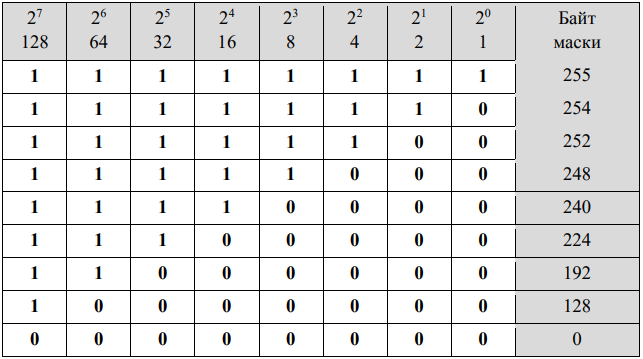
Команды IOS



Возможные значения октетов маски

**Команды первой лабы**

Команды режима глобального конфигурирования router(config)#

**enable password <пароль>** – Задаёт пароль на привилегированный режим.

**line console 0** – Переход в режим конфигурирования консоли управления.

**line vty 0 15** – Переход в режим конфигурирования виртуальных терминалов удаленного доступа (vty) с 0 по 15.

**service password-encryption** – Включает шифрование всех паролей в конфигурационном файле.

**banner motd <баннер>** – Определяет баннерное сообщение.

Команды режима конфигурирования консоли и vty router(config-line)#

**password <пароль>** – Определяет пароль для консольной строки.

**login** - Разрешает удаленное подключение и включает аутентификацию по паролю при входе в систему.

**Команды второй лабы**

Команды привилегированного режима // switch#

**show mac-address table** – выводит таблицу MAC – адресов (допустима фильтрация по интерфейсу, номеру виртуальной сети и др., см. параметры команды во встроенной справке);

**clear mac address table** – очищает таблицу MAC – адресов;

**show spanning-tree** – команда без указания дополнительных параметров предоставляет краткие сведения о состоянии STP;

**show vlan** – выводит таблицу виртуальных сетей, известных коммутатору;

**show vtp status** – выводит информацию о состоянии протокола vtp на коммутаторе;

**show vtp password** – выводит пароль vtp;

**vlan [номер vlan]** – переход в режим конфигурирования виртуальной сети; создает виртуальную локальную сеть с заданным номером, если она не существует;

**vtp mode [server/client/transparent]** – переводит протокол vtp на текущем коммутаторе в выбранный режим работы;

**vtp domain [имя домена]** – задает домен для изолированной работы vtp;

**vtp password [пароль]** – задает пароль для vtp-домена на текущем

коммутаторе;

Команды режима глобального конфигурирования // swich(config)#

**interface [интерфейс].[номер]** – переход в режим конфигурирования суб-интерфейса; создает для указанного интерфейса суб-интерфейс с заданным номером, если он не существует;

Команды режима конфигурирования интерфейса // switch(config-if)#

**switchport mode [access/trunk]** – переводит порт коммутатора в выбранный режим работы (доступ или транк);

**switchport access vlan [номер vlan]** – назначает текущему интерфейсу (должен работать в режиме доступа) vlan с указанным номером. Если vlan с таким номером не существует, то он принудительно создаётся;

**switchport trunk allowed [номера vlan]** – задает список виртуальных сетей, которым разрешён доступ в текущий транк.

Команды режима конфигурирования интерфейса // switch(config-subif)#

**encapsulation dot1q [номер vlan]** – задает режим инкапсуляции на текущем суб-интерфейсе по стандарту IEEE 802.1q и назначает vlan с указанным номером;

Команды конфигурирования vlan

**name [текст]** – задать название виртуальной локальной сети

**Команды третьей лабы**

Команды привилегированного режима // router#

**show ip route** – выводит таблицу маршрутизации;

**show ip protocols** – выводит расширенную информацию об

используемых протоколах маршрутизации;

Команды режима глобального конфигурирования // router(config)#

**ip route [сеть назначения] [маска] [маршрут]** – добавляет в таблицу маршрутизации статический маршрут до указанной сети назначения. Маршрут может быть задан в виде исходящего интерфейса и/или (предпочтительно!) адреса next hop (IP-адреса входящего интерфейса следующего маршрутизатора на маршруте).

