- Projektni zadatak -

Aplikacija za nadgledanje mrežnih uređaja i protokola

Potrebno je izraditi softver koji nadgleda rad dela mreže ili neke njene funkcionalnosti korišćenjem SNMP protokola. Mreža koja se nadgleda je realizovana u okviru GNS3 simulatora, a celokupno okruženje je dato na virtuelnoj mašini za VMware player (operativni sistem virtuelne mašine je Ubuntu 19.04) koju studenti mogu da preuzmu sa https://drive.google.com/open?id=14J6_X-hv9xt2s1H_2p5NeccBQPZDMgDt. Virtuelna mašina je konfigurisana tako da ima 2GB RAM memorije, a za njen brži i komforniji rad se preporučuje povećanje na 4GB ukoliko to resursi računara na kojima se pokreće dozvoljavaju. Na virtuelnoj mašini se pored GNS3 softvera nalazi:

- **java** (proveriti da li je sve što treba tu)
- **Eclipse IDE**
- **Sublime** tekstualni editor
- **ireasoning MIB browser** koji može da pomogne u traženju SNMP promenljivih i objašnjenja njihovog funkcionisanja. MIB browser se startuje iz terminala sa: `/home/korisnik/Downloads/ireasoning/mibbrowser/browser.sh`

Ubuntu virtuelna mašina ima vezu sa internetom preko računara na kojem se nalazi, tako da je moguća instalacija dodatnog softvera ukoliko je potrebno.

Za nadgledanje uređaja može da se koristi SNMP Java API:
https://ireasoning.com/snmpapi.shtml
Dodatne informacije u vezi sa ovim APIjem su date ovde:
User guide: http://www.ireasoning.com/docs/SnmpUserGuide.pdf
FAQ: https://ireasoning.com/snmpfaq.shtml
Javadocs: http://www.ireasoning.com/javadocs/index.html

Uputstvo za rad u okruženju

Virtuelna mašina

Prilikom startovanja virtuelne mašine potrebno je startovati VMware player, otići na opciju „Open a Virtual Machine" i pronaći .vmx fajl. VMware player će prepoznati da VM nije kreirana na vašem računaru, te je potrebno kliknuti na opciju da je ova virtuelna mašina kopirana sa drugog računara. Nakon toga bi trebalo da se operativni sistem virtuelne mašina normalno učita, što će rezultirati login stranicom na kojoj treba kliknuti na Korisnik RTI i uneti lozinku. Korisničko ime korisnika „Korisnik RTI" je: korisnik, a lozinka je: lo**y**inka.

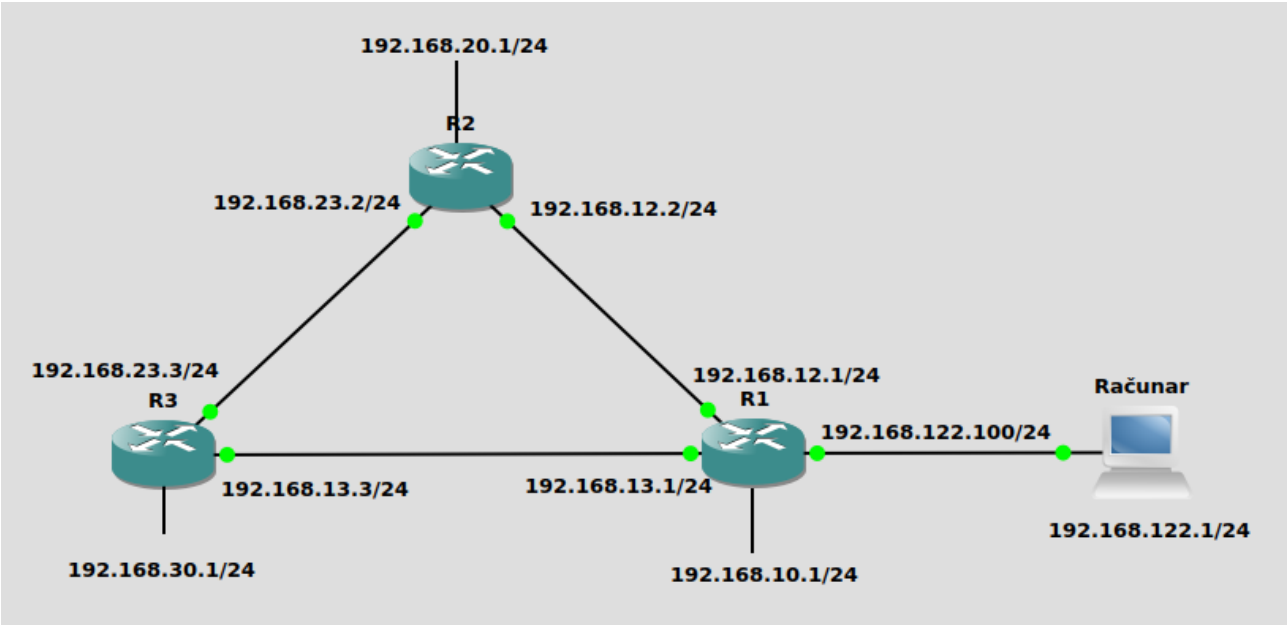
korisnik ima pravo da pokrene komande u sudo režimu, kada je potrebno ponovo ukucati lozinku korisnika. Home direktorijum korisnika je `/home/korisnik`.

