MPLS(-TE) (Traffic Engineering)

- Идея сохранения в маршрутной таблице только реально используемых виртуальных путей и легла в основу разработки протокола MPLS и сопряженных с ним протоколов маршрутизации (“раскраска путей”)
- MPLS допускает (но не требует) приоритетность или класс обслуживания, зависящие полностью или частично от метки. В этом случае, можно сказать, что метка представляет собой комбинацию *FEC* (Forward Equivalent Class), *приоритета* или

MPLS

- MPLS позволяет как агрегацию так и дисагрегацию трафика, традиционный IP – только агрегацию
- Если в каких-то узлах нет возможности декрементации TTL, возможно зацикливание пакетов

Формат меток VLAN на уровне L2

EtherType=TPID (Tagged Protocol Identifier) содержит код **0x8100 (802.1Q)**. Стек меток -> LIFO

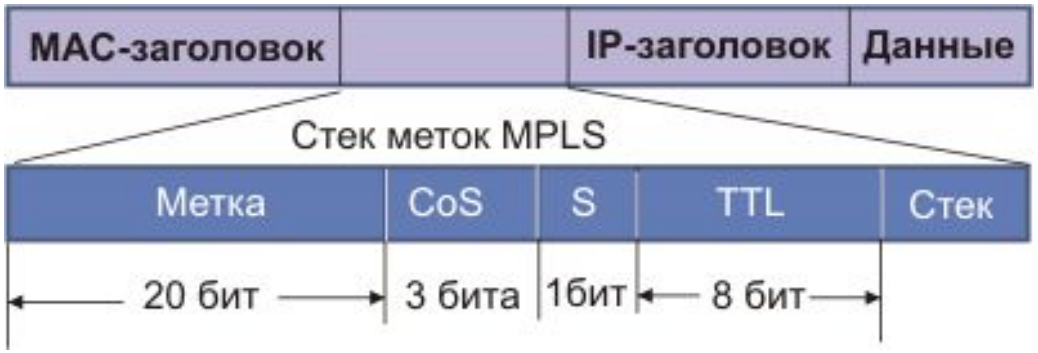
Поле *приоритета пользователя* - 3 бита,

1-битовое поле **CFI** (Canonical Format Identifier)

12-битовое поле **VID** (идентификатор виртуальной сети) называются **TCI** (Tagged Control Information).

3-битовое поле IP-приоритета размещается здесь без проблем.

Формат записи стека меток

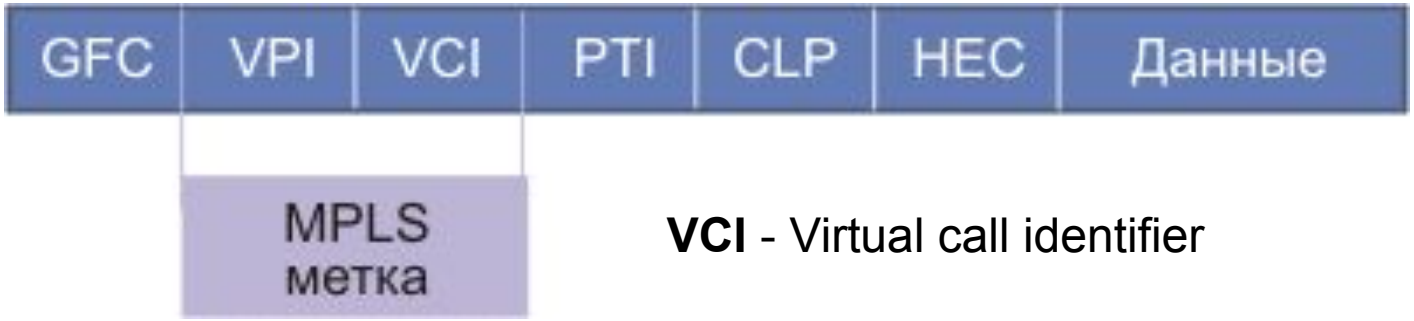


Дно стека (**S**)

Шестнадцатеричный код Ethertype **8847** используется для индикации того, что кадр содержит уникастный MPLS-пакет. Шестнадцатеричный код Ethertype **8848** служит для указания того, что кадр содержит MPLS-пакет. Эти значения Ethertype могут быть использованы либо при Ethernet-инкапсуляции, либо при инкапсуляции 802.3 LLC/SNAP для транспортировки помеченных пакетов.

Всегда анализируется только верхняя метка стека

Формат меток в ячейках ATM



Для одного и того же набора узлов можно сформировать несколько VPN с разными значениями QoS. **Несколько путей между двумя узлами позволяют увеличить пропускную способность.**
Метка = **FEC** + **приоритет** + **CoS** (Class of Service)
CoS может варьироваться вдоль маршрута
FEC – Forward Equivalent Class
IP-заголовки при переадресации MPLS не анализируются

