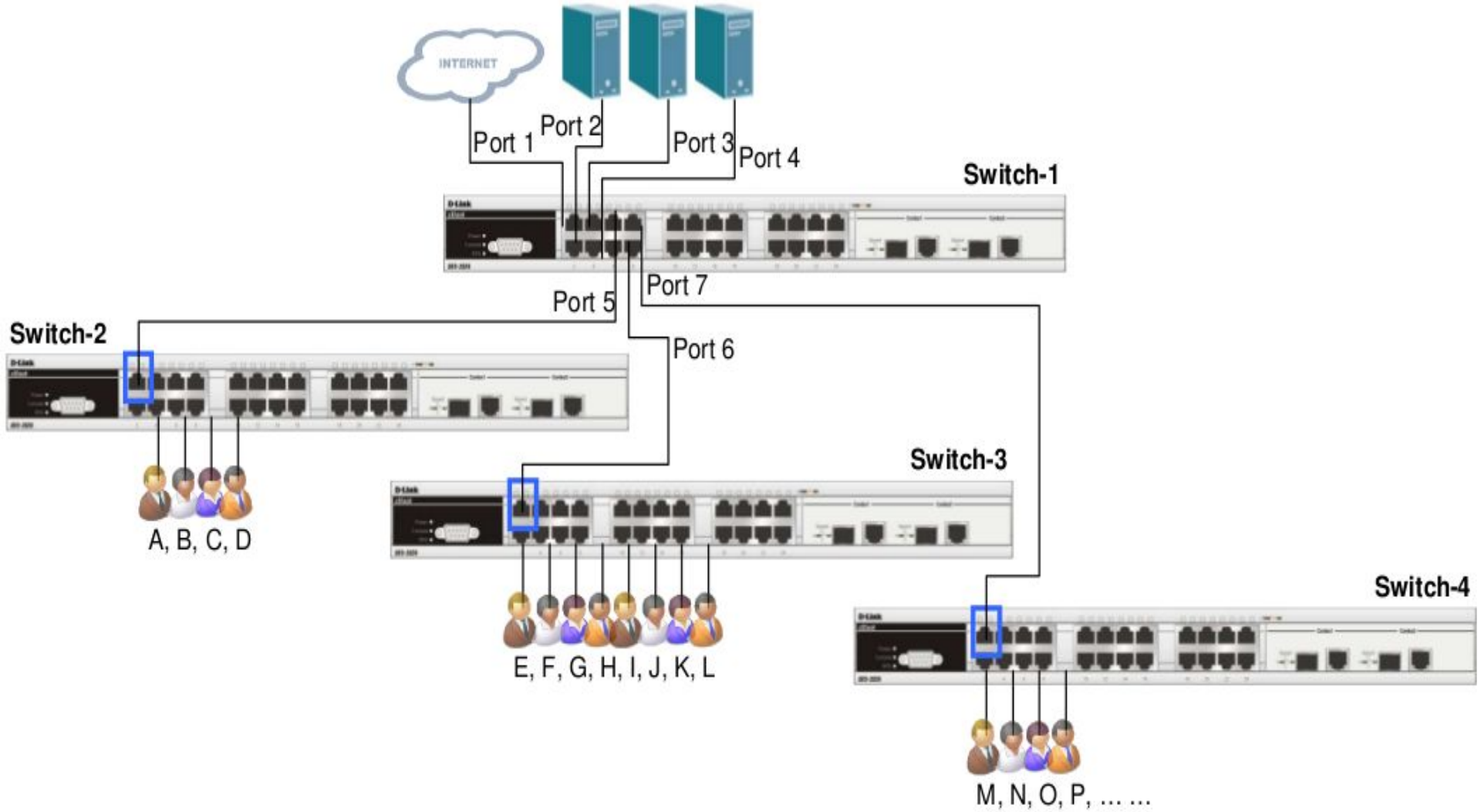
VLAN

Технологии защиты сетей

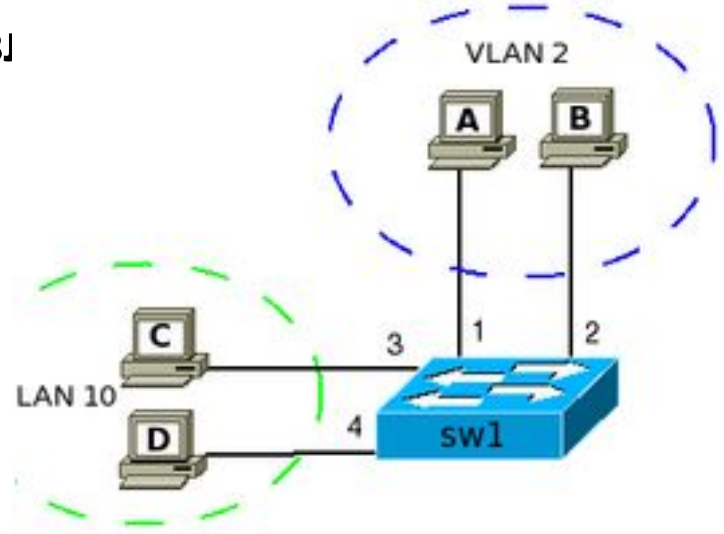
Иерархическая сегментация трафика для изоляции портов



VLAN

- **VLAN** (Virtual Local Area Network) — группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам
- **ПРЕИМУЩЕСТВА**
- **Гибкое разделение устройств на группы**
- **Уменьшение количества широковещательного трафика в сети**
- **Увеличение безопасности и управ**

