MCC-MSN

Лекция - Технологии VPN

Костюкович А.Е.
Каф.АЭС, СибГУТИ
www.aek-54.ru

Виртуальные сети и услуги – VPN

VPN – Virtual Private Network (ВЧС) – это операторская услуга предоставления сетевых ресурсов в рамках WAN / MAN для территориально распределенных клиентов, не владеющих собственной глобальной сетевой инфраструктурой.

Основная задача VPN – изоляция трафика, создание защищенных соединений и сетей в рамках публичной (незащищенной сети).

Услуги VPN можно обеспечить на разных уровнях OSI. Рассмотрим варианты:

Услуги VPN поддерживаются на различных уровнях OSI:

В рамках MAN – VPN предоставляются на базе технологий **уровня L2**:

- ATM (VPI – номер VPN, VCI – адреса ресурсов в VPN)
- MPLS, MPLS-TE
- PBB, PBT
- Q-in-Q (802.1ad)
- 802.1Q (**VLAN** – где VID – номер VPN)

В рамках WAN для организации VPN:

- **На уровне L3** используется протокол IP с шифрованием данных (IP-sec), туннели GRE
- **На уровне прикладных протоколов** – туннели, «псевдопровода» типа L2TP, PPTP, GTP,…
- **На уровне приложений** используется услуга VPN в IN/ОКС-7_ТфОП, SIP/VoIP,… (предоставление услуг виртуальной PBX в ТфОП)

Технологии, обеспечивающие VPN / QoS

		VPN, «Псевдопровод», туннель				VPN с гарантией QoS			
ISO	org	IETF	IETF	ETSI / 3GPP	IETF	IEEE 802.1…			IETF
	doc	RFC 2516	RFC 2637	09.60 / 29.060	RFC 2516				RFC 3032
L7 L6 L5	prot	L2TP	PPTP	GTP					
L4	Port TCP/ UDP	1701	1723	3386					
L3		GRE (Prot=47)							
		IP							MPLS (TE)
L2						…p/Q	…ad	…ah (ay)	
	prot				PPPoE	VLAN	Q-in-Q	PBB (TE)	
	TP				8863 8864	8100	9300 9200 9100 8100	88A8	8847 8848
		MAC (DA-SA-TP---DATA-CRC)							
L1		u-100BT (FE), z-1000BASE-ZX (GE)…							

Особенности VPN на различных уровнях OSI:

VPN в рамках WAN:

+ Не зависят от размеров сети/территории

+ Используются в гетерогенных сетях для организации VPN между разными операторами

- **Требуется поддержка уровней TCP-UDP / IP**
- **Не гарантируют сквозного качества для услуг реального времени**

Основное применение – организация туннелей через Интернет для не очень интенсивного трафика.

Пример популярной технологии – OpenVPN (https://openvpn.net/)

Особенности VPN на различных уровнях OSI:

