Основные понятия, функции и настройки управляемых коммутаторов

На примере коммутаторов D-Link DXS-3326GSR, DES-3526

Ver. 2.4

Содержание:

1. Понятие коммутаторов

Основы

Коммутатор Ethernet представляет собой устройство для организации сетей большого размера. Для того, чтобы лучше разобраться в устройстве и работе коммутаторов Ethernet, полезно понять основы технологии организации кабельных систем сети.

Повторители

В начале 80-х годов сети Ethernet организовывались на базе шинной топологии с использованием сегментов на основе коаксиального кабеля длиной до 500 метров. Увеличение размеров сетей поставило задачу преодоления 500-метрового барьера. Для решения этой задачи использовались повторители (repeater):

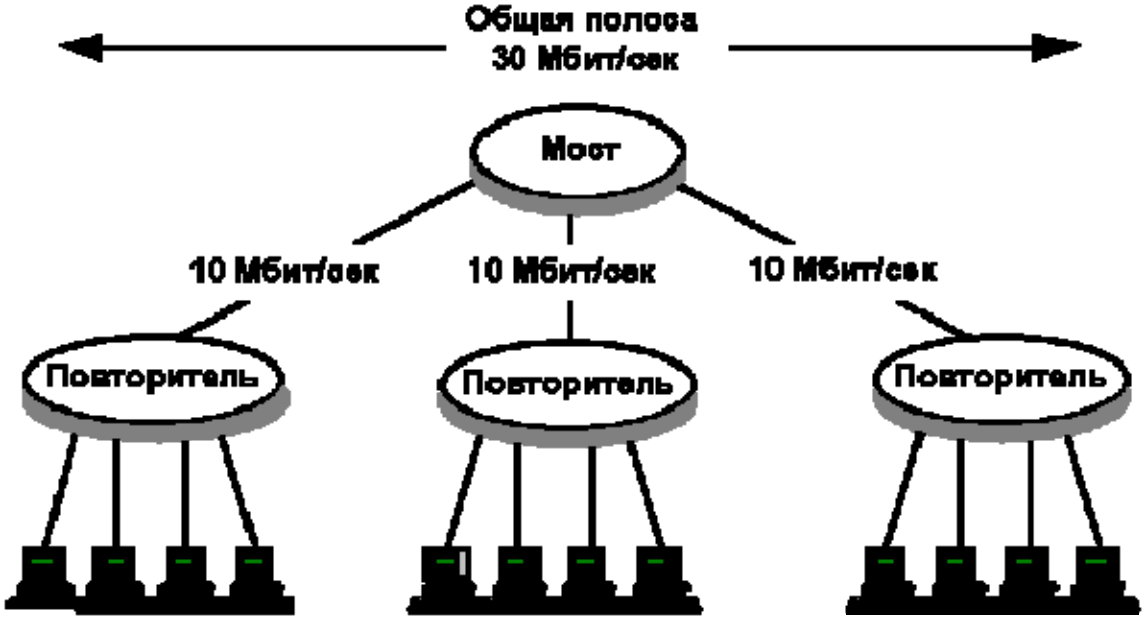
Повторитель просто копирует (пересылает) все пакеты Ethernet из одного сегмента во все другие, подключенные к нему. Основной задачей повторителя является восстановление электрических сигналов для передачи их в другие сегменты. За счет усиления и восстановления формы электрических сигналов повторителем становится возможным расширение сетей, построенных на основе коаксиального кабеля и увеличение общего числа пользователей сети

Мосты и маршрутизаторы

При использовании повторителей максимальная протяженность сети составляет 2500 метров. Для преодоления этого ограничения требуются другие устройства, называемые мостами (bridge). Мосты имеют много отличий от повторителей. Повторители передают все пакеты, а мосты только те, которые нужно. Если пакет не нужно передавать в другой сегмент, он фильтруется. Для мостов существуют многочисленные алгоритмы (правила) передачи и фильтрации пакетов минимальным требованием является фильтрация пакетов по адресу получателя.

Другим важным отличием мостов от повторителей является то, что сегменты, подключенные к повторителю образуют одну разделяемую среду, а сегменты, подключенные к каждому порту моста образуют свою среду с полосой 10 Mbps. При использовании моста пользователи одного сегмента разделяют полосу, а пользователи разных сегментов используют независимые Среды. Следовательно, мост обеспечивает преимущества как с точки зрения расширения сети, так и обеспечения большей полосы для каждого пользователя.

Поначалу в сетях Ethernet использовалась шинная топология на основе коаксиального кабеля, а для расширения сетей применялись 2-х портовые повторители или мосты. Однако, в конце 80-х годов началось широкое распространение сетей на основе кабеля со скрученными парами проводников (витая пара). Новая технология 10Base-T стала очень популярной и привела к трансформации топологии сетей от шинной магистрали к организации соединений типа "звезда". Требования к повторителям и мостам для таких сетей существенно изменились по сравнению с простыми двухпортовыми устройствами для сетей с шинной топологией - современные мосты и повторители представляют собой сложные многопортовые устройства. Мосты позволяют сегментировать сети на меньшие части, в которых общую среду разделяет небольшое число пользователей.



Маршрутизаторы, подобно мостам, также позволяют сегментировать сети Ethernet. маршрутизаторы фильтруют и пересылают сетевой трафик на основе алгоритмов и правил, существенно отличающихся от тех, что используются мостами. Такой способ сегментирования сетей более дорог многопортовые мосты и маршрутизаторы обычно стоят около $1,000 за порт.

Переключение портов

Сегодняшние модульные концентраторы (повторители) часто позволяют организовать несколько сегментов, каждый из которых предоставляет пользователям отдельную разделяемую полосу 10 Mbps. Некоторые концентраторы позволяют программным путем разделять порты устройства на независимые сегменты такая возможность называется переключением портов. Концентратор, к примеру, может содержать три различных сегмента Ethernet, организуемые внутренними

средствами хаба. Переключение портов обеспечивает администратору сети высокую гибкость организации сегментов, позволяя переносить порты из одного сегмента в другой программными средствами. Эта возможность особенно полезна для распределения нагрузки между сегментами Ethernet и снижения расходов, связанных с подобными операциями. Переключение портов статическое связывание портов с различными сегментами Ethernet - сильно отличается от описанной ниже коммутации Ethernet.

Атрибуты коммутаторов Ethernet

Коммутаторы Ethernet подобно мостам и маршрутизаторам способны сегментировать сети Ethernet. Как и многопортовые мосты коммутаторы передают пакеты между портами на основе адреса получателя, включенного в каждый пакет. реализация коммутаторов обычно отличается от мостов в части возможности организации одновременных соединений между любыми парами портов устройства - это значительно расширяет суммарную пропускную способность сети. Более того, мосты в соответствии со стандартом IEEE 802.1d должны получить пакет целиком до того, как он будет передан адресату, а коммутаторы могут начать передачу пакета, не приняв его полностью.

Виртуальные соединения

Коммутатор Ethernet поддерживает внутреннюю таблицу, связывающую порты с адресами подключенных к ним устройств (таблица 1). Эту таблицу администратор сети может создать самостоятельно или задать ее автоматическое создание средствами коммутатора.

Таблица 1

MAC-адрес	Номер порта
A	1
B	2
C	3
D	4

Используя таблицу адресов и содержащийся в пакете адрес получателя, коммутатор организует виртуальное соединение порта отправителя с портом получателя и передает пакет через это соединение. На рисунке 4 узел A посылает пакет узлу D. Найдя адрес получателя в своей внутренней таблице, коммутатор передает пакет в порт 4.