GNS3 topologija

GNS3 program se startuje klikom na ikonicu: 

U prvom prozoru treba kliknuti na opciju „Open projects/Recent project" i odabrati projekat „SNMP setup". Po startovanju topologije prikazaće se mreža koja je konfigurisana. Da bi se startovala simulacija mreže treba kliknuti na > i sačekati malo da sve veze postanu zelene, što je znak da su svi ruteri startovani i da je mreža počela da radi.

Mreža koja će se nadgledati, sa adresama svih uređaja i mreža je data na slici. Računar na ovoj slici je virtuelna mašina na kojoj je pokrenuta GNS3 simulacija.



Provera veze topologije sa virtuelnom mašinom

Da bi računar sa slike (virtuelna mašina) na kome se izvršava GNS3 simulacija mogao da komunicira sa svim ruterima u simulaciji potrebno je u terminalu virtuelne mašine dodati sledeće rute (pošto se komande izvršavaju sa root privilegijama prilikom unosa prve komande biće potrebno da se upiše lozinka korisnika):

```
sudo ip route add 192.168.10.0/24 via 192.168.122.100 dev virbr0
sudo ip route add 192.168.20.0/24 via 192.168.122.100 dev virbr0
sudo ip route add 192.168.30.0/24 via 192.168.122.100 dev virbr0
sudo ip route add 192.168.12.0/24 via 192.168.122.100 dev virbr0
sudo ip route add 192.168.13.0/24 via 192.168.122.100 dev virbr0
sudo ip route add 192.168.23.0/24 via 192.168.122.100 dev virbr0
```

Nakon ovoga tabela rutiranja virtuelne mašine treba da izgleda ovako (dobija se upotrebom komande route, a crveno su označene nove rute koje služe za pristup ruterima):

```
korisnik@ubuntu:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 ens33
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 ens33
192.168.10.0    192.168.122.100 255.255.255.0   UG    0      0        0 virbr0
192.168.12.0    192.168.122.100 255.255.255.0   UG    0      0        0 virbr0
192.168.13.0    192.168.122.100 255.255.255.0   UG    0      0        0 virbr0
192.168.20.0    192.168.122.100 255.255.255.0   UG    0      0        0 virbr0
192.168.23.0    192.168.122.100 255.255.255.0   UG    0      0        0 virbr0
192.168.30.0    192.168.122.100 255.255.255.0   UG    0      0        0 virbr0
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0
192.168.245.0   0.0.0.0         255.255.255.0   U     100    0        0 ens33
```

