

ВЕЖБА 1

Telnet и SSH као протоколи за удаљен приступ командној линији активних мрежних уређаја

Опис вежбе:

У овој вежби биће извршена анализа различитих метода приступа активној мрежној опреми, пре свега комутаторима и рутерима, са циљем конфигурације и администрације исте. Циљ вежбе је да студенти у лабораторији реализују сценаријо у оквиру кога ће успоставити комуникацију са наведеним уређајима преко конзолне конекције, а затим извршити основну конфигурацију уређаја користећи командну линију (CLI) и то тако да омогуће Telnet и SSH приступ уређају. На крају вежбе, студенти ће моћи да тестирају исправност конфигурације покушајем приступа командној линији рутера управо користећи Telnet и SSH протокол.

Активна мрежна опрема

Свака рачунарска мрежа, без обзира на модел мреже и технологију преноса, се састоји из пасивних и активних мрежних компоненти. Пасивне компоненте (каблови, каналице, ормари, прикључнице...) чине саму инфраструктуру, док активна мрежна опрема (комутатори или енгл. *Switch*, рутери, бежичне приступне тачке, заштитне баријере или енгл. *Firewalls*, итд.) ту инфраструктуру ставља у функцију. Аспекти комуникације како унутар једне, тако и између различитих рачунарских мрежа дефинишу се на активној мрежној опреми конфигурацијом исте.

У зависности од произвођача, мрежни уређаји долазе са или без подразумеване конфигурације. У случају да уређај има подразумевану конфигурацију, зарад додатне конфигурације, уређају се може приступити преко фабрички подешеног мрежног интерфејса користећи неки од наведених метода приступа које је произвођач дефинисао:

- приступ преко Web интерфејса;
- приступ користећи Telnet протокол;
- приступ користећи SSH протокол.

У случају да мрежни уређај нема подразумевану конфигурацију, односно да нема унапред конфигурисан мрежни порт, иницијални приступ и конфигурација се може извести коришћењем интерфејса који је специјално одређен за ту намену. На пример, код Cisco произвођача мрежне опреме тај специјални интерфејс се назива конзолна линија (енгл. *Console*). Повезивањем путем таквог интерфејса могуће је извршити иницијалну конфигурацију која би омогућила и приступ уређају кроз рачунарску мрежу користећи Telnet или SSH протокол.

У даљем тексту биће објашњен начин како се приступа Cisco рутеру који нема никакву конфигурацију помоћу конзолне линије (порта), а затим како се подешава мрежни интерфејс уз конфигурацију Telnet и SSH протокола како би омогућили да рутер прихвата такве захтеве за конекцијом. Сличан принцип важи и за Cisco комутаторе. На слици 1 је приказан изглед конзолног порта на једном Cisco рутеру.



Слика 1 - Конзолни порт на рутеру

Приступ рутеру преко конзолне линије

Повезивање на конзолни порт се врши помоћу конзолног – rollover кабла, који на једном крају има RJ-45 конектор којим се повезује на рутер, а на другој страни има DB9 конектор којим се повезује на серијски порт рачунара (слика 2). У случају да рачунар не поседује серијски порт (као што је случај са новијим преносивим рачунарима), може се искористити конвертер са USB порта на DB9 конектор (слика 3).

