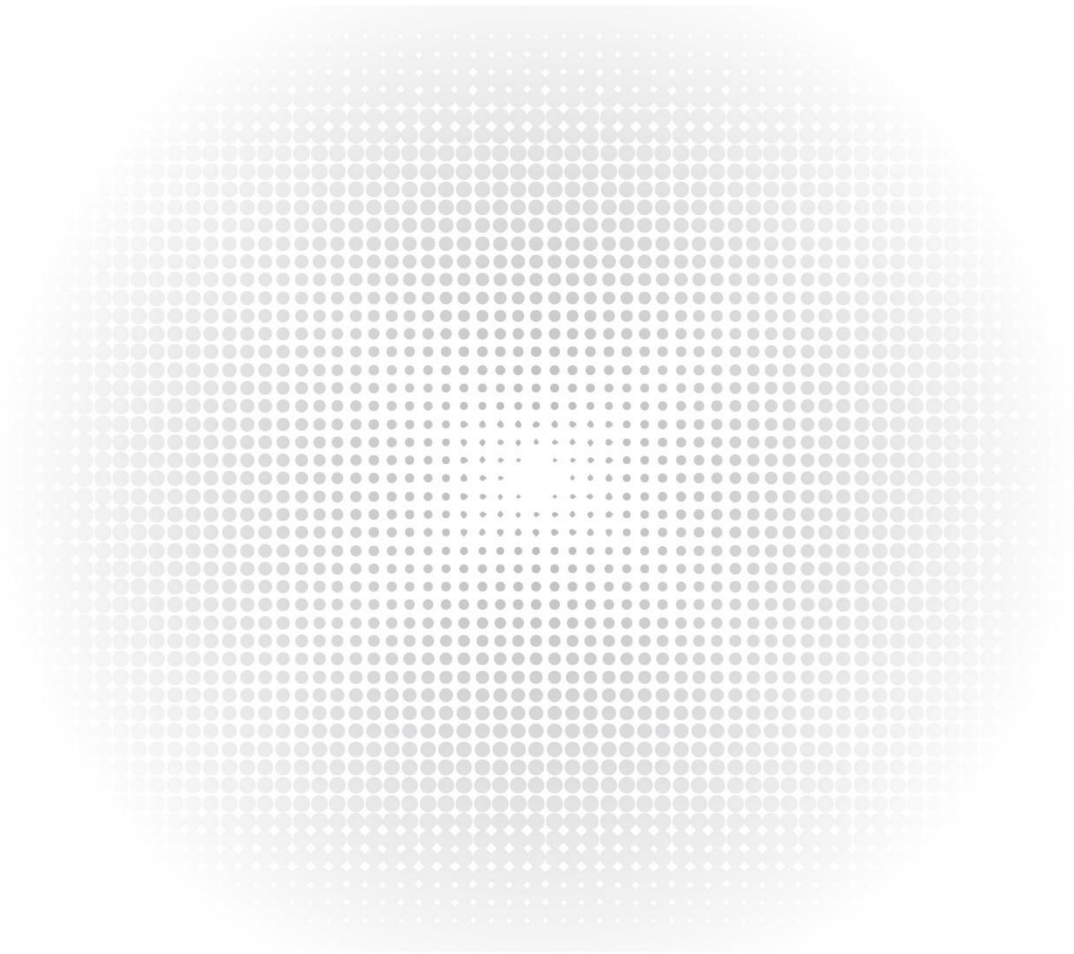


PicOS® Quick Configuration Guide



Contents

Chapter 1 Initial Setup	1
1.1 Powering on the Switch	1
1.2 Logging in Switch through the Console Port	1
Chapter 2 Basic Configuration	3
2.1 Entering CLI Configuration Mode	3
2.2 Configuring a Host Name	4
2.2.1 Overview	4
2.2.2 Procedure	4
2.2.3 Verifying the Configuration	4
2.2.4 Other Configurations	4
2.3 Configuring the Management IP Address	4
2.3.1 Overview	4
2.3.2 Procedure	4
2.3.3 Verifying the Configuration	5
2.3.4 Other Configurations	5
Chapter 3 Network Configuration	6
3.1 Configuring an Interface	6
3.1.1 Configuring a loopback interface	6
3.1.2 Configuring a Routed interface	7
3.1.3 Configuring a VLAN Interface	8
3.2 Configuring the Routing	9
3.2.1 Configuring the Static Routing	10
3.2.2 Configuring the Dynamic Routing	10
Chapter 4 Security Configuration	13
4.1 Configuring an ACL	13
4.2 Configuring the SSH Access	14
Chapter 5 Typical Configuration Example	16
5.1 Overview	16
5.2 Procedure	17

5.3 Verifying the Configuration	21
--	-----------

Chapter 1 Initial Setup

Before performing the following operations, you should make sure that the device has been installed successfully. For detailed information of installing PicOS, see [Installing or Upgrading PICOS](#).

