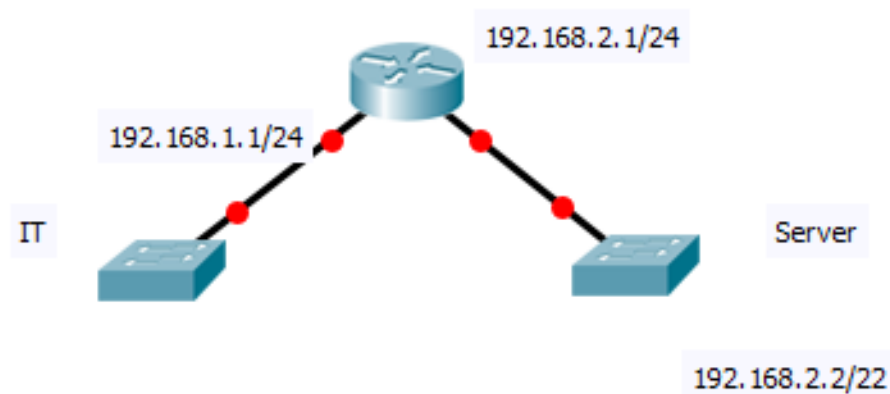


Климанов. Лекция 13

27 ноября 2018 г.

1 Proxy Arp



Проблема: если установим неправильную маску для Server, мы можем потерять контроль над Server. Например, если мы поставим маску /16 для нашего сервера, то он будет применять ее в том числе и для адреса источника, который после применения маски будет выглядеть как находящийся в той же сети. Соответственно, вместо пересылки ответа через роутер, будет составляться ARP-запрос, на который очевидно не будет получен ответ => попытка установления TCP провалится. **Proxy Arp** позволяет роутеру выступать в качестве "источника" он принимает адресованный источнику ARP-запрос, пересылает свой адрес в ответ и, соответственно, обеспечивает доставку информации до источника.

Не должен использоваться на постоянной основе, создает слишком большую нагрузку на сеть и CPU маршрутизаторов

2 DHCP

Dynamic Host Configuration Protocol - позволяет автоматически настроить IP адреса и еще некоторые параметры.

Основные 4 типа сообщений DHCP, которые используются для получения параметров:

Номер	Клиент	Сервер
1	DHCP-Discover - широковещательная рассылка, поиск DHCP-серверов	
2		DHCP-offer - отправляет свое "предложение"
3	Принимается "offer". Отправляется DHCP-request - перепроверка и запрос на использование параметров сервера	
4		ACK - подтверждение

После этой цепочки за клиентом закрепляются выданные параметры на время *lease-time* (?).
Адреса могут даваться на долгое время в стабильных сетях

2.1 Еще сообщения DHCP

Отказ DHCP

Если после получения подтверждения (DHCPACK) от сервера клиент обнаруживает, что указанный сервером адрес уже используется в сети, он рассылает широковещательное сообщение отказа DHCP (DHCPDECLINE), после чего процедура получения IP-адреса повторяется. Использование IP-адреса другим клиентом можно обнаружить, выполнив запрос ARP.

Сообщение отмены DHCP (DHCPNAK). При получении такого сообщения соответствующий клиент должен повторить процедуру получения адреса.

Освобождение DHCP

Клиент может явным образом прекратить аренду IP-адреса. Для этого он отправляет сообщение освобождения DHCP (DHCPRELEASE) тому серверу, который предоставил ему адрес в аренду. В отличие от других сообщений DHCP, DHCPRELEASE не рассылается широковещательно.

Информация DHCP

Сообщение информации DHCP (DHCPINFORM) предназначено для определения дополнительных параметров TCP/IP (например, адреса маршрутизатора по умолчанию, DNS-серверов и т. п.) теми клиентами, которым не нужен динамический IP-адрес (то есть адрес которых настроен вручную). Серверы отвечают на такой запрос сообщением подтверждения (DHCPACK) без выделения IP-адреса.

2.2 DHCP сервер в сети

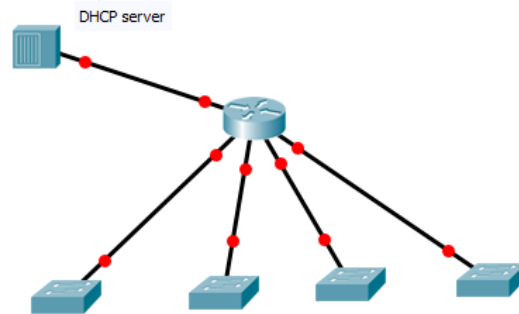


Рис. 1: Пример топологии

DHCP запросы проходят через роутер на DHCP-сервер, подключенный к нему (широковещательные пакеты (определенного вида) переправляются роутером к DHCP). Для управления адресным пространством может быть, например, IRAM

2.3 DHCP-Snooping

Прослушиваем процесс обмена DHCP сообщений, составляем свою собственную базу, включающую IP и MAC, отбрасываем все странные пакеты.

Защищает от атаки вида "Подмена IP-адресов".

3 Топологии в современных датацентрах

(...) Core - внутренний уровень Distribution Acc/QoS - внешний

3.1 Clos

Делим коммутаторы на 2 категории: Leaf и Spine, Обычно берут немного Spine и много Leaf и соединяют каждый Leaf к каждому Spin'у. Все подключения к сети и сети к другим сетям происходит на уровне Leaf, эта технология позволяет удобно масштабировать сеть.

3.1.1 VXLAN

Тоннель между Leaf'ами Spanning tree не используется в таких сетях, вместо него технология vxlan