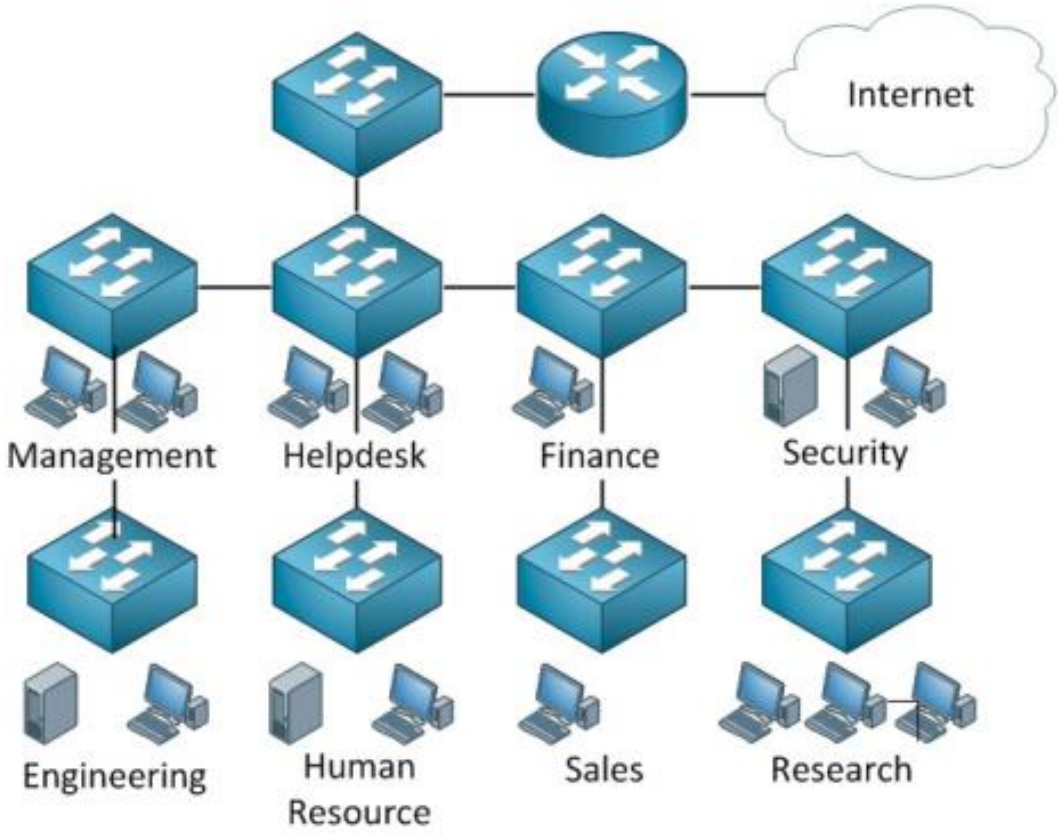
Рачунарске мреже (вежбе – термин 7)

