Pica8 Technote: Automate NAC Configurations

Automate Network Access Control Configurations for Access Switches

Automate Network Access Control Configurations for Access Switches

This document provides details on best practices for Network Access Control (NAC) configurations and how to automate NAC configurations for Access Switches.

Best Practice NAC configurations with PicOS Software

Configurations are color coded as follows to simplify the automated config generation process:

- **Blue color configuration** – Configuration common between all Access Switches
- **Purple color configuration** – Access Switch specific configuration. This configuration's command set varies between different switches
- **Red color configuration** – Security configuration that is common between all switches
- **Green color configuration** – NAC configuration for all access ports

The following sections go over the basic configuration steps in a PicOS switch needed for the RADIUS Authentication.

1. Configure Data and Voice VLAN and basic Access Switch Configuration

   a. Create for example Data VLAN 10 and Voice VLAN 800 in the PicOS switch

```
set vlans vlan-id 800
set vlans vlan-id 10 l3-interface vlan10
set l3-interface vlan-interface vlan10 address 192.168.42.170 prefix-length 24
```

   Following config is needed for Central Web Authentication (CWA) only. We will create VLAN 20. Unknown user devices will be placed in Blocked VLAN (20 in this case) until user authenticates via Guest portal using CWA.

```
set protocols dot1x block-vlan-id 20
set vlans vlan-id 20 vlan-name "Vlan20"
set vlans vlan-id 20 l3-interface "Vlan20"
set l3-interface vlan-interface Vlan20 address 192.168.44.1 prefix-length 24
```

   b. Configure uplink port for inband VLAN 10

```
set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 10
set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 800
set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode "trunk"
```

   c. Enable PoE on all interfaces

```
set poe interface all
```

   d. Enable basic switching and routing configuration

```
set system hostname P8-Access-BR-1-SW-2
set ip routing enable true
set protocols lldp enable true
set system inband vlan-interface vlan10
set system ntp server-ip 132.163.96.1
set system timezone America/Los_Angeles
set protocols static route 0.0.0.0/0 next-hop 192.168.42.1
set system services ssh idle-timeout 3600
```

2. Configure the RADIUS server information

   a. Provide IP address and shared key of the RADIUS server. By default, RADIUS server uses UDP protocol and port 1812 for authentication.

   ```
   set protocols dot1x aaa radius authentication server-ip 192.168.42.110 shared-key xxxxx
   ```

   b. Configure the access profile

   Network Access Server (NAS) is the frontline of authentication. In this case it is PicOS switch. This Attribute indicates the identifying IP Address of the NAS (PicOS-Switch) which is requesting authentication of the user.

   ```
   set protocols dot1x aaa radius nas-ip 192.168.42.170
   ```

   c. Configure a RADIUS dynamic authorization client from which the switch accepts the Change of Authorization (CoA) messages. This configuration is used for CWA.

   ```
   set protocols dot1x aaa radius dynamic-author client 192.168.42.110 shared-key xxxxx
   ```

   d. Configure the interval for re-sending the authentication messages to the AAA server when the AAA server does not respond during NAC authentication. Here retry interval is set to 3 seconds.

   ```
   set protocols dot1x aaa radius authentication server-ip 192.168.42.110 retry-interval 3
   ```

3. Configure 802.1x, MAB and CWA authentication modes and multiple host mode on all access ports

   Any users or endpoint devices can be connected to any switch ports and authentication is needed due to Zero Trust. 802.1x, MAB and Web Authentication modes are enabled on all ports. Based on the user or endpoint device a specific authentication method will be used. Also multiple-host mode is enabled on all ports. In the following example x is the port number.

   ```
   set protocols dot1x interface ge-1/1/x auth-mode 802.1x
   set protocols dot1x interface ge-1/1/x auth-mode mac-radius
   set protocols dot1x interface ge-1/1/x auth-mode web
   set protocols dot1x interface ge-1/1/x host-mode “multiple”
   set interface gigabit-ethernet ge-1/1/x family ethernet-switching port-mode “trunk
   ```

Automate and verify NAC configuration for Access Switches

Access switch deployment configuration can be automated using AmpCon Automation and Management Platform 1.6 version. You can deploy a complete configuration on a bare-metal switch using the following mechanisms.