SNMP konfiguracija

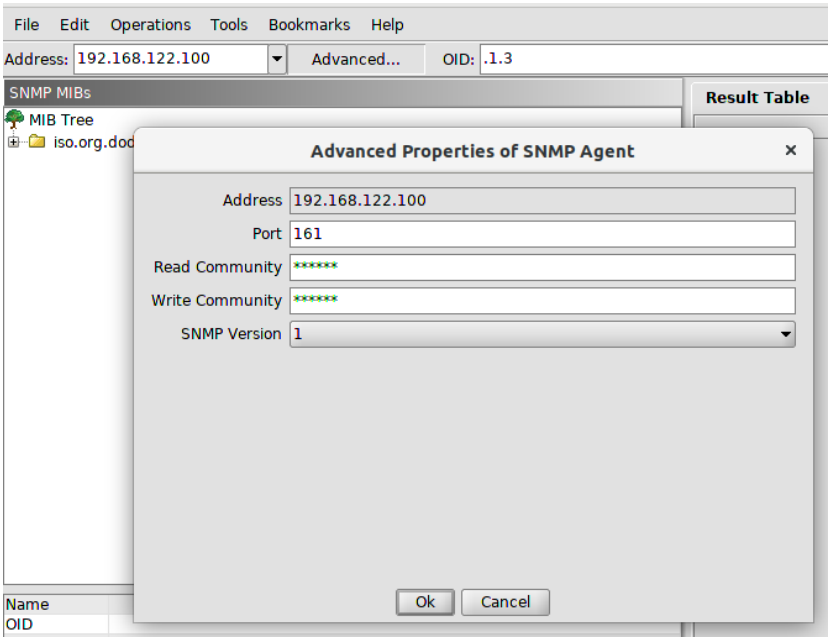
Na svim ruterima u virtuelnoj mreži je konfigurisan SNMP protokol koji radi u verzijama 1 i 2c sa podešenim *community* vrednostima `si2019` za čitanje i upisivanje podataka. Adrese rutera koje mogu da se koriste za pristup putem SNMP protokola su:

- ☐ R1: 192.168.10.1
- ☐ R2: 192.168.20.1
- ☐ R3: 192.168.30.1

ireasoning MIB browser

Da bi se isprobalo funkcionisanje SNMP protokola na ruterima, a i da bi se videlo čemu služe pojedine SNMP promenljive može da se koristi MIB browser koji je instaliran na virtuelnoj mašini. MIB browser se startuje iz terminala komandom:

```
/home/korisnik/Downloads/ireasoning/mibbrowser/browser.sh
```



Po startovanju u polje Address treba da se unese IP adresa rutera koji se nadgleda, a klikom na dugme Advanced se otvara prozor u koji treba uneti community vrednosti za Read i Write (si2019). Izborom promenljive u MIB stablu i klikom na komande Get ili GetBulk i Go dobijaju se vrednosti promenljivih kako su zabeležene na ruteru.

Ukoliko je potrebno učitati MIB za neku posebnu funkcionalnost, to se radi preko menija File/Load MIB.

Opis problema

Varijanta 1:

Aplikacija treba da očitava i prati statuse svih interfejsa na svim ruterima u mreži i da prikazuje za svaki interfejs sledeće podatke: opis, tip, MTU, brzinu interfejsa, fizičku adresu, administrativni i operativni status. Administrativni i operativni status treba da se prikazuje u formi dvobojnog (crveno/zeleno) indikatora za stanja down (crveno - 🔴) i up (zeleno - 🟢). Podaci se prikupljaju periodično sa periodom od 10s, tako da se poslednji očitani status prikazuje na ekranu. Podatke treba grupisati po ruteru, na sledeći način:

- ☐ Ruter 1
  - ◦ interfejs 1
    - ▪ opis
    - ▪ tip
    - ▪ ...
  - ◦ interfejs 2
    - ▪ opis
    - ▪ tip
    - ▪ ...
  - ◦ ...
- ☐ Ruter 2
  - ◦ interfejs...

Verifikacija rešenja:

Verifikacija rešenja će se vršiti promenama statusa interfejsa (shut/no shut), što treba da se vidi u aplikaciji kao promena odgovarajućeg statusa.