Порт коммутатора	VLAN	MAC-адрес хоста
1	2	A
2	2	B
3	10	C
4	10	D

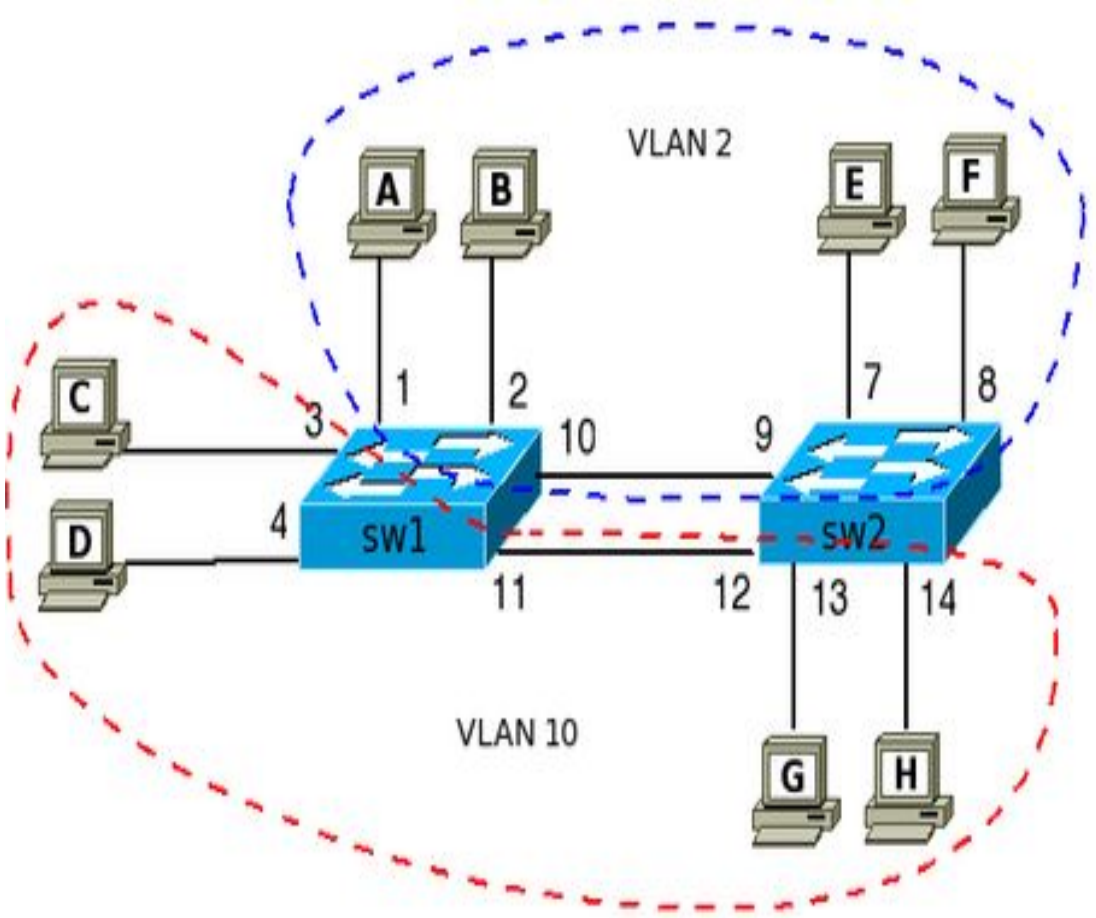


Тегированные порты

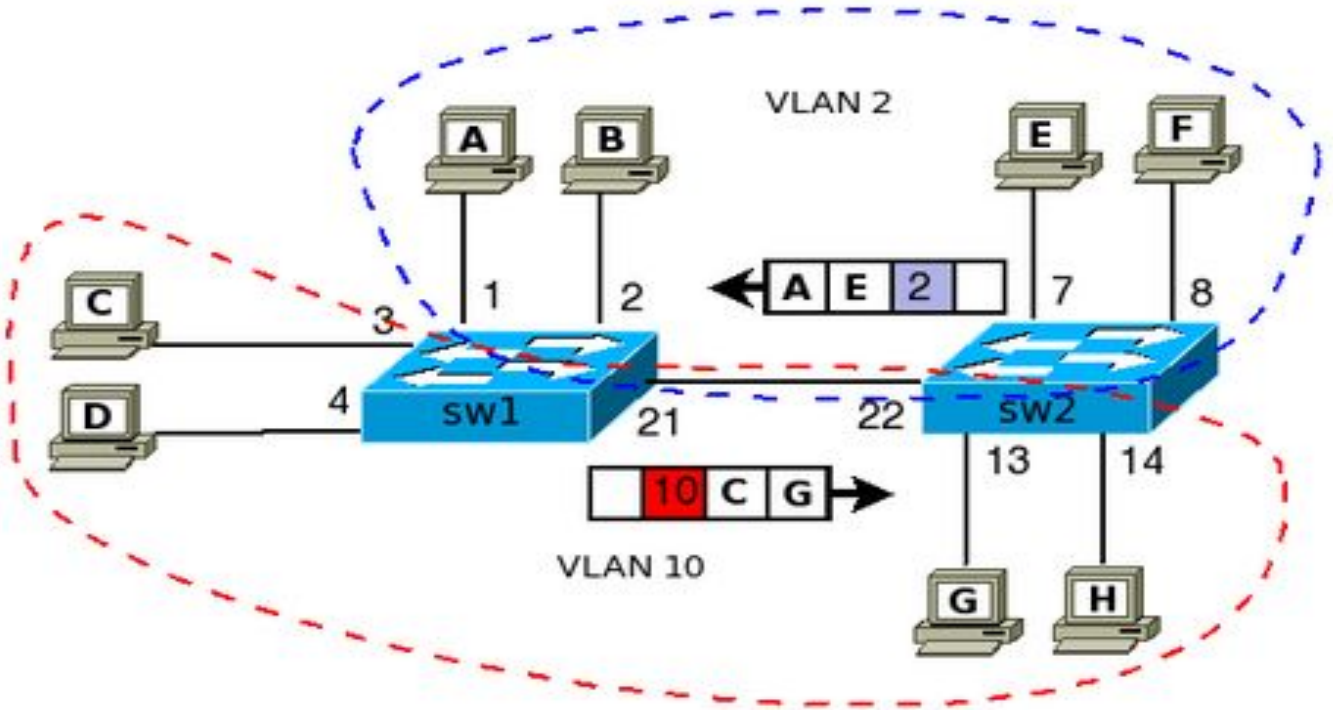
Порт коммутатора	MAC-адрес хоста
3	C
4	D
11	G
11	H

Таблица коммутации **sw2 для VLAN 10**:

Порт коммутатора	MAC-адрес хоста
13	G
14	H
12	C
12	D



Тегированные/Транковые порты



- Например, если хост E передает фрейм хосту A, то коммутатор sw2 проверяет свою таблицу и видит, что хост A доступен через порт 22. Так как порт настроен как тегированный, то когда фрейм выходит с порта 22 в нём проставляется тег, который указывает какому VLAN'у принадлежит этот фрейм. В данном случае проставляется тег с VLAN'ом 2.