1.1 Powering on the Switch

Connect the switch to a power supply through the power cord, and then press the power button to power on the switch.

1.2 Logging in Switch through the Console Port

For initial system configuration, you should connect the switch to a terminal through the Console port.

Procedure

Step1: Connect the console port of the switch to the serial port of a PC through a console cable, as shown in the figure below.

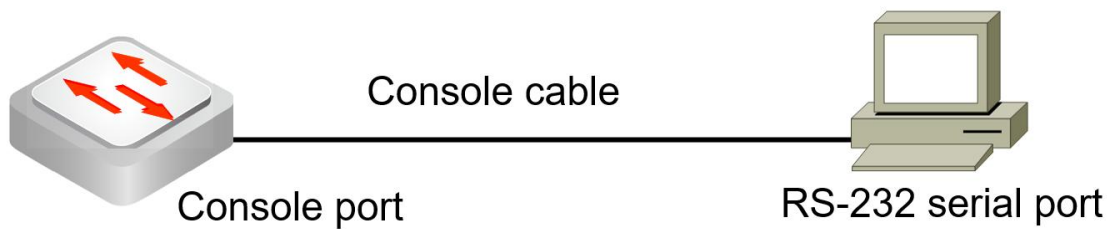


Figure 1-1 Connexion of Console cable

Step2: Open a terminal emulator (e.g., PuTTY) and configure it with the appropriate COM port settings, which should be the same with the switch related parameters. As shown in the figure below.

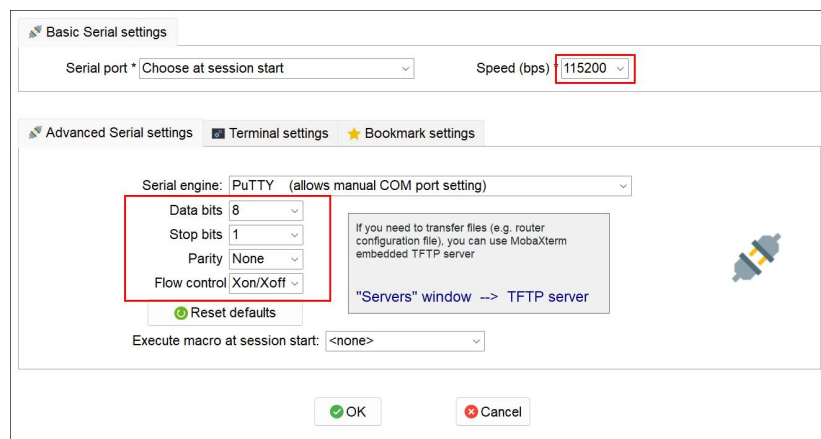
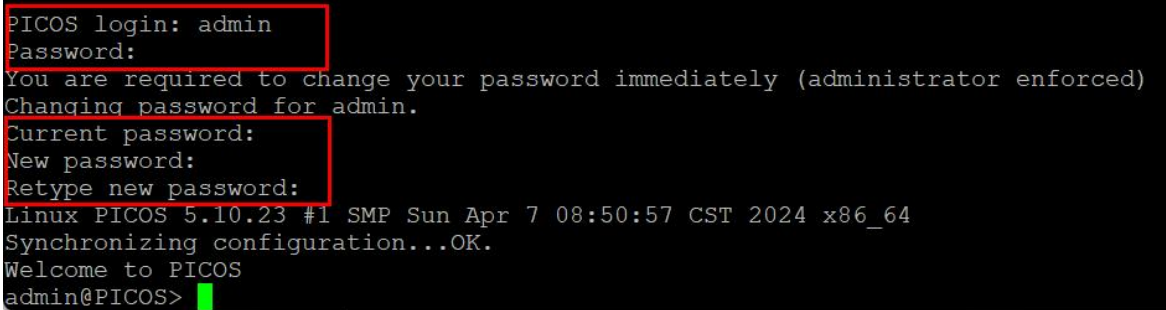


Figure 1-2 Serial Settings of Terminal Emulator

Step3: Enter the default administrator name **admin** and password **pica8** at the **PICOS login** and **password** prompts, and press **Enter**. Change the default password according to prompts, press **Enter**, and you can successfully log in CLI. As shown in the figure below.

