**CDP**

**Cisco Discovery Protocol (CDP)** — проприетарный протокол Cisco второго уровня, который позволяет сетевым устройствам анонсировать в сеть информацию о себе и о своих возможностях, а также собирать эту информацию о соседних устройствах.

Устройство посылает мультикаст-анонс (advertisement) на MAC-адрес 01-00-0c-cc-cc-cc. В конфигурации по умолчанию анонсы рассылаются каждые 60 секунд на порты Ethernet, Frame Relay и ATM. Каждое устройство, понимающее анонсы, сохраняет полученную информацию в CDP-таблице и позволяет посмотреть её по команде show cdp neighbors, и более детально по команде show cdp entry устройство. Если устройство трижды не прислало анонс (при значениях по умолчанию — 3 минуты (180 секунд)), оно удаляется из таблицы.

В анонсах также содержится информация о времени жизни пакета (Time To Live — TTL) или времени удержания информации (holdtime). Последний параметр определяет время, в течение которого будет храниться CDP информация, прежде чем она будет уничтожена.

Протокол работает на канальном уровне и позволяет двум системам получить информацию друг о друге даже в том случае, если они используют различные протоколы сетевого уровня.

Протокол CDP обеспечивает получение информации о каждом соседнем устройстве путём передачи информации в формате TLV (Type Length Value — запись тип — длина — значение). Записи TLV — это блоки информации, внедрённые в CDP анонсы. Значения TLV конкретного устройства включают в себя такую информацию:

* Идентификатор устройства;
* Номер и тип локального интерфейса;
* Время удержания информации (время, по истечении которого записи из CDP-таблицы удаляются);
* Тип устройства (маршрутизатор, коммутатор, сетевой мост и т.д.);
* Физическую платформу устройства (модель подключенного устройства, например, Сisco 2961);
* Номер и тип удаленного интерфейса;
* Доменное имя VTP (только в случае использования протокола CDPv2);
* Номер собственной сети VLAN (только в случае использования протокола CDPv2);
* Информацию о дуплексности соединения (только в случае использования протокола CDPv2).

Руководства по безопасности требуют отключения протокола CDP на интерфейсах, выходящих за защищённый периметр, так как передаваемая информация (например, версия IOS) может использоваться для подготовки атаки через уязвимость конкретной версии IOS. Выключение производится командой no cdp run глобально, no cdp enable для интерфейса.