Configuration Notes of NAC

When configuring NAC on a device, pay attention to the following points:

- 802.1X client authentication software is required on the supplicant when you use the 802.1X authentication to control the network access of the supplicant. If you only use MAB authentication to control network access of the clients, the 802.1X client software is not required.
- The MAB authentication is performed each time when the port link goes down and then up.
- 802.1X authentication is used on the port connected to the host user. It is not supported for the port connected to the AAA server.
- It is strongly recommended not to use both voice VLAN and dynamic VLAN on the port enabled with NAC function.
- The link type for the port of dynamic VLAN should be trunk port.
- 802.1X authentication only supports RADIUS protocol between the authenticator and the authentication server. It does not support TACACS /TACACS+ authentication.
- A maximum of eight NAC authenticated users are supported on each port.
- 802.1X authentication and MAB authentication cannot be configured on a LAG port or a physical port that belongs to a LAG. When we need to configure these functions on the physical port that belongs to a LAG, we must first remove the physical port from the LAG port before configuration.
- The recommended AAA servers are ClearPass, ISE and PacketFence.
- The link type of the port used for NAC function should be trunk port.
- The static firewall filter rule (set by the commands **set firewall filter** *XX*) cannot be applied to the port used for NAC function. Similarly, if a static firewall filter rule is applied to a port, then the port cannot employ NAC.
- The Web authentication process relies on MAB authentication. If you want to deploy Web authentication, you need to enable MAB authentication on the switch first.
- In CLI configuration, you need to enable MAB authentication before enable CWA authentication.
- The CWA authentication process will be implemented after the MAB authentication fails.
- Three AAA servers can be configured (using command **set protocols dot1x aaa radius authentication server-ip** <ipv4-address> [**shared-key** <*key-string*>]); only one Web authentication server can be configured (using command **set protocols dot1x aaa web server-ip** <*ipv4-address*> **port** <*port-number*>).
- For the NAC authentication, if dynamic VLAN is not provided by the AAA server, the native VLAN will be used instead.
- The static MACs also need to be authenticated if the port is enabled with NAC.
- Rapid PVST+ blocks traffic from the dynamic VLAN delivered from the RADIUS authentication server.