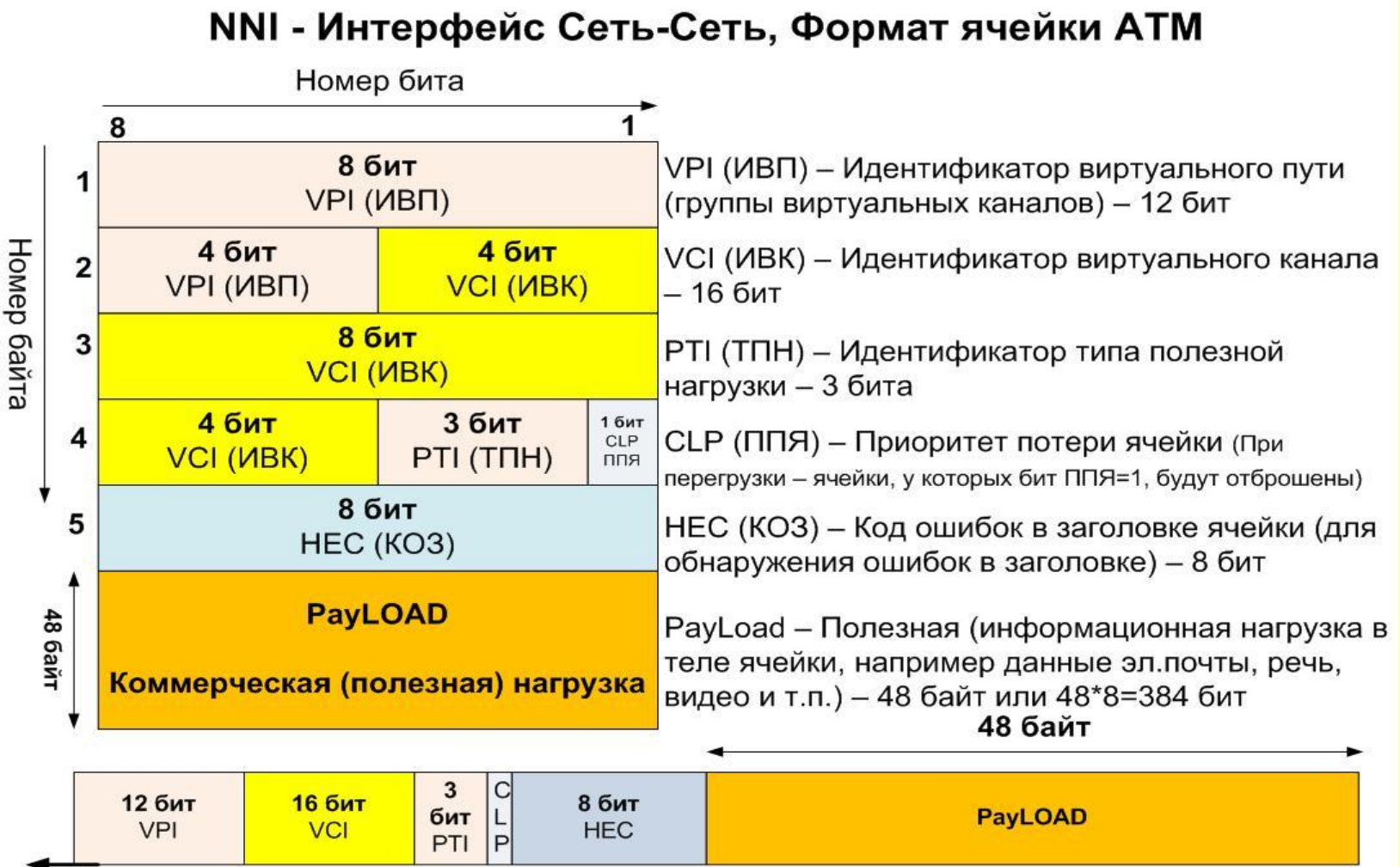
VPN в рамках MAN уровня L2:

+ Гарантируется качество услуг в рамках сети данного оператора

- **Пока недостаточно развиты в межоператорских связях**
- **Требуется разработка нормативной базы для организации межоператорского взаимодействия как по тарифам, так и по качеству**

