Основные команды iOS сетевого оборудования Cisco

Общие команды iOS

1. Войти в привилегированный режим:
   #enable
2. Войти в режим глобального конфигурирования:
   #configure terminal
3. Задать незашифрованный пароль xxx на привилегированный режим:
   #enable password xxx
4. Задать зашифрованный пароль xxx на привилегированный режим:
   #enable secret xxx
5. Создать пользователя xxx с незашифрованным паролем yyy:
   #username xxx password yyy
6. Создать пользователя xxx с зашифрованным паролем yyy:
   #username xxx secret yyy
7. Задать (сменить) имя устройства (узла) на new-name:
   #hostname new-name
8. Конфигурирование группы портов Fast Ethernet с 1-го по 10-й:
   #interface fa0/1-10
9. Конфигурирование группы sub-интерфейсов Gigabit Ethernet с 10-го по 15:
   #interface gi0/0.10-15
10. Просмотреть выполненные конфигурационные настройки:
    #show running-config
11. Выйти из всех режимов:
    #end
12. Сохранить конфигурацию устройства:
    #write memory

Настройка терминального доступа по telnet

13. Настроить пароли на привилегированный режим и на режим конфигурации терминала:
    #enable – войти в привилегированный режим;
    #configure terminal – войти в режим глобальной конфигурации;
    #enable password cisco – задать пароль "cisco" на привилегированный режим;
    #service password-encryption – зашифровать пароль на привилегированный режим;
14. Создать пользователя с административными полномочиями:

 # username admin privilege 15 password cisco – создать пользователя "admin" с паролем "cisco" и наивысшим уровнем привилегий;
#enable secret cisco – задать пароль на доступ к режиму глобальных конфигураций (он сразу зашифрован);

15. Настроить терминальные линии для подключения к устройству через порты (интерфейсы):

#line vty 0 15 – войти в конфигурирование терминальных линий для портов с 0 по 15;
#login local – указать локальную базу данных пользователей для подключения по терминальным линиям;
#transport input telnet – задать telnet как способ подключения к устройству;
#exec-timeout 10 – установить время для отключения соединения 10 минут при отсутствии активности (эта команда не обязательна);
#exit – выйти из режима настройки терминальных линий;
 # logging synchronous – отключить вывод служебных сообщений при подключении (эта команда не обязательна);

16. На виртуальном интерфейсе vlan 1 задать IP-адрес для последующего удалённого подключения по сети с помощью telnet:

#interface vlan 1 – настроить сетевой интерфейс на виртуальной сети для подключения по telnet;
#ip address 192.168.1.1 255.255.255.0 – задать IP-адрес на интерфейсе;
#no shutdown – поднять порт (интерфейс);
#exit – выйти из настроек сетевого интерфейса.

Команды агрегирования каналов

17. Агрегирование каналов на коммутаторе:

#interface range fa0/1-2 – войти в настройки группы портов fa0/1-2;
#channel-protocol lacp – включить на этих портах протокол агрегирования каналов LACP;
#channel-group 1 mode active - включить эти порты в группу агрегированных каналов с номером 1;
#exit – выйти из режима конфигурирования группы портов.

18. Просмотр настройки протоколов агрегирования каналов на каждом из коммутаторов командами:

#show etherchannel summary
#show etherchannel port-channel

Настройка виртуальных сетей

19. Создание виртуальной сети:

#enable;
#configure terminal;

#vlan 123 – создание на коммутаторе vlan с номером 123;
#name VLAN123 – задание настраиваемой vlan имени VLAN123;
#exit

20. Переключение порта в режим доступа:

#interface fa0/1 – войти в конфигурирование интерфейса fa0/1;
#switchport mode access – переключить порт в режим доступа;
#switchport access vlan 123 – подключить к порту доступа vlan с номером 123;
#exit

21. Настройка транкового порта:

#interface fa0/1 – войти в конфигурирование транкового порта fa0/1;
#switchport mode trunk – задать для порта режим транка;
#switchport trunk allowed vlan x1,x2 – разрешить пропускать через транковый порт виртуальные сети с номерами x1 и x2;
#exit.