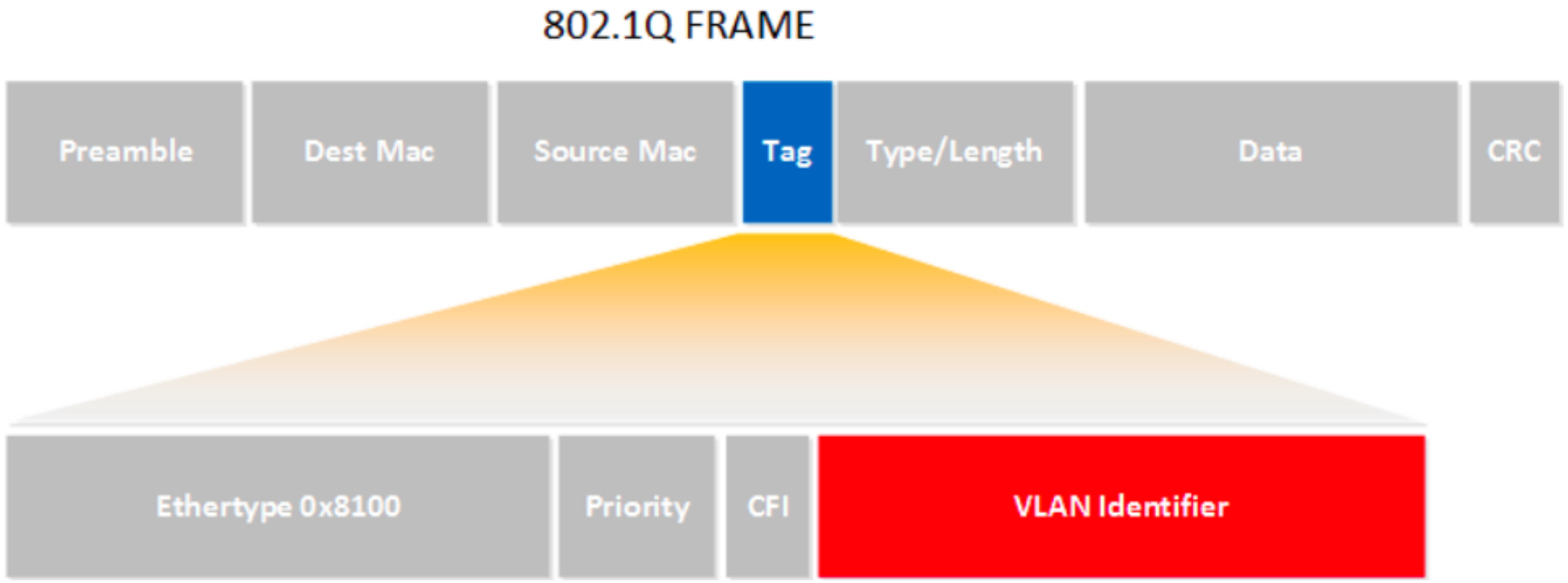
VLAN и Port-security

Увод VLAN

- Виртуални LAN (VLAN) представља логичку поделу на групе уређаја који физички деле LAN, где је саобраћај између група изолован