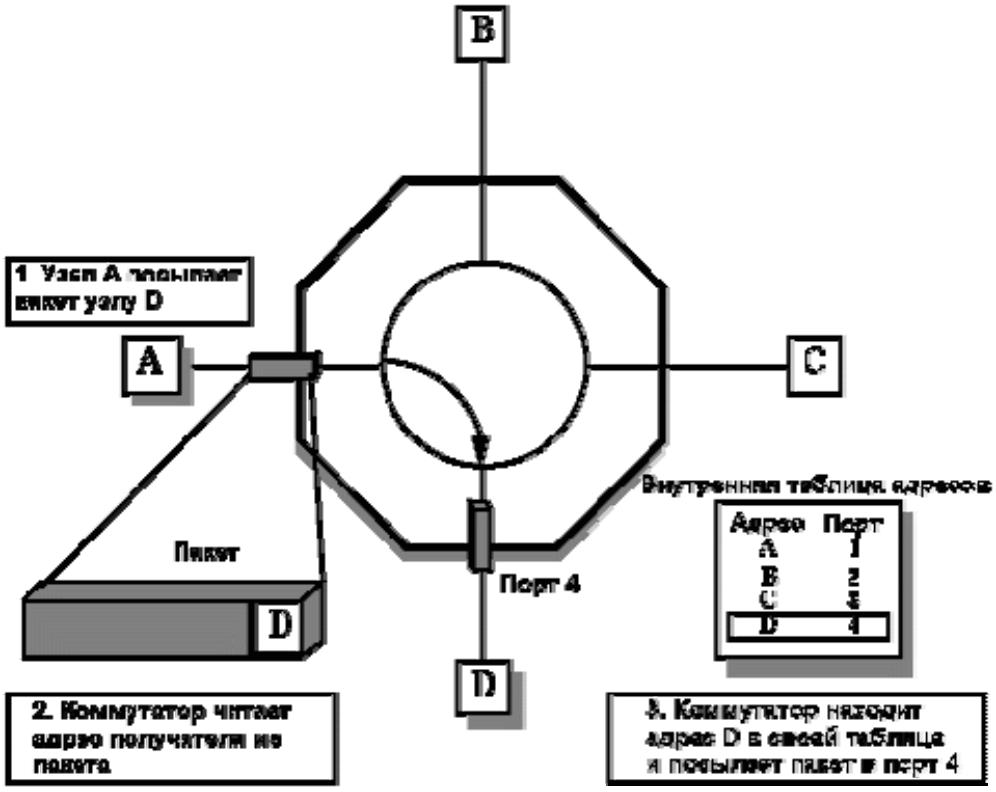


Рисунок 4

Виртуальное соединение между портами коммутатора сохраняется в течение передачи одного пакета, т.е. для каждого пакета виртуальное соединение организуется заново на основе содержащегося в этом пакете адреса получателя.

Поскольку пакет передается только в тот порт, к которому подключен адресат, остальные пользователи (в нашем примере - B и C) не получат этот пакет. Таким образом, коммутаторы обеспечивают средства безопасности, недоступные для стандартных повторителей Ethernet (см. раздел "Сравнение сетевых устройств").

Одновременные соединения

В коммутаторах Ethernet передача данных между любыми парами портов происходит независимо и, следовательно, для каждого виртуального соединения выделяется вся полоса канала. Например, коммутатор 10 Mbps на рисунке 5 обеспечивает одновременную передачу пакета из A в D и из порта B в порт C с полосой 10 Mbps для каждого соединения.

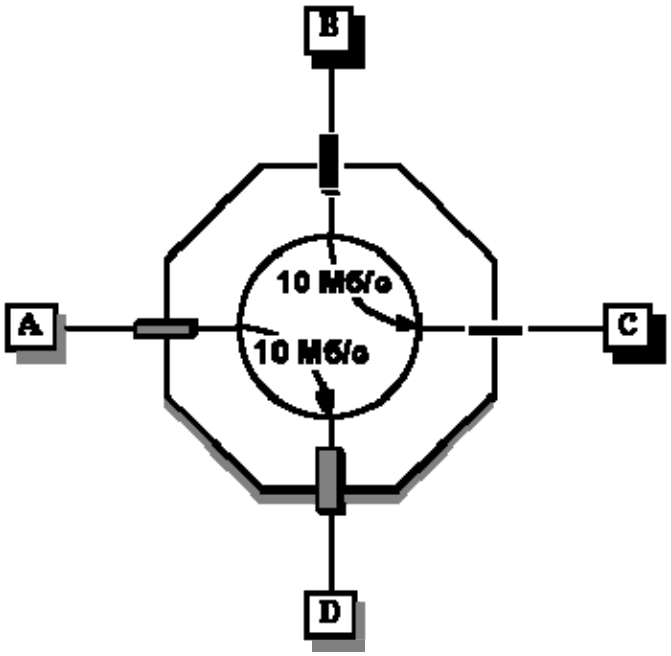


Рисунок 5

Поскольку для каждого соединения предоставляется полоса Mbps, суммарная пропускная способность коммутатора в приведенном примере составляет 20 Mbps. Если данные передаются между большим числом пар портов, интегральная полоса соответственно расширяется. Например, 24 портовый коммутатор Ethernet может обеспечивать интегральную пропускную способность до 120 Mbps при одновременной организации 12 соединений с полосой 10 Mbps для каждого из них. теоретически, интегральная полоса коммутатора растет пропорционально числу портов. Однако, в реальности скорость пересылки пакетов, измеренная в Mbps, меньше чем суммарная полоса пар портов за счет так называемой внутренней блокировки. Для коммутаторов высокого класса блокировка весьма незначительно снижает интегральную полосу устройства.

Коммутатор Ethernet 10 Mbps может обеспечить высокую пропускную способность при условии организации одновременных соединений между всеми парами портов. Однако, в реальной жизни трафик обычно представляет собой ситуацию "один ко многим" (например, множество пользователей сети обращается к ресурсам одного сервера). В таких случаях пропускная способность коммутатора в нашем примере не будет превышать 10 Mbps, и коммутатор не обеспечит существенного преимущества по сравнению с обычным концентратором (повторителем).

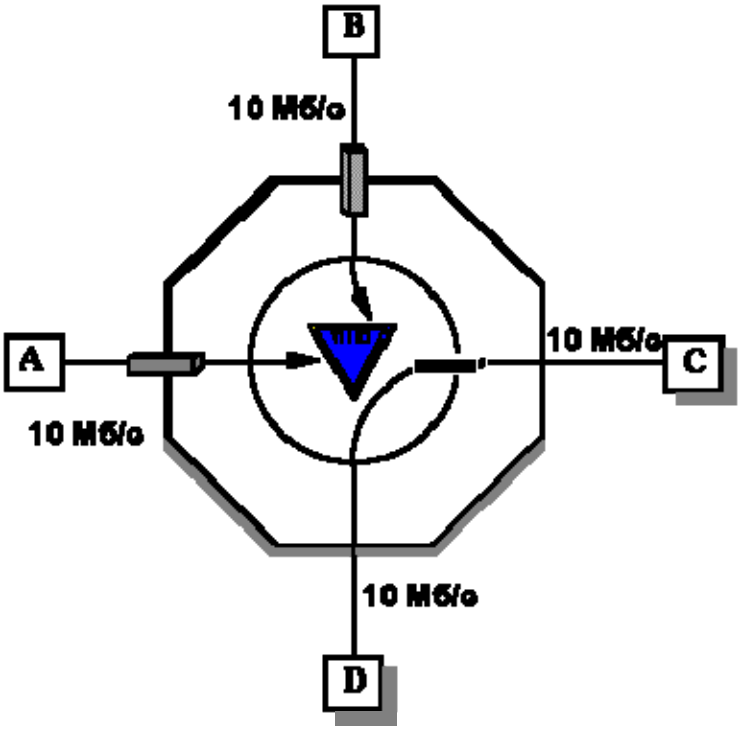


Рисунок 6

На рисунке 6 три узла A, B и D передают данные узлу C. Коммутатор сохраняет пакеты от узлов A и B в своей памяти до тех пор, пока не завершится передача пакета из узла D. После завершения передачи пакета коммутатор начинает передавать хранящиеся в памяти пакеты от узлов A и B. В данном случае пропускная способность коммутатора определяется полосой канала C (в данном случае 10 Mbps). Описанная в данном примере ситуация является другой формой блокировки.

Производительность коммутатора

Другим важным параметром коммутатора является его производительность. Для того, чтобы охарактеризовать ее используются несколько параметров:

1. скорость передачи между портами
2. общая пропускная способность
3. задержка

Скорость передачи между портами

При полосе 10 Mbps Ethernet может передавать 14880 пакетов в секунду (PPS) для пакетов минимального размера (64 байта). Этот параметр определяется свойствами среды. Коммутатор, который способен обеспечить скорость 14880 PPS между портами, полностью использует возможности среды. Полоса пропускания среды является важным параметром, поскольку коммутатор, обеспечивающий передачу пакетов с такой скоростью, полностью использует возможности среды, предоставляя пользователям максимальную полосу.

