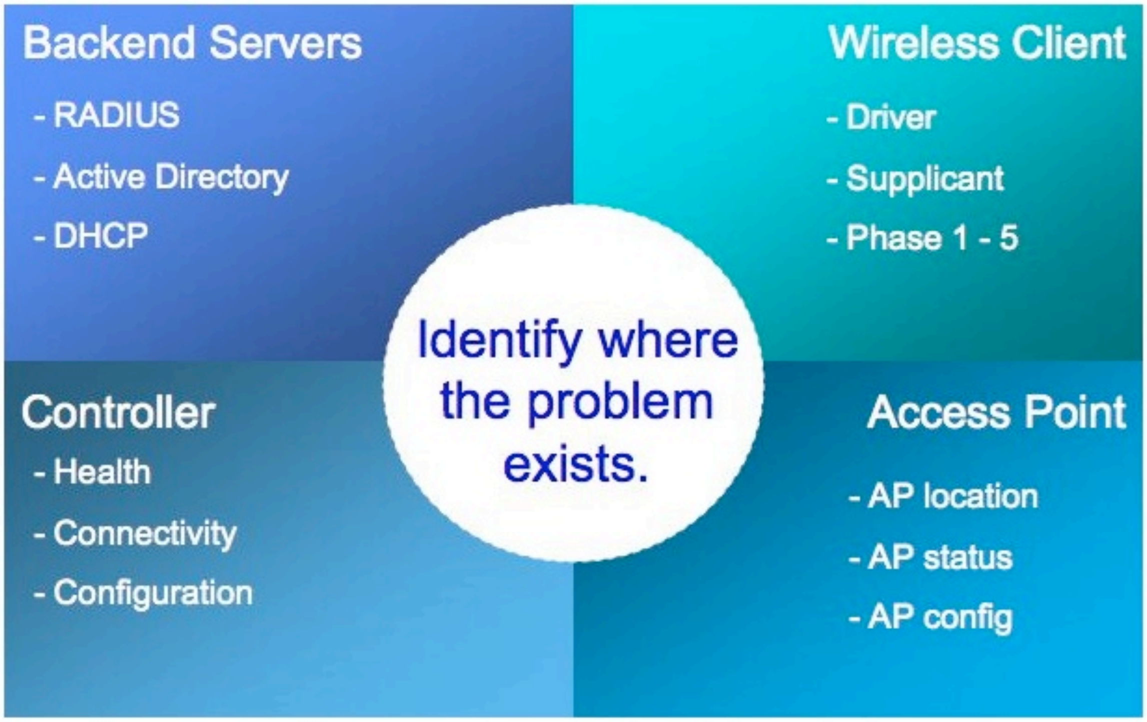
Troubleshooting Cheat Sheet



Backend Servers
- RADIUS
- Active Directory
- DHCP

Wireless Client
- Driver
- Supplicant
- Phase 1 - 5

Identify where the problem exists.

Controller
- Health
- Connectivity
- Configuration

Access Point
- AP location
- AP status
- AP config

Infrastructure Issues

- AP can’t connect to controller
- Master doesn’t see all controllers
- Controller can’t reach other resources
- Poor radio coverage
- VRRP
- Roaming

User Issues

- Can’t see SSID
- Can’t associate
- Can’t authenticate
- No IP Address
- Poor performance
- Dropped connections

Logging

Enable Logging

```
(192.168.2.181) (config) #logging level debugging ?
ap-debug                Debug an AP
bssid-debug             Debug a Bssid
essid-debug             Debug an Essid
network                 Network logs
security                Security logs
system                  System logs
user                    User logs
user-debug              Debug a User
wireless                Wireless logs
```

View Log Files

```
(192.168.2.181) (config) #show log ?
ap-debug                AP Debug Logs
bssid-debug             Bssid Debug Logs
errorlog                Logging for System errors or critical
information
essid-debug             Essid Debug Logs
network                 Network logs
security                Security logs
system                  System logs
user                    User logs
user-debug              User Debug Logs
wireless                Wireless logs
```

```
# show logging level verbose
```

The logging levels follow syslog convention:

- Emergency - A panic condition in which the system becomes unusable.
- Alert - A condition that should be corrected immediately.
- Critical - Critical conditions, e.g., hard device errors.
- Errors – Error conditions.
- Warning – Warning messages
- Notice – Normal but significant conditions
- Informational - Informational messages.
- Debug - Messages that contain information normally of use only when debugging a particular module.

The default level is “informational”

Packet Captures

Port mirroring

E.g., All traffic sent to/from interface 1/0 to be copied to interface 1/22

```
(Aruba2400) (config) #interface fastethernet 1/22
(Aruba2400) (config-if)#port monitor fastethernet 1/0
```

Session mirroring

In the GUI when creating a session check the “Mirror” box

```
(Aruba800) (config-sess-test)#user network 10.10.10.0 255.255.255.0
svc-dns permit mirror
```

Air capture (AP/AM)

Capture AP Radio traffic: Select an AP from “Switch > Access Points” and click on “Packet Capture” button, then select either the 802.11a or 802.11g radio. The controller will set up the capture filters to capture the selected AP Radio traffic and will send to the packet capturing client’s “Target IP” address.