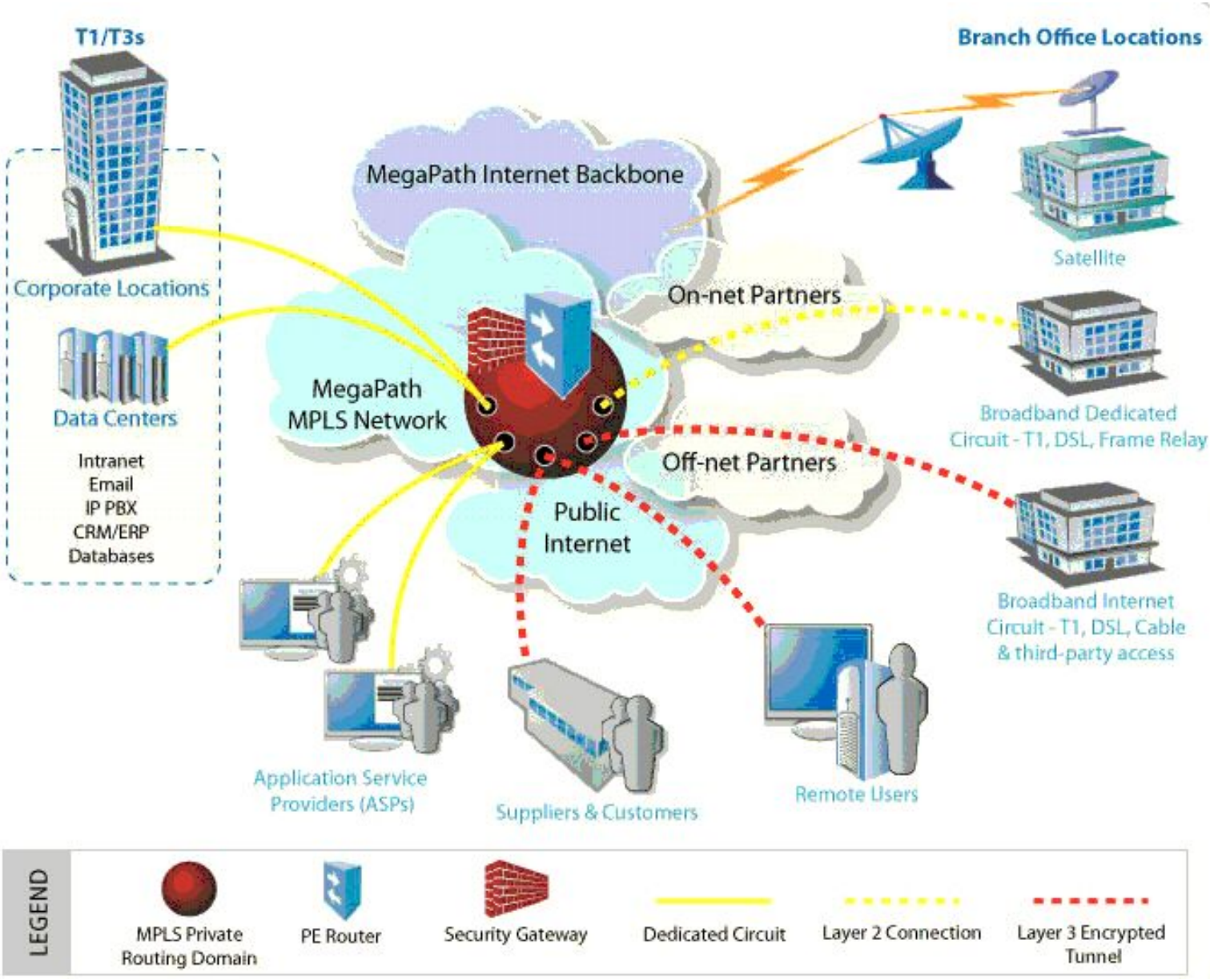
Особенности маршрутизации MPLS

- Пакеты, вошедшие через разные порты, помечаются по-разному. В традиционной схеме это не возможно (идентичность интерфейса не путешествует вместе с пакетом)
- Хакеру труднее перенаправить пакет по нужному адресу
- MPLS может использоваться совместно с PPP **PPP** (Point-to-Point Protocol). PPP предоставляет стандартный метод транспортировки многопротокольных дейтограмм через каналы точка-точка.

MPLS

- Определение MTU пути будет работать корректно, только если в точке, где может потребоваться фрагментация помеченной IP-дейтограммы, возможна посылка отправителю ICMP сообщения “Destination Unreachable”. (MPLS-дейтограмма может увеличивать свою длину при движении по маршруту)
- Особенности для дейтограмм IPv6 (их нельзя фрагментировать !)

Site-to-site MPLS VPN



Стек меток

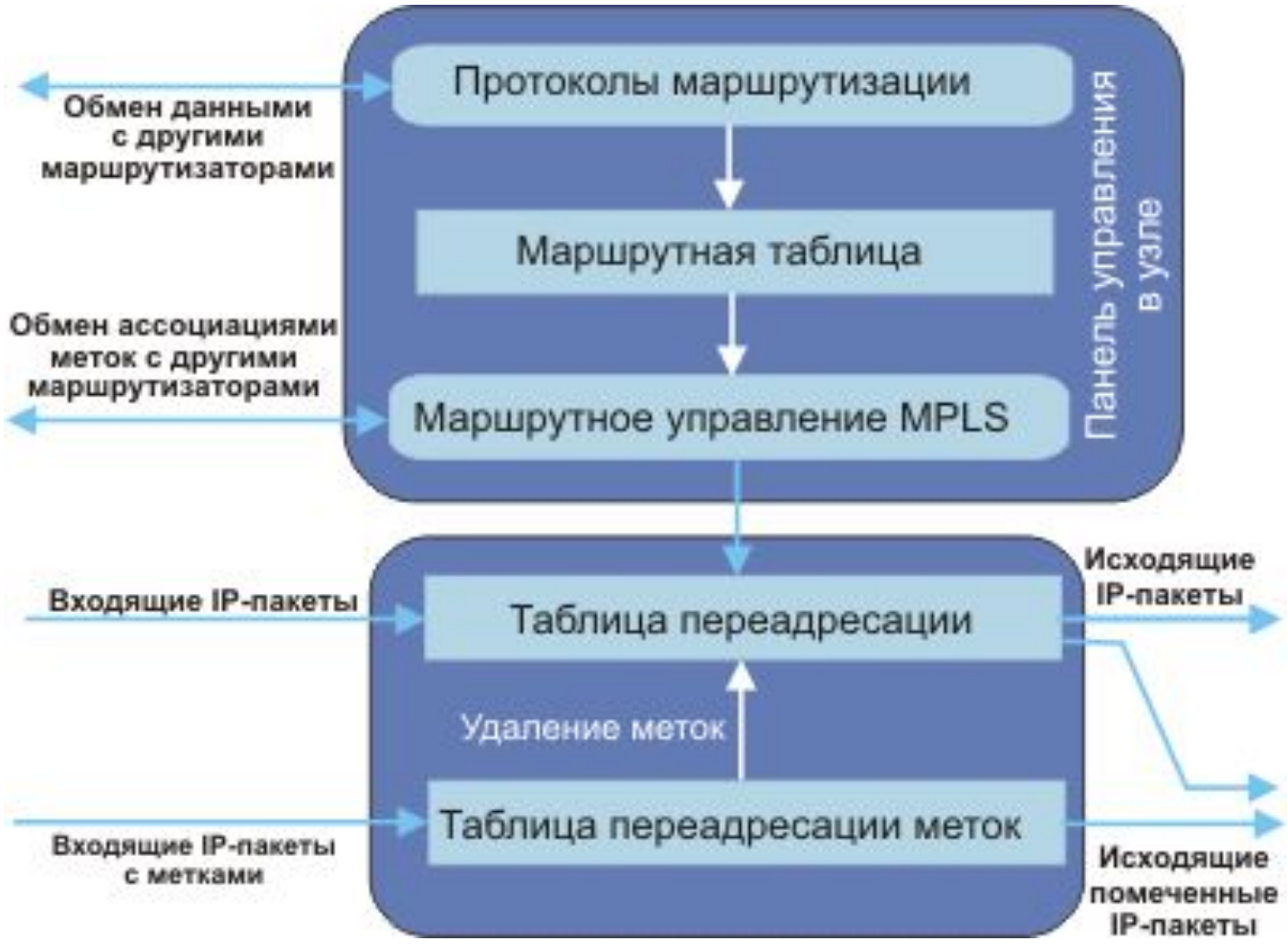
Формат меток должен согласовываться отправителем и получателем