A terminal window with a black background and white text. The text shows the login process for PICOS. The first two lines, 'PICOS login: admin' and 'Password:', are enclosed in a red rectangular box. The subsequent lines are: 'You are required to change your password immediately (administrator enforced)', 'Changing password for admin.', 'Current password:', 'New password:', and 'Retype new password:', which are also enclosed in a red rectangular box. Below these prompts, the system output shows: 'Linux PICOS 5.10.23 #1 SMP Sun Apr 7 08:50:57 CST 2024 x86_64', 'Synchronizing configuration...OK.', 'Welcome to PICOS', and the prompt 'admin@PICOS>' followed by a green cursor bar.

```
PICOS login: admin
Password:
You are required to change your password immediately (administrator enforced)
Changing password for admin.
Current password:
New password:
Retype new password:
Linux PICOS 5.10.23 #1 SMP Sun Apr 7 08:50:57 CST 2024 x86_64
Synchronizing configuration...OK.
Welcome to PICOS
admin@PICOS> █
```

Figure 1-3 Password Modification for First login

Chapter 2 Basic Configuration

2.1 Entering CLI Configuration Mode

PicOS supports different CLI modes, which are indicated by different prompts. Some commands can only be run in certain modes.

- Operation mode

When log in PicOS CLI, you are in the operation mode by default. You can execute some basic configurations in this mode, such as clear and show, etc. > indicates the operation mode, as shown in the figure below.

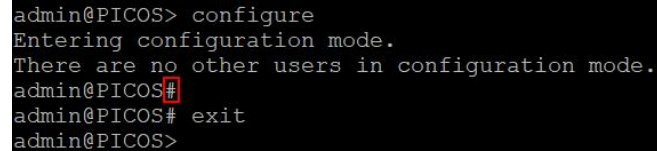


```
admin@PICOS>
```

Figure 2-1 Prompt of Operation Mode

- Configuration mode

You can configure the switch function in this mode, such as interface, routing, etc. Run **configure** in the operation mode to enter the configuration mode, and run **exit** to return to the operation mode. # indicates the configuration mode, as shown in the figure below.

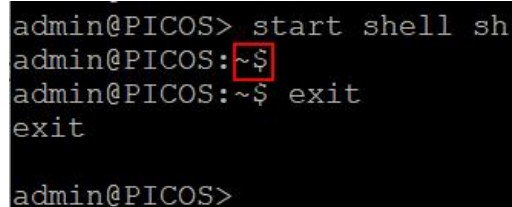


```
admin@PICOS> configure
Entering configuration mode.
There are no other users in configuration mode.
admin@PICOS#
admin@PICOS# exit
admin@PICOS>
```

Figure 2-2 Prompt of Configuration Mode

- Linux shell mode

Run **start shell sh** in the operation mode to enter the Linux shell mode, and run **exit** to return to the operation mode. ~\$ indicates the Linux shell mode, as shown in the figure below.



```
admin@PICOS> start shell sh
admin@PICOS:~$
admin@PICOS:~$ exit
exit
admin@PICOS>
```

Figure 2-3 Prompt of Linux Shell Mode

2.2 Configuring a Host Name

2.2.1 Overview

A host name distinguishes one device from another. The default host name is the system name PICOS. You can modify the host name as required.

2.2.2 Procedure

Step1: In the configuration mode, specify or modify a host name for the switch.

```
set system hostname <hostname>
```

Step2: Commit the configuration.

```
commit
```

2.2.3 Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show system name** command to view the new host name.

2.2.4 Other Configurations

To reset the hostname to default, use **delete system hostname** command.

2.3 Configuring the Management IP Address

2.3.1 Overview

To facilitate the device management and meet the requirement of separating the management traffic from the data traffic, the switch supports the management interface. By default, the management interface is eth0 and the IP address is null.

2.3.2 Procedure

Step1: In the configuration mode, specify the IP address for management interface eth0.

```
set system management-ethernet eth0 ip-address {IPv4 | IPv6} <ip-address>
```

Step2: Commit the configuration.

```
commit
```

2.3.3 Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show system management-ethernet** command to view the MAC address, IP address, state and traffic statistics.

2.3.4 Other Configurations

To clear the configuration of management interface, use **delete system management-ethernet eth0 ip-address** command.

Chapter 3 Network Configuration

3.1 Configuring an Interface

- Physical interface: exists on interface cards, which can be used for management and service.
 - Management interface: the switch supports a management interface eth0 by default, which is used to log in devices for configuration and management. For detailed information for the management interface, see [Configuring the Management IP Address](#).
 - Service interface: can be used for service transmission, which includes Layer 2 Ethernet interfaces and Layer 3 Ethernet interfaces. By default, service interfaces of switch are all Layer 2 interfaces. To configure a Layer 2 interface as a Layer 3 interface, see the following chapter.
- Logical interface: not exists physically and is configured manually, which is used for service transmission. It includes Layer 3 interfaces, routed interfaces, loopback interfaces, etc.

It includes the following chapters:

3.1.1 Configuring a loopback interface

1. Overview

The loopback interface is always up to ensure network reliability, which has the following features:

- It is always up and has the loopback feature.
- It can be configured with the mask of all 1s.

Based on the features, the loopback interface has the following applications:

- The IP address of a loopback interface is specified as the source address of packets to improve network reliability.
- When no Router ID is configured for dynamic routing protocols, the maximum IP address of the loopback interface is configured as the router ID automatically.

