GigaX2024B/M

Layer 2 Managed Switch

CLI Manual

E2644

May 2006 V1

Table of content

CLI Command Modes

Command mode	Access method	Prompt	Exit or Access Next Mode.
User EXEC	This is the first level of access.(For the switch) Change terminal settings, perform basic tasks, and list system information.	Switch>	Exit to enter the EXIT command. To enter privileged EXEC mode, enter the enable command.
Privileged EXEC	From user EXEC mode, enter the enable command.	Switch#	To exit to user EXEC mode, enter the disable command. To enter global configuration mode, enter the configure terminal command.
Global configuration	From privileged EXEC mode, enter the configure command.	Switch (config)#	To exit to privileged EXEC mode, enter the exit or end command, or press Ctrl-Z. To enter interface configuration mode, enter the interface IFNAME configuration command.
Interface configuration	From global configuration mode, specify an interface by entering the interface command followed by an interface identification.	Switch (config-if)#	To exit to privileged EXEC mode, enter the end command, or press Ctrl-Z. To exit to global configuration mode, enter the exit command.
Config-vlan	In global configuration mode, enter the vlan vlan-id command.	Switch (config-vlan)#	To exit to global configuration mode, enter the exit command. To return to privileged EXEC mode, enter the end command, or press Ctrl-Z.
mac access-list extended [NAME]	In global configuration mode, enter the ACL NAME command.	Switch (config-ext-mac)#	To exit to global configuration mode, enter the exit command. To return to privileged EXEC mode, enter the end command, or press Ctrl-Z.

1. IGMP

1.1 ip igmp snooping

Syntax: ip igmp snooping

Parameters: igmp Internet Group Management Protocol

snooping IGMP snooping on all the existing VLANs

Command Mode: Configure terminal mode

No/clear: no ip igmp snooping

Show: show ip igmp snooping

Default: The default setting of IGMP snooping is globally disable

Description: This command sets the IGMP snooping function enabled globally.

Example: ASUS(config)# ip igmp snooping

1.2 ip igmp snooping last-member-query-interval TIMEVALUE

Syntax: ip igmp snooping last-member-query-interval TIMEVALUE

Parameters: igmp Internet Group Management Protocol

snooping IGMP snooping on all the existing VLANs

last-member-query-interval the interval for which the switch waits before updating the table entry

TIMEVALUE the interval for the IGMP queries sent by the switch (default 1 sec) ,valid range is 100~1000 milliseconds.

Command Mode: Configure terminal mode

No/clear: no ip igmp snooping last-member-query-interval

Show: show ip igmp snooping

Default: The default is 1second

Description: This command sets the interval time for the IGMP queries sent by switch.

Example: ASUS(config)# ip igmp snooping last-member-query-interval 100

1.3 ip igmp snooping vlan <1-3000>

Syntax: ip igmp snooping vlan <1-3000>

Parameters:

igmp	Internet Group Management Protocol
snooping	IGMP snooping on all the existing VLANs
vlan	IGMP Snooping enable for a specified vlan
<1-3000>	Vlan number

Command Mode: Configure terminal mode

No/clear: no ip igmp snooping vlan <1-3000>

Show: show ip igmp snooping

show ip igmp snooping vlan <1-3000>

Default: The default setting of IGMP snooping on each vlan is enable after IGMP snooping function is globally enable.

Description: This command sets the IGMP snooping function enabled on indicated vlan.

Example: ASUS(config)# ip igmp snooping vlan 1

1.4 ip igmp snooping vlan <1-3000> immediate-leave

Syntax: ip igmp snooping vlan <1-3000> immediate-leave

Parameters:

igmp	Internet Group Management Protocol
snooping	IGMP snooping on all the existing VLANs
vlan	IGMP Snooping enable for a specified vlan
<1-3000>	Vlan number
immediate-leave	Enable IGMP Immediate-Leave processing

Command Mode: Configure terminal mode

No/clear: no ip igmp snooping vlan <1-3000> immediate-leave

Show: show ip igmp snooping vlan <1-3000>

Default: The default setting of igmp immediate-leave on each vlan is

disabled after IGMP snooping function is globally enable.

Description: This command sets the IGMP snooping immediate-leave function enabled on indicated vlan.

Example: ASUS(config)# ip igmp snooping vlan 1 immediate-leave

1.5 show ip igmp snooping

Syntax: show ip igmp snooping

Parameters: snooping Snooping information on all Vlans

Command Mode: Privileged EXEC mode

Default: None or depends on ODM customer

Description: Use the show ip igmp privileged EXEC command to view all configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile.

Example: ASUS# show ip igmp snooping

1.6 show ip igmp snooping vlan <1-3000>

Syntax: show ip igmp snooping vlan <1-3000>

Parameters: vlan Snooping information on a specified vlan

<1-3000> VLAN number

Command Mode: Privileged EXEC mode

Default: None or depends on ODM customer

Description: Use the show ip igmp snooping vlan privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping vlan for the switch or multicast information for the selected parameter. Use with the vlan keyword to display the VLAN or information about the selected parameter for the VLAN.

Example: ASUS# show ip igmp snooping vlan 1

LACP:

2.1 lacp aggregation-link group <1-32> (add|set) IFLIST

GX2024B GROUPID range is 1-6

Syntax	lacp aggregation-link trunk <1-32> (add|set) IFLIST	
Parameters	aggregation-link	aggregation-link
	<1-32>	GROUPID
	add	append ports to lacp enabled port list
	set	set lacp enabled port list for this group
	PORTLIST valid format is port_id,[,port_id...],[-port_id,...],...	
Command Mode	Configure terminal mode	
No/clear	lacp aggregation-link group delete IFNAME	
	no lacp aggregation-link group <1-32>	
Show	show lacp [GROUPID]	
Default	No default lacp aggregation-link trunk group enable	
Description	This command sets the Link Aggregation Control Protocol (LACP) operation add/set for the trunk group ports on the switch stack or on a standalone switch.	
Example	ASUS(config)# lacp aggregation-link group <1-32> (add|set) fa1/0/1-4	

2.2 lacp aggregation-link group delete IFNAME

Syntax	lacp aggregation-link group delete IFNAME	
Parameters	aggregation-link	aggregation-link
	group	group
	delete	remove ports from lacp enabled port list
	IFNAME	interface name
Command Mode	Configure terminal mode	

No/clear	lacp aggregation-link group delete IFNAME
Show	show aggregation-link group [GROUPID]
Default	No default lacp aggregation-link trunk group enable
Description	This command sets the Link Aggregation Control Protocol (LACP) operation add/set or disable for the trunk group ports on the switch stack or on a standalone switch.
Example	ASUS(config)# lacp aggregation-link group delete fa1/0/1

2.3 lacp system-priority <1-65535>

Syntax	lacp system-priority <1-65535>	
Parameters	system-priority	Priority of the system
	<1-65535>	Valid values are from 1 to 65535
Command Mode	Configure terminal mode	
No/clear	no lacp system-priority	
Show	show lacp system-priority / show running-config	
Default	The default is 32768.	
Description	This command sets the system priority for the Link Aggregation Control Protocol (LACP) on the switch stack or on a standalone switch.	
Example	ASUS(config)# lacp system-priority 2000	

2.4 show lacp [GROUPID]

GX2024B GROUPID range is 1-6

Syntax	show lacp [GROUPID]
Parameters	[GROUPID] valid group-id range is 1 to 32
Command Mode	Privileged EXEC mode
Default	None or depends on ODM customer
Description	Use the show lacp user EXEC command to display Link Aggregation Control Protocol (LACP) channel-group information.
Example	ASUS#show lacp 1

3. Static Link Aggregation

3.1 aggregation-link group <1-32> PORTLIST

GX2024B GROUPID range is 1-6

Syntax	aggregation-link trunk <1-32> PORTLIST	
Parameters	aggregation-link	static trunk aggregation link information
	group	link trunk group
	GROUPID	Trunk group ID 1-32
Command Mode	Configure terminal mode	
No/clear	no aggregation-link group <1-32>	
show	show aggregation-link group <1-32>	
Default	None or depends on ODM customer	
Description	Use the aggregation-link trunk group configuration command on the switch stack or standalone switch to configure trunk aggregation group.	
Example	ASUS(config)#aggregation-link group 1 fa1/0/1-4	

3.2 aggregation-link group <1-32> load-balance (src-mac |dst-mac |src-dst-mac |src-ip |dst-ip |src-dst-ip)

GX2024B GROUPID range is 1-6

Syntax	aggregation-link group <1-32> load-balance (src-mac ldst-mac lsrc-dst-mac lsrc-ip ldst-ip lsrc-dst-ip)	
Parameters	GROUPID	Trunk group ID 1-32
	src-mac ->	Source Mac address.
	dst-mac ->	Destination Mac address.
	src-dst-mac ->	Source and Destination Mac address.
	src-ip ->	Source IP address.

	dst-ip ->	Destination IP address.
	src-dst-ip ->	Source and Destination IP address.
Command Mode	Configure terminal mode	
No/clear		
show	show aggregation-link group <1-32>	
Default	None or depends on ODM customer	
Description	Use the aggregation-link trunk group configuration command on the switch stack or standalone switch to configure trunk load balancing by using source-based or destination-based forwarding methods.	
Example	ASUS(config)# aggregation-link group 1 load-balance src-mac	

3.3 show aggregation-link group [GROUPID]

GX2024B GROUPID range is 1-6

Syntax	show aggregation-link group [GROUPID]	
Parameters	aggregation-link	static trunk aggregation link information
	group	Trunk mode
	[GROUPID]	1-32
Command Mode	Privileged EXEC mode	
Default		
Description	To show aggregation-link trunk status.	
Example	ASUS# show aggregation-link group 1	

4. GVRP

4.1 clear gvrp statistics [IFNAME]

Syntax	clear gvrp statistics [IFNAME]
Parameters	[IFNAME] Interface's name, ex: fastethernet1/0/1 or gigabitethernet1/0/26
Command Mode	Configure terminal mode

No/clear

Show

Default None or depends on ODM customer

Description Use the clear gvrp statistics configuration command on the switch stack or standalone switch to clear all the GVRP statistics information on one or all interfaces.

Example ASUS(config)# clear gvrp statistics fa1/0/1

4.2 gvrp (enable|disable)

Syntax gvrp (enableldisable)

Parameters disable-> Disable GVRP feature globally on theswitch

enable -> Enable GVRP feature globally on the switch

Command Mode Configure terminal mode

No/clear gvrp disable

Show show gvrp

Default The default is disabled on the switch.

Description This command sets the GVRP feature globally enable or disable on the switch. Or enable with the interface

Example ASUS(config)#gvrp enable

4.3 gvrp (enable|disable)

Syntax gvrp (enableldisable)

Parameters disable -> Disable GVRP feature globally on the switch

enable -> Enable GVRP feature globally on the switch

Command Mode Interface Configure mode

No/clear gvrp disable

Show show gvrp

Default The default is disabled on the switch.

Description This command sets the GVRP feature enable or disable with the interface

Example ASUS(config-if)#gvrp enable

4.4 gvrp registration (normal|fixed|forbidden)

Syntax	gvrp registration (normal|fixed|forbidden)	
Parameters	registration	GVRP registration mode
	normal ->	normal registration mode
	fixed ->	fixed registration mode
	forbidden ->	forbidden registration mode
Command Mode	Interface Configure mode	
No/clear	clear gvrp statistics IFNAME	
Show	show gvrp interface IFNAME	
Default	The default is Normal on each interface after the indicated interface gvrp mode is enabled.	
Description	This command sets the gvrp registration type of the indicated interface.	
Example	ASUS(config-if)# gvrp registration fixed	

4.5 show gvrp

Syntax	show gvrp configuration IFNAME	
Parameters	gvrp	General Attribute Registration Protocol
Command Mode	Privileged EXEC mode	
Default		
Description	To show gvrp configuration status.	
Example	ASUS#show gvrp	

4.6 show gvrp statistics [IFNAME]

Syntax	show gvrp statistics [IFNAME]	
Parameters	gvrp	General Attribute Registration Protocol
	statistics	the GVRP statistics
	[IFNAME]	Interface's name, ex: fastethernet1/0/1 or gigabitethernet1/0/26
Command Mode	Privileged EXEC mode	

Default

Description To show gvrp statistics IFNAME status.

Example ASUS# show gvrp statistics fa1/0/1

4.7 show gvrp interface IFNAME

Syntax show gvrp interface IFNAME

Parameters gvrp General Attribute Registration Protocol

[IFNAME] Interface's name, ex: fastethernet1/0/1 or gigabitethernet1/0/26

Command Mode Privileged EXEC mode

Default

Description To show gvrp port status.

Example ASUS#show gvrp interface fa1/0/1 2

4.8 garp join-timer <1-100000000>

Syntax garp join-timer <1-100000000>

Parameters join-timer Join timer

<1-100000000> the timer values

Command Mode Interface mode

No/clear no garp join-timer

Show show garp timer IFNAME

Default The default is 20 (centi-seconds)

Description This command sets the garp join-timer value in the indicated interface port.

Example ASUS(config-if)#garp join-timer 20

4.9 garp leaveall-timer <1-100000000>

Syntax garp leaveall-timer <1-100000000>

Parameters leave-timer Leave timer

<1-100000000> the timer values

Command Mode	Interface mode
No/clear	no garp leaveall-timer
Show	show garp timer IFNAME
Default	The default is 1000 (centi-seconds)
Description	This command sets the garp leaveall-timer value in the indicated interface port.
Example	ASUS(config-if)#garp leaveall-time 2000

4.10 garp leave-timer <1-100000000>

Syntax	garp leave-timer <1-100000000>	
Parameters	leaveall-timer	Leaveall timer
	<1-100000000>	the timer values
Command Mode	Interface mode	
No/clear	no garp leave-timer	
Show	show garp timer IFNAME	
Default	The default is 60 (centi-seconds)	
Description	This command sets the garp leave-timer value in the indicated interface port.	
Example	ASUS(config-if)#garp leave-timer 60	

4.11 show garp timer IFNAME

Syntax	show garp timer IFNAME	
Parameters	timer	the setting timer values (join, leave, and leaveall timer)
	[IFNAME]	Interface's name, ex: fastethernet1/0/1 or gigabitethernet1/0/26
Command Mode	Privileged EXEC mode	
Default		
Description	To show garp timer IFNAME status.	
Example	ASUS# show garp timer fa1/0/1	

5. VLAN:

5.1 show vlan name VLANAME

Syntax show vlan name VLANAME

Parameters VLANAME vlan name

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description Use the show vlan user EXEC command to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch.

Example ASUS#show vlan name VLAN1

5.2 vlan <2-3000>

Syntax vlan <2-3000>

Parameters vid vlan id

No/clear no vlan <2-3000>

Command Mode Global configuration mode

Default None or depends on ODM customer

Description Use the vlan vid command to create vlan entry on the switch.

Example ASUS(config)#vlan 2

5.3 show vlan [VLANID]

Syntax show vlan [VLANID]

Parameters [VLANID] vlan id

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description Use the show vlan user EXEC command to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch.

Example ASUS#show vlan 2

5.4 name VLANAME

Syntax name VLANAME

Parameters VLANAME - vlan name string

No/clear no name

Command Mode Config-vlan mode

Default None or depends on ODM customer

Description Use the name string command to create vlan entry with string on the switch.

Example ASUS(config-vlan)#name ABC

5.5 switchport access vlan <1-3000>

Syntax switchport access vlan <1-3000>

Parameters

access	the interface in access mode
vlan	Virtual LAN
<1-3000>	valid vlan-id range is 1 to 3000

Command Mode Interface mode

No/clear no switchport access vlan

Show show vlan [VLANID]

Default None or depends on ODM customer

Description Set access mode characteristics of all interfaces and Set Virtual LAN

Example ASUS(config-if)#switchport access vlan 2

5.6 switchport mode (access|trunk)

Syntax switchport mode (access|trunk)

Parameters

access	the interface in access mode
trunk	the interface in trunk mode

Command Mode Interface mode

No/clear no switchport access vlan

Show	show interface [IFNAME]
Default	None or depends on ODM customer
Description	Set access mode characteristics of all interfaces and Set Virtual LAN
Example	ASUS(config-if)#switchport mode access

5.7 switchport trunk native vlan <1-3000>

Syntax	switchport trunk native vlan <1-3000>	
Parameters	trunk	the interface in trunk mode
	native	untag vlan
	vlan	Virtual LAN
	<1-3000>	valid vlan-id range is 1 to 3000
Command Mode	Interface mode	
No/clear		
Show	show vlan [VLANID]	
Default	None or depends on ODM customer	
Description	Set native vlan of the port	
Example	ASUS(config-if)#switchport trunk native vlan 2	

5.8 switchport trunk allowed vlan (add|remove) VLANLIST

Syntax	switchport trunk allowed vlan (addlremove) VLANLIST	
Parameters	trunk	trunk characteristics
	allowed	the allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode
	vlan	the allowed VLANs
	add	to add the list of allowed VLANs
	remove	to remove the list of allowed VLANs
	VLANLIST	valid format is vlan_atom, [,vlan_atom...], [-vlan_atom,...],...

Command Mode	Interface mode
No/clear	switchport trunk allowed vlan remove VLANLIST
Show	show vlan [VLANID]
Default	None or depends on ODM customer
Description	Use the switchport trunk allowed vlan configuration command on the switch stack or standalone switch to add or remove the allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode
Example	ASUS(config-if)# switchport trunk allowed vlan add 2-20

6. 802.1x:

6.1 dot1x guest-vlan <1-3000>

Syntax	dot1x guest-vlan <1-3000>
Parameters	<1-3000> valid vlan-id range is from 1 to 3000
Command Mode	Interface mode
No/clear	no dot1x guest-vlan
Show	show dot1x all / show dot1x interface IFNAME
Default	No default guest vlan
Description	Use the dot1x guest-vlan interface configuration command on the switch stack or on a standalone switch to specify an active VLAN as an 802.1X guest VLAN. Use the no form of this command to return to the default setting.
Example	ASUS(config-if)#dot1x guest-vlan 2

6.2 dot1x max-req <1-10>

Syntax	dot1x max-req <1-10>
Parameters	<1-10> max-req times ; valid values are from 1 to 10
Command Mode	Interface mode
No/clear	no dot1x max-req
Show	show dot1x all

Default The default is 2

Description Use the dot1x max-req interface configuration command on the switch stack or on a standalone switch to set the maximum number of times that the switch sends an Extensible Authentication Protocol (EAP)-request/identity frame (assuming that no response is received) to the client before restarting the authentication process. Use the no form of this command to return to the default setting.

Example ASUS(config-if)#dot1x max-req 2

6.3 dot1x port-control (auto|force-authorized| force-unauthorized)

Syntax dot1x port-control (autolforce-authorizedl force-unauthorized)

Parameters auto -> Enables 802.1x port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port

force-authorized -> Disables 802.1x port-based authentication

and causes the port to transition to the authorized state

without any authentication exchange required

force-unauthorized -> Causes the port to remain in the

unauthorized state, ignoring all attempts by the client to authenticate

Command Mode Interface mode

No/clear no dot1x port-control

Show show dot1x all / show dot1x interface IFNAME

Default The default is ForceAuthorized

Description Use the dot1x port-control interface configuration command on the switch stack or on a standalone switch to enable manual control of the authorization state of the port. Use the no form of this command to return to the default setting.

Example ASUS(config-if)# dot1x port-control auto

6.4 dot1x radius server A.B.C.D RADIUS_KEY [PORTID]

Syntax	dot1x radius server A.B.C.D RADIUS_KEY [PORTID]	
Parameters	A.B.C.D:	IP address
	RADIUS_KEY:	RADIUS key
	[PORTID]:	RADIUS port
Command Mode	Configure mode	
No/clear		
Show	show dot1x radius / show running-config	
Default		
Description	This command sets the radius server ip, radius key, and radius port for 802.1X configuration.	
Example	ASUS(config)# dot1x radius server 192.192.1.1 testing 1812	

6.5 dot1x radius secondary-server A.B.C.D RADIUS_KEY [PORTID]

Syntax	dot1x radius secondary-server A.B.C.D RADIUS_KEY [PORTID]	
Parameters	A.B.C.D:	IP address
	RADIUS_KEY:	RADIUS key
	[PORTID]:	RADIUS port
Command Mode	Configure terminal mode	
No/clear		
Show	show dot1x radius / show running-config	
Default		
Description	This command sets the secondary radius server ip, radius key, and radius port for 802.1X configuration.	
Example	ASUS(config)# dot1x radius secondary-server 192.192.1.2 testing 1812	

6.6 dot1x re-authenticate interface [IFNAME]

Syntax dot1x re-authenticate interface [IFNAME]

Parameters IFNAME: interface's name

Command Mode Configure terminal mode

No/clear

Show show dot1x interface IFNAME

Default

Description Use the dot1x reauthenticate privileged EXEC command on the switch stack or on a standalone switch to manually initiate a re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port.

Example ASUS(config)# dot1x re-authenticate interface fa1/0/1

6.7 dot1x reauthentication

Syntax dot1x reauthentication

Parameters reauthentication periodic reauthentication of the client

Command Mode Interface mode

No/clear no dot1x reauthentication

Show show dot1x all / show dot1x interface IFNAME

Default The dot1x reauthentication feature is default disable

Description Use the dot1x reauthentication interface configuration command on the switch stack or on a standalone switch to enable periodic re-authentication of the client. Use the no form of this command to return to the default setting.

Example ASUS(config-if)# dot1x reauthentication

6.8 dot1x system-auth-control

Syntax dot1x system-auth-control

Parameters system-auth-control enabled 802.1X globally

Command Mode Configure terminal mode

No/clear no dot1x system-auth-control

Show show dot1x / show running-config

Default The default is global disable

Description Use the dot1x system-auth-control global configuration command on the switch stack or on a standalone switch to globally enable 802.1X. Use the no form of this command to return to the default setting.

Example ASUS(config)# dot1x system-auth-control

6.9 dot1x timeout (reauth-period| quiet-period|tx-period| supp-timeout| server-timeout) TIMEVALUE

Syntax dot1x timeout (reauth-periodl quiet-periodltx-periodl supp-timeoutlserver-timeout) TIMEVALUE

Parameters reauth-period -> number of seconds between reauthentication attempts

quiet-period -> number of seconds that the system remains in the quiet state following a failed authentication exchange with the client

tx-period -> number of seconds that the system waits for a response to an EAP-request/identity frame from the

client before retransmitting the request

supp-timeout -> number of seconds that the system waits for a response from Authenticator to Supplicant

server-timeout -> number of seconds that the system waits for a response from Authenticator to Authentication Server

TIMEVALUE: 1~65535 seconds

Command Mode Interface mode

No/clear no dot1x timeout (quiet-periodl reauth-periodl server-timeoutl supp-timeoutl tx-period)

Show show dot1x all / show dot1x interface IFNAME

Default reauth-period: 3600 seconds

quiet-period: 60 seconds

tx-period: 30 seconds

supp-timeout: 30 seconds

server-timeout: 20 seconds

Description This command sets the dot1x reauthentication timer.