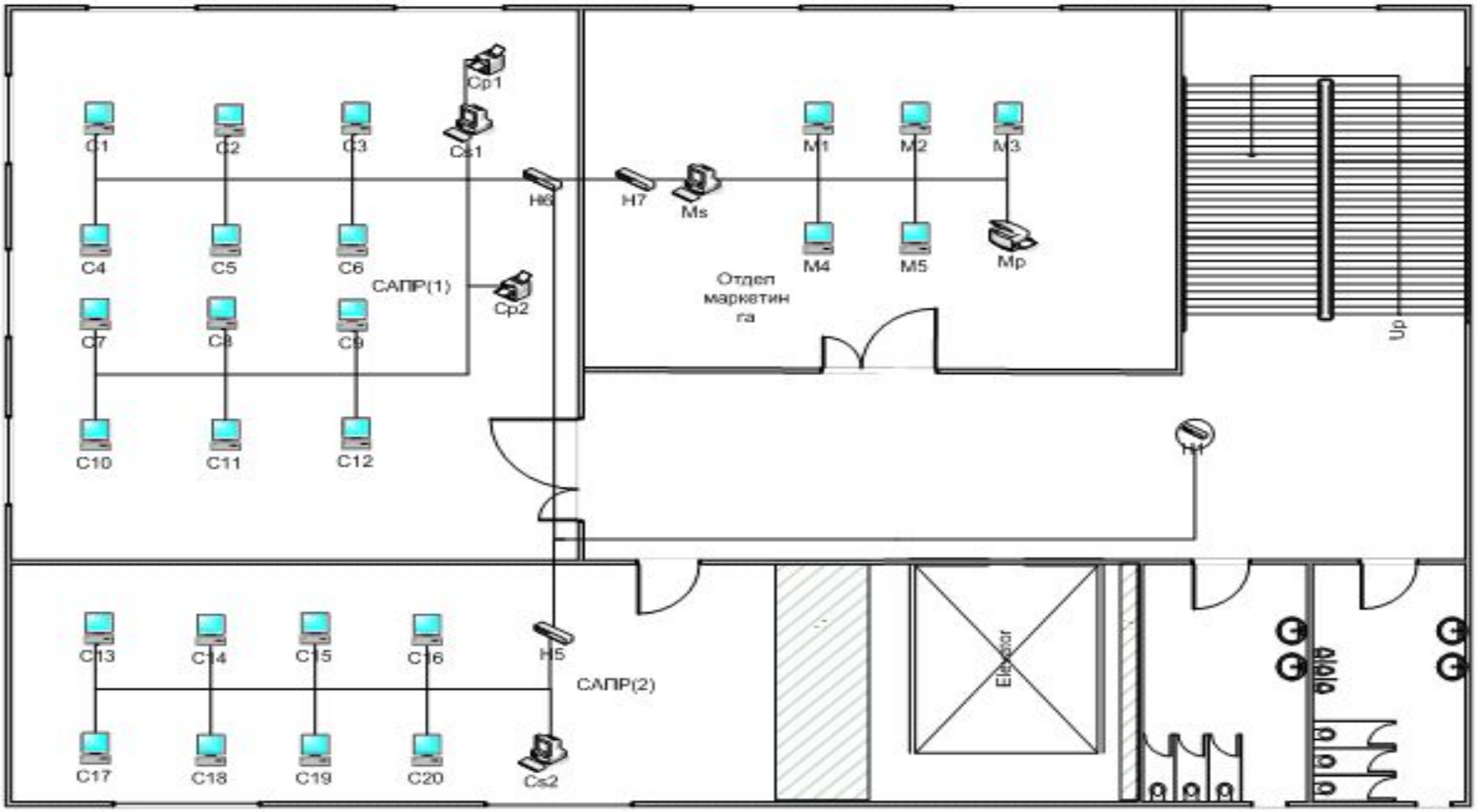
Проектирование сети

- Постановка задачи
- 1. Определение зон подключение
- 2. Разделение групп пользователей, участвующих в операционной деятельности и способы доступа к требуемой информации
- 3. Оценка необходимого оборудования и интерфейсов, каналов связи
- Согласование
- Разработка политики безопасности
- Разработка документации

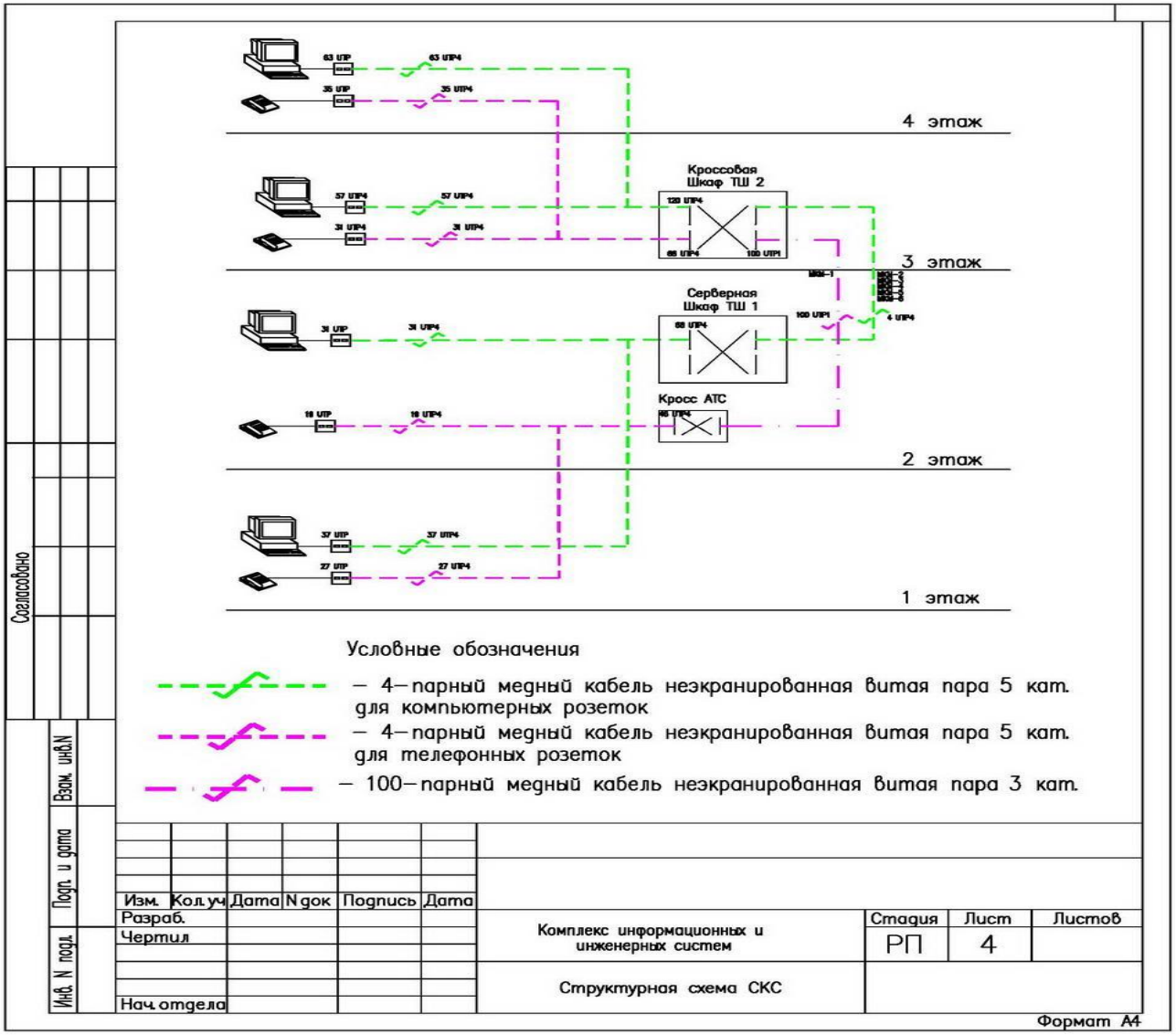
Документация сети

- Титульный лист;
- Оглавление;
- Пояснительная записка;
- Схема прокладки кабельных трасс (ЛВС, ВОЛС);
- Схем расположения и состава рабочих мест;
- Схема расположения оборудования и проводок;
- Таблица кабельных соединений (Кабельный журнал);
- Схема монтажа и размещения оборудования в коммутационных шкафах и помещениях;
- Структурная схема СКС, отражающая коммутацию портов и кроссового оборудования;
- Протокол тестирования СКС (по требованию заказчика, для проведения сертификации СКС);
- Руководство по эксплуатации СКС. (по требованию заказчика, содержит рекомендации по поддержанию работоспособного состояния СКС, перечень и сроки гарантийного и сервисного обслуживания).

Схема прокладки кабельных трасс, расположения и состава рабочих мест



Структурная схема СКС, отражающая коммутацию портов



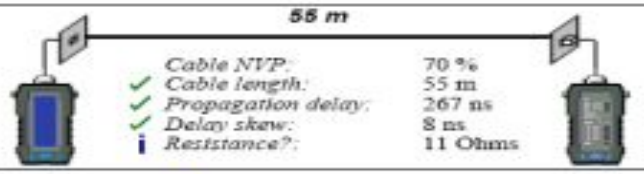
Пример протокола тестирования одной кабельной линии представлен на рисунке.

