Preporuke za menadžment i monitoring mreže

Dokument najbolje prakse
(smernice i preporuke)

Izrađen u okviru AMRES tematske grupe za oblast NMS
(AMRES BDP 101)

Autori: Esad Saitović, Ivan Ivanović

Februar, 2011.

Dokument broj: GN3-NA3-T4-AMRES-BPD-101
Verzija / datum: Februar, 2011.
Izvorni jezik : Srpski
Originalni naslov: „Preporuke za monitoring i menadžment mreže”
Originalna verzija / datum: Revizija 1 (dokumenta od 24. oktobara 2009.) / 2. februar 2011.
Kontakt: esad@rcub.bg.ac.rs, ivan.ivanovic@rcub.bg.ac.rs

AMRES/RCUB snosi odgovornost za sadržaj ovog dokumenta. U izradi dokumenta učestvovala je tematska grupa za NMS, organizovana u AMRESu radi sprovođenja zajedničkih aktivnosti na razvoju i širenju dokumenata sa tehničkim smernicama i preporukama za mrežne servise u višokoškolskim obrazovnim i istraživačkim ustanovama u Srbiji.

Dokument je nastao kao rezultat istraživanja koja su finansirana sredstvima Sedmog okvirnog programa Evropske zajednice (FP7/2007-2013) po ugovoru br. 238875, koji se odnosi na projekat „Multi-Gigabit European Research and Education Network and Associated Services (GN3)”.

Sadržaj

Rezime

Cilj ovog dokumenta je da pruži uvid u osnovne NMS aktivnosti, zajedno s preporukama za administratore kampus i/ili lokalnih mreža koji planiraju da primene NMS alat unutar svojih mreža.

Dokument počinje razmatranjem topologije mreže. Promene u topologiji su predložene u skladu sa idejom da bi većina NMS aktivnosti trebalo da se odvijaju kroz menadžment segment mreže. Dve alternative su razmatrane. Menadžment mreža i produkciona mreža mogu biti fizički odvojene mreže (out-band management segment) ili mogu da dele istu fiziču infrastrukturu (VLAN segment mreže).

Dokument identifikuje najmanje tri komponente koje bi trebalo da budu pokrivene Network Managament System-om. To su upravljanje konfiguracijama i upravljanje logovima, uz već prepoznatu Network Monitoring komponentu koja se impementira upotrebnom nekog od NMS softverskih paketa.

Dokument ukratko opisuje načešće korištene portokole za upravljanje i njihovu upotrebu u različitim okruženjima i na različitim tipovima uređaja u mreži (tj. mrežni uređaji, serveri, UPS uređaji, A/C), uz uslov da ne ugrožavaju sigurost mreže.

Uvod

Sistemi za menadžment mreža danas predstavljaju jedan od najvažnijih elemenata uspešnog funkcionisanja računarskih mreža. Održavanje i konfiguracija mrežnih uređaja, servera i servisa, kao i kontinualno nadgledanje rada svih uređaja u mreži, predstavljaju ključne elemente sistema za menadžment mreža. Za pozdan i bezbedan menadžment uređaja i servisa, neophodno je dizajnirati mrežu tako da se obezbedi najveći nivo sigurnosti i izolovanosti menadžment saobraćaja od produkcionog saobraćaja. Drugi aspekt uspešnog menadžmenta računarskih mreža jesu protokoli koji se za tu svrhu koriste, kao i njihova implementacija, odnosno način upotrebe. U prvom delu, dokument opisuje dizajn menadžment dela mreže (out-of-band, in-band), zatim preporuke za korišćenje protokola za pristup uređajima kao i metode za čuvanje (backup) konfiguracija. U drugom delu, dokument opisuje protokole za nadgledanje u računarskim mrežama i protokol za analizu saobraćaja (netflow), kao i njihovu implementaciju i način upotrebe.

1 Priprema mreže za implementaciju NMS-a

1.1 *In-band* vs *Out-of-band*

In-band menadžment podrazumeva da se za svrhu menadžmenta koriste interfjesi i mrežna oprema koja se ujedno koristi i za produkcioni saobraćaj.

Out-of-band menadžment podrazumeva korišcenje zasebne mrežne infrastrukture i zasebnih intefejsa za svrhu menadžmenta u odnosu na mrežne uređaje i interfejse uređaja koji se koriste za produkcioni saobraćaj.

Out-of-band menadžment se preporučuje za kampus mreže ili delove kampus mreža koje su koncipirane tako da se mrežna oprema i serveri nalaze u jednoj prostoriji (mašinskoj sali / server sobi / jednom čvorištu).

1.1.1 *In-band* okruženje

Prednosti:

- Ne zahteva dodatnu fizičku infrastrukturu (mrežne intefejse na serverima, zasebne mrežne uređaje, pasivnu infrastrukturu).

Mane:

- Smanjen nivo sigurnosti, obzirom da menadžment saobraćaj koji predstavlja "osetljiv" sadržaj, prolazi kroz istu infrastrukturu kao i produkcioni saobraćaj, odnosno, saobraćaj ka krajnjim korisnicima;
- U slučaju zagušenja (u normalnom radu, ili usled nekog *Denial of Service* napada), otežan je (možda i onemogućen) pristup uređajima radi intervencija koje bi pomogle eliminisanju problema.

1.1.2 *Out-of-band* okruženje

Prednosti:

- Fizički izdvojena infrastruktura pruža veću sigurnost za „osetljive“ menadžment informacije.
- Omogućen pristup i u slučaju problema na produkcionim linkovima (npr. prekid linka, zagušenje itd.)

Mane:

- Zasebna mrežna infrastruktura podrazumeva i troškove za nabavku opreme
- Zahveta veće inicijalno angažovanje administratorskog osoblja i troškove za implementaciju

1.2 Logička segmentacija mreže u *in-band* menadžment okruženju

Jedan od ključnih elemenata u organizaciji mreže jeste logička segmentacija mreže. Ovo se postiže definisanjem radnih grupa i kreiranjem VLAN-ova za svaku od grupa. Takođe, potrebno je definisati i VLAN za svrhu menadžmenta.

Definisanje VLAN-ova se može obaviti na sledeći način:

- VLAN-MGMT - VLAN za menadžment. Iako je uobičajeno da taj VLAN bude VLAN 1, zbog povećanja sigurnosti, preporučuje se da se za svrhu menadžmenta definiše neki drugi VLAN, kroz koji će prolaziti samo menadžment saobraćaj.
- VLAN-SERVER-ENT - VLAN za *enterprise* servere (DNS, proxy, e-mail, web ...)
- VLAN-SERVER-<workgroup> - VLAN za *workgroup* servere (razni aplikativni serveri, serveri baza podataka i sl.)
- VLAN-ADMIN - Administratorski VLAN
- VLAN-USER-<workgroup> - Korisnički VLAN-ovi u zavisnosti od radne grupe

2 Interfejsi za pristup uređajima

Potrebno je razmotriti koje mogućnosti su raspoložive za pristup različitim tipovima uređaja, kao i preporuke za primenu pojedinih rešenja u zavisnosti od topologije mreže. Definisane su tri grupe uređaja:

- Mrežni uređaji - ruteri, *layer2* i *layer3* svičevi
- Serveri
- Ostali uređaji - UPS, klima uređaji, štampači i sl.

2.1 Mrežni uređaji

Pristup mrežnim uređajima se može obaviti na neki od sledećih načina:

- *Console* port - pristup korišćenjem ovog porta predstavlja pristup interfejsu komandne linije (*Command Line Interface - CLI*). Ovakav vid pristupa uređaju ne zahteva komunikaciju kroz mrežu već se zahteva direktna veza serijskog (COM) porta računara sa kojim se pristupa uređaju i samog *Console* porta. Pristup uređajima putem *Console* porta se koristi za inicijalane konfiguracije uređaja, ažuriranje softvera na uređajima, resetovanje šifara za pristup, kao i za situacije kada uređaju nije moguće prići putem mrežnih intefejsa. Pristup se obavlja korišćenjem nekog od softvera za terminalni pristup (Hyper Terminal, Putty, SecureCRT itd.)
- AUX - predstavlja port koji se može iskoristiti za udaljeno povezivanje na uređaj korišcenjem *dial-in* veze. Kako ovaj dokument predstavlja preporuke za kampus i lokalne mreže, nema ozbiljnih situacija u kojima bi implementacija ovog rešenja za pristup bila opravdana.
- OOBM - pojedini proizvođači mrežne opreme ugrađuju *out-of-band* menadžment portove kojima se dodeljuje IP adresa i omogućava pristup kao i bilo kom mrežnom interfejsu, ali je ograničen pristup na podržane menadžment protokole (telnet, ssh, http...)
- Zaseban ethernet intefejs - Kada su u pitanju mrežni uređaji, izdvajanje zasebnog mrežnog intefejsa samo za namenu menadžmenta nije uobičajeno (može se reći i nije preporučljivo) obzirom da je cena "po interfejsu" na ruterima značajno velika. Kada su u pitanju svičevi sa velikim brojem portova, izdvajanje zasebnog interfejsa jeste preporučljivo rešenje, ali samo u okviru data centra, odnosno, ukoliko nije potrebno postavljanje dodatne pasivne infrastrukture (troškovi OOBM-a, pogledati poglavlje 2.)