Общая пропускная способность

Измеренная в Mbps или PPS, общая пропускная способность характеризует максимальную скорость, с которой пакеты могут передаваться через коммутатор адресатам. В коммутаторах, все порты которых имеют полосу 10 Mbps суммарная пропускная способность равна скорости порта,

умноженной на число виртуальных соединений, которые могут существовать одновременно (число портов коммутатора, поделенное на 2). Коммутатор, способный обеспечивать максимальную скорость передачи не имеет внутренней блокировки.

Задержка

Задержка - это промежуток времени между получением пакета от отправителя и передачей его получателю. Обычно задержку измеряют относительно первого бита пакета.

Коммутаторы Ethernet могут обеспечивать очень низкую задержку после того, как будет определен адресат. Поскольку адрес получателя размещается в начале пакета, передачу можно начать до того, как пакет будет полностью принят от отправителя. Такой метод называется коммутацией на лету (cut-through) и обеспечивает минимальную задержку. Малая задержка важна, поскольку с ней непосредственно связана производительность коммутатора. Однако метод коммутации на лету не проверяет пакеты на предмет ошибок.

При таком способе коммутатор передает все пакеты (даже те, которые содержат ошибки). Например, при возникновении коллизии после начала передачи пакета (адрес уже получен) полученный фрагмент все равно будет передан адресату. Передача таких фрагментов занимает часть полосы канала и снижает общую производительность коммутатора.

При передаче пакетов из низкоскоростного порта в высокоскоростной (например, из порта 10 Mbps в порт 100 Mbps) коммутацию на лету использовать вообще невозможно. Поскольку порт-приемник имеет большую скорость, нежели передатчик, при использовании коммутации на лету неизбежно возникнут ошибки. При организации виртуального соединения между портами с разной скоростью требуется буферизация пакетов.

Малая задержка повышает производительность сетей, в которых данные передаются в виде последовательности отдельных пакетов, каждый из которых содержит адрес получателя. В сетях, где данные передаются в форме последовательности пакетов с организацией виртуального канала, малая задержка меньше влияет на производительность.

В чем отличие НАСТРАИВАЕМЫХ, НЕУПРАВЛЯЕМЫХ и УПРАВЛЯЕМЫХ коммутаторов?

Настраиваемые коммутаторы - это коммутаторы, которые позволяют пользователю производить некоторые настройки, например конфигурирование VLAN. Могут быть и управляемыми и неуправляемыми. Пример неуправляемых, но настраиваемых коммутаторов - серия DES-12xx.

Неуправляемые коммутаторы - коммутаторы, которые не поддерживают управление по протоколам сетевого управления как SNMP. При этом неуправляемуе коммутаторы могут быть настраиваемыми. Неуправляемые и ненастраиваемые коммутаторы это DES-1005, DES-1008 и т.п.

Управляемые коммутаторы поддерживают протоколы сетевого управления и могут управляться по сети с использованием специального программного обеспечения как D-Link DView, HP Openview. К ним относятся DES-21xx, DES-3xxx и выше, DGS-3xxx и выше.

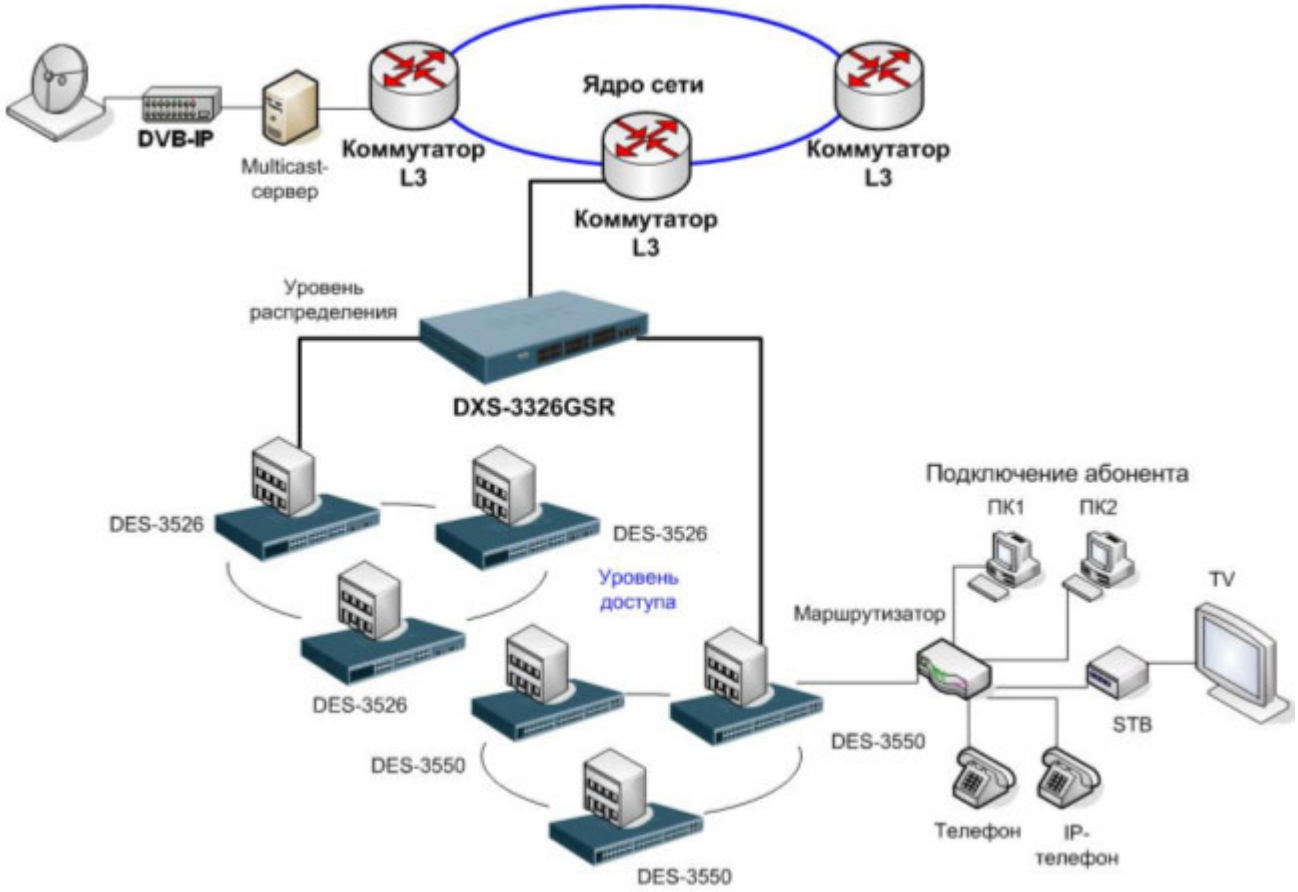
2. Основные функции коммутаторов L2 уровня доступа DES-3526:

Коммутаторы серии DES-3526 являются полнофункциональными устройствами L2 в линейке оборудования D-Link и предназначены для использования в качестве устройств уровня доступа в корпоративных сетях или сетях провайдеров услуг (ISP), где необходим основной функционал канального уровня и расширенные функции безопасности и управления.

