

УНИВЕРЗИТЕТ У ПРИШТИНИ
ПРИРОДНО-МАТЕМАТИЧКИ ФАКУЛТЕТ

Одсек за Информатику



Switchport port security

Пројектни задатак:

СИГУРНОСТ И ЗАШТИТА РАЧУНАРСКИХ СИСТЕМА

Ментор
Проф. Др. Стефан Панић

Кандидат:
Немања С. Лазаревић

Косовска Митровица, јун 2020. године

Садржај

Увод.....	3
Switch.....	4
Шта је Switch ?	4
Врсте Switch-а	5
Шта је и које су особине порт-а?.....	8
Примена заштите Switchport-а.....	9
Окружење	14
Назив окружења у којем се одвија решавање проблема?	14
Системски и хардверски захтеви за нормалан рад у окружењу	15
Рад у програму Cisco.....	17
Закључак.....	17
Референце.....	18

Увод

Пред дамном је постављен задатак на тему Switchport port security или у преводу свичпорт порт заштита. У даљем раду видећемо до чега се ова тема све дотиче. Неких од селекција које ћемо прећи су сам опис Switchport-а као и све његове утицаје на неки мрежни протокол, тј. на неки комуникациски проток информација између два или више рецептора што у овом случају представљају рачунари. Такође ћемо споменути како се Switchport-ови могу класификовати према основи мрежне архитектуре. Switch је уређај који управља протоком података између делова неке локалне мреже (LAN). Такође ћемо навести све врсте портова. За развојно окружење користи се пакетни програм Cisco чији језик је заснован на Cisco IOS® Software.

Switch

Шта је Switch ?

Switch представља мрежни хардвер који повезује уређаје на рачунарској мрежи коришћењем комутације пакета за примање и прослеђивање података до одредишног уређаја. Мрежни Switch тј. мрежни прекидач је мрежни мост са више портова који користи MAC (Media Access Control) адресе за прослеђивање података на слоју везе података OSI (Open Systems Interconnection) модела. Неки switch-еви такође могу да прослеђују податке на мрежном слоју тако што додатно укључују функцију рутирања. Такви switch-еви су обично познати као вишеслојни switch-еви [1].

Прекидач је уређај у рачунарској мрежи који повезује друге уређаје заједно. Више каблова за пренос података је прикључено на switch како би се омогућила комуникација између различитих умрежених уређаја. Прекидачи, тј. switch-еви управљају протоком података кроз мрежу тако што преносе примљени мрежни пакет само на један или више уређаја за које је пакет намењен. Сваки умрежени уређај повезан са комутатором може се идентификовати по својој мрежној адреси, омогућавајући комутатору да усмерава ток саобраћаја максимизирајући безбедност и ефикасност мреже [1].



Слика 1. Изглед Switch-а

Врсте Switch-а

За људе који се баве инсталиравањем мрежа, битно је који ће switch да изабере, тј. switch представља суштинску компоненту у њиховом плану изградње неке мреже. У имплементацији изградње мреже да би се постигао висок ниво перформанси мора да се обрати пажња на разне врсте switch-а у умрежавању. У даљем тексту ћу навести врсте switch-а које постоје и које су значајно имплементиране у одговарајућем умрежавању.

Постоји пет врста switch-ева и то :

- **LAN Switch (Local area network Switch)**
- **Unmanaged Switch**
- **Managed Switch**
- **PoE Switch**
- **Stackable Switch**

Прекидачи локалне мреже или **LAN** прекидачи се обично користе за повезивање тачака на интерном LAN-у компаније. Такође је познат као прекидач података или Ethernet switch или прекидач. Он блокира преклапање пакета података који пролазе кроз мрежу економичном алокацијом пропусног опсега. LAN прекидач испоручује пренети пакет података пре него што га усмери на планирани пријемник. Ови типови прекидача смањују загушење мреже или уска грла тако што дистрибуирају пакет података само примаоцу који је намењен [2].

Unmanaged Switch мрежни прекидачи се често користе у кућним мрежама, малим предузећима, па чак и у великим предузећима. Дозвољава уређајима на мрежи да се међусобно повежу, као што су рачунар на рачунар или штампач на рачунар на једној локацији. Unmanaged Switch не мора нужно бити конфигурисан или надгледан. Једноставан је и лак за постављање. Ако желите да додате више Ethernet портова, можете да користите ове типове прекидача за укључивање и употребу у умрежавању [2].

