01. ACL

1.1. ACL

ACL (Access Control List,) - IP-, , . **ACL** .

Access-list - . . , , , IP-, IP- , IP TCP, UDP.

:

- : **IP ACL** (3), **MAC ACL** (2) **MAC-IP ACL** (2 3).
- : (standard) (extended), .
- : .

ACL .

Access-group - **ACL** . , **ACL**.

ACL : **«» (permit) «» (deny)**. **Access-list** . , , , . , **ACL** , , .

1.2. ACL

1. Access-list:
    a. standard IP access-list;
    b. extended IP access-list;
    c. standard IP access-list:
        i. standard IP access-list;
        ii. permit \ deny ;
    d. extended IP access-list;
        i. extended IP access-list;
        ii. permit \ deny ;
    e. standard MAC access-list;
    f. extended MAC access-list;
    g. extended MAC access-list:
        i. extended MAC access-list;
        ii. permit \ deny ;
    h. extended MAC-IP access-list;
    i. extended MAC-IP access-list;
        i. extended MAC-IP access-list;
        ii. permit \ deny ;
    j. standard IPv6 access-list;
    k. standard IPv6 access-list;
        i. standard IPv6 access-list;
        ii. permit \ deny ;
2.
3.
4. access-group
5. ACL

1. Access-list:
    a. standard IP access-list;

access-list <num> {deny | permit} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} no access-list <num> **!**	standard IP access-list <num>, access-list , ACL. ACL <num>

b. extended IP access-list;

access-list <num> {deny | permit} icmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>][time-range<time-range-name>] **!**	ICMP extended IP access-list. ACL , .
access-list <num> {deny | permit} igmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>][time-range<time-range-name>] **!**	IGMP extended IP access-list. ACL , .
access-list <num> {deny | permit} tcp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} [s-port {<sPort> | range <sPortMin> <sPortMax>}] {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [d-port {<dPort> | range <dPortMin> <dPortMax>}] [ack+fin+psh+rst+urg+syn] [precedence <prec>] [tos <tos>][time-range<time-range-name>] **!**	TCP extended IP access-list. ACL , .
access-list <num> {deny | permit} udp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} [s-port {<sPort> | range <sPortMin> <sPortMax>}] {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [d-port {<dPort> | range <dPortMin> <dPortMax>}] [precedence <prec>] [tos <tos>][time-range<time-range-name>] **!**	UDP extended IP access-list. ACL , .
access-list <num> {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <protocol-num>} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [precedence <prec>] [tos <tos>][time-range<time-range-name>] **!**	, IP extended IP access-list. ACL , .
no access-list <num> **!**	ACL

c. standard IP access-list:

i. standard IP access-list

ip access-list standard <name> no ip access-list standard <name> **!**	standard IP access-list <name>, access-list , ACL. ACL <name>. ACL <name>

ii. permit \ deny ;

[no] {deny | permit} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} **! ACL**	ACL. [no] .

d. extended IP access-list;

i. extended IP access-list;

ip access-list extended <name> no ip access-list extended <name> **!**	extended IP access-list <name>, ACL <name>. ACL <name>

ii. permit \ deny ;

[no] {deny | permit} icmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>] [time-range<time-range-name>] **! ACL**	ICMP ACL. **[no]** .
[no] {deny | permit} igmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>][time-range<time-range-name>] **! ACL**	IGMP ACL. [no] .
[no] {deny | permit} tcp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} [s-port {<sPort> | range <sPortMin> <sPortMax>}] {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [d-port {<dPort> | range <dPortMin> <dPortMax>}] [ack+fin+psh+rst+urg+syn] [precedence <prec>] [tos <tos>][time-range<time-range-name>] **! ACL**	TCP ACL. [no] .
[no] {deny | permit} udp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} [s-port {<sPort> | range <sPortMin> <sPortMax>}] {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [d-port {<dPort> | range <dPortMin> <dPortMax>}] [precedence <prec>] [tos <tos>][time-range<time-range-name>] **! ACL**	UDP ACL. [no] .
[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <protocol-num>} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [precedence <prec>] [tos <tos>][time-range<time-range-name>] **! ACL**	, IP ACL. [no] .