Either Ethereal or AiroPeek will need to be running on device set as “Target IP” listening on the UDP port (UDP 5000 for Aeropeek or UDP 5555 for Ethereal)

PCAP

```
(Aruba2400) #packet-capture tcp all
(Aruba2400) #packet-capture udp all
(Aruba2400) #show packet-capture
Current Active Packet Capture Actions(current switch)
=====================================================
Packet filtering for all TCP ports enabled.
Packet filtering for all UDP ports enabled.
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets disabled.
Packet Capture Defaults(across switches and reboots if saved)
=====================================================
Packet filtering for TCP ports disabled.
Packet filtering for UDP ports disabled.
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets disabled.
(Aruba2400) #
(Aruba2400) #tar logs
(Aruba2400) #dir
-rw-r--r--    1 root     root        17190 Aug 10 02:55 aug10.cfg
-rw-r--r--    1 root     root        16451 Aug 10 05:45 default.cfg
-rw-r--r--    1 root     root       344064 Sep  4 05:51 logs.tar
(Aruba2400) #copy flash: logs.tar tftp: 172.16.0.251 logszzz.tar
```

Untar to retrieve filter.pcap file

Controller Zone

Hardware, software and process health

```
show cpuload

show memory

show inventory

show switchinfo
```

Look for ArubaOS version, boot partition, switch role (master or local)

```
show image version

show datapath utilization

show processes
```

Please send the file that is generated from “tar logs tech-support” to Aruba Technical support if you see any process in a state of “z” or “t” under the “S” column.

```
show storage
```

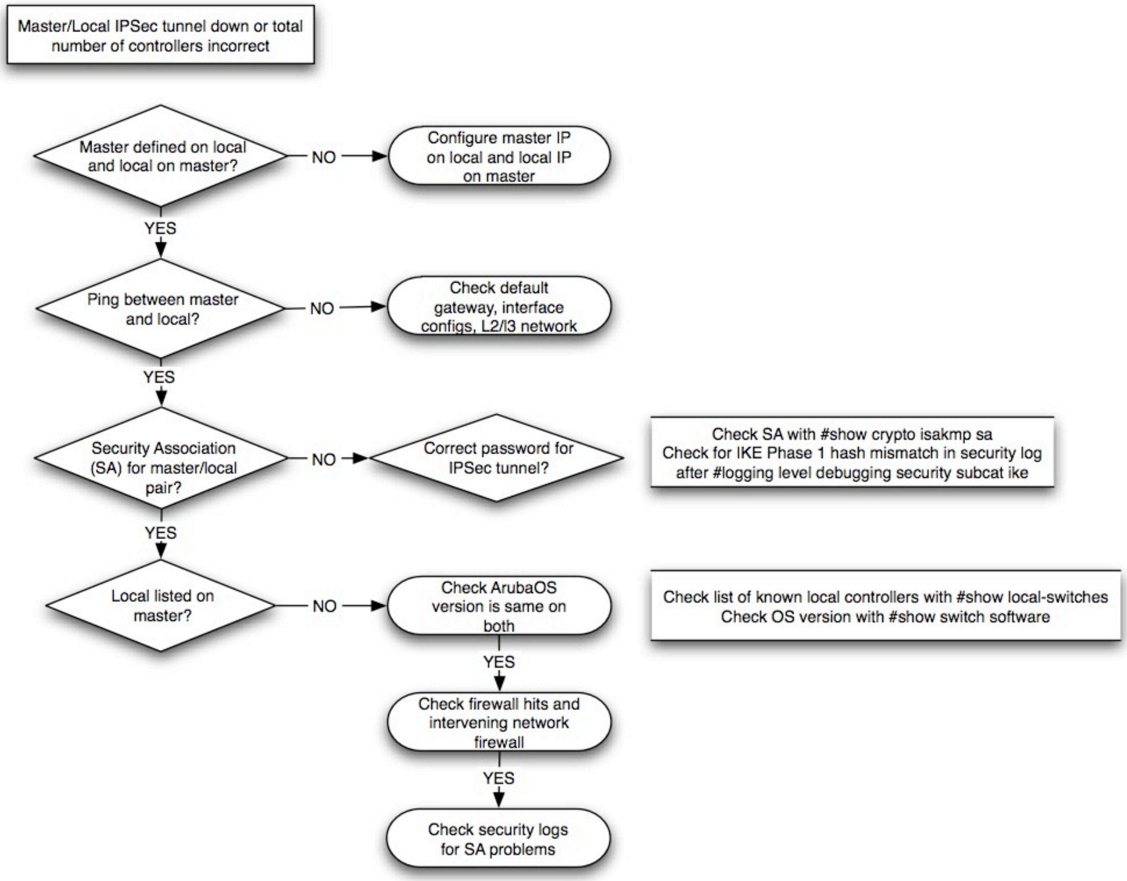
Keep /flash to more the 10MB free space

```
show netstat
```

L2/L3 information

```
show ip interface brief

show ip route

show interface fastethernet <slot>/<port>

show interface fastethernet <slot>/<port> switchport

show interface vlan <vlanid>

show interface counters

show arp

show datapath route table

show datapath route-cache table

show datapath bridge table

show datapath bridge counters

show datapath frame counters

show datapath crypto counters
```

