will also verify this situation.
- Reset the client NIC. If an internal error has caused the dropped association, a reset of the NIC may restore connectivity.

Client experiences poor performance

This scenario covers many different situations. In general, the complaint will be slow performance – download speeds may be low, application timeouts may occur, or general sluggishness may be reported.

- If the performance problems began while the user was moving, it is possible that roaming failed. Examine the client's current signal strength and data rate. If they are low, compare the user's physical location with the location of the currently associated AP. This is sometimes caused by an issue known as "client stickiness" – the tendency for a client to maintain an existing association and ignore closer APs even when signal strength has significantly degraded. Ideally, pre-deployment testing will identify client NICs and drivers that exhibit this problem so that they can be excluded from the deployment.
- Examine client statistics from the Aruba management GUI. Navigate to Monitoring > Clients > Enterprise Clients, select the affected client, and click on "Client Activity".
    - If RSSI – also known as signal strength - is low (below 20), the client has poor signal strength to the nearest AP. This may indicate a roaming failure, described above.
    - If "transmit retries" is high, the client is sending frames that are not being acknowledged by the AP. The client is then forced to re-transmit these frames, reducing performance. The cause may be interference or low signal strength.
    - If "receive retries" is high, the AP is sending frames that are not being acknowledged by the client. The AP is then forced to re-transmit these frames, reducing performance. The cause may be interference or low signal strength.
    - If the transmit or receive data rate is low, it indicates that the client or AP's rate adaptation algorithm has detected errors at higher data rates and is forcing a lower rate. This could indicate interference or low signal strength.
    - If signal strength is high, retry rate is high, and data rate is low, the cause may be localized interference. These symptoms indicate a client that is close to the AP with good signal strength, but with poor communication between the AP and client. Examine the Events tab in the GUI and look for any indications of detected interference.
    - If the above parameters are within acceptable ranges, but throughput is still low, it may indicate a congested AP. Perform activity monitoring on the entire AP rather than on the individual client to examine how much bandwidth is being consumed on the AP. If there are too many clients connected to a given AP, performance may be increased by reducing the maximum number of clients allowed on the AP.

- There may be congestion on the wired portion of the network. Examine the wired network using traditional tools such as “ping” and “traceroute” or using sniffer software.
- Perform a wireless packet capture to view any anomalous conditions in the area covered by the AP.

Authentication

Most enterprise wireless networks make use of some form of secure authentication. This typically means 802.1x or VPN, although other choices are possible. The troubleshooting process is different depending on which authentication scheme is in use.

802.1x

Authentication using 802.1x may be accomplished in combination with dynamic WEP key exchange, WPA with TKIP, or 802.11i with AES. The troubleshooting process for the authentication portion is identical in all cases.

Incorrect username/password (TTLS or PEAP)

A typical cause of authentication failure is an incorrect username, password, or one-time token. In most cases, this is a simple problem to troubleshoot, because the client will generate an error message indicating the cause of the failure. However, depending on the 802.1x supplicant in use, this error may not be obvious.

- Check the RADIUS server. The first line of troubleshooting for authentication problems should always involve the authentication server. Because the actual authentication exchange in 802.1x happens between the client and the authentication server, the server is the most accurate entity for examining logging information. Server log messages will often indicate what triggered the failure.
- If the RADIUS server is inaccessible, check authentication log messages on the Aruba switch. From the management GUI, navigate to Monitoring▫Process Logs and filter on Authentication. From the CLI, issue the command “show log arubaauth”. As an 802.1x authenticator, the Aruba switch can only see an 802.1x success or failure, but has no information about why a failure occurred. Checking this log will indicate that a failure was signaled by the authentication server, which can then lead to further troubleshooting.

Server certificate is not validated

802.1x operation in wireless networks (PEAP, EAP-TLS, and TTLS) relies on a valid certificate being transmitted from the authentication server to the client. The certificate must not be expired, must be valid for the server name, and must be trusted by the client (if the certificate is signed by a certificate authority, the certificate authority must be trusted by the client.)

