


*Создал(а) liceistezmrmrlg 5 месяцев назад.**Последним отредактировал(а) liceistezmrmrlg, 5 месяцев назад.*

# ШПД (Интернет)

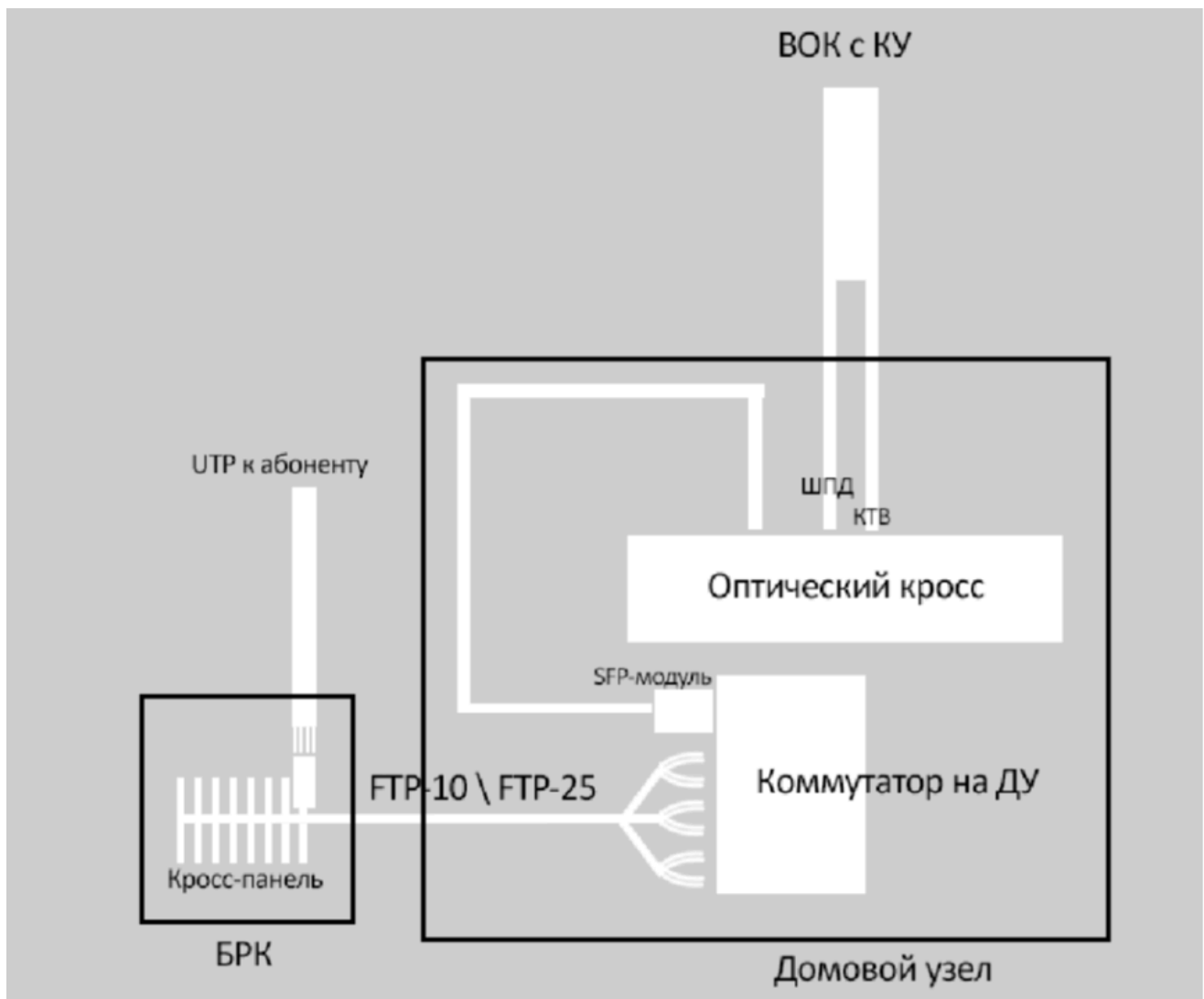
 Комментарии к документу

---

- ШПД (Интернет)

Общее описание (как работает \ предоставляется услуга ШПД)

Интернет для физических лиц предоставляется через протокол PPPoE. Это протокол защищенного соединения с сервером методом аутентификации по логину и паролю и идентификации сетевой устройства при его выходе в интернет по мак-адресу. Логин и пароль для настройки PPPoE-соединения выдается абоненту при подключении на листке «Памятка абонента», в дальнейшем абонент может изменить пароль в личном кабинете по своему усмотрению. Политикой компании предусмотрен лимит на количество мак-адресов, привязанных к одним учетным данным PPPoE в количестве 10. До момента достижения данного лимита абонент может авторизоваться в интернете с любого сетевого оборудования, поддерживающего PPPoE-соединение без каких-либо ограничений. По достижению же лимита у абонента будет возникать ошибка подключения пока он не освободит пул привязанных ранее мак-адресов.



