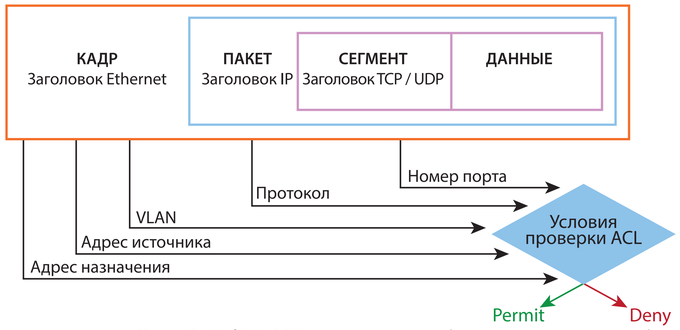
Технологии обеспечения безопасности в коммутируемых сетях

Списки 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.

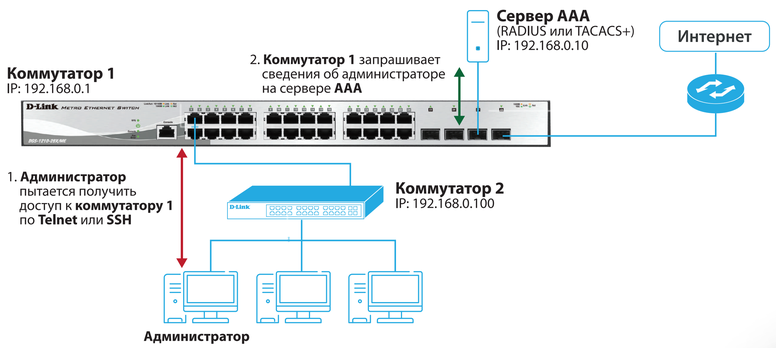
ACL представляют собой последовательность условий проверки параметров пакетов данных. Когда сообщения поступают на входной порт, коммутатор проверяет параметры пакетов данных на совпадение с критериями фильтрации, определенными в **ACL**, и выполняет над пакетами данных одно из действий: **Permit (Разрешить)** или **Deny (Запретить)**.

ACL используются для:

- ограничения типов приложений, разрешенных для использования в сети;
- контроля доступа пользователей к сети;
- классификации и маркировки пакетов для реализации требуемой политики QoS.

ACL позволяют бороться с атаками типа MAC Flooding.

Authentication, Authorization, Accounting (AAA)

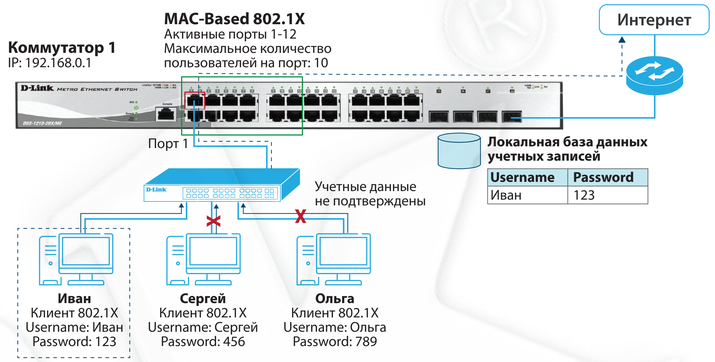


AAA - это основанная на стандартах структура, используемая для контроля:

- тех, кому разрешен доступ к сетевым ресурсам (через аутентификацию);
- что им разрешено делать (через авторизацию);
- регистрации действий, выполняемых при доступе к сети (посредством учета).

В сети используется сервер **AAA** (**TACACS+** или **RADIUS**), способный аутентифицировать пользователей, обрабатывать запросы на авторизацию и собирать учетные данные.

Аутентификация 802.1X

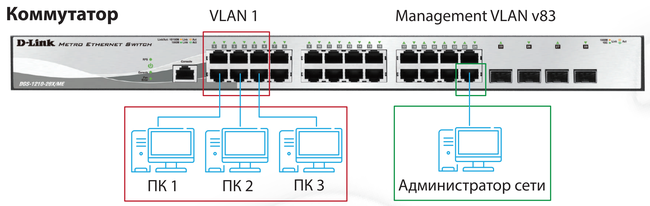


Стандарт **IEEE 802.1X** осуществляет контроль доступа и не позволяет неавторизованным устройствам подключаться к локальной проводной или беспроводной сети через порты устройства связи. Он описывает использование протокола **EAP (Extensible Authentication Protocol)** для поддержки аутентификации с помощью сервера аутентификации и определяет процесс инкапсуляции данных **EAP**, передаваемых между клиентами и серверами аутентификации.