Технологии VPN / L2 – ATM

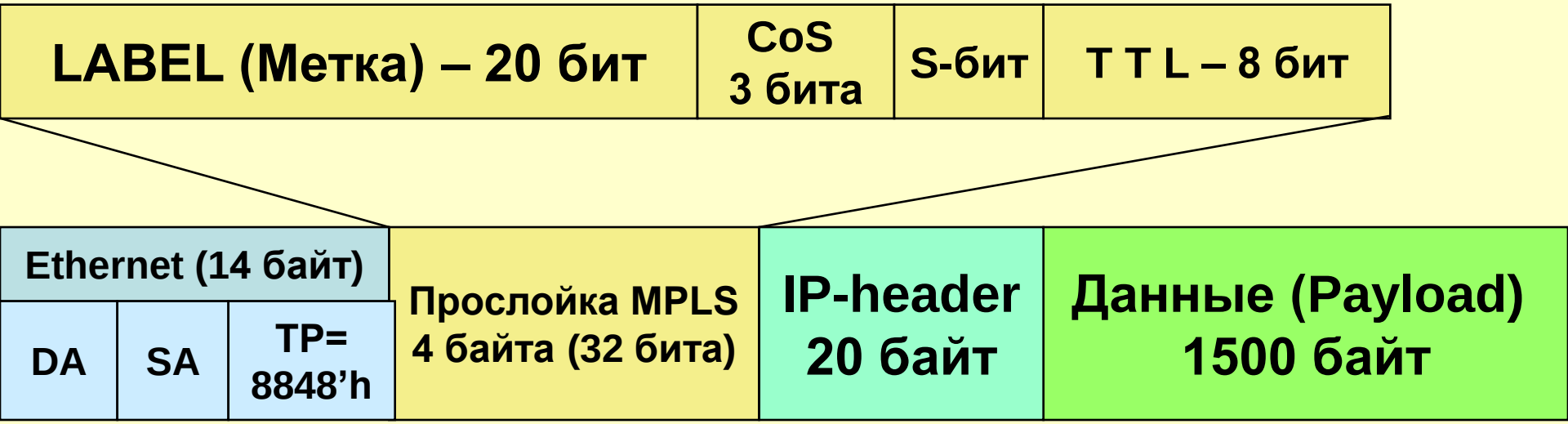
В технологии ATM VPN обеспечивается за счет адресного ресурса VPI.
Номер VPI соответствует номеру VPN.
В интерфейсе NNI – VPI обеспечивает до 2^{12}=4096 VPN
В интерфейсе UNI – VPI обеспечивает до 2^{8}=256 VPN



Технологии VPN уровня L2 поверх Ethernet

		IEEE 802. … - Ethernet технологии				
			IEEE 802.1…			IETF
L2			p/Q	ad	ah (ay)	RFC 3032
			VLAN	Q-in-Q	PBB (TE)	MPLS
	TP		8100	9300 9200 9100 8100	88A8	8847 8848
		(LLC - опционально)				
		MAC (DA-SA-TP---DATA-CRC)				
L1		u-100BT (FE), z-1000BASE-ZX (GE), …				

Технологии VPN / L2 – MPLS



Label обеспечивает до 2^{20}=1 000 000 VPN

S-бит обеспечивает стек меток при взаимодействии сетей и услуг.

Актуальна только одна метка, у которой S=1

Благодаря стекированию меток можно поддерживать неограниченное количество VPN.

Технологии VPN / L2 - IEEE 802.1p/Q (VLAN)

MAC DA	MAC SA	Type/ Size	Data	CRC
6 байт	6 байт	2 байт	46...1500 байт	4 байта

MAC DA	MAC SA	802.1p/Q				Type/ Size	Data	CRC
		8бит	8бит	8бит	8бит			
6 байт	6 байт	Tp=8100'Hex		CoS/CFI/VID		2 байт		4 байта