У поређењу са **unmanaged** switch-евима, предност **managed** switch-ева је у томе што се могу прилагодити да побољшају функционалност одређене мреже. Они нуде неке функције као што су QoS (Квалитет услуге), Simple Network Management Protocol (SNMP) и тако даље. Ови типови прекидача у умрежавању могу подржати низ напредних функција дизајнираних да их контролише професионални администратор. Поред тога, постоји паметни switch-ови, врсте managed switch-а тј. прекидача. Има неке функције које има managed (управљани) прекидач, али су ограниченије. Паметни мрежни прекидач се обично користи за мрежне уређаје као што су VLAN или Virtual Local Area Network [2].

PoE (Power over Ethernet) Gigabit Ethernet switch је мрежни прекидач који користи снагу преко Ethernet технологије. Када су повезани са више других мрежних уређаја, PoE switch-еви могу да подрже пренос напајања и података преко једног мрежног кабла у исто време. Ово у великој мери поједностављује процес каблирања. Ови типови прекидача у умрежавању пружају већу флексибилност и никада нећете морати да бринете о утичници када постављате мрежне уређаје [2].

Stackable switches или прекидачи који се могу слагати пружају начин да се поједностави и повећа доступност мреже. На пример, уместо да појединачно конфигуришете, управљате и решавате проблеме са осам прекидача са 48 портова, можете управљати са свих осам као једном јединицом помоћу склопивих прекидача. Са правим комутатором који се може слагати, тих осам прекидача (укупно 384 порта) функционишу као један прекидач. Постоје драгоцене оперативне предности коришћења ових типова прекидача у умрежавању. Неке од њих су то да можете креирати групе за агрегацију линкова које се протежу на више јединица у стеку, саобраћај пресликавања портова од једне јединице у стеку на другу или подешавање ACLs/QoS-а који обухватају све јединице [2].



Слика 2.

LAN Switch

(Local area network Switch)



Слика 3.

Unmanaged Switch



Слика 4. Managed Switch



Слика 5. PoE Switch



Слика 6. Stackable Switch

Шта је и које су особине порт-а?

На мрежном прекидачу односно switch-у, порт комутатора је физички отвор у који се може прикључити кабл за пренос података. Генерално, портови комутатора су правоугаони са три стране са тачком у облику слова В на врху или на дну. Повезивање различитих уређаја на портове мрежног прекидача омогућава им да међусобно комуницирају путем преноса података унутар прекидача. Већина мрежних уређаја се такође повезује на интернет, омогућавајући уређајима да добију приступ интернету преко портова комутатора [3].

Када је реч о томе колико портова треба да има један switch то ће зависити од саме функције уређаја тј. switch-а. Типичан кућни рутер може имати пет портова, док switch за велику мрежу може имати до 52 порта. Број уређаја који могу да се повежу на Ethernet прекидач, тј. switch је за један мањи од броја физичких портова, јер је један порт резервисан за кабл који повезује комутатор са рутером [3].

Мрежни прекидачи се често користе за креирање и управљање VLAN-овима. У овој врсти мреже постоје три основна типа портова комутатора: **приступни**, **магистрални** и **хибридни**. Сваки тип порта има јединствену функцију, а стандардни Ethernet интерфејс може да функционише као било који од ових портова [3].

Приступни порт повезује мрежни хост са једним VLAN-ом и управља саобраћајем података за ту виртуелну мрежу. Пошто подаци могу да иду само напред-назад на одређеном VLAN-у, приступни порт рукује неозначеним Ethernet оквирима [3].

Магистрални порт се обично повезује са другим прекидачем и може да комуницира са неколико VLAN-ова. На сложеној мрежи са више VLAN-ова, магистрални порт управља преносом података у те виртуелне мреже и са њих. Да би то урадио, **магистрални** порт препознаје ознаке оквира које одређују намеравано одредиште за податке [3].