e. standard MAC access-list;

access-list<num>{deny|permit}{any-source-mac|{host-source-mac<host_smac>}| {<smac><smac-mask>}} no access-list <num> **!**	standard MAC access-list <num>, access-list , ACL. ACL <num>

f. extended MAC access-list;

access-list<num> {deny|permit} {any-source-mac| {host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac<host_dmac>}|{<dmac><dmac-mask>}}[untagged-eth2 | tagged-eth2 | untagged-802-3 | tagged-802-3] no access-list <num> **!**	extended MAC access-list <num>, access-list , ACL. ACL <num>

g. extended MAC access-list:

i. extended MAC access-list;

mac-access-list extended <name> no mac-access-list extended <name> **!**	extended MAC access-list <name>, ACL <name>. ACL <name>

ii. permit \ deny ;

[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>} |{<dmac> <dmac-mask>}} [cos <cos-val> [<cos-bitmask>] [vlanId <vid-value> [<vid-mask>] [ethertype<protocol>[<protocol-mask>]]]] **! ACL**	extended MAC ACL Cos 802.1p Vlanid. [no] .
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac<host_dmac>}|{<dmac><dmac-mask>}}[untagged-eth2 [ethertype <protocol> [protocol-mask]]] **! ACL**	extended MAC ACL ethernet 2 vlan. [no] .
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}} [untagged-802-3] **! ACL**	extended MAC ACL 802.3 vlan. [no] .
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac<host_dmac>}|{<dmac><dmac-mask>}}[tagged-eth2 [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]] [ethertype<protocol> [<protocol-mask>]]] **! ACL**	extended MAC ACL ethernet 2 vlan. [no] .
[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac<host_dmac>}|{<dmac><dmac-mask>}} [tagged-802-3 [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]]] **! ACL**	extended MAC ACL 802.3 c vlan. [no] .

h. extended MAC-IP access-list;

access-list<num>{deny|permit} {any-source-mac| {host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac><dmac-mask>}} icmp {{<source> <source-wildcard>} |any-source| {host-source <source-host-ip>}} {{<destination> <destination-wildcard>} | any-destination | {host-destination <destination-host-ip>}} [<icmp-type> [<icmp-code>]] [precedence <precedence>] [tos <tos>] [time-range <time-range-name>] **!**	MAC-ICMP extended MAC-IP ACL. ACL , .
access-list<num>{deny|permit}{any-source-mac| {host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}igmp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} {{<destination><destination-wildcard>}|any-destination| {host-destination<destination-host-ip>}} [<igmp-type>] [precedence <precedence>] [tos <tos>][time-range<time-range-name>] **!**	MAC-IGMP extended MAC-IP ACL. ACL , .
access-list<num>{deny|permit}{any-source-mac| {host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}tcp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} [s-port {<port1> | range <sPortMin> <sPortMax>}] {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [d-port {<port3> | range <dPortMin> <dPortMax>}] [ack+fin+psh+rst+urg+syn] [precedence <precedence>] [tos <tos>][time-range<time-range-name>] **!**	MAC-TCP extended MAC-IP ACL. ACL , .

access-list<num>{deny|permit}{any-source-mac| {host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}udp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} [s-port {<port1> | range <sPortMin> <sPortMax>}] {{<destination><destination-wildcard>}|any-destination| {host-destination<destination-host-ip>}} [d-port {<port3> | range <dPortMin> <dPortMax>}] [precedence <precedence>] [tos <tos>][time-range<time-range-name>] **!**	MAC-UDP extended MAC-IP ACL. ACL , .
access-list<num>{deny|permit}{any-source-mac| {host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}} {eigrp|gre|igrp|ip|ipinip|ospf|{<protocol-num>}} {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} {{<destination><destination-wildcard>}|any-destination| {host-destination<destination-host-ip>}} [precedence <precedence>] [tos <tos>][time-range<time-range-name>] **!**	, IP extended MAC-IP ACL. ACL , .
no access-list <num> **!**	ACL

i. extended MAC-IP access-list;

i. extended MAC-IP access-list;

mac-ip-access-list extended <name> no mac-ip-access-list extended <name> **!**	extended MAC-IP access-list <name>, ACL <name>. ACL <name>

ii. permit \ deny ;