Local can’t communicate with master


Master/Local IPSec tunnel down or total number of controllers incorrect
Master defined on local and local on master?
NO
Configure master IP on local and local IP on master
YES
Ping between master and local?
NO
Check default gateway, interface configs, L2/l3 network
YES
Security Association (SA) for master/local pair?
NO
Correct password for IPSec tunnel?
Check SA with #show crypto isakmp sa
Check for IKE Phase 1 hash mismatch in security log after #logging level debugging security subcat ike
YES
Local listed on master?
NO
Check ArubaOS version is same on both
Check list of known local controllers with #show local-switches
Check OS version with #show switch software
YES
Check firewall hits and intervening network firewall
YES
Check security logs for SA problems

Basic commands

```
(Aruba200) # show datapath tunnel table
```

Look for inbound and outbound IPSec tunnels

```
(Master) #show crypto isakmp sa
```

```
(Master) #show log security
```

Look for:

```
IKE Aggressive Mode Phase 1 succeeded for peer <ip address>
ike_quick_mode.c:checkIpsecSelectors_LocalMaster:3601 ipsec_map peer
IP:0.0.0.0 SA IP:<ip address> map_name default-local-master-ipsecmap
```

Wrong IKE passphrase

```
(Master) (config) #logging level debugging security subcat ike
```

Look for:

```
IKE Phase 1 hash mistmatch.  Most likely because IKE pre-shared key or
certificate mismatch
```

VRRP Issues

Correct interfaces in same VLAN?
Preempt enabled?
Active/Standby roles at correct locations?
Priority value set?
Passwords enabled and/or matching?
L2 connectivity exist between participants?
Controllers running same code level?
AP L3 connectivity to standby device when failover occurs?

Basic commands

```
(Aruba200) #show vrrp statistics 1
```

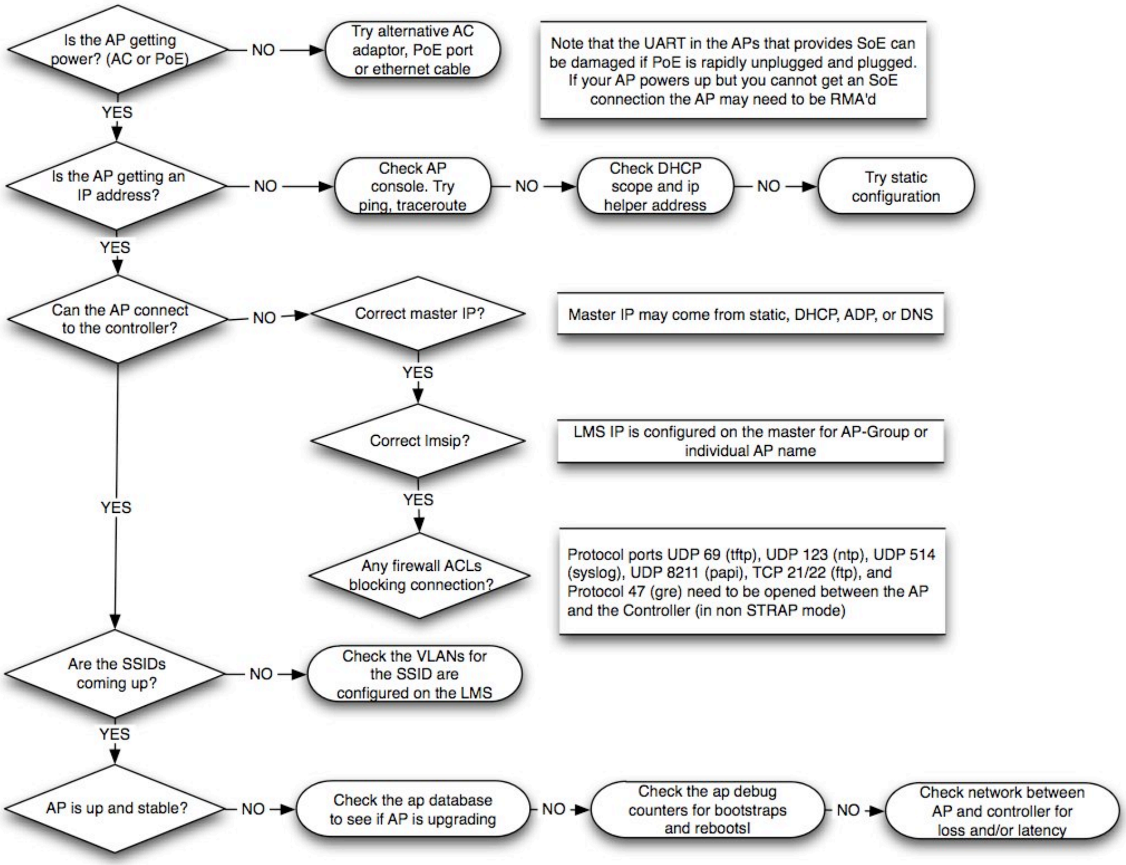
Look at Admin State, VR State, Advertisements sent and received, authentication failures

```
(Aruba200) #show log network
```