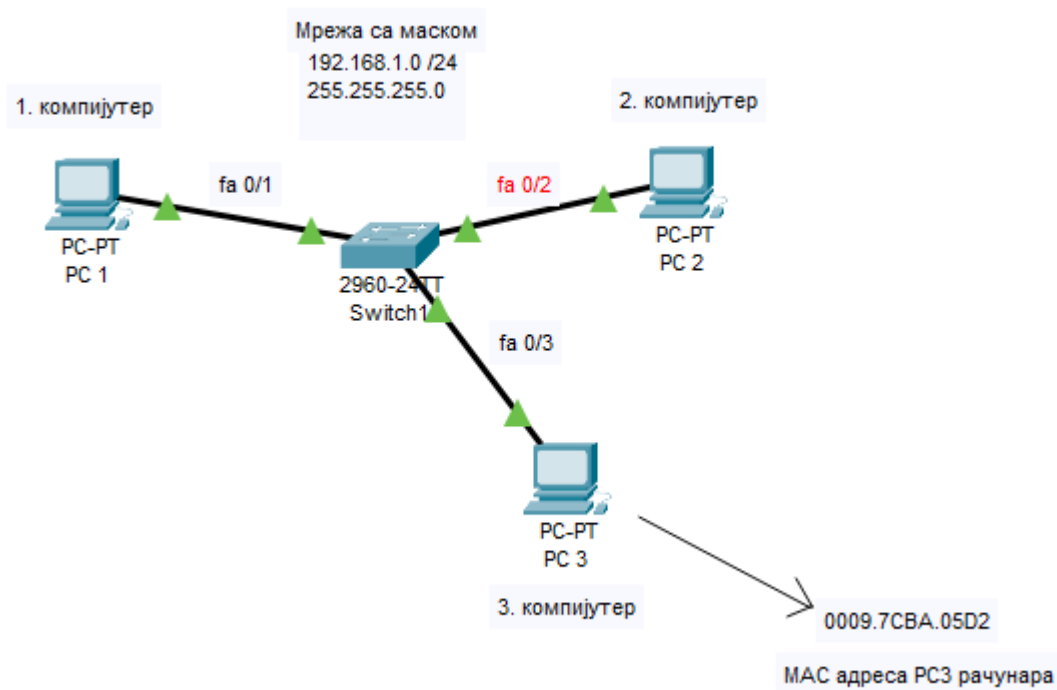
Хибридни порт може да функционише и као приступни и као магистрални порт. Може да управља и означеним и неозначеним оквирима и може да прима податке са више од једног VLAN-а. Преко хибридног порта могу се повезати и кориснички и мрежни уређаји [3].

Како рутер тако и switch има конзолни порт који контролише рад самог switch-а. Корисник може да повеже рачунар на порт конзоле прекидача, а затим да конфигурише прекидач користећи интерфејс рачунара.

Примена заштите Switchport-a

У суштини **switchport** заштита се најбоље може показати на примерима у програму Cisco. Зато ћемо кроз неколико примера показати како се заштићује Switchport порт.

Пример 1.



