ArubaOS 6.1.3.1-RNG

Release Notes

ArubaOS 6.1.3.1-RNG is the companion controller release for the Aruba Instant 6.1.3.1-3.0.0.0 release. This controller release provides an ability to terminate VPN and GRE tunnels from the Instant AP and provides corporate connectivity to the branch Instant AP network. For details on all the features described in the following sections, see the *Aruba Instant 6.1.3.1-3.0.0.0 User Guide*.

VPN features are ideal for:

- enterprises with many branches that do not have a dedicated VPN connection to the HQ.
- branch offices that require multiple APs.
- individuals working from home, connecting to the VPN.

This new architecture and form factor seamlessly adds the survivability feature of Instant APs with the VPN connectivity of RAPs — providing corporate connectivity to branches.

All Aruba controllers that are supported on the ArubaOS 6.1.x release will work on RNG 6.1.3.1.

What's New in this Release

This section provides a brief summary of the new features included in this release of Aruba Instant.

Termination of IAP VPN tunnels

IAPs have the ability to terminate VPN tunnels on controllers. The IAP cluster creates a tunnel from the Virtual Controller to an Aruba mobility controller in your corporate office. The controller acts a VPN end-point and does not provide the Instant AP with any configuration. For more information on how to create a VPN tunnel from Virtual Controller to an Aruba mobility controller, see the *Aruba Instant 6.1.3.1-3.0.0.0 User Guide*.

Termination of IAP GRE tunnels

IAPs have the ability to terminate GRE tunnels on controllers. The IAP cluster creates a tunnel from the Virtual Controller to an Aruba mobility controller in your corporate office. The controller acts a GRE end-point and does not provide the Instant AP with any configuration. For more information on how to create a GRE tunnel from Virtual Controller to an Aruba mobility controller, see the *Aruba Instant 6.1.3.1-3.0.0.0 User Guide*.

L2/L3 network mode support

The Virtual Controller (VC) on an Instant AP enables different DHCP pools (various deployment models) in addition to allocating IP subnets to each branch. The following modes of DHCP server are supported:

- L2 Switching Mode: In this mode, Instant supports distributed L2 and centralized L2 switching modes of connection to corporate. When an Instant AP registers with the controller and has a L2 mode DHCP pool configured, the controller automatically adds the GRE or VPN tunnel associated to this IAP into the VLAN multicast table. This allows the clients connecting to this L2 mode VLAN to be part of the same L2 domain on controller.
- L3 Routing Mode: In this mode, Instant supports L3 routing mode of connection to corporate. The VC assigns an IP addresses from the configured subnet and forwards traffic to both corporate and non-corporate destinations. Instant AP takes care of routing on the subnet and also adds a route on the controller after the VPN tunnel is set up during the registration of the subnet. When the Instant

AP registers with a L3 mode DHCP pool, the controller automatically adds a route to this DHCP subnet enabling routing of traffic from the corporate to clients on this VLAN in the branch.

VPN Configuration

The following VPN configuration steps on the controller, enable IAPs to terminate their VPN connection on the controller:

Whitelist DB Configuration

Controller Whitelist DB

You can use the following CLI command to configure the whitelist DB if the controller is acting as the whitelist entry:

```
(Aruba3400) #local-userdb-ap add mac-address 00:11:22:33:44:55 ap-group test
(Aruba3400) #
```

The `ap-group` parameter is not used for any configuration, but needs to be configured. The parameter can be any valid string. If an external whitelist is being used, the MAC address of the AP needs to be saved in the Radius server as a lower case entry without any delimiter.

External Whitelist DB

The external whitelist functionality enables you to configure the RADIUS server to use an external whitelist for authentication of MAC addresses of RAPs.

If you are using Windows 2003 server, perform the following steps to configure external whitelist on it. There are equivalent steps available for Windows Server 2008 and other RADIUS servers.