Example ASUS(config-if)# dot1x timeout reauth-period 3600

6.10 dot1x host-mode (multi-host| single-host)

Syntax dot1x host-mode (multi-hostl single-host)

Parameters multi-host: Enable multiple-hosts mode on the switch

single-host: Enable single-host mode on the switch

Command Mode Interface mode

No/clear no dot1x host-mode

Show show dot1x all / show dot1x interface IFNAME

Default single-host

Description Allow multiple hosts (clients) on an 802.1X-authorized port.

Example ASUS(config-if)# dot1x host-mode multi-host

6.11 dot1x authentic-method (local | radius)

Syntax dot1x authentic-method (local l radius)

Parameters Local: Use the local username database for authentication

Radius: Use the Remote Authentication Dial-In User Service (RADIUS) servers for authentication

Command Mode Configure terminal mode

No/clear no dot1x authentic-method

Show show dot1x authentic_method

Default radius

Description Specify the authentic method for AAA.

Example ASUS(config)# dot1x authentic-method radius

6.12 dot1x user WORD PASSWORD <1-3000>

Syntax dot1x user WORD PASSWORD <1-3000>

Parameters First WORD : User Name

Second WORD : User Password

Command Mode Configure terminal mode

No/clear no dot1x username WORD

Show show dot1x username

Default N/A

Description Add user into local radius database.

Example ASUS(config)#dot1x user test testing123 1

6.13 show dot1x

Syntax show dot1x

Parameters dot1x Get IEEE 802.1x information

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description Use the show dot1x privileged EXEC command to display 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

Example ASUS#show dot1x

6.14 show dot1x interface IFNAME

Syntax show dot1x interface IFNAME

Parameters interface interface number

[IFNAME] designates the module and port number

ex: gigibitethernet1/0/3, gigabitethernet0/25...

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description Use the show dot1x privileged EXEC command to display 802.1X statistics, administrative status, and operational status for the switch or for the specified interface. Display the 802.1X status for the specified interface (including

type, stack member, module, and port number).

Example ASUS#show dot1x interface fa1/0/1

6.15 show dot1x radius

Syntax show dot1x radius

Parameters radius Remote Access Dial-In User Service

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description Use the show dot1x radius privileged EXEC command to display 802.1X Remote Access Dial-In User Service statistics, administrative status, and operational status for the switch or for the specified interface.

Example ASUS#show dot1x radius

6.16 show dot1x user

Syntax show dot1x user

Parameters N/A

Command Mode Privileged EXEC mode

Default N/A

Description Use the show dot1x username privileged EXEC command to display the username in local database.

Example ASUS# show dot1x user

7. Mirror

7.1 mirror session <1-8> destination IFNAME

Syntax mirror session <1-1> destination IFNAME

Parameters [IFNAME] designates the module and port number ex: fastethernet1/0/3, gigabitethernet1/0/25...

Command Mode Configuration mode

No/clear	No mirror session <1-8>
Default	Disable
Description	To set monitor port in mirror mode
Example	ASUS(config)# mirror session 1 destination fa1/0/1

7.2 mirror session <1-8> source IFLIST (rx|tx|both))

Syntax	mirror session <1-8> source IFLIST (rx|tx|both)
Parameters	IFLIST source interface list ,ex fa1/0/1,fai1/0/3-5,gi1/0/26 both -> received and transmitted traffic rx -> received traffic tx -> transmitted traffic
Command Mode	Configure terminal mode
No/clear	no mirror session 1 source fa1/0/2-4
Show	show mirror port / show running-config
Default	No mirror rule is setting
Description	This command mirrors the source interface list traffic to the destination interface. The mirror type support received traffic, Transmitted traffic, or both.
Example	ASUS(config)#mirror session 1 source fa1/0/2-4

7.3 show mirror session

Syntax	Show mirror session
Parameters	mirror mirroring feature
Command Mode	Priviliedge mode
Default	
Description	To show current mirror features
Example	ASUS#show mirror session

7.4 no mirror session <1-8> source IFLIST

Syntax	no mirror session <1-8> source IFLIST	
Parameters	no	Negate a command or set its defaults
	IFLIST	source interface list ,ex fa1/0/1,fa1/0/3-5,fai1/0/7
Command Mode	Configure terminal mode	
Show	show mirror session	
Default	There are some mirroring rules on Switch.	
Description	This command resets the source interfaces' received or transmitted traffic or both the destination interface.	
Example	ASUS(config)#no mirror session 1 source fa1/0/2-4	

8. QoS/CoS

8.1 cos cos-map PRIORITY QUEUE

GX2024B Queue range is 1-4

Syntax	cos cos-map <0-7> <1-6>	
Parameters	PRIORITY	802.1p priority
	QUEUE	internal class of service queues
Command Mode	Configure terminal mode	
No/clear	no cos cos-map	
Show	show cos cos-map	
Default	None or depends on ODM customer	
Description	Use the queue cos-map configuration command on the switch stack or standalone switch to set which Cos queue a given priority should map into.	
Example	ASUS(config)#cos cos-map 3 1	

8.2 show cos cos-map

Syntax	show cos cos-map

Parameters

Command Mode Privileged EXEC mode

No/clear

Show

Default None or depends on ODM customer

Description Show which cos queue agiven priority current maps to

Example ASUS# show cos cos-map

8.3 cos policy wrr-queue weight <1-10> <1-10> <1-10> <1-10> <1-10> <1-10>

GX2024B Queue weight parameter is 4.

Syntax cos policy wrr-queue weight <1-10> <1-10> <1-10> <1-10> <1-10> <1-10>

Parameters

<1-10>	weight for cos queue 1
<1-10>	weight for cos queue 2
<1-10>	weight for cos queue 3
<1-10>	weight for cos queue 4
<1-10>	weight for cos queue 5
<1-10>	weight for cos queue 6

Command Mode Configure terminal mode

No/clear no ingress-queue cos-map

Show show qos wrr-queue weights

Default

Description This command show the weight for each cos queue

Example ASUS(config)#cos policy wrr-queue weight 2 3 4 5 6 7

8.4 cos policy strict

Syntax cos policy strict

Parameters high_first All High before Low

Command Mode	Configure terminal mode
No/clear	No low-queue delay bound
Show	show qos mode
Default	The default setting of qos mode is highfirst mode
Description	This command sets qos mode to highfirst mode
Example	ASUS(config)# cos policy strict

8.5 show cos policy

Syntax	show cos policy	
Parameters	qos	quality of service (QoS)
	mode	CoS Scheduling mode of IEEE 802.1p
Command Mode	Privileged EXEC mode	
No/clear	no max bridge transmit delay bound	
Show	show max bridge transmit delay bound	
Default		
Description	This command show the qos mode.	
Example	ASUS# show cos policy	

8.6 show qos egress bandwidth [IFNAME]

Syntax	show qos egress bandwidth [IFNAME]	
Parameters	egress	Egress keyword
	[IFNAME]	Interface's name, ex: fa1/0/1 or fa1/0/12
Command Mode	Privileged EXEC mode	
No/clear		
Show		
Default	None or depends on ODM customer	
Description	This command used to show the Qos bandwidth informational parameter for the outcoming packets.	
Example	ASUS# show qos egress bandwidth fa1/0/1	

8.7 show qos Ingress bandwidth [IFNAME]

Syntax	show qos ingress bandwidth [IFNAME]	
Parameters	inress	ingress keyword
	[IFNAME]	Interface's name, ex: fa1/0/1 or fa1/0/12
Command Mode	Privileged EXEC mode	
No/clear		
Show		
Default	None or depends on ODM customer	
Description	This command used to show the Qos bandwidth informational parameter for the outcoming packets.	
Example	ASUS# show qos ingress bandwidth fa1/0/1	

8.8 qos egress bandwidth <1-1000>

GX2024B doesn't support this function.

Syntax	qos egress bandwidth <1-1000>	
Parameters	egress	Outgoing packets
	bandwidth	Set bandwidth informational parameter
	<1-1000>	Limit in 64-kilo-bits per second
Command Mode	Interface mode	
No/clear	no qos egress bandwidth	
Show	show qos egress bandwidth [IFNAME]	
Default	None or depends on ODM customer	
Description	This command used to set the Qos bandwidth informational parameter for the outcoming packets.	
Example	ASUS(config-if)# qos egress bandwidth 20	

8.9 no qos egress bandwidth

GX2024B doesn't support this function.

Syntax no qos egress bandwidth

Parameters	egress	Outgoing packets
	bandwidth	Set bandwidth informational parameter
Command Mode	Interface mode	
No/clear		
Show		
Default	None or depends on ODM customer	
Description	This command used to disable the Qos bandwidth informational parameter for the outcoming packets.	
Example	ASUS(config-if)#no qos egress bandwidth	

8.10 qos ingress bandwidth <1-1000>

Syntax	qos ingress bandwidth <1-1000>	
Parameters	ingress	Ingoing packets
	bandwidth	Set bandwidth informational parameter
	<1-1000>	Limit in magabits per second (GX2024B)
	<1-1000>	64-kilo-bits per second (GX2024M)
Command Mode	Interface mode	
No/clear	no qos ingress bandwidth	
Show	show qos ingress bandwidth [IFNAME]	
Default	None or depends on ODM customer	
Description	This command used to set the Qos bandwidth informational parameter for the outcoming packets.	
Example	ASUS(config-if)# qos ingress bandwidth 20	

8.11 no qos ingress bandwidth

Syntax	no qos ingress bandwidth	
Parameters	ingress	Ingoing packets
	bandwidth	Set bandwidth informational parameter
Command Mode	Interface mode	
No/clear		

Show

Default None or depends on ODM customer

Description This command used to disable the Qos bandwidth informational parameter for the outcoming packets.

Example ASUS(config-if)#no qos ingress bandwidth

8.12 cos policy fifo

Syntax cos policy fifo

Parameters Fcfs first come fisrt service

Command Mode Configure terminal mode

No/clear No low-queue delay bound

Show show qos mode

Default The default setting of qos mode is highfirst mode

Description This command sets qos mode to fcfs mode

Example ASUS(config)#cos policy fifo

8.13 no cos policy

Syntax no cos policy

Parameters

Command Mode Configure terminal mode

No/clear

Show show qos mode

Default The default setting of qos mode is highfirst mode

Description This command sets qos mode to highfirst mode

Example ASUS# no cos policy

9. Storm control

9.1 storm-control (broadcast|dlf|multicast)

<1-262143>

Syntax	storm-control (broadcast|dlf|multicast) <1-262143>	
Parameters	broadcast	Broadcast packets
	dlf	Destination Lookup Failure
	multicast	Multicast packets
	LIMIT_RATE	value 1~262143 (packets/s)
Command Mode	Interface mode (GX2024M)/ Configure terminal mode(GX2024B)	
No/clear	no storm-control (broadcast|dlf|multicast)	
Show	show storm-control IFNAME (broadcast|dlf|multicast)	
Default	None or depends on ODM customer	
Description	Use the storm-control configuration command on the switch stack or standalone switch to set the limit rate of the port's total bandwidth used by broadcast/dlf/multicast.	
Example	ASUS(config-if)# storm-control multicast 4096	

9.2 no storm-control (broadcast|dlf|multicast)

Syntax	no storm-control (broadcast|dlf|multicast)	
Parameters	broadcast	Broadcast packets
	dlf	Destination Lookup Failure
	multicast	Multicast packets
Command Mode	Interface mode	
No/clear		
Show		
Default	None or depends on ODM customer	
Description	Use the no storm-control configuration command on the switch stack or standalone switch to disable the limit rate of the port's total bandwidth used by broadcast/dlf/multicast.	
Example	ASUS(config-if)#no storm-control multicast	

9.3 show storm-control (broadcast|dlf|multicast)

Syntax	show storm-control (broadcast|dlf|multicast)	
Parameters	broadcast	Broadcast packets
	dlf	Destination Lookup Failure
	multicast	Multicast packets
Command Mode	Privileged EXEC mode	
No/clear		
Show		
Default		
Description	Use the show storm-control configuration command on the switch stack or standalone switch to show the limit rate of the port's total bandwidth used by broadcast/dlf/multicast.	
Example	ASUS# show storm-control dlf	

10. MAC address management Configuration:

10.1 clear mac-address-table dynamic vlan <1-3000>

Syntax	clear mac-address-table dynamic vlan <1-3000>	
Parameters	dynamic	dynamic L2 MAC addresses in the database
	<1-3000>	vlan id
Command Mode	Configure terminal mode	
No/clear		
Show		
Default	None or depends on ODM customer	
Description	Use the write configuration command on the switch stack or standalone switch to clear dynamic L2 MAC addresses in the	

database.

Example ASUS(config)# clear mac-address-table dynamic vlan 1

10.2 mac-address-table aging-time TIMEVALUE

Syntax mac-address-table aging-time TIMEVALUE

Parameters aging-time the length of time that a dynamic entry remains in the MAC address table

TIMEVALUE Aging time in seconds (10~1000000)

Command Mode Configure terminal mode

No/clear no mac-address-table aging-time

Show show mac-address-table aging-time

Default The default is 300 seconds.

Description Use the mac-address-table aging-time configuration command on the switch stack or on a standalone switch to set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.

The real aging-time is the triple of the command input radix number.

Example ASUS(config)# mac-address-table aging-time 300

10.3 no mac-address-table aging-time

Syntax no mac-address-table aging-time

Parameters aging-time the length of time that a dynamic entry remains in the MAC address table

Command Mode Configure terminal mode

No/clear

Show

Default

Description Use the no mac-address-table aging-time configuration command on the switch stack or on a standalone switch to disable dynamic entry remains in the MAC address table after the entry is used or updated.

The real aging-time is the triple of the command input radix number.

Example ASUS(config)# no mac-address-table aging-time

10.4 show mac-address-table aging-time

Syntax show mac-address-table aging-time

Parameters aging-time the length of time that a dynamic entry remains in the MAC address table

Command Mode Privileged EXEC mode

No/clear

Show

Default

Description Use the show mac-address-table aging-time configuration command on the switch stack or on a standalone switch to show dynamic entry remains in the MAC address table after the entry is used or updated.

The real aging-time is the triple of the command input radix number.

Example ASUS# show mac-address-table aging-time

10.5 mac-address-table static MACADDR VLANID IFNAME

Syntax mac-address-table static MAC_ADDR VLANID IFNAME

Parameters

static	Static keyword
MACADDR	Destination MAC address xxxx.xxxx.xxxx (multicast) to the address table
VLANID	Valid range is 1 ~ 3000
IFNAME	Interface's name, ex: fa1/0/1 or fa1/0/12

Command Mode Configure terminal mode

No/clear no mac-address-table static MACADDR VLANID IFNAME

Show show mac-address-table static

Default No static addresses are configured.

Description Use the mac-address-table static configuration command on the switch stack or on a standalone switch to add unicast static addresses to the MAC address table.

Example ASUS(config)# mac-address-table static 0000.0000.0001 2 fa1/0/2

10.6 mac-address-table multicast MACADDR vlan VLANID interface IFLIST COS_DEST

Syntax mac-address-table multicast MACADDR vlan VLANID interface IFLIST COS_DEST

Parameters

multicast	Multicast
MACADDR	Destination MAC address xxxx.xxxx.xxxx (multicast) to the address table
vlan	Vlan
VLANID	Valid range is 1 ~ 3000
interface	the specified interface
IFNAME	Interface's name, ex: fa1/0/1 or fa1/0/12
COS_DEST	COS prioriyt

Command Mode Configure terminal mode

No/clear

Show

Default No static addresses are configured.

Description Use the ac-address-table multicast configuration command on the switch stack or on a standalone switch to add multicast static addresses to the MAC address table.

Example ASUS(config)# mac-address-table multicast 0100.5e0a.0a0a vlan 1 interface fa1/0/2-5 3

10.7 no mac-address-table multicast MACADDR vlan VLANID interface IFLIST COS_DEST

Syntax no mac-address-table multicast MACADDR vlan VLANID

	interface IFLIST COS_DEST	
Parameters	multicast	Multicast
	MACADDR	Destination MAC address xxxx.xxxx.xxxx (multicast) to the address table
	vlan	Vlan
	VLANID	Valid range is 1 ~ 3000
	interface	the specified interface
	IFLIST	Interface's name list, ex: fa1/0/1-12
	COS_DEST	Cos priority
Command Mode	Configure terminal mode	
No/clear		
Show		
Default	No static addresses are configured.	
Description	Use the no mac-address-table multicast configuration command on the switch stack or on a standalone switch to remove multicast static port to the MAC address table.	
Example	ASUS(config)# no mac-address-table multicast 0100.5e0a.0a0a vlan 1 interface fa1/0/2-5 3	

10.8 show mac-address-table multicast

Syntax	show mac-address-table multicast
Parameters	
Command Mode	Privileged EXEC mode
Default	None or depends on ODM customer
Description	Use the show mac-address-table multicast user EXEC command to display the Layer 2 multicast entries for all VLANs. Use the command in privileged EXEC mode to display specific multicast entries.
Example	ASUS# show mac-address-table multicast

10.9 show mac-address-table static mac [MAC_ADDR]

Syntax	show mac-address-table static mac [MAC_ADDR]
Parameters	[MAC_ADDR] MAC address
Command Mode	Privileged EXEC mode
Default	None or depends on ODM customer
Description	Use the show mac-address-table ucast static user EXEC command to display static/dynamic ucast MAC address table entries only.
Example	ASUS# show mac-address-table static mac 0000.0000.0001

10.10 show mac-address-table static interface [IFNAME]

Syntax	show mac-address-table static interface [IFNAME]
Parameters	[IFNAME] Interface's name
Command Mode	Privileged EXEC mode
Default	None or depends on ODM customer
Description	Use the show mac-address-table ucast static user EXEC command to display static ucast MAC address table entries only.
Example	ASUS# show mac-address-table static interface fa1/0/1

10.11 show mac-address-table static vlan [VLANID]

Syntax	show mac-address-table static vlan [VLANID]
Parameters	[VLANID] vlan range (1~3000)
Command Mode	Privileged EXEC mode
Default	None or depends on ODM customer
Description	Use the show mac-address-table ucast static user EXEC command to display static/dynamic ucast MAC address table entries only.
Example	ASUS# show mac-address-table static vlan 1

10.12 show mac-address-table static

Syntax show mac-address-table static

Parameters

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description Use the show mac-address-table ucast static user EXEC command to display static ucast MAC address table entries only.

Example ASUS# show mac-address-table static

10.13 show mac-address-table

Syntax show mac-address-table

Parameters

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description Use the show mac-address-table user EXEC command to display static/dynamic ucast MAC address table entries only.

Example ASUS# show mac-address-table

10.14 show mac-address-table multicast MACADDR vlan VLANID

Syntax show mac-address-table multicast MACADDR vlan VLANID

Parameters

multicast	Multicast
MACADDR	Destination MAC address xxxx.xxxx.xxxx (multicast) to the address table
vlan	Vlan
VLANID	Valid range is 1 ~ 3000

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description Use the show mac-address-table multicast user EXEC command to display the Layer 2 multicast entries for a VLAN.

	Use the command in privileged EXEC mode to display specific multicast entries.
Example	ASUS# show mac-address-table multicast 0100.5e0a.0a0a vlan 1

10.15 show mac-address-table dynamic

Syntax	show mac-address-table dynamic
Parameters	
Command Mode	Privileged EXEC mode
Default	None or depends on ODM customer
Description	Use the show mac-address-table ucast dynamic user EXEC command to display static ucast MAC address table entries only.
Example	ASUS# show mac-address-table dynamic

10.16 show mac-address-table dynamic interface [IFNAME]

Syntax	show mac-address-table dynamic interface [IFNAME]
Parameters	[IFNAME] Interface's name
Command Mode	Privileged EXEC mode
Default	None or depends on ODM customer
Description	
	Use the show mac-address-table ucast dynamicc user EXEC command to display dynamic ucast MAC address table entries only.
Example	ASUS# show mac-address-table dynamic interface fa1/0/1

10.17 show mac-address-table dynamic mac [MAC_ADDR]

Syntax	show mac-address-table dynamic mac [MAC_ADDR]
Parameters	[MAC_ADDR] MAC address
Command Mode	Privileged EXEC mode

Default None or depends on ODM customer

Description Use the show mac-address-table ucast dynamic user EXEC command to display dynamic ucast MAC address table entries only.

Example ASUS# show mac-address-table dynamic mac 0000.0000.0001

10.18 show mac-address-table dynamic vlan [VLANID]

Syntax show mac-address-table dynamic vlan [VLANID]

Parameters [VLANID] vlan range (1~3000)

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description Use the show mac-address-table ucast static user EXEC command to display dynamic ucast MAC address table entries only.

Example ASUS# show mac-address-table dynamic vlan 1

10.19 clear mac-address-table mac MAC_ADDR

Syntax clear mac-address-table mac MAC_ADDR

Parameters address mac address

MAC_ADDR -> MAC address xxxx.xxxx.xxxx (unicast) to add to the address table

Command Mode Configure terminal mode

No/clear

Show

Default None or depends on ODM customer

Description Use the write configuration command on the switch stack or standalone switch to clear dynamic L2 MAC addresses in the database.

Example ASUS(config)# clear mac-address-table mac 0000.0000.0001

10.20 clear mac-address-table dynamic

Syntax clear mac-address-table dynamic

Parameters

Command Mode Configure terminal mode

No/clear

Show

Default None or depends on ODM customer

Description Use the write configuration command on the switch stack or standalone switch to clear dynamic L2 MAC addresses in the database.

Example ASUS(config)# clear mac-address-table dynamic

10.21 clear mac-address-table dynamic interface IFNAME

Syntax clear mac-address-table dynamic interface IFNAME

Parameters [IFNAME] Interface's name

Command Mode Configure terminal mode

No/clear

Show

Default None or depends on ODM customer

Description Use the write configuration command on the switch stack or standalone switch to clear dynamic L2 MAC addresses in the database.

Example ASUS(config)# clear mac-address-table dynamic interface fa1/0/1

10.22 clear mac-address-table dynamic vlan VLANID

Syntax clear mac-address-table dynamic vlan VLANID

Parameters [VLANID] vlan range (1~3000)

Command Mode Configure terminal mode

No/clear

Show

Default None or depends on ODM customer

Description Use the write configuration command on the switch stack or standalone switch to clear dynamic L2 MAC addresses in the database.

Example ASUS(config)# clear mac-address-table dynamic vlan 1

10.23 clear mac-address-table interface IFNAME

Syntax clear mac-address-table interface IFNAME

Parameters [IFNAME] Interface's name

Command Mode Configure terminal mode

No/clear

Show

Default None or depends on ODM customer

Description Use the write configuration command on the switch stack or standalone switch to clear static L2 MAC addresses in the database.