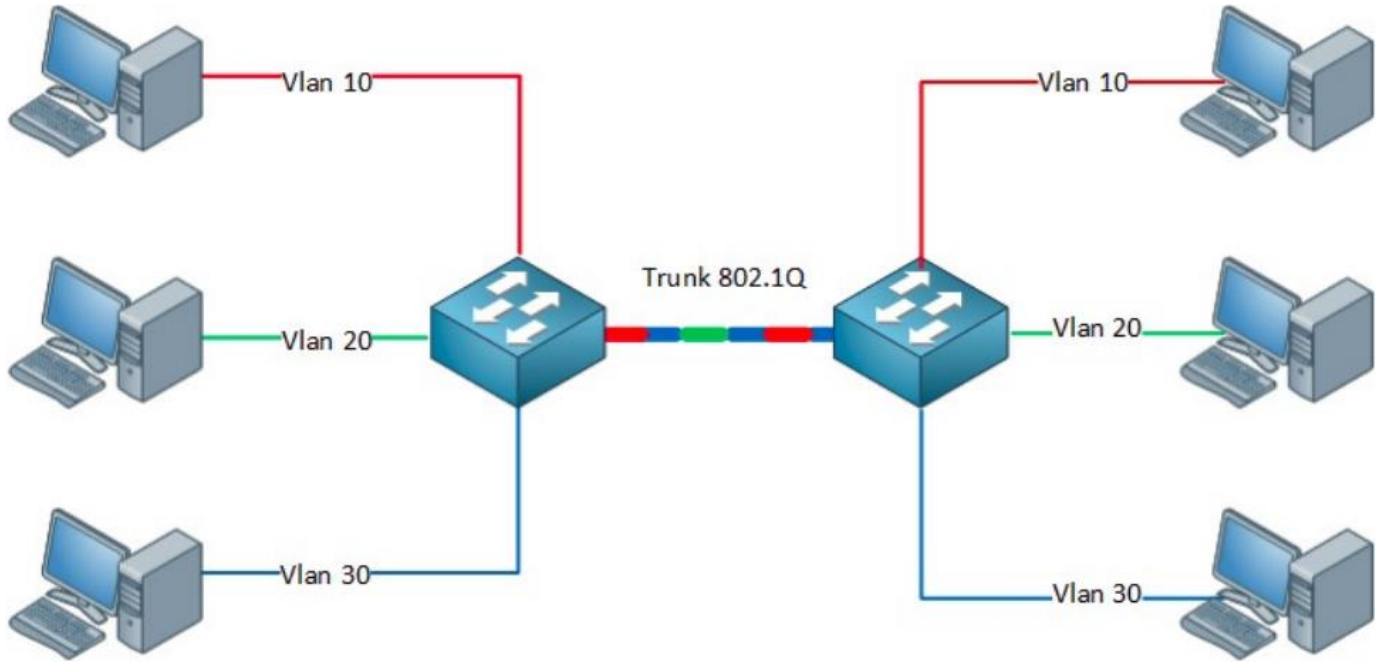


VLAN заглавље

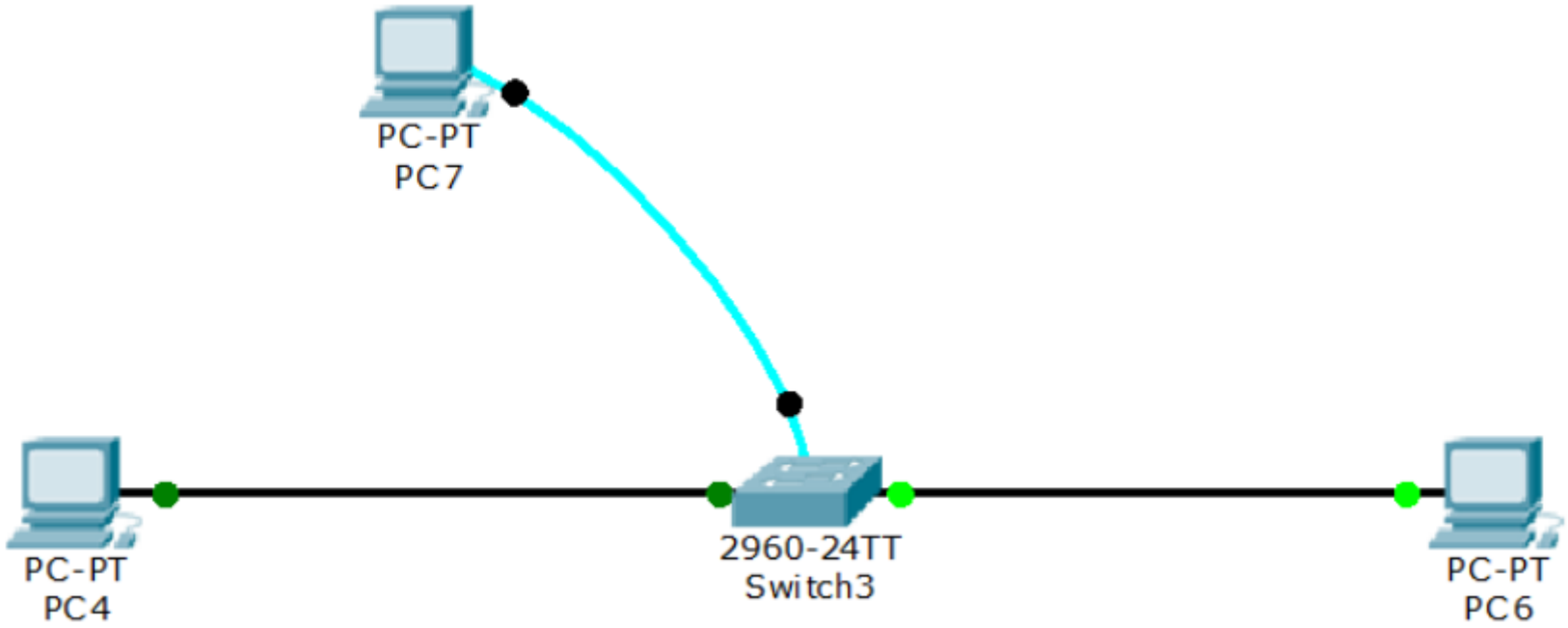


Модови

- Access
- Trunk
- Dynamic



Задатак 1



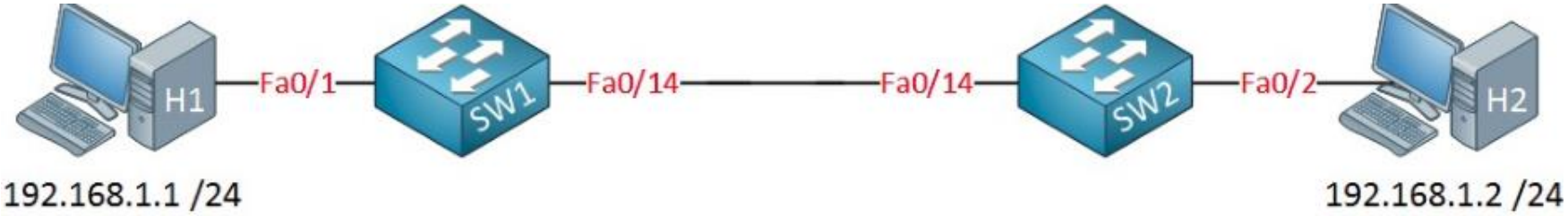
Задатак 1

- Табела VLAN-ова
  - >**enable**
  - #**show vlan**
- Креирање новог VLAN-а
  - >**enable**
  - #**configure terminal**
  - (config)#**vlan 50**
  - (config)#**name Testiranje**
  - (config)#**exit**
  - #**show vlan**

Задатак 1

- Након што је креиран VLAN, сада га треба додати на жељене интерфејсе.
  - >**enable**
  - #**configure terminal**
  - (config)#**interface fastEthernet 0/1**
  - (config-if)#**switchport mode access**
  - (config-if)#**switchport access vlan 50**
  - (config)#**exit**
  - #**show vlan**
- Поступак поновити и за интерфејс fastEthernet 0/2

Задатак 2



- С обзиром да ће се користити порт 14 за trunk комуникацију, потребно је исти порт конфигурисати на оба свича:
  - SW1>**enable**
  - SW1#**configure terminal**
  - SW1(config)#**interface fa0/14**
  - SW1(config-if)#**switchport mode trunk** (уколико се појави грешка о енкапсулацији, тада уписати **switchport trunk encapsulation dot1q** па поновити претходну команду)
- НАПОМЕНА: подразумевано Trunk ће пропуштати све VLAN-ове. Уколико желимо да на међусобном линку пропустимо само одређене VLAN-ове, тада настављамо конфигурацију као што је приказано:
  - SW1(config-if)#**switchport trunk allowed vlan 50**
- НАПОМЕНА: ове команде потребно је извести на оба свича.