Характеристики серии:

1. Наличие 2-х встроенных гигабитных комбо-портов;
2. 24/48 пользовательских портов 10/100 Мбит/с;
3. Статическая и динамическая привязка MAC-адреса к порту (Static MAC Function и Port Security) и логирование блокировки неразрешённых MAC-адресов;
4. Авторизация 802.1x (Radius) – на основе портов и MAC-адресов;
5. Привязка IP-адреса к MAC-адресу и к порту (IP-MAC-Port Binding), режимы ACL и ARP – http://www.dlink.ru/technical/pdf/hub_switch/FAQ_IP_MAC_Port_Binding.pdf ;
6. Механизм определения петель в неуправляемых сегментах за портами коммутатора (LoopBack Detection);
7. Расширенные средства работ с Multicast (IGMP Snooping v.3, D-Link ISM VLAN) - http://www.dlink.ru/technical/faq_hub_switch_54.php , http://www.dlink.ru/technical/faq_hub_switch_69.php , http://www.dlink.ru/technical/faq_hub_switch_84.php ;
8. Расширенные ACL (Access Control Lists) с привязкой по портам;
9. CPU Interface Filtering – ACL на интерфейс CPU - http://www.dlink.ru/technical/faq_hub_switch_78.php ;
10. SafeGuard Engine – механизм регулирования обработки ARP-пакетов - http://www.dlink.ru/technical/faq_hub_switch_77.php ;
11. Поддержка протокола MSTP – Multiple Spanning Tree Protocol – возможность функционирования нескольких копий протокола RSTP в сети, разбитой на VLAN-ы.
12. Расширенный механизм QoS – 4 очереди приоритета на порт, два механизма обработки очередей – строгий (strict priority) и круговой взвешенный (WRR – weighted round robin), поддержка TOS, DSCP, возможность перемаркировки трафика при помощи ACL (один 802.1p priority в другой, один DSCP приоритет в другой, 802.1p в DSCP, DSCP в 802.1p);
13. Поддержка DHCP Relay Option 82 – http://www.dlink.ru/technical/faq_hub_switch_72.php ;
14. Управление через CLI, telnet, WEB, SSH, SSL, SNMP v.1, v.2, v.3;
15. Поддержка технологии виртуального стекирования SIM (Single IP Management).

Схема применения в сетях провайдеров услуг:



Сервисы, применяемые в таких сетях:

- Передача данных
- VoIP (голос по IP-сетям)
- IP TV (телевидение по IP-сетям)
- VoD (видео по требованию)
- MoD (мультимедиа-контент по требованию)

Коммутаторы серии DES-35XX отвечают всем современным требованиям безопасности, благодаря наличию функций ACL, Port Security, IP-MAC-Port Binding (ACL и ARP режимы), 802.1x авторизации, аутентификации доступа и т.д.

Расширенная поддержка передачи Multicast-трафика (ISM VLAN, IGMP Snooping, Per Port Multicast Filtering), а также полная поддержка QoS, включая и перемаркировку трафика, позволяет применять эту серию в качестве устройств уровня доступа в сетях Triple Play.

Поддержка функции SafeGuard Engine позволяет настроить эффективную защиту от ARP Spoofing-а, например.

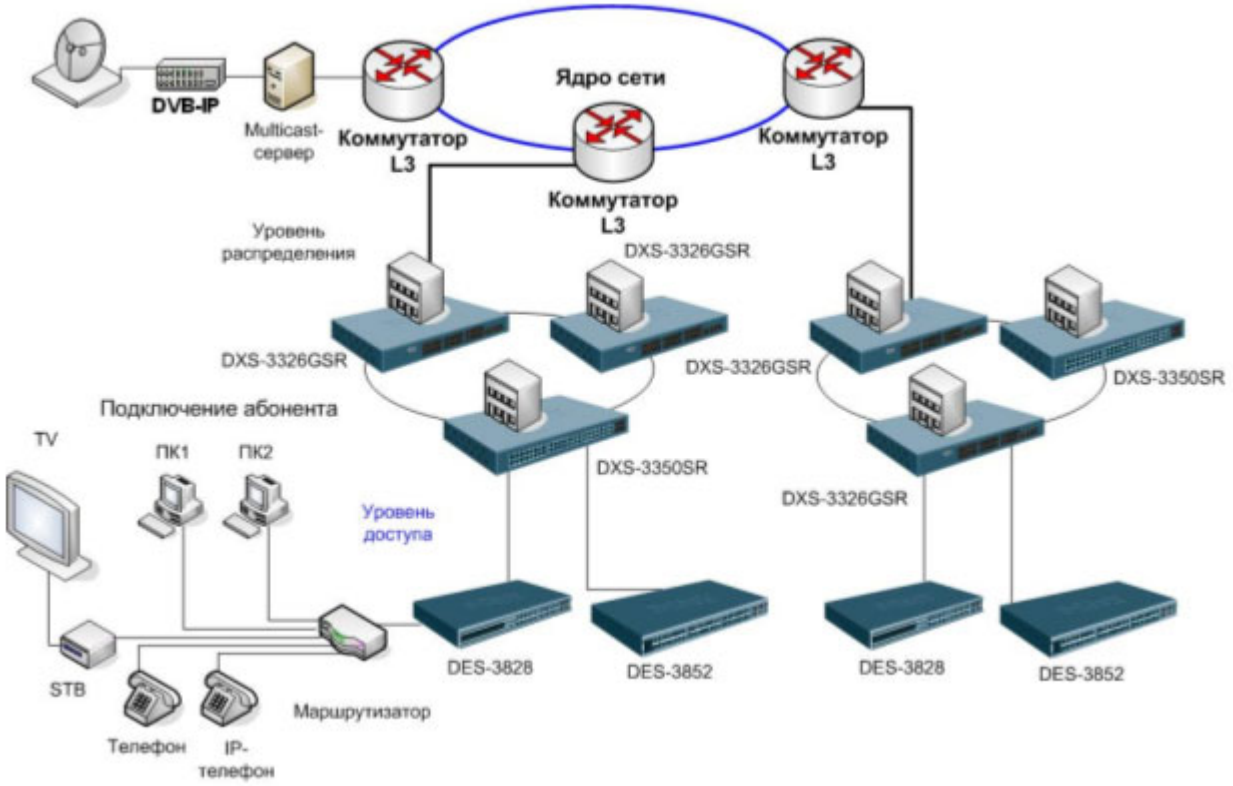
3. Основные функции коммутаторов L3 уровня доступа DES-3326GSR:

Коммутатор может применяться в качестве устройства уровня доступа при необходимости локальной маршрутизации, а также в качестве начального решения уровня распределения в корпоративных сетях и сетях провайдеров услуг.

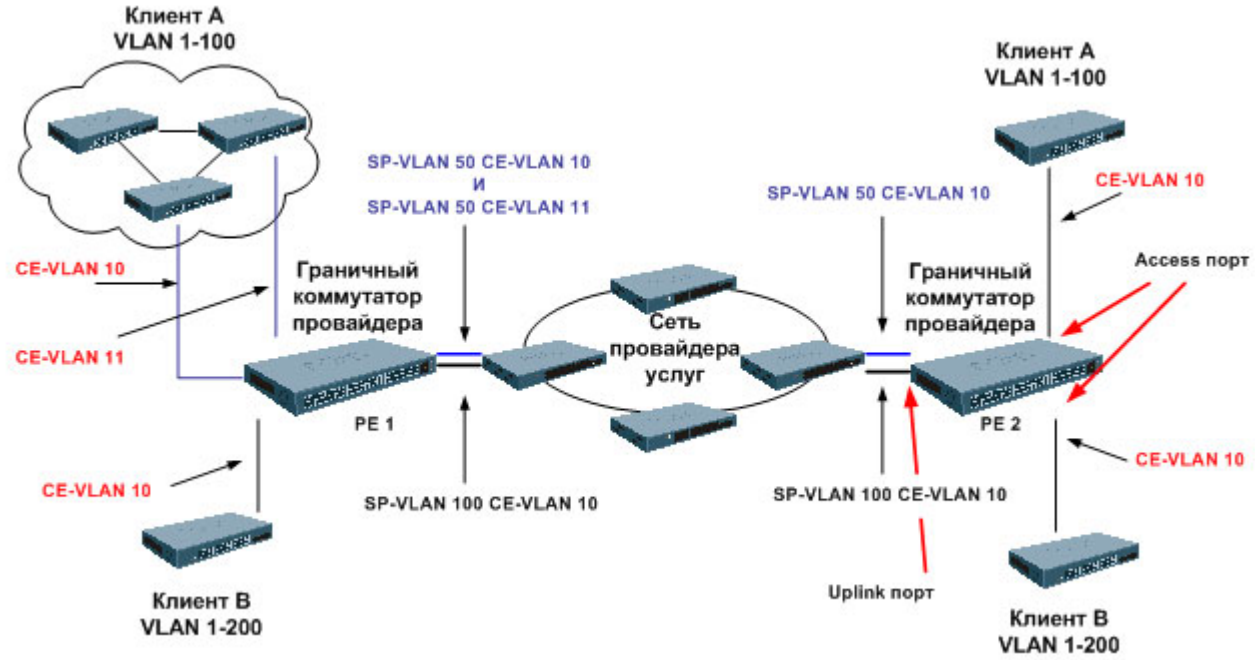
Характеристики серии:

