Configuring SNMP ACL

By default, no SNMP ACL list is configured on the switch and allows all network management station (NMS) to access the device through SNMP protocol. Users can configure access control white list for SNMP protocol on the device to restrict NMS access to the device, so as to improve the device security.

Concepts

SNMP ACL has two types of access control white list: As-per User List and Global List.

- As-per User List

The SNMP ACL that specifies the security name can be configured with multiple networks, is called the as-per user list. For example,

```
admin@XorPlus# set system snmp-acl security-name user1 network 10.10.50.0/24
```

Where "security-name" is the **community name** for SNMPv1 and SNMPv2, and the **usm-user** name in command **set protocols snmp v3 usm-user** *<user-name>* for SNMPv3.

- Global List

SNMP ACLs that do not specify a security name but only networks are called the global list. For example,

```
admin@XorPlus# set system snmp-acl network 10.10.50.0/24
admin@XorPlus# set system snmp-acl network 10.10.51.0/24
```

The global list is applied to NMS that are not configured with an as-per user list.

Matching Procedure

As-per user list and global list can be configured together. The matching procedure for SNMP ACL is as follows:

1. For the NMS that accesses the device (assuming its security name is ***s1***), if a valid as-per user list is configured on the device (i.e., an SNMP ACL with security name ***s1*** and network is configured), as-per user list matching is performed.

- If the SNMP query matches the as-per user list, allowing NMS to access to devices through SNMP protocol.
- If no as-per user list entry is matched, the NMS who sent the SNMP query is denied access to this device.

NOTE:

If an SNMP ACL with security name s1 is configured, but no network list is configured under it, the as-per user list is empty and invalid, then global list matching will be performed.

2. If no as-per user list is configured for this NMS (i.e., the SNMP ACL with security name ***s1*** is not configured), then global list matching is performed.

- If the SNMP query matches a global list, allowing NMS to access devices through SNMP protocol.
- If no global list entry is matched, the NMS who sent the message is denied access to this device.
- If global list is not configured then the NMS is allowed to access the device through SNMP protocol.

Examples

Three examples are given to illustrate the SNMP ACL procedure.

Example 1

The following configurations were set on the switch:

```
admin@XorPlus# set system snmp-acl network 10.10.50.0/24
admin@XorPlus# set system snmp-acl security-name user1 network 10.10.51.0/24
admin@XorPlus# set system snmp-acl security-name user1 network 10.10.52.0/24
```

- In case of ***user1***, SNMP queries from 10.10.10.51.0/24 and 10.10.52.0/24 are allowed to go to SNMP agent. And others will be denied.
- For other users, only SNMP queries from 10.10.50.0/24 (SNMP ACL global list configuration) are accepted.

Example 2

The following configurations were set on the switch:

```
admin@XorPlus# set system snmp-acl security-name user1 network 10.10.11.0/24
admin@XorPlus# set system snmp-acl security-name user1 network 10.10.12.0/24
```

- In case of ***user1***, SNMP queries from 10.10.10.11.0/24 and 10.10.12.0/24 are allowed to go to SNMP agent. And others will be denied.
- For other users, SNMP queries will be accepted by SNMP agent, as SNMP ACL global list configuration is NULL.

Example 3

The following configurations were set on the switch:

```
! SNMPv3 user pica8test123
    admin@XorPlus# set protocols snmp v3 mib-view readall subtree 1 mask ff
    admin@XorPlus# set protocols snmp v3 group Pica8 security-level AuthPriv
    admin@XorPlus# set protocols snmp v3 group Pica8 read-view readall
    admin@XorPlus# set protocols snmp v3 usm-user pica8test123 group Pica8
    admin@XorPlus# set protocols snmp v3 usm-user pica8test123 authentication-mode md5
    admin@XorPlus# set protocols snmp v3 usm-user pica8test123 authentication-key P3Ca8536bl4
    admin@XorPlus# set protocols snmp v3 usm-user pica8test123 privacy-mode des
    admin@XorPlus# set protocols snmp v3 usm-user pica8test123 privacy-key P3Ca8536bl8
    admin@XorPlus# set system snmp-acl security-name pica8test123 network 192.168.42.0/24


! SNMPv3 user pica8test321
    admin@XorPlus# set protocols snmp v3 mib-view readall subtree 1 mask ff
    admin@XorPlus# set protocols snmp v3 group Pica8 security-level AuthPriv
    admin@XorPlus# set protocols snmp v3 group Pica8 read-view readall
    admin@XorPlus# set protocols snmp v3 usm-user pica8test321 group Pica8
    admin@XorPlus# set protocols snmp v3 usm-user pica8test321 authentication-mode md5
    admin@XorPlus# set protocols snmp v3 usm-user pica8test321 authentication-key P3Ca8536bl4
    admin@XorPlus# set protocols snmp v3 usm-user pica8test321 privacy-mode des
    admin@XorPlus# set protocols snmp v3 usm-user pica8test321 privacy-key P3Ca8536bl8
    admin@XorPlus# set system snmp-acl security-name pica8test321 network 192.168.43.0/24
```

- Get switch model using SNMPv3 from an NMS IP located in the 172.168.42.0/24 network using the *pica8test123* user credentials. The expected result is: Switch model for switch at IP *192.168.42.171* is provided.

```
admin@NMS# snmpwalk -v3 -u pica8test123 -l AuthPriv -a md5 -A P3Ca8536bl4 -x des -X P3Ca8536bl8 192.168.42.171
1.3.6.1.4.1.35098.1.13.0
iso.3.6.1.4.1.35098.1.13.0 = STRING: "N3248P-ON"
```

- Get switch model using SNMP v3 from an NMS IP located in the 172.168.42.0/24 network using the *pica8test321* user credentials. Switch model for switch at IP *192.168.42.171* is not provided. The requesting SNMP server IP is not in 192.168.43.0/24 network, hence it is not allowed to get the switch model.

```
admin@NMS# snmpwalk -v3 -u pica8test321 -l AuthPriv -a md5 -A P3Ca8536bl4 -x des -X P3Ca8536bl8 192.168.42.171
1.3.6.1.4.1.35098.1.13.0
Timeout: No Response from 192.168.42.171
```

- After deleting SNMP ACL for pica8test321, it is able to get the hardware model:

```
admin@NMS# snmpwalk -v3 -u pica8test321 -l AuthPriv -a md5 -A P3Ca8536bl4 -x des -X P3Ca8536bl8 192.168.42.171
1.3.6.1.4.1.35098.1.13.0
iso.3.6.1.4.1.35098.1.13.0 = STRING: "N3248P-ON"
```