22. Просмотреть настройку виртуальных сетей:

#show vlan
#show vlan brief

Настройка виртуальных и физических портов маршрутизатора или L3-коммутатора

23. Настройка транк-порта gi0/1 на L3-коммутаторе:

#enable – привилегированный режим
#configure terminal – режим глобального конфигурирования
#interface gigabitEthernet 0/1 – настройка порта gi0/1
#switchport trunk encapsulation dot1q – включение режима инкапсуляции на порту
#switchport mode trunk – переключение порта в режим транка
#switchport trunk allowed vlan 11,12,13 – пропуск через порт виртуальных сетей vlan 11, 12 и 13
#exit – выход из настройки порта

24. Включение порта на маршрутизаторе или L3-коммутаторе:

#interface fa0/1 – войти в настройки порта fa0/1;
#no shutdown – включить порт;
#exit.

25. Настройка виртуальных интерфейсов на L3-коммутаторе:

#interface vlan xx – настройка виртуального интерфейса vlan xx;
#ip address 192.168.xx.1 255.255.255.0 – задание ip-адреса для интерфейса vlan xx;
#no shutdown –«поднять» (включить) настроенный виртуальный интерфейс;

#exit – выход из режима настройки интерфейса.

26. Настройка sub-интерфейсов на роутере:

#interface fa0/0.2 – начать конфигурирование sub-interface (под-интерфейса) с номером 2 на интерфейсе с номером 0, к которому подключён коммутатор;
#encapsulation dot1q 100 – подключить к sub-интерфейсу vlan с номером 100 в режиме инкапсуляции dot1q;
#ip address 192.168.100.1 255.255.255.0 – задать sub-интерфейсу ip-адрес, который будет шлюзом vlan;
#no shutdown – включить порт sub-интерфейса, который по умолчанию на роутере тоже выключен;
#exit.

27. Задание ip-адреса для порта маршрутизатора:

#interface fa0/0 – входим в настройки порта
#no shutdown – включаем порт
#ip address 192.168.30.1 255.255.255.0 – присвоили порту ip-адрес из новой 70-й подсети
#exit

Настройка статической маршрутизации

28. Задание статического маршрута на роутере или L3-коммутаторе:

#enable
#configure terminal
#ip route 192.168.11.0 255.255.255.0 192.168.15.2 – прописан маршрут к сети 192.168.11.0 через порт маршрутизатора 192.168.15.2
#end

29. Задание дефолтного маршрута:

#enable
#configure terminal
#ip route 0.0.0.0 0.0.0.0 192.168.30.1
#exit

30. Включение маршрутизации на L3-коммутаторе:

ip routing – включить маршрутизацию на L3-коммутаторе.

Настройка динамической раздачи IP-адресов (DHCP)

31. Войти в конфигурирование пула адресов DHCP-сервера с именем name1:

#ip dhcp pool name1

32. Задать диапазон адресов в виде адреса сети для выбранного пула:

#network 172.16.0.0 255.255.0.0

33. Указать порт, по которому доступен DHCP-сервер:

#default-router 172.16.2.1

34. Задать адрес, который должен быть исключён из пула адресов DHCP-сервера:

#ip dhcp excluded-address 172.16.1.100

35. Включение команды перенаправления DHCP-запросов на sub-интерфейсе с номером 7 (для виртуальной сети 7):

#interface fastEthernet 0/0.7

#ip helper-address 192.168.4.2 – указали в качестве адреса адрес DHCP-сервера.

#exit

36. Просмотр таблицы выдачи IP-адресов протоколом DHCP:

#show ip dhcp binding

Настройка трансляции сетевых адресов (NAT)

37. Указать настраиваемый порт как внешний для NAT:

#ip nat outside

38. Указать настраиваемый порт как внутренний для NAT:

#ip nat inside

39. Создать в режиме глобального конфигурирования список доступа для NAT:

#ip access-list standard NatList

40. Выдать разрешения на трансляцию NAT для указанной сети (в режиме конфигурирования access-list):

#permit 192.168.xx.0   0.0.0.255

41. Задать в качестве исходных адресов для трансляции NatList. В качестве внешнего адреса указать порт fa0/0, а также параметр overload, задающий тип трансляции – перегруженный NAT, т.е. PAT:

#ip nat inside source list NatList interface fastEthernet0/0 overload

42. Просмотреть таблицу трансляции сетевых адресов на маршрутизаторе:

#show ip nat translation

Настройка динамической маршрутизации по протоколу OSPF

43. Настройка loopback-интерфейса для протокола OSPF:

#interface loopback 0 – входим в конфигурацию интерфейса

#ip address 192.168.100.1 255.255.255.255 – задаём адрес и маску для одного узла

#no shutdown – включаем интерфейс

#exit – выходим из режима конфигурации loopback-интерфейса

44. Войти в режим конфигурирования роутера и запустить OSPF как процесс с номером 1:

#router ospf 1

45. Прописать все сети, которые будет маршрутизировать протокол OSPF:

#network 192.168.1.0 0.0.0.255 area 0

46. Просмотр «соседей» данного роутера:

#show ip ospf neighbor

47. Просмотр таблицы маршрутизации:

#show ip route

48. Передача сообщений о прописанном дефолтном статическом маршруте всем другим маршрутизаторам:

#router ospf 1

#default-information originate

49. Запуск протокола EIGRP:

#router eigrp 1 – войти в настройки протокола EIGRP для автономной системы с номером 1;

#network 192.168.1.0 0.0.0.255 – разрешить маршрутизацию сети 192.168.1.0

#network 10.10.x1.0 0.0.0.255 – разрешить маршрутизацию сети 10.10.x1.0

#network 10.10.x2.0 0.0.0.255 – разрешить маршрутизацию сети 10.10.x2.0

#no auto-summary – отключить опцию суммирования маршрутов

Настройка списков доступа Access Lists:

50. Создание в режиме конфигурации терминала стандартного списка доступа с именем List1:

#ip access-list standard List1

51. Создание в режиме конфигурации терминала расширенного списка доступа с именем List2:

#ip access-list extended List2

52. Примеры разрешающих правил для стандартных списков доступа:

#permit host 192.168.1.1 – разрешить трафик с узла с IP 192.168.1.1

#permit 192.168.1.0 0.0.0.255 – разрешить трафик из сети 192.168.1.0/24

#permit any – разрешить трафик с любых узлов

53. Примеры запрещающих правил для стандартных списков доступа:

#deny host 192.168.1.1 – запретить трафик с узла с IP 192.168.1.1

#deny 192.168.1.0 0.0.0.255 – запретить трафик из сети 192.168.1.0/24

#deny any – запретить трафик с любых узлов

54. Примеры разрешающих правил для расширенных списков доступа:

#permit ip 192.168.1.0 0.0.0.255 172.0.1.0 0.0.255.255 – разрешить весь трафик из сети 192.168.1.0/24 в сеть 172.16.0.0/16.

#permit tcp host 192.168.1.100 192.168.10.0 0.0.0.255 eq 80 – разрешить трафик с узла 192.168.1.100 на сеть 192.168.10.0/24 на 80-й порт TCP (веб-серфинг).

#permit tcp 172.16.0.0 0.0.255.255 host 192.168.100.100 eq 20 – разрешить трафик из сети 192.16.0.0/16 на узел 192.168.100.100 по 20-му порту TCP (FTP-протокол)

#permit ip any any – разрешить весь трафик во всех направлениях

55. Примеры запрещающих правил для расширенных списков доступа:

#deny ip 192.168.1.0 0.0.0.255 172.0.1.0 0.0.255.255 – запретить весь трафик из сети 192.168.1.0/24 в сеть 172.16.0.0/16.

#deny tcp host 192.168.1.100 192.168.10.0 0.0.0.255 eq 80 – запретить трафик с узла 192.168.1.100 на сеть 192.168.10.0/24 на 80-й порт TCP (веб-серфинг).

#deny tcp 172.16.0.0 0.0.255.255 host 192.168.100.100 eq 20 – запретить трафик из сети 192.16.0.0/16 на узел 192.168.100.100 по 20-му порту TCP (FTP-протокол)

#deny ip any any – запретить весь трафик во всех направлениях

56. Подключение списка доступа List1 на входящий трафик порта (выполняется в режиме настроек соответствующего порта):

#ip access-group List1 in

57. Подключение списка доступа List2 на исходящий трафик порта (выполняется в режиме настроек соответствующего порта):

#ip access-group List2 out