

Расширенные функции



6.1 DHCP Relay (Option 82) – информация от агента DHCP Relay

DHCP Relay (Option 82) – информация от агента DHCP Relay

- Option 82 используется Relay Agent (агентом перенаправления запросов) для добавления дополнительной информации в DHCP – запрос клиента. Эта информация может быть использована для применения политик, направленных на увеличение уровня безопасности и эффективности сети.
- Она описана в стандарте RFC 3046.

D-Link

DHCP Relay (Option 82) – информация от агента DHCP Relay

Когда вы включаете опцию DHCP relay agent option 82 на коммутаторе D-link, происходит следующее:

• Компьютер в сети (DHCP - клиент) генерирует DHCP - запросы и <u>широковещательно</u> рассылает их в сеть.

D-Link

- Коммутатор (DHCP Relay Agent) перехватывает DHCP запрос packet и добавляет в него информацию relay agent information option (option 82). Эта информация содержит MAC – адрес коммутатора (поле опции remote ID) и SNMP ifindex порта, с которого получен запрос (поле опции circuit ID).
- Коммутатор <u>перенаправляет DHCP запрос с полями опции option-82 на DHCP сервер.</u>
- DHCP сервер получает пакет. Если сервер поддерживает опцию option-82, <u>он может использовать поля remote ID и/или circuit ID для назначения IP-адреса и применения политик</u>, таких как ограничения количества IP-адресов, выдаваемых одному remote ID или circuit ID. Затем DHCP сервер копирует поле опции option-82 в DHCP ответе. Если сервер не поддерживает option 82, он игнорирует поля этой опции и не отсылает их в ответе.
- <u>DHCP сервер отвечает в Unicast-е агенту перенаправления запросов</u>. Агент проверяет предназначен ли он его клиенту, путём анализа IP адреса назначения пакета.
- <u>Агент удаляет поля опции option-82 и направляет пакет на порт, к которому подключён</u> <u>DHCP - клиент,</u> пославший пакет DHCP – запроса.

Формат полей опции DHCP option 82 специализированного DHCP Relay Agent-а

Поле опции DHCP option 82 имеет следующий формат :

Формат поля опции Circuit ID:

1.	2.	3.	4.	5.	6.	7.
1	6	0	4	VLAN	Modul	Port
1 байт	1 байт	1 байт	1 байт	2 байта	1 ба 9 т	1 байт



1. Тип подопции

D-Link

- 2. Длина: длина поля с октета 3 по октет 7
- 3. Тип Circuit ID
- 4. Длина: длина поля с октета 5 по октет 7

Формат поля опции Remote ID:

- 5. VLAN: номер VLAN ID в DHCP пакете клиент.
- Модуль: Для отдельно стоящего коммутатора, поле Модуль всегда равно 0; Для коммутатора в стеке, поле Модуль это Unit ID.
- 7. Порт: номер порта, с которого получен DHCP запрос, номер порта начинается с 1.

1.	2.	3.	4.	5.

2806MAC address

1 байт 1 байт 1 байт 1 байт 6 байт

- 1. Тип подопции
- 2. Длина
- 3. Тип Remote ID
- 4. Длина
- 5. МАС-адрес: МАС-адрес коммутатора.

Для идентификации удалённого узла. DHCP – сервер может использовать эту опцию для выбора специфических параметров пользователей, узлов. Поле remote ID должно быть уникально в сети.

Локальный идентификатор агента,

который получил DHCP – пакет от клиента.

Формат поля опции Circuit ID



Формат поля опции Remote ID





Пример настройки Option 82



Устройства:

- 1. DHCP сервер 192.168.0.221 в подсети 192.168.0.0/24
- Маршрутизатор или коммутатор L3, выступающий в роли шлюза для 2-ух подсетей 192.168.0.1 в подсети 192.168.0.0/24
 10.100.10.1 в подсети 10.100.10.0/24
- Коммутатор L2 (DES-3200-10) выступает в роли DHCP Relay Agent 192.168.0.170 в подсети 192.168.0.0/24
 MAC адрес 00-24-01-FC-8F-D8
- 1. 3 ноутбука, выступающих в роли DHCP клиентов, подключённых к коммутатору L2 порты 1, 2 и 5

Сервер с поддержкой DHCP Option 82

 DHCP – сервер использует динамический пул IP-адресов 10.100.10.200 – 10.100.10.250 для назначения IP-адресов любому DHCP – клиенту, запрос от которого будет перенаправлен DHCP Relay Agent-ом 192.168.0.170 (Если DHCP – клиент, подключён к любому порту коммутатора, кроме портов 1 и 2, он получит IP-адрес из пула.)