Слика 7. Проста конфигурација умрежених рачунара

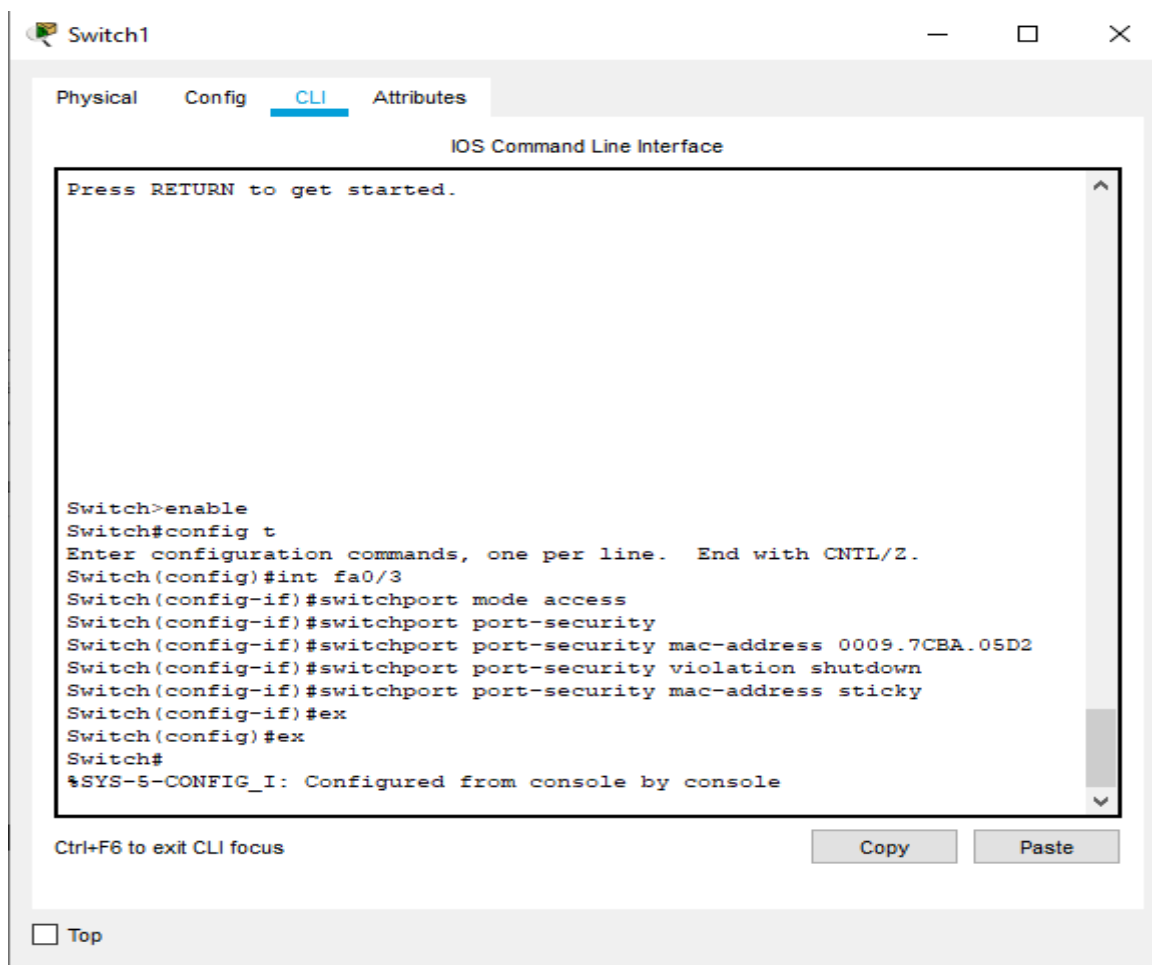
Прво што треба да урадимо јесте да уђемо у Switch кликом на исти. Затим на селекцију CLI или command-line interface тог Switch-а. Затим куцамо следеће команде у том CLI прозору:

- enable
- config t
- int fa0/3
- switchport mode access
- switchport port-security
- switchport port-security mac-address 0009.7CBA.05D2
- switchport port-security violation shutdown
- switchport port-security mac-address sticky

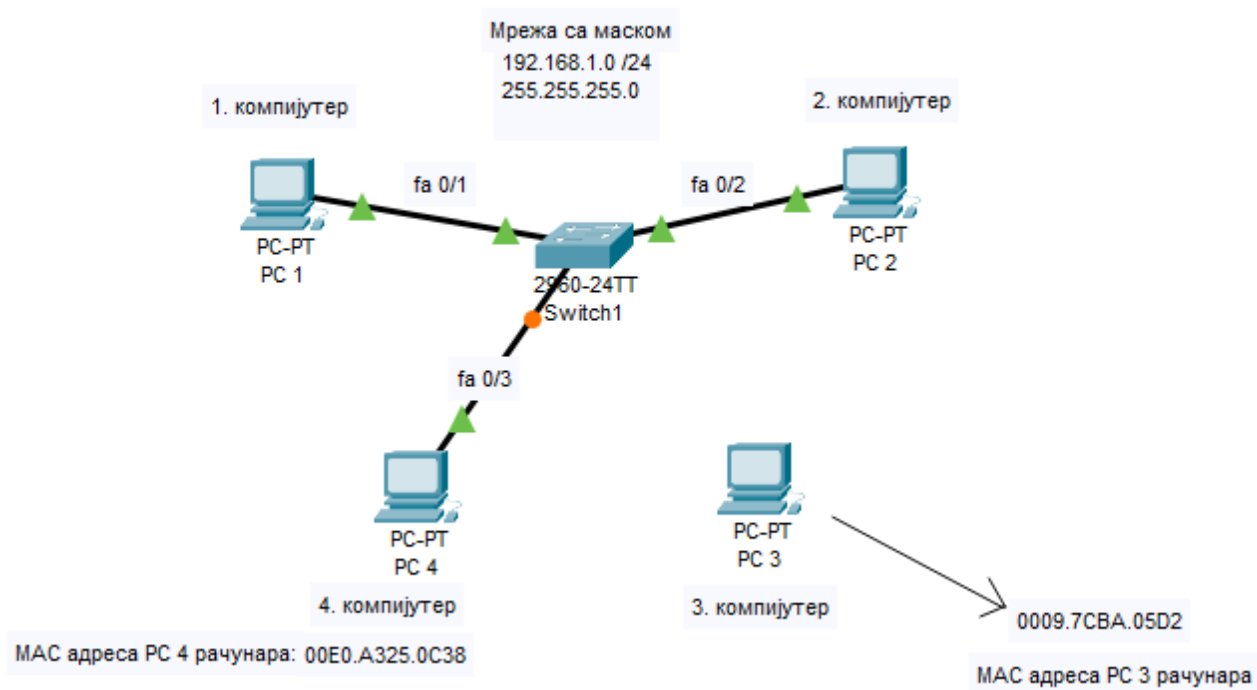
Уз помоћ команде `enable` укључујемо `switch`, затим с командом `conf t` приступамо конфигурационом терминалу. Код следеће команде `interface` или скраћено `int fa 0/3` мора се обратити пажња којем интерфејсу ћемо приступити и одрадити неке функције. Као што можемо видети ми смо приступили интерфејсу `fa 0/3` зато што ћемо на истом забранити комукацију на том порту ако је **MAC** адреса различита од **0009.7CBA.05D2**.