Присваивает метку нижестоящий узел и посылает это предложение вышестоящему (**downstream-on-demand**)

Одновременно могут использоваться несколько протоколов рассылки меток (BGP,LDP,RSUP-TUNNELS…)

- **Unsolicited-downstream** -> LSR рассылает метки другим LSR, которые об этом не просили.
- Удаление меток, так как сетевой интерфейс компьютера этого не поймет
- Проблема посылки ICMP при ошибке
- Пакеты с определенным FEC из конкретного узла будут двигаться по одному и тому же LSP
- DSCP не эквивалентно CoS

Обработка помеченных и обычных IP-пакетов



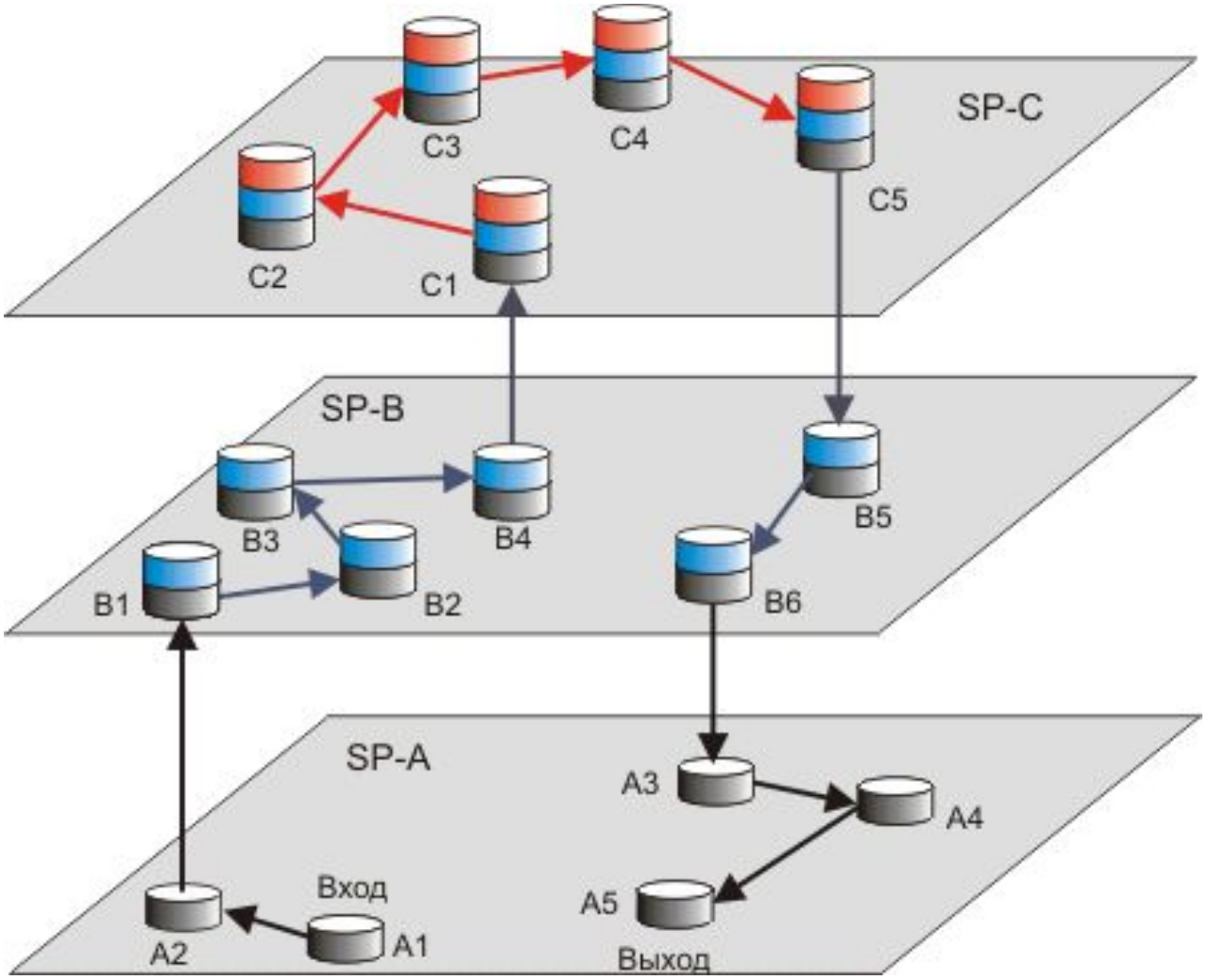
Документы и обозначения

- RFC -3496(ATM), -3785, -3811, -3812, -3813, -3815, -3919, -4023, -4105, -4127, -4182, -4216, -4221, -4247, 4368, -4377, -4378, -4379, -4385, -4448, -4618, -4619(FR), -4687, -4717(ATM), -4736, -4798, -4901, -4920, -4928, -4929, -4972, -5129, -5143(SDH).
- **FEC** - Forwarding Equivalence Classes
- **LSP** - Label Switched Path
- **LSR** - Label Switching Router
- **NHLFE** - Next Hop Label Forwarding Entry (элемент маршрутной таблицы)

MPLS

- Когда говорится, что пакеты посланы из Ru в Rd, это не означает, что пакеты сформированы в Ru или, что местом назначения является Rd. Скорее, мы подразумеваем, что пересылаемые пакеты поступают в один или оба LSR.
- *Способ, которым обрабатывается поле TTL, может варьироваться в зависимости от того, размещены ли значения меток MPLS в прослойке между заголовками [MPLS-SHIM], или метки MPLS транспортируются в заголовке L2, таком как заголовок ATM [MPLS-ATM] или заголовок frame relay [MPLS-FRMRLY].*

Коммутация по меткам



IntServ - DiffServ

- **RSVP**
- WRED -> Буфер -> WFQ -> Интернет (DiffServ)
- **MPLS-TE**
- **RSVP-TE**
- Механизмы резервирования ресурсов
- Механизмы реализации резервирования для пакетов
- В традиционном MPLS путь должен начинаться и завершаться в LSR (а GMPLS в LSR того же типа)

Существует три фундаментальных проблемы, относящиеся к управлению трафиком в MPLS

- 1. Как определять соответствие пакетов определенному классу FEC (Forwarding Equivalence Class).
- 2. Как определять соответствие FEC и каналов передачи данных.
- 3. Как определять соответствие каналов передачи данных физической топологии сети через маршруты с коммутацией по меткам.