Look for messages from fpapps

AP Zone

AP config and bootup


Is the AP getting power? (AC or PoE)
NO
Try alternative AC adaptor, PoE port or ethernet cable
YES
Is the AP getting an IP address?
NO
Check AP console. Try ping, traceroute
NO
Check DHCP scope and ip helper address
NO
Try static configuration
YES
Can the AP connect to the controller?
NO
Correct master IP?
YES
Correct lmsip?
YES
Any firewall ACLs blocking connection?
YES
Are the SSIDs coming up?
NO
Check the VLANs for the SSID are configured on the LMS
YES
AP is up and stable?
NO
Check the ap database to see if AP is upgrading
NO
Check the ap debug counters for bootstraps and reboots!
NO
Check network between AP and controller for loss and/or latency

Note that the UART in the APs that provides SoE can be damaged if PoE is rapidly unplugged and plugged. If your AP powers up but you cannot get an SoE connection the AP may need to be RMA'd

Master IP may come from static, DHCP, ADP, or DNS

LMS IP is configured on the master for AP-Group or individual AP name

Protocol ports UDP 69 (tftp), UDP 123 (ntp), UDP 514 (syslog), UDP 8211 (papi), TCP 21/22 (ftp), and Protocol 47 (gre) need to be opened between the AP and the Controller (in non STRAP mode)

AP basic commands

```
(Aruba200) #show ap database
```

AP may be upgrading or rebooting

```
(Aruba200) #show ap debug counters ap-name <ap-name>
```

Check for incrementing bootstrap or reboot counter

```
(Aruba200) # show ap active

(Aruba200) # show ap bss-table

(Aruba200) # show datapath tunnel table

(Aruba200) # show ap config ap-name <ap-name>

# show datapath session table <ap-ip>
```

Look for GRE (protocol 47) and PAPI (UDP port 8211)

Use Serial over Ethernet

```
(config)# telnet soe
telnet <controller-ip> 2300
```

```
Trying 192.168.0.100...
Connected to 192.168.0.100.
Escape character is '^]'.

User: admin
Password: *******
Available commands:
  connect <slot/port>
  exit (no args)
soe> connect 1/1
```

AP 'show tech'

```
show ap tech-support ap-name <ap-name>
```

```
Protocol ports UDP 69 (tftp), UDP 123 (ntp), UDP 514 (syslog), UDP 8211
(papi), TCP 21/22 (ftp), and Protocol 47 (gre) need to be opened
between the AP and the Controller (in non STRAP mode)
```

```
(Aruba200) #show profile-errors
```

VLANs for SSID may not be configured on the LMS

GRE heartbeat (default value is 8)

```
ap system-profile <system prof name> bootstrap-threshold <number of
missed heartbeats>
```

PAPI heartbeat (default value is 10 retries, 60 second interval, 10 request retries)

```
ap system-profile <system prof name> max-request-retries <maximum
number of retries>

ap system-profile <system prof name> keepalive-interval <value in
seconds>

ap system-profile <system prof name> request-retry-interval <value in
seconds>
```

Poor RF Coverage

Basic commands

```
(Aruba200) #show ap arm rf-summary ip-addr <ap ip address>
```

Interference index column displays the measured interference and is used to determine the best channel. The format for the column is a/b/c/d where:
A=That AP's measure of co-channel interference
B=That AP's measure of adjacent channel interference
C=The neighbor AP's measure of co-channel interference
D=The neighbor AP's measure of adjacent channel interference

To determine the best channel, add the four values together. The best channel will have the lowest value. By default, an AP will not switch channels unless the better measurement is at least twenty-five (25) less than the current channel assignment.

```
(Aruba200) #show ap active ip-addr <ap ip address>
```

Check to make sure:

- Channel Frame Retry Rate % is below 30%. If higher then too much interference.
- Channel Noise Floor is above 80. If Noise Floor is lower then too much non-802.11 interference

```
(Aruba200) #show ap monitor ap-list ip-addr <ap ip address>
```

Check for interferencing APs

Link quality

```
#rft test profile link-quality ip-addr 192.168.2.11 dest-mac
00:40:96:a4:e7:c1
Transaction ID: 1

# show rft result trans-id 1
```

Antenna connectivity

```
# show rft profile antenna-connectivity

#rft test profile antenna-connectivity ip-addr 172.16.100.101 dest-mac
00:15:00:26:f8:f5  phy a
Transaction ID: 1

#show rft result trans-id 1
```

Raw profile

```
#rft test profile raw ip-addr 172.16.100.101 dest-mac 00:15:00:26:f8:f5
phy a
Transaction ID: 1001

#show rft result trans-id 1001
```

Backend Server Zone

Radius

Check that Radius server is properly configured and that a user account can authenticate

```
show aaa authentication-server all
```

Check if Inservice and Requests count is increasing

```
aaa test-server <radius-server-name> <username> <password>
```

In ArubaOS3.1 or earlier - PAP only. PAP must be enabled on Radius server
Most common error is to not enable dial-up for a user in AD

```
aaa test-server pap <radius-server> <username> <password>

aaa test-server mschapv2 <radius-server-name> <username> <password>

show aaa authentication-server radius <radius-server-name>
```

Initial starting point for user debugging:

```
logging level informational user
```

Gives you info on server selection and role derivation in one place (show log user)

```
show auth-tracebuf mac <user mac>
```

More detailed debugging:

```
(Aruba200) (config) #logging level debugging user-debug <user mac>

show log user-debug all | include <mac addr>
```