Site:
Cable Label: **PT.102.01.1**

5E
PASS

Cable Certification Report (PowerSum data)

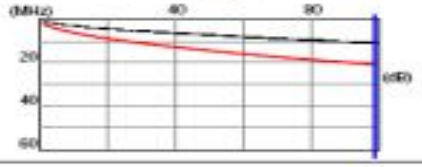
Limit: TIA-568B Category 5E Link
Tested: 21.07.2004 9:54
Cable: Avaya 1061 Power-Sum
WS 350 SG42301616 with Agilent Technologies Cat 6 Link (146)
DR 350 SG42302293 with Agilent Technologies Cat 6 Link (149)
Profile: Default Cat 5e



Cable NVP:	70 %
Cable length:	55 m
Propagation delay:	267 ns
Delay skew:	8 ns
Resistance?:	11 Ohms

✓ ***Attenuation (dB)***

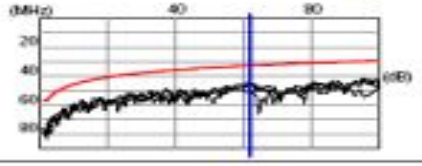
Worst pair:	*1 (4,5)*
Value (dB):	*11,2*
Limit (dB):	*20,8*
Margin (dB):	*9,6*
Frequency (MHz):	*98,75*

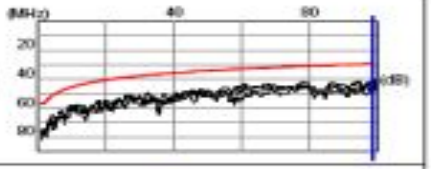


Wiremap (pairing T568B)

✓ ***PowerSum NEXT (dB)***

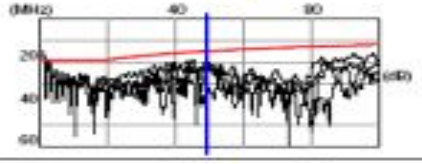
	@WS	***@DR***
Worst pair:	*3 (3,6)*	*1 (4,5)*
Value (dB):	*44,3*	*40,0*
Limit (dB):	*32,7*	*29,4*
Margin (dB):	*11,6*	*10,6*
Frequency (MHz):	*61,75*	*99,00*

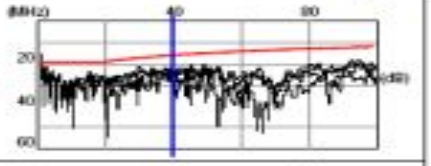




✓ ***Return Loss (dB)***

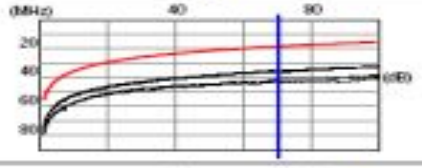
	@WS	***@DR***
Worst pair:	*1 (4,5)*	*3 (3,6)*
Value (dB):	*18,7*	*20,0*
Limit (dB):	*15,1*	*16,0*
Margin (dB):	*3,6*	*4,0*
Frequency (MHz):	*49,00*	*39,75*

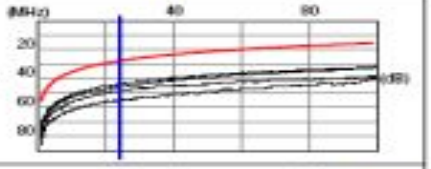




✓ ***PowerSum ELFEXT (dB)***

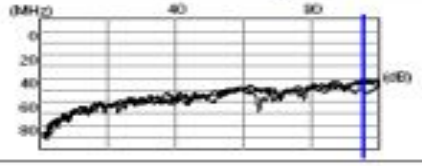
	Atten(TX)	***Atten(RX)***
Worst pair:	*2 (1,2)*	*2 (1,2)*
Value (dB):	*34,9*	*43,5*
Limit (dB):	*18,7*	*27,9*
Margin (dB):	*16,2*	*15,6*
Frequency (MHz):	*70,00*	*24,38*

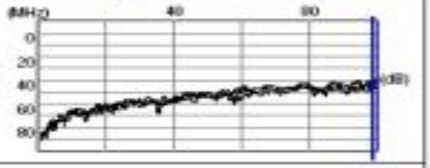




i ***PowerSum ACR? (dB)***

	@WS	***@DR***
Worst pair:	*1 (4,5)*	*1 (4,5)*
Value (dB):	*30,7*	*29,0*
Limit (dB):		
Margin (dB):		
Frequency (MHz):	*95,25*	*98,75*

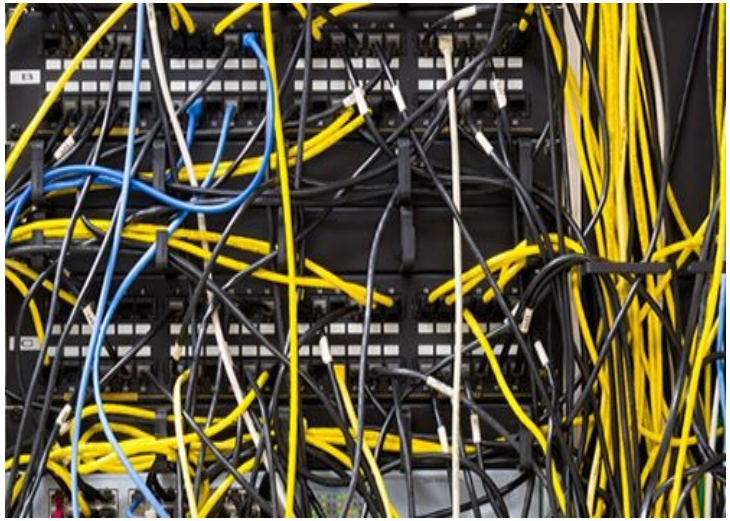


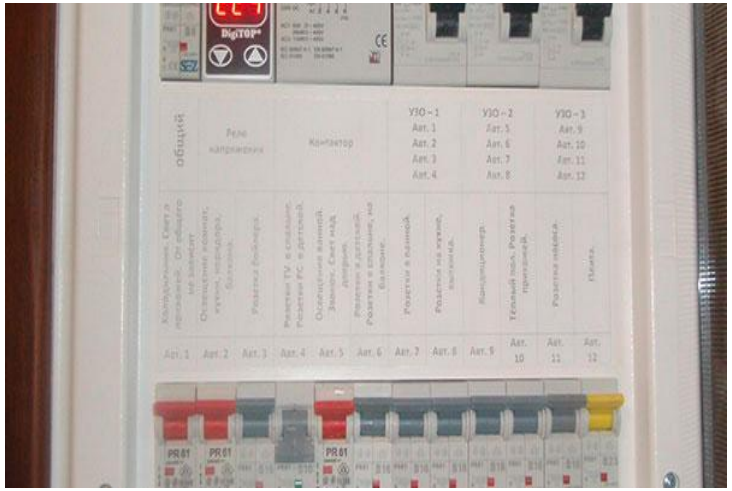


Networks tested

10 Base-T	***PASS***	*100 Base-Tx*	***PASS***	*1000 Base-T*	***PASS***

Маркировка





- Указываем: модель железки, установленная версия IOS, объем RAM\NVRAM, список интерфейсов, метки на кабелях