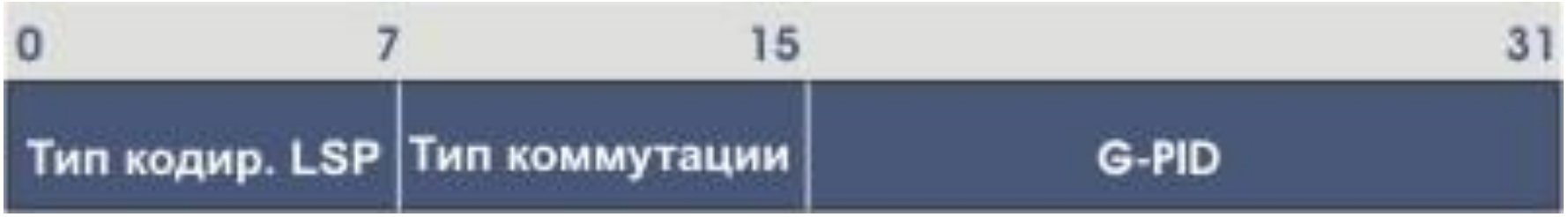
Процесс маршрутизации, базирующийся на ограничениях

Маршрутизацию на основе ограничений можно внедрить одним из двух способов.
1. Путем расширения существующих IGP протоколов, таких как OSPF и IS-IS для поддержки маршрутизации на основе ограничений.
2. Путем добавления процесса маршрутизации на основе ограничений в каждый маршрутизатор, который может сосуществовать с имеющимися IGP.

GMPLS

- RFC-3474, -3945, -4003, -4139, -4202, -4203, -4205, -4206, -4208, -4257, -4258, -4328, -4397, -4426, -4427, -4428, -4606, -4783, -4801, -4802(TE), -4803, -4872(RSVP-TE), -4873, -4974(TE), -4990, -5063, -5145(TE), -5150(TE), -5151(TE).
- В GMPLS возможно сочетание PSC И LSC
- (packet- или label-switch capable)
- Если обычный MPLS однонаправленный, то GMPLS может быть двунаправленным.
- Канал управления может отличаться от канала данных

GMPLS



Тип кодирования

1 Пакет
2 Ethernet
3 ANSI/ETSI PDH
4 Зарезервировано
5 SDH ITU-T G.707 / SONET ANSI T1.105
6 Зарезервировано
7 Цифровой конверт
8 Lambda (оптическое)
9 Волокно
10 Зарезервировано
11 FiberChannel

G-PID

5-19 – SDH
32 - ATM mapping
33 – Ethernet (λ)
43 - FibreChannel

Типы коммутации

- **1** Packet-Switch Capable-1 (**PSC-1**)
- **2** Packet-Switch Capable-2 (**PSC-2**)
- **51** Layer-2 Switch Capable (**L2SC**)
- **100** Time-Division-Multiplex Capable (**TDM**)
- **159** Lambda-Switch Capable (**LSC**)
- **200** Fiber-Switch Capable (**FSC**)
- Метка в GMPS характеризует:
- Одно из волокон пучка
- Один волновой диапазон в волокне
- Набор временных доменов
- Одну длину волны в волновом диапазоне

Fiber-Switch Capable (**FSC**)