Tag = TPID + TCI

TPID – 16 бит

TCI=CoS+CFI+VID

Tag Control Information

16 бит

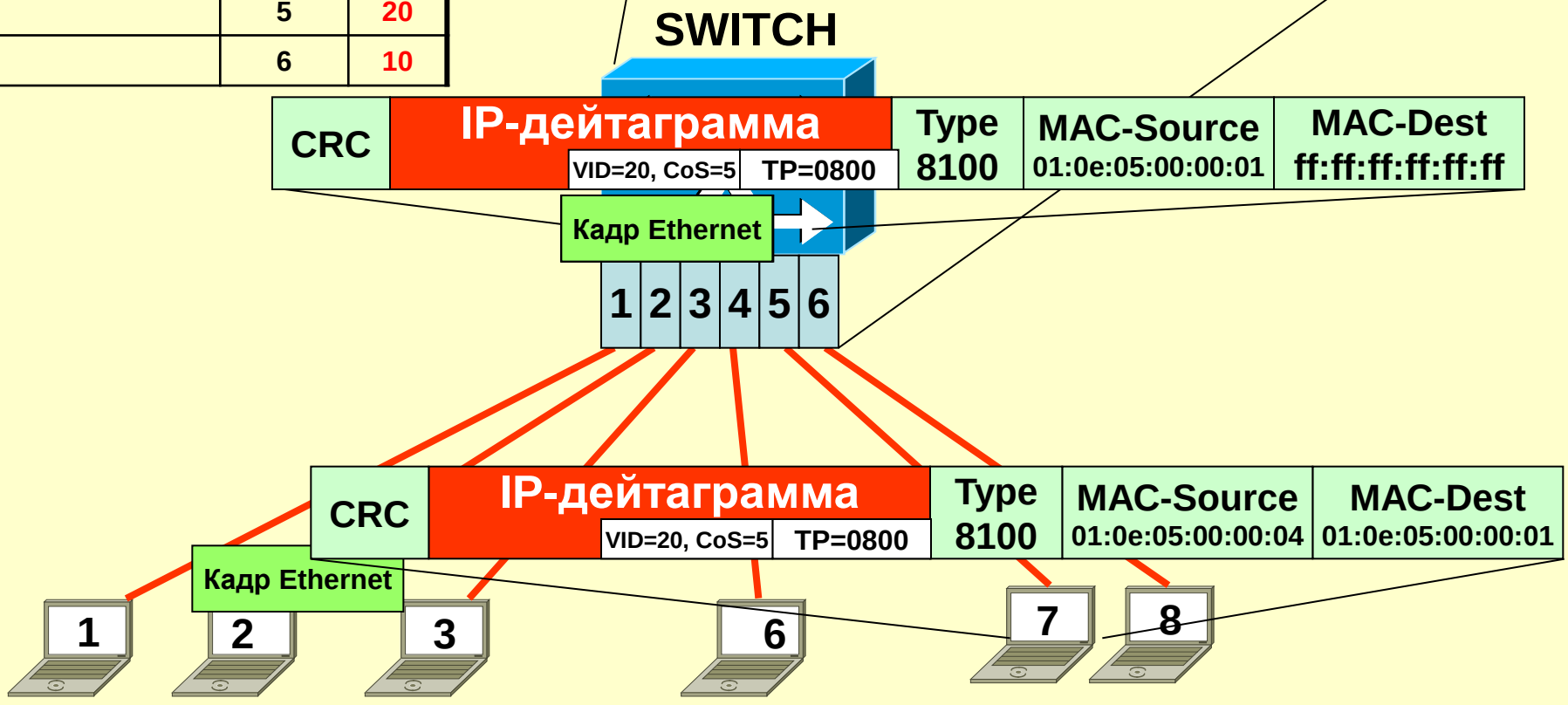
CoS Class of Service	CFI	VID VLAN Identifier
3 бита	1 бит	12 бит
Низкий 000	0 - канонический формат MAC-адреса	Поддержка до 2^{12}=4096 VLAN
001		
	1 - неканонический формат MAC-адреса	
Высокий 111		