1. AmpCon UX
2. AmpCon’s full suite of REST APIs now available with version 1.6
3. Ansible Playbooks deployed via AmpCon and Pica8’s Ansible module
4. Bulk Deployment mechanism where one can deploy a group of bare-metal switches (100 for example), in one click of a button. Please refer to Building Configuration Automatically for Group of Switches.

For more details refer to the AmpCon documentation given in the reference section of this guide.

The following are steps to deploy a NAC-enabled switch configuration on a bare-metal switch using UI of AmpCon’s UX. We are using a DELL switch model N3248P-ON in the following example..

1. **Global configuration file:** Create a text file called *N3248P-ON-GlobalConfig.txt* with **blue color configuration CLIs** given in the above section. These PicOS CLIs are common between all Access Switches.

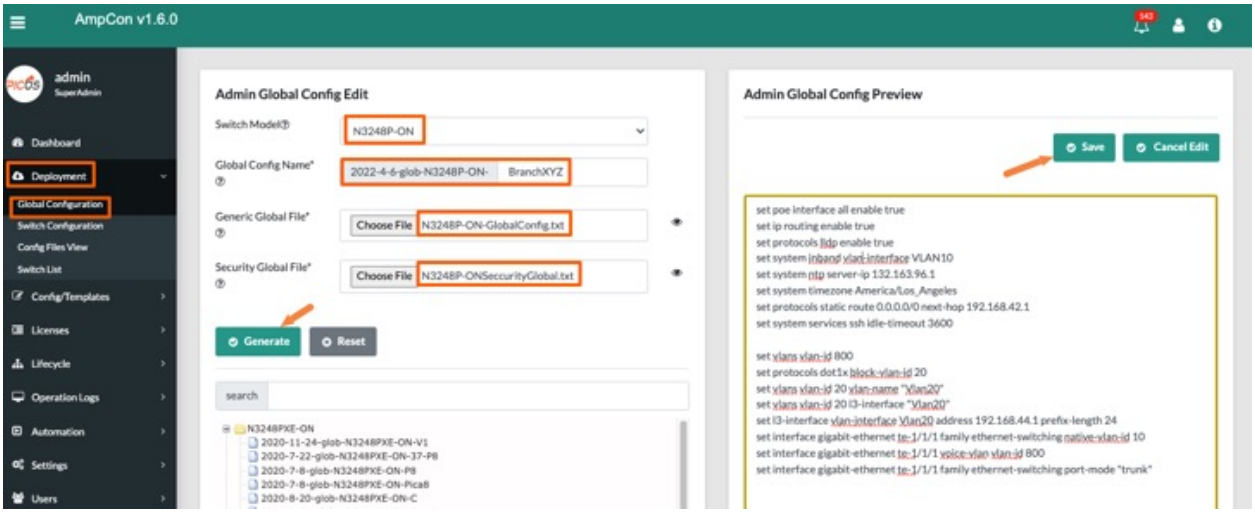
```
set poe interface all enable true
set ip routing enable true
set protocols lldp enable true
set system inband vlan-interface vlan10
set system ntp server-ip 132.163.96.1
set system timezone America/Los_Angeles
set protocols static route 0.0.0.0/0 next-hop 192.168.42.1
set system services ssh idle-timeout 3600

set vlans vlan-id 800
set protocols dot1x block-vlan-id 20
set vlans vlan-id 20 vlan-name “Vlan20”
set vlans vlan-id 20 l3-interface “Vlan20”
set l3-interface vlan-interface Vlan20 address 192.168.44.1 prefix-length 24
set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 10
set interface gigabit-ethernet te-1/1/1 family ethernet-switching vlan members 800
set interface gigabit-ethernet te-1/1/1 family ethernet-switching port-mode “trunk”
```