Other logging you can try:

```
(Aruba200) (config) #logging level debugging network

(Aruba200) (config) #logging level debugging security subcat dot1x

(Aruba200) (config) #logging level debugging security subcat aaa

(Aruba200) (config) #logging level debugging security process authmgr
subcat all

(Aruba200) (config) #logging level debugging user subcat dot1x

packet-capture udp <radius port>
```

Do a ‘tar logs’, move the logs.tar to server, untar and look for filter.pcap

If IAS/AD then check the Event Viewer on the server

If SBR check the Statistics page in SBR Administrator and log files (C:\Radius\Service)

DHCP

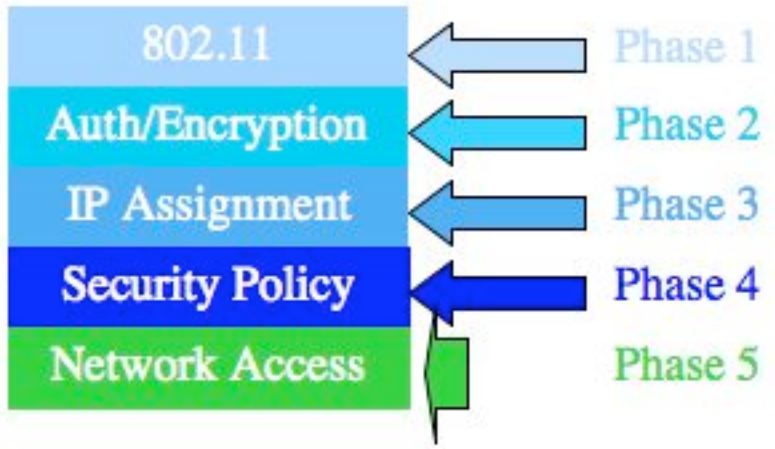
```
(Aruba200) (config) #logging level debugging network subcat dhcp
```

If Windows server check the Event Viewer on the server and look in DHCP config to confirm that scope exists and check Leases to see if any clients have obtained IP addresses

Check that wired switches have ‘ip helper-address’ properly set

If Aruba is DHCP server check that DHCP service is enabled (in GUI need to check the DHCP service box, click apply and then create scopes - cannot do both at the same time)

Wireless Client Zone



Client cannot find AP

Multiple Users
Hidden SSID/Disabled Probe Response
AP Offline
AP Provisioned as AM
SNR/Interference issues

Single User
Wrong radio band (e.g. 802.11b/g only NIC in an 802.11a network)
Driver issue
Wireless adapter disabled
Failed NIC

Client cannot associate

Shared authentication rather than Open/WPA/WPA2
SNR
Driver
NIC problem
Blacklisted
DoS
Minimum supported/basic rate may be higher than client supports

Track down the client

1. Get the MAC address of the wireless device

2. Find what BSSID the station is associated with (use AP troubleshooting if problems here)

```
show wms client <wireless device mac address>
```

3. Find which Controller the AP is connected with

```
show ap database long | include <AP name>
```

4. Log on to the Controller and search for the user

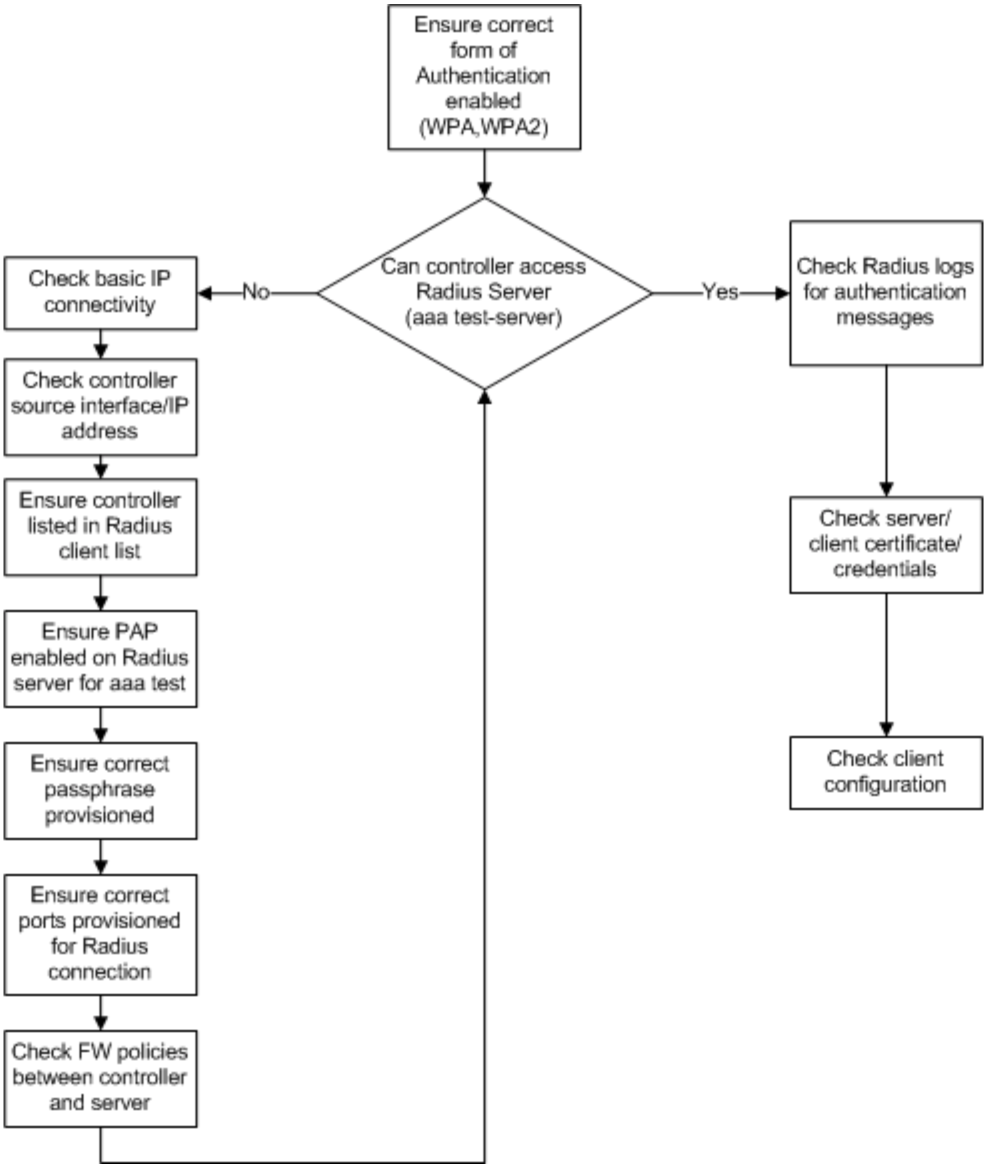
```
show user mac <wireless device mac address>
```