Example ASUS(config)# clear mac-address-table interface fa1/0/1

10.24 clear mac-address-table multicast MACADDR VLANID

Syntax clear mac-address-table multicast MACADDR VLANID

Parameters [VLANID] vlan range (1~3000)

Command Mode Configure terminal mode

No/clear

Show

Default None or depends on ODM customer

Description Use the write configuration command on the switch stack or standalone switch to clear multicast L2 MAC addresses in the database.

Example ASUS(config)# clear mac-address-table multicast

0100.5e0a.0a0a 1

10.25 clear mac-address-table vlan VLANID

Syntax	clear mac-address-table dynamic vlan VLANID	
Parameters	[VLANID]	vlan range (1~3000)
Command Mode	Configure terminal mode	
No/clear		
Show		
Default	None or depends on ODM customer	
Description	Use the write configuration command on the switch stack or standalone switch to clear dynamic L2 MAC addresses in the database.	
Example	ASUS(config)# clear mac-address-table dynamic vlan 1	
10.	Spanning Tree Protocol:	

10.26 show spanning-tree summary

Syntax	show spanning-tree summary	
Parameters	spanning-tree	the STP
	summary	Display spanning tree information for only active ports
Command Mode	Privileged EXEC mode	
Default		
Description	To show spanning-tree active.	
Example	ASUS# show spanning-tree summary	

10.27 show spanning-tree interface [IFNAME]

Syntax	show spanning-tree interface [IFNAME]	
Parameters	spanning-tree	the STP
	[IFNAME]	interface name eq. Fa1/0/1
Command Mode	Privileged EXEC mode	

Default

Description To show spanning-tree summary.

Example ASUS# show spanning-tree interface fa1/0/1

10.28 spanning-tree (enable|disable)

Syntax spanning-tree (enable|disable)

Parameters disable -> disables the Spanning Tree algorithm globally for the switch

enable -> enables the Spanning Tree algorithm globally for the switch

Command Mode Configure terminal mode

No/clear spanning-tree disable

Show show spanning-tree active

Default Enable

Description Enable/Disable the spanning tree

Example ASUS(config)# spanning-tree enable

10.29 spanning-tree cost <1-200000000>

Syntax spanning-tree cost <1-200000000>

Parameters cost the path cost

<1-200000000> Valid range is from 1 to 200,000,000

Command Mode Interface mode

No/clear no spanning-tree cost

Show show spanning-tree port detail IFNAME

Default 19

Description Use the spanning-tree cost configuration command on the switch stack or standalone switch to set the spanning-tree path cost.

Example ASUS(config-if)#spanning-tree cost 128

10.30 spanning-tree edge-port

Syntax	spanning-tree edge-port
Parameters	edge-port the interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node
Command Mode	Interface mode
No/clear	No spanning-tree edge-port
Show	show spanning-tree port detail IFNAME
Default	None or depends on ODM customer
Description	Use the spanning-tree cost configuration command on the switch stack or standalone switch to set the spanning-tree interface attached to a LAN segment that is at the end.
Example	ASUS(config-if)# spanning-tree edge-port

10.31 spanning-tree forward-time <4-30>

Syntax	spanning-tree forward-time <4-30>	
Parameters	forward-time	the bridge forward delay time (sec)
	<4-30>	Valid range is 4~30 secs
Command Mode	Configure terminal mode	
No/clear	No spanning-tree forward-time	
Show	show spanning-tree port detail IFNAME	
Default	15 sec	
Description	Use the spanning-tree cost configuration command on the switch stack or standalone switch to set the spanning-tree bridge forward delay time (sec).	
Example	ASUS(config)# spanning-tree forward-time 15	

10.32 spanning-tree hello time <1-10>

Syntax	spanning-tree hello time <1-10>	
Parameters	hello	hello BPDUs
	time	the interval (sec) between hello BPDUs
	<1-10>	valid range is 1~10 secs
Command Mode	Configure terminal mode	

No/clear	No spanning-tree hello time
Show	show spanning-tree port detail IFNAME
Default	2 sec
Description	Use the spanning-tree cost configuration command on the switch stack or standalone switch to set the hello time to send hello BPDUs.
Example	ASUS(config)# spanning-tree hello time 2

10.33 spanning-tree link-type (auto|point-to-point|shared)

Syntax	spanning-tree link-type (auto|point-to-point|shared)	
Parameters	link-type	the link type for the Rapid Spanning Tree
	auto ->	automatically determines if the interface is attached to a point-to-point link or to shared media
	point-to-point ->	a connection to exactly one other bridge
	shared ->	a connection to two or more bridges
Command Mode	Interface mode	
No/clear	no spanning-tree link-type	
Show	show spanning-tree port detail IFNAME	
Default	None or depends on ODM customer	
Description	Use the spanning-tree cost configuration command on the switch stack or standalone switch to set the spanning-tree link type for the Rapid Spanning Tree	
Example	ASUS(config-if)# spanning-tree link-type auto	

10.34 spanning-tree max-age <6-40>

Syntax	spanning-tree max-age <6-40>	
Parameters	max-age	the interval (sec) between messages the spanning tree receives from the root switch
	<6-40>	Valid range is 6~40 secs

Command Mode	Configure terminal mode
No/clear	No spanning-tree max-age
Show	show spanning-tree port detail IFNAME
Default	20 sec
Description	Use the spanning-tree max-age configuration command on the switch stack or standalone switch to set the spanning-tree interval (sec) between messages the spanning tree receive.
Example	ASUS(config)# spanning-tree max-age 20

10.35 spanning-tree port-priority <0-240>

Syntax	spanning-tree port-priority <0-240>	
Parameters	port-priority	the port priority
	<0-240>	Number from 0 to 240, in increments of 16
Command Mode	Interface mode	
No/clear	no spanning-tree port-priority	
Show	show spanning-tree port detail IFNAME	
Default	None or depends on ODM customer	
Description	Use the spanning-tree port-priority configuration command	
	on the switch stack or standalone switch to set the spanning-tree the port priority between 0 and 240.	
Example	ASUS(config-if)# spanning-tree port-priority 128	

10.36 spanning-tree priority <0-61440>

Syntax	spanning-tree priority <0-61440>	
Parameters	priority	the switch priority
	<0-61440>	valid range is 0 to 61440 in increments of 4096
Command Mode	Configure terminal mode	
No/clear	No spanning-tree priority	
Show	show spanning-tree port detail IFNAME	
Default	32768	

Description

Use the spanning-tree priority configuration command

on the switch stack or standalone switch to set the spanning-tree switch priority

Example ASUS(config)# spanning-tree priority 32768

10.37 spanning-tree transmission-limit <1-10>

Syntax spanning-tree transmission-limit <1-10>

Parameters

transmission-limit	the transmission of consecutive RSTP BPDUs
<1-10>	the minimum interval between the transmission of consecutive RSTP BPDUs ,valid range is 1~10

Command Mode Configure terminal mode

No/clear no spanning-tree transmission-limit

Show show spanning-tree active / show running-config

Default 3

Description Use the spanning-tree transmission-limit configuration command

on the switch stack or standalone switch to set the spanning-tree transmission of consecutive RSTP BPDUs

Example ASUS(config)# spanning-tree transmission-limit 3

10.38 spanning-tree mode (pvst|rapid-pvst)

Syntax spanning-tree mode (pvst|rapid-pvst)

Parameters

Pvst	stp mode
Rapid-pvst	rapid stp mode

Command Mode Configure terminal mode

No/clear

Show show spanning-tree active

Default Enable

Description the spanning tree mode

Example ASUS(config)# spanning-tree mode pvst

10.39 spanning-tree uplink-fast

Syntax spanning-tree uplink-fast

Parameters

Command Mode Configure terminal mode

No/clear No spanning-tree uplink-fast

Show show spanning-tree summary

Default disable

Description Accelerate the root port transitions to the forwarding state

Example ASUS(config)# spanning-tree uplink-fast

10.40 spanning-tree algorithm-timer <4-30> <6-40> <1-10>

Syntax spanning-tree algorithm-timer <4-30> <6-40> <1-10>

Parameters

forward-time	Set the forward delay for the spanning tree
hello	Set the hello interval for the spanning tree
max-age	Set the max age interval for the spanning tree

Command Mode Configure terminal mode

No/clear No spanning-tree algorithm-timer

Show show spanning-tree active

Default

Description This command sets spanning-tree parameter to default

Example ASUS(config)# spanning-tree algorithm-time 10 2 6

10.41 spanning-tree bpdu-guard (enable|disable)

Syntax spanning-tree bpdu-guard (enableldisable)

Parameters Enable

Disable

Command Mode Interface mode

No/clear

Show show spanning-tree port detail IFNAME

Default None or depends on ODM customer

Description If the switch recieve the bpdu send by self, the switch port will be blocked.

Example ASUS(config-if)# spanning-tree bpdu-guard enable

10.42 spanning-tree mst max-hops [1-40]

Syntax spanning-tree mst max-hops [1-40]

Parameters

Command Mode configuration terminal mode

No/clear no spanning-tree mst max-hops

Show

Default None or depends on ODM customer

Description □□MSTP BPDU max passed hop count(default:20hops)

Examples ASUS(config)# spanning-tree mst max-hops 20

10.43 no spanning-tree mst max-hops

Syntax no spanning-tree mst max-hops

Parameters

Command Mode configuration terminal mode

show

Default None or depends on ODM customer

Description □□MSTP BPDU max passed hop count□□,□□□□

Examples ASUS(config)# no spanning-tree mst max-hops

10.44 show spanning-tree mst

Syntax show spanning-tree mst

Parameters

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description □□□□MSTP□□□Configuration□Instance□□□□

Examples ASUS# show spanning-tree mst

10.45 show spanning-tree mst configuration

Syntax show spanning-tree mst configuration

Parameters

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description □□□□MSTP□□□Configuration□□(Region Name/Revision/VID Mapping)

Examples ASUS# show spanning-tree mst configuration

10.46 show spanning-tree mst <1-15>

Syntax show spanning-tree mst <1-15>

Parameters

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description □□□□MSTP□□□Instance□Configuration□□

Examples ASUS# show spanning-tree mst 1

10.47 show spanning-tree mst instance [1-15] interface [IF Name]

Syntax show spanning-tree mst instance [1-15] interface [IF Name]

Parameters

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description □□□□MSTP□指□Instance的target Port之Configuration資□

Examples ASUS# show spanning-tree mst instance 1 interface fa1/0/1

10.48 spanning-tree mode mst

Syntax spanning-tree mode mst

Parameters

Command Mode configuration terminal mode

Default None or depends on ODM customer

Description □□spanning tree□□□□□MSTP

Examples ASUS(config)# spanning-tree mode mst

10.49 spanning-tree mst revision <0-65535>

Syntax Spanning-trr mst revision <0-65535>

Parameters

Command Mode Configure terminal mode

Show

Default None or depends on ODM customer

Description 設□□□MSTP Region之設□□正□□□□

Result ASUS(config)# spanning-tree mst revision 1

10.50 no spanning-tree mst name

Syntax no spanning-tree name

Parameters

Command Mode Configure terminal mode

Show

Default None or depends on ODM customer

Description □□設定MSTP Region之區域名稱資訊,回復前次設定

Result ASUS(config)# no spanning-tree name

10.51 spanning-tree mst name [NAME]

Syntax Spanning-tree mst name [NAME]

Parameters

Command Mode Configure terminal mode

Show

Default None or depends on ODM customer

Description 設□目□MSTP Region□□域□□□□

Result ASUS(config)# spanning-tree mst name abcd

10.52 no spanning-tree mst instance [msti]

Syntax no spanning-tree mst instance [msti]

Parameters

Command Mode Configure terminal mode

Show

Default None or depends on ODM customer

Description □□□□□□mst instance之所有VLAN(VLAN ID)設定,回復前次設定

Result ASUS(config)# no spanning-tree mst instance 2

10.53 spanning-tree mst instance [msti] vlan [vids]

Syntax Spanning-tree mst instance [msti] vlan [vids]

Parameters

Command Mode Configure terminal mode

No/clear no instance [msti]

Show

Default None or depends on ODM customer

Description 設□□□或□□VLAN(VLAN ID)□入指□□mst instance

Result ASUS(config)# spanning-tree mst instance 2 vlan 3-100

10.54 spanning-tree mst [mstis] cost [value]

Syntax	spanning-tree mst [mstis] cost [value]	
Parameters	mstis	Instance of MST 1-15
	Value	1-200000000
Command Mode	Interface Mode	
No/clear	no spanning-tree mst [mstis] cost	
Show		
Default	None or depends on ODM customer	
Description	Setup path cost for a specific port	
Examples	ASUS(config)#interfcae fa1/0/1	
	ASUS(config-if)#spanning-tree mst 1 cost 2000	

10.55 spanning-tree mst [mstis] port-priority [value]

Syntax	spanning-tree mst [mstis] port-priority [value]	
Parameters	mstis	Instance of MST 1-15
	port-priority	0-240
Command Mode	Interface Mode	
No/clear	no spanning-tree mst [mstis] port-priority	
Show		
Default	128	
Description	Setup priority for a specific port Port Priority	
Examples	ASUS(config)#interfcae fa1/0/1	
	ASUS(config-if)#spanning-tree mst 1 port-priority 16	

11. SNMP

11.1 show rmon statistics [IFNAME]

Syntax	show rmon statistics [IFNAME]	
Parameters	rmon	Remote monitoring
	statistics	the contents of the switch's RMON statistics table
	[IFNAME]	Interface's name, ex: fa1/0/1 or gigabitethernet1/0/26
Command Mode	Privileged EXEC mode	
Default		
Description	To show rmon statistics IFNAME status.	
Examples	ASUS# show rmon statistics [fa1/0/1]	

11.2 show rmon statistics stack <1-8>

Syntax	show rmon statistics stack <1-8>	
Parameters	rmon	Remote monitoring
	statistics	the contents of the switch's RMON statistics table
	<1-8>	stack id
Command Mode	Privileged EXEC mode	
Default		
Description	To show rmon statistics with specific stack id.	
Examples	ASUS# show rmon statistics stack 1	

11.3 show snmp-server community

Syntax	show snmp-server community	
Parameters	snmp-server	the SNMP server
	community	SNMP server community
Command Mode	Privileged EXEC mode	
Default		
Description	To show snmp-server community.	

Examples ASUS# show snmp-server community

11.4 show snmp-server community network

Syntax show snmp-server community network

Parameters

	snmp-server	the SNMP server
	community	SNMP server community
	network	the network bind to this community

Command Mode Privileged EXEC mode

Default

Description To show snmp-server community network.

Examples ASUS# show snmp-server community network

11.5 show snmp-server contact

Syntax show snmp-server contact

Parameters

	snmp-server	the SNMP server
	contact	show the system contact string

Command Mode Privileged EXEC mode

Default

Description To show snmp-server contact.

Examples ASUS# show snmp-server contact

11.6 show snmp-server host

Syntax show snmp-server host

Parameters

	snmp-server	the SNMP server
	host	the recipient (host) of a SNMP notification operation

Command Mode Privileged EXEC mode

Default

Description To show snmp-server host.

Examples ASUS# show snmp-server host

11.7 show snmp-server location

Syntax show snmp-server location

Parameters

	snmp-server	the SNMP server
	location	show the system location string

Command Mode Privileged EXEC mode

Default

Description To show snmp-server location.

Examples ASUS# show snmp-server location

11.8 show snmp-server trap community

Syntax show snmp-server trap community

Parameters

	snmp-server	the SNMP server
	community	SNMP server community

Command Mode Privileged EXEC mode

Default

Description To show snmp-server trap community.

Examples ASUS# show snmp-server trap community

11.9 snmp-server community trap WORD

Syntax snmp-server community trap WORD

Parameters

	community	SNMP server community
	trap	for trap use
	WORD	a unique SNMP community string (max 30 characters) that acts like a pass word and permits access to the
	SNMP	protocol

Command Mode Configure terminal mode

No/clear

Show	show snmp-server trap community / show running-config
Default	Public
Description	This command sets the trap community string for SNMP protocol.
Examples	ASUS(config)# snmp-server community trap public

11.10 snmp-server community WORD (ro/rw) network A.B.C.D/MASK

Syntax	snmp-server community WORD (ro/rw) network A.B.C.D/MASK	
Parameters	community	SNMP server community
	WORD	create a new community string (max 30 characters)
	ro	a unique SNMP community string that acts like a password and permits access to the SNMP protocol
	rw	the relationship between the SNMP manager and the agent,ro->read-only, rw->read-write
	network	the network that allowed to access this community
	A.B.C.D/MASK	network and mask
Command Mode	Configure terminal mode	
No/clear	no snmp-server community WORD (rolrw) network A.B.C.D/MASK	
Show	show snmp-server community / show running-config	
Default	Public, and the network is 0.0.0.0/0.0.0.0	
Description	This command create a new community string (max 30 characters).	
Examples	ASUS(config)# snmp-server community public ro network 192.192.1.1/24	

11.11 snmp-server contact DWORD

Syntax	snmp-server contact DWORD	
Parameters	contact	the system contact string
	DWORD	string that describes the system contact information
Command Mode	Configure terminal mode	
No/clear	no snmp-server contact	
Show	show snmp-server contact	
Default	None or depends on ODM customer	
Description	This command sets the SNMP Contact information	
Examples	ASUS(config)# snmp-server contact asus@asus.com.tw	

11.12 snmp-server host A.B.C.D

Syntax	snmp-server host A.B.C.D	
Parameters	host	the recipient (host) of a SNMP notification operation
	A.B.C.D	IP address
Command Mode	Configure terminal mode	
No/clear	no snmp-server host A.B.C.D	
Show	show snmp-server host / show running-config	
Default	None or depends on ODM customer	
Description	This command sets the SNMP Contact information	
Examples	ASUS(config)# snmp-server host 192.192.1.1	

11.13 snmp-server location DWORD

Syntax	snmp-server location DWORD	
Parameters	location	the system location string
	DWORD	string that describes the system location information
Command Mode	Configure terminal mode	
No/clear	no snmp-server location	
Show	show snmp-server location	

Default	None or depends on ODM customer
Description	This command sets the SNMP location string.
Examples	ASUS(config)# snmp-server location ASUS

11.14 snmp-server user WORD WORD v3 noauth

Syntax	snmp-server user WORD WORD v3 noauth	
Parameters	WORD	Name of the user
	WORD	Group to which the user belongs
	v3	User using the v3 security model
	noauth	Specifies no authentication of a packet
Command Mode	Configure terminal mode	
No/clear	no snmp-server user WORD WORD v3	
Show	show snmp-server user	
Default	None	
Description	Define a user who can access the SNMP engine	
Examples	ASUS(config)# snmp-server user test g1 v3 noauth	

11.15 snmp-server user WORD WORD v3 auth (md5|sha) WORD

Syntax	snmp-server user WORD WORD v3 auth (md5lsha) WORD	
Parameters	WORD	Name of the user
	WORD	Group to which the user belongs
	v3	User using the v3 security model
	auth	Specifies authentication of a packet without encrypting it (md5lsha)
	md5	Use HMAC MD5 algorithm for authentication
	sha	Use HMAC SHA algorithm for authentication
	WORD	Authentication pasword for user
Command Mode	Configure terminal mode	

No/clear	no snmp-server user WORD WORD v3
Show	show snmp-server user
Default	None
Description	Define a user who can access the SNMP engine
Examples	ASUS(config)# snmp-server user test g1 v3 auth sha 12345678

11.16 snmp-server user WORD WORD v3 priv (md5|sha) WORD des WORD

Syntax	snmp-server user WORD WORD v3 priv (md5|sha) WORD des WORD	
Parameters	WORD	Name of the user
	WORD	Group to which the user belongs
	v3	User using the v3 security model
	priv	Specifies authentication of a packet with encryption (md5|sha)
	md5	Use HMAC MD5 algorithm for authentication
	sha	Use HMAC SHA algorithm for authentication
	WORD	Authentication pasword for user
	des	Use DES algorithm for encryption
	WORD	Encryption pasword for user
Command Mode	Configure terminal mode	
No/clear	no snmp-server user WORD WORD v3	
Show	show snmp-server user	
Default	None	
Description	Define a user who can access the SNMP engine	
Examples	ASUS(config)# snmp-server user test g1 v3 priv sha 12345678 des 12345678	

11.17 snmp-server group WORD v3 WORD

Syntax	snmp-server group WORD v3 WORD	
Parameters	group	Configure a new SNMP group, that maps SNMP users to SNMP users
	WORD	The name of the group
	v3	Using the SNMPv3 for security mode
	WORD	The name of the user who mapping to the group
Command Mode	Configure terminal mode	
No/clear	no snmp-server group WORD v3 (noauthlauthlpriv)	
Show	show snmp-server group	
Default	None	
Description	Configure a new SNMP group, that maps SNMP users to SNMP users	
Examples	ASUS(config)# snmp-server group g1 v3 test	

11.18 snmp-server group WORD v3 noauth

Syntax	snmp-server group WORD v3 noauth	
Parameters	group	Configure a new SNMP group, that maps SNMP users to SNMP users
	WORD	The name of the group
	v3	Using the SNMPv3 for security mode
	noauth	Specifies no authentication of a packet
Command Mode	Configure terminal mode	
No/clear	no snmp-server group WORD v3 (noauthlauthlpriv)	
Show	show snmp-server group	
Default	None	
Description	Configure a new SNMP group, that maps SNMP users to SNMP users	

Examples ASUS(config)# snmp-server group g1 v3 noauth

11.19 snmp-server group WORD v3 noauth read WORD

Syntax	snmp-server group WORD v3 noauth read WORD	
Parameters	group	Configure a new SNMP group, that maps SNMP users to SNMP users
	WORD	The name of the group
	v3	Using the SNMPv3 for security mode
	noauth	Specifies no authentication of a packet
	read	The option that allows you to specify a read view (default sysView)
	WORD	A string that he name of the view that enables you only to view the contents of the agent
Command Mode	Configure terminal mode	
No/clear	no snmp-server group WORD v3 (noauthlauthlpriv)	
Show	show snmp-server group	
Default	None	
Description	Configure a new SNMP group, that maps SNMP users to SNMP users	
Examples	ASUS(config)# snmp-server group g1 v3 noauth read r1	

11.20 snmp-server group WORD v3 noauth read WORD write WORD

Syntax	snmp-server group WORD v3 noauth read WORD write WORD	
Parameters	group	Configure a new SNMP group, that maps SNMP users to SNMP users
	WORD	The name of the group
	v3	Using the SNMPv3 for security mode
	noauth	Specifies no authentication of a packet

	read	The option that allows you to specify a read view (default sysView)
	WORD	A string that he name of the view that enables you only to view the contents of the agent
	write	The option that allows you to specify a write view (default none)
	WORD	A string that is the name of the view that enables you to enter and configure the contents of the agent

Command Mode Configure terminal mode

No/clear no snmp-server group WORD v3 (noauthlauthlpriv)