1. Add the MAC addresses for all the RAPs in the Active Directory of the Radius server:
   a. Open the **Active Directory and Computers** window, add a new user and specify the MAC address (without the colon delimiter) of the RAP for the user name and password.
   b. Right-click the user that you have just created and click **Properties**.
   c. In the **Dial-in** tab, select **Allow access** in the **Remote Access Permission** section and click **OK**.
   d. Repeat Step a through Step b for all RAPs.
2. Define the remote access policy in the Internet Authentication Service:
   a. In the **Internet Authentication Service** window, select **Remote Access Policies**.
   b. Launch the wizard to configure a new remote access policy.
   c. Define filters and select select **grant remote access permission** in the **Permissions** window.
   d. Right-click the policy that you have just created and select **Properties**.
   e. In the **Settings** tab, select the policy condition, and **Edit Profile...**.
   f. In the **Advanced** tab, select **Vendor Specific,** and click **Add** to add new vendor specific attributes.
   g. Add new vendor specific attributes and click **OK**.
   h. In the **IP** tab, provide the IP for the RAP and click **OK**.

VPN Local Pool Configuration

The VPN local pool is used to assign an IP Address to the IAP after successful XAUTH VPN.

```
(Aruba3400) # ip local pool "rapngpool" <startip> <endip>
(Aruba3400) #
```

VPN Profile Configuration

The VPN profile configuration defines the server used to authenticate the IAP (internal or an external server) and the role for IAP user. This role is used to define `src-nat` rule to Radius server to get Dynamic Radius proxy working.

```
(Aruba3400) (config) #ip access-list session iaprole
(Aruba3400) (config-sess-iaprole)#any host <radius-server-ip> any src-nat
(Aruba3400) (config-sess-iaprole)#any any any permit
(Aruba3400) (config-sess-iaprole)#!
(Aruba3400) (config) #user-role iaprole
(Aruba3400) (config-role) #session-acl iaprole
(Aruba3400) (config-role) #
(Aruba3400) (config) #aaa authentication vpn default-iap
(Aruba3400) (VPN Authentication Profile "default-iap") #server-group default
(Aruba3400) (VPN Authentication Profile "default-iap") #default-role iaprole
(Aruba3400) (VPN Authentication Profile "default-iap") #!
(Aruba3400) (config) #
```

For more information on VPN profile configuration, see the *Aruba Instant 6.1.3.1-3.0.0.0 User Guide*.

Radius proxy for VPN connected IAPs

The Radius proxy for VPN conntected IAPs functionality defines the server used to authenticate the IAP (internal or an external server) and the role for IAP user. This role is used to define src-nat rule to Radius server to get Dynamic Radius proxy working.

```
(Aruba3400) (config) #ip access-list session iaprole
(Aruba3400) (config-sess-iaprole)#any host <radius-server-ip> any src-nat
(Aruba3400) (config-sess-iaprole)#any any any permit
(Aruba3400) (config-sess-iaprole)#!
(Aruba3400) (config) #user-role iaprole
(Aruba3400) (config-role) #session-acl iaprole
(Aruba3400) (config-role) #
(Aruba3400) (config) #aaa authentication vpn default-iap
(Aruba3400) (VPN Authentication Profile "default-iap") #server-group default
(Aruba3400) (VPN Authentication Profile "default-iap") #default-role iaprole
(Aruba3400) (VPN Authentication Profile "default-iap") #!
(Aruba3400) (config) #
```

For more information on configuration of RADIUS proxy for VPN connected IAPs, see the *Aruba Instant 6.1.3.1-3.0.0.0 User Guide*.

Viewing branch status

To view the details of the branch information connected to the controller, issue the `show iap table` command.