- VLAN-MGMT pristup - Pristup mrežnim uređajima kroz logilčko odvajanje saobraćaja u zaseban VLAN za menadžment je preporučljivo, jer je za implementaciju potrebno izvršiti samo konfiguraciju postojeće aktivne opreme. Po uređajima, konfiguracija se svodi na sledeće:
    - Svičevi - sve veze izmedu svičeva treba da se nalaze u modu za prenos više VLAN-ova (generalno IEEE 802.1Q standard, kao što je trunk mod kod Cisco uređaja, ili tagging mod kod drugih proizvođača). Kroz taj link je potrebno "propustiti" i menadžment VLAN (VLAN-MGMT).
    - Ruteri - na ruterima je potrebno definisati podinterfejse (subinterface) sa IP adresom iz opsega definisanog za menadžment VLAN (takođe,uz korišćenje IEEE 802.1Q standarda).

Kada se konfiguriše obeležavanje frejmova (802.1Q), Cisco uređaji (možda još neki proizvođač) prekonfigurisano šalju frejmove iz VLAN1 kao 802.3 frejmove, odnosno šalju ih neobeležene.

Kod drugih proizvođača, potrebno je definisati koji se VLAN šalje kao neobeležen (*untagged*).

Radi povećanja sigurnosti preporuka je da se, ukoliko je to na uređajima moguće konfigurisati, saobraćaj za sve VLAN-ove šalje obeležen. Ukoliko na nekim uređajima nije moguće slati sve VLAN-ove obeležene, preporuka je da se definiše VLAN koji će biti izolovan od ostatka mreže (*black-hole*) i da se saobraćaj ovog VLAN-a šalje kao neobeležen.

2.2 Serveri

Pristup serverima u svrhu menadžmenta se može ostvariti na neki od sledećih načina:

- KVM svič - uobičajeno je da su serveri locirani na jednom mestu, rek ormanima, na stolovima u serverskoj sali i sl. Da bi se olakšao pritup samim serverima, praksa je da se koristi KVM svič koji omogućava vezu keyboard-video-mouse priključaka svih servera sa jednim fizičkim setom ovih komponenti (tastatura, monitor, miš). Menadžment servera se na ovaj način može vršiti samo ukoliko se administrator fizički nalazi u serverskoj sali gde se nalazi i KVM svič.
- OOBM - poznatiji proizvođači u servere ugrađuju i port za out-of-band menadžment. Ovaj port predstavlja još jedan mrežni interfejs, ali ima specijalnu namenu.

  Prednosti:

    - Ovaj port ima zaseban kontroler na matičnoj ploči i omogućava TCP/IP pristup serveru nezavisno od operativnog sistema na serveru. Ovim je omogućen udaljen pregled dešavanja na samom serveru kao da je u pitanju direktan pristup serveru (tastatura-monitor-miš), uključujući i sam proces startovanja servera (booting process)
    - Udaljeni pristup BIOS podešavanjima servera
    - Udaljena kontrola - uključivanje, isključivanje i restart servera

  Mane:

    - U zavisnosti od proizvođača, razlikuje se implementacija ovog rešenja - ne postoji uniformno rešenje
    - U osnovnoj (besplatnoj) verziji pristupa serveru po ovom portu, limitirane su funkcionalnosti. Za širi set funkionalnosti, kod pojedinih proizvođača, potrebno je platiti licence.
- Mrežni intefejs - preporuka je da serveri imaju najmanje dva mrežna interfejsa, što je uobičajen slučaj sa serverima koji su danas u prodaji. Sa druge strane, nije neuobičajeno da se za serverske funkcije koriste klijentski računari boljih performansi koji imaju samo jedan mrežni interfejs.

Pristup serverima u ovim različitim okolnostima tretiramo na sledeći način:

Serveri sa najmanje dva mrežna interfejsa:

- Preporuka je da se jedan od interfejsa servera konfiguriše kao menadžment interfejs, odnosno da se nalazi u mreži za menadžment (OOB deo mreže ili menadžment VLAN). Drugi (ostali) interfejsi servera ne bi trebali da se koriste za svrhu menadžmenta.
- Drugi (ostali) interfejsi servera se koriste za produkcioni pristup servisima koje server nudi.

Serveri koji imaju jedan mrežni interfejs

- Kako je kod ovih servera nemoguće fizički odvojiti menadžment saobraćaj od produkcijskog, preporučuju se dva pristupa u zavisnosti od hardvera. Pri bilo kom od ovih pristupa, preporučuje se korišćenje protokola za pristup koji kriptuju saobraćaj.
  - Ukoliko mrežna kartica podržava IEEE 802.1Q standard, preporučuje se da se na samoj kartici definišu logički interfejsi koji se pridružuju različitim VLAN-ovima, uključujući i jedan logicki interfejs pridružen menadžment VLAN-u.
  - Ukoliko mrežna kartica ne podržava IEEE 802.1Q standard, tada ni logički nije moguće odvojiti menadžment saobraćaj od produkcionog. U ovom slučaju, server ne bi trebalo da ima vezu sa menadžment delom mreže.

2.3 Ostali uređaji

Pod grupom ostali uređaji, definišemo sve uređaje kojima primarna namena nema potrebe za mrežnom komunikacijom (npr. uređaji za neprekidno napajanje, klima uređaji, senzori za vlagu). Pristup radi menadžmenta se obavlja preko sledećih intefejsa:

- Serijski port - menadžment korišćenjem serijskog porta na uređajima se obavlja koristeći namenski softver proizvođača. Uobičajeno je da ukoliko postoji i mrežni interfejs na uređaju, serijski port služi samo za inicijalna podešavanja IP parametara radi prelaska na pristup po mrežnom interfejsu.
- Mrežni interfejs - poznatiji proizvođači u paleti proizvoda imaju i kartice sa mrežnim interfejsom koje se ugrađuju u njihove uređaje za svrhu menadžmenta.

3 Pristup menadžment mreži

Za definisanje načina pritupa menadžment mreži potrebno je definisati:

- IP adresiranje uređaja u menadžment mreži
- Metode pristupa menadžment mreži
- Nivo međusobne izolovanosti uređaja u menadžment mreži

3.1 IP adresiranje

Radi povećanja sigurnosti menadžment delova mreže, preporučuje se da se za te delove mreže definišu zasebni IP adresni opsezi. Ovo važi za *out-of-band* menadžment mrežu, kao i za menadžment VLAN segment. Ovi opsezi adresa ne bi trebalo da se oglašavaju (rutiraju) ostatku mreže.

3.2 Pristup menadžment delovima mreže od strane administratorskog osoblja

Potrebno je definisati metode pristupa menadžment delovima mreže u različitim okruženjima i situacijama.

Ovde smo definisali tri metode pristupa:

Pristup uređajima iz menadžment dela mreže:

- Za ovaj vid pristupa potrebno je da u menadžment delu mreže postoji računar čiji je jedini mrežni interfejs priključen u samu menadžment mrežu.
- Ovom računaru je dozvoljen pristup samo u okviru menadžment dela mreže.