Show show snmp-server group

Default None

Description Configure a new SNMP group, that maps SNMP users to SNMP users

Examples ASUS(config)# snmp-server group g1 v3 noauth read r1 write w1

11.21 snmp-server group WORD v3 noauth read WORD write WORD notify WORD

Syntax snmp-server group WORD v3 noauth read WORD write WORD notify WORD

Parameters	group	Configure a new SNMP group, that maps SNMP users to SNMP users
	WORD	The name of the group
	v3	Using the SNMPv3 for security mode
	noauth	Specifies no authentication of a packet
	read	The option that allows you to specify a read view (default sysView)
	WORD	A string that he name of the view that enables you only to view the contents of the agent
	write	The option that allows you to specify a write view (default none)

	WORD	A string that is the name of the view that enables you to enter and configure the contents of the agent
	notify	The option that allows you to specify a notify view (default none)
	WORD	A string that is the name of the view that enables you to specify a notify, inform, or trap

Command Mode Configure terminal mode

No/clear no snmp-server group WORD v3 (noauthlauthlpriv)

Show show snmp-server group

Default None

Description Configure a new SNMP group, that maps SNMP users to SNMP users

Examples ASUS(config)# snmp-server group g1 v3 noauth read r1 write w1 notify n1

11.22 snmp-server group WORD v3 auth

Syntax snmp-server group WORD v3 auth

Parameters	group	Configure a new SNMP group, that maps SNMP users to SNMP users
	WORD	The name of the group
	v3	Using the SNMPv3 for security mode
	auth	Specifies authentication of a packet without encrypting it

Command Mode Configure terminal mode

No/clear no snmp-server group WORD v3 (noauthlauthlpriv)

Show show snmp-server group

Default None

Description Configure a new SNMP group, that maps SNMP users to SNMP users

Examples ASUS(config)# snmp-server group g1 v3 auth

11.23 snmp-server group WORD v3 auth read WORD

Syntax snmp-server group WORD v3 noauth read WORD

Parameters group Configure a new SNMP group, that maps SNMP users to SNMP users

WORD The name of the group

v3 Using the SNMPv3 for security mode

auth Specifies authentication of a packet without encrypting it

read The option that allows you to specify a read view (default sysView)

WORD A string that he name of the view that enables you only to view the contents of the agent

Command Mode Configure terminal mode

No/clear no snmp-server group WORD v3 (noauth|auth|priv)

Show show snmp-server group

Default None

Description Configure a new SNMP group, that maps SNMP users to SNMP users

Examples ASUS(config)# snmp-server group g1 v3 auth read r1

11.24 snmp-server group WORD v3 auth read WORD write WORD

Syntax snmp-server group WORD v3 noauth read WORD write WORD

Parameters

group	Configure a new SNMP group, that maps SNMP users to SNMP users
WORD	The name of the group
v3	Using the SNMPv3 for security mode
auth	Specifies authentication of a packet without encrypting it
read	The option that allows you to specify a read view (default sysView)

	WORD	A string that he name of the view that enables you only to view the contents of the agent
	write	The option that allows you to specify a write view (default none)
	WORD	A string that is the name of the view that enables you to enter and configure the contents of the agent

Command Mode Configure terminal mode

No/clear no snmp-server group WORD v3 (noauthlauthlpriv)

Show show snmp-server group

Default None

Description Configure a new SNMP group, that maps SNMP users to SNMP users

Examples ASUS(config)# snmp-server group g1 v3 auth read r1 write w1

11.25 snmp-server group WORD v3 auth read WORD write WORD notify WORD

Syntax snmp-server group WORD v3 auth read WORD write WORD notify WORD

Parameters

	group	Configure a new SNMP group, that maps SNMP users to SNMP users
	WORD	The name of the group
	v3	Using the SNMPv3 for security mode
	auth	Specifies authentication of a packet without encrypting it
	read	The option that allows you to specify a read view (default sysView)
	WORD	A string that he name of the view that enables you only to view the contents of the agent
	write	The option that allows you to specify a write view (default none)
	WORD	A string that is the name of the view that

		enables you to enter and configure the contents of the agent
	notify	The option that allows you to specify a notify view (default none)
	WORD	A string that is the name of the view that enables you to specify a notify, inform, or trap

Command Mode Configure terminal mode

No/clear no snmp-server group WORD v3 (noauthlauthlpriv)

Show show snmp-server group

Default None

Description Configure a new SNMP group, that maps SNMP users to SNMP users

Examples ASUS(config)# snmp-server group g1 v3 auth read r1 write w1 notify n1

11.26 snmp-server group WORD v3 priv

Syntax snmp-server group WORD v3 priv

Parameters

group	Configure a new SNMP group, that maps SNMP users to SNMP users
WORD	The name of the group
v3	Using the SNMPv3 for security mode
priv	Specifies authentication of a packet with encryption

Command Mode Configure terminal mode

No/clear no snmp-server group WORD v3 (noauthlauthlpriv)

Show show snmp-server group

Default None

Description Configure a new SNMP group, that maps SNMP users to SNMP users

Examples ASUS(config)# snmp-server group g1 v3 priv

11.27 snmp-server group WORD v3 priv read WORD

Syntax	snmp-server group WORD v3 priv read WORD	
Parameters	group	Configure a new SNMP group, that maps SNMP users to SNMP users
	WORD	The name of the group
	v3	Using the SNMPv3 for security mode
	priv	Specifies authentication of a packet with encryption
	read	The option that allows you to specify a read view (default sysView)
	WORD	A string that he name of the view that enables you only to view the contents of the agent
Command Mode	Configure terminal mode	
No/clear	no snmp-server group WORD v3 (noauthlauthlpriv)	
Show	show snmp-server group	
Default	None	
Description	Configure a new SNMP group, that maps SNMP users to SNMP users	
Examples	ASUS(config)# snmp-server group g1 v3 priv read r1	

11.28 snmp-server group WORD v3 priv read WORD write WORD

Syntax	snmp-server group WORD v3 priv read WORD write WORD	
Parameters	group	Configure a new SNMP group, that maps SNMP users to SNMP users
	WORD	The name of the group
	v3	Using the SNMPv3 for security mode
	priv	Specifies authentication of a packet with encryption
	read	The option that allows you to specify a read

		view (default sysView)
	WORD	A string that he name of the view that enables you only to view the contents of the agent
	write	The option that allows you to specify a write view (default none)
	WORD	A string that is the name of the view that enables you to enter and configure the contents of the agent

Command Mode Configure terminal mode

No/clear no snmp-server group WORD v3 (noauthlauthlpriv)

Show show snmp-server group

Default None

Description Configure a new SNMP group, that maps SNMP users to SNMP users

Examples ASUS(config)# snmp-server group g1 v3 priv read r1 write w1

11.29 snmp-server group WORD v3 priv read WORD write WORD notify WORD

Syntax snmp-server group WORD v3 priv read WORD write WORD notify WORD

Parameters

group	Configure a new SNMP group, that maps SNMP users to SNMP users
WORD	The name of the group
v3	Using the SNMPv3 for security mode
priv	Specifies authentication of a packet with encryption
read	The option that allows you to specify a read view (default sysView)
WORD	A string that he name of the view that enables you only to view the contents of the agent
write	The option that allows you to specify a write view (default none)

	WORD	A string that is the name of the view that enables you to enter and configure the contents of the agent
	notify	The option that allows you to specify a notify view (default none)
	WORD	A string that is the name of the view that enables you to specify a notify, inform, or trap

Command Mode Configure terminal mode

No/clear no snmp-server group WORD v3 (noauthlauthlpriv)

Show show snmp-server group

Default None

Description Configure a new SNMP group, that maps SNMP users to SNMP users

Examples ASUS(config)# snmp-server group g1 v3 priv read r1 write w1 notify n1

11.30 snmp-server view WORD WORD (included|excluded)

Syntax snmp-server view WORD WORD (includedlexcluded)

Parameters

	view	Create a view entry
	WORD	The view name is used to reference the record
	WORD	To identify the subtree, specify a text string consisting of numbers, such as .1.3.6.2.4, or a word (default, .1)
	(includedlexcluded)	Type of view

Command Mode Configure terminal mode

No/clear no snmp-server view WORD

Show show snmp-server view

Default None

Description Create a view entry

Examples ASUS(config)# snmp-server view v1 .1.3.6.2.4 include

11.31 show snmp-server view

Syntax	show snmp-server view	
Parameters	snmp-server	the SNMP server
	view	Show the view name which is used to reference the record
Command Mode	Privileged EXEC mode	
Default		
Description	Show the view name which is used to reference the record.	
Examples	ASUS# show snmp-server view	

11.32 show snmp-server group

Syntax	show snmp-server group	
Parameters	snmp-server	the SNMP server
	group	Show SNMPv3 groups
Command Mode	Privileged EXEC mode	
Default		
Description	Show SNMPv3 groups	
Examples	ASUS# show snmp-server group	

11.33 show snmp-server user

Syntax	show snmp-server user	
Parameters	snmp-server	the SNMP server
	user	Show SNMPv3 users
Command Mode	Privileged EXEC mode	
Default		
Description	Show SNMPv3 users	
Examples	ASUS# show snmp-server user	

11.34 snmp-server host A.B.C.D version (1|2) [COMMUNITY]

Syntax	snmp-server host A.B.C.D version (1l2) [COMMUNITY]	
Parameters	host	the recipient (host) of a SNMP notification
	operation	
	A.B.C.D	IP address
	Version(1l2)	snmp version1 or version2
	COMMUNITY	trap community name
Command Mode	Configure terminal mode	
No/clear	no snmp-server host A.B.C.D	
Show	show snmp-server host / show running-config	
Default	None or depends on ODM customer	
Description	This command sets the SNMP Contact information	
Examples	ASUS(config)# snmp-server host 192.192.1.11 version 1 abcd	

11.35 no snmp-server community trap

Syntax	No snmp-server community trap	
Parameters	community	SNMP server community
	trap	for trap use
Command Mode	Configure terminal mode	
No/clear		
Show	show snmp-server trap community / show running-config	
Default	Public	
Description	This command sets the trap community string for SNMP protocol.	
Examples	ASUS# no snmp-server community trap	

11.36 show rmon alarms

Syntax	show rmon alarms

Parameters

Command Mode Privileged EXEC mode

Default

Description Displays the RMON alarm table

Examples ASUS# show rmon alarms

11.37 show rmon events

Syntax show rmon alarms

Parameters

Command Mode Privileged EXEC mode

Default

Description Displays the RMON event table

Examples ASUS# show rmon events

11.38 show rmon history

Syntax show rmon history

Parameters

Command Mode Privileged EXEC mode

Default

Description Displays the RMON historytable

Examples ASUS# show rmon history

11.39 rmon alarm <1-65536> OID <1-4294967295> (absolute|delta) rising-threshold VALUE <1-65535> falling-threshold VALUE <1-65535> [OWNER]

Syntax rmon alarm <1-65536> OID <1-4294967295> (absolute|delta) rising-threshold VALUE <1-65535> falling-threshold VALUE <1-65535> [OWNER]

Parameters

<1-65536>	Specify the alarm number
OID	The MIB object, 1.3.6.1.2.1.16.1.1.1.5.1 for

		etherStatsPkts of port 1
	<1-4294967295>	The time interval of alarm monitor, in seconds
	absolute	To test each MIB variable directly
	delta	To test the change between samples of a MIB variable
	VALUE	The rising threshold value, the range is -2147483648 to 2147483647
	<1-65535>	Specify the RMON event to trigger when rising threshold exceeds
	VALUE	The falling threshold value, the range is -2147483648 to 2147483647
	<1-65535>	Specify the RMON event to trigger when falling threshold exceeds
	[OWNER]	Specify the owner of this RMON alarm

Command Mode Configure terminal mode

No/clear no rmon alarm <1-65536>

Default

Description To add rmon alarm entry

Examples ASUS(config)# rmon alarm 33 1.3.6.1.2.1.16.1.1.1.5.1 10 delta rising-threshold 10000 10 falling-threshold 1000 20 asus

11.40 rmon alarm <1-65536> OID <1-4294967295> (absolute|delta) rising-threshold VALUE <1-65535> falling-threshold VALUE [OWNER]

Syntax rmon alarm <1-65536> OID <1-4294967295> (absolute|delta) rising-threshold VALUE <1-65535> falling-threshold VALUE [OWNER]

Parameters	<1-65536>	Specify the alarm number
	OID	The MIB object, 1.3.6.1.2.1.16.1.1.1.5.1 for etherStatsPkts of port 1
	<1-4294967295>	The time interval of alarm monitor, in seconds

	absolute	To test each MIB variable directly
	delta	To test the change between samples of a MIB variable
	VALUE	The rising threshold value, the range is -2147483648 to 2147483647
	<1-65535>	Specify the RMON event to trigger when rising threshold exceeds
	VALUE	The falling threshold value, the range is -2147483648 to 2147483647
	[OWNER]	Specify the owner of this RMON alarm

Command Mode Configure terminal mode

No/clear no rmon alarm <1-65536>

Default

Description To add rmon alarm entry

Examples ASUS(config)# rmon alarm 33 1.3.6.1.2.1.16.1.1.1.5.1 10 delta rising-threshold 10000 10 falling-threshold 1000 asus

11.41 rmon alarm <1-65536> OID <1-4294967295> (absolute|delta) rising-threshold VALUE falling-threshold VALUE <1-65535> [OWNER]

Syntax rmon alarm <1-65536> OID <1-4294967295> (absolute|delta) rising-threshold VALUE falling-threshold VALUE <1-65535> [OWNER]

Parameters	<1-65536>	Specify the alarm number
	OID	The MIB object, 1.3.6.1.2.1.16.1.1.1.5.1 for etherStatsPkts of port 1
	<1-4294967295>	The time interval of alarm monitor, in seconds
	absolute	To test each MIB variable directly
	delta	To test the change between samples of a MIB variable
	VALUE	The rising threshold value, the range is -2147483648 to 2147483647

	VALUE	The falling threshold value, the range is -2147483648 to 2147483647
	<1-65535>	Specify the RMON event to trigger when falling threshold exceeds
	[OWNER]	Specify the owner of this RMON alarm
Command Mode	Configure terminal mode	
No/clear	no rmon alarm <1-65536>	
Default		
Description	To add rmon alarm entry	
Examples	ASUS(config)# rmon alarm 33 1.3.6.1.2.1.16.1.1.1.5.1 10 delta rising-threshold 10000 falling-threshold 1000 10 asus	

11.42 rmon alarm <1-65536> OID <1-4294967295> (absolute|delta) rising-threshold VALUE falling-threshold VALUE [OWNER]

Syntax	rmon alarm <1-65536> OID <1-4294967295> (absolute|delta) rising-threshold VALUE falling-threshold VALUE [OWNER]	
Parameters	<1-65536>	Specify the alarm number
	OID	The MIB object, 1.3.6.1.2.1.16.1.1.1.5.1 for etherStatsPkts of port 1
	<1-4294967295>	The time interval of alarm monitor, in seconds
	absolute	To test each MIB variable directly
	delta	To test the change between samples of a MIB variable
	VALUE	The rising threshold value, the range is -2147483648 to 2147483647
	VALUE	The falling threshold value, the range is -2147483648 to 2147483647
	[OWNER]	Specify the owner of this RMON alarm
Command Mode	Configure terminal mode	
No/clear	no rmon alarm <1-65536>	

Default

Description To add rmon alarm entry

Examples ASUS(config)# rmon alarm 33 1.3.6.1.2.1.16.1.1.1.5.1 10 delta rising-threshold 10000 falling-threshold 1000 asus

11.43 rmon event <1-65536> description NAME [OWNER]

Syntax rmon event <1-65536> description NAME [OWNER]

Parameters

<1-65536>	Specify the event number
NAME	The description string
[OWNER]	Specify the owner of this RMON event

Command Mode Configure terminal mode

No/clear no rmon evnet <1-65536>

Default

Description To add RMON event entry

Examples ASUS(config)# rmon event 20 description falling-threshold asus

11.44 rmon event <1-65536> description NAME log [OWNER]

Syntax rmon event <1-65536> description NAME log [OWNER]

Parameters

<1-65536>	Specify the event number
NAME	The description string
log	Generate an RMON log when the event is triggered
[OWNER]	Specify the owner of this RMON event

Command Mode Configure terminal mode

No/clear no rmon evnet <1-65536>

Default

Description To add RMON event entry

Examples ASUS(config)# rmon event 20 description falling-threshold log asus

11.45 rmon event <1-65536> description NAME trap COMMUNITY [OWNER]

Syntax	rmon event <1-65536> description NAME trap COMMUNITY [OWNER]	
Parameters	<1-65536>	Specify the event number
	NAME	The description string
	trap triggered	Generate an SNMP trap when the event is
	COMMUNITY	The SNMP community string
	[OWNER]	Specify the owner of this RMON event
Command Mode	Configure terminal mode	
No/clear	no rmon evnet <1-65536>	
Default		
Description	To add RMON event entry	
Examples	ASUS(config)# rmon event 20 description falling-threshold trap public asus	

11.46 rmon event <1-65536> description NAME log trap COMMUNITY [OWNER]

Syntax	rmon event <1-65536> description NAME trap COMMUNITY [OWNER]	
Parameters	<1-65536>	Specify the event number
	NAME	The description string
	log triggered	Generate an RMON log when the event is
	trap triggered	Generate an SNMP trap when the event is
	COMMUNITY	The SNMP community string
	[OWNER]	Specify the owner of this RMON event
Command Mode	Configure terminal mode	
No/clear	no rmon evnet <1-65536>	

Default

Description To add RMON event entry

Examples ASUS(config)# rmon event 20 description falling-threshold log trap public asus

11.47 rmon history <1-65536> IFNAME [OWNER]

Syntax rmon history <1-65536> IFNAME [OWNER]

Parameters

<1-65536>	Specify the RMON group of statistics
IFNAME	Interface name (e.g.; fastethernet1/0/1)
[OWNER]	Specify the owner of this RMON history group

Command Mode Configure terminal mode

No/clear no rmon history <1-65536>

Default

Description To add RMON history entry

Examples ASUS(config)# rmon history 20 fa1/0/1 asus

11.48 rmon history <1-65536> IFNAME buckets <1-100> [OWNER]

Syntax rmon history <1-65536> IFNAME buckets <1-100> [OWNER]

Parameters

<1-65536>	Specify the RMON group of statistics
IFNAME	Interface name (e.g.; fastethernet1/0/1)
buckets	Specify the maximum number of buckets for RMON history
<1-100>	The bucket request number, default is 50
[OWNER]	Specify the owner of this RMON history group

Command Mode Configure terminal mode

No/clear no rmon history <1-65536>

Default

Description To add RMON history entry

Examples ASUS(config)# rmon history 20 fa1/0/1 buckets 30 asus

11.49 rmon history <1-65536> IFNAME interval <1-4294967295> [OWNER]

Syntax	rmon history <1-65536> IFNAME interval <1-4294967295> [OWNER]	
Parameters	<1-65536>	Specify the RMON group of statistics
	IFNAME	Interface name (e.g.; fastethernet1/0/1)
	interval	Specify the time period of polling interval
	<1-4294967295>	The polling interval, in seconds
	[OWNER] group	Specify the owner of this RMON history
Command Mode	Configure terminal mode	
No/clear	no rmon history <1-65536>	
Default		
Description	To add RMON history entry	
Examples	ASUS(config)# rmon history 20 fa1/0/1 interval 30 asus	

11.50 rmon history <1-65536> IFNAME buckets <1-100> interval <1-4294967295> [OWNER]

Syntax	rmon history <1-65536> IFNAME buckets <1-100> interval <1-4294967295> [OWNER]	
Parameters	<1-65536>	Specify the RMON group of statistics
	IFNAME	Interface name (e.g.; fastethernet1/0/1)
	buckets for RMON history	Specify the maximum number of buckets
	<1-100>	The bucket request number, default is 50
	interval	Specify the time period of polling interval
	<1-4294967295>	The polling interval, in seconds
	[OWNER] group	Specify the owner of this RMON history

Command Mode	Configure terminal mode
No/clear	no rmon history <1-65536>
Default	
Description	To add RMON history entry
Examples	ASUS(config)# rmon history 20 fa1/0/1 buckets 30 interval 30 asus

12. ACL : MAC Filter

12.1 mac access-list extended WORD

Syntax	mac access-list extended WORD	
Parameters	Access-list	named access-list
	extended	extended access-list
	WORD	a access-list name
Command Mode	Configure terminal mode	
No/clear	no mac access-list extended WORD	
Show	Show acces-lists [numberlname]	
Default		
Description	This command define an extended MAC access list using a name , and enter access-list configuration mode.	
Examples	ASUS(config)# mac access-list extended abc	

12.2 show mac access-group [IFNAME]

Syntax	show mac access-group [IFNAME]
Parameters	[IFNAME] ex: fa1/0/1
Command Mode	Privileged EXEC mode
Default	None or depends on ODM customer
Description	Use the show mac access-group [IFNAME] EXEC command to

display the parameters for an mac access on the switch.

Examples ASUS# show mac access-group [fa1/0/1]

12.3 show mac access-list [ACLNAME]

Syntax show mac access-list [ACLNAME]

Parameters [ACLNAME] ex: mac access list name

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description Use the show mac access-list [IFNAME] EXEC command to display the parameters for an mac access on the switch.