[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}icmp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [<icmp-type> [<icmp-code>]] [precedence <precedence>][tos<tos>][time-range<time-range-name>] **! ACL**	MAC-ICMP extended MAC-IP ACL. [no] .
[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}igmp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [<igmp-type>] [precedence <precedence>] [tos <tos>][time-range<time-range-name>] **! ACL**	MAC-IGMP extended MAC-IP ACL. [no] .
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}tcp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} [s-port {<port1> | range <sPortMin> <sPortMax>}] {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [d-port {<port3> | range <dPortMin> <dPortMax>}] [ack+fin+psh+rst+urg+syn] [precedence<precedence>][tos<tos>][time-range<time-range-name>] **! ACL**	MAC-TCP extended MAC-IP ACL. [no] .
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}udp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} [s-port {<port1> | range <sPortMin> <sPortMax>}] {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [d-port {<port3> | range <dPortMin> <dPortMax>}] [precedence <precedence>] [tos <tos>][time-range<time-range-name>] **! ACL**	MAC-UDP extended MAC-IP ACL. [no] .
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}} {eigrp|gre|igrp|ip|ipinip|ospf|{<protocol-num>}} {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} {{<destination><destination-wildcard>}|any-destination| {host-destination<destination-host-ip>}} [precedence<precedence>][tos<tos>][time-range<time-range-name>] **! ACL**	, IP extended MAC-IP ACL. [no] .

j. standard IPv6 access-list;

ipv6 access-list <num> {deny | permit} {{<sIPv6Addr> <sPrefixlen>} | any-source | {host-source <sIpv6Addr>}} no ipv6 access-list <num> **!**	standard ACL IPv6. ACL , ACL. ACL

k. standard IPv6 access-list;

i. standard IPv6 access-list;

ipv6 access-list standard <name> no ipv6 access-list standard <name> **!**	standard ACL IPv6. standard ACL IPv6.

ii. permit \ deny ;

[no] {deny | permit} {{<sIPv6Prefix/sPrefixlen>} | any-source | {host-source <sIPv6Addr> }} **! ACL**	standard ACL IPv6. [no]

2.

firewall enable firewall disable **!**	

3.

time-range <time_range_name> time-range <time_range_name> **!**	<time_range_name> <time_range_name>
[no] absolute-periodic {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} <start_time> to {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} <end_time> **! time-range**	. [no] .
[no] periodic {{Monday+Tuesday+Wednesday+Thursday+ Friday+Saturday+Sunday} | daily | weekdays | weekend} <start_time> to <end_time> **! time-range**	. [no] .
[no] absolute start <start_time> <start_data> [end <end_time> <end_data>] **! time-range**	. [no]

4. access-group

{ip|ipv6|mac|mac-ip} access-group <acl-name> in [traffic-statistic] no {ip|ipv6|mac|mac-ip} access-group <acl-name> {in} **!**	ACL <acl-name> . traffic-statistic access-group ACL <acl-name>

5. ACL

show access-group statistic [ethernet <interface-name>] **!**	, access-group ethernet <interface-name>
clear access-group statistic [ethernet <interface-name>] **!**	, access-group ethernet <interface-name>

1.3. ACL

1: 1/0/10 10.0.0.0/24, FTP .

:

```
Switch(config)#access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
Switch(config)#firewall enable
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#ip access-group 110 in
```

:

```
Switch#show firewall

Firewall status: enable.

Switch#show access-lists

access-list 110(used 1 time(s)) 1 rule(s)
access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch#show access-group interface ethernet 1/0/10

interface name:Ethernet1/0/10
the ingress acl use in firewall is 110, traffic-statistics Disable.
```

2: 802.3 1/0/10 MAC- 00-12-11-23-00-00 00-00-00-00-ff-ff.

