

www.raisecom.com

SNMP Commands-1



CONTENTS



Chapter 1	SNMP Commands	1
1.1	show snmp access	1
1.2	show snmp community	2
1.3	show snmp config	2
1.4	show snmp group	3
1.5	show snmp host	4
1.6	show snmp statistics	5
1.7	show snmp trap remote	6
1.8	show snmp user	7
1.9	show snmp view	8
1.10	snmp trap remote	9
1.11	snmp-server access	9
1.12	snmp-server community	11
1.13	snmp-server community	13
1.14	snmp-server contact	14
1.15	snmp-server enable traps	15
1.16	snmp-server group	15
1.17	snmp-server host	17
1.18	snmp-server location	18
1.19	snmp-server user	19
1.20	snmp-server view	20

Chapter 1 SNMP Commands

1.1 show snmp access

[Function]

Use **show snmp access** to show snmp access group information.

[Command Format]

show snmp access

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

Show snmp access group information.

[Example]

Show snmp access group information:

Raisecom#**show snmp access**

```
Index:          0
Group:          initial
Security Model:  usm
Security Level:  authnopriv
Context Prefix:  --
Context Match:   exact
Read View:       internet
Write View:       internet
Notify View:      internet

Index:          2
Group:          initialnone
Security Model:  usm
Security Level:  noauthnopriv
Context Prefix:  --
Context Match:   exact
Read View:       system
Write View:       --
Notify View:      internet
```

[Related commands]

Commands	Description
snmp-server access	Add or modify access control group.
no snmp-server access	Delete access control group.

1.2 show snmp community**[Function]**

Use **show snmp community** to show the community information of snmp protocol.

[Command Format]

show snmp community

[Command Modes]

Privileged EXEC, privileged user

[Executing Command Instruction]

Use **show snmp community** to show the community information of snmp protocol.

[Example]

Show the community information of snmp protocol :

Raisecom#**show snmp community**

<i>Index</i>	<i>Community Name</i>	<i>View Name</i>	<i>Permission</i>

<i>1</i>	<i>public</i>	<i>internet</i>	<i>ro</i>

[Related commands]

Commands	Description
snmp community	Set snmp group information.
show snmp view	Show snmp view information

1.3 show snmp config**[Function]**

Use **show snmp config** command to show the basic config information of snmp.

[Command Format]

show snmp config

[Command Modes]

Privileged EXEC, privileged user

[Executing Command Instruction]

Use this command to show the different quantity statistics that is received or sent by SNMP

Agent.

[Example]

Show the basic config information of snmp:

Raisecom#**show snmp config**

Contact Information: support@Raisecom.com

Device location : world china raisecom

SNMP trap status: Enable

SNMP keepalive trap status: Enable

Send keepalive trap per 500 seconds

SNMP EngineID: 800022b603000e5e1a2b3c

[Related commands]

Commands	Description
snmp-server location	Set location information of snmp
snmp-server contact	Set snmp contact information
snmp-server enable traps	Enable snmp traps
snmp-server keepalive-trap	Enable/disable send keepalive trap periodically.
snmp-server keepalive-trap interval	Set interval of switch to sent keepalive trap to SNMP website station.

1.4 show snmp group

[Function]

Use **show snmp group** to show the map relationship between snmp user and access group.
(Available to devices of ISCOM2000/2100/2800/2900/3000 series and RC5xx series.)

[Command Format]

show snmp group

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

Show the map relationship between snmp user and access control group.

[Example]

Show the map relationship between snmp user and access control group:

Raisecom#**show snmp group**

Index: 0

Group: group1

User Name: guestuser1

Security Model: usm

Index: 1
Group: initialN/A
User Name: raisecomN/A
Security Model: usm

Index: 2
Group: initial
User Name: raisecommd5nopriv
Security Model: usm

Index: 3
Group: initial
User Name: raisecomshanopriv
Security Model: usm

[Related commands]

Commands	Description
snmp-server group	Add or modify the map relationship from one user to access control group.
no snmp-server group	Delete the map relationship from one user to access control group.