Examples ASUS# show mac access-list rd10

12.4 (permit|deny) any any [IFNAME]

Syntax (permitldeny) any any [IFNAME]

Parameters

permit->	Specify packets to forward
deny->	Specify packets to reject.
any	any source Mac address
any	any destination Mac address
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no (permitldeny) any any [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)# permit any any [fa1/0/1]

12.5 (permit|deny) MACADDR MACADDR any [IFNAME]

Syntax (permitldeny) MACADDR MACADDR any [IFNAME]

Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	MACADDR	Source MAC address xxxx.xxxx.xxxx
	MACADDR	Source MAC address mask xxxx.xxxx.xxxx
	any	any destination Mac address
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no (permit|deny) MACADDR MACADDR any [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)# permit 0000.0000.0001 0000.0000.0000 any [fa1/0/1]	

12.6 (permit|deny) host MACADDR any [IFNAME]

Syntax	(permit|deny) host MACADDR any [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	host	A single source host
	MACADDR	Source MAC address xxxx.xxxx.xxxx
	any	any destination Mac address
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	(permit|deny) host MACADDR any [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	

Examples ASUS(config)# permit host 0000.0000.0001 any[fa1/0/2]

12.7 (permit|deny) host MACADDR host MACADDR [IFNAME]

Syntax	(permitldeny) host MACADDR host MACADDR [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	host	A single source host
	MACADDR	Source MAC address xxxx.xxxx.xxxx
	host	A single destination host
	MACADDR	Destination MAC address xxxx.xxxx.xxxx
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no (permitldeny) host MACADDR host MACADDR [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)# permit host 0000.0000.0001 host 0000.0000.0002 [fa1/0/2]	

12.8 (permit|deny) MACADDR MACADDR MACADDR MACADDR [IFNAME]

Syntax	(permitldeny) MACADDR MACADDR MACADDR MACADDR [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	MACADDR	Source MAC address xxxx.xxxx.xxxx
	MACADDR	Source MAC address mask xxxx.xxxx.xxxx
	MACADDR	Destination MAC address xxxx.xxxx.xxxx

	MACADDR xxxx	Destination MAC address mask xxxx.xxxx.
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no (permit|deny) MACADDR MACADDR MACADDR MACADDR [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)# permit 0000.0000.0001 0000.0000.0000 0000.0000.0002 0000.0000.0000 [fa1/0/2]	

12.9 (permit|deny) host MACADDR MACADDR MACADDR [IFNAME]

Syntax	(permit|deny) host MACADDR MACADDR MACADDR [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	host	A single source host
	MACADDR	Source MAC address xxxx.xxxx.xxxx
	MACADDR	Destination MAC address xxxx.xxxx.xxxx
	MACADDR xxxx	Destination MAC address mask xxxx.xxxx.
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no (permit|deny) host MACADDR MACADDR MACADDR [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	

Examples ASUS(config)# permit host 0000.0000.0001 0000.0000.0002 0000.0000.0000 [fa1/0/2]

12.10 (permit|deny) MACADDR MACADDR host MACADDR [IFNAME]

Syntax	(permitldeny) MACADDR MACADDR host MACADDR [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	MACADDR	Source MAC address xxxx.xxxx.xxxx
	MACADDR	Source address mask xxxx.xxxx.xxxx
	host	A single destination host
	MACADDR	Destination MAC address xxxx.xxxx.xxxx
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no (permitldeny) MACADDR MACADDR host MACADDR [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)# permit 0000.0000.0001 0000.0000.0000 host 0000.0000.0002 [fa1/0/2]	

12.11 (permit|deny) any host MACADDR [IFNAME]

Syntax	(permitldeny) any host MACADDR [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	.any	any source Mac address
.	host	A single destination host
.	MACADDR	Destination MAC address xxxx.xxxx.xxxx

	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no (permit|deny) any host MACADDR [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)# permit any host 0000.0000.0002 [fa1/0/1]	

12.12 (permit|deny) any MACADDR MACADDR [IFNAME]

Syntax	(permit|deny) any MACADDR MACADDR [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	any	any source MAC address
	MACADDR	Destination MAC address xxxx.xxxx.xxxx
	MACADDR xxxx	Destination MAC address mask xxxx.xxxx.
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no (permit|deny) any MACADDR MACADDR [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)# permit any 0000.0000.0001 0000.0000.0000 [fa1/0/2]	

12.13 mac access-group WORD in

Syntax	mac access-group WORD in

Parameters	Access-list	named access-list
	extended	extended access-list
	WORD	access-list name
Command Mode	Interface mode	
No/clear	no mac access-group WORD	
Show	show mac access-group [INTERFACE]	
Default		
Description	This command define an extended MAC access list using a name , and enter access-list configuration mode.	
Examples	ASUS(config-if)# mac access-group abc in	

13. ACL: IP Filter

13.1 ip access-list extended (<100-199>|<2000-2699>|WORD)

Syntax	ip access-list extended (<100-199>I<2000-2699>IWORD)	
Parameters	Ip	Global IP configuration subcommands
	Access-list	named access-list
	extended	extended access-list
	<100-199>	Extended IP access-list number
	<2000-2699>	Extended IP access-list number (expanded range)
	WORD	a access-list name
Command Mode	Configure terminal mode	
No/clear	no ip access-list extended (<100-199>I<2000-2699>IWORD)	
Show	Show acces-lists [numberIname]	
Default		
Description	This command define an extended IP access list using a name or number, and enter access-list configuration mode.	

Examples ASUS(config)# ip access-list extended 100

13.2 ip access-list standard (<1-99>|<1300-1999>|WORD)

Syntax ip access-list standard (<1-99>I<1300-1999>IWORD)

Parameters

Ip	Global IP configuration subcommands
Access-list	named access-list
standard	standard access-list
<1-99> ->	standard IP access-list number
<1300-1999> ->	standard IP access-list number (expanded range)
WORD ->	a access-list name

Command Mode Configure terminal mode

No/clear no ip access-list standard (<1-99>I<1300-1999>IWORD)

Show Show acces-lists [numberIname]

Default

Description This command define an standard IP access list using a name or number, and enter access-list configuration mode.

Examples ASUS(config)# ip access-list standard 99

13.3 show ip access-group [IFNAME]

Syntax show ip access-group [IFNAME]

Parameters IFNAME: interface name

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description Show ip access rule to attach with the specific interface

Examples ASUS# show ip access-group fa1/0/1

13.4 show ip access list

Syntax show ip access list

Parameters

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description Use the show ip access list EXEC command to display the parameters for all ip access on the switch.

Examples ASUS# show ip access list

13.5 show ip access list WORD

Syntax show ip access list WORD

Parameters WORD ip access name.

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description Use the show ip access lists WORD EXEC command to display the parameters for an ip access on the switch.

Examples ASUS# show ip access list abc

13.6 show ip access list (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)

Syntax show ip access list (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)

Parameters Standard or extended ID

Command Mode Privileged EXEC mode

Default None or depends on ODM customer

Description Use the show ip access list EXEC command to display the parameters for an ip access on the switch.

Examples ASUS# show ip access list 100

13.7 (permit|deny) any [IFNAME]

Syntax (permit|deny) any [IFNAME]

Parameters permit-> Specify packets to forward

	deny->	Specify packets to reject.
	any	Any source host
	[IFNAME]	Egress interface name
Command Mode	IP standard access-list mode	
No/clear	no (permit|deny) any [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-std-nacl)#permit any [fa1/0/1]	

13.8 (permit|deny) host IPADDR [IFNAME]

Syntax	(permit|deny) host IPADDR [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	host	A single host address
	IPADDR	Host address
	[IFNAME]	Egress interface name
Command Mode	IP standard access-list mode	
No/clear	no (permit|deny) host IPADDR [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-std-nacl)#permit host 10.0.0.1 [fa1/0/1]	

13.9 (permit|deny) IPADDR MASK [IFNAME]

Syntax	(permit|deny) IPADDR MASK [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.

	host	A single host address
	IPADDR	Host address
	MASK	Wildcard bits
	[IFNAME]	Egress interface name
Command Mode	IP standard access-list terminal mode	
No/clear	no (permit|deny) host IPADDR A.B.C.D [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description		
	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-std-nacl)#permit 10.0.0.1 0.0.0.0 [fa1/0/1]	

13.10 (permit|deny) (ip|tcp|udp|icmp) any any [IFNAME]

Syntax	(permit|deny) (ip|tcp|udp|icmp) any any [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	any	any source address
	any	any destination address
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (ip|tcp|udp|icmp) any any [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or	

permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)#permit ip any any [fa1/0/1]

13.11 (permit|deny) (tcp|udp) any [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]

Syntax (permit|deny) (tcp|udp) any [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]

Parameters

permit->	Specify packets to forward
deny->	Specify packets to reject.
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
any	any source address
eq	Match only packets on a given port numbe
<0-65535>	Port number
any	any destination address
eq	Match only packets on a given port numbe
<0-65535>	Port number
[IFNAME]	Egress interface name

Command Mode IP extended access-list mode

No/clear no (permit|deny) (tcp|udp) any [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)#permit tcp any eq 100 any eq 100 [fa1/0/1]

13.12 (permit|deny) icmp any any [<1-255>] code [<1-255>] [IFNAME]

Syntax (permit|deny) icmp any any [<1-255>] code [<1-255>] [IFNAME]

Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	any	any source address
	any	any destination address
	<1-255>	ICMP message type
	<1-255>	ICMP message code
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) icmp any any [<1-255>] code [<1-255>] [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit icmp any any 12 code 12 [fa1/0/1]	

13.13 (permit|deny) (ip|tcp|udp|icmp) IPADDR MASK any [IFNAME]

Syntax	(permit|deny) (ip|tcp|udp|icmp) IPADDR MASK any [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	IPADDR	Source address
	MASK	Source wildcard bits
	any	any destination address
	[IFNAME]	Egress interface name

Command Mode IP extended access-list mode

No/clear no (permitIdeny) (ipItcpludplicmp) IPADDR MASK any [IFNAME]

Show Show acces-lists [numberIname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)#permit ip 10.0.0.1 0.0.0.0 any [fa1/0/1]

13.14 (permit|deny) (tcp|udp) IPADDR MASK [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]

Syntax (permitIdeny) (tcpludp) IPADDR MASK [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]

Parameters

permit->	Specify packets to forward
deny->	Specify packets to reject.
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
IPADDR	Source address
MASK	Source wildcard bits
eq	Match only packets on a given port numbe
<0-65535>	Port number
any	any destination address
eq	Match only packets on a given port numbe
<0-65535>	Port number
[IFNAME]	Egress interface name

Command Mode IP extended access-list mode

No/clear no (permitIdeny) (tcpludp) IPADDR MASK [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]

Show Show acces-lists [numberIname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)#permit tcp 10.0.0.1 0.0.0.0 eq 12 any eq 12 [fa1/0/1]

13.15 (permit|deny) icmp IPADDR MASK any <1-255> code <1-255> [IFNAME]

Syntax (permit|deny) icmp IPADDR MASK any [<1-255>] code [<1-255>] [IFNAME]

Parameters

permit->	Specify packets to forward
deny->	Specify packets to reject.
Icmp->	Internet Control Message Protocol
IPADDR	Source address
MASK	Source wildcard bits
any	any destination address
<1-255>	ICMP message type
<1-255>	ICMP message code
[IFNAME]	Egress interface name

Command Mode IP extended access-list mode

No/clear no (permit|deny) icmp IPADDR MASK any [<1-255>] code [<1-255>] [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)#permit icmp 10.0.0.1 0.0.0.0 any 12 code 12 [fa1/0/1]

13.16 (permit|deny) (ip|tcp|udp|icmp) host IPADDR any [IFNAME]

Syntax (permit|deny) (ip|tcp|udp|icmp) host IPADDR any [IFNAME]

Parameters

permit->	Specify packets to forward
deny->	Specify packets to reject.

	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	host	A single source host
	IPADDR	Source address.
	any	any destination address
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	No (permit|deny) (ip|tcp|udp|icmp) host IPADDR any [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit ip host 10.0.0.1 any [fa1/0/1]	

13.17 (permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]

Syntax	(permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	host	A single source host
	IPADDR	Source address.
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	any	any destination address
	eq	Match only packets on a given port numbe

	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permitldeny) (tcpludp) host IPADDR [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit tcp host 10.0.0.1 eq 6 any eq 65 [fa1/0/1]	

13.18 (permit|deny) icmp host IPADDR any [<1-255>] code [<1-255>] [IFNAME]

Syntax	(permitldeny) icmp host IPADDR any [<1-255>] code [<1-255>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	host	A single source host
	IPADDR	Source address.
	any	any destination address
	<1-255>	ICMP message type
	<1-255>	ICMP message code
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	No (permitldeny) icmp host IPADDR any [<1-255>] code [<1-255>] [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or	

permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)# permit icmp host 10.0.0.1 any 12 code 12 [fa1/0/1]

13.19 (permit|deny) (ip|tcp|udp|icmp) host IPADDR host IPADDR [IFNAME]

Syntax (permit|deny) (ip|tcp|udp|icmp) host IPADDR host IPADDR [IFNAME]

Parameters

permit->	Specify packets to forward
deny->	Specify packets to reject.
Ip ->	Any Internet Protocol
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
Icmp->	Internet Control Message Protocol
host	A single source host
IPADDR	Source address
host	A single destination host
IPADDR	Destination address
[IFNAME]	Egress interface name

Command Mode IP extended access-list mode

No/clear no (permit|deny) (ip|tcp|udp|icmp) host IPADDR host IPADDR [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)#permit icmp host 10.0.0.1 host 10.0.0.25 [fa1/0/1]

13.20 (permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]

Syntax	(permitldeny) (tcpludp) host IPADDR [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	host	A single source host
	IPADDR	Source address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	host	A single destination host
	IPADDR	Destination address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permitldeny) (tcpludp) host IPADDR [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit tcp host 10.0.0.1 eq 655 host 10.0.0.2 eq 65 [fa1/0/2]	

13.21 (permit|deny) icmp host IPADDR host IPADDR [<1-255>] code [<1-255>] [IFNAME]

Syntax	(permitldeny) icmp host IPADDR host IPADDR [<1-255>] code

	[<1-255>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	host	A single source host
	IPADDR	Source address
	host	A single destination host
	IPADDR	Destination address
	<1-255>	ICMP message type
	<1-255>	ICMP message code
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permitldeny) icmp host IPADDR host IPADDR [<1-255>] code [<1-255>] [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit icmp host 10.0.0.1 host 10.0.0.2 2 code 2 [fa1/0/1]	

13.22 (permit|deny) (ip|tcp|udp|icmp) IPADDR MASK IPADDR MASK [IFNAME]

Syntax	(permitldeny) (ipltcpludplicmp) IPADDR MASK IPADDR MASK [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol

	IPADDR	Source address
	MASK	Source address mask
	IPADDR	Destination address
	MASK	Destination address mask
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (ip|tcp|udp|icmp) IPADDR MASK IPADDR MASK [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit ip 10.0.0.1 0.0.0.0 10.0.0.2 0.0.0.0 [fa1/0/1]	

13.23 (permit|deny) (tcp|udp) IPADDR MASK [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]

Syntax	(permit|deny) (tcp|udp|) IPADDR MASK [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	IPADDR	Source address
	MASK	Source address mask
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	IPADDR	Destination address
	MASK	Destination address mask

	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp|l) IPADDR MASK [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit tcp 10.0.0.1 0.0.0.0 eq 2 10.0.0.2 0.0.0.0 eq 3 [fa1/0/1]	

13.24 (permit|deny) icmp IPADDR MASK IPADDR MASK <1-255> code <1-255> [IFNAME]

Syntax	(permit|deny) icmp IPADDR MASK IPADDR MASK <1-255> code <1-255> [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	IPADDR	Source address
	MASK	Source address mask
	IPADDR	Destination address
	MASK	Destination address mask
	<1-255>	ICMP message type
	<1-255>	ICMP message code
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) icmp IPADDR MASK IPADDR MASK <1-255> code <1-255> [IFNAME]	
Show	Show acces-lists [number|name]	

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)#permit icmp 10.0.0.1 0.0.0.0 10.0.0.2 0.0.0.0 2 code 2 [fa1/0/2]

13.25 (permit|deny) (ip|tcp|udp|icmp) host IPADDR IPADDR MASK [IFNAME]

Syntax (permit|deny) (ip|tcp|udp|icmp) host IPADDR IPADDR MASK [IFNAME]

Parameters

permit->	Specify packets to forward
deny->	Specify packets to reject.
host	A single source host
Ip ->	Any Internet Protocol
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
Icmp->	Internet Control Message Protocol
IPADDR	Source address
IPADDR	Destination address
MASK	Destination address mask
[IFNAME]	Egress interface name

Command Mode IP extended access-list mode

No/clear no (permit|deny) (ip|tcp|udp|icmp) host IPADDR IPADDR MASK [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)#permit tcp host 10.0.0.1 10.0.0.2 0.0.0.0 [fa1/0/2]

13.26 (permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]

Syntax	(permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	host	A single source host
	IPADDR	Source address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	IPADDR	Destination address
	MASK	Destination address mask
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit tcp host 10.0.0.1 eq 2 10.0.0.2 0.0.0.0 eq 2 [fa1/0/2]	

13.27 (permit|deny) icmp host IPADDR IPADDR MASK <1-255> code <1-255> [IFNAME]

Syntax	(permitldeny) icmp host IPADDR IPADDR MASK <1-255> code <1-255> [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	host	A single source host
	IPADDR	Source address
	IPADDR	Destination address
	MASK	Destination address mask
	<1-255>	ICMP message type
	<1-255>	ICMP message code
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permitldeny) icmp host IPADDR IPADDR MASK <1-255> code <1-255> [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit icmp host 10.0.0.1 10.0.0.2 0.0.0.0 2 code 2 [fa1/0/2]	

13.28 (permit|deny) (ip|tcp|udp|icmp) IPADDR MASK host IPADDR [IFNAME]

Syntax	(permitldeny) (ipltcpludplicmp) IPADDR MASK host IPADDR [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.

	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	IPADDR	Source address
	MASK	Source address mask
	host	A single destination host
	IPADDR	Destination address
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permitldeny) (ipltcpludplicmp) IPADDR MASK host IPADDR [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit tcp 10.0.0.1 0.0.0.0 host 10.0.0.2 [fa1/0/2]	

13.29 (permit|deny) (tcp|udp) IPADDR MASK [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]

Syntax	(permitldeny) (tcpludp) IPADDR MASK [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	IPADDR	Source address
	MASK	Source address mask
	eq	Match only packets on a given port numbe
	<0-65535>	Port number

	host	A single destination host
	IPADDR	Destination address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) IPADDR MASK [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit tcp 10.0.0.1 0.0.0.0 eq 65 host 10.0.0.2 eq 64 [fa1/0/2]	

13.30 (permit|deny) icmp IPADDR MASK host IPADDR <1-255> code <1-255> [IFNAME]

Syntax	(permit|deny) icmp IPADDR MASK host IPADDR <1-255> code <1-255> [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	IPADDR	Source address
	MASK	Source address mask
	host	A single destination host
	IPADDR	Destination address
	<1-255>	ICMP message type
	<1-255>	ICMP message code
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) icmp IPADDR MASK host IPADDR <1-255>	

code <1-255> [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)# permit icmp 10.0.0.1 0.0.0.0 host 10.0.0.2 1 code 1 [fa1/0/2]

13.31 (permit|deny) (ip|tcp|udp|icmp) any host IPADDR [IFNAME]

Syntax (permit|deny) (ip|tcp|udp|icmp) any host A.B.C.D [IFNAME]

Parameters

permit->	Specify packets to forward
deny->	Specify packets to reject.
Ip ->	Any Internet Protocol
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
Icmp->	Internet Control Message Protocol
any	any source address
host	A single destination host
IPADDR	Destination address
[IFNAME]	Egress interface name

Command Mode IP extended access-list mode

No/clear no (permit|deny) (ip|tcp|udp|icmp) any host IPADDR [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)#permit tcp any host 10.0.0.1 [fa1/0/2]

13.32 (permit|deny) (tcp|udp) any [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]

Syntax	(permitldeny) (tcpludp) any [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	.any	any source address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	.host	A single destination host
	IPADDR	Destination address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permitldeny) (tcpludp) any [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit tcp any eq 12 host 10.0.0.1 eq 12 [fa1/0/2]	

13.33 (permit|deny) icmp any host IPADDR <1-255> code <1-255> [IFNAME]

Syntax	(permitldeny) icmp any host IPADDR <1-255> code <1-255> [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	any	any source address
	host	A single destination host
	IPADDR	Destination address
	<1-255>	ICMP message type
	<1-255>	ICMP message code
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permitldeny) icmp any host IPADDR <1-255> code <1-255> [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit icmp any host 10.0.0.1 2 code 2 [fa1/0/2]	

13.34 (permit|deny) (ip|tcp|udp|icmp) any IPADDR MASK [IFNAME]

Syntax	(permitldeny) (ipltcpludplicmp) any IPADDR MASK [IFNAME]	
Parameters	permit->	Specify packets to forward

	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	any	any source address
	IPADDR	Destination address
	MASK	Destination address mask
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (ip|tcp|udp|icmp) any IPADDR MASK [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit tcp any 10.0.0.1 0.0.0.0 [fa1/0/2]	

13.35 (permit|deny) (tcp|udp) any [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]

Syntax	(permit|deny) (tcp|udp) any [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	any	any source address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	IPADDR	Destination address
	MASK	Destination address mask

	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) any [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit tcp any eq 65 10.0.0.1 0.0.0.0 eq 43 [fa1/0/2]	

13.36 (permit|deny) icmp any IPADDR MASK <1-255> code <1-255> [IFNAME]

Syntax	(permit|deny) icmp any IPADDR MASK <1-255> code <1-255> [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	any	any source address
	IPADDR	Destination address
	MASK	Destination address mask
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) icmp any IPADDR MASK <1-255> code <1-255> [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	

Examples ASUS(config-ext-acl)# permit icmp any 10.0.0.1 0.0.0.0 2 code 3 [fa1/0/2]

13.37 (permit|deny) (tcp|udp) IPADDR MASK IPADDR MASK [eq] [<0-65535>] [IFNAME]

Syntax (permitldeny) (tcpludpl) IPADDR MASK IPADDR MASK [eq] [<0-65535>] [IFNAME]

Parameters

permit->	Specify packets to forward
deny->	Specify packets to reject.
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
IPADDR	Source address
MASK	Source address mask
IPADDR	Destination address
MASK	Destination address mask
eq	Match only packets on a given port numbe
<0-65535>	Port number
[IFNAME]	Egress interface name

Command Mode IP extended access-list mode

No/clear no (permitldeny) (tcpludpl) IPADDR MASK IPADDR MASK [eq] [<0-65535>] [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)#permit tcp 10.0.0.1 0.0.0.0 10.0.0.2 0.0.0.0 eq 23 [fa1/0/1]

13.38 (permit|deny) (tcp|udp) IPADDR MASK [eq] [<0-65535>] IPADDR MASK [IFNAME]

Syntax (permitldeny) (tcpludpl) IPADDR MASK [eq] [<0-65535>]

	IPADDR MASK [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	IPADDR	Source address
	MASK	Source address mask
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	IPADDR	Destination address
	MASK	Destination address mask
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp|) IPADDR MASK [eq] [<0-65535>] IPADDR MASK [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit tcp 10.0.0.1 0.0.0.0 eq 23 10.0.0.2 0.0.0.0 [fa1/0/1]	

13.39 (permit|deny) (tcp|udp) IPADDR A.B.C.D [eq] [<0-65535>] any [IFNAME]

Syntax	(permit|deny) (tcp|udp) IPADDR MASK [eq] [<0-65535>] any [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	IPADDR	Source address

	MASK	Source wildcard bits
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	any	any destination address
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) IPADDR MASK [eq] [<0-65535>] any [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit tcp 10.0.0.1 0.0.0.0 eq 22 any [fa1/0/1]	

13.40 (permit|deny) (tcp|udp) IPADDR MASK any [eq] [<0-65535>] [IFNAME]

Syntax	(permit|deny) (tcp|udp) IPADDR MASK any [eq] [<0-65535>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	IPADDR	Source address
	MASK	Source wildcard bits
	any	any destination address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) IPADDR MASK any [eq] [<0-65535>]	

	[IFNAME]
Show	Show acces-lists [number|name]
Default	
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.
Examples	ASUS(config-ext-acl)# permit tcp 10.0.0.1 0.0.0.0 any eq 22 [fa1/0/1]

13.41 (permit|deny) (tcp|udp) IPADDR MASK [eq] [<0-65535>] host IPADDR [IFNAME]

Syntax	(permit|deny) (tcp|udp) IPADDR MASK [eq] [<0-65535>] host IPADDR [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	IPADDR	Source address
	MASK	Source address mask
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	host	A single destination host
	IPADDR	Destination address
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) IPADDR MASK [eq] [<0-65535>] host IPADDR [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit tcp 10.0.0.1 0.0.0.0 eq 2 host	