1. Наличие 24-х встроенных оптических гигабитных портов и 4-х комбо-портов 1000Base-T на передней панели;
2. 24/48 пользовательских порта 10/100/1000 Мбит/с;
3. Контроль полосы пропускания на всех портах с шагом 64 Кбит/с;
4. Статическая и динамическая привязка MAC-адреса к порту (Static MAC Function и Port Security) и логирование блокировки неразрешённых MAC-адресов;
5. Авторизация 802.1x (Radius)– на основе портов и MAC-адресов;
6. Привязка IP-адреса к MAC-адресу (IP-MAC Binding);
7. Расширенный механизм QoS – 8 очередей приоритетов на порт, два механизма обработки очередей – строгий (strict priority) и круговой взвешенный (WRR – weighted round robin), возможность перемаркировки трафика при помощи ACL (один 802.1p priority в другой, один DSCP приоритет в другой, 802.1p в DSCP, DSCP в 802.1p);
8. Механизм определения петель в неуправляемых сегментах за портами коммутатора (LoopBack Detection);
9. Расширенные средства работы с Multicast (IGMP Snooping v.3, IGMP v.1 v.2 v.3) – http://www.dlink.ru/technical/faq_hub_switch_54.php, http://www.dlink.ru/technical/faq_hub_switch_69.php;
10. Маршрутизация Multicast-трафика (DVMRP, PIM DM) – http://www.dlink.ru/technical/faq_hub_switch_85.php ;
11. Расширенные ACL (Access Control Lists) с привязкой по портам;
12. CPU Interface Filtering – ACL на интерфейс CPU - http://www.dlink.ru/technical/faq_hub_switch_78.php ;
13. SafeGuard Engine – механизм регулирования обработки ARP-пакетов - http://www.dlink.ru/technical/faq_hub_switch_77.php ;
14. Поддержка DHCP Relay Option 82 – http://www.dlink.ru/technical/faq_hub_switch_72.php ;
15. Протоколы маршрутизации IP-трафика (RIP v1 v2, OSPF);
16. Поддержка Q-in-Q (Double VLAN) – http://www.dlink.ru/technical/faq_hub_switch_86.php ;
17. Маршрутизация IP v.6;
18. Поддержка VRRP (резервирование соединений на третьем уровне).
19. Поддержка WAC (WEB Access Control) – авторизация пользователей в сети через WEB – http://www.dlink.ru/technical/faq_hub_switch_88.php ;
20. Управление через CLI, telnet, WEB, SSH, SSL, SNMP v.1, v.2, v.3;
21. Поддержка технологии виртуального стекирования SIM (Single IP Management).

Схема применения в сетях провайдеров услуг в качестве устройства уровня доступа:



Коммутаторы серии DES-33XX благодаря поддержки технологии Double VLAN (Q-in-Q) позволяют более эффективно использовать пространство номеров VLAN (VLAN ID) в крупных сетях провайдеров.



Сервисы, применяемые в таких сетях:

- Передача данных
- VoIP (голос по IP-сетям)
- IP TV (телевидение по IP-сетям)
- VoD (видео по требованию)
- MoD (мультимедиа-контент по требованию)

Коммутаторы серии DES-38XX обладают всем необходимым функционалом в области безопасности (ACL, Port Security, IP-MAC Binding, 802.1x авторизации, Guest VLAN, WAC, аутентификации доступа и т.д.) для организации производительного уровня доступа или распределения при необходимости локальной маршрутизации (поддержка RIP v.1, v.2, OSPF v.2).

Расширенная поддержка передачи и маршрутизации Multicast-трафика (IGMP Snooping, Per Port Multicast Filtering, IGMP v.3, PIM-DM, DVMRP), а также полная поддержка QoS, включая и перемаркировку трафика, позволяет применять эту серию в качестве устройств уровня доступа в сетях Triple Play.

Аппаратная поддержка функции SafeGuard Engine позволяет настроить эффективную защиту от ARP Spoofing-а, например.

Коммутаторы серии DES-33XX обладают всем необходимым функционалом в области безопасности (ACL, Port Security, IP-MAC Binding, 802.1x авторизации, Guest VLAN, WAC, аутентификации доступа и т.д.) для организации производительного уровня доступа или при необходимости локальной маршрутизации (поддержка RIP v.1, v.2, OSPF v.2).

4. Настройка коммутаторов D-Link DXS-3326GSR, DES-3526:

Настройка коммутаторов производится в 3 этапа:

1. – Настройка IP адреса, шлюза, пароля;
2. – Добавление комментариев местонахождения и серийного номера коммутатора;
3. – Обновление прошивки и конфигурации.

Примечание: Проверить общие настройки коммутатора можно при помощи команды:
Command: show switch

Device Type	: DES-3526 Fast-Ethernet Switch
Combo Port Type	: 1000Base-T + 1000Base-T
MAC Address	: 00-13-46-98-CE-2C
IP Address	: **10.100.1.1** (Manual)
VLAN Name	: **management** - *в каком VLAN`не расположен менеджмент коммутатора*
Subnet Mask	: 255.255.0.0
Default Gateway	: **10.100.0.17** – *шлюз по умолчанию*
Boot PROM Version	: Build 3.00.005
Firmware Version	: **Build 4.01-B34** – *версия прошивки*
Hardware Version	: 3A1
Device S/N	:
Power Status	: Main - Normal, Redundant - Not Present
System Name	: **1:100/1.0#1-DRxxxxxxxxxx** – *номер точки…*
System Location	: **Ryazanskiy_pr-t_30/15** – *физическое месторасположение*
System Contact	: **v2.10** – *версия конфига*
Spanning Tree	: Enabled
GVRP	: Disabled
IGMP Snooping	: Disabled
TELNET	: Enabled (TCP 23)
SSH	: Disabled
WEB	: Disabled (TCP 80)
RMON	: Disabled

4.1. Настройка IP адреса, шлюза, пароля:

Ниже приводится пошаговый пример того, как это можно сделать:

1. Настройка IP адреса:

Command: config ipif **System** ipaddress 10.100.1.1/16

Примечание: Для проверки имени и количества интерфейсов:
Command: show ipif

IP Interface Settings

Interface Name : **System**
IP Address : 10.100.1.1
Subnet Mask : 255.255.0.0
VLAN Name : default
Admin. State : Enabled
Link Status : Link UP
Member Ports : 1-26

Total Entries : 1

2. Настройка шлюза по умолчанию:

Command: create iproute default **10.100.0.17**

Примечание: Для проверки маршрута по умолчанию:
Command: show iproute

Routing Table

IP Address/Netmask	Gateway	Interface	Hops	Protocol
0.0.0.0	**10.100.0.17**	System	1	Default
10.100.0.0/16	0.0.0.0	System	1	Local

Total Entries : 2

2.1. В случае, если маршрут по умолчанию был прописан ранее и требуется его изменить:

Command: delete iproute default

далее повторить п.2

3. Настройка имени пользователя и пароля:

Command: create account admin admin

уровень доступа ↔ имя пользователя

Enter a case-sensitive new password:********
Enter the new password again for confirmation:********

ВНИМАНИЕ!!!

Настройка имени пользователя и пароля производится строго в соответствии с внутренними правилами компании!

Примечание: Проверить наличие учетной записи вы можете при помощи команды:
Command: show account

Current Accounts:
Username Access Level
--- ---
admin Admin

Total Entries : 1

3.1. В случае, если пользователь уже существует и требуется только сменить пароль:
Command: config account admin

Enter a old password:********
Enter a case-sensitive new password:********
Enter the new password again for confirmation:********

ВНИМАНИЕ!!!

Настройка имени пользователя и пароля производится строго в соответствии с внутренними правилами компании!

4. Сохранение конфигурации:
Command: save

Saving all configurations to NV-RAM... Done.