2. **Global Security Configuration file:** Create a text file called *N3248P-ONSecurityGlobal.txt* with **red color CLIs** given in the above section. These security related PicOS CLIs are common between all Access Switches..

```
set protocols dot1x aaa radius authentication server-ip 192.168.42.110 shared-key xxxxx
set protocols dot1x aaa radius dynamic-author client 192.168.42.110 shared-key xxxxx
set protocols dot1x aaa radius authentication server-ip 192.168.42.110 retry-interval 3
```

3. **Upload Global Configuration files to AmpCon:** Following are the steps to upload your newly created Configuration files created to AmpCon:

   a. Log into the AmpCon UI and select *Deployment->Global Configuration* menu
   b. Select the switch model matching your switch for deployment (i.e. in this case the DELL N3248P-ON)
   c. Enter the name of the Global Config file that will be stored in AmpCon, upload Global Configuration file and Security Global file
   d. Click *Generate*, then review the generated config on left pane and click *Save* as shown below.



4. **Create an automation Deployment Template file:** Create a text file called *N3248P-ON-Access-Switches-Template.j2*

An AmpCon Automation Deployment Template contains the following information:

- **Switch specific CLI commands using variables** in the Template
- **Interface related CLI commands**

Note: Pica8 templates make applying changes to multiple interfaces easy!

AmpCon Automation Deployment Templates are in the *Jinja2* format and it is divided into the following two sections:

a. Top section of the template contains switch specific PicOS CLI commands with variables and logic for generating PicOS CLI commands for making changes to multiple switch ports
b. Bottom section of the template contains *Variables* definitions for use in the template, and for AmpCon's UX to turn the template and its variables into a Wizard-Driven-Form that anyone at any skill level can use to deploy changes to the network.

Following is an example Template file *N3248P-ON-Access-Switches-Template.j2* . Reserved words are marked in a **brown color**. Comments are **colored in grey** Switch specific Variables are encapsulated with curly braces and marked in a **light green** color as shown below.

```
name: 3248P-ON-BranchAYC
description: 3248P-ON-BranchAYC
platform: N3248P-ON
content_start:

{#::::: For input Variable::::#}
set system hostname {{ Hostname }}
set protocols dot1x aaa radius nas-ip {{Data_VLAN_IP_Address}}
set vlans vlan-id 10 l3-interface vlan10
set l3-interface vlan-interface vlan10 address {{Data_VLAN_IP_Address}} prefix-length 24
{#:::::For ports 1/1/1 through 1/1/48::::::#}
{% for i in range(1,47) %}
  set interface gigabit-ethernet ge-1/1/{{ i }} family ethernet-switching port-mode "trunk"
  set protocols dot1x interface ge-1/1/{{ i }} host-mode "multiple"
  set protocols dot1x interface ge-1/1/{{ i }} auth-mode 802.1x
  set protocols dot1x interface ge-1/1/{{ i }} auth-mode mac-radius
  set protocols dot1x interface ge-1/1/{{ i }} auth-mode web
{% endfor %}

content_end$

param_start:
{
        "Hostname": {
                "param_default": "P8-Access-BR-1-SW-1",
                "type": "text",
                "required": "not required",
                "description": "Configure the hostname",
                "param_check": ""
        },
        "Data_VLAN_IP_Address": {
```

```
                "param_default": "192.168.42.210",
                "type": "text",
                "required": "required",
                "description": "Configure management IP mask.e.g. 192.168.42.210",
                "param_check": ""
        }
}
param_end$
```