Pristup uređajima iz administratorskog VLAN segmenta:

- Korišćenje NAT funkionalnosti za administratorske računare koji prilaze uređajima u menadžment delu mreže
- Adrese u koje se transliraju administratorski računari su iz adresnog opsega menadžment dela mreže. Na ovaj način se postiže efekat pristupa iz same menadžment mreže

Pristup uređajima sa udaljenih lokacija:

- Obavezno korišćenje VPN tehnologije za pristup
- Kao i za pristup iz administratorskog VLAN segmenta i ovde se primenjuje funkcija NAT-a po istom modelu

3.3 Međusobna izolovanost uređaja u menadžment mreži

Radi postizanja većeg nivoa sigurnosti, potrebno je ograničiti međusobnu komunikaciju uređaja u menadžment mreži. Preporuke za ova ograničenja su:

- Menadžment serverima se omogućava komunikacija sa svim ostalim uređajima u menadžment mreži, ali samo za menadžment protokole.
- Ostali uređaji međusobno ne mogu da komuniciraju kroz menadžment mrežu

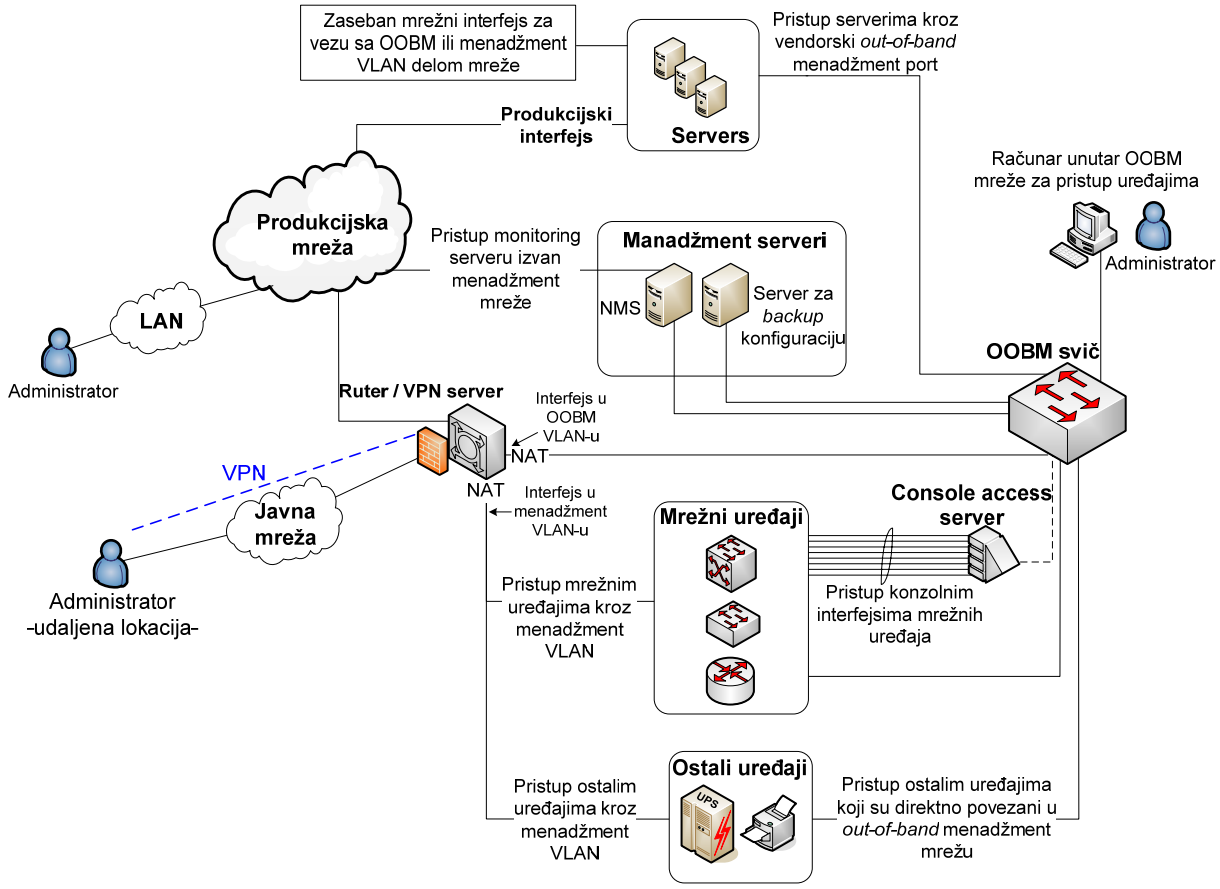
Ovaj nivo izolovanosti se na Cisco uređajima (možda na uređajima još nekog proizvođača) može postići korišćenjem sledećih funkcionalnosti na OOBM sviču.

- Private VLAN
  - Portovi na OOBM sviču, na koje su povezani svi uređaji (osim menadžment servera) se nalaze u Isolated modu rada. Portovi koji se nalaze u Isolated modu rada mogu da komuniciraju samo sa portovima koji se nalaze u Promiscuous modu rada.
  - Portovi na OOBM sviču, na koje su povezani menadžment serveri (kao i portovi za pristup OOBM mreži od strane administratora) se nalaze u Promiscuous modu rada. Portovi koji se nalaze u Promiscuous modu rada mogu da komuniciraju sa svim portovima, bez obzira na njihov mod rada.
- MAC-Access Control List
  - Omogućava se filtriranje unutar broadcast domena, bazirano na MAC adresama uređaja.

3.4 Primeri topologija

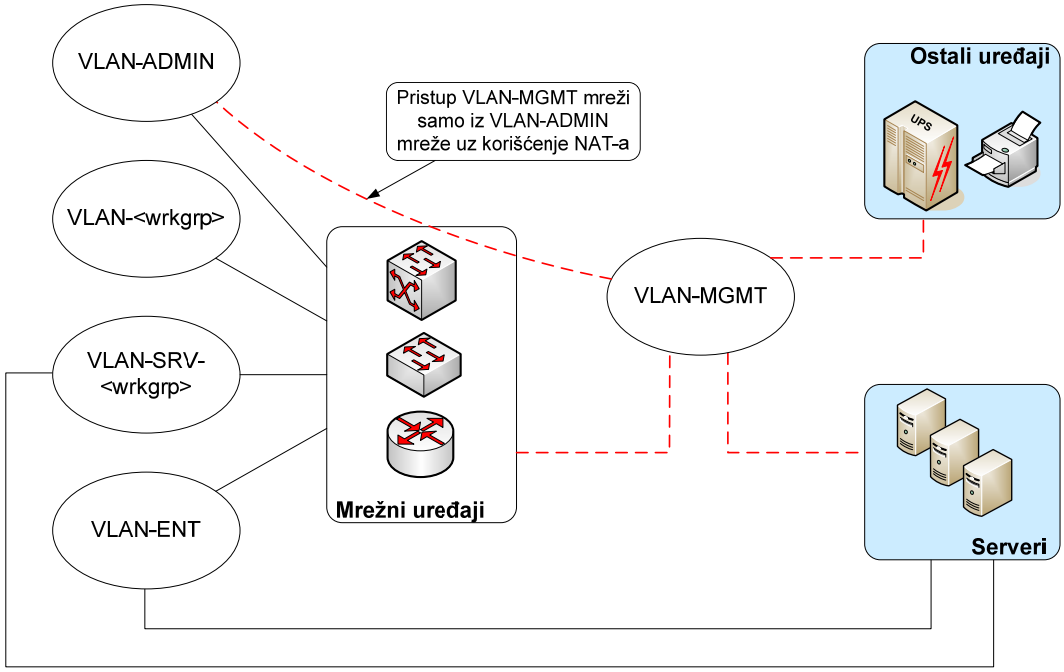
Na slici 3-1 je prikazan sveobuhvatni primer topologije menadžment mreže. Na primeru su prikazani:

- *Out-of-band* menadžment mreža
- Tri metoda pristupa menadžment mreži (racunar u OOBM-u, pristup iz administratorskog VLAN-a, udaljeni pristup kroz VPN)
- Pristup menadžment VLAN mreži iz OOBM mreže
- Veze mrežnih uredaja sa OOBM mrežom korišćenjem *console* porta, specijalizovanog OOBM porta
- Veza mrežnih uredaja sa menadžment mrežom kroz menadžment VLAN
- Dodatni intefejs servera za vezu sa OOBM ili menadžment VLAN delom mreže
- Veze ostalih uređaja sa OOBM ili menadžment VLAN delom mreže
- Pozicije menadžment servera i veze sa menadžment delom mreže, kao i sa ostatkom mreže u slučaju monitoring sistema.



Slika 3-1 Primer sveobuhvatne topologije menadžment mreže

Na slici 3-2 je prikazan primer segmentacije mreže i veze uređaja sa menadžment VLAN-om.



Slika 3-2 Topologija segmentirane mreže i veze uređaja sa menadžment VLAN-om

4 Logički pristup uređajima (protokoli za pristup uređajima)

4.1 Protokoli za kontrolu i konfigurisanje uređaja

Nakon definisanih načina fizičkog pristupa uređajima, potrebno je definisati i komunikacione protokole koji se preporučuju za korišcenje u različitim okolnostima.

Prvo su dati opisi protokola sa osnovnim karakteristikama a zatim i preporuke za korišćenje, zasebno za tipove uređaja sa kojima se komunicira.

TTY - Karakteristike:

- Protokol za asinhronu serijsku komunikaciju. Koristi se u komunikaciji sa Console portom mrežnih uređaja.

Telnet - Karakteristike:

- Omogućava pristup komandnoj liniji (Command Line Interface - CLI)
- Protokol je podržan na gotovo svim uređajima
- Komunikacija između telnet klijenta (uređaja sa kojeg se pristupa) i telnet servera (uređaja kojem se pristupa) se obavlja u ne-enkriptovanom modu (clear text) što je ključna mana ovog protokola.