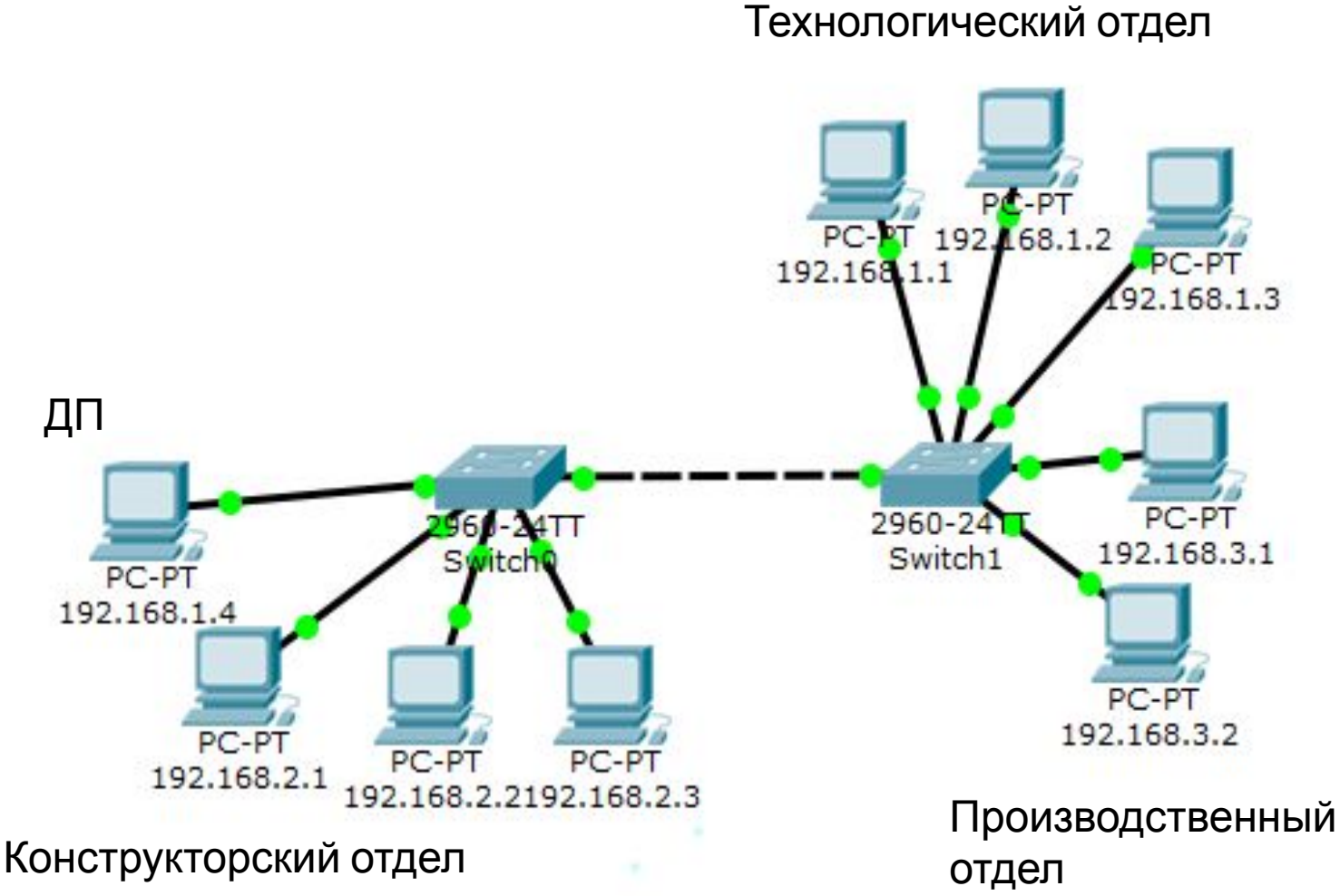
Планирование

- Представим, что у компании есть два офиса, территориально расположенных удаленно друг от друга
- Имеется четыре группы пользователей: Бухгалтерия, Финансово-экономический отдел, Производственный отдел, Технологический и Конструкторский отделы. А так же есть сервера, которые вынесены в отдельную группу.
- Все группы разграничены и не имеют прямого доступа друг к другу. Пользователи производственного, технологического и конструкторского отделов расположенный отдельно от других отделов компании.
- Подготовьте схему сети и IP-план.

Планирование

- При проектировании сети следует
- придерживаться иерархической модели сети, которая имеет много достоинств по сравнению с “плоской сетью”
- модель подразумевает модульность,
- масштабируемость
- повышенная отказоустойчивость за счет дублирования устройств и/или соединений и/или реконфигурации
- распределение функций по обеспечению работоспособности сети по различным устройствам.

Разработка структурной схемы подсети



Планирование. Таблица VLANов

- Каждая группа выделяется в отдельную подсеть, это позволяет ограничить трафик и широковещательные домены.
- Необходимо предусмотреть расширение подсетей за счет присоединения новых пользователей (оставляем порты) и номеров подсетей (в случае создания новых отделов или реорганизации)

VLAN	VLAN name	Примечание
1	technological	Технологический отдел
2	constuctor	Конструкторский отдел
3	production	Производственный отдел

Планирование. Таблица VLANов

- Выделение адресов в подсетях в общем-то произвольное, соответствующее только числу узлов в этой локальной сети. В примере все подсети имеют стандартную маску /24 (/24=255.255.255.0).

IP-адрес	Примечание	VLAN
192.168.1.0/24	**Технологический отдел**	1
192.168.1.1	Шлюз	
192.168.1.2— 192.168.1.254	Пул для пользователей	
192.168.2.0/24	**Конструкторский отдел**	2
192.168.2.1	Шлюз	
192.168.1.2— 192.168.2.254	Пул для пользователей	
192.168.3.0/24	**Производственный отдел**	3
192.168.3.1	Шлюз	
192.168.3.2— 192.168.3.254	Пул для пользователей	

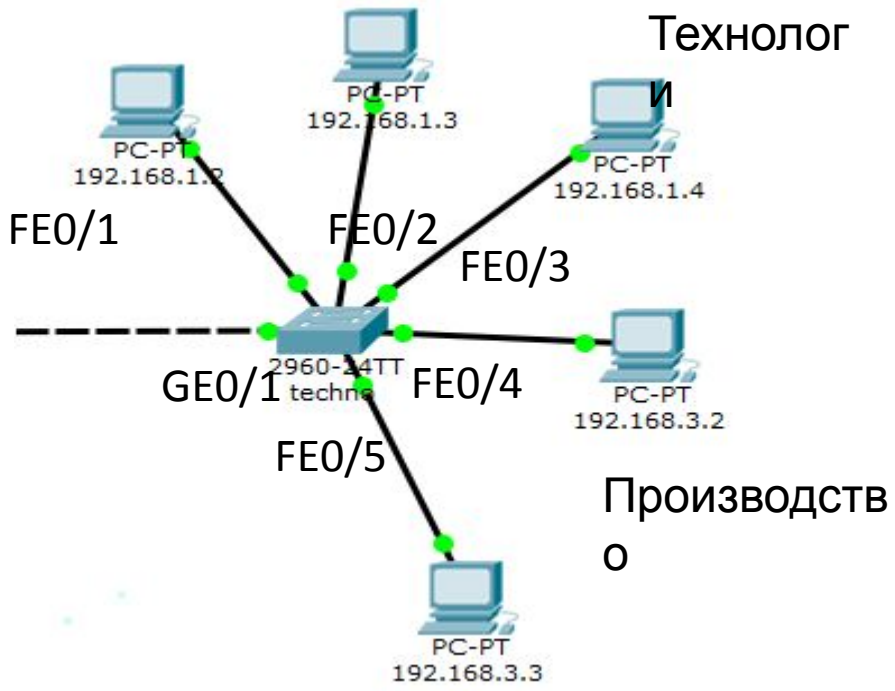
Планирование. Подключение по портам

- Внутрисетевое разделение по портам необходимо для правильного построения сети и межсегментного разделения трафика. Это позволяет правильно сформировать стек протоколов маршрутизации.