2. Procedure

Step1: In the configuration mode, specify the name and IP address for the loopback interface.

```
set l3-interface loopback <loopback-name> address <ipv4-address> prefix-length 32
set l3-interface loopback <loopback-name> address <ipv6-address> prefix-length 128
```

Step2: Commit the configuration.

```
commit
```

3. Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show l3-interface loopback** <loopback-name> command to view the state, IP address, description and traffic statistics.

4. Other Configurations

By default, the loopback interface is enabled when created. To disable the loopback interface, use **set l3-interface loopback** <interface-name> **disable** command.

To clear the configuration of loopback interface, use **delete l3-interface loopback interface** <interface-name> command.

3.1.2 Configuring a Routed interface

1. Overview

All Ethernet ports of switch are Layer 2 interfaces by default. When you need to use an Ethernet port for Layer 3 communication, you can enable the Ethernet port as a routed interface. The routed interface is a Layer 3 interface which can be assigned an IP address and can be configured with a routing protocol to connect to other Layer 3 routing devices.

2. Procedure

Step1: In the configuration mode, set reserved VLANs for the use of routed interface.

```
set vlans reserved-vlan <reserved-vlan>
```

- **reserved-vlan** <reserved-vlan>: specifies the reserved VLANs. The valid VLAN numbers range is 2-4094. User can specify a range of VLAN numbers, e.g. 2,3,50-100. System supports up to 128 reserved VLANs.

Step2: Select a physical interface as the routed interface and specify a name.

```
set interface gigabit-ethernet <interface-name> routed-interface name <string>
```

- **routed-interface name** <string>: specifies a routed interface name.

Note: The name must start with "rif-", for example, rif-ge1.

Step3: Enable the routed interface.

```
set interface gigabit-ethernet <interface-name> routed-interface enable true
```

Step4: Configure an IP address for the routed interface.

```
set l3-interface routed-interface <string> address <ipv4-address | ipv6-address> prefix-length <prefix-number>
```

- **prefix-length** <prefix-number>: specifies the network prefix length. The range is 4-32 for IPv4 address, and 1-128 for IPv6 address.

Step5: Commit the configuration.

```
commit
```

3. Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show l3-interface routed-interface** <interface-name> command to view the state, IP address, MAC address, VLAN, MTU, description and traffic statistics.

4. Other Configurations

To disable the routed interface, use **set interface gigabit-ethernet** <interface-name> command.

3.1.3 Configuring a VLAN Interface

1. Overview

By default, the native VLAN of all physical interfaces is VLAN 1, which can implement Layer 2 communication. To implement Layer 3 communication between users in different VLANs and network segments, you can configure the VLAN interface, which is a Layer 3 logical interface.

2. Procedure

Step1: In the configuration mode, create a VLAN.

Note: The VLAN ID has been pre-configured in system from version 4.3.2 and you don't need to configure it.

```
set vlans vlan-id <vlan-id>
```

vlan-id <vlan-id>: specifies the VLAN tag identifier. The valid VLAN numbers range 1-4094. User can specify a range of VLAN numbers, e.g. 2,3,5-100.

Step2: Specify the created VLAN as the native VLAN for a physical interface.

```
set interface gigabit-ethernet <interface-name> family ethernet-switching native-vlan-id <vlan-id>
```

Step3: Associate a Layer 3 interface with the VLAN.

```
set vlans vlan-id <vlan-id> l3-interface <interface-name>
```

l3-interface <interface-name>: specifies a name for the Layer 3 interface.

Step4: Configure an IP address for the VLAN interface.

```
set l3-interface vlan-interface <vlan-id> address <ipv4-address | ipv6-address> prefix-length  
<prefix-number>
```

Step5: Commit the configuration.

```
commit
```

3. Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show l3-interface vlan-interface <vlan-id>** command to view the state, IP address, MAC address, VLAN, MTU, description and traffic statistics.

4. Other Configurations

To clear the configuration of VLAN interface, use **delete l3-interface vlan-interface <vlan-id>** command.

3.2 Configuring the Routing

Routing is a process of forwarding packets from one network to a destination address in another network. The implement of route selection and packet forwarding is based on various routes stored in the routing table. To maintain the routing table, you can manually add or configure different routing protocols.

The switch supports direct routing, static routing and dynamic routing.

- Direct routing: discovered by a data link layer protocol.
- Static routing: manually configured.
- Dynamic routing: discovered by a dynamic routing protocol.

It includes the following chapters:

3.2.1 Configuring the Static Routing

1. Overview

The static routing is manually configured, which requires low system performance and is applicable to small-size network with simple and stable topologies.

2. Procedure

Before configuring the routing, make sure that the Layer 3 interface has been configured.