SSH (*Secure Shell*) - Karakteristike:

- Omogućava pristup komandnoj liniji (vizuelno, identican Telnet protokolu)
- Komunikacija između SSH klijenta i SSH servera se obavlja u enkriptovanom obliku, zbog čega se preporučuje za primenu umesto Telnet protokola, gde god je to moguće
- Za podršku ovom protokolu uređaji moraju imati softversku podršku za kriptovanje

RDP (*Remote Desktop Protocol*) - Karakteristike:

- Omogućava grafički pristup serveru (pristup desktopu)
- Razvijen od strane Microsoft-a, ali postoje implementacije i za druge OS platforme
- Nivo kriptovanja podataka koji se prenose u komunikaciji RDP klijent - RDP server, se može podesiti na RDP serveru (windows server platforme). Koristi se algoritam RSA RC4, koji ima svoje nedostatke i ne može se okarakterisati kao potpuno siguran.

- Korišćenje se preporučuje kroz VPN mreže

VNC (*Virtual Network Computing*) - Karakteristike:

- U pitanju je aplikacija bazirana na RFB protokolu (Remote FrameBuffering)
- Kao i RDP, omogućava grafički pristup serverima
- Postoji nekoliko verzija VNC aplikacija i implementacija koje su besplatne, kao i onih za koje su potrebne licence
- VNC u svojoj osnovnoj (besplatnoj) verziji ne podržava nikakve mehanizme enkriptovanja saobraćaja.
- Korišćenje se preporučuje kroz VPN mreže

HTTP(S) {*HyperText Transfer Protocol (Secure)*} - Karakteristike

- Omogućava *web* pristup uredajima
- U osnovnoj varijanti ne podržava enkripciju. HTTPS (*HTTP Secure*) predstavlja kombinaciju HTTP i SSL/TLS protokola koji se smatra dovoljno sigurnim za prenos podataka.

4.2 Pristup mrežnim uređajima

Kada su u pitanju mrežni uređaji, korišćenje pojedinih protokola se preporučuje u sledećim okolnostima:

TTY protokol, odnosno pristup Console portu uređaja se preporučuje:

- Kada je potrebno resetovati šifre za pristup uređaju
- Kada nije obezbeđen pristup uređaju kroz mrežu, nekim od protokola opisanih u nastavku
- U slučaju da je otežan ili onemogućen pristup kroz mrežu usled nekog DoS napada, obrisane konfiguracije i/ili pogrešne konfiguracije koja blokira pristup uređaju, itd.

Telnet protokol se preporucuje:

- Kada nije moguća direktna veza na Console port uređaja
- Kada na uredajima ne postoji podrška za SSH pristup, što zavisi od verzije i podržanih funkcija operativnog sistema samog uređaja.
- Ukoliko postoji VPN mreža kroz koju se ostvaruje veza sa sigurnim delom mreže kroz koji se pristupa uređajima (out-of-band segment). Ili ukoliko postoji direktna veza sa menadžment VLAN-om.

SSH protokol se preporučuje:

- Ukoliko operativni sistem uređaja ima podršku za kriptovanje saobraćaja, odnosno, podršku za sam protokol
- Kada ne postoji direktna veza sa mrežom iz koje se sigurno pristupa uređajima (out-of-band segment) ili sa menadžment VLAN-om.

HTTP(S) protokol se preporučuje:

- Ukoliko postoji podrška za HTTP protokol i pod sledećim uslovima:
  - Za osnovnu verziju protokola (HTTP) važe iste preporuke kao za Telnet protokol
  - Za kombinaciju protokola HTTP + SSL/TLS (HTTPS), važe iste preporuke kao i za SSH protokol

4.3 Pristup serverima

Pristup serverima u svrhu menadžmenta se može fleksibilnije podesiti, obzirom da za najveći broj operativnih sistema postoji softverska implementacija gotovo svih protokola za pristup. Okruženja u kojima se preporučuju pojedini protokoli:

SSH pristup se preporučuje:

- Kada su u pitanju Unix bazirani operativni sistemi, pristup korišcenjem SSH protokola je uobičajena praksa i nje se treba držati.

Grafički pristup:

- Protokoli za grafički pristup (RDP, VNC i sl.) se preporučuju za primenu isključivo kroz menadžment mrežu (*out-of-band* i/ili menadžment VLAN)
- Preporučuje se primena ovih protokola i van menadžment dela mreže ali isključivo ako se koristi VPN veza od klijenta do menadžment dela mreže.

Telnet pristup se preporučuje:

- Iako su retki slučajavi kada je serverima potrebno prići Telnet protokolom, preporuka je da se ovaj protokol koristi samo ukoliko se pristupa serverima kroz interfejs koji se nalazi u menadžment mreži (*out-of-band* ili menadžment VLAN-u). Ovo podrazumeva obavezno postojanje minimum dva mrežna intefejsa servera (poglavlje 2.2)
- Ukoliko postoji VPN veza klijenta (računara sa kojeg se pristupa) sa menadžment delom mreže

4.4 Pristup ostalim uređajima

Prisutup "ostalim" uređajima (UPS, klima uređaji itd.) zavisi od tipa konkretnih uređaja, kao i od hardverskog pristupa uređaju, odnosno od tipova mrežnih intefejsa i protokola koji su podržani. Uobičajeni načini pristupa sa preporukom korišćenja su:

Telnet pristup:

- Korišćenje Telnet protokola se preporučuje isključivo ako je mrežni interfejs uređaja u menadžment delu mreže (*out-of-band* i/ili menadžment VLAN-u)
- Ukoliko nije moguće povezati mrežni intefejs uređaja u zaštićeni menadžment deo mreže, Telnet protokol se ne preporučuje.

Web pristup:

- Ukoliko postoji podrška za *web* (HTTP) pristup, preporuka je korišćenje istih samo ukoliko je mrežni interfejs u zaštićenom menadžment delu mreže. *Web* pristup korišćenjem HTTPS protokola je preporučljivo koristiti i ukoliko mrežni interfejs uređaja nije povezan u zaštićeni menadžment deo mreže.

4.5 Protokoli za nadgledanje uređaja

Dosta današnjih mrežnih sistema se oslanja na monitoring pomoću SNMP protokola. Sam SNMP protokol je dizajniran tako da veoma malo opterećuje mrežu. Naziva se prostim protokolom zato što koristi proste (nestrukturirane) tipove podataka. Ovaj protokol aplikativnog nivoa OSI modela sastavni je deo TCP/IP steka protokola. Sastoji se od skupa standarda kojima se definišu: način upravljanja mrežom, baze podataka za čuvanje informacija i strukture korišćenih podataka. Koristi UDP kao transportni protokol, mada je moguće podesiti i rad preko TCP-a. Korišćenje SNMP protokola preko TCP-a nije preporučljivo u velikim mrežama usled uspostavljanja velikog broja konekcija, što može opteretiti uređaje, i zbog veličine zaglavlja TCP protokola, što može povećati saobraćaj na linku. Trenutno su aktuelne dve verzije SNMP protokola, SNMP v2c i SNMP v3. Karakteristike verzija sa stanovišta sigurnosti su date u tabeli 4.5.1.

Tabela 4.5.1 – Karakteristike SNMP protokola.

SNMP Security modeli i nivoi				
Model	Nivo	Autentifikacija	Enkripcija	Princip rada
v1	noAuthNoPriv	Community String	-	Koristi Community string za autentifikaciju.
v2c	noAuthNoPriv	Community String	-	Koristi Community string za autentifikaciju.
v3	noAuthNoPriv	Korisničko ime	-	Koristi Korisničko ime za autentifikaciju.
v3	authNoPriv	MD5 ili SHA	-	Autentifikacija se bazira na HMAC-MD5 ili HMAC-SHA algoritmu. Umesto šifre se šalje MD5 ili SHA hash.
v3	authPriv	MD5 ili SHA	DES/AES	Autentifikacija se bazira na MD5 ili SHA algoritmu. Omogucuje DES/AES enkripciju prilikom prenosa podataka.

Dva osnovna moda rada SNMP protokola su READ i READ/WRITE mod. READ mod omogućuje samo očitavanje SNMP promenjivih sa udaljenog uređaja, dok READ/WRITE omogućuje postavljanje pojedinih varijabli na udaljenom uređaju, odnosno kontrolu uređaja (restart rutera, backup trenute konfiguracije...). Prilikom konfigurisanja agenta na udaljenom uređaju moguće je podesiti ograničenja na MIB bazi (*Management Information Base*). Ako se READ/WRITE opcija koristi za setovanje samo jedne OID varijable, u MIB bazi treba izvršiti ograničenja na SNMP agentu samo na tu OID vrednost. Tada bi podešavanje ostalih OID vrednosti bilo zabranjeno. Ovi primeri ce biti dati u sekciji koja se odnosi na podešavanje agenata na pojedinim tipovima uređaja.