Имя устройства	Порт	Название	VLAN
Access	Trunk		
switch0	FE0/24	Технологический отдел	1
switch0	FE0/24	Конструкторский отдел	2
switch0	GE0/1		
switch1	FE0/24	Производственный отдел	3
switch1	GE0/1	msk-rubl-asw1	

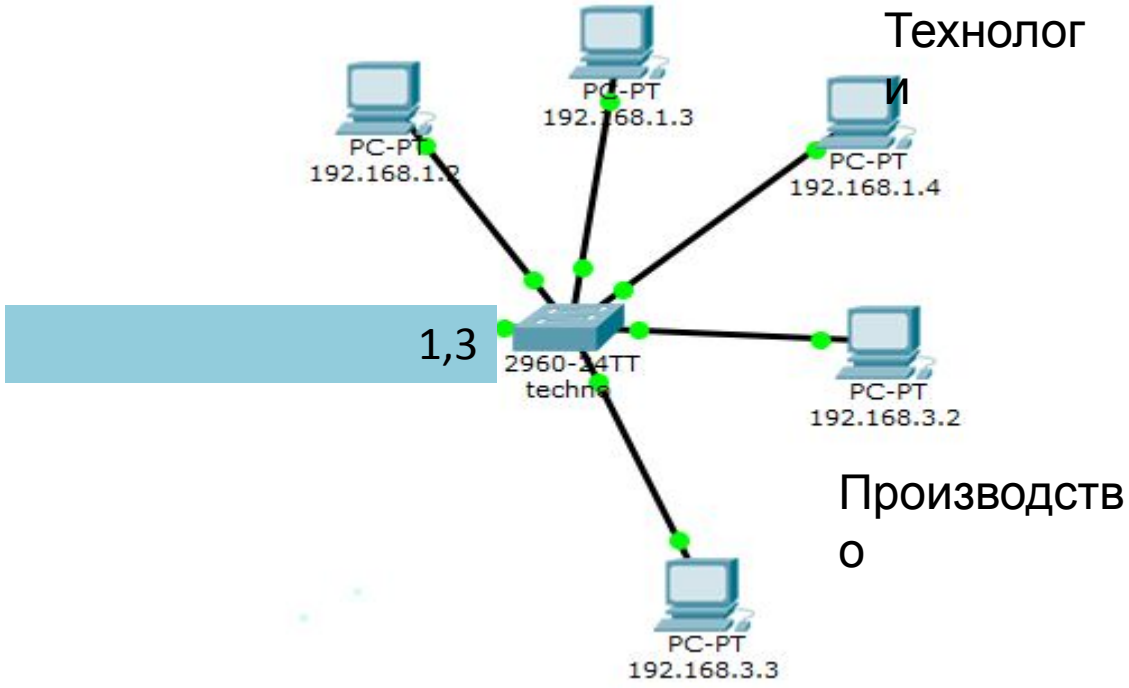
Разработка структурной схемы подсети

- На основании этих данных можно составить все три схемы сети на этом этапе L1 (физический уровень)
- То есть на схеме L1 мы отражаем физические устройства сети с номерами портов: что куда подключено.



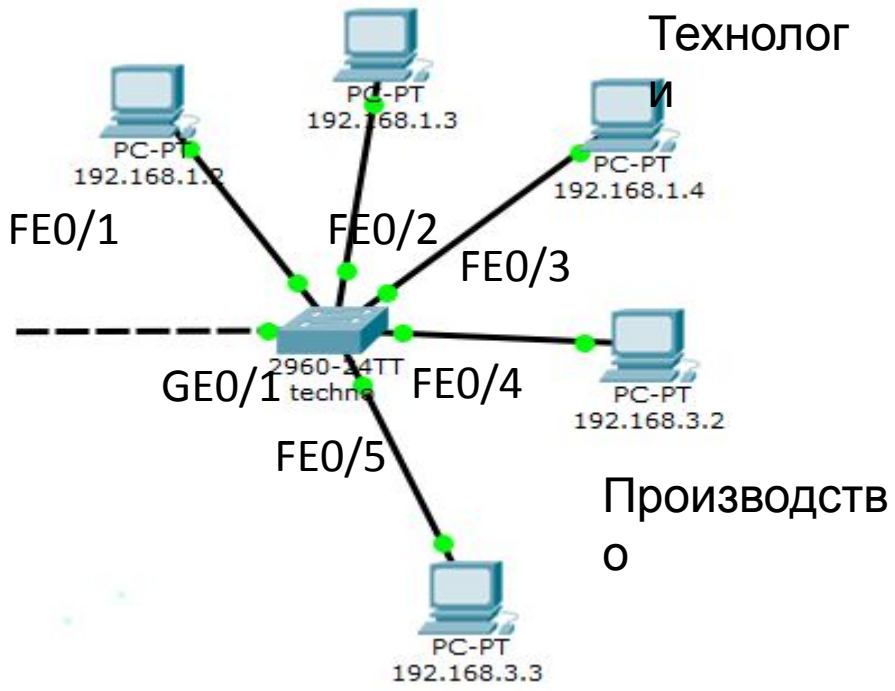
Разработка структурной схемы подсети

- На схеме второго уровня L2 указываем наши VLAN’ы
- Схема третьего уровня L3 показывает подключение маршрутизаторов, ее представим в следующих лекциях