Varijanta 2:

Potrebno je očitavati i pratiti **broj paketa i protok (broj bita u jedinici vremena)** koji ulaze i izlaze kroz sve interfejse svih rutera. Podatke prikupljati periodično sa periodom od 10s. Prikupljene podatke prezentovati u obliku grafika koji prikazuje promenu očitanog parametra u vremenu. Sa svakom očitanom novom vrednošću grafik se dopunjava. Kako su na ruterima promenljive koje opisuju broj bajtova koji su prošli kroz ruter kumulativne, za protok je potrebno prikazati razliku vrednosti između dva intervala kao:
protok (bit/s)=8*(broj_bajtova(t)-broj_bajtova(t-10s))/10s

Verifikacija rešenja:

Pustiće se saobraćaj između rutera (npr. veliki broj ping paketa). U zavisnosti od toga kuda paketi prolaze, treba da se ovaj protok vidi na grafiku.

Varijanta 3:

Potrebno je prikazati sadržaj tabela rutiranja za sve rutere u mreži. Tabela rutiranja treba da sadrži adrese ruta, njihove maske, next hop adrese na koje te rute ukazuju, poreklo rute (iz kog protokola rutiranja potiču). Podatke prikupljati periodično sa periodom od 10s i osvežavati prikaz u skladu sa eventualnim promenama. Podatke grupisati tabelarno.

Verifikacija rešenja:

U mreži će se dodavati ili povlačiti neke rute dodavanjem novih loopback interfejsa na ruterima, a to treba da se vidi u aplikaciji, tako što će ona u svakom trenutku prikazivati ažurnu verziju tabele rutiranja ekvivalentnu onoj koja je u tabeli rutiranja.

Varijanta 4:

Potrebno je očitati i prikazati skup BGP suseda jednog od rutera u mreži i njihove osobine kao što su:

- Identifikator suseda
- stanje BGP sesije sa susedom (ime stanja u mašini stanja)
- verzija BGP koja se koristi
- IP adresa suseda
- Autonomni sistem u kojem je sused
- Broj primljenih update poruka
- Broj poslatih update poruka po susedu
- Keepalive vreme
- Elapsed time od kako je dobijen poslednji update od svih suseda

Poruke treba da se ažuriraju sa periodom od 10s i u svakom trenutku aplikacija treba da prikaže ažurne vrednosti ovih informacija.

Verifikacija rešenja:

U mreži će se dodavati nove mreže koje se oglašavaju putem BGP-a što treba da bude vidljivo u promenjenom broju update poruka i vremenu od poslednje poruke, takođe, mogu da se promene stanja BGP sesija kroz ukidanje BGP-a na susednom ruteru što takođe treba da se vidi prikazano u aplikaciji.

Varijanta 5:

Potrebno je očitati sadržaj BGP tabele i prikazati skup svih BGP ruta na jednom od rutera, kao i sve njihove atribute. Atributi koji treba da se prikažu za svaku rutu su:

- Origin
- AS-Path
- Next Hop
- MED
- Local Preference
- Atomic aggregate
- Aggregator AS
- Aggregator Address
- Da li je ruta najbolja (najbolju rutu prikazati drugom bojom)

Rute i njihove atribute prikazati u tabelarnom obliku. Informacije o rutama treba da se očitavaju sa periodom od 10s, tako da aplikacija u svakom trenutku prikazuje poslednju očitanu vrednost.

Verifikacija rešenja:

U topologiji će se dodavati nove mreže ili povlačiti postojeće koje se oglašavaju putem BGP-a što treba da bude vidljivo tako što će se pojaviti nove rute ili će se gubiti stare. Takođe, menjaće se topologija mreže ili neki atributi ruta kako bi se promenili atributi ruta i neke druge mreže proglasile za najbolje, a sve ovo treba da bude korektno prikazano u aplikaciji.