--- Для обычного DHCP – запроса клиента

D-Link

 Когда какой-либо DHCP – клиент подключается к порту 1 коммутатора L2, DHCP – сервер выдаст ему IP-адрес 10.100.10.101; когда DHCP – подключается к порту 2 коммутатора L2, DHCP – сервер выдаст ему IP-адрес 10.100.10.102. (например, DHCP – клиент, подключённый к порту 1 коммутатора, получит IP-адрес 10.100.10.101)

---- Для DHCP – запросов клиента с option 82

Конфигурация коммутатора L3

Настройка коммутатора L3 (DGS-3627):

Настройте влан, в котором будут находиться DHCP – клиенты

create vlan client tag 555

config vlan client add tagged 1-12

Настройте управляющий влан, в котором будет находиться DHCP сервер

create vlan management tag 1234

config vlan management add tagged 1-12

config vlan default delete 24

config vlan management add untagged 24

Сконфигурируйте и создайте IP-интерфейсы в VLAN client и management

config ipif System ipaddress 10.90.90/24

create ipif client_gw 10.100.10.1/24 client state enable

create ipif manag_gw 192.168.0.1/24 management state enable

Сохраните настройки

save

Конфигурация коммутатора L2

Настройка коммутатора L2 (DES-3200-10):

Настройте клиентский и управляющий вланы на DES-3200-10

config vlan default delete 1-10

create vlan client tag 555

config vlan client add tagged 9-10

config vlan client add untagged 1-8

create vlan management tag 1234

config vlan management add tagged 9-10

Настройте управляющий интерфейс

config ipif System ipaddress 192.168.0.170/24 vlan management

Настройте DHCP Relay

enable dhcp_relay

config dhcp_relay option_82 state enable

config dhcp_relay option_82 check disable

config dhcp_relay option_82 policy replace

config dhcp_relay option_82 remote_id default

config dhcp_relay add ipif System 192.168.0.221

Paspeшите клиентам доступ в управляющем влане, только к DHCP серверу. Остальное запретите create access_profile ip destination_ip 255.255.255.255 profile_id 5 config access_profile profile_id 5 add access_id 1 ip destination_ip 192.168.0.221 port 1-8 permit create access_profile ip destination_ip 255.255.255.0 profile_id 6 config access_profile profile_id 6 add access_id 1 ip destination_ip 192.168.0.0 port 1-8 deny # Сохраните настройки

save

Настройка DHCP – сервера - 1

Рассмотрим пример настройки сервера isc-dhcpd. Ниже приведено содержимое dhcpd.conf:

Настройка основных параметров

lease-file-name "/var/log/dhcpd.leases"; log-facility local7; authoritative; default-lease-time 86400; ddns-update-style none; local-address 192.168.0.221; one-lease-per-client true; deny duplicates;

Настройка логирования (в лог записываются МАС адрес, влан и порт клиента, запросившего IP адрес)

```
if exists agent.circuit-id {
  log(info, concat("Lease"," IP ",binary-to-ascii(10, 8,".",leased-address),
  " MAC ",binary-to-ascii(16,8,":",substring(hardware,1, 6)),
  " port ",binary-to-ascii(10,16, "",substring(option agent.circuit-id, 4,
  2)),
  " VLAN ",binary-to-ascii(10, 16,"",substring(option agent.circuit-id, 2, 2))
));
}
```

Сравниваются Remote ID и Circuit ID с заданными. Согласно дизайну преобразования binary-to-ascii незначащие нули слева отбрасываются

```
class "sw170-1" {
  match if binary-to-ascii(16, 8, ":", suffix(option agent.remote-id, 5))
  = "24:1:fc:8f:d8" and binary-to-ascii(10, 8, "", suffix(option
  agent.circuit-id, 1)) = "1";
  }
  class "sw170-2" {
  match if binary-to-ascii(16, 8, ":", suffix(option agent.remote-id, 5))
  = "24:1:fc:8f:d8" and binary-to-ascii(10, 8, "", suffix(option
  agent.circuit-id, 1)) = "2";
}
```

Настройка DHCP – сервера - 2

Продолжение содержимого файла dhcpd.conf:

shared-network test {

Включить опцию, позволяющую клиенту корректно продлевать аренду IP адреса прямым запросом на сервер, не содержащим Option 82 (минуя DHCP Relay Agent) stash-agent-options true;

Запретить выдавать IP-адреса из подсети 192.168.0.0/24 (в этой подсети находятся управляющие интерфейсы коммутаторов и доступ клиентов в эту подсеть должен быть ограничен)

subnet 192.168.0.0 netmask 255.255.255.0 { deny unknown-clients;