10.0.0.2 [fa1/0/1]

13.42 (permit|deny) (tcp|udp) IPADDR MASK host IPADDR [eq] [<0-65535>] [IFNAME]

Syntax	(permitldeny) (tcpludp) IPADDR MASK host IPADDR [eq] [<0-65535>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	IPADDR	Source address
	MASK	Source address mask
	host	A single destination host
	IPADDR	Destination address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permitldeny) (tcpludp) IPADDR MASK host IPADDR [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit tcp 10.0.0.1 0.0.0.0 host 10.0.0.2 eq 2 [fa1/0/1]	

13.43 (permit|deny) (tcp|udp) any [eq] [<0-65535>] IPADDR MASK [IFNAME]

Syntax	(permitldeny) (tcpludp) any [eq] [<0-65535>] IPADDR MASK [IFNAME]

Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	any	any source address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	IPADDR	Destination address
	MASK	Destination address mask
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) any [eq] [<0-65535>] IPADDR MASK [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit tcp any eq 2 10.0.0.1 0.0.0.0 [fa1/0/1]	

13.44 (permit|deny) (tcp|udp) any IPADDR MASK [eq] [<0-65535>] [IFNAME]

Syntax	(permit|deny) (tcp|udp) any IPADDR MASK [eq] [<0-65535>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	any	any source address
	IPADDR	Destination address
	MASK	Destination address mask

	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) any IPADDR MASK [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit tcp any 10.0.0.1 0.0.0.0 eq 2 [fa1/0/1]	

13.45 (permit|deny) (tcp|udp) any any [eq] [<0-65535>] [IFNAME]

Syntax	(permit|deny) (tcp|udp) any any [eq] [<0-65535>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	any	any source address
	any	any destination address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) any any [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	

Examples ASUS(config-ext-acl)#permit tcp any any eq 2 [fa1/0/1]

13.46 (permit|deny) (tcp|udp) any [eq] [<0-65535>] any [IFNAME]

Syntax	(permitldeny) (tcpludp) any [eq] [<0-65535>] any [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	any	any source address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	any	any destination address
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permitldeny) (tcpludp) any [eq] [<0-65535>] any [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit tcp any eq 2any [fa1/0/1]	

13.47 (permit|deny) (tcp|udp) any [eq] [<0-65535>] host IPADDR [IFNAME]

Syntax	(permitldeny) (tcpludp) any [eq] [<0-65535>] host IPADDR [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol

	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	.any	any source address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	.host	A single destination host
	IPADDR	Destination address
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) any [eq] [<0-65535>] host IPADDR [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit tcp any eq 2 host 10.0.0.2 [fa1/0/1]	

13.48 (permit|deny) (tcp|udp) any host IPADDR [eq] [<0-65535>] [IFNAME]

Syntax	(permit|deny) (tcp|udp) any host IPADDR [eq] [<0-65535>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	any	any source address
	host	A single destination host
	IPADDR	Destination address

	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) any host IPADDR [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit tcp any host 10.0.0.2 eq 2 [fa1/0/1]	

13.49 (permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] host IPADDR [IFNAME]

Syntax	(permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] host IPADDR [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	host	A single source host
	IPADDR	Source address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	host	A single destination host
	IPADDR	Destination address
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] host IPADDR [IFNAME]	
Show	Show acces-lists [number|name]	

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)#permit tcp host 10.0.0.1 eq 2 host 10.0.0.2 [fa1/0/1]

13.50 (permit|deny) (tcp|udp) host IPADDR host IPADDR [eq] [<0-65535>] [IFNAME]

Syntax (permit|deny) (tcp|udp) host IPADDR host IPADDR [eq] [<0-65535>] [IFNAME]

Parameters

permit->	Specify packets to forward
deny->	Specify packets to reject.
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
host	A single source host
IPADDR	Source address
host	A single destination host
IPADDR	Destination address
eq	Match only packets on a given port numbe
<0-65535>	Port number
[IFNAME]	Egress interface name

Command Mode IP extended access-list mode

No/clear no (permit|deny) (tcp|udp) host IPADDR host IPADDR [eq] [<0-65535>] [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)# permit tcp host 10.0.0.1 host 10.0.0.2 eq 2 [fa1/0/1]

13.51 (permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] IPADDR MASK [IFNAME]

Syntax	(permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] IPADDR MASK [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	host	A single source host
	IPADDR	Source address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	IPADDR	Destination address
	MASK	Destination address mask
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] IPADDR MASK [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit tcp host 10.0.0.1 eq 2 10.0.0.2 0.0.0.0 [fa1/0/1]	

13.52 (permit|deny) (tcp|udp) host IPADDR IPADDR MASK [eq] [<0-65535>] [IFNAME]

Syntax	(permit|deny) (tcp|udp) host IPADDR IPADDR MASK [eq] [<0-65535>] [IFNAME]	
Parameters	permit->	Specify packets to forward

	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	host	A single source host
	IPADDR	Source address
	IPADDR	Destination address
	MASK	Destination address mask
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name

Command Mode IP extended access-list mode

No/clear no (permit|deny) (tcp|udp) host IPADDR IPADDR MASK [eq] [<0-65535>] [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)# permit tcp host 10.0.0.1 10.0.0.2 0.0.0.0 eq 2 [fa1/0/1]

13.53 (permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] any [IFNAME]

Syntax (permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] any [IFNAME]

Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	host	A single source host
	IPADDR	Source address.
	eq	Match only packets on a given port numbe

	<0-65535>	Port number
	any	any destination address
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) host IPADDR [eq] [<0-65535>] any [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit tcp host 10.0.0.1 eq 2 any [fa1/0/1]	

13.54 (permit|deny) (tcp|udp) host IPADDR any [eq] [<0-65535>] [IFNAME]

Syntax	(permit|deny) (tcp|udp) host IPADDR any [eq] [<0-65535>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	host	A single source host
	IPADDR	Source address.
	any	any destination address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) (tcp|udp) host IPADDR any [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [number|name]	
Default		

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)# permit tcp host 10.0.0.1 any eq 2 [fa1/0/1]

13.55 (permit|deny) icmp IPADDR MASK IPADDR MASK <1-255> [IFNAME]

Syntax (permit|deny) icmp IPADDR MASK IPADDR MASK <1-255> [IFNAME]

Parameters

permit->	Specify packets to forward
deny->	Specify packets to reject.
Icmp->	Internet Control Message Protocol
IPADDR	Source address
MASK	Source address mask
IPADDR	Destination address
MASK	Destination address mask
<1-255>	ICMP message type
[IFNAME]	Egress interface name

Command Mode IP extended access-list mode

No/clear no (permit|deny) icmp IPADDR MASK IPADDR MASK <1-255> [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config-ext-acl)#permit icmp 10.0.0.1 0.0.0.0 10.0.0.2 0.0.0.0 2 [fa1/0/1]

13.56 (permit|deny) icmp host IPADDR IPADDR MASK <1-255> [IFNAME]

Syntax (permit|deny) icmp host IPADDR IPADDR MASK <1-255> [IFNAME]

Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	host	A single source host
	IPADDR	Source address
	IPADDR	Destination address
	MASK	Destination address mask
	<0-255>	ICMP message type
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permitIdeny) icmp host IPADDR IPADDR MASK <1-255> [IFNAME]	
Show	Show acces-lists [numberIname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit icmp host 10.0.0.1 10.0.0.2 0.0.0.0 2 [fa1/0/1]	

13.57 (permit|deny) icmp IPADDR MASK host IPADDR <1-255> [IFNAME]

Syntax	(permitIdeny) icmp IPADDR MASK host IPADDR <1-255> [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	IPADDR	Source address
	MASK	Source address mask
	host	A single destination host
	IPADDR	Destination address
	<1-255>	ICMP message type

	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) icmp IPADDR MASK host IPADDR <1-255> [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit icmp 10.0.0.1 0.0.0.0 host 10.0.0.2 2 [fa1/0/1]	

13.58 (permit|deny) icmp any host IPADDR <1-255> [IFNAME]

Syntax	(permit|deny) icmp any host IPADDR <1-255> [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	.any	any source address
	.host	A single destination host
	IPADDR	Destination address
	<1-255>	ICMP message type
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) icmp any host IPADDR <1-255> [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	

Examples ASUS(config-ext-acl)#permit icmp any host 10.0.0.1 2 [fa1/0/1]

13.59 (permit|deny) icmp any IPADDR MASK <1-255> [IFNAME]

Syntax	(permitldeny) icmp any IPADDR MASK <1-255> [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	any	any source address
	IPADDR	Destination address
	MASK	Destination address mask
	<1-255>	ICMP message type
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permitldeny) icmp any IPADDR MASK <1-255> [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)# permit icmp any 10.0.0.1 0.0.0.0 2 [fa1/0/1]	

13.60 (permit|deny) icmp any any [<1-255>] [IFNAME]

Syntax	(permitldeny) icmp any any [<1-255>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	any	any source address
	any	any destination address

	<1-255>	ICMP message type
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) ICMP any any [<1-255>] [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit icmp any any 2 [fa1/0/1]	

13.61 (permit|deny) icmp IPADDR MASK any [<1-255>] [IFNAME]

Syntax	(permit|deny) icmp IPADDR MASK any [<1-255>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	IPADDR	Source address
	MASK	Source wildcard bits
	any	any destination address
	<1-255>	ICMP message type
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) icmp IPADDR MASK any [<1-255>] [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit icmp 10.0.0.1 0.0.0.0 any 2 [fa1/0/1]	

13.62 (permit|deny) icmp host IPADDR any [<1-255>] [IFNAME]

Syntax	(permit|deny) icmp host IPADDR any [<1-255>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	host	A single source host
	IPADDR	Source address.
	any	any destination address
	<1-255>	ICMP message type
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	No (permit|deny) icmp host IPADDR any [<1-255>] [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit icmp host 10.0.0.1 any 2 [fa1/0/1]	

13.63 (permit|deny) icmp host IPADDR host IPADDR [<1-255>] [IFNAME]

Syntax	(permit|deny) icmp host A.B.C.D host A.B.C.D [<1-255>] [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	host	A single source host
	IPADDR	Source address
	host	A single destination host

	IPADDR	Destination address
	<1-255>	ICMP message type
	[IFNAME]	Egress interface name
Command Mode	IP extended access-list mode	
No/clear	no (permit|deny) icmp host IPADDR host IPADDR [<1-255>] [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-ext-acl)#permit icmp host 10.0.0.1 host 10.0.0.2 2 [fa1/0/1]	

13.64 (permit|deny) IPADDR [IFNAME]

Syntax	(permit|deny) A.B.C.D [IFNAME]	
Parameters	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	IPADDR	Host address
	[IFNAME]	Egress interface name
Command Mode	IP standard access-list terminal mode	
No/clear	no (permit|deny) host IPADDR [IFNAME]	
Show	Show acces-lists [number|name]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config-std-nacl)#permit 10.0.0.1 [fa1/0/1]	

13.65 remark .LINE

Syntax	remark .LINE
Parameters	.LINE description string
Command Mode	IP standard access-list terminal mode

No/clear no remark

Show Show running-config

Default

Description This command add a description to a specify ACL group.

Examples ASUS(config-std-nacl)# remark abc

13.66 access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>) remark .LINE

Syntax access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>) remark .LINE

Parameters .LINE string

Command Mode Configure terminal mode

No/clear no access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>) remark .LINE

no access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>) remark

Show Show acces-lists [number|name]

Default

Description This command is to add a description with a specify access-list number.

Examples ASUS(config)# access-list 22 remark asus

13.67 access-list (<1-99>|<1300-1999>) (deny|permit) IPADDR MASK [IFNAME]

Syntax access-list (<1-99>|<1300-1999>) (deny|permit) IPADDR A.B.C.D [IFNAME]

Parameters

Access-list	Add an access list entry
<1-99> ->	standard IP access-list number
<1300-1999> ->	standard IP access-list number (expanded range)
permit->	Specify packets to forward

	deny->	Specify packets to reject.
	IPADDR	Source address
	MASK	Source address mask
	[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<1-99>|<1300-1999>) (deny|permit) IPADDR MASK [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)# access-list 99 permit 1.1.1.1 0.255.255.0

13.68 access-list (<1-99>|<1300-1999>) (deny|permit) host IPADDR [IFNAME]

Syntax access-list (<1-99>|<1300-1999>) (deny|permit) host IPADDR [IFNAME]

Parameters	Access-list	Add an access list entry
	<1-99> ->	standard IP access-list number
	<1300-1999> ->	standard IP access-list number (expanded range)
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Host	A single host address
	IPADDR	Source address
	[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<1-99>|<1300-1999>) (deny|permit) host IPADDR [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)# access-list 99 permit host 1.1.1.1

13.69 access-list (<1-99>|<1300-1999>) (deny|permit) any [IFNAME]

Syntax access-list (<1-99>l<1300-1999>) (denylpermit) any [IFNAME]

Parameters

Access-list	Add an access list entry
<1-99> ->	standard IP access-list number
<1300-1999> ->	standard IP access-list number (expanded range)
permit->	Specify packets to forward
deny->	Specify packets to reject.
Any	Any source host
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<1-99>l<1300-1999>) (denylpermit) any [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)# access-list 99 permit any

13.70 access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) IPADDR MASK IPADDR MASK [IFNAME]

Syntax access-list (<100-199>l<2000-2699>) (denylpermit) (iplicpludplicmp) IPADDR MASK IPADDR MASK [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number

	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	IPADDR	Source address
	MASK	Source wildcard bits
	IPADDR	Destination address
	MASK	Destination wildcard bits
	[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>|<2000-2699>) (denylpermit) (ipltcpludplicmp) IPADDR MASK IPADDR MASK [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)# access-list 100 permit ip 1.1.1.1 0.0.0.0 1.1.1.3 0.0.0.0

13.71 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) IPADDR MASK [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]

Syntax access-list (<100-199>|<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]

Parameters	Access-list	Add an access list entry

<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
IPADDR	Source address
MASK	Source wildcard bits
eq	Match only packets on a given port numbe
<0-65535>	Port number
IPADDR	Destination address
MASK	Destination wildcard bits
eq	Match only packets on a given port numbe
<0-65535>	Port number
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) IPADDR MASK [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)# access-list 100 permit tcp 1.1.1.1 0.0.0.0 eq 21 1.1.1.3 0.0.0.0 eq 22

13.72 access-list (<100-199>|<2000-2699>) (deny|permit) icmp IPADDR MASK IPADDR MASK <0-255> code <0-255> [IFNAME]

Syntax access-list (<100-199>|<2000-2699>) (deny|permit) icmp

	IPADDR MASK IPADDR MASK <0-255> code <0-255> [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699>	Extended IP access-list number (expanded range)
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	IPADDR	Source address
	MASK	Source wildcard bits
	IPADDR	Destination address
	MASK	Destination wildcard bits
	<0-255>	ICMP message type
	<0-255>	ICMP message code
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) icmp IPADDR MASK IPADDR MASK <0-255> code <0-255> [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit icmp 1.1.1.1 0.0.0.0 1.1.1.3 0.0.0.0 22 code 3	

13.73 access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) IPADDR MASK any [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (iplticpludplicmp) IPADDR MASK any [IFNAME]

Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	IPADDR	Source address
	MASK	Source wildcard bits
	Any	Any destination host
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (ipltcpludplicmp) IPADDR MASK any [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit icmp 1.1.1.1 0.0.0.0 any	

13.74 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) IPADDR MASK [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number

	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	IPADDR	Source address
	MASK	Source wildcard bits
	Any	Any destination host
	[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>|<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]

Show Show acces-lists [numberlname]

Default

Description

This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit tcp 1.1.1.1 0.0.0.0 eq 23 any eq 22

13.75 access-list (<100-199>|<2000-2699>) (deny|permit) icmp IPADDR MASK any <0-255> code <0-255> [IFNAME]

Syntax access-list (<100-199>|<2000-2699>) (denylpermit) icmp IPADDR MASK any <0-255> code <0-255> [IFNAME]

Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward

	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	IPADDR	Source address
	MASK	Source wildcard bits
	Any	Any destination host
	<0-255>	ICMP message type
	<0-255>	ICMP message code
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) icmp IPADDR MASK any <0-255> code <0-255> [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit icmp 1.1.1.1 0.0.0.0 any 2 code 3	

13.76 access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) any IPADDR MASK [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (iplicpludplicmp) any IPADDR MASK [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol

	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	Any	Any Source host
	IPADDR	destination address
	MASK	destination wildcard bits
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (iplticpludplicmp) any IPADDR MASK [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit icmp any 1.1.1.1 0.0.0.0	

13.77 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) any [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Any	Any Source host
	eq	Match only packets on a given port numbe

	<0-65535>	Port number
	IPADDR	destination address
	MASK	destination wildcard bits
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) any [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit tcp any eq 21 1.1.1.1 0.0.0.0 eq 22

13.78 access-list (<100-199>|<2000-2699>) (deny|permit) icmp any IPADDR MASK <0-255> code <0-255> [IFNAME]

Syntax access-list (<100-199>l<2000-2699>) (denylpermit) icmp any IPADDR MASK <0-255> code <0-255> [IFNAME]

Parameters Access-list Add an access list entry

<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Ip ->	Any Internet Protocol
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
Icmp->	Internet Control Message Protocol

	Any	Any Source host
	IPADDR	destination address
	MASK	destination wildcard bits
	<0-255>	ICMP message type
	<0-255>	ICMP message code
	[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>|<2000-2699>) (deny|permit) icmp any IPADDR MASK <0-255> code <0-255> [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp any 1.1.1.1 0.0.0.0 2 code 3

13.79 access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) any any [IFNAME]

Syntax access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) any any [IFNAME]

Parameters		
	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	Any	Any Source host

	Any	Any destination host
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (ipltcpludplicmp) any any [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit icmp any any	

13.80 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) any [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Any	Any Source host
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	Any	Any destination host
	eq	Match only packets on a given port numbe
	<0-65535>	Port number

	[IFNAME]	Egress interface name
	Command Mode	Configure terminal mode
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) any [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit tcp any eq 21 any eq 22	

13.81 access-list (<100-199>|<2000-2699>) (deny|permit) icmp any any <0-255> code <0-255> [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) icmp any any <0-255> code <0-255> [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	Any	Any Source host
	Any	Any destination host
	<0-255>	ICMP message type
	<0-255>	ICMP message code
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) icmp any any <0-255> code <0-255> [IFNAME]	
Show	Show acces-lists [numberlname]	

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp any any 2 code 3

13.82 access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) IPADDR MASK host IPADDR [IFNAME]

Syntax access-list (<100-199>l<2000-2699>) (denylpermit) (ipltcpludplicmp) IPADDR MASK host IPADDR [IFNAME]

Parameters

	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	IPADDR	source address
	MASK	source wildcard bits
.	host	A single destination host
	IPADDR	Destination address
	[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>l<2000-2699>) (denylpermit) (ipltepludplicmp) IPADDR MASK host IPADDR [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp 1.1.1.1 0.0.0.0 host 1.1.1.4

13.83 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) IPADDR MASK [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]

Syntax access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
IPADDR	source address
MASK	source wildcard bits
eq	Match only packets on a given port numbe
<0-65535>	Port number
.host	A single destination host
IPADDR	Destination address
eq	Match only packets on a given port numbe
<0-65535>	Port number
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit udp 1.1.1.1 0.0.0.0 eq 21 host 1.1.1.4 eq 22

13.84 access-list (<100-199>|<2000-2699>) (deny|permit) icmp IPADDR MASK host IPADDR <0-255> code <0-255> [IFNAME]

Syntax access-list (<100-199>|<2000-2699>) (deny|permit) icmp IPADDR MASK host IPADDR <0-255> code <0-255> [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Icmp->	Internet Control Message Protocol
IPADDR	source address
MASK	source wildcard bits
host	A single destination host
IPADDR	Destination address
<0-255>	ICMP message type
<0-255>	ICMP message code
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>|<2000-2699>) (deny|permit) icmp IPADDR MASK host IPADDR <0-255> code <0-255> [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp 1.1.1.1 0.0.0.0 host 1.1.1.4 2 code 3

13.85 access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) host IPADDR IPADDR MASK [IFNAME]

Syntax access-list (<100-199>l<2000-2699>) (denylpermit) (ipltcpludplicmp) host IPADDR IPADDR MASK [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Ip ->	Any Internet Protocol
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
Icmp->	Internet Control Message Protocol
.host	A single Source host
IPADDR	Source address
IPADDR	destination address
MASK	destination wildcard bits
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>l<2000-2699>) (denylpermit) (ipltepludplicmp) host IPADDR IPADDR MASK [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or

permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp host 1.1.1.1 1.1.1.4 0.0.0.0

13.86 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host IPADDR [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]

Syntax access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
host	A single Source host
IPADDR	Source address
eq	Match only packets on a given port numbe
<0-65535>	Port number
IPADDR	destination address
MASK	destination wildcard bits
eq	Match only packets on a given port numbe
<0-65535>	Port number
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR [eq] [<0-65535>] IPADDR MASK [eq] [<0-65535>] [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit tcp host 1.1.1.1 eq 21 1.1.1.4 0.0.0.0 eq 22

13.87 access-list (<100-199>|<2000-2699>) (deny|permit) icmp host IPADDR IPADDR MASK <0-255> code <0-255> [IFNAME]

Syntax access-list (<100-199>l<2000-2699>) (denylpermit) icmp host IPADDR IPADDR MASK <0-255> code <0-255> [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Icmp->	Internet Control Message Protocol
host	A single Source host
IPADDR	Source address
IPADDR	destination address
MASK	destination wildcard bits
<0-255>	ICMP message type
<0-255>	ICMP message code
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>l<2000-2699>) (denylpermit) icmp host IPADDR IPADDR MASK <0-255> code <0-255> [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp host 1.1.1.1 1.1.1.4 0.0.0.0 2 code 3

13.88 access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) host IPADDR host IPADDR [IFNAME]

Syntax access-list (<100-199>l<2000-2699>) (denylpermit) (ipltcpludplicmp) host IPADDR host IPADDR [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Ip ->	Any Internet Protocol
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
Icmp->	Internet Control Message Protocol
.host	A single Source host
IPADDR	Source address
.host	A single destination host
IPADDR	Destination address
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>l<2000-2699>) (denylpermit) (ipltcpludplicmp) host IPADDR host IPADDR [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or

permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp host 1.1.1.1 host 1.1.1.4

13.89 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host IPADDR [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]

Syntax access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
.host	A single Source host
IPADDR	Source address
eq	Match only packets on a given port numbe
<0-65535>	Port number
.host	A single destination host
IPADDR	Destination address
eq	Match only packets on a given port numbe
<0-65535>	Port number
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp host 1.1.1.1 eq 21 host 1.1.1.4 eq 21

13.90 access-list (<100-199>|<2000-2699>) (deny|permit) icmp host IPADDR host IPADDR <0-255> code <0-255> [IFNAME]