Выше представлена общая схема подключения услуги ШПД на доме. По волоконно-оптическому кабелю (ВОК) на дом приходит два волокна (в случае если проектом предусмотрены резервные волокна их может быть больше): по одному сигнал по ШПД, по второму – сигнал по КТВ. Данные волокна развариваются в оптическом кроссе и далее из кросса через оптический патч-корд сигнал по ШПД идет на коммутатор и подключается в него через SFP-модуль. От коммутатора в БРК установленные в разных подъездах уходит FTP-10 или FTP-25 (десяти- и двадцатипятипарка соответственно). В БРК кабель FTP расшивается на кросс-панели. В кросс-панель забивается плашка с расшитым UTP-кабелем, который далее уходит к абоненту где на конце обжимается коннектором RJ-45. При обращении абонентов по отсутствию шпд первым делом проверяем наличие сессии и доступность коммутатора (даже если сессия есть необходимо убедиться в наличии линка на порту, т.к. нередко встречаются зависшие сессии). Если коммутатор недоступен проверяем информацию о наличии общей аварийной ситуации на форуме и в телеграм-канале «ТП аварийный». Если таковой информации нет – уточняем у абонента информацию о наличии услуг, есть ли электропитание в квартире, подъезде и передаем информацию дежурному специалисту. Здесь также важно уточнить, что коммутатор может быть недоступен по причине того, что он снят. Поэтому проверяем вышеупомянутые форум и телеграм-канал на наличие информации о том, что снималось оборудование или нет.

## Синтаксис команд D-Link

### Авторизация

UserName: user PassWord: listtrb

#### 1. Диагностика кабеля.

Command: `cable_diag ports 1`

Perform Cable Diagnostics ...

Port	Type	Link	Status	Test Result	Cable Length (M)
------	------	------	--------	-------------	------------------

1	FE	LinkUp	OK		80
---	----	--------	----	--	----

При подключенном кабеле `Test Result` будет - OK

При отключенном кабеле `Test Result` будет отображать метраж по всем доступным парам.

Command: `cable_diag ports 2`

Perform Cable Diagnostics ...

Port Type Link Status Test Result Cable Length (M)

2 FE Link Down Pair1 Open at 80 M - Pair2 Open at 82 M

В данном случае мы видим что кабель открыт по двум парам на длине 80 и 82 метра. То есть он либо не подключен в конечное оборудование, либо же повреждён.

Краткая выноска возможных сообщений при использовании команды:

<b>OK</b>	Исправное состояние кабеля
<b>Short in Cable</b>	Короткое замыкание в кабеле
<b>Open in Cable</b>	Кабель, подключенный к порту коммутатора, поврежден или не подключен на другой стороне
<b>Mismatched</b>	Возникли ошибки при диагностике кабеля, требуется перезапустить тест на том же порту
<b>Line Driver</b>	Обнаружено высокое электрическое сопротивление на другой стороне кабеля
<b>Cable Fault Distance (meters)</b>	Расстояние от порта коммутатора до поврежденного участка (при длине кабеля менее 2 метров будет сообщение об отсутствии кабеля "No Cable" )
<b>Cable Length (meter)</b>	При исправном кабеле (результат "OK") отобразит общую длину подключенного к порту кабеля



## 2. Проверка приходящего MAC - address (Мак - адреса) на порту.

Command: show fdb port

VID VLAN Name MAC Address Port Type

2118 vlan0 C4-6E-1F-E2-23-77 4 Dynamic

VID - номер vlan VLAN name - его имя. MAC Address - мак оборудования, который подключен по патчу к этому порту.

Port - номер порта на коммутаторе.

Все физ. лица подключенные к нашей компании работают по vlan0, обязательно смотрим на VLAN Name. Если же vlan name содержит только номер vlan. Уточняем у ведущего специалиста - является ли данный vlan вланом для PPPoE.