**Команды четвёртой лабы**

Команды привилегированного режима // router#

**show ip rip […]** – выводит подробную информацию о конфигурации и работе протокола RIP; список возможных параметров см. во встроенной справке IOS;

**show ip ospf […]** – выводит подробную информацию о конфигурации и работе протокола OSPF; список возможных параметров см. во встроенной справке IOS;

Команды режима глобального конфигурирования // router(config)#

**router rip** – включение протокола маршрутизации RIP и вход в режим конфигурации этого протокола;

**router ospf [номер процесса]** – включение протокола маршрутизации OSPF c указанным номером процесса и вход в режим конфигурации этого протокола; номер процесса нужен для обеспечения возможности запуска нескольких процессов OSPF (например, для граничных маршрутизаторов) и их различия; номер процесса имеет локальное значение и не включается в сообщения маршрутизации, следовательно номера процессов не обязательно должны совпадать на соседних маршрутизаторах;

Команды режима конфигурирования протокола RIP // router(config-router)#:

**version [1 или 2]** – включает протокол RIP выбранной версии; напомним, что RIPv2 является протоколом бесклассовой маршрутизации и включает маску сети в маршрутные сообщения; по умолчанию используется версия 1, рекомендуется версия 2;

**no auto-summary** – отключает автоматическое суммирование маршрутов (по умолчанию включена); рекомендуется отключать автосуммирование, т.к. оно является распространенной причиной возникновения ошибок маршрутизации, в т.ч. петель;

**network [IP-адрес сети]** – включает протокол RIP на всех интерфейсах, входящих в указанную сеть;

**passive-interface [интерфейс]** – переводит интерфейс в пассивный режим; пассивные интерфейсы не осуществляют рассылку маршрутных сообщений; как правило, пассивный режим включается на интерфейсах, подключенным к локальным сетям или сети провайдера, чтобы не загружать сеть бесполезным служебным трафиком;

**default-information originate** – маршрутизатор включает в маршрутные сообщения маршрут по умолчанию; как правило, команда вводится на маршрутизаторе, подключенному к провайдеру (ISP, Interner Service Provider), таким образом он сообщит остальным маршрутизатором, что

через него можно выйти в Интернет.

Команды режима конфигурирования протокола OSPF // router(config-router)#:

**network [IP-адрес сети] [wildcard маска] area [номер зоны]** – включает данный процесс протокола OSPF на всех интерфейсах, входящих в указанную сеть, и помещает их в выбранную зону;

**passive-interface [интерфейс]** – переводит интерфейс в пассивный режим; пассивные интерфейсы не осуществляют рассылку маршрутных сообщений;

**default-information originate** – маршрутизатор включает в маршрутные сообщения маршрут по умолчанию;

**area [номер зоны] authentication message-digest** – включает md5- аутентификацию для всех интерфейсов данной зоны (можно также задать метод аутентификации отдельно для каждого интерфейса, см. ниже);

Команды конфигурации интерфейса // router(config-if)#:

**ip ospf authentication message-digest** – включает md5-аутентификацию для протокола OSPF на текущем интерфейсе; это необходимо лишь в том случае, если такой метод аутентификации уже не выбран для всех для всех интерфейсов данной зоны в режиме конфигурирования OSPF

(см. выше); имеет приоритет по отношению к общему методу аутентификации для зоны – может назначать другой метод аутентификации для текущего интерфейса;

**ip ospf message-digest-key [номер ключа] md5 [пароль – текстовая строка]** – создает md5-ключ с указанным порядковым номером и паролем; порядковый номер необходим для управления версиями ключей – при смене ключа каждый следующий номер должен быть больше предыдущего; номер и пароль должны совпадать на соседних маршрутизаторах, но не рекомендуется использовать одинаковые значения во всей зоне.

**Команды пятой лабы**

Команды привилегированного режима router#

**show access-lists [номер или имя ACL]** – выводит указанный ACL или все ACL, если конкретный не указан; здесь и далее в квадратных скобках указаны необязательные параметры команд.

Команды режима глобального конфигурирования router(config)#

**access-list <номер списка от 1 до 99> {permit | deny | remark} {<адрес сети> <wildcard-маска> | any | host <IP-адрес узла>} [log]** – создает стандартный нумерованный ACL и/или добавляет в него команду – разрешить или запретить трафик с данного источника; параметры команды: действие: permit – разрешить, deny – запретить, remark – добавить комментарий (текстовое пояснение, не является правилом фильтрации); источник трафика: сеть с данной wildcard-маской, any – любой источник; host [IP-адрес] – конкретный узел; ключевое слово log (опционально) включает логирование пакетов, удовлетворяющих текущему правилу;

**access-list <номер списка от 100 до 199> {permit | deny | remark} <протокол> {<адрес сети> <wildcardмаска> | any | host <IP-адрес узла>} [<operator> <порт или название протокола>] {<адрес сети> <wildcard-маска> | any | host <IP-адрес узла>} [<operator> <порт или название протокола>] [established]** – создает расширенный нумерованный ACL и/или добавляет в него команду – разрешить или запретить трафик указанного протокола от указанного источника (можно указать номера портов источника) к данному получателю (можно указать номера портов назначения); параметры команды: действие: permit/deny/remark – см. выше; протокол: какой протокол разрешаем/запрещаем (например: icmp, ip, tcp, udp, ospf и т.д.); источник трафика: сеть/any/host – см. выше; назначение трафика: сеть/any/host – аналогично источнику; operator: фильтр портов источника/назначения; принимает значения: eq [port] – точное совпадение (конкретный номер порта); gt [port] – номера портов, больше указанного; lt [port] – номера портов, меньше указанного; neq [port] – любые номера портов, кроме указанного; range [port1 port2] – все номера портов в указанном промежутке; ключевое слово established разрешает прохождение TCPсегментов, которые являются частью уже созданной TCP-сессии;