Коммутаторы D-Link поддерживают две реализации аутентификации 802.1X:

- 802.1X на основе портов: после того как порт был авторизован, любой компьютер, подключенный к нему, может получить доступ к сети.
- 802.1X на основе MAC-адресов: аутентификация множества клиентов на одном физическом порту коммутатора. Каждый узел должен проходить аутентификацию индивидуально для доступа к порту.

Функция Management VLAN



Management VLAN (VLAN управления) - это подсеть, которая используется только для управления сетевыми устройствами.

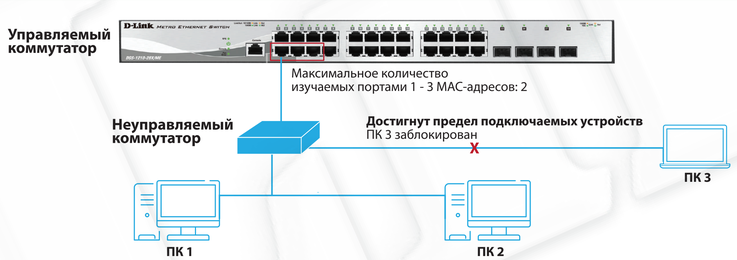
Основное назначение **Management VLAN** - повышение сетевой безопасности. Когда весь трафик управления находится в отдельной VLAN, неавторизованным пользователям труднее отслеживать его и выполнять вредоносные действия в сети. Рабочая станция администратора, с которой выполняется управление коммутаторами, должна находиться в этой подсети.

По умолчанию управляющей **VLAN** является **VLAN 1** (**default VLAN**).

Рекомендуется:

- не использовать настройки по умолчанию и создать новую VLAN, которую сделать управляющей;
- с помощью списков управления доступом запретить доступ к управляющей VLAN из других VLAN, созданных в сети.

Функция Port Security



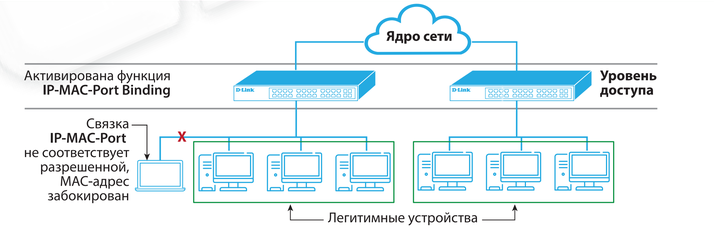
Функция **Port Security** используется для контроля доступа устройств к портам коммутаторов.

Устройства, которым разрешено подключаться к порту, определяются по MAC-адресам. MAC-адреса могут быть изучены динамически или настроены вручную.

Можно ограничить количество изучаемых портом MAC-адресов, тем самым, ограничив количество подключаемых к нему узлов.

Функция **Port Security** позволяет бороться с атаками типа MAC Flooding, MAC Spoofing.

Функция IP-MAC-Port Binding (IMPB)



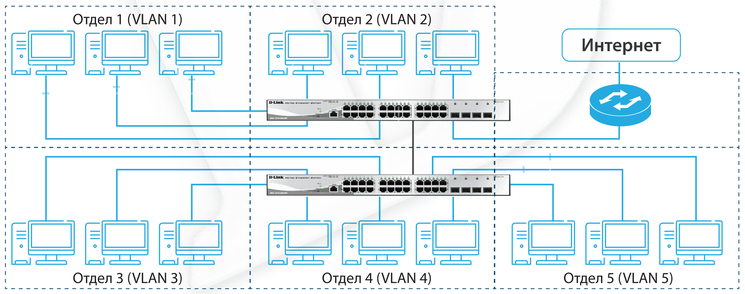
Функция **IP-MAC-Port Binding (IMPB)** позволяет контролировать доступ компьютеров в сеть на основе их IP/MAC-адресов и порта подключения.