:

```
Switch(config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac untagged-802-3
Switch(config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any tagged-802
Switch(config)#firewall enable
Switch(config)#interface ethernet1/0/10
Switch(Config-If-Ethernet1/0/10)#mac access-group 1100 in
```

:

```
Switch#show firewall
Firewall Status: Enable.
Switch #show access-lists
access-list 1100(used 1 time(s))
access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
untagged-802-3
access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
Switch #show access-group interface ethernet 1/0/10
interface name:Ethernet1/0/10
MAC Ingress access-list used is 1100,traffic-statistics Disable.
```

3: FTP ICMP - 00-12-11-23-00-00 00-00-00-00-ff-ff IP 10.0.0.0/24.

:

```
Switch(config)#access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac tcp 10.0.0.0
0.0.0.255 any-destination d-port 21
Switch(config)#access-list 3110 deny any-source-mac 00-12-11-23-00-00 00-00-00-00-ff-ff icmp any-source
10.0.0.0 0.0.0.255
Switch(config)#firewall enable
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#mac-ip access-group 3110 in
```

:

```
Switch#show access-lists
access-list 3110(used 1 time(s))
access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
access-list 3110 deny any-source-mac 00-12-11-23-00-00 00-00-00-00-ff-ff icmp any-source 10.0.0.0 0.0.0.255
Switch #show access-group interface ethernet 1/0/10
interface name:Ethernet1/0/10
MAC-IP Ingress access-list used is 3110, traffic-statistics Disable.
```

4. IPv6 interface vlan 600 2003:1:1:1::0/64. 2003:1:1:1:66::0/80 .

```
Switch(config)#ipv6 access-list 600 permit 2003:1:1:1:66::0/80 any-destination
Switch(config)#ipv6 access-list 600 deny 2003:1:1:1::0/64 any-destination
Switch(config)#firewall enable
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#ipv6 access-group 600 in
Switch(Config-If-Ethernet1/0/10)#exit
Switch(config)#exit
```

:

```
Switch#show firewall
Firewall Status: Enable.
Switch#show ipv6 access-lists
Ipv6 access-list 600(used 1 time(s))
ipv6 access-list 600 deny 2003:1:1:1::0/64 any-source
ipv6 access-list 600 permit 2003:1:1:1:66::0/80 any-source
Switch #show access-group interface ethernet 1/0/10
interface name:Ethernet1/0/10
IPv6 Ingress access-list used is 600, traffic-statistics
Disable.
```

5. 1/0/1, 2, 5, 7 VLAN 100, IP 192.168.0.1 .

:

```
Switch (config)#firewall enable
Switch (config)#vlan 100
Switch (Config-Vlan100)#switchport interface ethernet 1/0/1;2;5;7
Switch (Config-Vlan100)#exit
Switch (config)#access-list 1 deny host-source 192.168.0.1
Switch (config)#interface ethernet1/0/1;2;5;7
Switch (config-if-port-range)#ip access-group 1 in
```

:

```
Switch (config)#show access-group interface vlan 100
Interface VLAN 100:
Ethernet1/0/1: IP Ingress access-list used is 1, traffic-statistics Disable.
Ethernet1/0/2: IP Ingress access-list used is 1, traffic-statistics Disable.
Ethernet1/0/5: IP Ingress access-list used is 1, traffic-statistics Disable.
Ethernet1/0/7: IP Ingress access-list used is 1, traffic-statistics Disable.
```

1.4. ACL

1. **ACL** ;
2. - , **ACL** **ACL**;
3. **ACL MAC-IP**, **ACL MAC**, **ACL IP** **ACL IPv6**;
4. **ACL** , **ACL** :
   - **IPv6 ACL**
   - **MAC-IP ACL**
   - **IP ACL**
   - **MAC ACL**
5. **ACL**, , **ACL** . , **ACL** - ;
6. **ACL** (, “**permit tcp any any-destination**” “**deny tcp any any-destination**”), **ACL** ;