4.5.1 SNMP v2c

Trenutno najzastupljenija verzija SNMP protokola je SNMP v2c (RFC 1901-1908). Kod verzije SNMP v2c se autentifikacija vrši pomoću community stringa i on se šalje u čistom tekstu preko mreže. U slučaju da neko "uhvati" ovaj saobraćaj pomoću neke sniffing aplikacije, može vrlo lako otkriti community string i na taj način biti u mogućnosti da ugrozi ispravan rad mreže. Korišćenje SNMP v2c se preporučuje samo kada sami uređaji ne podržavaju verziju SNMP v3, ali tada se obavezno uvode drugi mehanizmi za zaštitu prilikom prenosa podataka (ACL, Firewalls....). Za nadgledanje mreže preporučuje se korišćenje READ moda, a u slučaju potrebe za kontrolom mreže (READ/WRITE) putem SNMP protokola preporučuje se uvođenje ograničenja u MIB bazi. Prilikom pokretanja SNMP v2c agenta na uređajima obično postoji predefinisana vrednost za community string i ona je postavljena na vrednost "public". Taj, već svima poznati, predefinisani community string treba obavezno promeniti na neku drugu vrednost po mogućstvu kombinaciju brojeva i slova.

4.5.2 SNMP v3

Potreba za sigurnošcu u mreži dovela je do razvoja SNMP v3.

SNMP v3 uvodi važne bezbednosne aspekte:

1. Integritet poruke (Message integrity), sprečava mogućnost izmene paketa prilikom prenosa
2. Autentifikacija, potvrda da je poruka stigla sa pravog izvorišta
3. Kriptovanje paketa, sprečavanje čitanja poruka od strane neautorizovanog izvora

Iz tabele 4.5.1 se vidi da se kod SNMP v3 uvodi tri različita nivoa sigurnosti. Najsigurniji nivo koristi autentifikaciju baziranu na SHA algoritmu i koristi DES ili AES enkripciju. Pre uvođenja nivoa sigurnosti treba proveriti da li mrežni uređaji podržavaju enkripciju saobraćaja. U slučaju da uređaji ne podržavaju enkripciju, može se koristiti niži nivo sigurnosti koji koristi samo autentifikaciju. Treći, najslabiji nivo sigurnosti se ponaša praktično kao SNMP v2c i koristi korisničko ime, isto kao što SNMP v2c koristi community string, za pristup uređaju. Prilikom pokretanja SNMP v3 agenta preporučeno je uvesti ograničenja u MIB bazi za READ i READ/WRITE mod na pojedine OID vrednosti.

5 Održavanje konfiguracija

5.1 *Backup* konfiguracija

Kako uvek može doci do nenadanog otkaza nekog od uredaja, ili dela njegove funkcionalnosti, poželjno je da se pri zameni istog, uredaj postavi u stanje funkcionalnosti koje je imao pre otkaza i to uz minimizaciju vremena otkaza (down-time). Ovo je moguce ukoliko se pravilno i redovno održava backup konfiguracija svih uredaja u mreži.

Kada su pojedinačni tipovi uredaja u pitanju, pri *backup*-u konfiguracija, prvenstveno se misli na mrežne uredaje. *Backup* konfiguracije kod mrežnih uredaja je uobicajeno da se vrši primenom nekog od jednostavnih protokola za prenos podataka kao što su TFTP i RCP.

Zajednicka mana ovih protokola je prenos podataka u neenkriptovanom obliku. Ovo predstavlja problem, jer su često poverljive informacije upravo u konfiguracijama koje se *backup*-uju (*korisničko ime/šifra*, verzije operativnog sistema i sl.). TFTP se smatra još nesigurnijim protokolom, obzirom da nema funkciju autentifikacije pristupa serveru.

Zbog svega gore navedenog, preporucuje se da se *backup* konfiguracija vrši tako da su serveri za *backup* (TFTP i/ili RCP) **obavezno** povezani **samo** u zašticeni menadžment deo mreže i izolovani od ostatka mreže.

Kada su u pitanju serveri, potrebno je *backup*-ovati sve konfiguracione parametre nekog servisa. Ovo je izvodljivo ukoliko se konfiguracioni parametri nalaze u nekom konfiguracionom fajlu, pa se isti može preneti nekim protokolom za prenos podataka kao što su FTP ili SCP na server za *backup*.

Preporucuje se korišcenje SCP protokola za prenos, obzirom da za razliku od FTP-a, enkriptuje podatke pri prenosu.

Eventualno, moguce je vršiti *backup* ukoliko sama serverska (klijentska) aplikacija ima implementiran neki mehanizam za *backup*.

6 Nms server

6.1 Pozicija NMS servera u mreži

Pri definisanju pozicije NMS servera u mreži potrebno je striktno definisati politiku pristupa NMS serveru. Za kampus mreže preporuke su sledeće:

- NMS server mora da ima jedan mrežni interfejs koji se nalazi u menadžment mreži (OOBM ili menadžment VLAN-u). Ovaj interfejs služi kako za menadžment samog NMS servera, tako i za komunikaciju NMS alata sa ostalim uređajima u mreži.
- NMS može, ukoliko je to potrebno, imati dodatni mrežni interfejs u produkcijskom delu mreže. Ovaj interfejs bi imao ulogu pristupa monitoring sistemu radi nadgledanja trenutnog statusa uređaja i detekcije alarma. Pristup po ovom interfejsu bi trebao biti limitiran na *read only* mod, sa mogućnošću izvršavanja pojedinih predefinisanih akcija radi dijagnostike. Takođe, potrebno je limitirati pristup preko ovog interfejsa samo na željene korisnike (administratori i *helpdesk* služba).

6.2 Preporučena verzija SNMPa na mrežnim uređajima i serverima

Većina uređaja podržava verziju SNMP v2c dok samo noviji uređaji podržavaju verziju SNMP v3. Verzija SNMP protokola kod servera zavisi isključivo od tipa operativnog sistema koji se koristi. Kako Windows OS ne podržava verziju SNMP v3 potrebno je naći SNMP agenta koji je podžava i instalirati ga. Jedna od besplatnih Windows verzija SNMP v3 agenta, koja je bazirana na linux-ovom paketu “NET-SNMP”, može se preuzeti sa sledećeg sajta (http://marksw.com/snmpv3agent/windowsagent.html). Postoji dosta besplatnih varijanti Windows SNMP agenata koje se mogu preuzeti sa Interneta. U okviru instalacije Linux OS postoji paket “NET-SNMP” koji podržava verziju SNMP v3 i koji može da se instalira zajedno sa operativnim sistemom. Implementacija SNMP v3 kod servera neće imati veliki uticaj na performanse uređaja tako da je SNMP v3 sa najvišim nivoom sigurnosti preporučena za korišćenje kod servera. U slučaju rutera i svičeva problem se može javiti ako su memorija i CPU već opterećeni sa nekim drugim procesima tako da pokretanje SNMP v3 može imati uticaj na performanse uređaja, naručito ako se očitava cela MIB baza i pritom se koristi nivo sigurnosti koji koristi enkripciju. U tom slučaju bez obzira što uređaji podržavaju verziju SNMP v3 nije preporučljivo pokretati enkripciju SNMP saobraćaja da ne bi došlo do degradacije peformansi uređaja, već pokrenuti nivo koji koristi samo autentifikaciju.

6.3 Preporučene promenjive za nadgledanje

Pre implementacije monitoring sistema u mrežu potrebno je definisati parametre koji će se nadgledati. MIB baza pruža veliki broj OID parametara i pitanje je kako odabrati vrednosti koje nam pružaju najbitnije informacije o stanju mrežnih uređaja i linkova. Tendencija u IT svetu je da se koriste standardne IETF MIB baze koje svaki proizvođač uređaja treba da podržava.

6.3.1 Mrežni uređaji

Parametri koji se najčešće prate kod mrežnih uređaja kao što su ruteri i svičevi su:

1. Stanje Interfejsa (L2 i L3 veza)
2. Protok na interfejsu (dobija se indirektno uzastopnim očitavanjem brojača i deljenjem sa vremenskim intervalom izmedu očitavanja)
    i. Standardan In/Out saobraćaj(bits/sec)
    ii. Odbačen In/Out saobraćaj(bits/sec)
    iii. Preneti saobraćaj po In/Out paketima(packets/sec)
3. Opterećenje procesora
4. Opterećenje memorije
    i. I/O memorija
    ii. CPU memorija

U slučaju potrebe za praćenjem funkcija koje se ne sreću na svim uređajima odnosno koje su karakteristične za pojedine proizvođače potrebno je ispitati MIB baze proizvođača koji je napravio taj uređaj.