1.5 show snmp host

[Function]

Use **show snmp host** to show the information of target host server.

[Command Format]

show snmp host

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

Use the command to show the information of target host server.

[Example]

Show the information of snmp target host server:

Raisecom#**show snmp host**

Index: 0
IP address: 10.168. 0. 16
Port: 162

User Name: testuser2

SNMP Version: v3

Security Level: authnopriv

TagList: bridge config interface rmon snmp ospf

[Related commands]

Commands	Description
snmp-server host	Add or modify target host address.
no snmp-server host	Delete target address.

1.6 show snmp statistics

[Function]

Use **show snmp statistics** to show snmp statistical information.

[Command Format]

show snmp statistics

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Use this command to show the quantity statistics that are received and sent by SNMP agent.

[Example]

Show snmp statistical information:

Raisecom#**show snmp statistics**

SNMP packets input:162

Unsupported SNMP version SNMP PDUs: 0

Unknown SNMP community name SNMP PDUs: 0

SNMP community not allowed operation SNMP PDUs: 0

ASN.1 or BER errors SNMP PDUs: 0

Too big SNMP PDUs: 0

Name error SNMP PDUs: 0

Bad value SNMP PDUs: 0

ReadOnly SNMP PDUs: 0

GenErrs SNMP PDUs: 0

Get-Request and Get-Next PDUs MIB objects SNMP PDUs: 0

Set-Request MIB objects SNMP PDUs: 0

Get-Request MIB objects SNMP PDUs: 0

Getnext-Request MIB objects SNMP PDUs: 0

Set-Request MIB objects SNMP PDUs: 0

Get-Response PDUs SNMP PDUs: 0

Received Traps SNMP PDUs: 0

SNMP packets output:0

Error name SNMP PDUs: 0

Too big SNMP PDUs: 0

Bad value SNMP PDUs: 0

Gen Errs SNMP PDUs: 0

Get request SNMP PDUs: 0

Get-next SNMP PDUs: 0

Set Request SNMP PDUs: 0

Get Responses SNMP PDUs: 0

Trap SNMP PDUs: 0

Unsupported security level SNMP PDUs: 0

Not in time window SNMP PDUs: 0

Unknown user name SNMP PDUs: 0

Unknown EngineID SNMP PDUs: 0

Wrong Digests SNMP PDUs: 0

Decryption Errors SNMP PDUs: 0

1.7 show snmp trap remote

[Function]

Show the enable configuration of remote trap.

[Command Format]

show snmp trap remote

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

Use the command to show the enable configuration of remote trap.

[Command executing echo]

Show the enable configuration of remote trap:

SNMP Remote Trap: Enable

[Example]

Show the enable configuration of remote trap:

Raisecom(config)#**show snmp trap remote**

[Related commands]

Commands	Description
snmp trap remote { <i>enable/ disable</i> }	Enable/disable remote trap.

1.8 show snmp user

[Function]

Use **show snmp user** to show snmp user information.

[Command Format]

show snmp user

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Show snmp user information.

[Example]

Show snmp user information:

Raisecom#**show snmp user**

```

Index:          0
User Name:      guestuser1
Security Name:  guestuser1
EngineID:       800022b603000e5e1a2b3c
Authentication: MD5
Privacy:        NoPriv

Index:          1
User Name:      raisecomnone
Security Name:  raisecomnone
EngineID:       800022b603000e5e1a2b3c
Authentication: NoAuth
Privacy:        NoPriv

Index:          2
User Name:      raisecommd5nopriv
Security Name:  raisecommd5nopriv
EngineID:       800022b603000e5e1a2b3c
Authentication: MD5
Privacy:        NoPriv

```

Index: 3
User Name: raisecomshanopriv
Security Name: raisecomshanopriv
EngineID: 800022b603000e5e1a2b3c
Authentication: SHA
Privacy: NoPriv

[Related commands]

Commands	Description
snmp-server user	Add or modify user list.
no snmp-server user	Delete a snmp user

1.9 show snmp view

[Function]

Use **show snmp view** to show snmp view information.