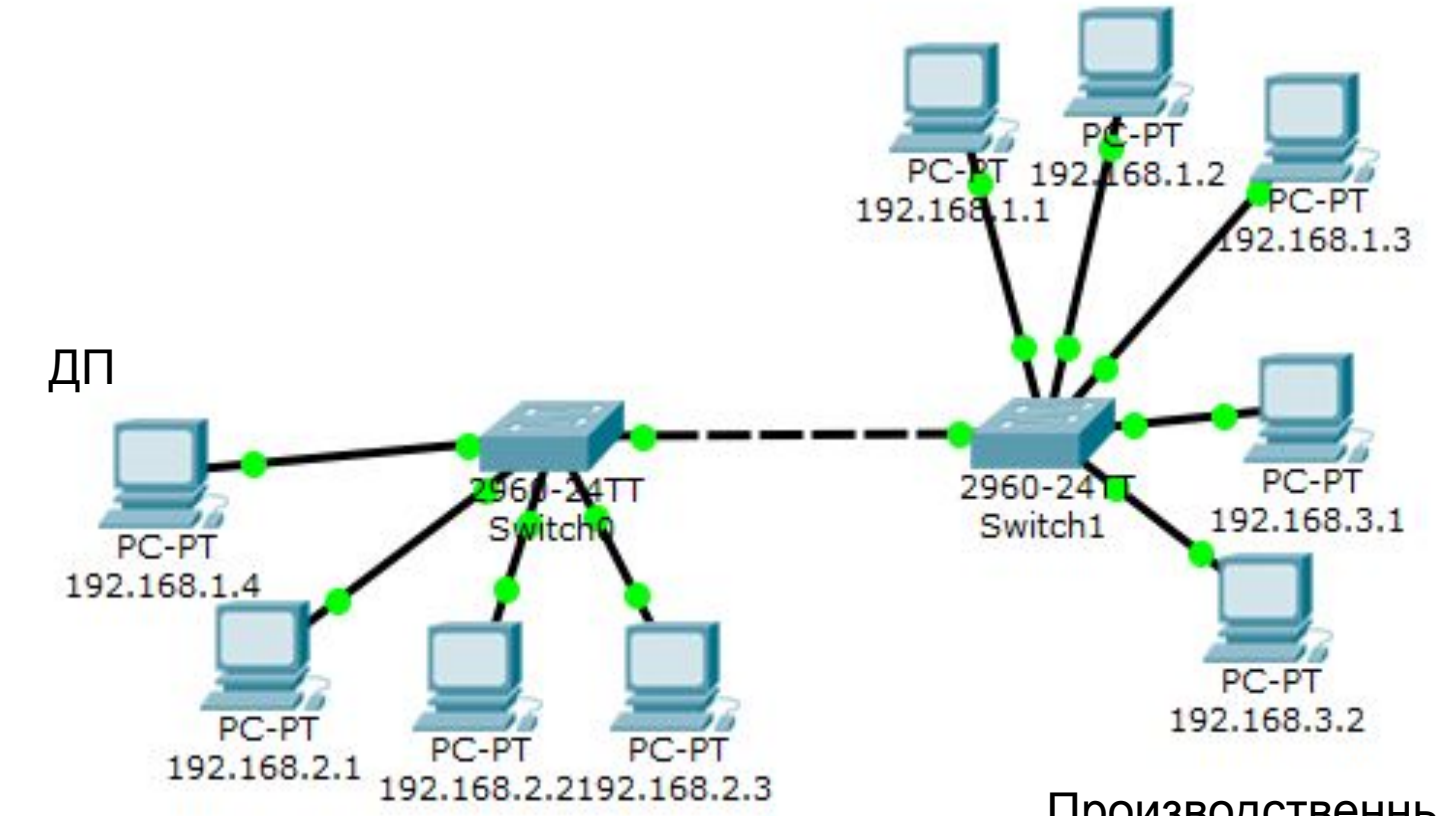
Разработка структурной схемы подсети

- На основании этих данных можно составить все три схемы сети на этом этапе L1 (физический уровень)
- То есть на схеме L1 мы отражаем физические устройства сети с номерами портов: что куда подключено.



Подключение устройств

Технологический отдел



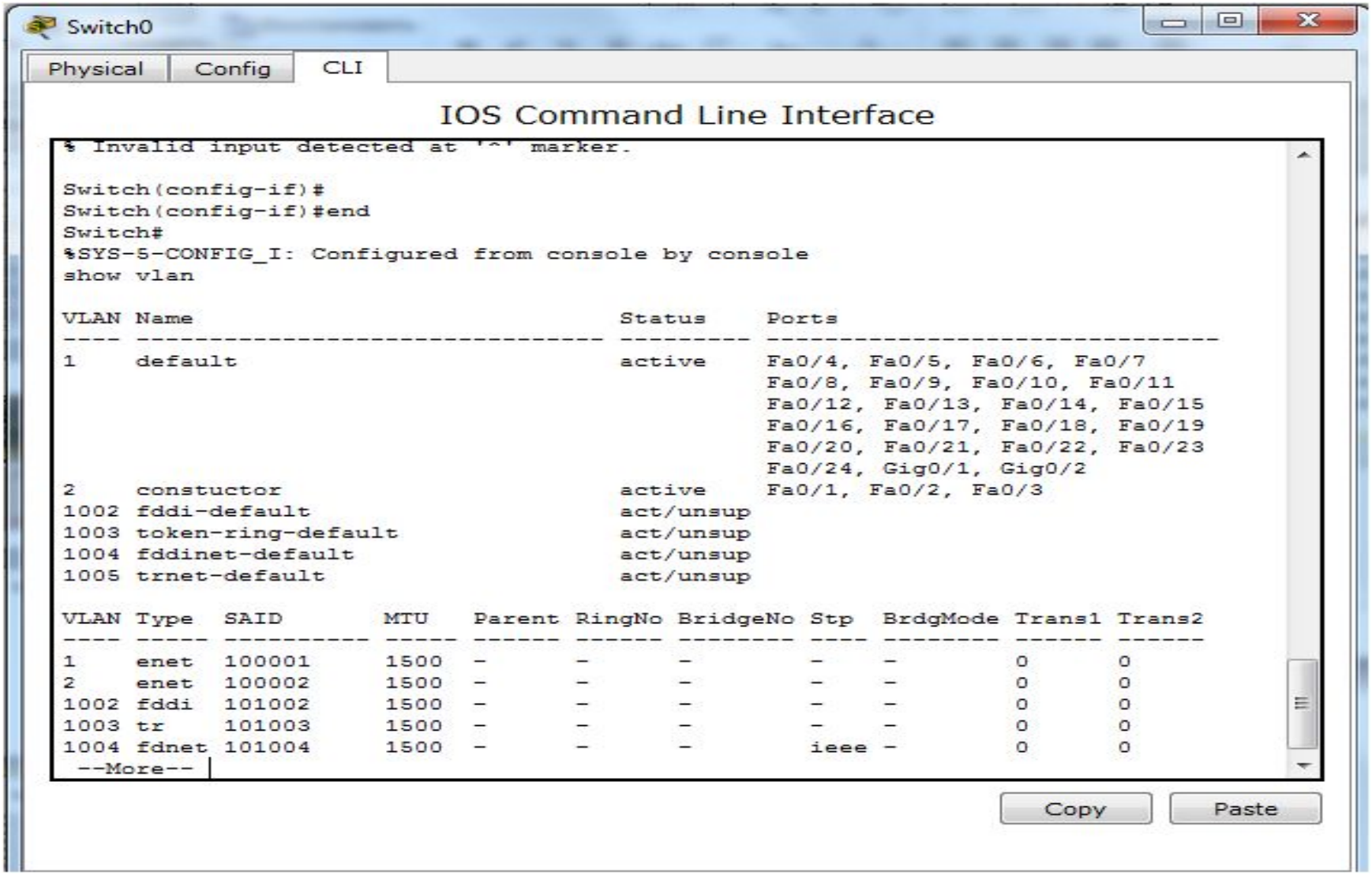
Конструкторский отдел

Производственный отдел

Привязка интерфейсов портов к VLAN

```
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#
```

