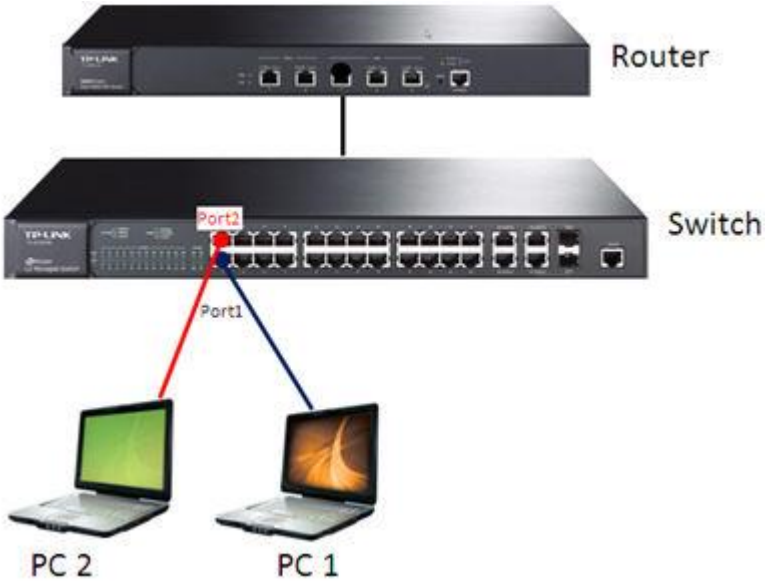
How to configure Extended IP ACL

ACL (Access Control List) is used to filter packets by configuring match rules and process policies of packets in order to control the access of the illegal users to the network. Besides, ACL functions can be used to control traffic flows and save network resources.

Here is a case to give you some instructions to configure the Extend-IP ACL.

Extend-IP ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses, destination IP addresses, IP protocol and other information of this sort carried in the packets.

In this case, we want to achieve the demand that the PC (or other devices) connected to the specified port of the switch cannot get IP address through DHCP Server. As the picture shows below, the PC 2 cannot get IP from the router (the Router embedded DHCP Server function).

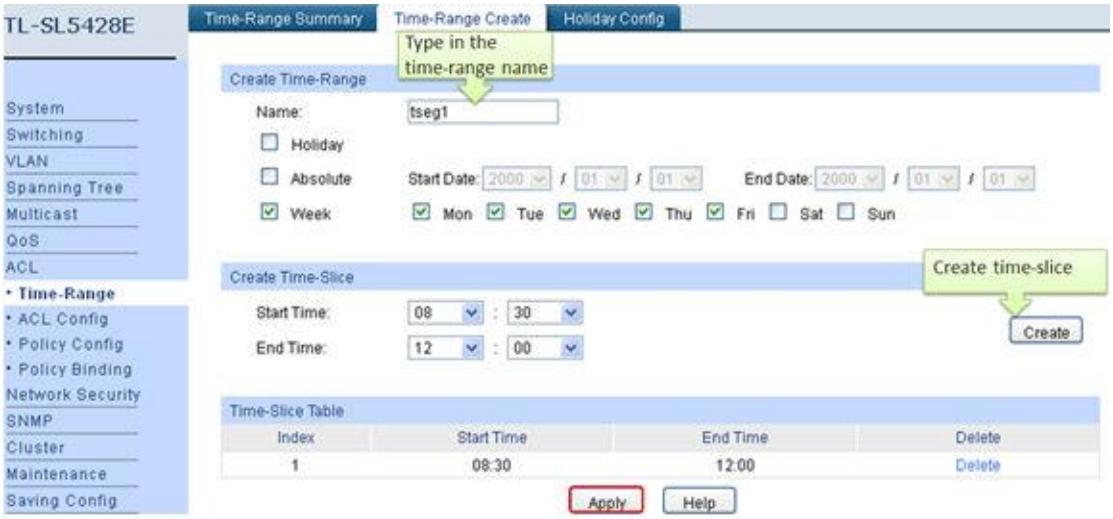


We can configure the switch via web management page or CLI. And we will give you instructions of the 2 methods.