Certificate errors may or may not be indicated by the client. For example, the Funk Odyssey client will turn an icon red and indicate an explicit error when a certificate problem occurs. The Microsoft supplicant built into Windows XP will not.

- If a certificate problem is suspected, most 802.1x supplicants provide an option to disable server certificate validation. As a troubleshooting mechanism, temporarily disable this option if available. If authentication is successful after this option is disabled, a certificate problem has been confirmed. **Note:** Do not leave the "validate server certificate" option turned off in the 802.1x supplicant. This opens a security vulnerability making a man-in-the-middle attack possible.
- Verify that the client configuration matches the standard enterprise client configuration. Most 802.1x problems are caused by a misconfigured client. For example, the wrong certificate authority or wrong server domain name may have been selected, or password authentication may be selected when one-time token use is required by the authentication server.
- Perform a wireless packet capture. If 802.1x authentication is observed to begin, and then abruptly stops, a certificate error may be the cause. The 802.1x supplicant should not proceed with authentication if it detects an invalid server certificate.

Client Certificate is not accepted (EAP-TLS only)

When using EAP-TLS as an 802.1x authentication method, a client certificate must be validated by the RADIUS server in order for authentication to succeed. If the client certificate cannot be validated, authentication will fail.

- Examine the RADIUS server log files. In most cases, the RADIUS server will provide necessary clues to troubleshoot the problem.
- A common problem for client certificates is an incorrect Common Name (CN). If the CN is not recognized by the RADIUS server, the RADIUS server cannot locate the user in the database. Check the RADIUS server documentation for the correct format. For example, Microsoft IAS expects the certificate CN to be in the form "user@domain" in order to locate the user correctly in Active Directory.
- Verify that the client certificate has not expired by examining the certificate "Valid to" date.
- Verify that the client certificate has not been revoked. The certification authority Certificate Revocation List (CRL) contains all revoked certificates.

Client is using the wrong form of PEAP

PEAP (Protected Extensible Authentication Protocol) is a widely-deployed authentication method for 802.1x. There are two different forms of PEAP in use – Microsoft PEAP and Cisco PEAP. Both client and server must be using the same form of PEAP. If the RADIUS server is Microsoft IAS and the client is Microsoft Windows using the built-in Wireless Zero Configuration utility, for example, it is likely that both sides are using Microsoft PEAP. However, in a mixed environment, mismatches may occur.

- The client may not provide useful information on which type of PEAP is in use. However, a clue may be to examine the PEAP "inner" authentication protocol. Microsoft PEAP allows MS-CHAP v2 and a smart card/certificate as the inner authentication protocol. Cisco PEAP also supports one-time passwords or token cards as the inner authentication protocol. If a one-time password or secure token is available in the client's PEAP configuration, Cisco PEAP is most likely being used.
- Current versions of Cisco's ACS RADIUS server support both MS-PEAP and Cisco PEAP. However, older versions of ACS do not support MS-PEAP. Ensure that an updated version of ACS is being run if MS-PEAP is used by clients.

RADIUS Server reports "Authentication Method Not Supported"

This error message is caused by the client and server using different 802.1x authentication methods.

- Verify that the RADIUS server and client are configured for the same 802.1x authentication method. For example, if the RADIUS server is configured to use PEAP, the client must also be configured this way. Microsoft clients default to EAP-TLS (Smart card or other certificate).

Client stops communicating after roaming (WPA)

In a network running WPA/TKIP, the NIC card may fail to re-negotiate encryption keys after roaming to a new AP. This behavior will manifest itself as the client continuing to hold an active association, but unable to communicate to the network. Resetting the NIC card will clear the problem.

- This problem has been seen with Proxim Orinoco A/B/G cards with driver version 2.4.2.17. After roaming to a new AP, the client will generate MIC (Message Integrity Check) failures during phase 2 of the 4-way WPA key exchange handshake.
- Verify the problem by enabling 802.1x debugging on the Aruba switch:

```
(config) # logging console debug
# debug arubaauth dot1x dot1xtrace
```

VPN

VPN Dialer displays "Interface is down or no route"

This message indicates that the client does not have an IP address or a route to reach the Aruba switch. To view the IP address and default gateway for the client, click the "Network Info" button in the VPN dialer.