802.11 Negotiation

```
logging level debugging security process authmgr subcat packet-trace
logging level debugging user-debug 00:16:cf:af:bb:e2 subcat all

show logging level verbose
show ap debug mgmt-frames client-mac <mac address>
show log user-debug all | include <mac address>
show log user all | include <mac address>
```

Use AP remote packet capture to analyze 802.11 negotiation

Client cannot authenticate - 802.1x


Ensure correct form of Authentication enabled (WPA,WPA2)
Can controller access Radius Server (aaa test-server)
No
Yes
Check basic IP connectivity
Check controller source interface/IP address
Ensure controller listed in Radius client list
Ensure PAP enabled on Radius server for aaa test
Ensure correct passphrase provisioned
Ensure correct ports provisioned for Radius connection
Check FW policies between controller and server
Check Radius logs for authentication messages
Check server/ client certificate/ credentials
Check client configuration

Enable 802.1x related debugging

```
logging level debugging network process dhcpd subcat dhcp
logging level debugging network process dhcpd subcat packet-dump
logging level debugging security process authmgr subcat dot1x
logging level debugging security process authmgr subcat packet-trace
logging level debugging user process authmgr subcat dot1x
logging level debugging user process authmgr subcat radius
logging level debugging user-debug <client mac> subcat all
```

View debug output

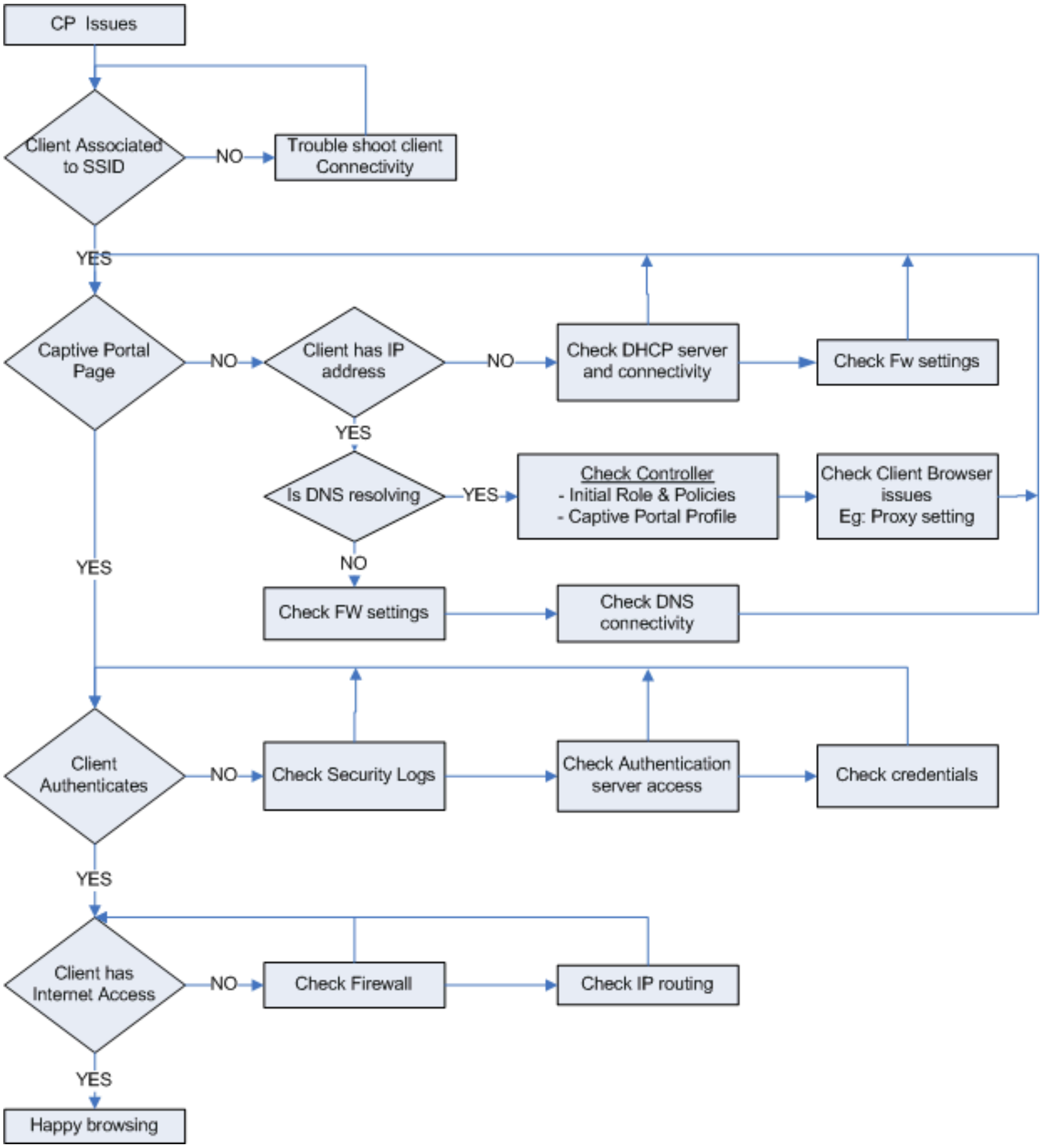
```
show logging level verbose
show ap debug mgmt-frames client-mac <mac address
show log user-debug all | include <mac address>
show log user all | include <mac address>
show log network all | include <mac address>
show log security all | include authmgrshow auth-tracebuf mac <client
mac>
show dot1x supplicant-info list-all
show dot1x supplicant-info statistics
show dot1x counters
```