Описать выдаваемые клиенту по DHCP параметры
subnet 10.100.10.0 netmask 255.255.255.0 {
 option broadcast-address 10.100.10.255;
 option domain-name-servers 10.100.10.1;
 option routers 10.100.10.1;
 option subnet-mask 255.255.255.0;
Задать адреса, получаемые клиентами :
клиентом , подключенным к порту 1
pool { range 10.100.10.101; allow members of "sw170-1";}
клиентом , подключенным к порту 2
pool { range 10.100.10.102; allow members of "sw170-2";}
клиентами, находящимися на других портах
pool { range 10.100.10.200 10.100.10.250;}

Информация DHCP Relay Agent (Option 82)

Результаты теста:

D-Link

- 1. Клиенту A будет выдан IP-адрес **10.100.10.101**
- 2. Клиенту Б будет выдан ІР-адрес 10.100.10.102
- 3. Клиенту В будет выдан IP-адрес 10.100.10.200



6.2 RSPAN



- Функция RSPAN может использоваться для зеркалирования клиентского трафика на порт удаленного коммутатора.
- Нет необходимости подключаться сниффером (анализатором трафика) к коммутатору клиента.
- Для работы RSPAN необходима настройка на всех коммутаторах в цепочке от клиента и до сниффера.
- Зеркалироваться может весь трафик как входящий, так и исходящий, либо по отдельности.
- Термины RSPAN:

- Порт источник (Source port) порт, трафик с которого копируется на порт со сниффером
- Порт назначения (Destination port) порт, на который посылается копия трафика и к которому подключается сниффер.
- RSPAN VLAN это VLAN, по которому передается зеркалируемый трафик между коммутаторами в цепочке.

Пример использования RSPAN

• Коммутатор А:

create vlan rspanvlan tag 4094 create rspan vlan vlan_name rspanvlan config rspan vlan vlan_name rspanvlan source add ports 1 both enable rspan config mirror port 26 enable mirror

• Коммутатор В:

create vlan rspanvlan tag 4094 config vlan rspanvlan add tagged 21,22 create rspan vlan vlan_name rspanvlan config rspan vlan vlan_name rspanvlan redirect add port 22 enable rspan

• Kommytatop C: create vlan rspanvlan tag 4094 config vlan rspanvlan add tagged 26 create rspan vlan vlan_name rspanvlan config rspan vlan vlan_name rspanvlan redirect add port 1 enable rspan При данных настройках весь трафик Comp A будет попадать на Sniffer





6.4 Диагностика кабеля

Диагностика кабеля (Cable Diagnostics)



Функция диагностики кабеля позволяет оперативно узнавать информацию о состоянии кабельной системы, в том числе определять длину кабеля между коммутатором и клиентом, а также с довольно большой точностью* находить место возникновения неисправности

* Отклонение результата измерения диагностики кабеля от фактического значения не превышает 5-ти метров



Результаты работы функции диагностики кабеля

<u>Результаты работы функции диагностики кабеля могут быть</u> <u>следующими:</u>

ОК: кабель исправен.

Ореп: обрыв кабеля на указанной позиции.

Short: короткое замыкание на указанной позиции.

Open-Short: не удалось установить точную причину возникновения неисправности: короткое замыкание, либо обрыв на указанной позиции. Диагностику кабеля лучше провести повторно.

Crosstalk: неисправность вызвана наличием перекрестных помех на указанном участке.

Unknown: не удалось получить информацию о состоянии кабеля. Диагностику кабеля лучше провести повторно.

No Cable: кабель не подключен.

Важно: при запуске диагностики кабеля на гигабитных портах происходит кратковременное отключение линка, поэтому нужно с осторожностью использовать этот функционал на портах, которыми коммутаторы соединены между собой.

Примеры работы функции диагностики кабеля

В качестве примера произведем диагностику кабеля на 1 и 9 портах коммутатора:

DES-320 Command	00-10:5#c l: cable_	able_diag ports : diag ports 1	1					
Perfo	em Cable	Diagnostics						
Port	Т уре	Link Status	10.00000	Test	Result	Cable	Length	(M)
1	FE	Link Up	ОК	1			1	
DES-320 Command	00-10:5#c l: cable_	able_diag ports ' diag ports 9	9					
Perfo	em Cable	Diagnostics						
Port	Туре	Link Status		Test	Result	Cable	Length	(M)
9	GE	Link Up	No	Cable		1993 전1992년99	_	

Как видно из результата работы функции кабель, подключенный в первый порт коммутатора, исправен. Длина его составляет 1 метр.

В девятый порт коммутатора кабель не подключен.

D-Link



6.3 LLDP (802.1ab)

LLDP (802.1ab)

LLDP определяет стандартный метод для устройств в сети коммутаторы, маршрутизаторы Ethernet, таких как И беспроводные точки доступа, с помощью которого устройства распространяют информацию о себе среди других узлов в сети и сохраняют полученные данные. В частности, LLDP определяет набор общих информационных сообщений, протокол для их передачи и метод хранения. Множество таких сообщений посылается устройством через локальную сеть с помощью одного пакета в форме поля «тип, длина, значение». Все LLDPустройства должны обязательно поддерживать сообщения с идентификаторами шасси (chassis ID) и портов (port ID) а также такие параметры, как системное имя (system name), системный дескриптор (system descriptor) и системные возможности (system capabilities). Первые два из них обеспечивают полезную информацию для сбора инвентаризационных данных.