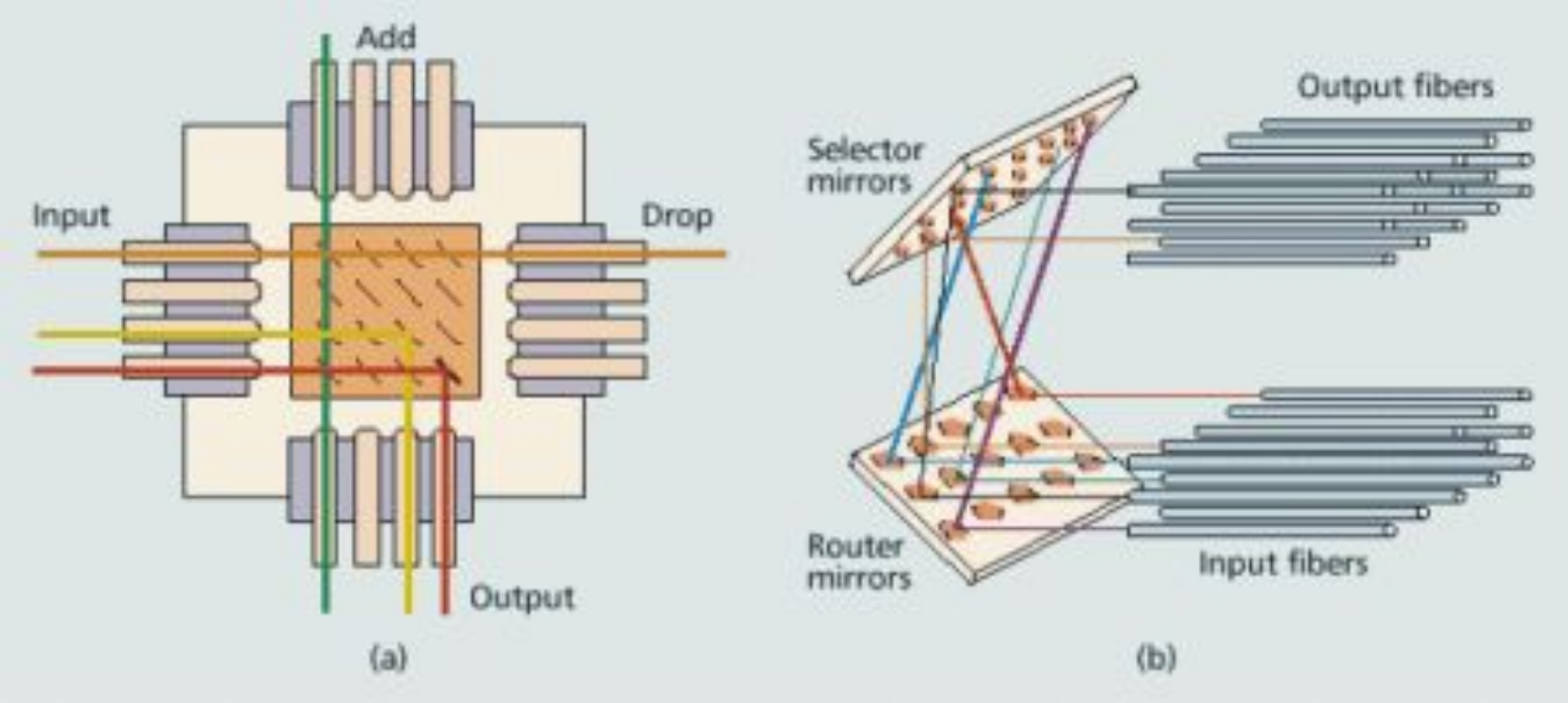
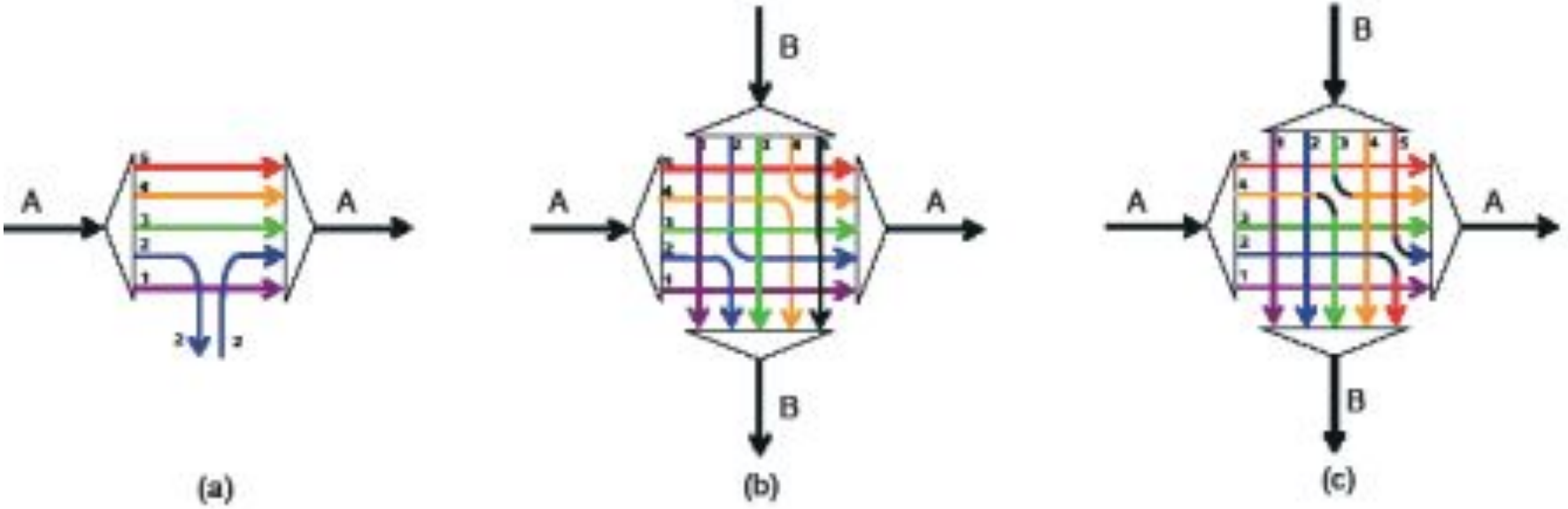
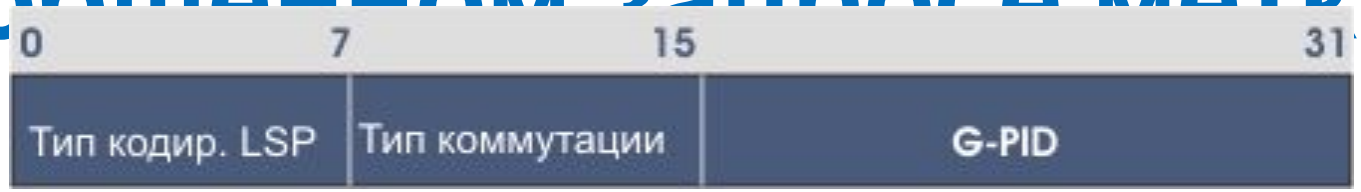


Схема перенаправления оптических информационных потоков со сменой длины волны и без



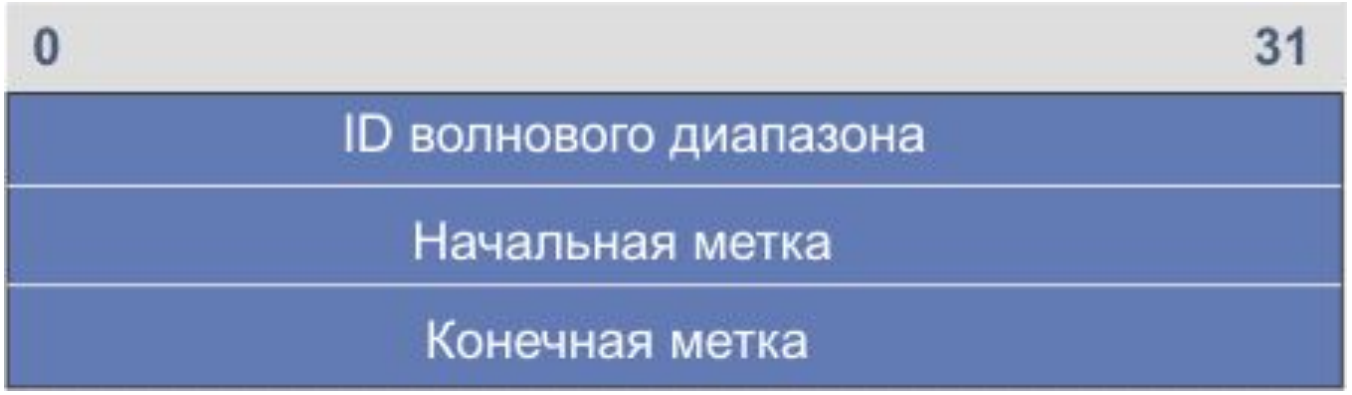
(a) **OADM** - (Optical adddrop multiplexer),
(b) **OXC** - (optical cross-connect) - оптическая коммутация ,
(c) **OXC** со сменой длины волны.