5. **Upload Template file in AmpCon:**

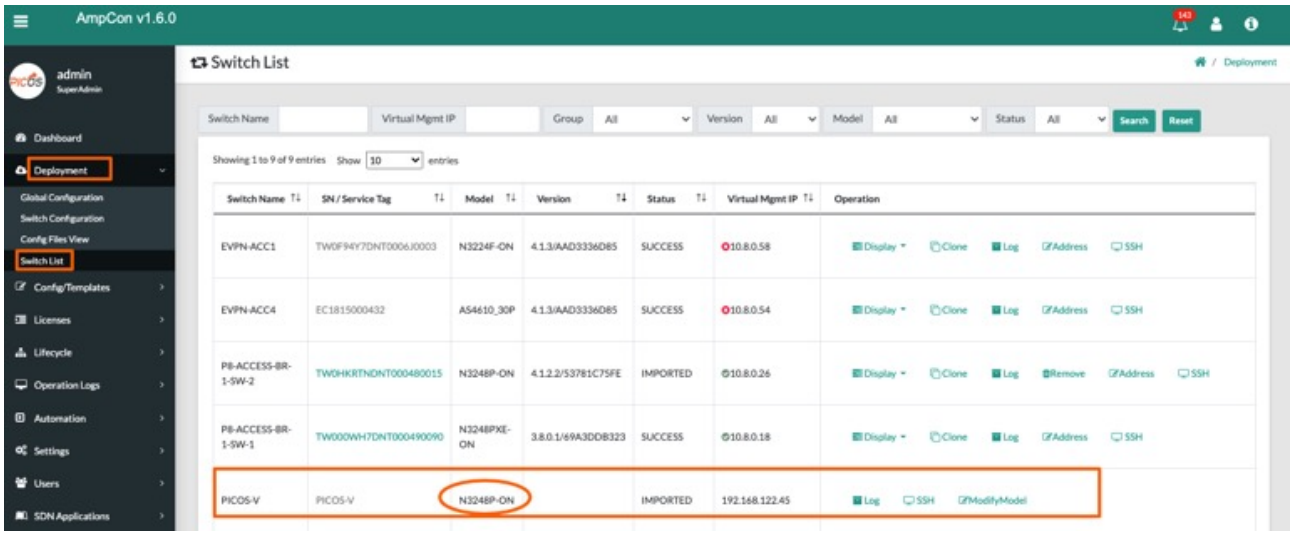
   a. Select *Config/Templates->Template* List menu
   b. Enter the *Name* for the Template, *Description*
   c. Click *Choose File* and select the Template file you created in the prior step, and click *Upload* as shown below.

6. **Generate Switch Specific Configuration:** Generate switch specific configuration and verify switch specific configuration that is being deployed to the nested PicOS-V VM that is running inside the AmpCon VM.

   Set PicOS-V Hardware Model

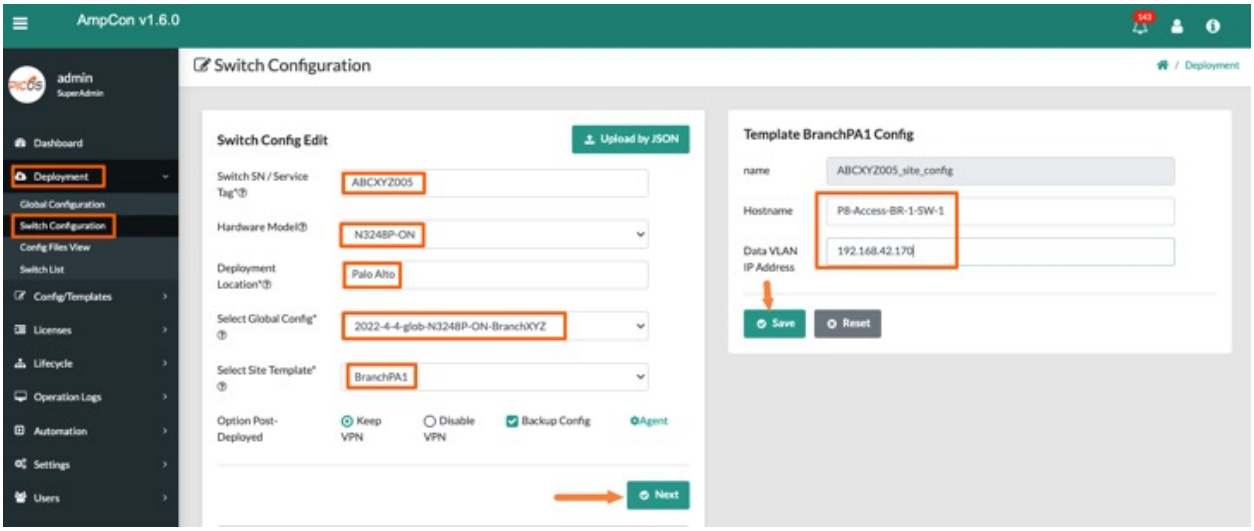
   Before you perform this step, make sure PicOS-V VM running in AmpCon is set to the hardware model you are planning to test. In this example we have set to the hardware model of PicOS-V to Dell N3248P-ON. This matches with the hardware model referred in Global Config and Template files.