Пошто смо приступили интерфејсу - `int fa 0/3` затим помоћу команде `switchport mode access` хоћемо да приступимо моду приступа. Затим куцамо `switchport port-security` да дефинишемо заштиту на порту. Потом са командом `switchport port-security mac-address 0009.7CBA.05D2` говоримо да приступ том порт има ова **MAC** адреса.

После унетих команда треба да кажемо шта ако се на тај порт се прикључи рачунар са **MAC** адресом која је различита од **0009.7CBA.05D2**. Нормално помоћу команди `switchport port-security violation shutdown` и `switchport port-security mac-address sticky` говоримо да ће се порт искључити и тиме онемогућити комуникацију кроз тај интерфејс.



Слика 8. Куцање команди у CLI од Switch-a



Слика 9. Проста конфигурација умрежених рачунара 2

Као што можемо да видимо ако прикључимо PC 4 чија MAC адреса је 00E0.A325.0C38 на прикључак тј. порт 0/3 ће се искључити. Искључен порт се на слици може видети у облику наранџасте куглице на интерфејсу 0/3. Када би опет прикључили PC 3 и рестартовали switch порт 0/3 би опет прорадио и успешно обављао комуникацију са рачунаром као и слање и примање података са истог и ка истом.

Као што можемо да видимо на слици испод да су сва 4 пакета са подацима послата и примљена, што значи да је комуникација обављена.

```

C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
  
```

Слика 10. Комуникација успешна

На овој слици за разлику од предходне када смо на порт 0/3 прикључили PC 4 са другом MAC адресом и покушали да извршимо комуникацију од PC 4 рачунара ка било ком другом рачунару у овој мрежи, добили смо обавештење о Request timed out. То јест да комуникација на том порт са тог рачунара није могућа зато што се MAC адресе не поклапају.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

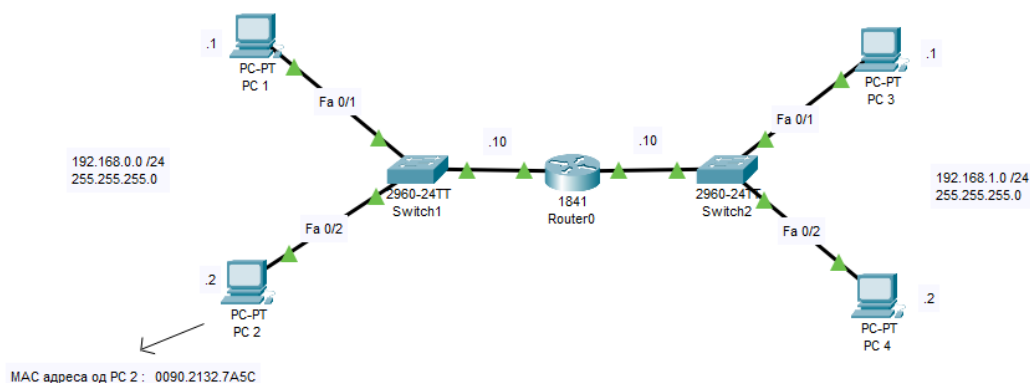
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Слика 11. Комуникација неуспешна

Пример 2.

У следећем примеру забранићемо да на порту fa 0/2 switch-а 1 не може нико осим рачунара са MAC адресом 0090.2132.7A5C да се прикључи. На следећој слици представљена је конфигурација другог примера.