- If there is no IP address on the interface, verify that the interface is configured to obtain an address via DHCP.
- Verify that association to the wireless network succeeded. Examine the output of "show user" on the Aruba switch to view the client's association state.
- Verify that the DHCP server is active. If the Aruba internal DHCP server is in use, the command "show log dhcp" will provide information on DHCP server activity.

VPN Dialer displays "No Aruba switches detected"

When this error message is displayed, it indicates that the VPN dialer could not verify that the client was associated to an Aruba switch. The mechanism used to determine if an Aruba switch is present is a DNS lookup. If the client is associated to an Aruba switch, the DNS request will be intercepted by the Aruba switch and a response sent back to the client.

The likely cause of this error message is that the client has no DNS server configured or learned through DHCP. If the client has no DNS server to use for lookups, the client will not generate DNS requests, and the Aruba switch will not be able to intercept the request and respond to it. There are three possible solutions:

- Configure the DHCP server so that it supplies clients with a DNS server address.
- Statically configure the client with the address of a DNS server.
- In the Aruba VPN dialer, turn off the option labeled "Wait for wireless". Note that with this option disabled, the VPN dialer will try to establish a connection any time the wireless NIC is connected to a network and has an IP address.

VPN Dialer displays “There was no answer”

This is a generic message indicating that the VPN client was unable to connect. Common causes are a mismatch between the dialer configuration on the client and the VPN configuration on the switch, or an internal Windows error.

- Examine log files on the Aruba switch. First, examine the output of “show log crypto”. The following error messages are common:
  - NO_PROPOSAL_CHOSEN: Indicates the client and switch are not configured in a like manner. If using the Aruba dialer, verify that the lifetime, encryption, and hash for both IKE and IPSEC match.
  - INVALID_HASH_INFORMATION: Indicates that the client and switch's IKE pre-shared keys do not match. If using a 3rd-party VPN client, the IKE pre-shared key is sometimes called the "group key" or "group password".
  - INVALID_PAYLOAD_TYPE, INVALID_COOKIE, and PAYLOAD_MALFORMED: May indicate that the IKE pre-shared key does not match between the client and switch.
- Examine the output of “show crypto isakmp sa”. This command will list all IKE security associations (SAs) currently active in the switch. If no SA appears for the client in question, it is likely that the IKE pre-shared keys do not match between the client and switch.
- Examine the output of “show crypto ipsec sa”. Once IKE negotiation has succeeded (an IKE SA appears for the client), this command will list all IPSEC security associations (SAs) currently active in the switch. If no SA appears for the client in question, it is likely that the client and switch have mismatching lifetimes, encryption types, or hash configuration.

VPN Dialer hangs while showing “Connecting”

- One possible cause of this problem is a lack of IP connectivity to the Aruba switch. It is unlikely that this is the cause when the client is attempting a VPN connection to the switch with which it is associated. However, the VPN client is sometimes used across multi-hop IP networks. If this problem appears, it may mean that the client has an IP address and a default route, but an upstream router does not have a path to the VPN termination point.
- Another possible cause of this problem is that the Windows IPSEC service is not running. Bring up the Windows “Services” control panel by navigating to Start▫Settings▫Control Panel▫Administrative Tools▫Services. Look for the IPSEC service, and verify it is configured as the following figure shows. Note that the IPSEC service in turn depends on the Remote Procedure Call (RPC) service – verify that both are enabled.

Figure 4 - Windows IPSEC Service

IPSEC is up, but dialer does not display "Logging on" message

This message indicates that IPSEC was successful, but L2TP was not.

- Verify the diagnosis by examining the output of "show crypto ipsec sa". If a security association exists for the client, IPSEC was successful. Examine the output of "show vpdn tunnel l2tp". If L2TP has failed, no tunnel will exist for the client in question.
- This is an error condition. Contact Aruba Technical Support for assistance.

Dialer displays "Logging on", but never displays "Connected"

This condition normally indicates that there is no IP address pool configured for the VPN, or that the address pool has been exhausted.