Проверка подключения к VLAN



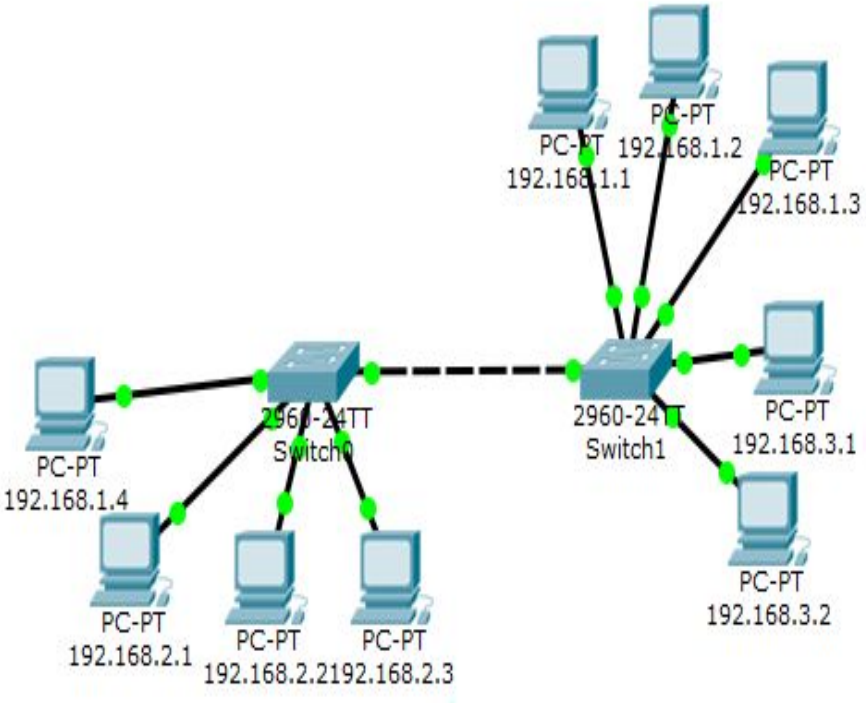
Проверка подключения к VLAN

192.168.1.3

Physical | Config | Desktop | Custom Interface

Command Prompt

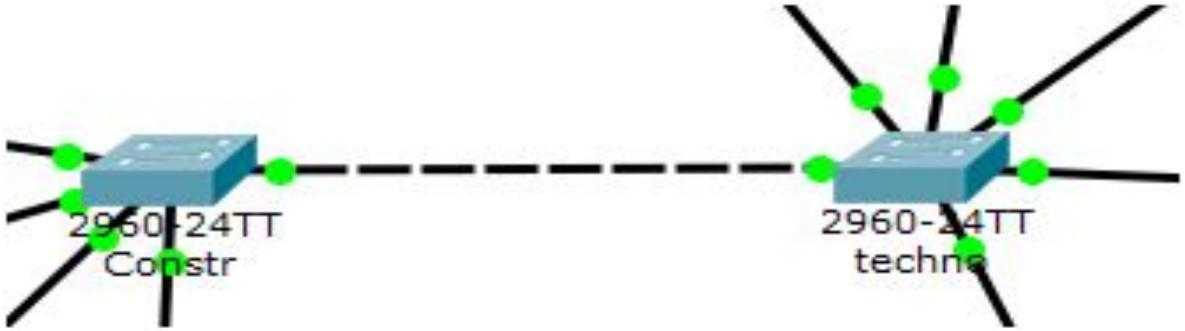
```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```



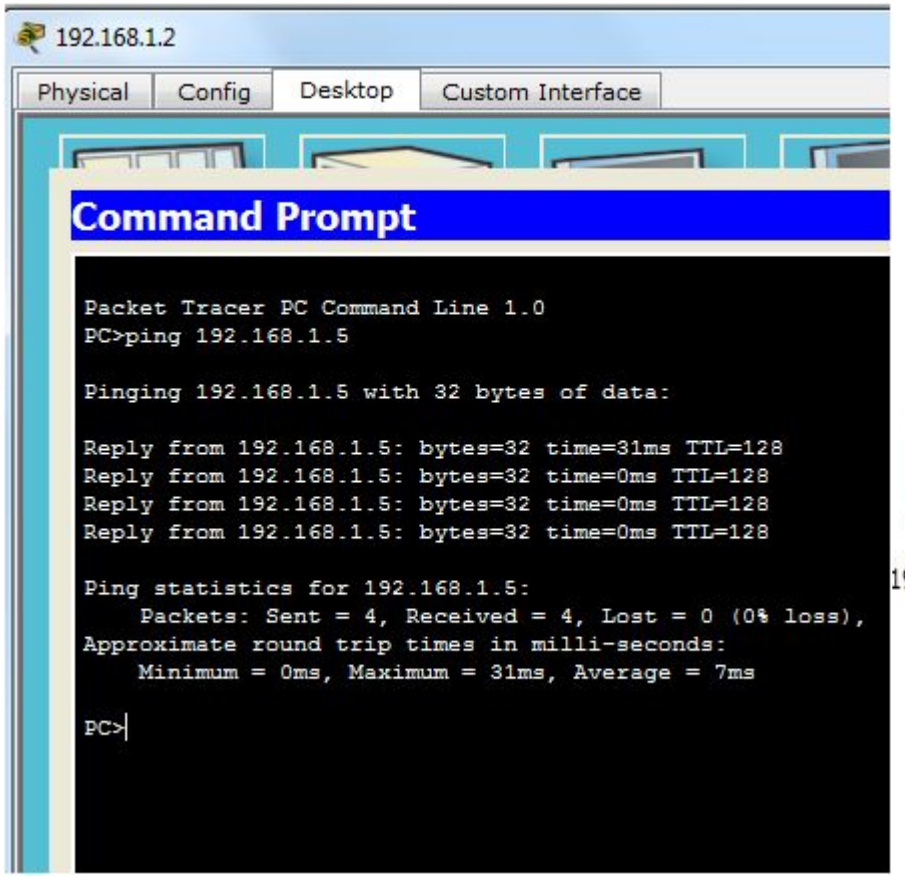
Ping от 192.168.1.3 к 192.168.1.3 успешно

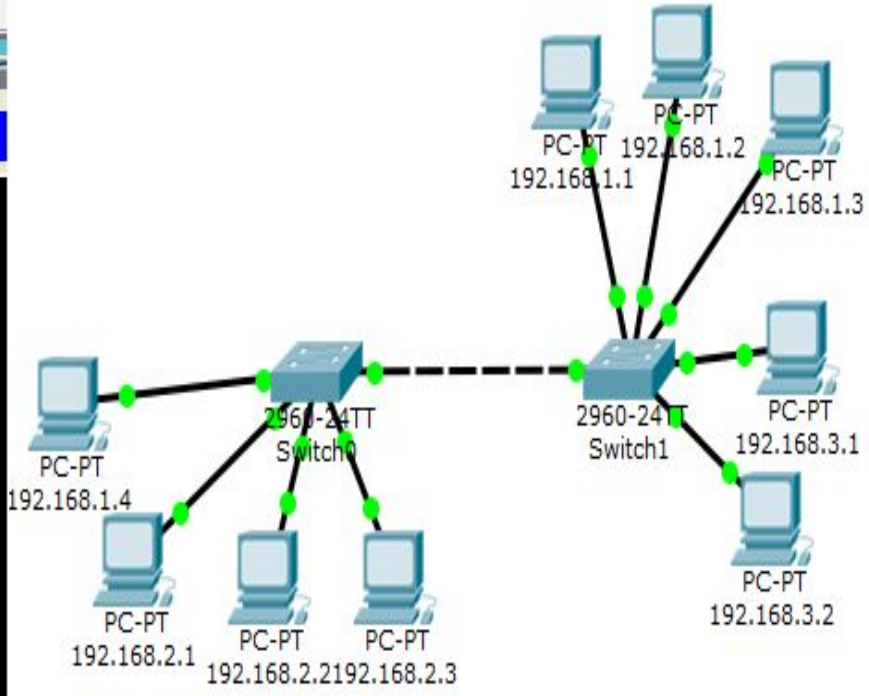
Настройка транковых портов

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gi0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 2
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#end
```



Проверка подключения к VLAN





Проверка подключения к VLAN