Method 1: Web management page

Step 1: Configure the Time-Range

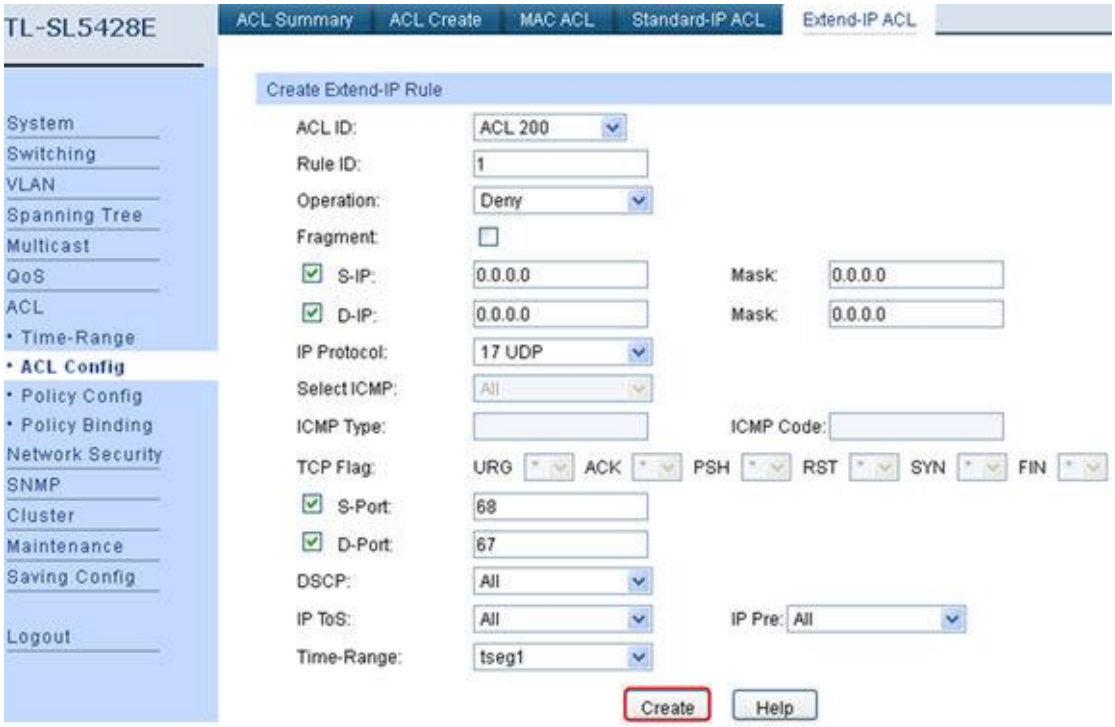
If an ACL is needed to be effective in a specified time-range, you should specify a time-range in the ACL firstly. Please choose the menu **ACL->Time-Range->Time-Range Create**, here we create a time-rangetseg1 for example, and you can type in the parameters as you want, then click **Apply** to complete the settings of the time-range.



Step 2: Configure the ACL Setting

Choose the menu **ACL->ACL Config->ACL Create**; Create an Extend-IP ACL number (here we created 200 for example).