Syntax access-list (<100-199>|<2000-2699>) (deny|permit) icmp host IPADDR host IPADDR <0-255> code <0-255> [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Icmp->	Internet Control Message Protocol
host	A single Source host
IPADDR	Source address
host	A single destination host
IPADDR	Destination address
<0-255>	ICMP message type
<0-255>	ICMP message code
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>|<2000-2699>) (deny|permit) icmp host IPADDR host IPADDR <0-255> code <0-255> [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp host 1.1.1.1 host 1.1.1.4 3 code 3

13.91 access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) any host IPADDR [IFNAME]

Syntax access-list (<100-199>l<2000-2699>) (denylpermit) (ipltcpludplicmp) any host IPADDR [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Ip ->	Any Internet Protocol
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
Icmp->	Internet Control Message Protocol
Any	Any Source host
.host	A single destination host
IPADDR	Destination address
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>l<2000-2699>) (denylpermit) (ipltcpludplicmp) any host IPADDR [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp any host 1.1.1.1

13.92 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]

Syntax access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) any [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
Any	Any Source host
eq	Match only packets on a given port numbe
<0-65535>	Port number
.host	A single destination host
IPADDR	Destination address
eq	Match only packets on a given port numbe
<0-65535>	Port number
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) any [eq] [<0-65535>] host IPADDR [eq] [<0-65535>] [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit tcp any eq 21 host 1.1.1.1 eq 22

13.93 access-list (<100-199>|<2000-2699>) (deny|permit) icmp any host IPADDR <0-255> code <0-255> [IFNAME]

Syntax access-list (<100-199>|<2000-2699>) (deny|permit) icmp any host IPADDR <0-255> code <0-255> [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Icmp->	Internet Control Message Protocol
Any	Any Source host
.host	A single destination host
IPADDR	Destination address
<0-255>	ICMP message type
<0-255>	ICMP message code
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>|<2000-2699>) (deny|permit) icmp any host IPADDR <0-255> code <0-255> [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp any host 1.1.1.1 2 code 3

13.94 access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) host IPADDR any [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (ipltcpludplicmp) host IPADDR any [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Ip ->	Any Internet Protocol
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Icmp->	Internet Control Message Protocol
	.host	A single Source host
	IPADDR	Source address
	Any	Any destination host
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (ipltepludplicmp) host IPADDR any [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit icmp host 1.1.1.1 any	

13.95 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host IPADDR [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	.host	A single Source host
	IPADDR	Source address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	Any	Any destination host
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR [eq] [<0-65535>] any [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit tcp host 1.1.1.1 eq 21 any eq 21	

13.96 access-list (<100-199>|<2000-2699>) (deny|permit) icmp host IPADDR any <0-255> code <0-255> [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) icmp host IPADDR any <0-255> code <0-255> [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	.host	A single Source host
	IPADDR	Source address
	Any	Any destination host
	<0-255>	ICMP message type
	<0-255>	ICMP message code
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) icmp host IPADDR any <0-255> code <0-255> [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit icmp host 1.1.1.1 any 2 code 2	

13.97 access-list (<1-99>|<1300-1999>) (deny|permit) IPADDR [IFNAME]

Syntax	access-list (<1-99>l<1300-1999>) (denylpermit) IPADDR [IFNAME]	
Parameters	Access-list	Add an access list entry
	<1-99>	Standard IP access-list number
	<2000-2699> range)	Standard IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	IPADDR	Source address
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<1-99>l<1300-1999>) (denylpermit) IPADDR [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 88 permit 10.0.0.1	

13.98 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) IPADDR MASK IPADDR MASK eq <0-65535> [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) IPADDR A.B.C.D IPADDR A.B.C.D eq <0-65535> [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded

	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	IPADDR	Source address
	MASK	Source wildcard bits
	IPADDR	Destination address
	MASK	Destination wildcard bits
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>|<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK IPADDR MASK eq <0-65535> [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit tcp 1.1.1.1 0.0.0.0 1.1.1.4 0.0.0.0 eq 21

13.99 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) IPADDR MASK [eq] [<0-65535>] IPADDR MASK [IFNAME]

Syntax access-list (<100-199>|<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK [eq] [<0-65535>] IPADDR MASK [IFNAME]

Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699>	Extended IP access-list number (expanded range)
	permit->	Specify packets to forward

	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	IPADDR	Source address
	MASK	Source wildcard bits
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	IPADDR	Destination address
	MASK	Destination wildcard bits
	[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>|<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK [eq] [<0-65535>] IPADDR MASK [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit tcp 1.1.1.1 0.0.0.0 eq 21 1.1.1.4 0.0.0.0

13.100 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) IPADDR MASK any [eq] [<0-65535>] [IFNAME]

Syntax access-list (<100-199>|<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK any [eq] [<0-65535>] [IFNAME]

Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.

	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	IPADDR	Source address
	MASK	Source wildcard bits
	Any	Any destination host
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK any [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit tcp 1.1.1.1 0.0.0.0 any eq 21	

13.101 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) IPADDR MASK [eq] [<0-65535>] any [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) IPADDR A.B.C.D [eq] [<0-65535>] any [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol

	IPADDR	Source address
	MASK	Source wildcard bits
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	Any	Any destination host
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK [eq] [<0-65535>] any [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit tcp 1.1.1.1 0.0.0.0 eq 21 any	

13.102 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) IPADDR MASK [eq] [<0-65535>] host IPADDR [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK [eq] [<0-65535>] host IPADDR [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	IPADDR	source address
	MASK	source wildcard bits

	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	.host	A single destination host
	IPADDR	Destination address
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK [eq] [<0-65535>] host IPADDR [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit tcp 1.1.1.1 0.0.0.0 eq 21 host 1.1.1.4	

13.103 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) IPADDR MASK host IPADDR [eq] [<0-65535>] [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK host IPADDR [eq] [<0-65535>] [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	IPADDR	source address
	MASK	source wildcard bits
.	host	A single destination host

	IPADDR	Destination address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) IPADDR MASK host IPADDR [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit tcp 1.1.1.1 0.0.0.0 host 1.1.1.4 eq 21	

13.104 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any IPADDR MASK [eq] [<0-65535>] [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) any IPADDR MASK [eq] [<0-65535>] [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Any	Any Source host
	IPADDR	destination address
	MASK	destination wildcard bits
	eq	Match only packets on a given port numbe

	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) any IPADDR MASK [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit tcp any 1.1.1.1 0.0.0.0 eq 21	

13.105 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any any [eq] [<0-65535>] [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) any any [eq] [<0-65535>] [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699>	Extended IP access-list number (expanded range)
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Any	Any Source host
	Any	Any destination host
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	

No/clear	no access-list (<100-199>|<2000-2699>) (denylpermit) (tcpludp) any any [eq] [<0-65535>] [IFNAME]
Show	Show acces-lists [numberlname]
Default	
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.
Examples	ASUS(config)#access-list 100 permit tcp any any eq 21

13.106 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any [eq] [<0-65535>] any [IFNAME]

Syntax	access-list (<100-199>|<2000-2699>) (denylpermit) (tcpludp) any [eq] [<0-65535>] any [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Any	Any Source host
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	Any	Any destination host
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>|<2000-2699>) (denylpermit) (tcpludp) any [eq] [<0-65535>] any [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit tcp any eq 21 any

13.107 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any [eq] [<0-65535>] IPADDR MASK [IFNAME]

Syntax access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) any [eq] [<0-65535>] IPADDR A.B.C.D [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
Any	Any Source host
eq	Match only packets on a given port numbe
<0-65535>	Port number
IPADDR	destination address
MASK	destination wildcard bits
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) any [eq] [<0-65535>] IPADDR MASK [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit tcp any eq 21 10.0.0.1 0.0.0.0

13.108 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any [eq] [<0-65535>] host IPADDR [IFNAME]

Syntax access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any [eq] [<0-65535>] host IPADDR [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
Any	Any Source host
eq	Match only packets on a given port numbe
<0-65535>	Port number
host	A single destination host
IPADDR	Destination address
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any [eq] [<0-65535>] host IPADDR [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit tcp any eq 21 host 10.0.0.1

13.109 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any host IPADDR [eq] [<0-65535>] [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) any host IPADDR [eq] [<0-65535>] [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	Any	Any Source host
	.host	A single destination host
	IPADDR	Destination address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) any host IPADDR [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit tcp any host 10.0.0.1 eq 21	

13.110 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host IPADDR IPADDR MASK [eq] [<0-65535>] [IFNAME]

Syntax access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host IPADDR IPADDR MASK [eq] [<0-65535>] [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699>	Extended IP access-list number (expanded range)
permit->	Specify packets to forward
deny->	Specify packets to reject.
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
.host	A single Source host
IPADDR	Source address
IPADDR	destination address
MASK	destination wildcard bits
eq	Match only packets on a given port numbe
<0-65535>	Port number
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host IPADDR IPADDR MASK [eq] [<0-65535>] [IFNAME]

Show Show acces-lists [number|name]

Default

Description

This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit tcp host 10.0.0.1 10.0.0.4 0.0.0.0 eq 21

13.111 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host IPADDR [eq] [<0-65535>] IPADDR MASK [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR [eq] [<0-65535>] IPADDR MASK [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
.	host	A single Source host
	IPADDR	Source address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	IPADDR	destination address
	MASK	destination wildcard bits
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR [eq] [<0-65535>] IPADDR MASK [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit tcp host 10.0.0.1 eq 21 10.0.0.4 0.0.0.0	

13.112 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host IPADDR any [eq] [<0-65535>] [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR any [eq] [<0-65535>] [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	.host	A single Source host
	IPADDR	Source address
	Any	Any destination host
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR any [eq] [<0-65535>] [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit tcp host 10.0.0.1 any eq 21	

13.113 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host IPADDR [eq] [<0-65535>] any [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR [eq] [<0-65535>] any [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	.host	A single Source host
	IPADDR	Source address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	Any	Any destination host
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR [eq] [<0-65535>] any [IFNAME]	
Show	Show acces-lists [numberlname]	
Default	Pass	
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit tcp host 10.0.0.1 eq 21 any	

13.114 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host IPADDR [eq] [<0-65535>] host IPADDR [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR [eq] [<0-65535>] host IPADDR [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Tcp->	Transmission Control Protocol
	Udp->	User Datagram Protocol
	.host	A single Source host
	IPADDR	Source address
	eq	Match only packets on a given port numbe
	<0-65535>	Port number
	.host	A single destination host
	IPADDR	Destination address
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR [eq] [<0-65535>] host IPADDR [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit tcp host 10.0.0.1 eq 21 host 10.0.0.4	

13.115 access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host IPADDR host IPADDR [eq] [<0-65535>] [IFNAME]

Syntax access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR host IPADDR [eq] [<0-65535>] [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Tcp->	Transmission Control Protocol
Udp->	User Datagram Protocol
.host	A single Source host
IPADDR	Source address
.host	A single destination host
IPADDR	Destination address
eq	Match only packets on a given port numbe
<0-65535>	Port number
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>l<2000-2699>) (denylpermit) (tcpludp) host IPADDR host IPADDR [eq] [<0-65535>] [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit tcp host 10.0.0.1 host 10.0.0.4 eq 21

13.116 access-list (<100-199>|<2000-2699>) (deny|permit) icmp IPADDR MASK IPADDR MASK <0-255> [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) icmp IPADDR MASK IPADDR MASK <0-255> [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	IPADDR	Source address
	MASK	Source wildcard bits
	IPADDR	Destination address
	MASK	Destination wildcard bits
	<0-255>	ICMP message type
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) icmp IPADDR MASK IPADDR MASK <0-255> [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit icmp 10.0.0.1 0.0.0.0 10.0.0.4 0.0.0.0 1	

13.117 access-list (<100-199>|<2000-2699>) (deny|permit) icmp IPADDR MASK any <0-255> [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) icmp IPADDR MASK any <0-255> [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	IPADDR	Source address
	MASK	Source wildcard bits
	Any	Any destination host
	<0-255>	ICMP message type
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) icmp IPADDR MASK any <0-255> [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit icmp 10.0.0.1 0.0.0.0 any 1	

13.118 access-list (<100-199>|<2000-2699>) (deny|permit) icmp any any <0-255> [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) icmp any any <0-255> [IFNAME]

Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699>	Extended IP access-list number (expanded range)
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	Any	Any Source host
	Any	Any destination host
	<0-255>	ICMP message type
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) icmp any any <0-255> [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit icmp any any 1	

13.119 access-list (<100-199>|<2000-2699>) (deny|permit) icmp IPADDR MASK host IPADDR <0-255> [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) icmp IPADDR MASK host IPADDR <0-255> [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699>	Extended IP access-list number (expanded range)
	permit->	Specify packets to forward
	deny->	Specify packets to reject.

	Icmp->	Internet Control Message Protocol
	IPADDR	source address
	MASK	source wildcard bits
	.host	A single destination host
	IPADDR	Destination address
	<0-255>	ICMP message type
	[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>|<2000-2699>) (deny|permit) icmp IPADDR MASK host IPADDR <0-255> [IFNAME]

Show Show acces-lists [number|name]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp 10.0.0.1 0.0.0.0 host 10.0.0.4 1

13.120 access-list (<100-199>|<2000-2699>) (deny|permit) icmp host IPADDR IPADDR MASK <0-255> [IFNAME]

Syntax access-list (<100-199>|<2000-2699>) (deny|permit) icmp host IPADDR IPADDR MASK <0-255> [IFNAME]

Parameters

	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699>	Extended IP access-list number (expanded range)
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	.host	A single Source host
	IPADDR	Source address

	IPADDR	destination address
	MASK	destination wildcard bits
	<0-255>	ICMP message type
	[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>|<2000-2699>) (denylpermit) icmp host IPADDR IPADDR MASK <0-255> [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp host 10.0.0.1 10.0.0.4 0.0.0.0 1

13.121 access-list (<100-199>|<2000-2699>) (deny|permit) icmp host IPADDR host IPADDR <0-255> [IFNAME]

Syntax access-list (<100-199>|<2000-2699>) (denylpermit) icmp host IPADDR host IPADDR <0-255> [IFNAME]

Parameters

	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699>	Extended IP access-list number (expanded range)
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	.host	A single Source host
	IPADDR	Source address
	.host	A single destination host
	IPADDR	Destination address
	<0-255>	ICMP message type

	[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>l<2000-2699>) (denylpermit) icmp host IPADDR host IPADDR <0-255> [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp host 10.0.0.1host 10.0.0.4 1

13.122 access-list (<100-199>|<2000-2699>) (deny|permit) icmp any host IPADDR <0-255> [IFNAME]

Syntax access-list (<100-199>l<2000-2699>) (denylpermit) icmp any host IPADDR <0-255> [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Icmp->	Internet Control Message Protocol
Any	Any Source host
.host	A single destination host
IPADDR	Destination address
<0-255>	ICMP message type
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>l<2000-2699>) (denylpermit) icmp any host IPADDR <0-255> [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp any host 10.0.0.1 1

13.123 access-list (<100-199>|<2000-2699>) (deny|permit) icmp host IPADDR any <0-255> [IFNAME]

Syntax access-list (<100-199>|<2000-2699>) (denylpermit) icmp host IPADDR any <0-255> [IFNAME]

Parameters

Access-list	Add an access list entry
<100-199>	Extended IP access-list number
<2000-2699> range)	Extended IP access-list number (expanded
permit->	Specify packets to forward
deny->	Specify packets to reject.
Icmp->	Internet Control Message Protocol
.host	A single Source host
IPADDR	Source address
Any	Any destination host
<0-255>	ICMP message type
[IFNAME]	Egress interface name

Command Mode Configure terminal mode

No/clear no access-list (<100-199>|<2000-2699>) (denylpermit) icmp host IPADDR any <0-255> [IFNAME]

Show Show acces-lists [numberlname]

Default

Description This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.

Examples ASUS(config)#access-list 100 permit icmp host 10.0.0.1 any 1

13.124 access-list (<100-199>|<2000-2699>) (deny|permit) icmp any IPADDR MASK <0-255> [IFNAME]

Syntax	access-list (<100-199>l<2000-2699>) (denylpermit) icmp any IPADDR MASK <0-255> [IFNAME]	
Parameters	Access-list	Add an access list entry
	<100-199>	Extended IP access-list number
	<2000-2699> range)	Extended IP access-list number (expanded
	permit->	Specify packets to forward
	deny->	Specify packets to reject.
	Icmp->	Internet Control Message Protocol
	Any	Any Source host
	IPADDR	destination address
	MASK	destination wildcard bits
	<0-255>	ICMP message type
	[IFNAME]	Egress interface name
Command Mode	Configure terminal mode	
No/clear	no access-list (<100-199>l<2000-2699>) (denylpermit) icmp any IPADDR MASK <0-255> [IFNAME]	
Show	Show acces-lists [numberlname]	
Default		
Description	This command specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.	
Examples	ASUS(config)#access-list 100 permit icmp any 10.0.0.1 0.0.0.0 1	

14. Port Security

14.1 show port-security

Syntax show port-security

Parameters

Command Mode Privileged EXEC mode

Default

Description To show port-security status.

Examples ASUS# show port-security

14.2 show port-security address [IFNAME]

Syntax show port-security address [IFNAME]

Parameters [IFNAME] Interface's name, ex: fastethernet1/0/1 or gigabitethernet1/0/26

Command Mode Privileged EXEC mode

Default

Description To show secure addresses of the port.

Examples ASUS# show port-security address fa1/0/1

14.3 show port-security interface [IFNAME]

Syntax show port-security interface [IFNAME]

Parameters [IFNAME] Interface's name, ex: fastethernet1/0/1 or gigabitethernet1/0/26

Command Mode Privileged EXEC mode

Default

Description To show port-security status of the port.

Examples ASUS# show port-security interface fa1/0/1

14.4 switch port-security

Syntax switch port-security

Parameters

Command Mode Interface mode

No/clear no switch port-security

Default Disable port security

Description To enable port-security of the port.

Examples ASUS(config-if)# switch port-security

14.5 switch port-security aging-time <0-1440>

Syntax switch port-security aging-time <0-1440>

Parameters <0-1440> aging time, 0 means no age.

Command Mode Interface mode

No/clear no switch port-security aging-time

Default Aging time is 0.

Description To enable port-security aging of the port.

Examples ASUS(config-if)# switch port-security aging-time 5

14.6 switch port-security aging-type (absolute|inactivity)

Syntax switch port-security aging-type (absolute|inactivity)

Parameters Absolute Absolute aging (default)

Inactivity Aging based on inactivity time period

Command Mode Interface mode

No/clear no switch port-security aging type

Default Absolute aging

Description To select port-security aging type of the port.

Examples ASUS(config-if)# switch port-security aging-type inactivity

14.7 switch port-security mac-address MACADDR

Syntax switch port-security mac-address MACADDR

Parameters MACADDR MAC address xxxx.xxxx.xxxx

Command Mode Interface mode

No/clear no switch port-security mac-address MACADDR

Default

Description To configure secure mac of the port.

Examples ASUS(config-if)# switch port-security mac-address 0011.2222.3344

14.8 switch port-security maximun <1-132>

Syntax switch port-security maximun <1-132>

Parameters <1-132> Number of addresses (default is 1).

Command Mode Interface mode

No/clear no switch port-security switch port-security maximun

Default Default is 1

Description To configure maximun secure mac addresses of the port.

Examples ASUS(config-if)# switch port-security maximum 5

14.9 switch port-security reup

Syntax switch port-security reup

Parameters

Command Mode Interface mode

No/clear

Default

Description To reup the port when it was shutdown by port security

Examples ASUS(config-if)# switch port-security reup

14.10 switch port-security shutdown <10-1440>

Syntax switch port-security shutdown <10-1440>

Parameters <10-1440> Interface maximum shutdown time

Command Mode Interface mode

No/clear	No switch port-security shutdown
Default	
Description	To configure maximum shutdown time
Examples	ASUS(config-if)# switch port-security shutdown 30

14.11 switch port-security violation (protect|restrict|shutdown)

Syntax	switch port-security violation (protect|restrict|shutdown)	
Parameters	protect	Protect mode, drop packets when security violation occurs
	restrict	Restrict mode, notify user when security violation occurs
	shutdown	Shutdown mode, shutdown this port when security violation occurs (default)
Command Mode	Interface mode	
No/clear	No switch port-security violation	
Default	Shutdown mode	
Description	To configure port security violation mode	
Examples	ASUS(config-if)# switch port-security violation restrict	

15. Interface configuration:

15.1 ingress filter (enable|disable)

Syntax	ingress filter (enable|disable)	
Parameters	filtering	filtering rules
	disable ->	disables 802.1Q ingress filtering feature
	enable ->	enables 802.1Q ingress filtering feature
Command Mode	Interface mode	

No/clear

Show show ingress filtering IFNAME

Default The default is disable

Description This command sets the 802.1Q ingress filtering features

Examples ASUS(config-if)#ingress filter enable

15.2 show ingress filter IFNAME

Syntax show ingress filter IFNAME

Parameters [IFNAME] Interface's name, ex: fastethernet1/0/1 or gigabitethernet1/0/26

Command Mode Privileged EXEC mode

Default

Description To show ingress filtering IFNAME status.

Examples ASUS# show ingress filter fa1/0/1

15.3 ip access-group (<1-199>|<1300-2699>|WORD) in

Syntax ip access-group (<1-199> I<1300-2699>IWORD) in

Parameters <1-199><1300-2699> lword filter id or name

Command Mode Interface mode

No/clear no ip access-group

Show show ingress filtering IFNAME

Default The default is disable

Description This command sets the 802.1Q ingress filtering features

Examples ASUS(config-if)#ip access-group 100 in

15.4 interface IFNAME

Syntax interface IFNAME

Parameters IFNAME: interface's name

Command Mode Configure terminal mode

No/clear no interface IFNAME

Show show interface IFNAME

Default

Description This command changes the operation to interface command mode.

Examples ASUS(config)#interface fa1/0/1

15.5 show interface IFNAME

Syntax Show interface IFNAME

Parameters IFNAME: interface's name

Command Mode Privileged EXEC mode

Default

Description This command shows the interface detail status.

Examples ASUS#show interface fa1/0/1

15.6 show interface status

Syntax Show interface status

Parameters

Command Mode Privileged EXEC mode

Default

Description This command shows the interface status.

Examples ASUS#show interface status

15.7 show interface stack <1-8>

Syntax show interface stack <1-8>

Parameters <1-8>: stack ID

Command Mode Privileged EXEC mode

Default

Description This command shows the interface detail status with specific stack .

Examples ASUS#show interface stack 1

15.8 interface vlanVLAN-ID

Syntax interface vlanVLAN-ID

Parameters

vlan	Select a vlan to configure
VLAN-ID	Vlan's id

Command Mode Configure terminal mode

No/clear

Show show vlan[VLANID]

Default

Description This command changes the system vlan to specific vlan interface command mode.

