

Access Control Lists Work Sheet

1. Standard Access list filter based on Dirección IP origen.
2. Extended Access list filter based on Dirección IP origen, dirección IP destino, puerto de origen o destino and protocolo.
3. Standard IP Access list are numbered Desde la 1 hasta la 99 y de la 1300 a la 1999.
4. Extended IP Access list are numbered Comprende los rangos de 100 a 199 y de 2000 a 2699.
5. When using a wildcard mask, what number is used to indicate that the bits should be “ignored”? 1
6. When using wildcard mask, what number is used to indicate that the bits should be “checked” or “matched”? 0

Create all the appropriate IP Access list statement (s) necessary for the following to work:

7. Permit only traffic from host: 195.101.20.5

access-list 10 permit host 195.101.20.5

8. Deny all traffic from network : 195.101.25.0

access list 10 deny 195.101.25.0 0.0.0.255

access-list permit any

9. Permit only traffic from network 195.100.1.0 except for host 195.100.1.1 y 195.100.1.2

access-list 10 deny host 195.100.1.1

access-list 10 deny host 195.100.1.2

access-list 10 permit 195.100.1.0 0.0.0.255

10. Permit all traffic from 175.100.10.0 to any device on 210.200.5.0, but deny all other traffic from network 175.100.0.0 to network 210.200.0.0

access-list 100 permit 175.100.10.0 0.0.0.255 210.200.5.0 0.0.0.255

access-list 100 deny 175.100.0.0 0.0.255.255 210.200.0.0 0.0.255.255

11. Deny all traffic from 195.100.10.0 to the following host: 210.200.5.1 y 210.200.12.5

access-list 100 deny 195.100.10.0 0.0.0.255 host 210.200.5.1

access-list 100 deny 195.100.10.0 0.0.0.255 host 210.200.12.5

access-list 100 permit any any

12. Permit only telnet traffic from 195.100.10.0 to any device on 210.200.15.0

`access-list 100 permit tcp 195.100.10.0 0.0.0.255 210.200.15.0 0.0.0.255 eq Telnet`

13. Deny only ftp traffic from 195.100.10.0 to any device on 210.200.15.0

`access-list 100 deny tcp 195.100.10.0 0.0.0.255 210.200.15.0 0.0.0.255 eq 21`

`access-list 100 deny tcp 195.100.10.0 0.0.0.255 210.200.15.0 0.0.0.255 eq 20`

`access-list 100 permit any any`

14. Deny all traffic from subnet 195.100.32.0 through 195.100.63.0 to any device on network 210.200.15.0

`access-list 100 deny 195.100.32.0 0.0.31.255 210.200.15.0 0.0.0.255`

`access-list 100 permit any any`

15. What is the command that must be entered to actually apply the IP Access list statements?

Para aplicar un access list a una interfaz, los comandos a ejecutar son `int INTNAME`, `ip access-group (Access list number/Access list name)` y finalizar con el comando `end`.

16. What is the command to monitor the actual Access list statements that you have created, once they have been applied?

`show access-list`

17. What is the command used to monitor to see if the Access list has been

`Show run`

18. Once an Access list has been applied, what is the command to remove that Access list from the interface?

`no ip access-group NAME/NUMBER`

19. What is a wildcard mask? (select one)

- A. A 16 bit quantity used in conjunction with an IP Address to determine which bits in an IP address should be checked or ignored when comparing that address with another IP address.
- B. A 32 bit quantity used in conjunction with an IP address to determine which bits in an IP address should be checked or ignored when comparing that address with another IP address.
- C. A 42 bit quantity used in conjunction with an IP address to determine which bits in an IP address should be checked or ignored when comparing that address with another IP address.
- D. An 8 bit quantity used in conjunction with an IP address to determine which bits in an IP address should be checked or ignored when comparing that address with another IP address.

To specify all host in the class B IP network 172.16.0.0 which wildcard access list mask would you use?

- A. 255.255.0.0
- B. 255.255.255.0
- C. 0.0.255.255
- D. 0.255.255.255
- E. 0.0.0.255

Which of the following are valid ways to refer only to host 172.16.30.55 in an IP access list?

- A. 172.16.30.55.0.0.0.255
- B. 172.16.30.55.0.0.0.0
- C. Any 172.16.30.55
- D. Host 172.16.30.55
- E. Ip any 172.16.30.55

Which of the following access list will allow only WWW traffic into network 196.15.7.0?

- A. Access-list 100 permit tcp any 196.15.7.0.0.0.255 eq www
- B. Access-list 10 deny tcp any 196.15.7.0 eq www
- C. Access-list 100 permit 196.15.7.0.0.0.255 eq wwwj
- D. Access-list 10 permit tcp any 196.15.7.0.0.0.255
- E. Access-list 100 permit www 196.15.7.0.0.0.255

What are three ways to monitor IP access lists?

- A. Sh int
- B. Sh ip interface
- C. Sh run
- D. Sh access-lists

Which access configuration allows only traffic from network 172.16.0.0 to enter int s0?

- A. Access-list 10 permit 172.16.0.0.0.255.255, int s0, ip access-list 10 in
- B. Access-list 10 permit 172.16.0.0.0.255.255, int s0, ip access-list 10 out
- C. Access-list 10 permit 172.16.0.0.0.255.255, int s0, ip access-group 10 in
- D. Access-list 10 permit 172.16.0.0.0.255.255, int s0, ip access-group 10 out

In an IP access list, you want to refer to host 172.16.50.1. What mask would you use to make list as specific as possible?

- A. 255.255.0.0
- B. 0.0.0.0
- C. 0.0.255.255
- D. 0.255.255.255

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xs/sec-data-acl-xe-3s-book/sec-access-list-ov.html