- Examine the output of "show vpdn l2tp configuration". Verify that an IP address pool has been assigned.
- Examine the output of "show vpdn l2tp local pool". Verify that there are IP addresses free. If there are not, it will be necessary to configure an additional IP address pool.

Appendix: Sample Packet Captures

Broadcast Probe Request Frame

Packet Info
Flags: 0x00
Status: 0x01
Packet Length: 54
Timestamp: 17:04:36.126816600 04/09/2004
Data Rate: 2 *1.0 Mbps*
Channel: 1 *2412 MHz*
Signal Level: 68%
Signal dBm: -42
Noise Level: 0%

802.11 MAC Header
Version: 0
Type: %00 *Management*
Subtype: %0100 *Probe Request*
Frame Control Flags: %00000000
0... .... Non-strict order
.0.. .... WEP Not Enabled
..0. .... No More Data
...0 .... Power Management - active mode
.... 0... This is not a Re-Transmission
.... .0.. Last or Unfragmented Frame
.... ..0. Not an Exit from the Distribution System
....0 Not to the Distribution System
Duration: 0 *Microseconds*
Destination: FF:FF:FF:FF:FF:FF *Ethernet Broadcast*
Source: 00:04:E2:64:C1:C0 *SMC Net:64:C1:C0*
BSSID: FF:FF:FF:FF:FF:FF *Ethernet Broadcast*
Seq. Number: 349
Frag. Number: 0

802.11 Management - Probe Request
SSID
Element ID: 0 *SSID*
Length: 0
Supported Rates
Element ID: 1 *Supported Rates*
Length: 8
Supported Rate: 1.0 *(Not BSS Basic Rate)*
Supported Rate: 2.0 *(Not BSS Basic Rate)*
Supported Rate: 5.5 *(Not BSS Basic Rate)*
Supported Rate: 11.0 *(Not BSS Basic Rate)*
Supported Rate: 6.0 *(Not BSS Basic Rate)*
Supported Rate: 12.0 *(Not BSS Basic Rate)*
Supported Rate: 24.0 *(Not BSS Basic Rate)*
Supported Rate: 36.0 *(Not BSS Basic Rate)*
Extended Supported Rates
Element ID: 50 *Extended Supported Rates*
Length: 4
Supported Rate: 9.0 *(Not BSS Basic Rate)*
Supported Rate: 18.0 *(Not BSS Basic Rate)*
Supported Rate: 48.0 *(Not BSS Basic Rate)*
Supported Rate: 54.0 *(Not BSS Basic Rate)*

FCS - Frame Check Sequence
FCS (Calculated): 0xCF771F24

Specific Network Probe Request Frame

Packet Info

Flags: 0x00
Status: 0x01
Packet Length: 54
Timestamp: 17:04:36.126816600 04/09/2004
Data Rate: 2 *1.0 Mbps*
Channel: 1 *2412 MHz*
Signal Level: 68%
Signal dBm: -42
Noise Level: 0%

802.11 MAC Header

Version: 0
Type: %00 *Management*
Subtype: %0100 *Probe Request*
Frame Control Flags: %00000000
0... .... Non-strict order
.0.. .... WEP Not Enabled
..0. .... No More Data
...0 .... Power Management - active mode
.... 0... This is not a Re-Transmission
.... .0.. Last or Unfragmented Frame
.... ..0. Not an Exit from the Distribution System
....0 Not to the Distribution System

Duration: 0 *Microseconds*
Destination: FF:FF:FF:FF:FF:FF *Ethernet Broadcast*
Source: 00:04:E2:64:C1:C0 *SMC Net:64:C1:C0*
BSSID: FF:FF:FF:FF:FF:FF *Ethernet Broadcast*
Seq. Number: 349
Frag. Number: 0