Examples ASUS(config)#interface vlan1

15.9 ip address A.B.C.D/M

Syntax ip address A.B.C.D/M

Parameters

address	Set the IP address of an interface
A.B.C.D/M	IP address (e.g. 10.0.0.1/8)

Command Mode L3 Interface mode

No/clear no ip address A.B.C.D/M

Show show running-config

Default

Description This command sets the ip address for indicated interface.

Examples ASUS(config-if)# ip address 192.192.1.11/24

15.10 acceptable frame-type

Syntax acceptable frame-type (alll discardalll vlan-tagged-only)

Parameters

all ->	any kind of frame type is accepted

	discardall ->	discard all frame is accepted
	vlan-tagged-only ->	only vlan-tag frame is accepted
Command Mode	Interface mode	
No/clear		
show	show interface IFNAME	
Default	None or depends on ODM customer	
Description	Use the acceptable frame type configuration command on the switch stack or standalone switch to set the type of the acceptable	
	frame, for any kind of frame type is accepted or only vlan-tag frame is accepted.	
Examples	ASUS(config-if)#acceptable frame-type all	

15.11 duplex (full|half)

Syntax	duplex (fulllhalf)	
Parameters	full ->	Port is in half-duplex mode
	half ->	Port is in full-duplex mode
Command Mode	Interface mode	
No/clear	no duplex	
Show	show interface IFNAME	
Default	The default is Full	
Description	Use the duplex interface configuration command on the switch stack or on a standalone switch to specify the duplex mode of operation for Fast Ethernet and Gigabit Ethernet ports. Use the no form of this command to return the port to its default value.	
Examples	ASUS(config-if)# duplex full	

15.12 flowcontrol (rx|tx|both) (on|off)

Syntax	flowcontrol (receivelsendlboth) (onloff)	
Parameters	rx ->	sets whether the interface can receive flow-control packets from a remote device

tx -> sets whether the interface can send flow-control packets to a remote device

both -> sets whether the interface can receive and send flow-control packets from a remote device

off -> disable an interface to operate with an attached device that is required to send or receive flow-control packets

on -> allows an interface to operate with an attached device that is required to send or receive flow-control packets

Command Mode Interface mode

No/clear No flowcontrol

Show show interface IFNAME

Default receive on, send on

Description This command sets the interface flowcontrol method.

Examples ASUS(config-if)# flowcontrol both on

15.13 auto-negotiation

Syntax auto-negotiation

Parameters

Command Mode Interface mode

No/clear no auto-negotiation

Show show l2_interface IFNAME

Default None or depends on ODM customer

Description Use the auto-negotiation configuration command on the switch stack or standalone switch to set auto-negotiation status of the port.

Examples ASUS(config-if)# auto-negotiation

15.14 speed (10|100|1000)

Syntax speed (10|100|1000)

Parameters

Command Mode Interface mode

No/clear no speed

Show show l2_interface IFNAME

Default None or depends on ODM customer

Description Use the speed configuration command on the switch stack or standalone switch to set speed status of the port.

Examples ASUS(config-if)#speed 100

15.15 shutdown

Syntax shutdown

Parameters

Command Mode Interface configuration

No/clear no shutdown

Show show running-config

Default

Description The shutdown command for a port causes it to stop forwarding. You can enable the port with the no shutdown command.

The no shutdown command has no effect if the port is a static-access port assigned to a VLAN that has been deleted, suspended, or shut down. The port must first be a member of an active VLAN before it can be re-enabled.

Only one management VLAN interface can be active at a time. The remaining VLANs are shut down.

In the show running-config command, the active management VLAN interface is the one without the shutdown command displayed.

Examples ASUS(config-if)# shutdown

15.16 default-priority <0-7>

Syntax default-priority <0-7>

Parameters <0-7> Cos priority

Command Mode Interface mode

No/clear	no default-priority
Show	
Default	None or depends on ODM customer
Description	Use the default_priority configuration command on the switch stack or standalone switch to set cos priority of the port.
Examples	ASUS(config-if)# default-priority 3

15.17 mdix

Syntax	mdix
Parameters	
Command Mode	Interface mode
No/clear	no mdix
Show	
Default	None or depends on ODM customer
Description	Use the mdix command on the switch stack or standalone switch to set mdix of the port.
Examples	ASUS(config-if)#mdix

15.18 description .LINE

Syntax	description .LINE
Parameters	String
Command Mode	Interface mode
No/clear	no description
Show	
Default	None or depends on ODM customer
Description	Use the description command on the switch stack or standalone switch to set description of the port.
Examples	ASUS(config-if)#description rd10

15.19 line loopback

Syntax Line loopback

Parameters

Command Mode Interface mode

No/clear no line loopback

Show

Default Enable or depends on ODM customer

Description Use the line loopback command on the switch stack or standalone switch to detect loopback of the port.

Examples ASUS(config-if)#no line loopback

16. DHCP Client:

16.1 ip dhcp client

Syntax ip dhcp client

Parameters

Command Mode Interface mode

Default

Description Start dhcp client

Examples ASUS(config-if)#ip dhcp client

16.2 no ip dhcp client

Syntax no ip dhcp client

Parameters

Command Mode Interface mode

Default

Description Stop dhcp client

Examples ASUS(config-if)# no ip dhcp client

16.3 ip dhcp client renew

Syntax ip dhcp client renew

Parameters

Command Mode Interface mode

Default

Description To get the dhcp ip again

Examples ASUS(config-if)# ip dhcp client renew

17. DHCP Snooping:

17.1 ip dhcp snooping

Syntax ip dhcp snooping

Parameters

Command Mode Configure Terminal Mode

No/clear no ip dhcp snooping

show show ip dhcp snooping

Default

Description Enable dhcp snooping globally.

Examples ASUS(config)# ip dhcp snooping

17.2 ip dhcp snooping vlan VLAN

Syntax ip dhcp snooping vlan VLAN

Parameters VLAN Range

Command Mode Configure Terminal Mode

No/clear no ip dhcp snooping vlan VLAN

show show ip dhcp snooping

Default

Description	Enable DHCP snooping on a VLAN or range of VLANs. The range is 1 to 3000. You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.
Examples	ASUS(config)# ip dhcp snooping vlan 1-100

17.3 ip dhcp snooping trust

Syntax	ip dhcp snooping trust
Parameters	
Command Mode	Interface Mode
No/clear	no ip dhcp snooping trust
show	show ip dhcp snooping
Default	
Description	(Optional) Configure the interface as trusted or untrusted. You can use the no keyword to configure an interface to receive messages from an untrusted client. The default is untrusted.
Examples	ASUS(config-if)# ip dhcp snooping trust

17.4 show ip dhcp snooping

Syntax	show ip dhcp snooping
Parameters	
Command Mode	Enable Mode
No/clear	
show	
Default	
Description	DHCP snooping configuration is displayed
Examples	ASUS#show ip dhcp snooping

17.5 show ip dhcp snooping binding

Syntax	show ip dhcp snooping binding
Parameters	
Command Mode	Enable Mode
No/clear	
show	
Default	
Description	To display logged information, If “binding” is given, snooped DHCP bindings are displayed.
Examples	ASUS#show ip dhcp snooping binding

18. IP Route:

18.1 ip forwarding

Syntax	ip forwarding	
Parameters	forwarding	Turn on IP forwarding
Command Mode	Configure terminal mode	
No/clear	no ip forwarding	
Show	show ip forwarding	
Default	IP forwarding is default on	
Description	This command will turn on IP forwarding function	
Examples	ASUS(config)#ip forwarding	

18.2 ip route A.B.C.D A.B.C.D (A.B.C.D|INTERFACE)

Syntax	ip route A.B.C.D A.B.C.D (A.B.C.DIINTERFACE)	
Parameters	route	Establish static routes
	A.B.C.D	IP destination prefix

	A.B.C.D	IP destination prefix mask
	A.B.C.D	IP gateway address
	INTERFACE	IP gateway interface name
Command Mode	Configure terminal mode	
No/clear	no ip route A.B.C.D A.B.C.D (A.B.C.DIINTERFACE)	
Show	show ip route	
	show ip route A.B.C.D	
	show running-config	
Default		
Description	This command sets the ip route in this system	
Examples	ASUS(config)#ip route 192.192.1.254 255.255.255.0	

18.3 ip route A.B.C.D A.B.C.D (A.B.C.D|INTERFACE) <1-255>

Syntax	ip route A.B.C.D A.B.C.D (A.B.C.DIINTERFACE) <1-255>	
Parameters	route	Establish static routes
	A.B.C.D	IP destination prefix
	A.B.C.D	IP destination prefix mask
	A.B.C.D	IP gateway address
	INTERFACE	IP gateway interface name
	<1-255>	Distance value for this route
Command Mode	Configure terminal mode	
No/clear	no ip route A.B.C.D A.B.C.D (A.B.C.DIINTERFACE) <1-255>	
Show	show ip route	
	show running-config	
Default		
Description	This command sets the ip route in this system with distance value for this route.	
Examples	ASUS(config)#ip route 192.192.1.254 255.255.255 10	

18.4 ip route A.B.C.D/M (A.B.C.D|INTERFACE)

Syntax	ip route A.B.C.D/M (A.B.C.DIINTERFACE)	
Parameters	route	Establish static routes
	A.B.C.D/M	IP destination prefix (e.g. 10.0.0.0/8)
	A.B.C.D	IP gateway address
	INTERFACE	IP gateway interface name
Command Mode	Configure terminal mode	
No/clear	no ip route A.B.C.D/M (A.B.C.DIINTERFACE)	
Show	show ip route	
	show ip route A.B.C.D/M	
	show running-config	
Default		
Description	This command sets the ip route in this system	
Examples	ASUS(config)#ip route 192.192.1.254/24	

18.5 ip route A.B.C.D/M (A.B.C.D|INTERFACE) <1-255>

Syntax	ip route A.B.C.D/M (A.B.C.DIINTERFACE) <1-255>	
Parameters	route	Establish static routes
	A.B.C.D/M	IP destination prefix (e.g. 10.0.0.0/8)
	A.B.C.D	IP gateway address
	INTERFACE	IP gateway interface name
	<1-255>	Distance value for this route
Command Mode	Configure terminal mode	
No/clear	no ip route A.B.C.D/M (A.B.C.DIINTERFACE) <1-255>	
Show	show ip route	
	show running-config	
Default		
Description	This command sets the ip route in this system with distance	

value for this route

Examples ASUS(config)#ip route 192.192.1.254/24 10

18.6 show ip route supernets-only

Syntax show ip route supernets-only

Parameters

Command Mode Privileged EXEC mode

No/clear

Default

Description

Examples ASUS# show ip route supernets-only

19. System Management:

19.1 show switch

GX2024M stacking only

Syntax show switch

Parameters

Command Mode Privileged EXEC mode

No/clear

Show

Default None or depends on ODM customer

Description Show stacking information

Examples ASUS# show switch

19.2 show switch status

GX2024M stacking only

Syntax show switch status

Parameters

Command Mode Privileged EXEC mode

No/clear

Show

Default None or depends on ODM customer

Description Show stacking information

Examples ASUS# show switch status

19.3 switch <1-8>

GX2024M stacking only

Syntax switch <1-8>

Parameters <1-8> stack id

Command Mode Configure terminal mode

No/clear

Default

Description To configure the stack id the switch belong to.

Examples ASUS(config)# switch 3

19.4 switch priority <1-8>

GX2024M stacking only

Syntax Switch priority <1-8>

Parameters <1-8> priority value

Command Mode Configure terminal mode

No/clear

Default

Description To configure the priority the switch belong to. highest priority will be elected as master

Examples ASUS(config)# switch priority 3

19.5 archive download-sw /overwrite tftp: IMAGE

Syntax archive download-sw /overwrite tftp: IMAGE

Parameters IMAGE Image file

Command Mode Privileged EXEC mode

No/clear

Show

Default None or depends on ODM customer

Description Use the archive download-sw /overwrite configuration command on the switch stack or standalone switch to download a new copy of software from a server and overwrite an existing image.

Examples ASUS# archive download-sw /overwrite tftp:192.192.1.131/ image.img

19.6 configure terminal

Syntax configure terminal

Parameters terminal Configuration terminal

Command Mode Privileged EXEC mode

No/clear

Show

Default None or depends on ODM customer

Description Use the write configuration command on the switch stack or standalone switch to configuration from vty interface.

Examples ASUS# configure terminal

19.7 copy running-config startup-config

Syntax copy running-config startup-config

Parameters running-config Copy from current system configuration

startup-config Copy from startup configuration

Command Mode Privileged EXEC mode

No/clear

Show

Default None or depends on ODM customer

Description Use the copy configuration command on the switch stack or standalone switch to copy running configuration startup-config.

Examples ASUS# copy running-config startup-config

19.8 copy startup-config tftp: URL

Syntax copy startup-config tftp: URL

Parameters

startup-config	Copy from startup configuration
ftp:	Copy to tftp: file system
URL	A URL beginning with this prefix

Command Mode Privileged EXEC mode

No/clear

Show

Default None or depends on ODM customer

Description Copy the file in Flash memory to the root directory of the TFTP server.

Examples ASUS# copy startup-config tftp: 192.192.1.131

19.9 copy tftp: URL startup-config

Syntax copy tftp: URL startup-config

Parameters

ftp:	Copy to tftp: file system
URL	A URL beginning with this prefix
startup-config	Copy from startup configuration

Command Mode Privileged EXEC mode

No/clear

Show

Default None or depends on ODM customer

Description Copy the file in the TFTP server to the Flash memory.

Examples ASUS# copy tftp: 192.192.1.31 startup-config

19.10 disable

Syntax disable

Parameters

Command Mode Privileged EXEC mode

No/clear

Show

Default

Description This command turn off privileged mode and back to user mode

Examples ASUS#disable

19.11 enable

Syntax enable

Parameters

Command Mode User mode

No/clear

Show

Default

Description This command let user enter enable mode and turn on privileged mode command.

Examples ASUS>enable

19.12 end

Syntax end

Parameters

Command Mode Privileged EXEC mode , Configure terminal mode, Interface mode

No/clear

Show

Default

Description This command let user end current mode and down to enable mode.

Examples ASUS(config)#end

19.13 exit

Syntax exit

Parameters

Command Mode User mode, Privileged EXEC mode , Configure terminal mode, Interface mode

No/clear

Show

Default

Description This command let user exit current mode and down to previous mode.

Examples ASUS(config)#exit

19.14 hostname WORD

Syntax hostname WORD

Parameters WORD: This system's network name

Command Mode Configure terminal mode

No/clear No hostname [HOSTNAME]

Show show running-config

Default The default system's network name is Switch

Description This command sets the system's network name

Examples ASUS(config)#hostname ASUS

19.15 list

Syntax list

Parameters

Command Mode User mode, Privileged EXEC mode, Configure terminal mode, Interface mode

No/clear

Show

Default

Description This command lists all of the command of the operation mode.

Examples ASUS#list

19.16 tracelog add (dhcp-snooping|dot1x|gvrp|igmp-snooping|lacp|stp)

Syntax tracelog add (dhcp-snooping|dot1x|gvrp|igmp-snooping|lacp|stp)

Parameters

Command Mode Configure terminal mode

No/clear tracelog delete (dhcp-snooping|dot1x|gvrp|igmp-snooping|lacp|stp)

Show

Default Disable tracelog

Description This command starts the system logging the function.

Examples ASUS(config)#tracelog add dot1x

19.17 tracelog level (critical | high | low)

Syntax tracelog level (critical | high | low)

Parameters

Command Mode Configure terminal mode

No/clear

Show

Default The default is critical

Description This command is to decide how much message will be print.

Examples ASUS(config)#tracelog level low

19.18 ping ip WORD

Syntax	ping ip WORD
Parameters	WORD Ping destination address or hostname
Command Mode	Privileged EXEC mode
No/clear	
Show	
Default	Enable
Description	This command used to send echo messages to ping destination address or hostname
Examples	ASUS#ping ip 192.192.1.1

19.19 ping WORD

Syntax	ping WORD
Parameters	WORD Ping destination address or hostname
Command Mode	Privileged EXEC mode
No/clear	
Show	
Default	Enable
Description	This command used to send echo messages to ping destination address or hostname
Examples	ASUS#ping 192.192.1.1

19.20 quit

Syntax	quit
Parameters	
Command Mode	User mode, Privileged EXEC mode
No/clear	
Show	
Default	None or depends on ODM customer

Description Use the command to exit current mode and down to previous mode.

Examples ASUS#quit

19.21 reboot

Syntax reboot

Parameters

Command Mode Privileged EXEC mode

No/clear

Show

Default None or depends on ODM customer

Description Use this command to reboot the system.

Examples ASUS#reboot

19.22 reload default-config file

Syntax reload default-config file

Parameters default-config the default-config file

file the running-config file

Command Mode Privileged EXEC mode

No/clear

Show

Default None or depends on ODM customer

Description Use this command to copy a default-config file to replace the current one

Examples ASUS# reload default-config file

19.23 show running-config

Syntax show running-config

Parameters running-config Current operating configuration

Command Mode Privileged EXEC mode

Default

Description To show running-config fule.

Examples ASUS# show running-config

19.24 show startup-config

Syntax show startup-config

Parameters startup-config Contentes of startup configuration

Command Mode Privileged EXEC mode

Default

Description To show startup-config.

Examples ASUS# show startup-config

19.25 show version

Syntax show version

Parameters version Displays ISS version

Command Mode Privileged EXEC mode

Default

Description To show firmware version.

Examples ASUS# show version

19.26 show cable-diagnostic interface [IFNAME]

Syntax show cable-diagnostic interface [IFNAME]

Parameters IFNAME interface name (e.q.: fastethernet1/0/1)

Command Mode Privileged EXEC mode

No/clear

Default

Description To show cable-diagnostic information

Examples ASUS# show cable-diagnostic interface

19.27 show private health

Syntax show private health

Parameters

Command Mode Privileged EXEC mode

No/clear

Default

Description To show system monitor information

Examples ASUS# show private health

19.28 show private led

Syntax show private led

Parameters

Command Mode Privileged EXEC mode

No/clear

Default

Description To show system led information

Examples ASUS# show private led

19.29 show private model

Syntax show private model

Parameters

Command Mode Privileged EXEC mode

No/clear

Default

Description To show model name

Examples ASUS# show private model

19.30 show uptime

Syntax	show uptime
Parameters	
Command Mode	Privileged EXEC mode
No/clear	
Default	
Description	To display system uptime
Examples	ASUS# show uptime

19.31 show clock

Syntax	show clock
Parameters	
Command Mode	Privileged EXEC mode
No/clear	
Default	
Description	To show clock
Examples	ASUS# show clock

19.32 clock set TIME MONTH DAY YEAR

Syntax	clock set TIME MONTH DAY YEAR	
Parameters	TIME	hh:mm:ss Current Time
	MONTH	<1-12> Month of the year
	DAY	<1-31> Day of the month
	YEAR	<1970-2037> Year
Command Mode	Privileged EXEC mode	
No/clear		
Default		
Description	To set time	
Examples	ASUS# clock set 15:26:02 4 6 2006	

19.33 show syslog

Syntax show syslog

Parameters

Command Mode Privileged EXEC mode

No/clear

Default

Description To show system log messages

Examples ASUS# show syslog

19.34 show syslog configuration

Syntax show syslog configuration

Parameters

Command Mode Privileged EXEC mode

No/clear

Default

Description To show system log configuration

Examples ASUS# show syslog configuration

19.35 syslog (enable|disable)

Syntax syslog (enable|disable)

Parameters

disable	Disable syslog protocol
enable	Enable syslog protocol

Command Mode Configure terminal mode

No/clear

Default

Description To enable/disable system log protocol

Examples ASUS(config)# syslog enable

19.36 syslog facility <0-23>

Syntax	syslog facility <0-23>	
Parameters	facility	Assign message facility
	<0-23>	Facility code
Command Mode	Configure terminal mode	
No/clear		
Default		
Description	To configure system log Facility code	
Examples	ASUS(config)# syslog facility 3	

19.37 syslog hostname

Syntax	syslog hostname
Parameters	
Command Mode	Configure terminal mode
No/clear	
Default	
Description	Turn on message hostname
Examples	ASUS(config)# syslog hostname

19.38 syslog server-ip A.B.C.D

Syntax	syslog server-ip A.B.C.D	
Parameters	A.B.C.D	IP address
Command Mode	Configure terminal mode	
No/clear		
Default		
Description	To configure Syslog server IP address	
Examples	ASUS(config)# syslog server-ip 192.168.1.1	

19.39 syslog severity <0-7>

Syntax syslog severity <0-7>

Parameters <0-7> Severity code

Command Mode Configure terminal mode

No/clear

Default

Description Assign message priority

Examples ASUS(config)# syslog severity 2

19.40 syslog timestamp

Syntax syslog timestamp

Parameters

Command Mode Configure terminal mode

No/clear

Default

Description Turn on message timestamp

Examples ASUS(config)# syslog timestamp

19.41 telnet WORD

Syntax telnet WORD

Parameters WORD IP address or hostname of a remote system

Command Mode User mode, Privileged EXEC mode

No/clear

Show

Default None or depends on ODM customer

Description to telnet a ip address

Examples ASUS# telnet 192.192.1.11

19.42 telnet WORD PORT

Syntax	telnet WORD PORT	
Parameters	WORD	IP address or hostname of a remote system
	PORT	TCP Port number
Command Mode	User mode, Privileged EXEC mode	
No/clear		
Show		
Default	None or depends on ODM customer	
Description	to telnet a ip address	
Examples	ASUS# telnet 192.192.1.11 21	

19.43 traceroute WORD

Syntax	traceroute WORD	
Parameters	WORD	Trace route to destination address or hostname
Command Mode	User mode, Privileged EXEC mode	
No/clear		
Show		
Default	None or depends on ODM customer	
Description		
Examples	ASUS# traceroute 192.192.1.11	

19.44 write

Syntax	write
Parameters	
Command Mode	Privileged EXEC mode
No/clear	
Show	
Default	None or depends on ODM customer

Description Use the write configuration command on the switch stack or standalone switch to write running configuration to memory, network, or terminal

Examples ASUS#write

19.45 show arp

Syntax show arp

Parameters

Command Mode Privileged EXEC mode

Default

Description To show arp table.

Examples ASUS#show arp

19.46 no arp A.B.C.D

Syntax no arp A.B.C.D

Parameters

Command Mode Privileged EXEC mode

Default

Description To delete arp table.

Examples ASUS#no arp 10.0.0.1

19.47 user add ACCOUNT PASSWORD

Syntax user add ACCOUNT PASSWORD

Parameters

ACCOUNT	user name
PASSWORD	password

Command Mode Configure terminal mode

Default

Description To add a new user account

Examples ASUS# user add test test

19.48 user delete USERNAME

Syntax user delete USERNAME

Parameters ACCOUNT user name

Command Mode Privileged EXEC mode

Default

Description To delete a user account

Examples ASUS# user delete test

19.49 show user

Syntax show user

Parameters ACCOUNT user name

Command Mode Privileged EXEC mode

Default

Description To show a user account

Examples ASUS# show user