Step1: By default, the IP routing function is disabled. In the configuration mode, enable the IP routing function.

```
set ip routing enable true
```

Step2: Specify the destination address, and configure one of next-hop IP address and outgoing interface as needed.

```
set protocols static route <ip/prefixlen> next-hop <nexthop-address>
```

- **route <ip/prefixlen>**: specifies a destination IPv4 or IPv6 address and the prefix length of 1 to 32 for IPv4 and 1 to 128 for IPv6.
- **next-hop <nexthop-address>**: specifies the next-hop IP address.

```
set protocols static interface-route <ip/prefixlen> interface <interface-name>
```

- **interface <interface-name>**: specifies the Layer 3 interface as an outgoing interface. The value could be a VLAN interface, loopback interface, routed interface or sub-interface.

Step3: Commit the configuration.

```
commit
```

3. Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show route static** command to view all static routing entries.

4. Other Configurations

To clear the configuration of static interface, use **delete protocols static route<ip/prefixlen>** command.

3.2.2 Configuring the Dynamic Routing

The dynamic routing is based on algorithm, which requires higher system performance. It is applicable to network with a large number of Layer 3 devices, and can automatically adapt to the changeable network topology.

The switch supports multiple dynamic routing, such as OSPF, BGP, IS-IS, etc. OSPF is the IGP (Interior Gateway Protocol) recommended by PicOS. Take the OSPF routing as an example to introduce how to configure a dynamic routing.

1. Overview

OSPF (Open Shortest Path First) is developed by IETF (Internet Engineering Task Force), which uses the shortest path first (SPF) algorithm to calculate a shortest path tree (SPT) to all destination addresses based on the network topology, and is advertised through link state advertisements (LSAs). It is applicable to the network with several hundred devices, such as small and medium-sized enterprises networks.

PicOS supports OSPFv2 and OSPFv3, which is respectively intended for IPv4 and IPv6.

2. Procedure

Before configuring the routing, make sure that the Layer 3 interface has been configured.

Step1: By default, the IP routing function is disabled. In the configuration mode, enable the IP routing function.

```
set ip routing enable true
```

Step2: Set the OSPF router ID.

```
set protocols ospf router-id <router-id>
```

- **router-id** <router-id>: specifies the OSPF router ID, which can uniquely identify the switch within the domain. The value is in IPv4 dotted decimal format.

Step3: Add the specified network segment to an area. Area 0 is required.

```
set protocols ospf network <ipv4/prefixlen> area {<area-id>| ipv4}
```

- **network** <ipv4/prefixlen>: specifies the network prefix and prefix length in IPv4 format.
- **area** {<area-id>| ipv4}: specifies the OSPF area, the value could be in IPv4 dotted decimal format or an integer ranging from 0 to 4294967295.

Step4: Commit the configuration.

```
commit
```

3. Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show route ospf** command to view all OSPF

routing entries.

4. Other Configurations

To delete the OSPF routing configuration, use **delete protocols ospf** command.

Chapter 4 Security Configuration

4.1 Configuring an ACL

1. Overview

ACL (Access Control List) is packet filtering rules through defining conditions of source addresses, destination addresses, interfaces, etc. The switch permits or denies packets according to the configured action of ACL rules.

ACL can manage network access behaviors, prevent network attacks, and improve bandwidth utilization through accurately identifying and controlling packets, which ensures network security and service quality.

2. Procedure

Step1: Set the sequence number of priority.

```
set firewall filter <filter-name> sequence <sequence-number>
```

- **sequence** <sequence-number>: specifies the sequence number. Smaller values represent higher priorities. The range is 0-9999.

Step2: Specify the source address and source port to filter matched packets.

```
set firewall filter <filter-name> sequence <sequence-number> from {source-address-ipv4  
<address/prefix-length> | source-address-ipv6 <address/prefix-length> | source-mac-address  
<mac-address> | source-port <port-number>}
```

- **source-port** <port-number>: specifies the source port number or port number range, for example, 5000 or 7000..7050.

Step3: Specify the execution action for packets matching the filter.

```
set firewall filter <filter-name> sequence <sequence-number> then action {discard | forward}
```

- **action** {discard | forward}: discards or forwards matched packets.

Step4: Specify the physical interface, VLAN interface or routed interface to filter matched incoming and egress packets.

```
set firewall filter <filter-name> input {interface <interface-name> | vlan-interface <vlan-interface-name> |  
routed-interface <routed-interface-name>}
```

```
set firewall filter <filter-name> output {interface <interface-name> | vlan-interface <vlan-interface-name> |  
routed-interface <routed-interface-name>}
```

Step5: Commit the configuration.

```
commit
```

3. Verifying the Configuration

After the configuration is completed, in the configuration mode, use **run show filter <filter-name> [sequence <sequence-number>]** command to view the matching condition of specified filter.

4. Other Configurations

To delete the configured filter, use **delete firewall filter<filter-name>** command.