**access-list {standard | extended} <имя ACL>** – создает стандартный или расширенный именованный ACL и/или переводит консоль в режим конфигурирования ACL;

**access-list resequence <имя ACL> <номер0> <шаг>** – выполняет перенумерацию строк в указанном списке контроля доступа; новые порядковые номера правил начинаются с указанного номера и следуют с указанным шагом;

Команды конфигурирования ACL router(config-ext-nacl)#

**[номер] {permit | deny | remark} …** – добавляет строку в ACL и присваивает ей указанный порядковый номер (если параметр указан – иначе правило помещается в конец списка); формат строки зависит от типа ACL: стандартный или расширенный;

Команды конфигурирования интерфейса router(config-if)#

**ip access-group <номер или имя ACL> {in | out}** –прикрепляет указанный ACL к текущему интерфейсу в указанном направлении.

**Команды шестой лабы**

Команды режима глобального конфигурирования router(config)#

**ip nat inside source static tcp 10.0.1.1 80 11.1.1.21 80**

**ip nat inside source static udp 10.0.1.1 5060 11.1.1.21 7877** – Статические преобразования одного порта.

Команды привилегированного режима router#

show ip nat translations – Отображает список активных трансляций IP-адресов.

Команды режима глобального конфигурирования router(config)#

**ip nat inside source static <Локальный IP-адрес> <Глобальный IP-адрес>** – Создает статическое NAT-отображение указанного локального адреса в указанный глобальный.

*ПРИМЕЧАНИЕ. Для включения указанного отображения необходима активация NAT хотя бы на одном внутреннем и одном внешнем интерфейсах.*

**ip nat pool <Имя пула> <Начальный IP-адрес пула> <Конечный IPадрес пула> netmask <маска>** – Создает пул глобальных IP-адресов для последующего использования в динамическом NAT-преобразовании; границами пула являются заданные начальный и конечный IP-адреса (могут совпадать, тогда трансляция будет в 1 адрес); опция netmask позволяет вырезать из диапазона адресов в пуле те адреса, которые являются адресами SUBNET или BROADCAST при данной маске.

*ПРИМЕЧАНИЕ. Для включения отображения необходима активация NAT хотя бы на одном внутреннем и одном внешнем интерфейсах, а также создание самого преобразования – связь пула со списком контроля доступа.*

**ip nat inside source list <ACL> pool <Имя пула>** – Создает динамическое NAT-отображение для трафика, отбираемого с помощью заданного ACL, в указанный пул глобальных адресов.

*ПРИМЕЧАНИЕ. Для включения указанного отображения необходима активация NAT хотя бы на одном внутреннем и одном внешнем интерфейсах.*

**ip nat inside source list <ACL> interface <Имя интерфейса> overload** – Создает перегруженное динамическое NAT-отображение для трафика, отбираемого с помощью заданного ACL, в (глобальный) адрес указанного внешнего интерфейса.

*ПРИМЕЧАНИЕ. Для включения указанного отображения необходима активация NAT хотя бы на одном внутреннем интерфейсе, а также на интерфейсе отображения (как на внешнем).*

**ip dhcp pool <имя пула>** – Создает на маршрутизаторе dhcp-пул с указанным именем и переводит

маршрутизатор в режим конфигурирования dhcp;

**ip dhcp excluded address <начальный (или единственный) IPадрес> [конечный IP-адрес]** – Исключает из пула dhcp-адресов один (или несколько) адресов, например, если они присвоены каким-то устройствам статически. Среди исключаемых обязательно должен быть адрес основного шлюза!

Команды конфигурирования интерфейса router(config-if)#

**ip nat {inside | outside}** – Активирует на текущем интерфейсе функцию NAT-преобразования и помечает данный интерфейс как внутренний или внешний.

**ip helper-address <ip-адрес>** – Включает пересылку dhcp-запросов на удаленный интерфейс

(используется на интерфейсе – основном шлюзе, если dhcp-сервер не является основным шлюзом для клиентских устройств в сети).

Команды конфигурирования dhcp router(dhcp-config)#

**network <IP-адрес сети> <сетевая маска>** – Задает диапазон адресов пула, которые будут раздаваться клиентам, а также маску подсети.

**Router(dhcp-config)#dns-server <IP-адрес основоного DNSсервера> [IP-адреса других DNS-серверов]** – Задает адрес DNS-сервера для клиентов.

**Router(dhcp-config)#default-router 192.168.100.1** – Задает адрес основного шлюза.