Network flow, security, and performance policies are applied to all traffic from users who have successfully authenticated into any wired port or wireless SSID. Policies are defined by means of a role derivation process utilizing the configuration profiles in the AP group assigned to that AP.

Figure 40 *Role Derivation Flowchart*

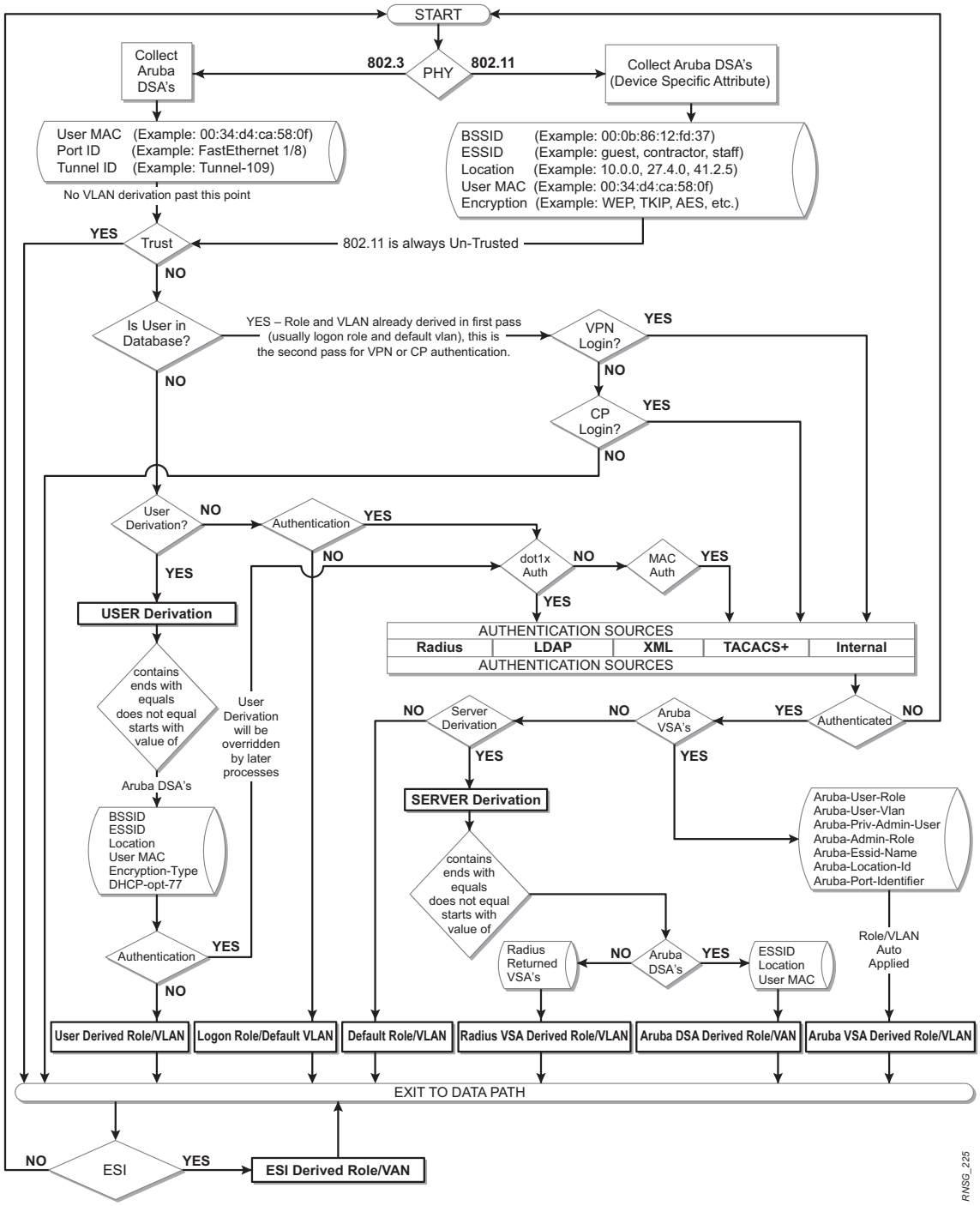

Figure 40 shows the logic tree associated with the role derivation process, which is applied individually to every wired and wireless device that attempts to authenticate to an Aruba network. For example, high-security and legacy users are placed on a VLAN with access to internal network resources; you can further refine this setup with sophisticated firewall rules applied on a per-packet basis. For example, a dual-mode Wi-Fi voice device is placed on a voice-only VLAN and only permitted to contact a SIP server and transmit RTP traffic. Any attempt by the device to do something else would automatically 'blacklist'