4.2. Добавление комментариев местонахождения и серийного номера коммутатора:

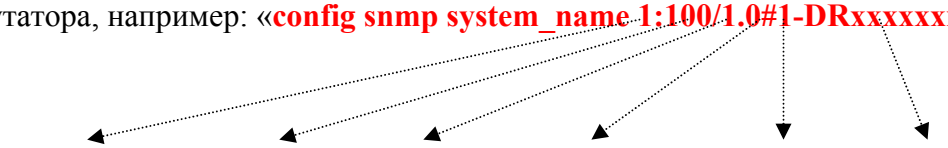
Ниже приводится пошаговый пример того, как это можно сделать:

1. Добавление комментария о физическом местонахождении коммутатора:
   Command: config snmp system_location <sw_location>

   <sw_location> - полный физический адрес местоположения коммутатора, например: «**config snmp system_location Ryazanskiy_pr-t_30/15**»

2. Добавление комментария о порядковом номере точки, а также серийного номера коммутатора:
   Command: config snmp system_name <sw_name>

   <sw_name> - номер точки по топологии + порядковый номер коммутатора + серийный номер коммутатора, например: «**config snmp system_name 1:100/1.0#1-DRxxxxxxxxxxx**»



№ района / № подсети / № сегмента / № точки / № коммутатора / серийный номер

3. Добавление комментария к порту:
   Command: config ports 26 description <desc 32>

   <desc 32> - ваш комментарий (не должен превышать 32 символа и не должен содержать пробелы), например: «**config ports 26 description UPLINK!!!->10.100.0.17**»

4.3. Обновление прошивки и конфигурации:

Ниже приводится пошаговый пример того, как это можно сделать:

1. Обновление прошивки:

1.1. Загрузка новой прошивки для коммутатора DES-3326GSR:

Command: download firmware_fromTFTP 85.21.79.12 dxs3326_430b11.had image_id **2**

Connecting to server..... Done.
Download firmware..... Done. Do not power off!
Delete image..... Done.
Please wait, programming flash.. Done.

Примечание: Для определения прошивки по умолчанию
Command: show firmware information

ID	Version	Size(B)	Update Time	From	User
*1	4.01-B34	2746312	00000 days 00:00:00	Serial Port (PROM)	Unknown
2	4.01-B31	2737545	00008 days 17:42:50	85.21.79.12(T)	Unknown

'*' means boot up section
(T) means firmware update through TELNET
(S) means firmware update through SNMP
(W) means firmware update through WEB
(SIM) means firmware update through Single IP Management

Free space: 2621440 bytes

1.2. Загрузка новой прошивки для коммутатора DES-3526:

Command: download firmware 85.21.79.12 des3526_401b19.had image_id **1**

Connecting to server..... Done.
Download firmware..... Done. Do not power off!
Delete image..... Done.
Please wait, programming flash.. Done.

Примечание: Для определения прошивки по умолчанию
Command: show firmware information

ID	Version	Size(B)	Update Time	From	User
1	4.01-B34	2746312	00000 days 00:00:00	Serial Port (PROM)	Unknown
*2	4.01-B31	2737545	00008 days 17:42:50	85.21.79.12(T)	Unknown

'*' means boot up section
(T) means firmware update through TELNET
(S) means firmware update through SNMP
(W) means firmware update through WEB
(SIM) means firmware update through Single IP Management

Free space: 2621440 bytes

1.3. Настройка с какой прошивкой коммутатор будет загружаться:
Command: config firmware image_id <int 1-2> boot_up

<int 1-2> - это порядковый номер image_id загруженной ранее прошивки

1.4. Сохранение конфигурации:
Command: save

Saving all configurations to NV-RAM... Done.

1.5. Перезагрузка коммутатора для применения изменений:
Command: reboot

Are you sure to proceed with the system reboot?(y/n)y

2. Обновление конфигурации коммутатора:

2.1. Загрузка конфигурационного файла для коммутатора DXS-3326GSR:
Command: download cfg_fromTFTP 85.21.79.12 <filename_on_TFTP> increment

ВНИМАНИЕ!!!

Не забывайте писать INCREMENT, т.к. он предполагает изменение только тех настроек конфигурации, которые явно указаны в загружаемом файле. Не использование данной переменной предполагает изменение всех настроек конфигурации системы, что может привести к сбросу всех остальных настроек в системе, которые явно не указаны в загружаемом файле, к примеру IP адреса и шлюза!

2.2. Загрузка конфигурационного файла для коммутатора DES-3526:
Command: download configuration 85.21.79.12 <filename_on_TFTP> increment

ВНИМАНИЕ!!!

Не забывайте писать INCREMENT, т.к. он предполагает изменение только тех настроек конфигурации, которые явно указаны в загружаемом файле. Не использование данной переменной предполагает изменение всех настроек конфигурации системы, что может привести к сбросу всех остальных настроек в системе, которые явно не указаны в загружаемом файле, к примеру IP адреса и шлюза!

2.3. Сохранение конфигурации:
Command: save

Saving all configurations to NV-RAM... Done.

5. Дополнительные возможности коммутаторов D-Link DXS-3326GSR и DES-3526:

1. Детальный просмотр конфигурации коммутатора:

1.1. Детальный просмотр текущей конфигурации коммутатора:
Command: show config current_config

1.2. Детальный просмотр сохраненной конфигурации коммутатора:
Command: show config config_in_nvram

2. Просмотр статистики по портам:

2.1. Общая статистика по портам:
Command: show utilization ports

Port	TX/sec	RX/sec	Util	Port	TX/sec	RX/sec	Util
1	969	0	1	22	0	0	0
2	0	0	0	23	0	0	0
3	0	0	0	24	0	0	0
4	969	0	1	25	0	0	0
5	0	0	0	26	0	968	1
6	0	0	0				
7	0	0	0				
8	0	0	0				
9	0	0	0				
10	0	0	0				
11	0	0	0				
12	0	0	0				
13	0	0	0				
14	0	0	0				
15	0	0	0				
16	0	0	0				
17	0	0	0				
18	0	0	0				
19	0	0	0				
20	0	0	0				
21	0	0	0				

3. Настройка VLAN:

В данном примере рассматривается возможность подключения юридического лица (точка-точка) методом проброса до ТКД клиента отдельного VLAN, при этом обычные домашние пользователи должны работать в другом VLAN.

VLAN 955 – management (пользователи)
VLAN 848 – marka-p2p (юридическое лицо)

На УЗЛЕ:
- Порт ТКД на узле расположен в 2 порту коммутатора;

На ТКД:
- UPLINK располагается в 26 порту коммутатора;
- Юридическое лицо расположено в 11 порту;

3.1. Создаем новый VLAN для домашних пользователей:
Command: create vlan management tag 955

3.2. Создаем новый VLAN для юридического лица:
Command: create vlan marka-p2p tag 848

3.3. Добавляем в TAGGED порты наших домашних пользователей, а также добавляем приходящий порт (UPLINK).
Command: config vlan management add tagged 1-10,12-26

3.4. Добавляем в TAGGED порты нашего юридического лица, а также добавляем приходящий порт (UPLINK).
Command: config vlan marka-p2p add tagged 11,26

3.5. Настраиваем менеджмент коммутатора в нужном нам VLAN`не:
Command: config ipif System vlan management ipaddress 10.100.1.1/16 state enable

3.6. Выставляем порт ТКД на узле в TAGGED для VLAN management:
Command: config vlan management add tagged 2

3.7. Освобождаем все порты из Default VLAN:
Command: config vlan default delete 1-26

3.8. Добавляем в UNTAGGED порты наших домашних пользователей:
Command: config vlan management add untagged 1-10,12-25

3.9. Добавляем в UNTAGGED порты нашего юридического лица:
Command: config vlan marka-p2p add untagged 11

3.10. Сохраняем конфигурацию.
Command: save

Saving all configurations to NV-RAM... Done.