6.3.2 Serveri

OID promenjive koje se mogu očitavati kod servera zavise od operativnog sistema. U opštem slučaju svi operativni sistemi podržavaju standardne IETF MIB baze, tako da je dosta OID vrednosti univerzalno za sve uređaje koji podržavaju SNMP. Preporučene su sledeće vrednosti:

1. Stanje Interfejsa (L2 i L3 veza)
2. Statistika interfejsa (dobija se indirektno)
    i. Standardan In/Out saobraćaj (bits/sec)
    ii. Odbacen In/Out saobraćaj(bits/sec)
    iii. Protok po In/Out paketima(packets/sec)
    iv. Koliko dugo je interfejs aktivan
3. Opterećenje procesora
4. Opterećenje memorije
    i. HDD memorija
    ii. RAM memorija
5. Swap space memorija
6. Broj sistemskih procesa
7. Lista pokrenutih servisa na serveru
8. Broj uspostavljenih TCP konekcija
9. Broj trenutno ulogovanih sistemskih korisnika

6.3.3 UPS-evi

U slučaju praćenja SNMP promenjivih UPS uređaja, većina OID vrednosti se mora naći u MIB bazama proizvođača. Preporučene varijable su:

1. Trentno stanje UPS-a, odnosno mod rada (battery mod, online mod, malfunction.....)
2. Kapacitet batrije UPS-a
3. Koliko dugo UPS može da radi u battery modu.
4. Temperatura baterije
5. Izlazno opterećenje UPS-a
6. Ulazni napon
7. Izlazni napon
8. Ulazna struja
9. Izlazna struja

6.4 MIB varijable

Varijable u MIB bazi se dele na dve grupe. Prva grupa predstavlja skup varijabli koje se mogu naći na svim uređajima (standardne varijable) dok druga grupa predstavlja varijable koje su specifične samo za pojedine proizvođače mrežnih uređaja (privatne varijable).

6.4.1 Standardne MIB varijable

Standardne IETF MIB baze se nalaze pod MIB-2 (.1.3.6.1.2.1) čvorom u MIB stablu. Neke od najčešće korišćenih varijabli iz ovog čvora su:

1. interfaces (.1.3.6.1.2.1.2) - Ovde se nalaze sve informacije o stanju interfejsa na uređaju.
2. ifMIB (.1.3.6.1.2.1.31) - ifMIB Predstavlja proširenje interfaces MIB baze sa 32bit-nih brojača na 64bit-ne brojače.
3. tcp (.1.3.6.1.2.1.6) - Ovde se nalaze parametri koji opisuju tcp konekcije.
4. host (.1.3.6.1.2.1.25) - Host tabela sadrži informacije o stanju procesora i memorije na serverima.

6.4.2 Privatne MIB varijable

Privatne MIB varijable definiše i implementira proizvođač mrežnih uređaja i one se mogu koristiti samo na uređajima tog proizvođača. Sve privatne MIB varijable se nalaze pod enterprises (.1.3.6.1.4.1) čvorom u MIB bazi. U daljem tekstu su dati primeri MIB varijabli pojedinih proizvođača mrežnih uređaja.

1. Cisco(.1.3.6.1.4.1.9) – Sadrži sve privatne MIB varijable koje su podržane na različitim tipovima Cisco uređaja.
2. APC(.1.3.6.1.4.1.318) – Sadrži sve privatne MIB varijable koje su podržane na različitim tipovima APC uređaja.
3. juniperMIB(.1.3.6.1.4.1.2636) - Sadrži sve privatne MIB varijable koje su podržane na različitim tipovima Juniper uređaja.

6.5 *Trap* mod rada

SNMP protokol se koristi za periodično očitavanje podataka sa udaljenih uređaja. Kada bi se desila promena na udaljenom uređaju ona bi bila detektovana tek kada bi je NMS (Network Monitoring System) server očitao, a taj vremenski interval može biti dosta dug. Zato je uveden koncept trap poruka. U slučaju da se desi neka promena na udaljenom uređaju sam udaljeni uređaj bi generisao SNMP trap poruku ka NMS serveru u kojoj bi definisao promenu koja se javila. SNMP trap mod rada je tako dizajniran da isporučuje SNMP trap poruke putem udp-a po portu 162 i to samo u jednom smeru, bez zahteva za potvrdom o tome da li je primljen trap ili ne. SNMP v2c šalje trap poruku sa community stringom u čistom tekstu. Verzija SNMP v3 trap informacije šalje tačno određenom korisniku sa određenom šifrom i određenim engineID-om i ta cela informacija, u zavisnosti od sigurnosnog modela, može biti enkriptovana. Iz ovoga sledi da sam NMS server mora znati korisničko ime, šifru i engineID koji je konfigurisan na udaljenom uređaju da bi mogao da dekriptuje primljeni SNMP v3 trap. Podešavanja koja se koriste za SNMP v3 na udaljenim uređajima se moraju isto podesiti i na NMS serveru. Umesto da se kreira ogroman broj različitih korisnika na NMS, na svim uređajima se može generisati isti korisnik i to samo kao korisnik koji šalje trap poruke. Kako se prilikom kreiranja korisnika na udaljenim uređajima automatski generiše engineID, potrebno je ručno promeniti enginID tako da bude isti za trap korisnika na svim uređajima. Prednosti korišćenja SNMP v3 kod trapa su u tome što nam omogućuju sigurnost prilikom primanja trap poruka, ali ako je mreža dizajnirana tako da nije lako moguće izvršiti bilo kakav vid DoS napada na NMS može se koristiti i SNMP v2c trap mod rada. Kompleksnost konfiguracije za trap kod SNMP v3 je jedan od glavnih razloga zašto se češće koristi SNMP v2c za trap mod rada.

6.6 Primeri konfiguracija SNMP-a na uredajima

U konfiguracijama koje su korišćenje u primerima u nastavku teksta, vrednosti parametra (npr. community string) su prikazane u italic formi.

6.6.1 CISCO Ruter

6.6.1.1 *SNMP v2c*

U ovom primeru su prikazane komande za podešavanje verzije SNMP v2c protokola.

Pomoću sledeće komande, koja se koristi u konfiguracionom modu, pokreće se SNMP agent na ruteru.

```
1. SNMPTEST(config)#snmp-server community donotusepublic ro acl10
```

String koji se koristi kao autentifikacija *donotusepublic* predstavlja vid zaštite tako da će ruter odgovoriti samo onom uređaju koji mu pošalje zahtev koji sadrži baš ovaj string. Opcija **ro** naglašava da je moguće samo očitati podatke a ne i menjati ih (ro-read only). Takođe je moguće i menjati pojedine varijable (wr-write komanda) što može dovesti do promene rada rutera (restart rutera), zato je veoma bitno da se ne koriste fabrički predefinisane vrednosti za community string i da se SNMP upiti ograniče samo na mogućnost očitavanja a ne i menjanja varijabli. Konačno na kraju komande je definisana access lista acl10 pomoću koje se može definisati pristup SNMP agentu na uređaju samo sa određenih ip adresa.

Da bi se ispravno podesio i snmp trap mod rada potrebno je definisati community string za trap mod, pokrenuti SNMP-trap i definisati destinacionu adresu na koju će se slati trap poruke.

```
2. SNMPTEST(config)#snmp server enable traps snmp linkup likdown

3. SNMPTEST(config)#snmp server host 192.168.10.1 version 2c donotusepublic
```

U prvoj komandi se definiše tip akcije za trap. Ako padne link ili se povrati generisaće se trap poruka.
U drugoj komandi se definiše IP adresa na koju će se slati trap-ovi, verzija SNMP-a koja će se koristiti i community string.

6.6.1.2 *SNMP v3*

Pomoću sledećih komanda se pokreće SNMP v3 protokol na Cisco uređajima.

```
1. SNMPTEST(config)#snmp-server view MYGROUPV interfaces included

2. SNMPTEST(config)#snmp server group MYGROUP  v3 auth read MYGROUPV

3. SNMPTEST(config)#snmp server user pera MYGROUP  v3 auth md5 perapass priv
des56 pera1234

4. SNMPTEST(config)#snmp server enable traps linkup linkdown

5. SNMPTEST(config)#snmp server host 192.168.10.1 traps version 3 priv MYGROUP
```

U prvoj komandi se definišu vrednosti u MIB bazi OID-ova koji mogu biti očitani sa uređaja. U ovom slučaju je omogućeno očitavanje OID-a (**interface**) koji opisuju stanje interfejsa na uređaju. Ako se ne definiše ovakva grupa predpostavlja se da je dozvoljen pogled na sve vrednosti u MIB bazi.
Druga komanda definiše grupu **MYGROUP** koja koristi SNMP v3 protokol i koja koristi autentifikaciju. Ova grupa ima mogućnost očitavanja podataka iz MIB baze i to samo onih koji su definisani u "**pogledu**" ***MYGROUPV.***.

Treća komanda definiše korisnika ***pera*** koji pripada grupi ***MYGROUP*** koji koristi SNMP v3, autentifikaciju pomoću ***md5*** algoritma i ima šifru ***perapass***. Poslednjom opcijom u komandi 3 ***des56 pera1234*** se definiše passphrase koji se koristi za **des56** enkripciju SNMP saobraćaja.

