***Негосударственное образовательное частное учреждение высшего образования «Московский финансово-промышленный университет «Синергия»***

***Институт информационных систем и технологий***

***Кафедра Цифровой экономики***

*Дисциплина «*Администрирование информационных систем*»*

*ЭССЕ*

*Тема* Список управления доступом (Access Control List /ACL).

*Выполнил Студент Тилаков Акмал*

*группа ВБИо-302рсоб*

*Принял Сиберев И.В.*

**Пример настройки списков управления доступом (Access Control List, ACL)**

**Списки управления доступом (Access Control List, ACL) являются средством фильтрации потоков данных без потери производительности, так как проверка содержимого пакетов данных выполняется на аппаратном уровне. Фильтруя потоки данных, администратор может ограничить типы приложений, разрешённых для использования в сети, контролировать доступ пользователей к сети и определять устройства, к которым они могут подключаться. Также ACL могут использоваться для определения политики QoS, путём классификации трафика и переопределения его приоритета. ACL представляют собой последовательность условий проверки параметров пакетов данных: коммутатор проверяет параметры пакетов данных на совпадение с критериями фильтрации, определёнными в ACL, и выполняет над пакетами одно из действий: Permit (Разрешить) или Deny (Запретить). В коммутаторах D-Link со стандартным CLI списки управления доступом (ACL) можно разделить на 3 группы: • Стандартный список доступа (standard ACL); • Расширенный список доступа (extended ACL); • Экспертный список доступа (expert ACL). Среди стандартных списков доступа выделяются: • Стандартный список доступа IP (standard IP ACL); • Стандартный список доступа IPv6 (standard IPv6 ACL). Среди расширенных списков доступа выделяются: • Расширенный список доступа MAC (extended MAC ACL); • Расширенный список доступа IP (extended IP ACL); • Расширенный список доступа IPv6 (extended IPv6 ACL). Каждому списку управления доступом назначается имя и номер. Для каждого типа списка зарезервирован свой диапазон номеров: стандартные списки доступа IP 1—1999 расширенные списки доступа IP 2000—3999 расширенные списки доступа MAC 6000—7999 экспертные списки доступа 8000—9999 стандартные списки доступа IPv6 11000—12999** **расширенные списки доступа IPv6 13000—14999 Имя списка доступа должно быть уникальным. Если при создании списка доступа указывается только его имя, то автоматически будет назначен самый большой неиспользуемый номер из диапазона номеров, соответствующего типу списка доступа, и для каждого следующего списка будет уменьшаться на единицу. Каждый ACL может состоять из множества правил. Все правила в ACL также нумеруются. Если правило создано без указания определенного порядкового номера, он будет присвоен автоматически. Если это первая запись, то будет присвоен начальный порядковый номер 10. Последующим записям правила назначается номер, больший на значение шага 10, а самый большой порядковый номер в списке доступа будет стоять в конце. Пользователь может использовать команду access-list resequence для смены начального порядкового номера и значения шага записей для указанного списка доступа. После применения команды новым записям без указанного порядкового номера будет задан номер в соответствии с новыми настройками указанного списка доступа. При назначении порядкового номера вручную, лучше иметь зарезервированный интервал для будущих записей с меньшим порядковым номером. Иначе будет сложно вставить запись с еще меньшим порядковым номером. Порядковый номер должен быть уникальным в домене списка доступа. При вводе занятого порядкового номера появится сообщение об ошибке. В стандартном IP ACL критериями фильтрации могут выступать только IP-адреса источника и получателя пакета. В расширенном IP ACL в числе критериев фильтрации могут выступать IP-адреса источника и получателя, порты протоколов транспортного уровня, поля ToS и DSCP в заголовке IP и некоторые другие параметры. В расширенном MAC ACL в числе критериев фильтрации выступают MAC-адреса источника и получателя, тег VLAN, значение поля Ethertype и поле приоритета CoS. Рекомендуется нумеровать правила в ACL с определенным интервалом, например: 10, 20, 30 и т.д. При создании правила для указания диапазона адресов используется инверсная маска (wildcard mask). Бит адреса, соответствующий значению 1 бита маски, будет игнорироваться. Бит, соответствующий значению 0 бита маски, будет проверяться. После создания ACL его нужно применить на одном или нескольких портах коммутатора (интерфейсах) и указать, для какого направления трафика должен использоваться этот фильтр — для входящего (in) или исходящего (out). Если группа доступа IP (IP access group) уже настроена на интерфейсе, примененная позднее команда заменит предыдущие настройки. К каждому интерфейсу можно**

**применить только один список доступа определенного типа, но списки доступа различных типов могут быть применены к одному и тому же интерфейсу. Привязка группы доступа (access group) к интерфейсу будет расходовать ресурсы из записей фильтрации коммутатора. Если ресурсов недостаточно для активации команды появится сообщение об ошибке. Число портов ограничено. Если применение команды исчерпает выбор доступных портов, появится сообщение об ошибке.**