Слика 12. Конфигурација другог примера у програму Cisco

Ако ping-емо PC 2 са PC 1 било којим другим рачунаром у мрежи проток информација ће се остварити што се да видети на следећој слици.

```

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

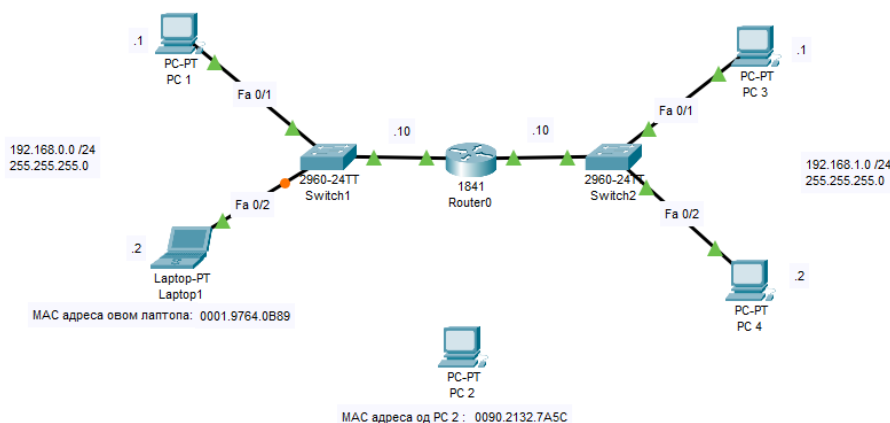
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

Слика 13. Комуникација успешна

Уколико на тај порт фа 0/2 прикључимо неки други рачунар комуникација се неће остварити као што већ и предпостављате.



Слика 14. Прикључивање лаптопа на interface fa 0/2

```

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

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

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

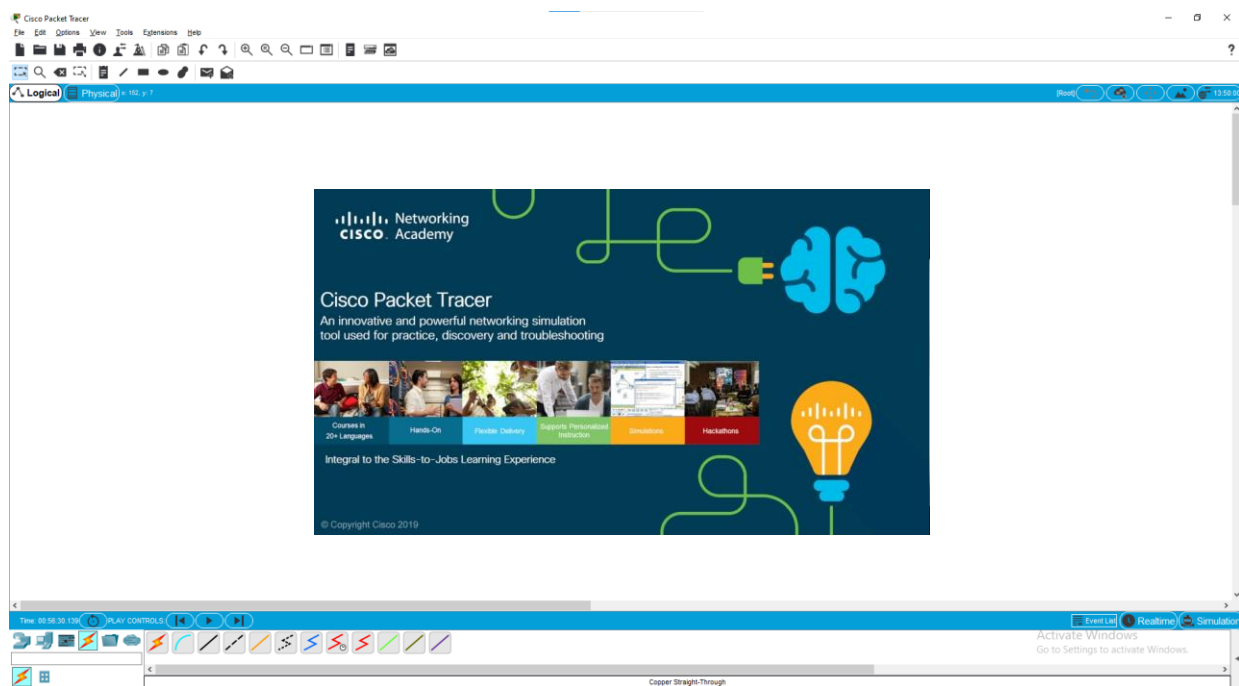
Слика 15. Неуспешна комуникација са лаптопом на порту fa 0/2

Као што можемо видети са 15. слике вршење комуникације лаптопа преко интерфејса fa 0/2 није могућа зато што MAC адреса лаптопа није 0090.2132.7A5C већ је 0001.9764.0B89.