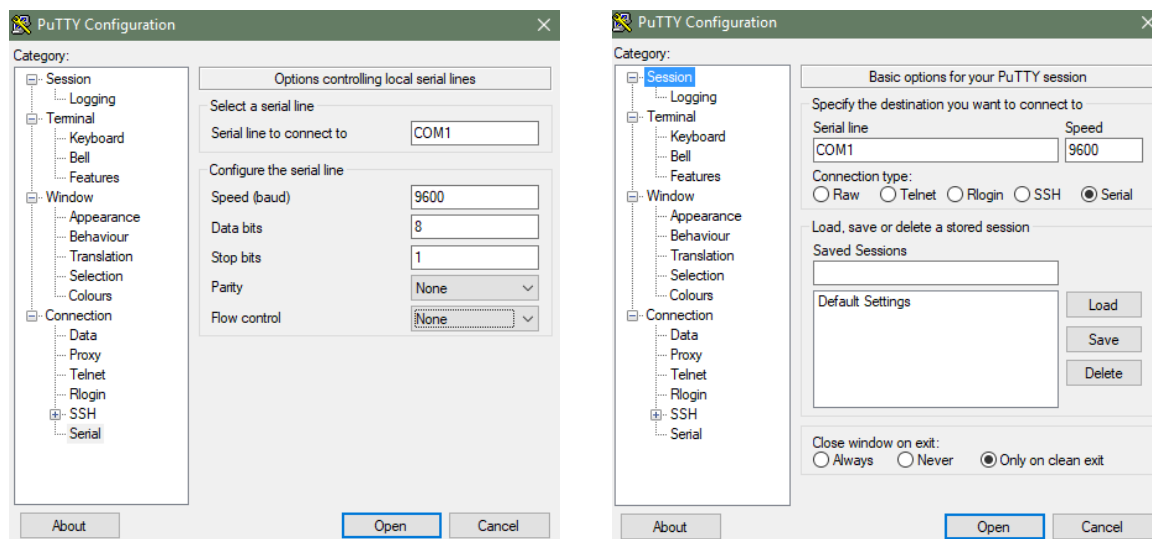


Слика 2 – Конзолни кабл RJ45-DB9



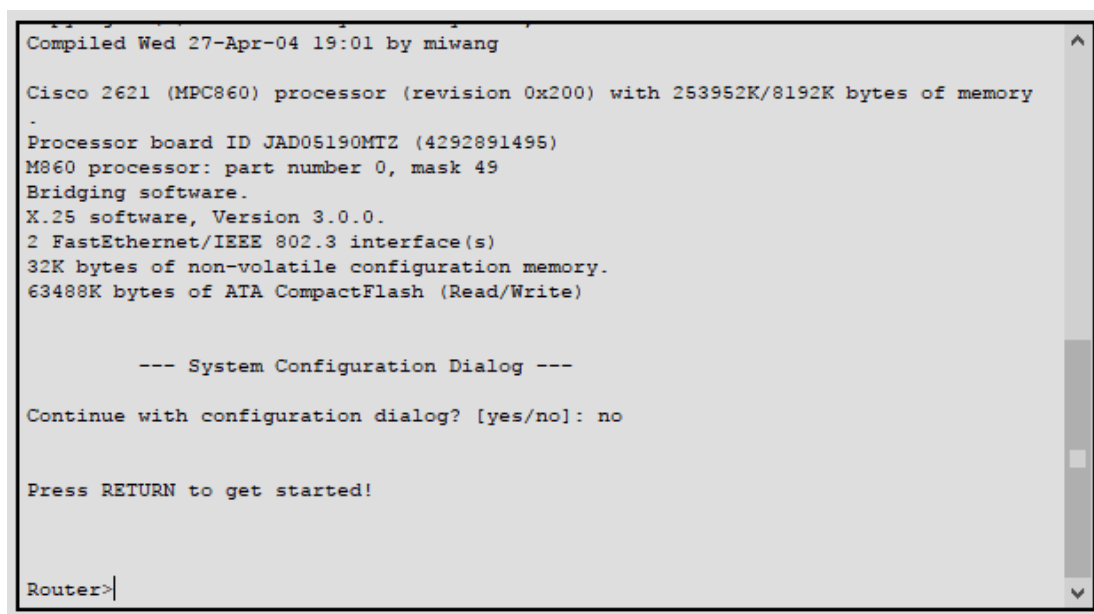
Слика 3 – Конвертер са USB на серијски порт

Како би са рачунара успоставили конекцију преко серијског интерфејса са конзолним портом на рутеру, неопходно је користити неки од програма који припадају категорији терминал емулатор програма. Најпознатији програми који имају могућност емулације терминала су: HyperTerminal, Putty, Kitty... На слици 4 је приказано подешавање Putty програма за потребе успостављања конекције са конзолним портом. Претпоставка је да је конзолни порт рутера повезан RJ45-DB9 каблом на серијски порт COM1 на рачунару.



Слика 4 – Параметри за серијску конекцију на конзолни порт у програму Putty

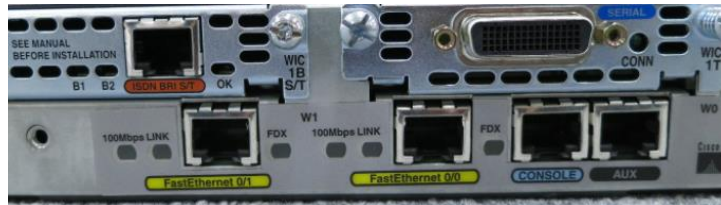
По успостављању конекције, у случају да рутер није конфигурисан, оперативни систем рутера (IOS) приказаће одзив као на слицизв слици 5. При том ће кориснику бити постављено питање да ли жели да настави са конфигурационим дијалогом, при чему треба одговорити са **No** и потврдити са тастером Ентер. Одзивни знак рутера се мења у **Router>** што говори да је рутер спреман да прихвати наредну команду.



Слика 5 – Одзив Cisco рутера који нема конфигурацију

Конфигурација етернет мрежног интерфејса на рутеру

Основна конфигурација етернет мрежног интерфејса (слика 6) на рутеру подразумева дефинисање IP адресе за тај интерфејс као и активирање интерфејса (није обавезно с обзиром да је етернет интерфејс подразумевано активан).