Validate client certificates - check date, signature and status

Make sure client has the correct certificate selected in “Validate server certificate”

Make sure client has correct EAP settings - machine authentication on/off, windows domain logon credentials on/off,

Client cannot authenticate - Captive Portal



Most common errors:

- Forgetting to assign a captive portal role to the initial (logon) role
- DNS cannot be resolved so redirection doesn't work (try http://1.1.1.1 or some IP address to check if this is the cause)
- Client has proxy settings which are preventing access to the captive portal

Client cannot obtain IP address

See DHCP debugging section in Backend Server Zone

Check VLAN assignment for the SSID - is there a DHCP scope?

General notes on client connectivity

- Network Card Driver controls association, roaming, and encryption/decryption
- WZC controls to which network the supplicant will connect
- 802.1x controls authentication and key exchanges/updates
- Always upgrade to the latest driver (after its tested on a lab laptop first)
- Always upgrade to the latest supplicant (after its tested on a lab laptop first)
- Keep the default driver configuration settings.

Common issues:

Inability to connect to the SSID

- Incorrect wireless config on the client's supplicant
- Incorrect config of authentication types/unsupported EAP types
- Authentication delays
- Missing CA certificates
- New Controller is not added to the approved RADIUS client list
- Check Controller CLI show ap debug mgmt-frames client-mac <client mac>

Intermittent connectivity

- Check if machine auth is enabled/disabled on both client and Controller
- Check Controller CLI

```
      show ap debug mgmt-frames client-mac <client mac>
```

- if client debug enabled with

```
      logging level debugging user-debug <client mac address>
      show log user all and show log user-debug all
```

Security Policy Issues

What role was assigned to the user?
How was the role derived?

```
#show user ip <ip address>
```

Will list role and how it was derived. It will also list the authentication protocol, authentication server

```
#show rights <role>
```

Check the session ACLs in the role that was assigned to the user. It will also indicate the ACL number

```
#show datapath acl <acl number>
```