Окружење

Назив окружења у којем се одвија решавање проблема?

Као што сам навео у уводу самог рада за решавање проблема око саме заштите switchport-a користићемо програм који се зове Cisco. Само окружење се може видети на слици испод :



Слика 11. Радно окружење у програму CISCO

Као што можемо видети окружење програма изгледа врло лепо и за руковање једноставно, у великој белој селекцији дефинишемо саме конфигурације које су нам потребне за прављење рачунарских мрежа. О самим функцијама у програму Cisco ће бити речи нешто касније у раду.

Системски и хардверски захтеви за нормалан рад у окружењу

За неометани рад у окружењу Cisco неопходно је имати минималну компијутерску конфигурацију како у хардверском тако и у софтверском смислу, која ће омогућити рад у програму Cisco.

Што се CPU-а тиче минималан одабир да би све функционисало уреду треба да буде један од ова три понуђена процесора :

- Mobile AMD Sempron Processor 3600+ at 2 GHz
- Intel ® Core 2 CPU T7400 at 2.16 GHz
- Intel Atom

Неопходно је да рачунар има 4 GB RAM-а као и простора на HARD или SSD диску за програм Cisco који у инсталационом пакету има око 147 MB. Пожељно је да најстарија верзија оперативног система буде Windows 8, а док се највише препоручује да буде Windows 10. Наравно могу бити и остали оперативни систему само да су новији од верзије Windows 8 укључујући и исти.

За преузимање и инсталацију програма Cisco можемо користити Google претраживач. Затим на официјалној страни Cisca можемо преузети инсталациони фајл програма. Инсталација самог програма је једноставна и онолико дуга у зависности од вашег процесора. После успешно обављене инсталације потребно је направити налог преко којег ћете се пријавити и тиме себи обезбедити доступност сви алата који програм има. Уколико вам је компликовано да направите налог, само пре уласка у програм Cisco обезбедите да ваш рачунар нема приступа интернету. Затим када успешно уђете у програм можете се поново повезати на интернет.

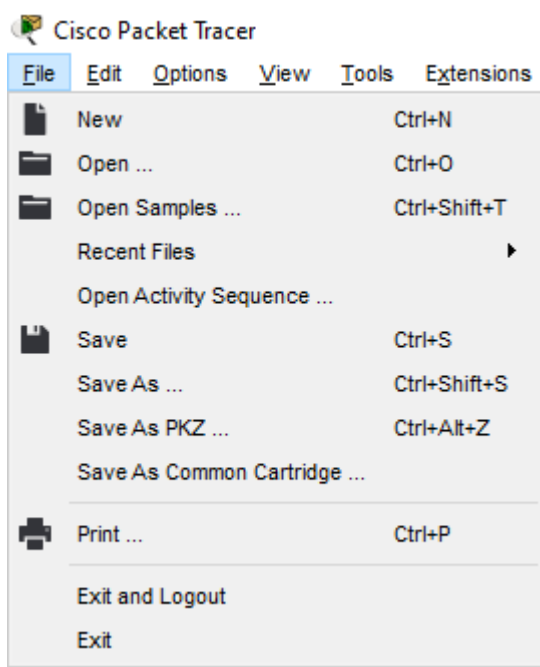
У даљем раду ће бити више речи о основним функцијама у програму Cisco, као што су креирање новог пројекта као и чување истог. Такође ћу вам олакшати рад са пречицама које и сам користим.

Основне функције у програму

New project – Што се тиче прављење новог пројекта у програму Cisco, то је врло просто. У прво падајућој листи под називом FILE требамо кликнути New или преко пречице на следећи начин CTRL + N.

Save project – Опција за чување пројекта се налази у истој падајућој листи само под називом Save или Save as или CTRL + S.

Open project – Све је исто само опција OPEN или CTRL + O.



Слика 12. Основне функције у програму Cisco

Comments – писање коментара можемо лакше одрадiti преко пречице N и кликом на белу позадину.

