С. Т. Оморова – ст.преп.ОшТУ
S.T. Omorova – senior teacher OshTU

ОПРЕДЕЛЕНИЕ ТОПОЛОГИИ СЕТИ НА УРОВНЯХ L2, L3 OSI

В статье описаны элементы методики определения топологии сети на канальном и сетевом уровнях.

Ключевые слова: локальный сеть, коммутатор, топология сети, компьютеры.

DEFINITION OF NETWORK TOPOLOGY ON THE LEVEL L2, L3 OSI

This article describes the elements of the methodology for determining the topology of the network at the data link and network layers.

Keywords: local net, switch, network topology, computers.

В настоящее время каждая крупная компания располагает своей внутренней локальной сетевой инфраструктурой. Во внутреннюю сеть входят как непосредственно рабочие станции, так и любые другие сетевые устройства, попадающие под понятие «хост».

Хост (от англ. Host) – конечный узел в стеке протоколов TCP/IP . Чаще всего этими устройствами в сети являются маршрутизаторы и коммутаторы.

Чем крупнее компания, тем объемнее и разветвленней ее сеть, которая включает в себя как внутрисетевые ресурсы, так и прочие сервисы и вложенные структуры, которые необходимо постоянно обслуживать и наблюдать. Именно с целью качественного мониторинга сети, быстрой ликвидации неполадок и внештатных ситуаций, выявления непроходимостей канала и решения прочих проблем необходимо знать топологию сети.

Топология сети - конфигурация графа, вершинам которого соответствуют конечные узлы сети (компьютеры) и коммуникационное оборудование (маршрутизаторы, коммутаторы), а ребрам — физические или информационные связи между вершинами. [1]

В большинстве случаев типом топологии является неполносвязное иерархическое дерево, когда от одного или нескольких корневых мощных серверов, маршрутизаторов, расходится вся паутина сети. И чем крупнее локальная сеть, тем сложнее ее обслуживать и детектировать неисправности в условиях отсутствия знаний ее архитектуры.

Разумеется, в настоящее время имеются некоторые готовые решения способные визуализировать граф сети с указанием всех входящих в нее узлов. В их число входят разные пакеты сетевого менеджмента, работающих в автоматическом режиме и не всегда корректно отображающих реальное состояние объектов.

Например, пакет HP OpenView Network Node Manager компании Hewlett-Packard и разного рода подобные ему продукты предоставляют информацию о топологии на уровне L3, но предоставляют не много сведений о подключении и отключении сетевых устройств. То есть для эффективного обнаружения узлов сети и существующих соединений между ними необходимо оперировать средствами определения топологии на уровне L2 работая в режиме обнаружения соединений на уровне коммутаторов и маршрутизаторов.

Существуют другие решения от конкретных крупных производителей сетевого оборудования, таких как Cisco Systems, Nortel Networks, разработавших собственные протоколы CDP, LLDP - стандарт для обслуживания сетей крупных предприятий. Но проблема заключена в следующем: зачастую многие сети реализованы на оборудовании разных производителей, подобранном по тем или иным причинам, параметрам или предпочтениям.

Следовательно, появляется необходимость разработать универсальный метод по определению топологии сетей, вне зависимости от поставщика оборудования и прочих

условий, который использовал бы разветвленный алгоритм анализа сети и ее узлов, а также предоставлял бы результаты в упрощенном наглядном виде, например, строя граф связности сети.

Реализовать это можно следующим образом. Входными данными для алгоритма станут аутентификационные параметры одного из корневых устройств сети и его IP-адрес. С него и начнется сбор информации о каждом устройстве посредством последовательного SNMP-опроса, используя определенную последовательность действий.

Для начала необходимо установить, какие протоколы активны и поддерживаются конкретным устройством, на рассматриваемом устройстве. Первичный анализ должен заключать в себя проверку активности протокола LLDP и CDP – наиболее простых путей обнаружения соседства между устройствами в сети. Link Layer Discovery Protocol (LLDP) — протокол канального уровня, позволяющий сетевым устройствам анонсировать в сеть информацию о себе и о своих возможностях, а также собирать эту информацию о соседних устройствах. [2]

Cisco Discovery Protocol (CDP) – протокол канального уровня, разработанный компанией Cisco Systems, позволяющий обнаруживать подключённое (напрямую или через устройства первого уровня) сетевое оборудование Cisco, его название, версию IOS и IP-адреса. [3]

Таким образом, если устройством поддерживается один из этих протоколов, алгоритм сразу же обращается к соответствующим разделам MIB-таблицы (Management Information Base), в которой находится вся информация о соседних устройствах, если они также анонсировали ее о себе. В нее входят IP-адреса, информация о портах, шасси и типах устройств.

Если же поддержка LLDP/CDP отсутствует, вторым шагом проверки станет SNMP-опрос локальной MIB текущего девайса на предмет получения информации об его активных интерфейсах и ARP-таблице.

При этом, в первую очередь процедура проверки запускается на коммутаторах. Используя ARP-таблицу (Address Resolution Protocol) коммутатора, алгоритм получит информацию о каждом подключенном устройстве в виде соответствия MAC-address– IP-address–interface– TTL

Поиск соседних устройств должен осуществляться посредством последовательного unicast опроса по всем найденным в ARP таблице MAC адресам. Ответ на ARP-запрос от искомого устройства по MAC-адресу и фиксация интерфейса, с которого ответ получен, станет фактом обнаружения устройства в сети. Идентифицировав соседство, производим процедуру сопоставления MAC-адресов: если на интерфейс первого устройства приходит ответ на запрос по MAC-адресу второго устройства и наоборот, на интерфейс второго устройства приходит ответ по запросу первого MAC адреса, то это гарантированная линия связи между двумя узлами. В итоге информация о соседстве содержит не только линию связи между узлами, но и информацию об интерфейсах, через которые они соединены.

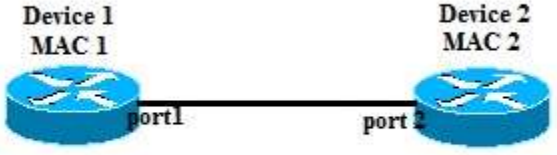

Рис. 1 Определение соседства устройств по MAC-адресам

Далее алгоритм переключается на следующий коммутатор и повторяет процедуру проверки, оставив запись в log-файле об уже посещенных девайсах и их параметрах, таким образом пройдя последовательно каждый узел в сети.

При проектировании данного метода и разработке алгоритма, не следует выпускать из вида несколько условий корректной его работы:

1. На устройствах должна быть обязательно включена поддержка SNMP протокола, предпочтительно версии 3.

2. Алгоритм должен уметь отличить виртуальные интерфейсы от реальных и строить граф связности по реальным физическим соединениям.

Выполнив необходимые условия работы и реализовав такого рода алгоритм, в итоге будет разработан универсальный метод определения топологии сети, который можно будет использовать как просто для визуализации графа связности сети, так и включить как модуль в состав другого более сложного алгоритма по выявлению и устранению неисправностей на уровнях L2, L3.

Литература:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы (4-ое изд.) – СПб: Питер, 2010. – 944с.
2. Link Layer Discovery Protocol (LLDP). Режим доступа:http://xgu.ru/wiki/ LLDP (дата обращения 12.03.2014)
3. Cisco Discovery Protocol (CDP) Режим доступа:http://ru.wikipedia.Org/ wiki/ CDP (дата обращения 12.03.2014)