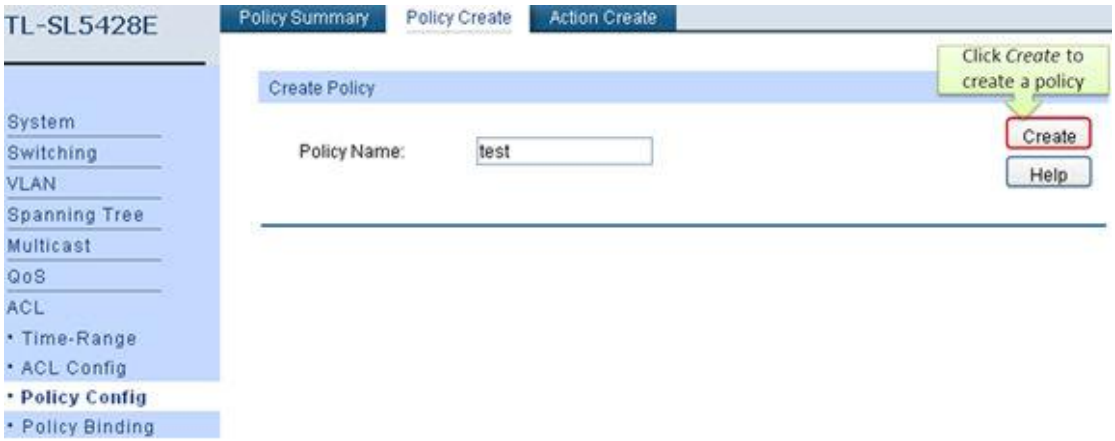
Then please choose the menu **ACL->ACL Config->Extend-IP ACL**. In this page we will configure the Extended-IP rule for the ACL 200. Firstly select the ACL ID 200, type in the rule ID 1, and select the operation Deny. Then type in the S-IP, D-IP and their Mask, here they all are 0.0.0.0, the IP Protocol should select 17 UDP, the S-Port is 68 and the D-Port is 67(here you can just type in the S-Port or the D-Port), then select the Time-Range tseg1. After that, click Create to complete the Extended-IP ACL setting.



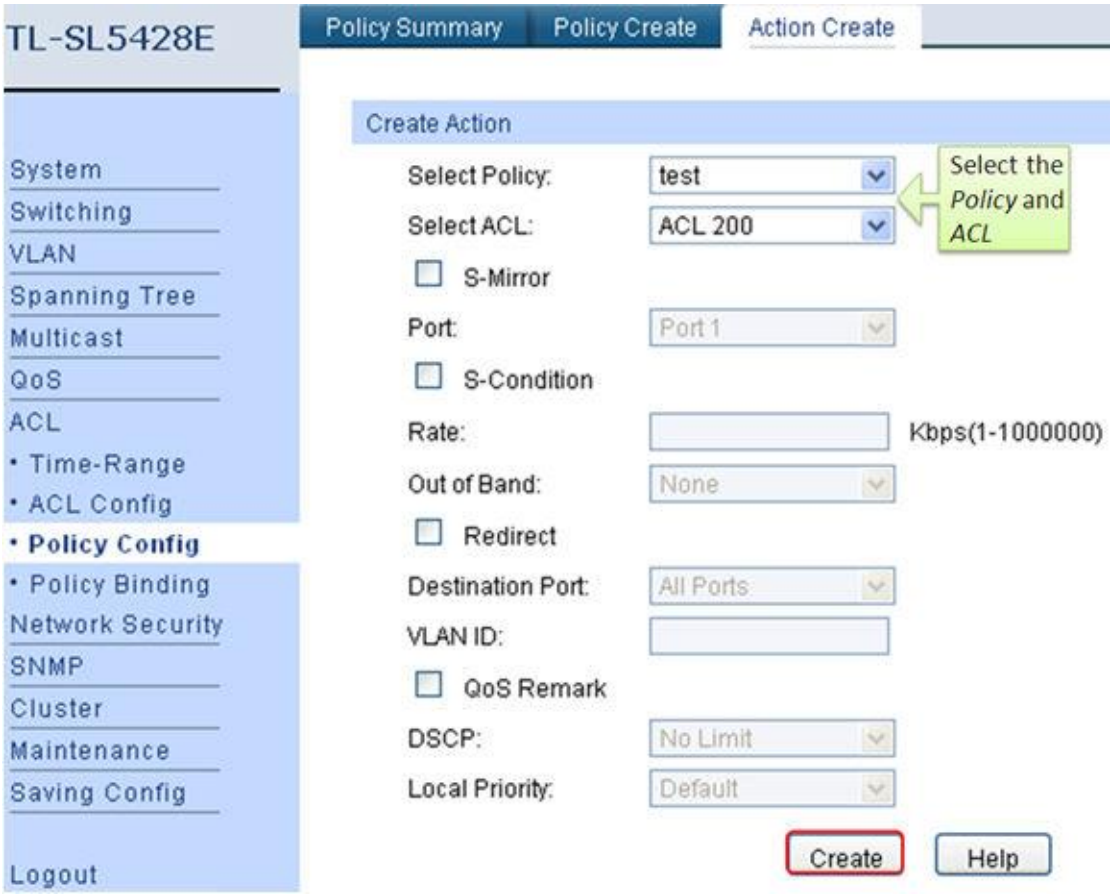
Step 3: Configure the Policy for specified ACL