More details on the ACL in the user role

Network Access Issues

```
show datapath session table <client ip>
```

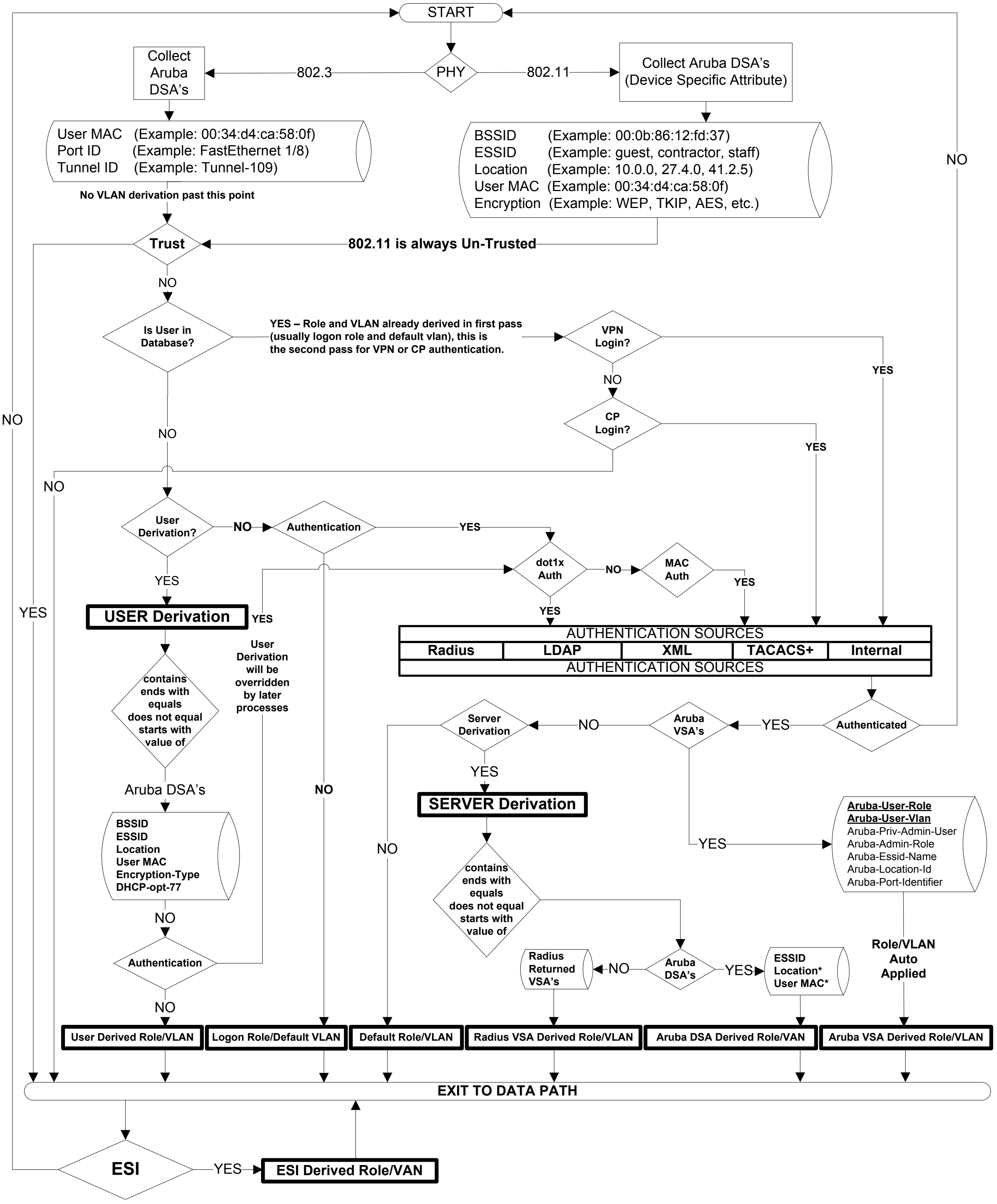
The most commonly used command - look for “D” flags which means the firewall policy is blocking access

Session mirroring

Use session mirror to debug application level issues - after L2 encryption is removed (cannot do this with wireless sniffing). You may want to avoid turning on mirroring for all users in a role. In that case create a new session ACL and a new role for the specific user or otherwise limit the traffic.

```
(config) #ip access-list session mirror_acl
(config-sess-mirror_acl) #any any any permit mirror
(config-sess-mirror) #exit
(config) #firewall session-mirror-destination ip-address <target ip>
```

Role Derivation


START
PHY
802.3
802.11
Collect Aruba DSA's
Collect Aruba DSA's (Device Specific Attribute)
User MAC (Example: 00:34:d4:ca:58:0f)
Port ID (Example: FastEthernet 1/8)
Tunnel ID (Example: Tunnel-109)
No VLAN derivation past this point
BSSID (Example: 00:0b:86:12:fd:37)
ESSID (Example: guest, contractor, staff)
Location (Example: 10.0.0, 27.4.0, 41.2.5)
User MAC (Example: 00:34:d4:ca:58:0f)
Encryption (Example: WEP, TKIP, AES, etc.)
Trust
802.11 is always Un-Trusted
NO
Is User in Database?
YES – Role and VLAN already derived in first pass (usually logon role and default vlan), this is the second pass for VPN or CP authentication.
VPN Login?
YES
NO
CP Login?
YES
NO
NO
NO
NO
User Derivation?
NO
Authentication
YES
dot1x Auth
NO
MAC Auth
YES
YES
YES
USER Derivation
YES
YES
User Derivation will be overridden by later processes
AUTHENTICATION SOURCES
Radius
LDAP
XML
TACACS+
Internal
AUTHENTICATION SOURCES
contains ends with equals does not equal starts with value of
Aruba DSA's
BSSID
ESSID
Location
User MAC
Encryption-Type
DHCP-opt-77
NO
Authentication
NO
NO
Server Derivation
NO
Aruba VSA's
YES
Authenticated
NO
YES
SERVER Derivation
NO
YES
Aruba-User-Role
Aruba-User-Vlan
Aruba-Priv-Admin-User
Aruba-Admin-Role
Aruba-Essid-Name
Aruba-Location-Id
Aruba-Port-Identifier
contains ends with equals does not equal starts with value of
Role/VLAN Auto Applied
Radius Returned VSA's
NO
Aruba DSA's
YES
ESSID
Location*
User MAC*
User Derived Role/VLAN
Logon Role/Default VLAN
Default Role/VLAN
Radius VSA Derived Role/VLAN
Aruba DSA Derived Role/VAN
Aruba VSA Derived Role/VLAN
EXIT TO DATA PATH
ESI
YES
ESI Derived Role/VAN