### 3. Поиск по MAC - Address (Мак адресу) на коммутаторе.

Если нам неизвестен номер порта, к которому подключен клиент - мы можем найти порт по мак адресу клиента командой:

```
Command: show fdb mac_address (мак клиента) C4-6E-1F-E2-23-77
```

```
VID VLAN Name MAC Address Port Type
```

```
2118 vlan0 C4-6E-1F-E2-23-77 4 Dynamic
```

### 4. Проверка ошибок на порту.

```
Command: show error ports 9
```

```
Port Number : 9
```

```
RX Frames TX Frames
```

```
CRC Error 809827 Excessive Deferral 0`
```

```
Undersize 0 CRC Error 0
```

```
Oversize 0 Late Collision 0
```

```
Fragment 308 Excessive Collision 0
```

```
Jabber 91 Single Collision 0
```

```
Drop Pkts 0 Collision 0
```

В данном блоке информации нас интересуют `CRC Error` и `Fragment`

**Ошибки CRC на порту коммутатора могут возникать по разным причинам.** Некоторые из них:

- **Аппаратное отключение от сети на стороне клиента.** Как следствие — плохой контакт между коннектором и портом сетевой карты.
- **Неисправность сетевой карты.**
- **Проблемы на стороне коммутатора.** Например, сырость, пыль, грязь, отсутствие гибких патчкордов.
- **Неисправность порта.** Например, после грозы или если коммутатор залили водой.
- **Повреждение по линии.**
- **На линии клиента есть скрутка которая расходится.**

**Fragment** на порту коммутатора — это **счётчик кадров с неправильной контрольной суммой или структурой кадра размером менее 64 байт**.

Такие кадры обычно возникают в результате коллизий в сети.

Ошибки Fragment могут появляться из-за некорректной работы передатчика, если используется линк full duplex, или могут возникнуть на линке half duplex

По сути возникают при тех же обстоятельствах что и CRC Error.

## 5. Проверка логов (История на оборудовании)

Команда `sh log`

Данная команда выводит историю “происшествий” на коммутаторе, за срок который он работает.

Command: `show log`

```
11822 2025-05-14 13:08:18 Successful login through Telnet (Username: root, IP: 2
17.25.208.2)
```

```
11816 2025-05-13 19:30:35 Port 28 link up, 100Mbps FULL duplex 11815
2025-05-13 19:30:33 Port 28 link down
```

То есть мы можем увидеть - падал ли линк, кто авторизовывался в какой промежуток времени. Так же на коммутаторах серии DGS можно увидеть перезагружали ли порт.

Так же отображается Loop - detected:

\*Command: `show log`\*

\*Index Date Time Level Log Text\*

```
• *-----*
  _*
```

```
*2 2000-01-01 00:56:50 CRIT(2) Port 4 VID 10 LBD loop occurred. Packet discard
begun*
```

```
*1 2000-01-01 00:56:50 INFO(6) Port 4 link up, 100Mbps FULL duplex*
```

## 6. Сегментация трафика

Функция Traffic Segmentation (сегментация трафика) служит для разграничения доменов на канальном уровне. Она позволяет настраивать порты или группы портов коммутатора таким образом, чтобы они были полностью изолированы друг от друга, но в то же время имели доступ к разделяемым портам, используемым для подключения серверов или магистрали сети

Command: `show traffic_segmentation`

#### Traffic Segmentation Table

##### Port Forward Portlist

1 25-28

2 25-28

3 25-28

4 25-28

5 25-28

6 25-28

7 25-28

8 25-28

9 25-28

10 25-28

11 25-28

12 25-28

13 25-28

14 25-28

15 25-28

16 25-28

17 25-28

18 25-28

19 25-28

20 25-28

21 25-28

22 25-28

23 25-28

24 25-28

25 1-28

26 1-28

27 1-28

28 1-28

То есть порты с 1 по 24 общаются только с магистральными портами. А магистральные порт с 25 по 28 общаются со всеми портами.