   1) Navigate to *Deployment-> Switch List* to check the switch simulated hardware model for PicOS-V VM shown below. In case switch hardware model is not what you expected, click *ModifyModel* and set the simulated hardware model.



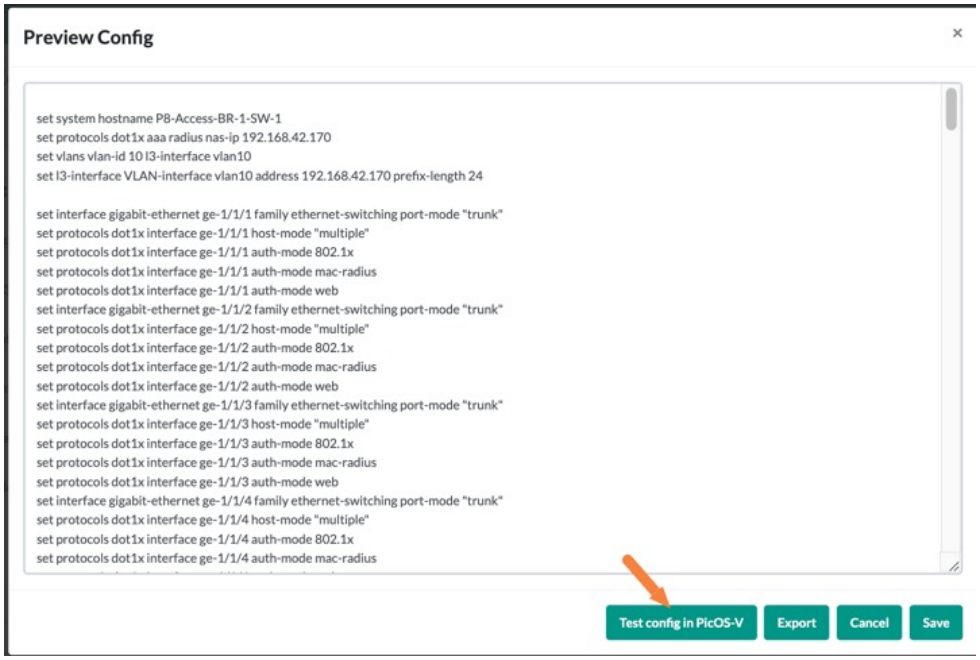
Generate Switch Specific Configuration

Navigate to *Deployment -> Switch Configuration* to generate switch specific configuration. Enter the serial number, hardware model, geo-location of the switch, name of the Global Config file saved in previous section and name of the template file and click *Next*. You need to enter value for the switch specific variables defined in the Template. We had two variables in the Template: Switch hostname and Data VLAN IP address. Enter the value for those variables and click *Save*.



Verify Template Generated Configuration

Click *Test Config in PicOS-V* to verify the full configuration of the switch. Full configuration includes configuration contained in Global Config files and Template generated configuration in PicOS-V VM running in AmpCon.



Once the full configuration is verified in PicOS-V virtual switch, the same config can be used to deploy on a bare-metal switch. For more details of Automated Deployment of bare-metal switches please refer to this AmpCon Deployment document.