Слика 6 – Приказ етернет интерфејса на Cisco рутеру

Како би конфигурисали интерфејс неопходно је прво ући у конфигурациони мод за одређени интерфејс, а затим извршити команду којом додељујемо IP адресу изабраном интерфејсу. На крају извршена је команда **no shutdown** којом стартујемо сам интерфејс и пребацујемо га у активно стање. Пример конфигурације етернет мрежног интерфејса са ознаком **FastEthernet0/0** је приказан на слици 7. По извршеној конфигурацији извршена је команда **show interface fastethernet0/0** која показује статус поменутог интерфејса.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show interface fastethernet0/0
FastEthernet0/0 is up, line protocol is down (disabled)
Hardware is Lance, address is 0003.e4d6.ca0c (bia 0003.e4d6.ca0c)
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
```

Слика 7 – Пример основне конфигурације етернет мрежног интерфејса

Конфигурација Telnet протокола на рутеру

Telnet протокол је протокол који припада апликативном слоју OSI референтног модела, а који служи за успостављање двосмерног комуникационог канала између два мрежна уређаја (рачунара, комутатора, рутера...) Основна верзија овог протокола је дефинисана у RFC 206 документу. Данас, Telnet користи TCP као протокол транспортног слоја. Најчешћа примена овог протокола је да омогући кориснику успостављање виртуелне сесије између уређаја на којем корисник тренутно ради и удаљеног уређаја са циљем приступа командној линији удаљеног уређаја и извршења команди.

Употреба овог протокола за удаљени приступ командној линији неког уређаја се данас никако не препоручује, првенствено због тога што комуникациони канал Telnet протокола није заштићен, при чему се корисничко име и лозинка, као и све команде које корисник задаје, шаљу у читљивом облику. Ово се према данашњим мерилима сматра врло небезбедним, јер треће лице може, на врло лак начин, прибавити креденцијале за приступ и све команде које су извршене на удаљеном уређају, једноставним ослушкивањем саобраћаја.

Предуслови за приступ рутеру путем Telnet протокола су:

- конфигурисан мрежни интерфејс са припадајућом IP адресом;
- да је тај мрежни интерфејс прикључен на рачуарску мрежу;
- конфигурисане виртуелне линије за прихват Telnet конекција (са дефинисаном лозинком за приступ;
- конфигурисану лозинку за прелазак у привилеговани мод на рутеру (*Enable* мод).

Пример комплетне конфигурације је дат на слици 8, док је на слици 8 приказан пример Telnet приступа конфигурисаном рутеру са рачунара који се налази на истој мрежи (IP адреса рутера је 192.168.1.1 док је IP адреса рачунара 192.168.1.2).

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 5
Router(config-line)#password kst-lozinka
Router(config-line)#login
Router(config-line)#exit
Router(config)#enable secret kst-lozinka-enable
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Слика 8 – Конфигурација виртуелних линија на рутеру за прихват Telnet конекција

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
Password:
Router>ena
Password:
Router#
```

Слика 9 – Telnet приступ рутеру са рачунара

Конфигурација SSH протокола на рутеру

SSH (енг. *Secure Shell*) представља апликативни протокол који, за разлику од Telnet протокола, служи за успоставу сигурног комуникационог канала између два мрежна уређаја кроз небезбедну рачунарску мрежу. Главна примена овог протокола се огледа у могућности приступа командној линији удаљеног уређаја, при чему је целокупна комуникација између SSH клијента и SSH сервера заштићена применом криптографије са јавним кључем.

Како би омогућили да рутер прихвата SSH конекције, неопходно је конфигурирати рутер тако да почне да ради у режиму SSH сервера (слика 10). Под претпоставком да рутер има конфигуриран мрежни интерфејс, следеће ставке је потребно додатно конфигурирати:

- конфигурирану лозинку за прелазак у привилеговани мод на рутеру (*Enable* мод).
- креиран кориснички налог са припадајућом лозинком на рутеру;
- конфигурирано име рутера;
- конфигурирано име домена коме рутер припада;
- генерисан RSA кључ који ће бити коришћен за енкрипцију комуникације;
- конфигуриране VTY линије да прихватају SSH конекције које ће бити аутентификоване користећи локалну базу корисника на рутеру.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable secret kst-lozinka-ena
Router(config)#username korisnik password kst-lozinka-kor
Router(config)#hostname RuterKST
RuterKST(config)#ip domain name kst.lab
RuterKST(config)#crypto key generate rsa
The name for the keys will be: RuterKST.kst.lab
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

RuterKST(config)#line vty 0 4
*Mar 1 1:22:36.958: %SSH-5-ENABLED: SSH 1.99 has been enabled
RuterKST(config-line)#login local
RuterKST(config-line)#transport in
RuterKST(config-line)#transport input ssh
RuterKST(config-line)#end
RuterKST#
%SYS-5-CONFIG_I: Configured from console by console
RuterKST#
```

Слика 10 – Изглед основне конфигурације SSH протокола на рутеру

```
PC>ssh -l korisnik 192.168.1.1
Open
Password:

RuterKST>enable
Password:
RuterKST#
```

Слика 11 – Пример приступа рутеру са рачунара користећи SSH протокол