4.2 Configuring the SSH Access

1. Overview

SSH (Secure Shell) is an encryption network protocol, which can perform secure access and file transmission in the unsecured network. It performs data exchange through a secure channel, which is established based on TCP. The default port is 22, which can be changed as required for security purposes.

2. Procedure

By default, the SSH service is enabled. You can log in switch through SSH protocol by directly access eth0. Besides, if you want to remotely log in and manage the switch through the Layer 3 interface, you should configure as follows:

Step1: In the configuration mode, specify the loopback interface, VLAN interface or routed interface as the inband management port, both management traffic and data plane traffic can be transmitted through the specified interface. The specified interface should be in the default VRF.

```
set system inband {loopback <ip-address> | vlan-interface <vlan-interface-name> | routed-interface  
<routed-interface-name>}
```

Step2: (Optional) Set the limit number of SSH connections.

set system services ssh connection-limit *<int>*

- **connection-limit** *<int>*: specifies the maximum number of allowed connections, the valid number ranges 0-250. Default value is 0, which removes the connection limit.

Step3: (Optional) Specify the listening port number of SSH server.

set system services ssh port *<port-number>*

- **port** *<port-number>*: specifies the listening port number of the SSH server. The value is an integer ranging from 1 to 65535. The default value is 22.

Step4: Commit the configuration.

commit

3. Verifying the Configuration

After the configuration is completed, use **ssh admin@<ip-address> -p <port>** to check whether the switch can be accessed through SSH.

4. Other Configurations

To disable the SSH service, use **set system services ssh disable true** command.

To delete the SSH configuration, use **delete system services ssh** command.

Chapter 5 Typical Configuration Example

5.1 Overview

Take the following topology as an example to introduce how to implement communication between PC1 and PC2.

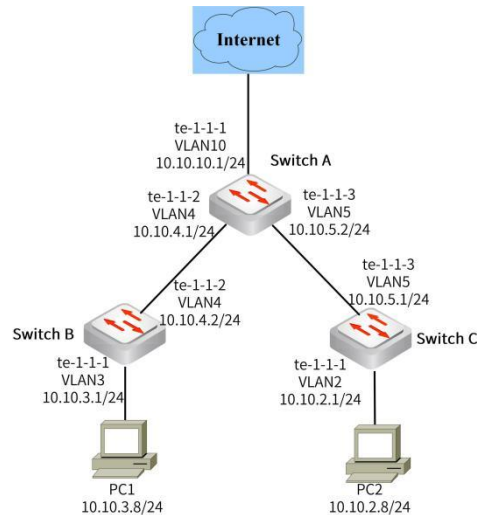


Figure 5-1 Topology of Access Network

The data plan is shown as below.

Device	Interface	VLAN and IP Address
Switch A	te-1-1-1	VLAN: 10 IP address: 10.10.10.1/24
	te-1-1-2	VLAN: 4 IP address: 10.10.4.1/24
	te-1-1-3	VLAN: 5 IP address: 10.10.5.2/24
Switch B	te-1-1-1	VLAN: 3 IP address: 10.10.3.1/24
	te-1-1-2	VLAN: 4 IP address: 10.10.4.2/24
Switch C	te-1-1-1	VLAN: 2 IP address: 10.10.2.1/24
	te-1-1-3	VLAN: 5 IP address: 10.10.5.1/24
PC1	10.10.3.8/24	
PC2	10.10.2.8/24	

5.2 Procedure

Before configuring the following steps, make sure you have logged in the specified switch through Console port or SSH.
For detailed information, see [Initial Setup](#) and [Configuring the SSH Access](#).

Step1: In the configuration mode, configure the host name of switch respectively as SwitchA, SwitchB and SwitchC.

Run the same command on other switches to change the hostname as SwitchB and SwitchC.

```
1.admin@PICOS> configure
2.admin@PICOS# set system hostname SwitchA
3.admin@PICOS# commit
4.admin@SwitchA#
```

Step2: Configure the interface and VLAN.

- **Switch A**

Interface te-1-1-1:

```
1.admin@SwitchA# set vlans vlan-id 10
2.admin@SwitchA# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 10
3.admin@SwitchA# set vlans vlan-id 10 l3-interface vlan10
4.admin@SwitchA# set l3-interface vlan-interface vlan10 address 10.10.10.1 prefix-length 24
5.admin@SwitchA# commit
```

Interface te-1-1-2:

```
1.admin@SwitchA# set vlans vlan-id 4
2.admin@SwitchA# set interface gigabit-ethernet te-1/1/2 family ethernet- admin@SwitchA# switching
native-vlan-id 4
3.admin@SwitchA# set vlans vlan-id 4 l3-interface vlan4
4.admin@SwitchA# set l3-interface vlan-interface vlan4 address 10.10.4.1 prefix-length 24
```

```
5.admin@SwitchA# commit
```