802.11 Management - Probe Request

SSID
Element ID: 0 *SSID*
Length: 16
SSID: wireless-network
Supported Rates
Element ID: 1 *Supported Rates*
Length: 8
Supported Rate: 1.0 *(Not BSS Basic Rate)*
Supported Rate: 2.0 *(Not BSS Basic Rate)*
Supported Rate: 5.5 *(Not BSS Basic Rate)*
Supported Rate: 11.0 *(Not BSS Basic Rate)*
Supported Rate: 6.0 *(Not BSS Basic Rate)*
Supported Rate: 12.0 *(Not BSS Basic Rate)*
Supported Rate: 24.0 *(Not BSS Basic Rate)*
Supported Rate: 36.0 *(Not BSS Basic Rate)*
Extended Supported Rates
Element ID: 50 *Extended Supported Rates*
Length: 4
Supported Rate: 9.0 *(Not BSS Basic Rate)*
Supported Rate: 18.0 *(Not BSS Basic Rate)*
Supported Rate: 48.0 *(Not BSS Basic Rate)*
Supported Rate: 54.0 *(Not BSS Basic Rate)*

FCS - Frame Check Sequence

FCS (Calculated): 0xCF771F24

Beacon Frame

Packet Info
- Flags: 0x00
- Status: 0x00
- Packet Length: 97
- Timestamp: 17:04:36.139436600 04/09/2004
- Data Rate: 2 *1.0 Mbps*
- Channel: 1 *2412 MHz*
- Signal Level: 38%
- Signal dBm: -73
- Noise Level: 0%

802.11 MAC Header
- **Version:** 0
- **Type:** %00 *Management*
- **Subtype:** %1000 *Beacon*

Frame Control Flags: %00000000
- *0... .... Non-strict order*
- *.0.. .... WEP Not Enabled*
- *..0. .... No More Data*
- *...0 .... Power Management - active mode*
- *.... 0... This is not a Re-Transmission*
- *.... .0.. Last or Unfragmented Frame*
- *.... ..0. Not an Exit from the Distribution System*
- *.... ...0 Not to the Distribution System*

- **Duration:** 0 *Microseconds*
- **Destination:** FF:FF:FF:FF:FF:FF *Ethernet Broadcast*
- **Source:** 00:0B:86:80:48:80 *Aruba Net:80:48:80*
- **BSSID:** 00:0B:86:80:48:80 *Aruba Net:80:48:80*
- **Seq. Number:** 3635
- **Frag. Number:** 0

802.11 Management - Beacon
- **Timestamp:** 82013696522 *Microseconds*
- **Beacon Interval:** 100

Capability Info: %0000000000110001
- *x..... ..... Reserved*
- *.x..... ..... Reserved*
- *..0.... ..... DSSS-OFDM is Not Allowed*
- *...x... ..... Reserved*
- *....0... ..... Robust Security Network Disabled*
- *.....0.. ..... G Mode Short Slot Time [20 microseconds]*
- *......x. ..... Reserved*
- *.......x ..... Reserved*
- *..... 0..... Channel Agility Not Used*
- *..... .0..... PBCC Not Allowed*
- *..... ..1..... Short Preamble*
- *..... ...1.... Privacy Enabled*
- *..... ....0... CF Poll Not Requested*
- *..... .....0.. CF Not Pollable*
- *..... ......0. Not an IBSS Type Network*
- *..... ....1 ESS Type Network*

SSID
- **Element ID:** 0 *SSID*
- **Length:** 16
- **SSID:** wireless-network

Supported Rates
- **Element ID:** 1 *Supported Rates*
- **Length:** 4
- **Supported Rate:** 1.0 *(BSS Basic Rate)*
- **Supported Rate:** 2.0 *(BSS Basic Rate)*
- **Supported Rate:** 5.5 *(Not BSS Basic Rate)*
- **Supported Rate:** 11.0 *(Not BSS Basic Rate)*

Direct Sequence Parameter Set
- **Element ID:** 3 *Direct Sequence Parameter Set*
- **Length:** 1
- **Channel:** 1