Četvrta komanda pokreće SNMP trap mod rada.

Peta komanda definiše NMS server koji će prikupljati trap poruke. U ovom slučaju prilikom komunikacije između NMS i Cisco uređaja koristiće se SNMP v3 i pravila koja su definisana pomoću grupe **MYGROUP**. Odavde se vidi da se engineID automatski generisao i u slučaju da želimo da NMS server može da primi trap poruke od user-a ***pera*** potrebno je videti koji je engineID usera ***pera*** i konfigurisati ga u SNMP agentu na NMS serveru.

Drugi način je da se pomoću sledeće komande manuelno postavi engineID za lokalnog ili udaljenog korisnika.

```
6. snmp server engineID [local engineid-string] | [remote ip-address udp-port
port- number engineid-string]
```

6.6.2 LINUX Server

6.6.2.1 *LINUX Server - SNMP v2c*

U slučaju podešavanja SNMP protokola na Linux operativnim sistemima prvo je potrebno instalirati SNMP deamon-a na server. U sledećem primeru biće opisana instalacija na CentOS 5.X operativnom sistemu pomoću YUM komande. Sledeća komanda omogućuje automatizovanu instalaciju SNMP deamona i korisnih komandi za kontrolu rada SNMP-a.

```
1. yum install net-snmp net-snmp-utils
```

Sledeći korak je podešavanje servisa da se automatski pokreće prilikom startovanja servera. Potrebno je uneti sledeću komandu.

```
2. chkconfig snmpd on
```

Sledeća stavka je podešavanje community stringa i OID objekata koji mogu biti očitani sa servera. Potrebno je editovati fajl snmpd.conf koji se obično nalazi u direktorijumu /etc/snmp/ i izmeniti sledeće redove. U redu

```
com2sec notConfigUser default public
```

potrebno je promeniti defaultni community string public u željeni community string.

U redu

```
view systemview included .1.3.6.1.2.1.1
```

se vidi de su uključeni svi OID-ovi koji se nalaze ispod cvora .1.3.6.1.2.1.1 u MIB drvetu. Pomoću komande excluded moguće je isključiti pojedine OID vrednosti, odnosno uvesti ograničenja u prikazu MIB baze. Ovde je potrebno definisati OID vrednosti koje će server vraćati kao odgovor na SNMP upite. Ako NMS zatraži OID koji nije ovde definisan server neće odgovoriti NMS-u.

Sada je potrebno pokrenuti servis sledećom komandom:

```
3. service snmpd start
```

Proveru je moguće uraditi pomoću sledeće komande:

```
4. snmpwalk -v 2c -c mojcommunity 127.0.0.1
```

Kao rezultat će se prikazati cela MIB tabela (drvo), ili deo MIB tabele, koji je definisan prethodnim komandama za ograničenje prilikom očitavanja MIB baze.

6.6.2.2 *LINUX Server - SNMP v3*

Instalacija SNMP v3 agenta je ista kao za prethodnu verziju 2c, samo je sada potrebno pokrenuti verziju SNMP v3. Potrebno je editovati fajl snmpd.conf, i dodati sledeće komande.

```
syslocation MojGradiliLokacija

syscontact mojemail@provajder.com

view mojpogled included .1.3.6.1.2.1.2.2

createUser john MD5 john1234 DES john5678

rouser john priv -V mojpogled
```

Prva dva parametra, *syslocation* i *syscontact* su podaci koji služe da daju opšte informacije o serveru. Oni nisu značajni za ispravan rad SNMP protokola i mogu se dodati bez obzira na verziju SNMP-a. Bitni su za administratore servera koji će imati pored osnovnih informacija o stanju servera i informaciju o lokaciji servera i kontakt osobi kojoj se mogu obratiti u slučaju pojave problema. *Syslocation* i *Syscontact* su neki od parametara koji se mogu naći na svim uređajima koji podržavaju SNMP protokol.
Treći red definiše pogled *mojpogled*, odnosno skup OID vrednosti iz MIB stabla. U ovom slučaju je definisana tabela interfejsa servera. Moguće je dodati više tabela ili pomoću komande *exclude* isključiti neke OID vrednosti. Ova ograničenja su veoma bitna zato što je pomoću SNMP-a moguće i postaviti neke parametre a to direktno može uticati na ispravan rad uređaja.

Četvrta komanda kreira korisnika *john* cija je šifra *john1234*. Prlikom autentifikacije koristi se *MD5* algoritam, a saobraćaj je enkriptovan pomoću *DES* algoritma. *Passphrase* koji se koristi prilikom enkripcije je *john5678*.

Peta komanda korisniku *john* daje read only (*rouser*) privilegije i to samo nad *mojpogled* pogledom na MIB bazu koji je definasn u trećoj komandi.

Nakon editovanja snmp konfiguracionih fajlova potrebno je restartovati servis da bi se primenile izmene koje su unešene u te fajlove.

Mana ovakog konfigurisanja je što se vrednosti koje su unešene u konfiguracione fajlove čuvaju u čistom tekstu.

Komanda za restart je:

```
1. service snmpd restart
```

Provera podešavanja SNMP v3 na serveru je moguća pomoću komande:

```
2. snmpwalk -v 3 -u john -l authPriv -a MD5 -A john1234 -x DES -X john5678
192.168.1.1
```

6.6.2.3 *Konfiguracija SNMP protokola pomoću Perl skripte*

Uz net-snmp paket se automatski instaliraju i Perl skripte koje omogućuju osnovna podešavanja SNMP agenta. Tri skripte koje omogućuju konfigurasanje SNMP agenta se zovu snmpconf, snmpusm i net-snmp-conf. Prva skripta omogućuje interaktivnu konfiguraciju osnovnih funkcija SNMP agenta dok se druga i treća skripta mogu koristiti za kreiranje SNMP v3 korisnika.

Prednost konfigurisanja pomoću perl skripti je što se posle restarta servisa osetljivi parametri čuvaju u enkriptovanom obliku. Ovo je preporučen princip konfigurisanja snmp agenta.

Podešavanja SNMP agenta su moguća na dva načina. Manuelnim editovanjem konfiguracionih fajlova snmpd.conf i snmptrapd.conf (kao u glavi 6.2.2.2) ili pomoću Perl skripti. Sve detaljne informacije o net-snmp paketu se mogu naći na http://net-snmp.sourceforge.net sajtu.

7 Čuvanje sistemskih logova (syslog)

7.1 SysLog protokol

SysLog protokol je razvijen kao mehanizam za sakupljanje informacija o promenama i događajima u Unix operativnim sistemima i jedna od veoma korisnih osobina mu je bila mogućnost slanja tih poruka preko mreže. Time se omogućilo prikupljanje poruka na centralnom serveru, a samim tim i lakše i brže otkrivanje i rešavanje problema. SysLog koristi UDP protokol (port 514) na transportnom sloju a na aplikativnom sloju ne postoji mehanizam koji bi obezbedio informaciju o tome da li je poruka ispravno preneta do odredišta, tako da je svrstan u klasu nesigurnih protokola. I pored ovih mana SysLog predstavlja jedan od često korišćenih protokola za sakupljanje informacija o stanju sistema.

Format poruka nosi sledeće informacije koje opisuju stanje sistema.

- Facility - Identifikuje objekat koji je generisao poruku. To može biti operativni sistem , proces ili neka aplikacija. Facility se predstavlja celobrojnom vrednošću i vrednosti od 0 do 15 su rezervisane za Unix operaivne sisteme dok su vrednosti od 16 do 23 tradicionalno predviđene za mrežne uređaje (rutere, svičeve…).

  U tabeli 7.1.1 je dat prikaz *Facility* vrednosti.

Integer	Facility
0	Kernel messages
1	User-level messages
2	Mail system
3	System daemons
4	Security/authorization messages
5	Messages generated internally by SysLogd
6	Line printer subsystem
7	Network news subsystem
8	UUCP subsystem
9	Clock daemon
10	Security/authorization messages
11	FTP daemon
12	NTP subsystem
13	Log audit

14	Log alert
15	Clock daemon
16	Local use 0 (local0)
17	Local use 1 (local1)
18	Local use 2 (local2)
19	Local use 3 (local3)
20	Local use 4 (local4)
21	Local use 5 (local5)
22	Local use 6 (local6)
23	Local use 7 (local7)

Tabela 7.1.1 – Facility vrednosti

- Severity - Može uzimati jednu od osam celbrojnih vrednosti i one opisuju trenutnu težinu problema. Moguće vrednosti su date u tabeli 7.1.2.:

Integer	Severity
0	Emergency: System is unusable.
1	Alert: Action must be taken immediately.
2	Critical: Critical conditions.
3	Error: Error conditions.
4	Warning: Warning conditions.
5	Notice: Normal but significant condition.
6	Informational: Informational messages.
7	Debug: Debug-level messages.