Примечание: Посмотреть общее количество VLAN`ов и их параметры вы можете выполнив команду:
Command: show vlan

VID	: 1	VLAN Name	: default
VLAN TYPE	: static	Advertisement	: Enabled
Member ports	:		
Static ports	:		
Current Untagged ports	:		
Static Untagged ports	:		
Forbidden ports	:		

VID	: 955	VLAN Name	: management

VLAN TYPE : static Advertisement : Enabled
Member ports : 1-10,12-26
Static ports : 1-10,12-26
Current Untagged ports : 1-10,12-25
Static Untagged ports : 1-10,12-25
Forbidden ports :

VID : 848 VLAN Name : marka-p2p
VLAN TYPE : static Advertisement : Enabled
Member ports : 11,26
Static ports : 11,26
Current Untagged ports : 11
Static Untagged ports : 11
Forbidden ports :

Total Entries : 3

6. Основные проблемы в сетях и методы их устранения

Основные проблемы в сетях:

1. Обнаружение и предотвращение образования ФЛУДА (FLOOD)

Флуд (англ. *flood*) - атака, связанная с большим количеством обычно бессмысленных или сформированных в неправильном формате запросов к компьютерной системе или сетевому оборудованию, имеющая своей целью или приведшая к отказу в работе системы из-за исчерпания ресурсов системы - процессора, памяти либо каналов связи.

Если атака (обычно флуд) производится одновременно с большого количества IP-адресов, то в этом случае она называется *распределённой* атакой на отказ в обслуживании (**DDoS**).

1.1. Broadcast и Multicast флуд:

Что такое широковещательный (broadcast) трафик?

Это пакеты информации, которые назначены для получения всеми компьютерами сети. Такие пакеты в основном предназначены для получения адреса какого-либо компьютера в сети (arp пакеты) или адреса компьютера, на котором работает какой-либо сетевой сервис (ip broadcast). В нормальном режиме работы одна машина в сети рассылает порядка 10-20 таких пакетов в минуту.

Что такое широковещательный (multicast) трафик?

Это многоадресная рассылка, в широком смысле слова – связь между ОДНИМ отправителем и несколькими получателями. В отличие от BROADCAST сообщений, посылаемым всем адресатам сети, MULTICAST сообщения отправляются определенной подгруппе сетевых адресов, которая представляет собой несуществующий MAC-адрес определенный в данном протоколе многоадресной рассылки.

Суть многоадресной рассылки (MULTICAST) в том, что она позволяет нескольким получателям принимать сообщения БЕЗ передачи сообщений каждому хосту BROADCAST домена. MULTICAST подобна почтовой рассылке: пользователь или приложение ПОДПИСЫВАЮТСЯ на определенную группу многоадресной рассылки. Если хост не подписан на группу, он не обрабатывает пакеты, ей адресованные. В BROADCAST коммуникации имеется глобальный адрес (255.255.255.255), на который отвечают все узлы. Многоадресная рассылка применяет адреса, на которые отвечают лишь некоторые узлы (которых подписали). Область MULTICAST охватывает адреса 224.0.0.0 – 239.255.255.255 . Управляется протоколами IGMP (Internet Group Management Protocol – есть несколько версий) и CGMP (CISCO Group Management Protocol – работает только на оборудовании CISCO).

Зачем нужна фильтрация широковещательного трафика?

Как уже было сказано, broadcast и multicast пакеты получают все компьютеры в сети и

соответственно на каждый пакет тратиться время на коммутаторах чтобы его переслать и на каждом компьютере на обработку этого пакета. При нормальном режиме это не вызывает каких либо проблем, но в последнее время появились вирусы, т.н. черви (worms) , которые после заражения машины начинают искать другие хосты в сети, котрые можно заразить, и делают это, рассылая broadcast или multicast пакеты со скоростью до 10000 в минуту. Несколько таких зараженных машин в сети достаточно, чтобы существенно понизить общую пропускную способность.

1.2. Способы решения проблемы в автономном режиме:

Разделить сеть на сегменты и настроить фильтрацию широковещательного трафика;

Каждые 5 секунд собирается статистика по всем широковещательным пакетам в сети, компьютер который превысил лимит в 10 фреймов в секунду - автоматически блокируется. Если в течении следующих 5 секунд broadcast или multicast флуд прекратился, то блок снимается, иначе блок продлевается ещё на 5 секунд.

Это можно реализовать выполнив следующие команды в коммутаторе:

Command: config traffic control 1-24 broadcast enable multicast enable threshold 10 action shutdown time_interval 5

config traffic control 1-3 dlf enable threshold 10

1.3. Способ решения проблемы в ручном режиме.

Как было сказано ранее клиентский компьютер не должен рассылать широковещательный пакет более 10 фреймов в секунду, руководствуясь этим мы можем зайти на коммутатор и проверить детальную статистику по портам выполнив команду:

Command: show packet ports 1-24

Port number : **1**

Frame Size	Frame Counts	Frames/sec	Frame Type	Total	Total/sec
64	20774085	42	RX Bytes	89394905	0
65-127	46231063	117	RX Frames	689108	0
128-255	28249945	29			
256-511	557036	0	TX Bytes	1106165733	1226137
512-1023	65681	4	TX Frames	123459262	1078
1024-1518	28270560	886			
Unicast RX	687889	0			
Multicast RX	159	**0**			
Broadcast RX	1060	**15**			

Если количество Фреймов в секунду (Frames/sec) превышает значение **10**, то данный порт мы считаем флудящим и блокируем его посылкой команды:

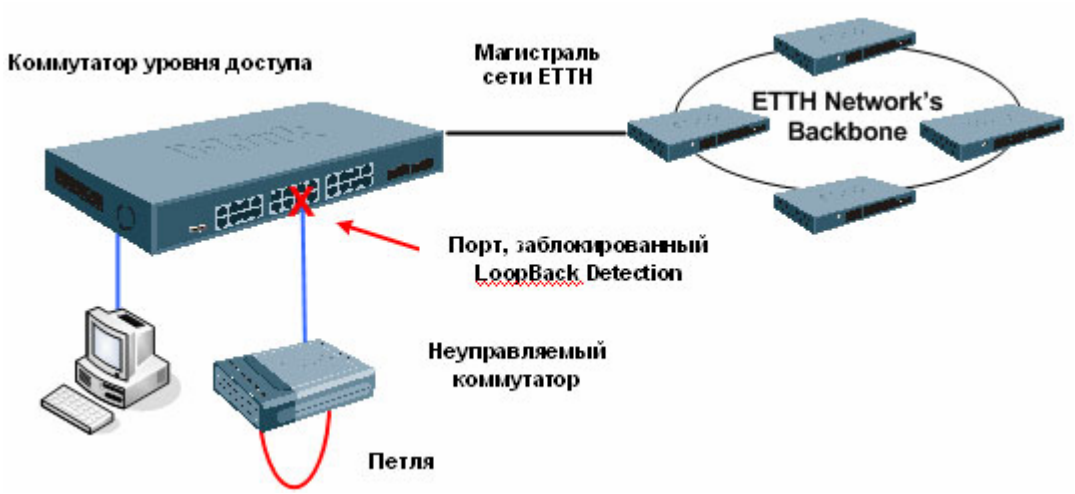
Command: config ports **1** state disable

После выполнения блокировки нужно **ОБЯЗАТЕЛЬНО** прописать комментарий на порту и создать глобальную проблему по дому с пометкой ИНФОРМАЦИЯ, в глобалке указываем какой порт, за что и на каком коммутаторе (с указанием IP адреса) мы его погасили, выполнить это можно посылкой команды:

Command: config ports 1 description FLOOD!!!-000000
номер тикета в HELPDESK`e

2. Обнаружение и предотвращение образование КОЛЕЦ (LOOPBACK)

2.1. Обнаружение петель на порту коммутатора: LoopBack Detection



Ситуация, показанная на рисунке, вынуждает управляемый коммутатор постоянно перестраивать «дерево» STP при получении своего же собственного BPDU. Новая функция LoopBack Detection отслеживает такие ситуации и блокирует порт, на котором обнаружена петля, тем самым предотвращая проблемы в сети.

2.2. Пример настройки функции LoopBack Detection (LBD):

- Задача: Обеспечить на оконечных портах DES-3526 (edge ports) отсутствие петель в неуправляемых сегментах.
- Команды для настройки коммутатора:
    1. **enable stp** (по умолчанию версия RSTP)
    2. **config stp ports 1-24 state enable edge true lbd enable**
    3. **config stp lbd_recover_timer 60** (lbd_recover_timer – время, в течение которого порты не будут принимать BPDU. Оно задаётся глобально на коммутаторе. Если необходимо отключить эту функцию, то следует установить его в 0).