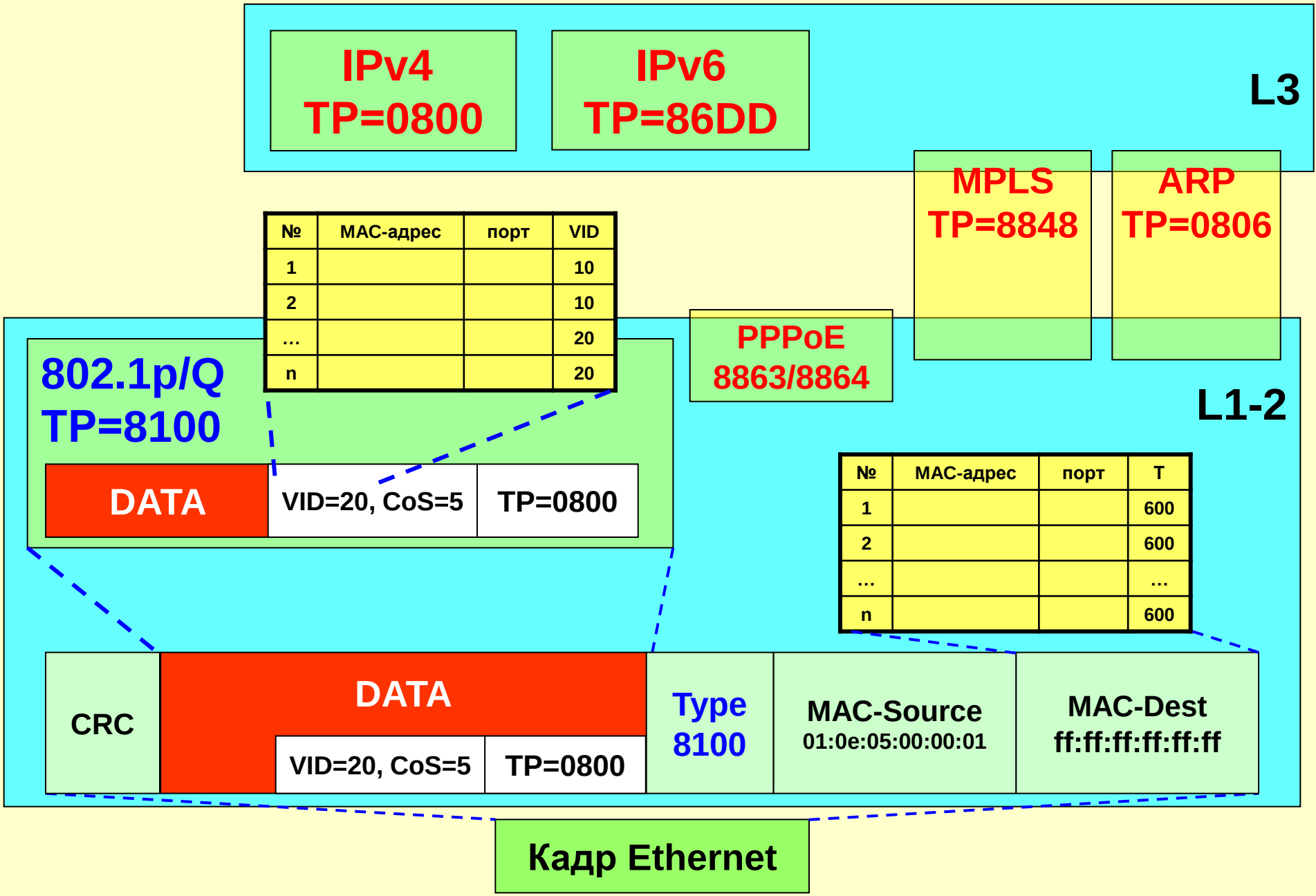
Построение таблицы коммутации (ТК) Ethernet-switch

1. Получив Ethernet-кадр, занести в ТК MAC-адрес источника и номер порта
2. Разослать этот кадр по всем портам коммутатора, кроме источника
3. Принимая кадры в ответ, заносить в ТК MAC-адрес источника и номер порта

№	MAC-адрес	порт	VID
1		1	20
2		2	20
3		3	10
4		4	10
5		5	20
6		6	10

№	MAC-адрес	порт	T
1	01:0e:05:00:00:01	2	600
2	01:0e:05:00:00:04	5	600
…			…
n			600




IPv4
TP=0800
IPv6
TP=86DD
L3
MPLS
TP=8848
ARP
TP=0806
№ MAC-адрес порт VID
1 10
2 10
… 20
n 20
PPPoE
8863/8864
802.1p/Q
TP=8100
L1-2
DATA
VID=20, CoS=5
TP=0800
№ MAC-адрес порт T
1 600
2 600
… …
n 600
CRC
DATA
VID=20, CoS=5
TP=0800
Type
8100
MAC-Source
01:0e:05:00:00:01
MAC-Dest
ff:ff:ff:ff:ff:ff
Кадр Ethernet

Недостатки 802.1Q

- Отсутствие масштабируемости (ограничение в 4096 VLAN)
- В мультисервисной сети не позволяет внедрять новые сервисы независимо от числа клиентов.
- Очень сложная перепланировка карт VLAN-ов при расширении сети как по клиентам так и по сервисам

Наиболее частое применение VLAN – разбиение сетей на подсети на уровне L2 в корпоративных сетях.