Информация, транспортируемая в обобщенном запросе метки



Значение	Тип коммутации
1	Packet-Switch Capable-1 (PSC-1)
2	Packet-Switch Capable-2 (PSC-2)
3	Packet-Switch Capable-3 (PSC-3)
4	Packet-Switch Capable-4 (PSC-4)
51	Layer-2 Switch Capable (L2SC)
100	Time-Division-Multiplex Capable (TDM)
150	Lambda-Switch Capable (LSC)
200	Fiber-Switch Capable (FSC)

Обобщенная метка



ID диапазона длин волн: 32 бит

Информация в наборе меток

Объект запроса обобщенной метки (RSVP-TE)

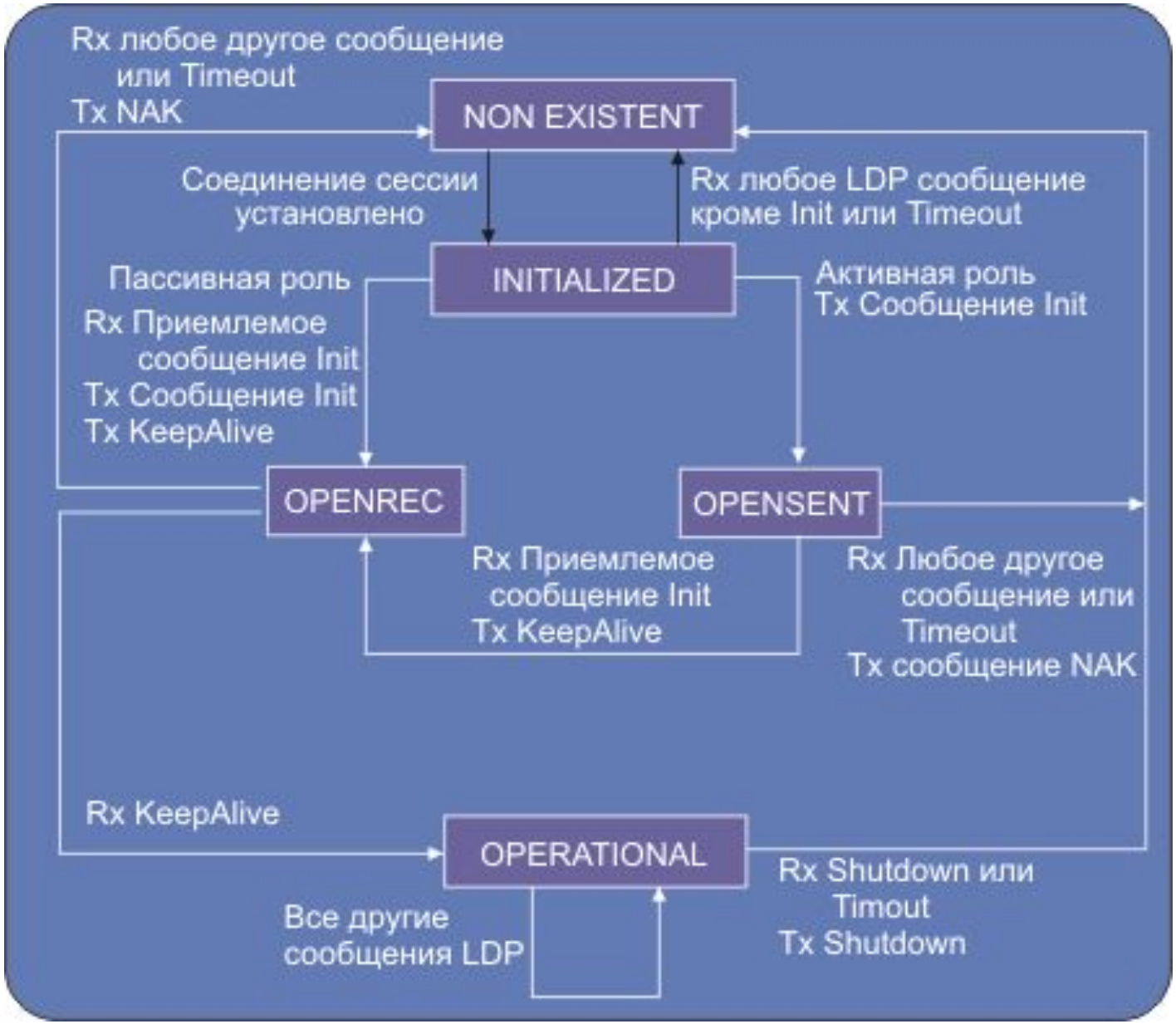
Обобщенный PID (**G-PID**): 16 бит

LSP Label Switched Path

Объект коммутируемого интервала длин волн

Объект набора меток (RSVP-TE)

LDP


Rx любое другое сообщение
или Timeout
Tx NAK
NON EXISTENT
Соединение сессии
установлено
Rx любое LDP сообщение
кроме Init или Timeout
INITIALIZED
Пассивная роль
Rx Приемлемое
сообщение Init
Tx Сообщение Init
Tx KeepAlive
Активная роль
Tx Сообщение Init
OPENREC
OPENSENT
Rx Приемлемое
сообщение Init
Tx KeepAlive
Rx Любое другое
сообщение или
Timeout
Tx сообщение NAK
Rx KeepAlive
OPERATIONAL
Все другие
сообщения LDP
Rx Shutdown или
Timout
Tx Shutdown

Существует четыре категории сообщений LDP:

- 1. Сообщения **выявления** (***Discovery***), используются для объявления и поддержания присутствия LSR в сети.
- 2. Сообщения **сессий**, используются для установления, поддержки и завершения сессий между LDP партнерами.
- 3. Сообщения **анонсирования** (***Advertisement***) , используются для формирования, изменения и ликвидации соответствия между меткой и FEC.
- 4. Сообщения **уведомления** (***Notification***), используются для предоставления рекомендаций и уведомления об ошибках.
- Транспорт TCP (идентификатор LDP – 6 октетов)
- Выявление соседей (Hello) осеществляется посредством UDP