3. Обнаружение и предотвращение возникновения ПОТЕРЬ

Потеря пакетов в сетях зачастую могут возникать в следующих случаях:

3.1. При возникновении флуда в сети см. п.1

3.2. При большой загрузке процессора (CPU) > 80%

Просмотр загрузки процессора (CPU):
Command: show utilization cpu

CPU utilization :

Five seconds - 29% One minute - 6% Five minutes - 19%

3.3. При возникновении ошибок на портах:

Проверка на наличие ошибок на портах:
Command: show error ports 1-2

Port number : 1

	RX Frames		TX Frames
	---		---
CRC Error	53	Excessive Deferral	0
Undersize	0	CRC Error	0
Oversize	0	Late Collision	0
Fragment	0	Excessive Collision	0
Jabber	0	Single Collision	0
Drop Pkts	1029	Collision	0

Port number : 2

	RX Frames		TX Frames
	---		---
CRC Error	1	Excessive Deferral	0
Undersize	0	CRC Error	0
Oversize	0	Late Collision	0
Fragment	0	Excessive Collision	0
Jabber	0	Single Collision	0
Drop Pkts	0	Collision	0

3.4. При несогласовании скорости передачи и приема на портах, например:

Объедены два коммутатора с помощью волоконно-оптического кабеля с применением одноволоконных конверторов.

На ближнем коммутаторе скорость порта выставлена, как **100 Half Duplex**, а на удаленном, как **100 Full Duplex**. В связи с этим при большой нагрузки канала могут возникать потери пакетов. Чтобы избежать этого, нужно выставлять одинаковую скорость порта, как на ближнем, так и на удаленном коммутаторе.

А проверить это можно послав коммутатору команду:
Command: show ports

Port	Port State	Settings Speed/Duplex/FlowCtrl	Connection Speed/Duplex/FlowCtrl	Address Learning	Trap State
-----	--------	----------	----------	--------	--------
1	Enabled	Auto/Disabled	Link Down	Enabled	Enabled
…					
23	Enabled	Auto/Disabled	Link Down	Enabled	Enabled
24	Enabled	Auto/Disabled	Link Down	Enabled	Enabled
25	Enabled	Auto/Disabled	Link Down	Enabled	Enabled
26	Enabled	Auto/Disabled	**100M/Full/None**	Enabled	Enabled

4. Обнаружение и предотвращение образования ЛЕВОГО DHCP СЕРВЕРА

4.1. Динамические IP-адреса

IP-адрес называют *динамическим*, если он назначается автоматически при подключении устройства к сети и используется в течение ограниченного промежутка времени, как правило, до завершения сеанса подключения.

Для получения IP-адреса клиент может использовать один из следующих протоколов:

- DHCP (RFC 2131) — наиболее распространённый протокол настройки сетевых параметров.
- BOOTP (RFC 951) — простой протокол настройки сетевого адреса, обычно используется для бездисковых станций.
- IPCP (RFC 1332) в рамках протокола PPP (RFC 1661).
- Zeroconf (RFC 3927) — протокол настройки сетевого адреса, определения имени, поиск служб.

4.2. Обнаружение и блокирование левого DHCP сервера в ручном режиме:

4.2.1. Для начала нужно определить IP адрес левого DHCP сервера.

Для этого нужно подцепиться ноутбуком к сети и получить автоматически левый IP адрес и в командной строке выполнить команду:

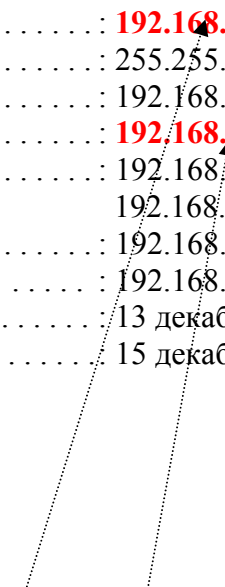
C:\Documents and Settings\users>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : users
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : гибридный
IP-маршрутизация включена . . . . . : нет
WINS-прокси включен . . . . . : нет
Порядок просмотра суффиксов DNS . . .:

Подключение по локальной сети - Ethernet адаптер:

DNS-суффикс этого подключения . . . . :
Описание . . . . . : Intel(R) PRO/100 VE Network Connecton
Физический адрес. . . . . : 00-17-32-37-A0-F6
Dhcp включен. . . . . : да
Автонастройка включена . . . . . : да
IP-адрес . . . . . : **192.168.245.77**
Маска подсети . . . . . : 255.255.240.0
Основной шлюз . . . . . : 192.168.240.223
DHCP-сервер . . . . . : **192.168.240.242**
DNS-серверы . . . . . : 192.168.240.89
192.168.240.156
Основной WINS-сервер . . . . . : 192.168.240.177
Дополнительный WINS-сервер. . . . . : 192.168.240.89
Аренда получена . . . . . : 13 декабря 2006 г. 15:04:54
Аренда истекает . . . . . : 15 декабря 2006 г. 7:04:54



C:\Documents and Settings\users>

4.2.2. По найденному IP адресу левого DHCP сервера нужно определить его MAC адрес:

4.2.2.1. Для этого выполняем команду PING до найденного нами IP адреса левого DHCP сервера, чтобы обновилась информация в ARP таблице:

C:\Documents and Settings\users>ping **192.168.240.242**

Обмен пакетами с 192.168.240.242 по 32 байт:

Ответ от 192.168.240.242: число байт=32 время<1мс TTL=64
Ответ от 192.168.240.242: число байт=32 время<1мс TTL=64
Ответ от 192.168.240.242: число байт=32 время<1мс TTL=64
Ответ от 192.168.240.242: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.240.242:
Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

4.2.2.2. Определяем MAC адрес левого DHCP с помощью выборки из ARP таблицы:

C:\Documents and Settings\users>arp -a

Интерфейс: **192.168.245.77** --- 0x10003

Адрес IP	Физический адрес	Тип
192.168.240.33	00-01-03-2e-a4-7b	динамический
192.168.240.89	00-0d-61-7b-c0-f7	динамический
192.168.240.123	00-30-48-81-7d-4e	динамический
192.168.240.177	00-0e-0c-4e-48-3c	динамический
192.168.240.223	00-15-f9-7a-fb-c0	динамический
192.168.240.242	**00-11-11-0c-97-e1**	динамический

4.2.3. Нужно обозначить пользователя на порту.

Данная функция предполагает определение местонахождения пользователя на порту по MAC адресу. Это полезно, если к примеру требуется найти определенного пользователя и заблокировать его.

В случае, если требуется определить MAC адрес клиента по уже известному IP адресу из ARP таблицы коммутатора, то это можно сделать следующим образом:
Command: show arpentry ipaddress **192.168.240.242**

ARP Aging Time : 20

Interface	IP Address	MAC Address	Type
System	**192.168.240.242**	**00-11-11-0C-97-E1**	Dynamic

Total Entries: 1

Определяем местонахождение MAC адреса на порту:
Command: show fdb mac_address **00-11-11-0C-97-E1**

VID	VLAN Name	MAC Address	Port	Type
955	management	**00-11-11-0C-97-E1**	**2**	Dynamic

Total Entries : 1

4.2.4. После обнаружения клиента на порту, блочим его посылкой команды:
Command: config ports **2** state disable

После выполнения блокировки нужно **ОБЯЗАТЕЛЬНО** прописать комментарий на порту и создать глобальную проблему по дому с пометкой ИНФОРМАЦИЯ, в глобалке указываем какой порт, за что и на каком коммутаторе (с указанием IP адреса) мы его погасили, выполнить это можно посылкой команды:
Command: config ports 1 description LEFT_DHCP-000000
номер тикета в HELPDESK`e

4.3. Обнаружение и блокирование левого DHCP сервера в автономном режиме:

Для этого нужно разделить сеть на сегменты и настроить фильтрацию DHCP запросов и ответов при помощи ACL на коммутаторах;

create access_profile ip udp src_port_mask 0xFFFF profile_id 100
config access_profile profile_id 100 add access_id 1 ip udp src_port **67** port **25-26** permit
config access_profile profile_id 100 add access_id 3 ip udp src_port **68** port **1-24** permit
config access_profile profile_id 100 add access_id 28 ip udp src_port 67 port 1-24 deny
DHCP ответ — служебные порты
DHCP запрос — клиентские порты