A Policy is used to control the data packets that match the corresponding ACL rules by configuring ACLs and actions together for effect. The operations include stream mirror, stream condition, QoS remarking and redirect.

Choose the menu **ACL->Policy Config->Policy Create**. Here we create a policy test for example.



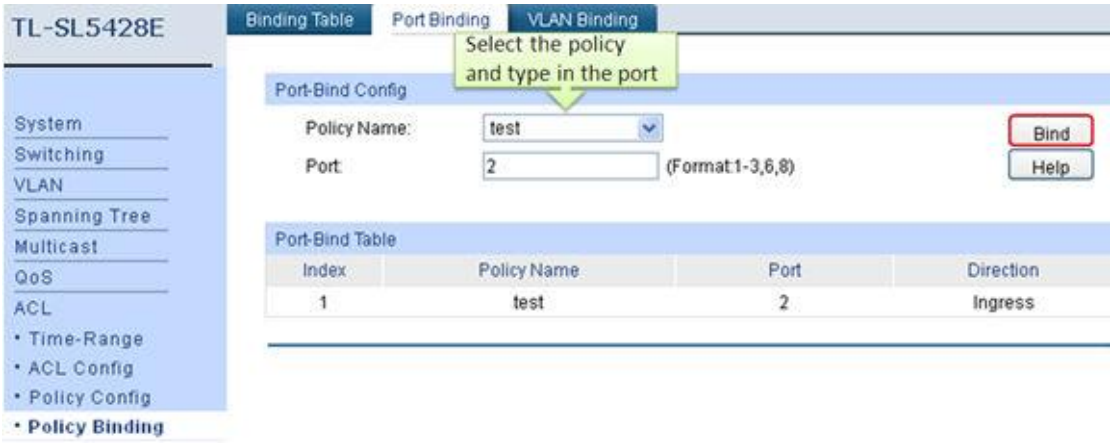
Choose the menu **ACL->Policy Config->Action Create**, bind the policy to ACL 200, and select the action you want(for this case, we need not configure any action). After that, click Create to complete action create setting.



Step 4: Bind the policy to specified port

Policy Binding function make the policy take effect on a specific port/VLAN. The policy will take effect only when it is bound to a port/VLAN. In the same way, the port/VLAN will receive the data packets and process them based on the policy only when the policy is bound to the port/VLAN.

Choose the menu **ACL->Policy Binding->Port Binding**. Here we bind the policy on port 2.



Now all configurations are completed, and the PC connected to port 2 won't get any IP address via router (DHCP server).

If you prefer to configure the switch via CLI, you can refer to method 2.

Method 2: CLI

Here we have provided the CLI command to achieve the same function as the web config above.

```
TP-LINK>enable
TP-LINK#configure
TP-LINK (config)#acl time-segment tseg1 start-time 08:30 end-time 12:00 week-day working-day
TP-LINK (config)#acl create 200
TP-LINK (config)#acl rule ext-acl 200 1 op discard dip 0.0.0.0 dmask 0.0.0.0 sip 0.0.0.0 smask 0.0.0.0 protocol 17 d-port 67 s-port 68 tseg tseg1
TP-LINK (config)#acl policy policy-add test
TP-LINK (config)#acl policy action-add test 200
TP-LINK (config)#acl bind to-port test 2
TP-LINK (config)#end
TP-LINK#user-config save
```

Please don’t forget to save the config after the configuration. And if you have any other issues or unknown contents, the User Guide will be a good helper.