[Command Format]

show snmp view

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Show snmp view information.

[Example]

Show snmp view information:

Raisecom#**show snmp view**

Index: 0
View Name: system
OID Tree: 1.3.6.1.2.1.1
Mask: --
Type: included

Index: 1
View Name: internet
OID Tree: 1.3.6
Mask: --
Type: included

[Related commands]

Commands	Description
snmp-server view	Add or modify view.
no snmp-server view	Delete view.

1.10 snmp trap remote

[Function]

Enable/disable remote trap.

[Command Format]

snmp trap remote *enable*

snmp trap remote *disable*

[Parameter]

enable: enable remote trap;

disable: disable remote trap.

[Default]

enable

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Use the command to enable/disable remote trap. When enable remote trap, it is authorized to sent trap to SNMP network management if receives remote OAM notification frame; when disable remote trap, can not sent trap to SNMP if receives remote OAM notification frame.

[Command executing echo]

Set the command successfully:

Set successfully

[Example]

Enable remote trap:

Raisecom(config)# **snmp trap remote** *enable*

[Related commands]

Commands	Description
[no] snmp-server enable traps	Enable snmp sends trap.

1.11 snmp-server access

[Function]

Add a SNMP access group. **no** command to delete.

[Command Format]

Add a SNMP access group:

```
snmp-server access groupname [read readview] [write writeview] [notify notifyview] {v1sm | v2csm}
```

```
snmp-server access groupname [read readview] [write writeview] [notify notifyview] [contextname {exact | prefix}] usm { noauthnopriv | authnopriv }
```

Delete a SNMP access group:

```
no snmp-server access groupname [context contextname] usm { noauthnopriv | authnopriv }
```

```
no snmp-server access groupname {v1sm | v2csm}
```

[Parameter]

groupname: group name, length should be less 32 characters;

read: specify read view;

readview: the name of readview, the length should be less than 32 characters;

write: specify write view;

writeview: the name of writview, length should be less than 32 character;

notify: specify general view;

notifyview: notify the name of the view, the length should be less than 32 characters;

context: Specify the name of context;

contextname: the name of context or prefix, length should be less than 32 characters;

exact: contextname fully match context;

prefix: contextname match frontal characters of the context;

v1sm: (Security Model)SNMPv1;

v2csm: (Community based Security Model)SNMPv2c;

usm: (User based Security Model)SNMPv3;

noauthnopriv: Security level; do not encrypt and distinguish;

authnopriv: Security level, distinguish but do not encrypt.

[Default]

Default readview is Internet scope including all the MIB variables in 1.3.6 tree. Default write is empty; default notifyview is Internet. Default context match option is **exact**.

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

Set the priority of access group, the relationship between access group and view including the name of access group, security model, security level, write and read notifyview and name matching of context. The general read and write view is the view which is set by **snmp-server**

view. When the last option is **exact**, the content name of incoming message should fully match the contextname of access group; when the last option is **prefix**, the contextname of incoming message only need to match the prefix of the context.

When the security is **v1sm** or **v2csm**, security level is **noauthnopriv**.

[Explanation of command execution echo]

Set successfully.

Group name too long!

Read view name too long!

Write view name too long!

Notify view name too long!

Context prefix too long!

Unsupported security model !

Unsupported security level !

Set unsuccessfully!

[Example]

Creat a guestgroup access group, the security mode is **usm**, the security level is distinguish but not encrypted, readview is **mib2**, writeview and notifyview are default view:

Raisecom(config)#**snmp-server access guestgroup read mib2 usm authnopriv**

Delete guestgroup:

Raisecom(config)#**no snmp-server access guestgroup usm authnopriv**

[Related commands]

Commands	Description
show snmp access	Show all the items in the access table.

1.12 snmp-server community

[Function]

Set community name and the corresponding view and access priority.