Varijanta 6:

Na ruterima R1, R2 i R3 podesiti SNMP trap-ove i to za ove promenljive iz BGP MIB-a:

- .iso.org.dod.internet.mgmt.mib-2.bgp.bgpNotification.bgpEstablishedNotification
- .iso.org.dod.internet.mgmt.mib-2.bgp.bgpNotification.bgpBackwardTransNotification

Napraviti aplikaciju koja kontinuirano osluškuje ove trap-ove i odmah po dobijanju izbacuje na ekran alarm da je došlo do jednog od ova dva događaja, na kom ruteru je došlo do ovog događaja i tačno vreme događaja.

Način konfigurisanja trapova na ruterima je opisan na ovoj stranici:

https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/13506-snmp-traps.html

Verifikacija rešenja:

Isprobaće se promene susedskih odnosa i pojava trapa na ekranu.

Varijanta 7:

Na ruteru R3 konfigurisati da sve rute koje dolaze od R1 dobiju Local Preference (LP) vrednost 100, a da sve rute koje dolaze od R2 da dobijaju LP vrednost 150. Na R3 konfigurisati da kada za neku mrežu primi rutu uz koju je dodata community vrednost 3:50, da se za tu rutu postavlja vrednost LP na 50, a da kada primi rutu sa Community vrednošću 3:200 da se za tu rutu postavlja LP na 200. Na ruteru R1 konfigurisati da se uz rutu 192.168.10.0/24 kada se oglašava ka R3 pridružuje Community vrednost 3:200. Način konfigurisanje Community vrednosti je dat ovde:

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/28784-bgp-community.html

Napraviti aplikaciju koja prati rad SNMP protokola na svim ruterima. Koristiti SNMP deo MIB-2. Aplikacija treba da svakih 10s prikuplja sledeće statističke parametre o radu SNMP na ruteru: Broj dolaznih SNMP paketa, broj odlaznih SNMP paketa, broj get zahteva, broj set zahteva, broj generisanih trap-ova, broj neispravnih community vrednosti u zahtevima.

Verifikacija rešenja:

Uključivanje trap-ova, generisanje zahteva sa pogrešnim community vrednostima, kontinuirano praćenje SNMP statistike.

Varijanta 8:

Napraviti aplikaciju koja kontinuirano prati rad svih rutera i prati zauzeće njihovih procesora i memorije. U okviru grafičkog interfejsa aplikacije postaviti da je moguće da se na početku rada aplikacije postavi vrednost za period sa kojim će aplikacija očitavati potrebne promenljive (u sekundama). Prikupljene podatke prezentovati u obliku grafika koji prikazuje promenu očitanog parametra u vremenu. Sa svakom očitanom novom vrednošću grafik se dopunjava. Potrebno je pratiti sledeće parametre: zauzeće procesora tokom prethodnih 5s, 1min i 5 min, količina zauzete i slobodne memorije u svim memorijskim poolovima koje poseduje ruter i oznake (imena tih pool-ova). Za ovo koristiti Cisco-ve SNMP MIBove: CISCO-MEMORY-POOL, CISCO-PROCESS-MIB.

Verifikacija rešenja:

Uključivanje novih funkcionalnosti na ruteru koje treba da povećaju opterećenje procesora (reset BGP sesije, dodavanje novih ruta i sl.).

Varijanta 9:

Napraviti aplikaciju koja kontinuirano prati sve TCP sesije koje su aktivne na ruteru i otvorene UDP portove. Sesije i portove treba proveravati svakih 5 sekundi i uvek prikazivati, u formi tabele koja će se ažurirati, samo one koje su aktivne (one koje su između dva upita nestale treba izbrisati, a nove dodavati). Za svaku sesiju je potrebno prikazati lokalnu i udaljenu IP adresu, lokalni i udaljeni port, a za otvorene UDP portove adrese i brojeve portova. Koristiti UDP i TCP delove SNMP MIB-2 stabla.

Na ruteru R1 konfigurisati veb server. Iz browsera na virtuelnoj mašini se povezivati na ruter i tako verifikovati rad aplikacije (stvoriće se nova TCP sesija). Način konfiguracije veb server na ruteru je dat ovde:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/https/configuration/12-2sy/https-12-2sy-book/nm-http-web.html

Verifikacija rešenja:

Kreiranje novih sesija i verifikacija njihovog prikazivanja.