Extended Supported Rates
  Element ID: 50 *Extended Supported Rates*
  Length: 8
  Supported Rate: 6.0 *(Not BSS Basic Rate)*
  Supported Rate: 9.0 *(Not BSS Basic Rate)*
  Supported Rate: 12.0 *(Not BSS Basic Rate)*
  Supported Rate: 18.0 *(Not BSS Basic Rate)*
  Supported Rate: 24.0 *(Not BSS Basic Rate)*
  Supported Rate: 36.0 *(Not BSS Basic Rate)*
  Supported Rate: 48.0 *(Not BSS Basic Rate)*
  Supported Rate: 54.0 *(Not BSS Basic Rate)*
ERP Information
  Element ID: 42 *ERP Information*
  Length: 1
  ERP Flags: %00000010
    x... .... Reserved
    .x.. .... Reserved
    ..x. .... Reserved
    ...x .... Reserved
    .... x... Reserved
    .... .0.. Not Barker Preamble Mode
    .... ..1. Use Protection
    ....0 Non-ERP Not Present
Reserved 171
  Element ID: 171 *Reserved 171*
  Length: 11
  Value: 0x000B86080400010A040026
Traffic Indication Map
  Element ID: 5 *Traffic Indication Map*
  Length: 4
  DTIM Count: 0
  DTIM Period: 1
  Traffic Ind.: 0
  Bitmap Offset: 0
  Part Virt Bmap: 0x00
FCS - Frame Check Sequence
  FCS (Calculated): 0xDCE7628D

Probe Response Frame

Packet Info

Flags: 0x00
Status: 0x00
Packet Length: 82
Timestamp: 14:33:18.161865000 02/10/2004
Data Rate: 2 *1.0 Mbps*
Channel: 1 *2412 MHz*
Signal Level: 45%
Signal dBm: 0
Noise Level: 0%
Noise dBm: 0

802.11 MAC Header

Version: 0
Type: %00 *Management*
Subtype: %0101 *Probe Response*
Frame Control Flags: %00000000
0... .... Non-strict order
.0.. .... WEP Not Enabled
..0. .... No More Data
...0 .... Power Management - active mode
.... 0... This is not a Re-Transmission
.... .0.. Last or Unfragmented Frame
.... ..0. Not an Exit from the Distribution System
....0 Not to the Distribution System
Duration: 11547 *Microseconds*
Destination: 00:04:E2:64:BE:08 *SMC Net:64:BE:08*
Source: 00:0B:86:80:18:00 *Aruba Net:80:18:00*
BSSID: 00:0B:86:80:18:00 *Aruba Net:80:18:00*
Seq. Number: 2948
Frag. Number: 0

802.11 Management - Probe Response

Timestamp: 16683297454 *Microseconds*
Beacon Interval: 100
Capability Info: %0000000000110001
x..... ..... Reserved
.x..... ..... Reserved
..0.... ..... DSSS-OFDM is Not Allowed
...x... ..... Reserved
....0.. ..... Robust Security Network Disabled
.....0. ..... G Mode Short Slot Time [20 microseconds]
......x. ..... Reserved
.......x ..... Reserved
..... 0..... Channel Agility Not Used
..... .0..... PBCC Not Allowed
....1.... Short Preamble
....1... Privacy Enabled
....0... CF Poll Not Requested
....0.. CF Not Pollable
....0. Not an IBSS Type Network
....1 ESS Type Network

SSID
Element ID: 0 *SSID*
Length: 4
SSID: air1

Supported Rates
Element ID: 1 *Supported Rates*
Length: 4
Supported Rate: 1.0 *(BSS Basic Rate)*
Supported Rate: 2.0 *(BSS Basic Rate)*
Supported Rate: 5.5 *(Not BSS Basic Rate)*
Supported Rate: 11.0 *(Not BSS Basic Rate)*

Direct Sequence Parameter Set
Element ID: 3 *Direct Sequence Parameter Set*
Length: 1
Channel: 1

802.11 Authenticate Frame

Packet Info

Flags: 0x00
Status: 0x00
Packet Length: 34
Timestamp: 14:33:23.619951000 02/10/2004
Data Rate: 2 *1.0 Mbps*
Channel: 1 *2412 MHz*
Signal Level: 48%
Signal dBm: 0
Noise Level: 0%
Noise dBm: 0