[Command Format]

snmp-server community *community-name* [*view view-name*] {**ro** | **rw**}

no snmp-server community *community-name*

[Parameter]

community-name: community name, string, less than 32;

view view-name: view name, less than 32;

ro: Gives read access to the community, but does not allow write access;

rw: Gives read and write access to authorized management stations to all objects in the MIB.

[Default]

Default view is internet.

[Command Modes]

Global configuration mode; privileged user mode

[Executing Command Instruction]

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the network management system to access the switch, the community string definitions on the NMS must match at least one of the three community string definitions on the switch.

Both SNMPv1 and SNMPv2 adopt community authentication solution. The SNMP message with community not complies with authenticated by device will be discarded. The community has read-only and read-write access privilege only. Just community with read-only privilege can query device information while community with read-write privilege can configure device.

This command can also designate view corresponding to community and makes the community can access designated MIB variable in switch only. If no view keyword was input, the community name corresponding to default view internet.

Explanation of command execution echo]

Set successfully!

Set community name successfully.

Community name is too long(less than 32)

The entered community name is longer than 32.

View name is too long(less than 32)

The entered view name is longer than 32.

No so many space for create community (less equal 8)

There are already 8 communities.

Set unsuccessfully.

Set community name unsuccessfully.

[Example]

Define community raisecom,the relative default view is internet,priority is read and write:

```
Raisecom(config)# snmp-server community raisecom rw
```

Define community guest,the default view is mib2,read-only priority:

```
Raisecom(config)# snmp-server view mib2 1.3.6.1.2.1 included
```

```
Raisecom(config)#snmp-server community guest view mib2 ro
```

[Related commands]

Commands	Description
snmp-server view	Set a view.
show snmp community	Show SNMP community information
show snmp view	Show SNMP view information

1.13 snmp-server community

[Function]

Set community name of remote device.

[Command Format]

```
snmp-server community community-name {ro | rw}
```

```
no snmp-server community community-name
```

[Parameter]

community-name: community name, string, less than 32;

ro: Gives read access to the community, but does not allow write access;

rw: Gives read and write access to authorized management stations to all objects in the MIB.

[Command Modes]

Remote configuration mode; privileged user

[Executing Command Instruction]

Use this command under remote configuration mode to configure remote device SNMP community name. The community is the index 3 in the community table, view as internet.

Explanation of command execution echo]

Remote device X does not support the command.

Remote device is not in support of this command, command executing fail. This result won't affect other device operation if operate several remote device at the same time.

Remote device X extended-oam link is not established.

Command executing fails for remote device has not establish extended OAM link.

Remote device X set unsuccessfully.

Command executing fails on remote device.

Set successfully

Command executing successfully.

Community name can not exceed 20 characters !

The community name is too long.

[Example]

Set remote device SNMP community name:

Raisecom(config-remote)# **write**

[Related commands]

Commands	Description
show remote-device information	Show remote device information.

1.14 snmp-server contact

[Function]

Configure the network administrator contact information.

[Command Format]

[no] snmp-server contact *sysContact*

[Parameter]

sysContact: the contact information of network administrator, character string type.

[Default]

The default contact information is `mailto:support@Raisecom.com`

[Command Modes]

Global configuration mode; privileged user mode

[Executing Command Instruction]

The information includes the contact information of network administrator, so when help is needed, please refer this information for help.

[Explanation of command execution echo]

Set successfully!

Set unsuccessfully

[Example]

Set up the contact information to service@raisecom.com:

Raisecom(config)# **snmp-server contact** service@raisecom.com

[Related commands]

Commands	Description
show snmp config	Show the contact information of network administrator.

1.15 snmp-server enable traps

[Function]

Enable the trap function of SNMP.

[Command Format]

[no] snmp-server enable traps

[Default]

Enable traps

[Command Modes]

Global configuration mode; privileged user mode

[Executing Command Instruction]

The switch will send notifications to SNMP managers when particular events occur if SNMP-server enables trap function.