- Проверити конективност између рачунара.

Задатак 2 - додатак

- Додати још два рачунара, формирати нови VLAN, придружити интерфејсе на којима су нови рачунари повезани у одговарајући влан. Тестирати конективност. Додати нови VLAN у TRUNK везу па поново тестирати конективност.
- Анализирати стање.
- Снимити конфигурацију.
- Снимити пројекат.

Port-security

- Помоћу технологије Port-security могуће је обезбедити да свич на датом порту може примати и слати пакете само уколико се MAC адреса пошиљаоца, тј примоца подударају. Овиме се обезбеђује заштита у виду блокирања или искључивања порта уколико злонамерни корисник покуша да се физички повеже са радном станицом која нема дату MAC адресу.
- Рачунар прикачен на одређен порт и даље може да лажира своју MAC адресу да би остварио приступ мрежи

Port-security

- Команде за креирање Port-Security-а
  - >**enable**
  - #**configure terminal**
  - (config)#**interface fastEthernet 0/1**
  - (config-if)#**switchport mode access**
  - (config-if)#**switchport port-security**
  - (config-if)#**switchport port-security mac-address <MAC, sticky>**
  - (config-if)#**switchport port-security maximum 1**
  - (config-if)#**switchport port-security violation shutdown**
- Команде за приказивање подешавања Port-Security-а
  - >**enable**
  - #**show port-security interface fastEthernet 0/1**
- **sticky** – уколико не желимо да ручно унисмо MAC адресу, већ да се она аутоматски очита са порта свича, тада користимо параметар sticky

Питања?