802.11 MAC Header

Version: 0
Type: %00 *Management*
Subtype: %1011 *Authentication*
Frame Control Flags: %00000000
0... .... Non-strict order
.0.. .... WEP Not Enabled
..0. .... No More Data
...0 .... Power Management - active mode
.... 0... This is not a Re-Transmission
.... .0.. Last or Unfragmented Frame
.... ..0. Not an Exit from the Distribution System
....0 Not to the Distribution System

Duration: 12315 *Microseconds*
Destination: 00:0B:86:80:18:00 *Aruba Net:80:18:00*
Source: 00:04:E2:64:BE:08 *SMC Net:64:BE:08*
BSSID: 00:0B:86:80:18:00 *Aruba Net:80:18:00*
Seq. Number: 0
Frag. Number: 0

802.11 Management - Authentication

Auth. Algorithm: 0 *Open System*
Auth. Seq. Num.: 1
Status Code: 0 *Reserved*

FCS - Frame Check Sequence

FCS (Calculated): 0x31C54ADD

802.11 Authenticate Response (Success)

Packet Info

Flags: 0x00
Status: 0x00
Packet Length: 34
Timestamp: 14:33:23.622964000 02/10/2004
Data Rate: 2 *1.0 Mbps*
Channel: 1 *2412 MHz*
Signal Level: 37%
Signal dBm: 0
Noise Level: 0%
Noise dBm: 0

802.11 MAC Header

Version: 0
Type: %00 *Management*
Subtype: %1011 *Authentication*
Frame Control Flags: %00000000
0... .... Non-strict order
.0.. .... WEP Not Enabled
..0. .... No More Data
...0 .... Power Management - active mode
.... 0... This is not a Re-Transmission
.... .0.. Last or Unfragmented Frame
.... ..0. Not an Exit from the Distribution System
....0 Not to the Distribution System

Duration: 9499 *Microseconds*
Destination: 00:04:E2:64:BE:08 *SMC Net:64:BE:08*
Source: 00:0B:86:80:18:00 *Aruba Net:80:18:00*
BSSID: 00:0B:86:80:18:00 *Aruba Net:80:18:00*
Seq. Number: 3009
Frag. Number: 0

802.11 Management - Authentication

Auth. Algorithm: 0 *Open System*
Auth. Seq. Num.: 2
Status Code: 0 *Successful*

FCS - Frame Check Sequence

FCS (Calculated): 0x0457AE08

Association Request Frame (includes WPA)

Packet Info

Flags: 0x00
Status: 0x00
Packet Length: 80
Timestamp: 14:33:23.624195000 02/10/2004
Data Rate: 2 *1.0 Mbps*
Channel: 1 *2412 MHz*
Signal Level: 37%
Signal dBm: 0
Noise Level: 0%
Noise dBm: 0

802.11 MAC Header

Version: 0
Type: %00 *Management*
Subtype: %0000 *Association Request*
Frame Control Flags: %00000000
0... .... Non-strict order
.0.. .... WEP Not Enabled
..0. .... No More Data
...0 .... Power Management - active mode
.... 0... This is not a Re-Transmission
.... .0.. Last or Unfragmented Frame
.... ..0. Not an Exit from the Distribution System
....0 Not to the Distribution System

Duration: 9499 *Microseconds*
Destination: 00:0B:86:80:18:00 *Aruba Net:80:18:00*
Source: 00:04:E2:64:BE:08 *SMC Net:64:BE:08*
BSSID: 00:0B:86:80:18:00 *Aruba Net:80:18:00*
Seq. Number: 1
Frag. Number: 0

802.11 Management - Association Request

Capability Info: %0000010000110001
x..... ..... Reserved
.x..... ..... Reserved
..0.... ..... DSSS-OFDM is Not Allowed
...x... ..... Reserved
....0... ..... Robust Security Network Disabled
.....1.. ..... G Mode Short Slot Time [9 microseconds]
......x. ..... Reserved
.......x ..... Reserved
..... 0..... Channel Agility Not Used
..... .0..... PBCC Not Allowed
....1..... Short Preamble
....1.... Privacy Enabled
....0... CF Poll Not Requested
....0.. CF Not Pollable
....0. Not an IBSS Type Network
....1 ESS Type Network