[Explanation of command execution echo]

Set successfully!

Set unsuccessfully

[Example]

Set send ospf protocol trap enable:

Raisecom(config)# **snmp-server enable traps ospf**

[Related commands]

Commands	Description
snmp-server host	Set target host of trap.

1.16 snmp-server group

[Function]

Add or delete the mapping relationship of a user and access group. **no** command is used to delete.

[Command Format]

[no] snmp-server group *groupname* **user** *username* { **v1sm** | **v2csm** | **usm** }

[Parameter]

groupname: group name, the length is less than 32 characters.

user: specify user name.

username: username, the length should be less than 32 characters.

v1sm: (Community based Security Model) SNMPv1.

v2csm: (Community based Security Model) SNMPv2c.

usm: (User based Security Model) SNMPv3.

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

A user will belong to an access group according to safety model, and different access group users have different access privilege.

[Explanation of command execution echo]

Set successfully

Command executing successfully.

Group name too long!

The length of access group name should not longer than 32 characters.

User name too long!

Please input user name in length lower than 32 characters.

Unsupported security model!

Set unsuccessfully!

Fail to set.

[Example]

Map guestuser1 with the security usm level to guestgroup:

Raisecom(config)#**snmp-server group** *guestgroup* **user** *guestuser1* *usm*

Delete the mapping from guestuser1 to guestgroup:

Raisecom(config)#**no snmp-server group** *guestgroup* **user** *guestuser1* *usm*

[Related commands]

Commands	Description
show snmp group	Display all the items in the mapping table.

1.17 snmp-server host

[Function]

Add or delete an IP address of trap target.

[Command Format]

Add a SNMP target host server address:

```
snmp-server host A.B.C.D version {1/2c} NAME [udpport <1-65535>] [bridge] [config]  
[interface] [rmon] [snmp] [ospf]
```

```
snmp-server host A.B.C.D version 3 {noauthnopriv/authnopriv} NAME [udpport  
<1-65535>] [bridge] [config] [interface] [rmon] [snmp] [ospf]
```

Delete a SNMP target host server address:

```
no snmp-server host A.B.C.D
```

[Parameter]

addrname: host server address name, length should be less than 32 characters.

paramsname: the parameter name of host server, used to select parameter, length should be less than 32 characters.

A.B.C.D: trap target host IP address, point decimal.

version: the SNMP version which is used by target host.

1: use SNMPv1

2c: use SNMPv2c

3: use SNMPv3\n

authnopriv: authentic but not privacy

noauthnopriv: neither authentic nor privacy.

NAME: SNMPv1/v2c group name or SNMPv3 use name.

udpport: specify UDP port.

<1-65535>: host address receive the udp port number of trap, range is 1-65525.

bridge: bridge trap;

config: config trap;

interface: interface trap;

rmon: rmon trap;

snmp: snmp trap;

ospf: ospf trap.

[Default]

The default UDP port is set to 162; traplist is all the trap.

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Add or delete a target host address.

[Explanation of command execution echo]

Set successfully

User name is too long !

If the user name is longer than 32 characters, display above information.

The input IP address is wrong!

Set unsuccessfully!

[Example]

Add a host address of host_1, ip address is 172.20.21.1, username is Raisecom, SNMP version is v3, authentic but not privacy, all the traps:

Raisecom(config)#**snmp-server host 172.20.21.1 version 3 authnopriv raisecom**

Delete host address-host_1:

Raisecom(config)#**no snmp-server host 172.20.21.1**

[Related commands]

Commands	Description
show snmp host	Show all the information in the host address table.

1.18 snmp-server location

[Function]

Set the description of switch physical location.

[Command Format]

[no] snmp-server location sysLocation

[Parameter]

sysLocation: define the physical location of switch

[Default]

No location description

[Command Modes]

Global configuration mode; privileged user mode

[Executing Command Instruction]

The physical location of the Switch can be viewed for the convenience of network administrators the locate it.

[Explanation of command execution echo]

Set successfully!