Example

This example shows the details of the branches connected to the controller.

```
(Aruba3400) (config) #show iap table
```

```
Branch Key                                                       Index Status  Inner IP        MAC Address
----------                                                       ----- ------  --------        -----------
d8f6095a01f89b7aea4340c080c3e3c8bd062758461c32c92d                 8     DOWN   0.0.0.0         d8:c7:c8:c0:01:6c
4619fa8b014ff058d99e9fe63286c19851e61466627d054968                 16    DOWN   0.0.0.0         00:1a:1e:08:21:e1
0e26e65a01732247f98b5d463f1fb56c0200d0944fab521e57                 3     DOWN   0.0.0.0         d8:c7:c8:c0:01:6c
cc0b838d014df7db3eb453ef4f513204df4d74bb4063e46587                 7     DOWN   0.0.0.0         d8:c7:c8:c0:b8:d0
6bccde5901997e534d14b10580371792ef4c13ca868c929150                 15    DOWN   0.0.0.0         d8:c7:c8:c0:01:6c
764f6038018f2c2765292911e55fedc0c98f86cf79331d8905                 6     UP     10.15.207.206   00:24:6c:c9:27:cf
c2b46b530119844dcbdb55ddb94ff308d1f08ec7cb4eda113c                 0     DOWN   0.0.0.0         d8:c7:c8:c0:b8:d6
9deb828c0106f4562b50c8141cfa28ad5c1a3f89b3e171efcc                 14    DOWN   0.0.0.0         00:1a:1e:08:23:f4
be5ffcf801eedd92a76b978ceee53f4e2284c8e8f3dbd84457                 5     DOWN   0.0.0.0         00:24:6c:c9:27:cf
b5d279460166c39a5fb9462a65559eb91266b9ac9f8e2356a0                 13    DOWN   0.0.0.0         d8:c7:c8:c0:01:6c
0f7057990174cde7901a0c8779baeb7393b26d974a45eb8602                 10    DOWN   0.0.0.0         00:24:6c:c0:41:f2
a1e23c1201cfb76a50fb3328e58c9825e716a259dd71874c67                 4     UP     10.15.207.207   00:24:6c:c9:18:64
47f930fc019317069d04fd1c2ffdf6a49a6e51c148c2164ed0                 9     DOWN   0.0.0.0         d8:c7:c8:c0:01:6c
0c478ce101df81e3c0a46fe4f3ab6eca9bb012151dea99a82f                 1     DOWN   0.0.0.0         d8:c7:c8:c0:01:6c
747c20ac0155736c3b11bd972c967ebdf7c9883e69ec2a01fb                 2     DOWN   0.0.0.0         d8:c7:c8:c0:b8:d0
0e40138601b34eb33fb57d94208848b0f8e37bba0a6a0d43ca                 12    DOWN   0.0.0.0         00:24:6c:c9:18:64
de2939190191967c8ac8f04a50fbd5b96c2af3d3576aa1dc2                  11    DOWN   0.0.0.0         d8:c7:c8:c0:b8:d8
208c416e01e1cfaf0fdc11190349ad43334879f39ba9e19188                 17    DOWN   0.0.0.0         d8:c7:c8:c0:01:6c

(Aruba3400) (config) #
```

The output of this command includes the following parameters:

Parameter	Description
Branch Key	Key for the branch, which is unique to each branch.
Index	Index assigned to the branch.
Status	Current status of the branch (UP/DOWN).
Inner IP	VPN inner IP of the branch.
MAC Address	MAC address of the VC of the branch.

Known Issues

The following is the known issue for RNG 6.1.3.1 release.

Table 1 *Known Issues*

Bug ID	Description
59380	Each L3 mode user on IAP consumes one user license on controller. This is in addition to the AP's VPN entry consuming a user license **Workaround:** None.

Contacting Support

Table 2 *Web Sites and Emails*

Web Site	
• Main Site	http://www.arubanetworks.com
• Support Site	https://support.arubanetworks.com
• Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support/wsirt.php
Support Emails	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

Table 3 *Contact Phone Numbers*

Telephone Numbers	
• Aruba Corporate	+1 (408) 227-4500
• FAX	+1 (408) 227-4550
Support	
United States	800-WI-FI-LAN (800-943-4526)
Universal Free Phone Service Number (UIFN): Australia, Canada, China, France, Germany, Hong Kong, Ireland, Israel, Japan, Korea, Singapore, South Africa, Taiwan, and the UK	+800-4WIFI-LAN (+800-49434-526)
All other countries	+1 (408) 754-1200