## 7. Вланы (Vlan 's)

Command: `show vlan`

**VID : 12 VLAN Name : vlangtr1 - влан управления**

**VID : 101 VLAN Name : voip - влан телефонии**

**VID : 2118 VLAN Name : vlang0 - влан для PPPoE**

**Разница между tagged и untagged портами** заключается в следующем:

1. **Tagged порты** (также известные как магистральные) **настроены на передачу данных для нескольких VLAN** (виртуальных локальных сетей). Для каждого пакета в них добавляется тег VLAN. Такие порты используются для соединения сетевого оборудования между собой, к конечным узлам сети тегированный трафик обычно не доставляется.
2. **Untagged порты** (порты доступа) **настроены на принадлежность к определённой VLAN**, но не добавляют теги VLAN к входящим или исходящим кадрам. Обычно используются для подключения конечных узлов сети, которые не должны ничего знать об иных VLAN и работать в собственном сегменте.

Таким образом, **tagged-порт ставит определённую метку на пакеты, а untagged-порт снимает её.**



## 8. ACL (Аксесс листы)

**ACL (списки управления доступом) в коммутаторах D-Link нужны для фильтрации потоков данных.** Проверка содержимого пакетов выполняется на аппаратном уровне.

С помощью ACL администратор может:

- ограничить типы приложений, разрешённых для использования в сети;
- контролировать доступ пользователей к сети и определять устройства, к которым они могут подключаться; <sup>1</sup>
- определить политику QoS, классифицировав трафик и переопределив его приоритет. <sup>1</sup>

Когда сообщения поступают на входной интерфейс, коммутатор проверяет параметры пакетов данных на совпадение с критериями фильтрации, определёнными в ACL, и выполняет над пакетами одно из действий: Permit («Разрешить») или Deny («Запретить»).

В нашей сети ACL используется для работа способности PPPoE клиентов.

**Command:** `show config current_config begin "ACL"`

```
create access_profile ethernet ethernet_type profile_id 2
```

```
config access_profile profile_id 2 add access_id 24 ethernet ethernet_type 0x8864 port 1  
permit config access_profile profile_id 2 add access_id 47 ethernet ethernet_type 0x8863  
port 1 permit
```

```
create access_profile ethernet source_mac 00-00-00-00-00-00 profile_id 3
```

```
config access_profile profile_id 3 add access_id 2 ethernet source_mac 00-00-00-00-00-  
00 port 25 permit
```

Если изъясняться проще, ACL должны быть прописаны изначально админами, мы проверяем их наличие и вид, в соответствии с другими прописанными “правилами” на портах.

## 9. Просмотр состояния порта.

**Command:** `show ports 23`

Port	State/	Settings	Connection	Address	Type	MDI	Speed/Duplex/FlowCtrl	Speed/Duplex/FlowCtrl	Learning
------	--------	----------	------------	---------	------	-----	-----------------------	-----------------------	----------

23	Enabled	Auto/Disabled	Link Up	Enabled	Auto				
----	---------	---------------	---------	---------	------	--	--	--	--

Обязательно обращаем внимание на State - для работы должен быть включен.

А так же на Speed/Duplex/FlowCtrl Порт должен быть на Auto/100mb/Full - это корректная работа порта. Если же она 100/Half или же на других значениях, обязательно проверяем состояние линии клиента. Если необходимо изменить параметры - обращаемся к ведущим.

## 10. Ограничение пропускной способности порта

Port	RX Rate	TX Rate	Effective RX	Effective TX	(Kbit/sec)	(Kbit/sec)	(Kbit/sec)	(Kbit/sec)
24	15424	15424	15424	15424				

Команда `show bandwidth_control` позволяет узнать, настроены ли какие-либо ограничения пропускной способности на определенном порту коммутатора. Это полезно для:

- **Диагностики проблем с производительностью сети:** Если пользователи жалуются на медленную работу сети, проверка ограничений пропускной способности может помочь выявить, не является ли причиной намеренное или случайное ограничение скорости на порту.
- **Проверки конфигурации:** Для клиентских устройств всегда должно быть указано "No Limit"

Если вы видите какие-либо другие значения, это значит, что на порт наложено ограничение, и это может быть причиной проблем со скоростью у пользователя. В таком случае, необходимо проверить конфигурацию и убедиться, что ограничение снято.

- **Устранения неполадок:** Если вы подозреваете, что ограничение пропускной способности мешает нормальной работе устройства, подключенного к порту, эта команда поможет подтвердить или опровергнуть эту гипотезу.

В общем, `show bandwidth_control` - это важный инструмент для мониторинга и управления пропускной способностью сети, позволяющий операторам контролировать трафик и обеспечивать оптимальную производительность для всех пользователей. Используйте ее для проверки настроек и выявления потенциальных проблем, связанных с ограничением скорости на портах коммутатора.