LLDP (802.1ab)

- Протоколом предусматривается передача данных только в одном направлении. То есть LLDP-устройства не обмениваются информацией в режиме запрос–ответ, а также не подтверждают ее получение. Каждый LLDP-пакет должен содержать четыре обязательных TLV:
- chassis ID TLV: идентифицирует шасси устройств LAN 802;
- port ID TLV: идентифицирует порт, через который передается LLDPпакет;
- TTL TLV: указывает отрезок времени в секундах, в течение которого полученная информация актуальна;
- end of TLV: определяет конец TLV.



LLDP (802.1ab)

Вот так выглядит LLDP пакет в пакетном анализаторе wireshark

Þ	Frame 30: 99 bytes on wire (792 bits), 99 bytes captur	ed (792 bits)	
Þ	Ethernet II, Src: D-Link_7a:7d:78 (00:17:9a:7a:7d:78),	Dst: LLDP_Multicast ((01:80:c2:00:00:0e)
~	Link Layer Discovery Protocol		
1	Chassis Subtype = MAC address, Id: 00:17:9a:7a:7d:78	Chassis I	ID
	> Port Subtype = Locally assigned, Id: 1/8	Port ID	
3	> Time To Live = 120 sec	TTL	
1	> Port Description = RMON Port 8 on Unit 1		
3	> System Name = D-Link		
	System Description = Fast Ethernet Switch		
3	> Capabilities		
	> End of LLDPDU	End of T	LV



LLDP (802.1ab)

Устройство с поддержкой LLDP может работать в 3-х режимах:

- -Только приём: Устройство может принимать и анализировать LLDP пакеты, поступающие на него, но не может ничего отослать
- -Только передача: Устройство может рассылать LLDP пакеты, но не принимает их
- -Приём и передача: Устройство рассылает LLDP пакеты, а также анализирует пакеты, принимаемые от друих устройств в сети.



LLDP (802.1ab)

Включаем поддержку LLDP

enable lldp

Задаём интервал отсылки пакетов

config lldp message_tx_interval 30

Задаём работу в режиме приёма и отправки

config lldp ports 1-28 admin_status tx_and_rx

Задаём какие дополнительные параметры будут добавляться в LLDP пакет

config lldp ports 1-28 basic_tlvs port_description system_name system_description system_capabilities enable

LLDP (802.1ab)

Пример отображения LLDP информации об удалённом устройстве

•DES- •Comm	3028:4#show lldp remote_ports 24 hand: show lldp remote_ports 24	
•Port	ID : 24	
•Remo •Enti •	<pre>bte Entities Count : 1 .ty 1 Chassis Id Subtype Chassis Id Port Id Subtype Port ID Port Description System Name System Description System Capabilities Management Address Count Port PVID PPVID Entries Count</pre>	 MAC Address 00-15-E9-AC-D7-EB Local 1/24 DES-3526 port 24 descr D-Link Fast Ethernet Switch Repeater, Bridge 0 0



6.4 Super VLAN



- Позволяет собрать несколько клиентских vlan на одном L3 интерфейсе, который является шлюзом (gateway) для хостов.
- Удобно при реализации схемы «vlan на пользователя».
- Экономится адресное пространство пользователи, находящиеся в разных L2 сегментах (каждый в отдельном vlan), находятся в одной L3 сети (у всех адрес из одной подсети, к примеру – 192.168.0.0/24) – нет необходимости на каждого выделять свою подсеть и шлюз.
- Механизм Proxy ARP позволяет хостам различных клиентских vlan общаться между собой через шлюз.
- Работает совместно в DHCP Relay

Пример использования Super VLAN

• Коммутатор А:

config vlan default delete 1-24
create vlan v100 tag 100
config vlan v100 add tagged 1
create vlan v200 tag 200
config vlan v200 add tagged 2
create vlan sv1000 tag 1000
create super_vlan sv1000
config super_vlan sv1000 add sub_vlan 100
config super_vlan sv1000 add sub_vlan 200
config super_vlan sv1000 add ip_range 192.168.0.2 to 192.168.0.127
config sub_vlan v200 add ip_range 192.168.0.128 to 192.168.0.254
create ipif svi1000 192.168.0.1/24 sv1000 state enable

- Трафик с DES-3200 тегирован
- Пользователи v100 и v200 находяится в разных vlan, но имеют один шлюз по умолчанию – svi1000





Спасибо!