Interface te-1-1-3:

```
1.admin@SwitchA# set vlans vlan-id 5

2.admin@SwitchA# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 5

3.admin@SwitchA# set vlans vlan-id 5 l3-interface vlan5

4.admin@SwitchA# set l3-interface vlan-interface vlan5 address 10.10.5.2 prefix-length 24

5.admin@SwitchA# commit
```

● Switch B**Interface te-1-1-1:**

```
1.admin@SwitchB# set vlans vlan-id 3

2.admin@SwitchB# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 3

3.admin@SwitchB# set vlans vlan-id 3 l3-interface vlan3

4.admin@SwitchB# set l3-interface vlan-interface vlan3 address 10.10.3.1 prefix-length 24

5.admin@SwitchB# commit
```

Interface te-1-1-2:

```
1.admin@SwitchB# set vlans vlan-id 4

2.admin@SwitchB# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 4

3.admin@SwitchB# set vlans vlan-id 4 l3-interface vlan4

4.admin@SwitchB# set l3-interface vlan-interface vlan4 address 10.10.4.2 prefix-length 24

5.admin@SwitchB# commit
```

● Switch C**Interface te-1-1-1:**

```
1.admin@SwitchC# set vlans vlan-id 2

2.admin@SwitchC# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 2

3.admin@SwitchC# set vlans vlan-id 2 l3-interface vlan2

4.admin@SwitchC# set l3-interface vlan-interface vlan2 address 10.10.2.1 prefix-length 24

5.admin@SwitchC# commit
```

Interface te-1-1-3:

```
1.admin@SwitchC# set vlans vlan-id 5

2.admin@SwitchC# set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 5

3.admin@SwitchC# set vlans vlan-id 5 l3-interface vlan5

4.admin@SwitchC# set l3-interface vlan-interface vlan5 address 10.10.5.1 prefix-length 24

5.admin@SwitchC# commit
```

Step3: Configure the IP address and default gateway of PC1 and PC2.

PC1:

```
1.root@UbuntuDockerGuest-1:~# ifconfig eth0 10.10.3.8/24

2.root@UbuntuDockerGuest-1:~# route add default gw 10.10.3.1
```

PC2:

```
1.root@UbuntuDockerGuest-2:~# ifconfig eth0 10.10.2.8/24

2.root@UbuntuDockerGuest-2:~# route add default gw 10.10.2.1
```

Step4: Configure the routing. You can configure the static routing or OSPF routing to connect network.

- **Connecting network through the static routing**

Switch A:

```
1.admin@SwitchA# set ip routing enable true

2.admin@SwitchA# set protocols static route 10.10.2.0/24 next-hop 10.10.5.1

3.admin@SwitchA# set protocols static route 10.10.3.0/24 next-hop 10.10.4.2

4.admin@SwitchA# commit
```

Switch B:

```
1.admin@SwitchB# set ip routing enable true

2.admin@SwitchB# set protocols static route 0.0.0.0/0 next-hop 10.10.4.1

3.admin@SwitchB# commit
```

Switch C:

```
1.admin@SwitchC# set ip routing enable true

2.admin@SwitchC# set protocols static route 0.0.0.0/0 next-hop 10.10.5.2

3.admin@SwitchC# commit
```

● Connecting network through the OSPF routing**Switch A:**

```
1.admin@SwitchA# set l3-interface loopback lo address 1.1.1.1 prefix-length 32

2.admin@SwitchA# set protocols ospf router-id 1.1.1.1

3.admin@SwitchA# set protocols ospf network 10.10.4.0/24 area 0

4.admin@SwitchA# set protocols ospf network 10.10.10.0/24 area 0

5.admin@SwitchA# set protocols ospf network 10.10.5.0/24 area 1

6.admin@SwitchA# commit
```

Switch B:

```
1.admin@SwitchB# set l3-interface loopback lo address 2.2.2.2 prefix-length 32

2.admin@SwitchB# set protocols ospf router-id 2.2.2.2

3.admin@SwitchB# set protocols ospf network 10.10.4.0/24 area 0

4.admin@SwitchB# set protocols ospf network 10.10.3.0/24 area 0

5.admin@SwitchB# commit
```

Switch C:

```
1.admin@SwitchC# set l3-interface loopback lo address 3.3.3.3 prefix-length 32

2.admin@SwitchC# set protocols ospf router-id 3.3.3.3

3.admin@SwitchC# set protocols ospf network 10.10.2.0/24 area 1

4.admin@SwitchC# set protocols ospf network 10.10.5.0/24 area 1

5.admin@SwitchC# commit
```

5.3 Verifying the Configuration

- View the routing table of each switch.