Delete – брисање компоненти се врши преко пречице Del и самим кликом на компоненту.

Esc – је пречица за нормалну стрелицу.

Рад у програму Cisco

Рад у програму Cisco је једноставан. У доњем углу имамо траку са понуђеним алатима тј. компонентама са којим можемо да изградимо саму архитектуру наше мреже.



Слика 13. Трака са компонентама за изградњу мреже

Као што можемо видети са предходне слике са леве стране видимо да можемо да одаберемо компоненте док са десне стране можемо да изаберемо тип компонената за изградњу наше мреже. Све остале опције и радње које се врше унутар компонената можемо приступити кликом на одређену компоненту коју желимо да дефинишемо или да едитујемо.

Закључак

У раду на теми **Switchport port security** објаснио сам како да своју или било чију рачунарску мрежу барем уз помоћ **Switchport-a** да заштитимо. На тај начин смо се обезбедили да треће лице тј. рачунар у мрежи не може да приступи одређеном порту на Switch-у и на тај начин изазове неки колапс или стање престанка рада тог комуникациског тока или те рачунарске мреже. Поред заштите научили смо типове **Switch-a** као и типове портове и за које намене служе.

Референце

- [1] *Network switch. (Admin). Retrieved Jun 2022, 10, from Wikipedia:*
https://en.wikipedia.org/wiki/Network_switch
- [2] *Different Types Of Switches In Networking. (2017, December 21). Retrieved Jun 2022, 10, from Fiber Optical Networking:*
<https://www.fiber-optical-networking.com/different-types-of-switches-in-networking.html>
- [3] *Holland, A. (2022, May 18). What Is a Switch Port? Retrieved Jun 10, 2022, from EasyTechJunkie:*
<https://www.easytechjunkie.com/what-is-a-switch-port.htm>
- [4] *System Requirements - Cisco Learning Network Space - User Information - Document - Cisco DevNet. (n.d.). Retrieved Jun 10, 2022, from Cisco DevNet:*
<https://developer.cisco.com/docs/learningspace/user/#!/system-requirements>
- Слика 1. *TP Link 5 Port Gigabit Ethernet Network Switch TL SG105 Ethernet Splitter Plug. Retrieved Jun 10, 2022, from Amazon.ae:*
<https://www.amazon.ae/Ethernet-Splitter-Optimization-Unmanaged-Protection/dp/B00A128S24>
- Слика 2. *TP-LINK Unmanaged LAN Switch 10/100/1000M (TL-SG108). (n.d.). Retrieved Jun 10, 2022, from wifi-stock.com:*
<https://www.wifi-stock.com/details/tp-link-unmanaged-lan-switch-101001000m-tl-sg108-v3.html>
- Слика 3. *Unmanaged switch, 24x 10/100 RJ-45, 19" (TP-Link TL-SF1024) . (n.d.). Retrieved Jun 10, 2022, from Atel-electronics.eu:*
<https://www.atel-electronics.eu/produkt.php?hash=05882>
- Слика 4. *Atel-electronics.eu. (n.d.). Edge-corE ES4548D, Managed switch L2, 44x 10/1000 RJ-45, 4 slide-in SFP / RJ-45 slots, IP stacking, IPv6 Retrieved Jun 10, 2022, from Atel-electronics.eu:*
<https://www.atel-electronics.eu/produkt.php?hash=05951>
- Слика 5. *Amazon.com: TP-Link TL-SG1005P V2 or later / 5 Port Gigabit PoE Switch / 4 PoE+ Ports @65W / Desktop / Plug & Play / Sturdy Metal w/ Shielded Ports / Fanless / Limited Lifetime Protection / QoS & IGMP Snooping : Electronics. Retrieved Jun 10, 2022, from Amazon:*
<https://www.amazon.com/TP-Link-Compliant-Shielded-Optimization-TL-SG1005P/dp/B076HZFY3F>

- Слика 6. *Cisco - SG550X-48P-K9-EU - SG550X-48P 48-port Gigabit PoE Stackable Switch - Switch - 1.000 Mbps new and refurbished buy online low prices. (n.d.). Retrieved Jun 10, 2022, from Tonitrus:*
<https://www.tonitrus.com/se/naetverk/cisco/switch/cisco-sg550x-switch/10128734-003-cisco-sg550x-48p-k9-eu-sg550x-48p-48-port-gigabit-poe-stackable-switch-switch-1.000-mbps/>