Имеет преимущества перед подсетями уровня L3:

- Проще и дешевле организация подсетей (без роутеров)
- Реализуется возможность управления качеством (пропускной способностью, приоритетами – CoS)

Технологии VPN / L2 - IEEE 802.1ad (Q-in-Q)

Стек IEEE 802.1ad				
8100	Inner VLAN	p/Q	Inner Tag	Tag4
9100	Q-in-Q	ad	PE VLAN Tag	Tag3
9200	Q-in-Q	ad	Metro Tag	Tag2
9300	Q-in-Q	ad	Outer Tag	Tag1
MAC (DA-SA-Tag1-Tag2-Tag3-Tag4-TP---DATA-CRC)				

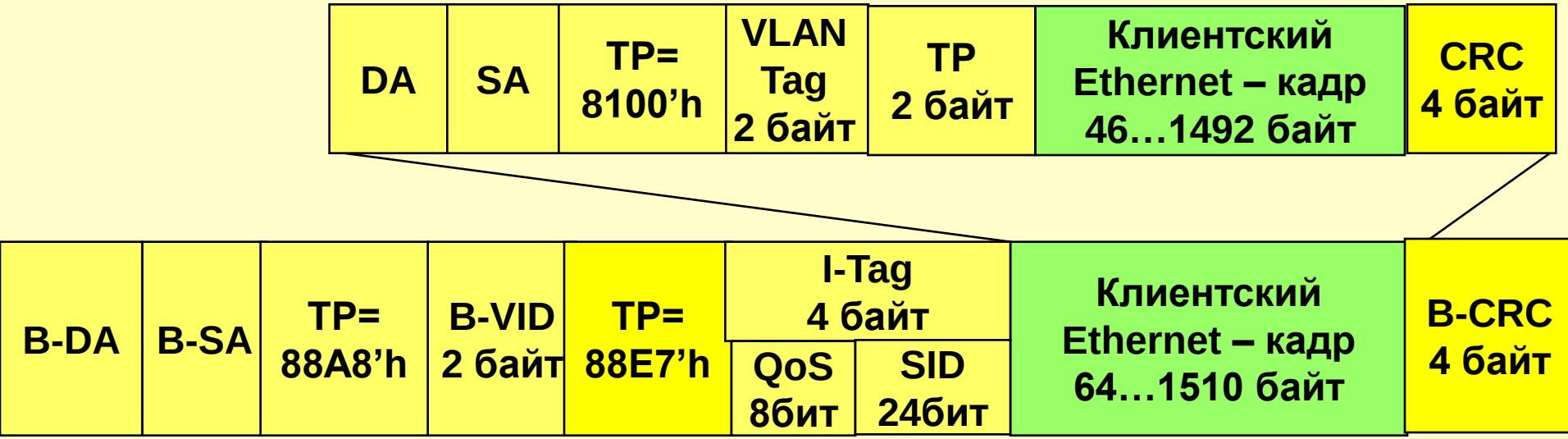
Технология Q-in-Q снимает ограничения на кол-во VLAN, позволяет агрегировать VLAN по видам сервиса и клиентам, упрощает взаимодействие между операторами

<table>
<tr><td rowspan="2">DA</td><td rowspan="2">SA</td><td>TP= 9100’h</td><td>CoS/CFI/VID</td><td>TP= 8100’h</td><td>CoS/CFI/VID</td><td rowspan="2">TP= 0800’h</td><td rowspan="2">IP-header 20 байт</td><td rowspan="2">Данные (Payload) 1500 – N байт</td></tr>
<tr><td colspan="2">TP = 9100’hex
802.1Q Outer Tag
4 байта (32 бита)</td><td colspan="2">TP = 8100’hex
802.1Q Inner Tag
4 байта (32 бита)</td></tr>
</table>

Технологии VPN / L2 - PBB-TE (IEEE 802.1Qay)

На основе технологии Nortel - PBT (Provider Backbone Transport) и 802.1ad (Q-in-Q)

Стек PBB-TE (IEEE 802.1Qay)				
8100	VLAN p/Q	p/Q	Inner Tag	Tag3
88E7	I-TAG	ad	Metro Tag	Tag2
88A8	B-VID	ad	Outer Tag	Tag1
MAC (DA-SA-Tag1-Tag2-Tag3-TP---DATA-CRC)				



Метка в опорной сети B-VID обеспечивает до 2^{16} = 65 000 VPN

Метка сервиса (I-Tag) содержит параметры QoS (8бит), а также поле SID размером 24 бит, которое используется для идентификации клиентов или сервисов.

СПАСИБО за ВНИМАНИЕ