1. Static Routing:

```
admin@SwitchA# run show route static
RIB entry for static
=====
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, D - SHARP, F - PBR,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

S>* 10.10.2.0/24 [1/0] via 10.10.5.1, vlan5, weight 1, 00:07:36
S>* 10.10.3.0/24 [1/0] via 10.10.4.2, vlan4, weight 1, 00:07:36
```

Figure 5-2 Static Routing Entries of SwitchA

```
admin@SwitchB# run show route static
RIB entry for static
=====
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, D - SHARP, F - PBR,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

S>* 0.0.0.0/0 [1/0] via 10.10.4.1, vlan4, weight 1, 00:10:38
```

Figure 5-3 Static Routing Entries of SwitchB

```
admin@SwitchC# run show route static
RIB entry for static
=====
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, D - SHARP, F - PBR,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

S>* 0.0.0.0/0 [1/0] via 10.10.5.2, vlan5, weight 1, 00:13:07
```

Figure 5-4 Static Routing Entries of SwitchC

2. OSPF Routing:

```
admin@SwitchA# run show route ospf
RIB entry for ospf
=====
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, D - SHARP, F - PBR,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

O>* 10.10.2.0/24 [110/200] via 10.10.5.1, vlan5, weight 1, 00:05:42
O>* 10.10.3.0/24 [110/200] via 10.10.4.2, vlan4, weight 1, 00:05:42
O 10.10.4.0/24 [110/100] is directly connected, vlan4, weight 1, 00:05:52
O 10.10.5.0/24 [110/100] is directly connected, vlan5, weight 1, 00:06:30
O 10.10.10.0/24 [110/100] is directly connected, vlan10, weight 1, 00:06:30
```

Figure 5-5 OSPF Routing Entries of SwitchA

```
admin@SwitchB# run show route ospf
RIB entry for ospf
=====
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, D - SHARP, F - PBR,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

O>* 10.10.2.0/24 [110/300] via 10.10.4.1, vlan4, weight 1, 00:10:41
O 10.10.3.0/24 [110/100] is directly connected, vlan3, weight 1, 00:11:27
O 10.10.4.0/24 [110/100] is directly connected, vlan4, weight 1, 00:11:27
O>* 10.10.5.0/24 [110/200] via 10.10.4.1, vlan4, weight 1, 00:10:41
O>* 10.10.10.0/24 [110/200] via 10.10.4.1, vlan4, weight 1, 00:10:41
```

Figure 5-6 OSPF Routing Entries of SwitchB

```

admin@SwitchC# run show route ospf
RIB entry for ospf
=====
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, D - SHARP, F - PBR,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

O   10.10.2.0/24 [110/100] is directly connected, vlan2, weight 1, 00:14:17
O>* 10.10.3.0/24 [110/300] via 10.10.5.2, vlan5, weight 1, 00:13:32
O>* 10.10.4.0/24 [110/200] via 10.10.5.2, vlan5, weight 1, 00:13:32
O   10.10.5.0/24 [110/100] is directly connected, vlan5, weight 1, 00:14:16
O>* 10.10.10.0/24 [110/200] via 10.10.5.2, vlan5, weight 1, 00:13:32

```

Figure 5-7 OSPF Routing Entries of SwitchC

- Run Ping command to check the connectivity between PC1 and PC2.

1. PC1 ping PC2:

```

root@UbuntuDockerGuest-1:~# ping 10.10.2.8
PING 10.10.2.8 (10.10.2.8) 56(84) bytes of data.
64 bytes from 10.10.2.8: icmp_seq=1 ttl=61 time=29.1 ms
64 bytes from 10.10.2.8: icmp_seq=2 ttl=61 time=1.99 ms
64 bytes from 10.10.2.8: icmp_seq=3 ttl=61 time=2.29 ms
64 bytes from 10.10.2.8: icmp_seq=4 ttl=61 time=3.27 ms
64 bytes from 10.10.2.8: icmp_seq=5 ttl=61 time=3.92 ms
64 bytes from 10.10.2.8: icmp_seq=6 ttl=61 time=2.44 ms

```

Figure 5-8 Result of PC1 Ping PC2

2. PC2 ping PC1:

```

root@UbuntuDockerGuest-2:~# ping 10.10.3.8
PING 10.10.3.8 (10.10.3.8) 56(84) bytes of data.
64 bytes from 10.10.3.8: icmp_seq=1 ttl=61 time=2.01 ms
64 bytes from 10.10.3.8: icmp_seq=2 ttl=61 time=2.92 ms
64 bytes from 10.10.3.8: icmp_seq=3 ttl=61 time=2.53 ms
64 bytes from 10.10.3.8: icmp_seq=4 ttl=61 time=2.62 ms
64 bytes from 10.10.3.8: icmp_seq=5 ttl=61 time=2.77 ms
64 bytes from 10.10.3.8: icmp_seq=6 ttl=61 time=2.49 ms

```

Figure 5-9 Result of PC2 Ping PC1