**Dynamic ARP Inspection**

**Dynamic ARP Inspection (Protection)** — функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP. Например, атаки ARP-spoofing, позволяющей перехватывать трафик между узлами, которые расположены в пределах одного широковещательного домена.

Dynamic ARP Inspection (Protection) регулирует только сообщения протокола ARP и не может повлиять напрямую на трафик пользователей или другие протоколы.

В коммутаторах Cisco функция называется Dynamic ARP Inspection, а в коммутаторах ProCurve — Dynamic ARP Protection. Далее, в описании функции будет использоваться термин Dynamic ARP Inspection, а в соответствующем разделе по настройке функции на коммутаторах ProCurve — Dynamic ARP Protection.

Dynamic ARP Inspection позволяет:

* защитить клиентов в сети от атак с использованием протокола ARP,
* регулировать какие сообщения протокола ARP отбрасывать, какие перенаправлять.

Для правильной работы Dynamic ARP Inspection, необходимо указать какие порты коммутатора будут доверенными (trusted), а какие — нет (untrusted, в дальнейшем — ненадёжными):

* Ненадёжные (Untrusted) — порты, к которым подключены клиенты. Для ненадёжных портов выполняется ряд проверок сообщений ARP.
* Доверенные (Trusted) — порты коммутатора, к которым подключен другой коммутатор. Сообщения протокола ARP полученные с доверенных портов не отбрасываются.

**Принципы работы Dynamic ARP Inspection**

Если порт ненадёжный:

* Коммутатор перехватывает все ARP-запросы и ARP-ответы на ненадёжных портах прежде чем перенаправлять их;
* Коммутатор проверяет соответствие MAC-адреса IP-адресу на ненадёжных портах.

Проверка соответствия MAC-адреса IP-адресу может выполняться на основании информации:

* Базы данных привязки DHCP,
* Статических записей