Listen Interval: 1

SSID
Element ID: 0 *SSID*
Length: 4
SSID: air1

Supported Rates
Element ID: 1 *Supported Rates*

Length: 8
Supported Rate: 1.0 *(Not BSS Basic Rate)*
Supported Rate: 2.0 *(Not BSS Basic Rate)*
Supported Rate: 5.5 *(Not BSS Basic Rate)*
Supported Rate: 11.0 *(Not BSS Basic Rate)*
Supported Rate: 6.0 *(Not BSS Basic Rate)*
Supported Rate: 9.0 *(Not BSS Basic Rate)*
Supported Rate: 12.0 *(Not BSS Basic Rate)*
Supported Rate: 24.0 *(Not BSS Basic Rate)*

Extended Supported Rates
Element ID: 50 *Extended Supported Rates*
Length: 4
Supported Rate: 18.0 *(Not BSS Basic Rate)*
Supported Rate: 36.0 *(Not BSS Basic Rate)*
Supported Rate: 48.0 *(Not BSS Basic Rate)*
Supported Rate: 54.0 *(Not BSS Basic Rate)*

WPA
Element ID: 221 *WPA*
Length: 24
OUI: 0x00-0x50-0xF2-0x01
Version: 1
Multicast cipher OUI: 0x00-0x50-0xF2-02 *TKIP*
Number of Unicast 1
Unicast cipher OUI: 0x00-0x50-0xF2-02 *TKIP*
Number of Auths 1
Auth OUI: 0x00-0x50-0xF2-01 *SSN*

Extra bytes (Padding):
.. 00 00
FCS - Frame Check Sequence
FCS (Calculated): 0x0499A2D5

Association Response

Packet Info
Flags: 0x00
Status: 0x00
Packet Length: 40
Timestamp: 14:33:23.627186000 02/10/2004
Data Rate: 2 *1.0 Mbps*
Channel: 1 *2412 MHz*
Signal Level: 47%
Signal dBm: 0
Noise Level: 0%
Noise dBm: 0

802.11 MAC Header
Version: 0
Type: %00 *Management*
Subtype: %0001 *Association Response*
Frame Control Flags: %00000000
0... .... Non-strict order
.0.. .... WEP Not Enabled
..0. .... No More Data
...0 .... Power Management - active mode
.... 0... This is not a Re-Transmission
.... .0.. Last or Unfragmented Frame
.... ..0. Not an Exit from the Distribution System
....0 Not to the Distribution System

Duration: 12059 *Microseconds*
Destination: 00:04:E2:64:BE:08 *SMC Net:64:BE:08*
Source: 00:0B:86:80:18:00 *Aruba Net:80:18:00*
BSSID: 00:0B:86:80:18:00 *Aruba Net:80:18:00*
Seq. Number: 3010
Frag. Number: 0

802.11 Management - Association Response
Capability Info: %0000010000110001
x..... ..... Reserved
.x..... ..... Reserved
..0..... ..... DSSS-OFDM is Not Allowed
...x... ..... Reserved
....0... ..... Robust Security Network Disabled
.....1.. ..... G Mode Short Slot Time [9 microseconds]
......x. ..... Reserved
.......x ..... Reserved
..... 0..... Channel Agility Not Used
..... .0..... PBCC Not Allowed
....1..... Short Preamble
....1.... Privacy Enabled
....0... CF Poll Not Requested
....0.. CF Not Pollable
....0. Not an IBSS Type Network
....1 ESS Type Network

Status Code: 0 *Successful*
Association ID: 0xC001
Supported Rates
Element ID: 1 *Supported Rates*
Length: 4
Supported Rate: 1.0 *(BSS Basic Rate)*
Supported Rate: 2.0 *(BSS Basic Rate)*
Supported Rate: 5.5 *(Not BSS Basic Rate)*
Supported Rate: 11.0 *(Not BSS Basic Rate)*

FCS - Frame Check Sequence
FCS (Calculated): 0xA470AA64