Анализ угроз на канальном уровне

1. Прописывать MAC адрес/адреса для портов в коммутаторе - тем самым можно исключить атаку MAC Overflow, когда злоумышленник переполнял таблицу коммутации, тем самым переводил коммутатор в режим трансаляции трафика;
2. DHCP Snooping - Защита от DHCP атак, поскольку запрещает злоумышленнику посылать любые типы сообщений протокола DHCP. Благодаря Доверенным/ Недоверенным портам можно настроить типы запросов DHCP, который могут быть отправлены по определенным портам:
   По доверенному порту можно отправлять любой из типов сообщений DHCP, по недоверенным - только запросы DHCP;
3. Динамическая проверка ARP - метод предотвращения ARP-спуфинга аналогичен DHCP Snooping. Он использует доверенные и ненадежные порты. Ответы ARP допускаются в интерфейс коммутатора только на доверенных портах. Если ответ ARP приходит на коммутатор на ненадежном порту, содержимое пакета ответа ARP сравнивается с таблицей привязки DHCP для проверки его точности. Если ответ ARP недействителен, ответ ARP отбрасывается и порт отключается. Дополнительно моэно подключить проверку Dynamic ARP Inspection на уровне коммутаторов. Это функция проверяет соответветствие MAC-адреса отправителя и содержания ARP-ответа;
4. Root Guard и BPDU-Guard - две техники защиты от атак на STP.Root Guard ограничивает порты коммутатора, из которых может быть согласован корневой мост. BPDU-Guard используется для защиты сети от проблем, которые могут быть вызваны приемом BPDU на портах доступа.
5. Для того, чтобы минимизировать риск сетевых атак на канальном уровне, необходимо разделять сеть на виртуальные сегменты - VLAN. Тогда запросы в переделах одного сегмента не пройдут дальше коммутатора. Однако есть такая, позволяющая это сделать - VLAN Hopping. Злоумышленник подключается к порту коммутатора и притворяется соседним коммутатором. Осуществляться такая атака может только если коммутатор установлен в режим авто-транка. Мерой предотвращения этого риска является удаление всех портов доступа из VLAN 1 по умолчанию, поскольку порт злоумышленника должен совпадать с портом собственной VLAN коммутатора. Отключить протокол DTP, убедиться в отключенном режиме работы авто-транк. Отключить и перенести в неиспользуемый VLAN неиспользуемые порты, а также всегда использовать специальные VLAN ID для всех транковых портов.