LDP сообщения

TLV - Type-Length-Value

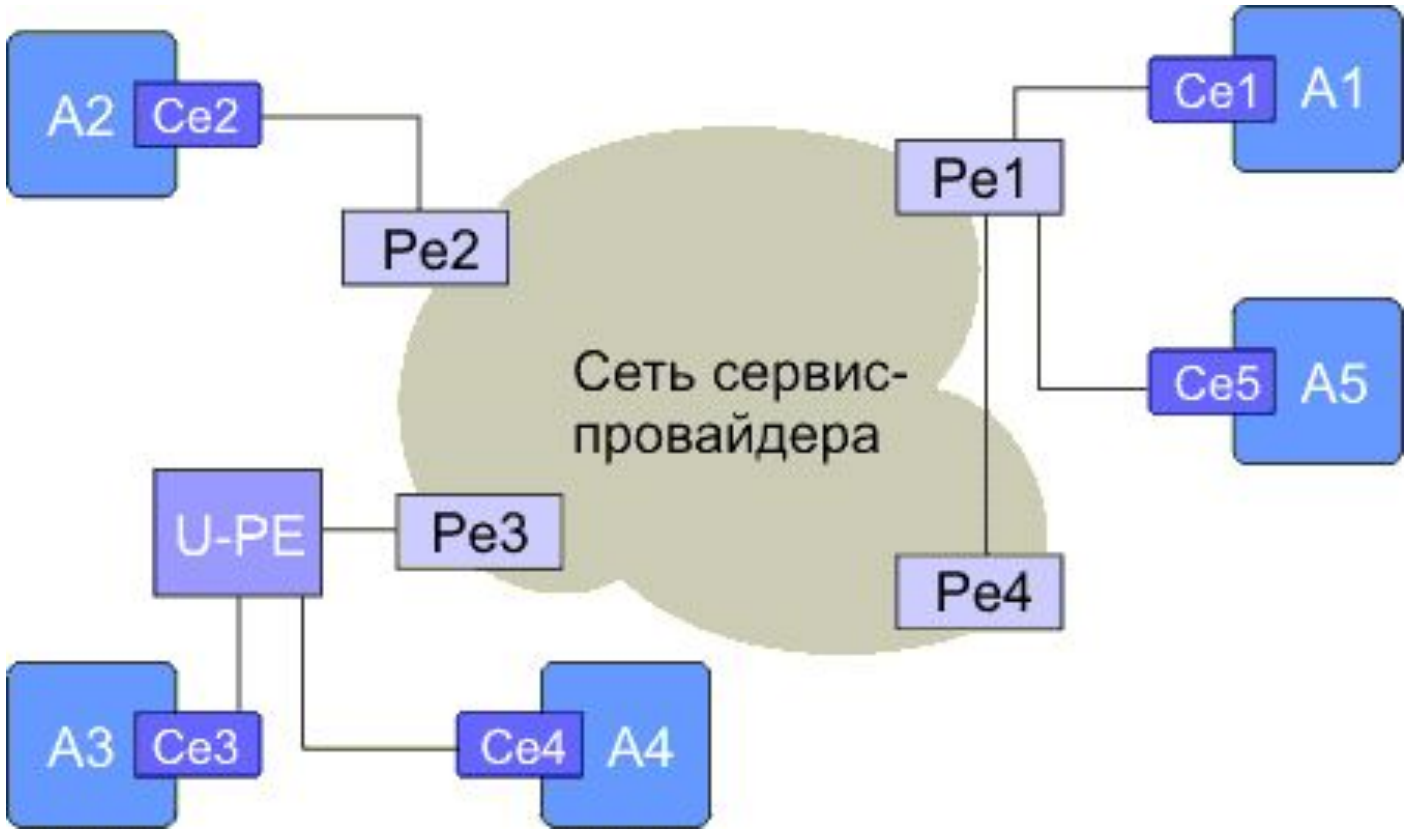
***U** бит - б*ит неизвестного TLV. Если U=0, отправителю сообщения следует послать предупреждение

F бит переадресации неизвестного TLV. Этот бит используется лишь в случае U=1

Тип - Определяет, как следует интерпретировать поле *значение*.

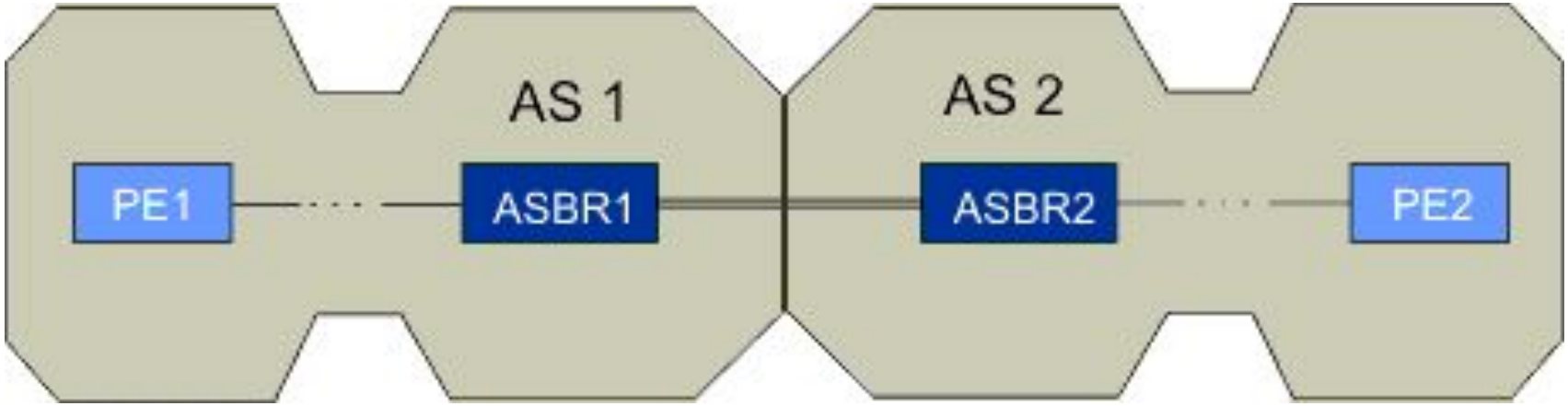
Длина - Специфицирует длину поля значение в октетах.

VPLS (*Virtual Private LAN Service*)



CE - Оконечное устройство клиента;
PE - Пограничный маршрутизатор провайдера;
u-PE - агрегация уровня L2;
A<n> - Сайт клиента n

VPLS между AS



AS - автономная система
ASBR – AS–Border Router

Квантовая криптография

- Протокол квантовой криптографии (BB84) был предложен и опубликован в 1984 году Беннетом и Брассардом
- Здесь используется квантовый принцип неопределенности, когда две квантовые величины не могут быть измерены одновременно с требуемой точностью.
- Поляризация фотонов может быть ортогональной диагональной или циркулярной. Измерение одного вида поляризации рэндомизует другую составляющую.
- Если отправитель и получатель не договорились между собой, какой вид поляризации брать за основу, получатель может разрушить посланный отправителем сигнал, не получив никакой полезной информации.

Квантовая криптография

Ячейки Покеля служат для импульсной вариации поляризации потока квантов передатчиком

Передатчик может формировать одно из четырех состояний поляризации (0, 45, 90 и 135 градусов).