Set unsuccessfully!

[Example]

Set the position of switch as HaiTaiEdifice8th:

Raisecom(config)# **snmp-server location** *HaiTaiEdifice8th*

[Related commands]

Commands	Description
show snmp location	Show the physical position information of switch

1.19 snmp-server user

[Function]

Add a new user. **No** command to delete the operation.

[Command Format]

Add a SNMP user:

snmp-server user *username* [**remote engineid**] **authentication**{**md5** | **sha**} *authpassword*

snmp-server user *username* [**remote engineid**]

Delete a SNMP user:

no snmp-server user *username* [**remote engineid**]

[Parameter]

username: username, length should less than 32 characters.

remote: remote SNMP engine ID;

engineid: remote SNMP engine ID. The SNMP engine ID by which username can contact it.

authentication: Specify authentication algorithm.

md5: Use authentication algorithm md5;

sha: Use authentication algorithm sha;

authpassword: authentication password.

[Default]

Default situation is that there are no authentication and no privacy; the authentication password and authentication algorithm have to be selected beforehand; default SNMP engine ID is local engine ID.

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Add or delete a user.

[Explanation of command execution echo]

Set sucessfully

Engine ID is too long!

Input engine ID is wrong!

Failed to get local engine ID!

Authentication key is wrong!

Set unsuccessfully!

[Example]

Add a user guestuser1, local engine ID; md5 authentication algorithm, authentication password is Raisecom; no privacy:

```
Raisecom(config)#snmp-server user guestuser1 authentication md5 raisecom
```

Add a user guestuser3, local engine ID; no authentication and no privacy:

```
Raisecom(config)#snmp-server user guestuser2
```

Delete user guestuser3, local engine ID:

```
Raisecom(config)#no snmp-server user guestuser2
```

[Related commands]

Commands	Description
show snmp user	Show all the items in the user table.

1.20 snmp-server view

[Function]

Add a SNMP view, **no** command to delete the operation.

[Command Format]

Add a snmp view:

```
snmp-server view view-name oid-tree [mask] {included | excluded}
```

Delete a SNMP view:

no snmp-server view *view-name oid-tree*

[Parameter]

view-name: View name, length is below 32;

oid-tree:OID number, length is below 128;

mask: OID tree mask, length is below 128, OID format, OID option can only be 0 or 1;

included: MIB variable in OID tree;

excluded:MIB variable out of OID tree.

[Default]

All the numbers of mask are 1.

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

SNMPv3 defines access mode based on view. Users can use the command to define a view. Mask is the mask of OID subtree, each of its digit corresponding to each option of its tree. If particular digit of the mask is 1, view should according to subtree corresponding option; if particular digit of the mask is 0, then it is not needed to match the subtree corresponding option. The mask length is 16 characters, that is to say it support the subtree with length 128. if subtree of a view is 1.3.6.1.2.1, mask is 1.1.1.1.0.1, the view contains actual subtree 1.3.6.1.x.1 (x can be any number), that is to say the first option of all nodes under 1.3.6.1.

[Explanation of command execution echo]

Set successfully

Name too long !

Oid tree Name NOT correct !

mask too long!

Mask NOT correct !

Set unsuccessfully!

View internet:1.3.6 should NOT be deleted!

[Example]

The following example display how to configure SNMP view:

Create view mib 2, view includes all the MIB variables under 1.3.6.1.2.1:

Raisecom(config)#**snmp-server view mib2 1.3.6.1.2.1 1.1.1.1.0.1 included**

Delete view mib2, subtree is 1.3.6.1.2.1:

```
Raisecom(config)# no snmp-server view mib2 1.3.6.1.2.1
```

[Related commands]

Commands	Description
show snmp view	Show all the information in SNMP view table.



北京瑞斯康达科技发展有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road,
Haidian District, Beijing Postcode: 100085 Tel: +86-10-82883305 Fax: +86-10-82883056
Email: export@raisecom.com <http://www.raisecom.com>