Работа функции основана на сравнении параметров входящих пакетов с параметрами хранящихся на коммутаторе записей, связывающих MAC- и IP-адреса клиентских устройств с портами подключения:

- при совпадении всех составляющих (IP/MAC-адресов и порта), пакеты будут передаваться, и клиенты получат доступ в сеть;
- при подключении клиента, связка MAC-IP-порт которого будет отличаться от параметров заранее сконфигурированной записи, коммутатор заблокирует MAC-адрес соответствующего узла с занесением его в «черный лист».

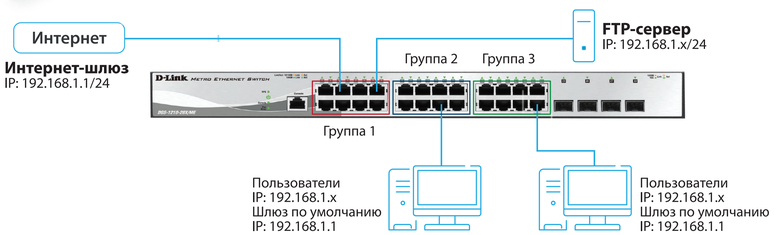
Функция **IMPB** позволяет бороться с атаками типа ARP Spoofing и атаками на протокол DHCP.

Виртуальные локальные сети (VLAN)



- **Виртуальной локальной сетью (Virtual LAN, VLAN)** называется логическая группа узлов сети, трафик которой полностью изолирован от других узлов сети на канальном уровне.
- Передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна независимо от типа адреса - индивидуального, группового или широковещательного.
- Использование **VLAN** позволяет повысить безопасность сети благодаря изоляции трафика различных групп узлов. Политику взаимодействия пользователей из разных виртуальных сетей можно определить с помощью фильтров или списков управления доступом, настроенных на коммутаторе или маршрутизаторе.

Сегментация трафика



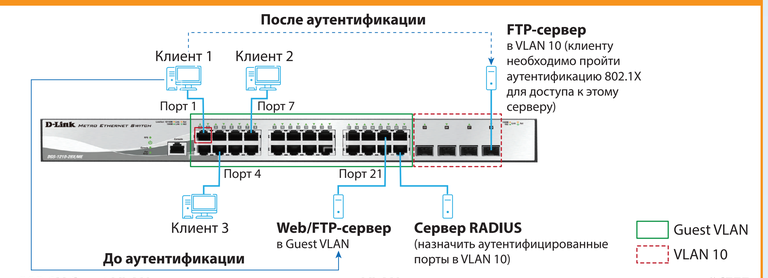
Функция **Traffic Segmentation (сегментация трафика)** служит для разграничения трафика на канальном уровне. Она позволяет настраивать порты или группы портов коммутатора таким образом, чтобы они были полностью изолированы друг от друга, но в то же время имели доступ к разделяемым портам, используемым для подключения серверов или магистрали сети.

В корпоративной сети функция может использоваться для защиты трафика отделов, работающих с критически важной информацией или для изоляции потенциально опасных отделов от остальной сети.

В сетях провайдеров сегментация трафика позволяет изолировать потоки данных клиентов.

Для повышения безопасности и стабильности работы сети сегментация трафика может использоваться внутри VLAN.

Функция 802.1X Guest VLAN



Функция **802.1X Guest VLAN** позволяет настроить гостевую **VLAN** для каждого порта коммутатора с поддержкой **IEEE 802.1X** для предоставления клиентам (например, посетителям компании) ограниченных сервисов.

Когда клиент подключается к порту коммутатора с активированной аутентификацией **802.1X** и функцией **Guest VLAN**, происходит процесс аутентификации:

- при успешной аутентификации клиент помещается в VLAN назначения (Target VLAN) в соответствии с предустановленным на сервере RADIUS атрибутом VLAN. Если этот параметр не определен, клиент будет возвращен в первоначальную VLAN (в соответствии с настройками порта подключения).
- при неуспешной аутентификации клиент останется в гостевой VLAN.

Члены гостевой VLAN могут взаимодействовать друг с другом в пределах этой VLAN независимо от того, прошли они аутентификацию 802.1X или нет.