На принимающей стороне после ячейки Покеля ставится кальцитовая призма, которая расщепляет пучок на два фотодетектора (ФЭУ), измеряющие две ортогональные составляющие поляризации

- Отправитель кодирует отправляемые данные, задавая определенные квантовые состояния, получатель регистрирует эти состояния. Затем получатель и отправитель совместно обсуждают результаты наблюдений. В конечном итоге со сколь угодно высокой достоверностью можно быть уверенным, что переданная и принятая кодовые последовательности тождественны. Обсуждение результатов касается ошибок, внесенных шумами или злоумышленником, и ни в малейшей мере не раскрывает содержимого переданного сообщения. Может обсуждаться четность сообщения, но не отдельные биты. При передаче данных контролируется поляризация фотонов. Поляризация может быть ортогональной (горизонтальной или вертикальной), циркулярной (левой или правой) и диагональной (45 или 135^0).
- В качестве источника света может использоваться светоизлучающий диод или лазер. Свет фильтруется,

- Получатель открыто сообщает отправителю, какую последовательность базовых состояний он использовал. Отправитель открыто уведомляет получателя о том, какие базовые состояния использованы корректно. Все измерения, выполненные при неверных базовых состояниях, отбрасываются. Измерения интерпретируются согласно двоичной схеме: лево-циркулярная поляризация или горизонтальная - 0, право-циркулярная или вертикальная - 1. Реализация протокола осложняется присутствием шума, который может вызвать ошибки. Вносимые ошибки могут быть обнаружены и устранены с помощью подсчета четности, при этом один бит из каждого блока отбрасывается.
- **Беннет** в 1991 году предложил следующий протокол.

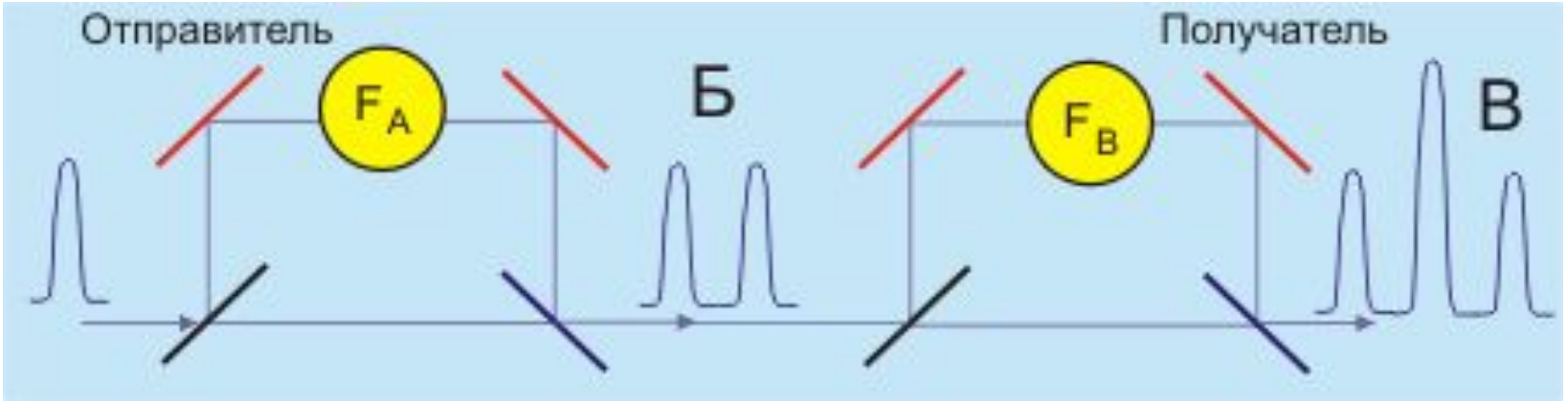
Протокол Беннета

- Отправитель и получатель договариваются о произвольной перестановке битов в строках, чтобы сделать положения ошибок случайными.
- Строки делятся на блоки размера k (k выбирается так, чтобы вероятность ошибки в блоке была мала).
- Для каждого блока отправитель и получатель вычисляют и открыто оповещают друг друга о полученных результатах. Последний бит каждого блока удаляется.
- Для каждого блока, где четность оказалась разной, получатель и отправитель производят итерационный поиск и исправление неверных битов.
- Чтобы исключить кратные ошибки, которые могут быть не замечены, операции пунктов 1-4 повторяются для большего значения k.

Протокол Беннета

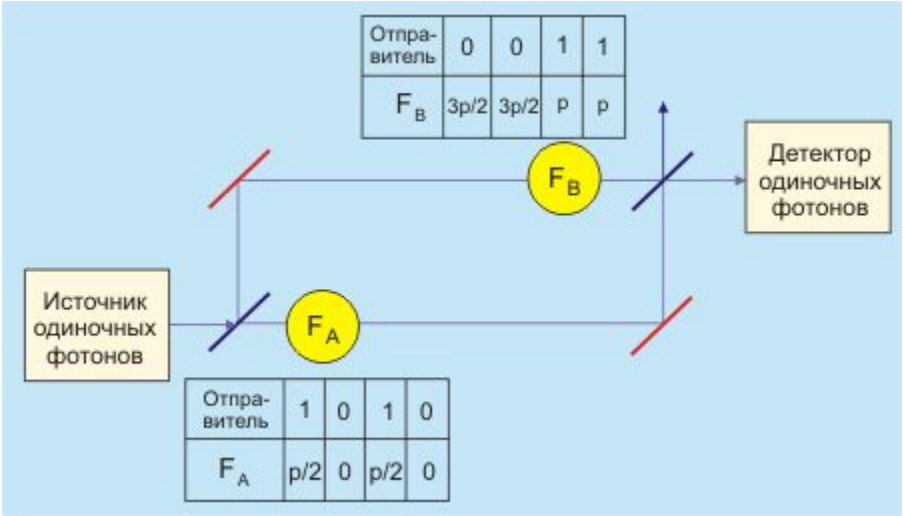
- **Для того чтобы определить, остались или нет необнаруженные ошибки, получатель и отправитель повторяют псевдослучайные проверки**:
- Получатель и отправитель открыто объявляют о случайном перемешивании позиций половины бит в их строках.
- Получатель и отправитель открыто сравнивают четности. Если строки отличаются, четности должны не совпадать с вероятностью 1/2.
- Если имеет место отличие, получатель и отправитель, использует двоичный поиск и удаление неверных битов.
- **Если отличий нет, после m итераций получатель и отправитель получают идентичные строки с вероятностью ошибки 2^{-m}.**

Реализация алгоритма B92



Отправитель определяет углы фазового сдвига, соответствующие логическому нулю и единице ($F_A=\pi/2$), а приемник задает свои фазовые сдвиги для логического нуля ($F_B=3\pi/2$) и единицы ($F_B=\pi$).
Вероятность того, что фотон, посланный отправителем, будет детектирован получателем равна $P_D = \cos^2\{(F_A - F_B)/2\}$

Лучших характеристик можно достичь, мультиплексируя оба пути фотонов в одно волокно



Практические измерения для транспортного кабеля длиной 14 км показали эффективность генерации бита ключа на уровне 2,2 10^{-3} при частоте ошибок (BER) около 1,2%.