Tabela 7.1.2 – Severity vrednosti

- Hostname – Sadrži IP adresu uređaja koji šalje SysLog podatke i to obično IP adresu interfejsa sa koga se poruke šalju.
- Timestamp – Informacija o vremenu kada je SysLog poruka generisana. Preporučuje se da se koristi NTP protokol kako bi postojala ispravna vremenska sinhronizacija na uređajima. Veoma je bitno da postoji tačan vremenski redosled između svih SysLog poruka.
- Message – Sadrži SysLog poruku koju je generisao uređaj kao i još neke dodatne informacije o procesu koji je generisao poruku.

7.2 Lokacija syslog servera

Česta je situacija da se aplikacija koja sakuplja syslog instalira na serveru koji prikuplja SNMP podatke. To je jednostavno i prihvatljivo rešenje za sisteme ako server ima dobre performanse i može da izdrži istovremenu obradu SNMP i SysLog podataka. Kritična tačka je rad baze u kojoj se obično čuvaju te poruke. Ogroman broj generisanih syslog poruka će dovesti do čestog upisa u bazu a samim tim i čest upis na hard disku. Tako da se ispravnim izborom hardwer-ske konfiguracije može izvršiti razdvajanje baza na razlicite hard diskove i dobijanje na performansama. Drugo rešenje, u slučaju velikog exporta SysLog poruka, je da se odvoji poseban server samo za SysLog aplikaciju.

Za poziciju SysLog servera u mreži važe iste preporuke koje su definisane za NMS server.

7.3 Instalacija

Pre pokretanja SysLog servisa u mreži veoma je bitno ispravno pokrenuti vremensku sinhronizaciju na mrežnim uređajima i na samom SysLog serveru. Ovo je bitno uraditi da bi poruke bile sačuvane u tačnom vremenskom redosledu u bazi SysLog kolektora. Preporučeno je da se eksportuju sve SysLog poruke a da se filtriranjem izdvajaju najbitnije, eventualno podesiti da se eksportuju SysLog poruke koje se vezane samo za pojedine bitne funkcije uređaja ili bitnih servisa. Pokretanje SysLog agenta na pojedinim uređajima je prikazano u daljem tekstu.

7.3.1 Mrežni uređaji

Pokretanje SysLog agenta na ruterima i svičevima je objašnjeno na Cisco uređajima.

SysLog servis se pokreće pomoću sledećih komandi.

```
1. ABC(config)#logging on

2. ABC(config)#logging host 10.10.5.1

3. ABC(config)#logging trap informational

4. ABC(config)#logging source-interface Loopback0

5. ABC(config)#logging buffered 100000

6. ABC(config)#logging buffered debug

7. ABC(config)#logging monitor informational

8. ABC(config)#no logging console
```

Pomoću prve komande se pokreće logovanje podataka.
Druga komanda definiše IP adresu SysLog servera (kolektora) na koji će se vršiti eksport podataka.

Treća komanda definiše do kog nivoa kriticnosti će se poruke eksportovati na server. Informational predstavlja level 6 što znači da će se skupljati sve poruke od kritičnosti 0 do kritičnosti 5.

Četvrta komanda definiše source adresu koja će se javljati u loggovima i preporučeno je postaviti loopback adresu pošto je ona uvek aktivna. U slučaju da je SysLog server nedostupan ili da želimo direktno na uređaju da očitamo poruke preporučuje se da se odvojiti sistemska memorija u kojoj će se čuvati ove poruke.

Peta komanda definiše veličinu bafera u bajtima.

Šesta komanda omogućuje logovanje debug komandi.

Sedma komanda definiše nivo kritičnosti za terminalne linije dok se u poslednjoj komandi isključuje slanje logova na konzolnu liniju.

7.3.2 Serveri

7.3.2.1 *Windows*

Windows operatini sistemi nemaju instaliranog SysLog agenta već se oslanjaju na svog agenta koji se zove Event Logger. U slučaju da želimo da skupljamo SysLog podatke, koje generiše server sa Windows platformom, potrebno je da instaliramo posebnog SysLog agenta koji će prevoditi poruke koje je generisao Event Logger u SysLog format i slati takve poruke na udaljeni SysLog server. Dve besplatne verzije ovakvih agenata se mogu preuzeti sa sledećeg sajta https://engineering.purdue.edu/ECN/Resources/Documents/UNIX/evtsys/ i http://ntsyslog.sourceforge.net/.

7.3.2.2 *LINUX*

Prilikom instalacije Linux OS automatski se instalira i SysLog agent. Agent je prekonfigurisan tako da sve poruke koje generiše sistem on sakuplja u fajlove koji se nalaze u /var/log/ direktorijumu. U slučaju da želimo da podesimo Facility i Severity parametre pojedinih delova sistema, kao i lokaciju gde će poruke biti sačuvane (lokalni fajl ili udaljeni server), potrebno je editovati i konfiguristai fajl /etc/syslog.conf.

Primer fajla /etc/syslog.conf je dat u daljem tekstu:

```
*.info;mail.none;authpriv.none;cron.none /var/log/messages

authpriv.* /var/log/secure

mail.* -/var/log/maillog

cron.* /var/log/cron

*.emerg *

local7.* /var/log/boot.log
```

Iz prve komande se vidi da će se sve poruke čiji je Severity veći ili jednak vrednosti info (informational), osim poruka čiji je Facility mail, authpriv ili cron, biti eksportovane u folder /var/log/messages.
Druga komanda eksportuje sve poruke čiji je Facility jednak authpriv i one će se eksportovati u folder /var/log/secure.

Treća komande eksportuje poruke čiji je Facility jednak cron a Severity može uzimati sve moguće vrednosti i poruke se eksportuju u folder -/var/log/maillog.

Četvrta komanda eksportuje sve poruke čiji je Severity jednak Emergency i to na konzolu svih ulogovanih korisnika.

Peta komanda eksportuje sve poruke čiji je Facility jednak local7 u folder /var/log/boot.log.

U slučaju da želimo da eksportujemo poruke na udaljeni centralizovani SysLog server (192.168.1.1) u konfiguracioni fajl /etc/syslog.conf potrebno je dodati sledeću komandu:

```
*.*   @192.168.1.1
```

Pomoću ove komande se eksportuju sve poruke na udaljeni SySlog kolektor.
Na kraju je potrebno restartovati SysLog agenta pomoću sledeće komande:

```
service syslog restart
```

U slučaju da želimo da sakupljamo SysLog poruke neke aplikacije koja radi na Linux serveru potrebno je podesiti aplikaciju tako da eksportuje svoje logove na bilo koji lokalni Facility, a u syslog.conf fajlu podesiti opciju tako da SysLog agent eksportuje taj lokalni Facility na udaljeni SysLog server.

Preporučuje se istovremeno čuvanje logova i u fajlovima, tako da u slučaju ako je centralni SysLog server nedostupan, administrator može imati uvid u promene na serveru koje je SysLog registrovao.

U slučaju da na serveru postoji pokrenut proces koji generiše dosta poruka fajlovi će se dosta brzo popunjavati i zauzimati memoriju. U tom slučaju je potrebno pokrenuti logrotate opciju koja čuva fajlove određeni vremenski period a onda ih briše.

Ove komande se zadaju u konfiguracionom fajlu /etc/logrotate.conf. Definiše se vremenski period, kompresija, privilegije, i veličina fajlova.

Na Linux platformama se danas često koristi novija verzija SysLoga pod nazivom *rsyslog*. Ova verzija SysLoga je poboljšana u odnosu na standardni syslog ali se ne nalazi kao standardni paket u svim distribucijama Linuxa.

Standardni SysLog agent se takođe može konfigurisati tako da prima poruke od drugih uređaja i ponaša se kao kolektor SysLog poruka. Jedan od dostupnih kolektora SysLog poruka koji radi na Linux operativnim sistemima se može skinuti sa sledećeg sajta http://code.google.com/p/php-syslog-ng/downloads/list.

8 Protokol za analizu saobraćaja

U današnjim mrežama je veoma bitno vršiti analizu/inspekciju saobraćaja, ne samo do L2 nivoa (SNMP - Broj prenetih bajtova/paketa na interfejsu uređaja) već i na L3 i L4 nivou. Na taj način se stiče uvid u prirodu saobraćaja kao i servise koji se najviše koriste (opterećuju mrežu), a i pruža informacija o količini prenetog saobraćaja.

8.1 NetFlow protokol

Primer protokola koji se danas najčešće koristi za prikupljanje statistike je Netflow protokol koji je razvila Cisco kompanija. Danas se u praksi najčešće sreću dve verzije Netflow protokola, verzija 5 i verzija 9. Za razliku od verzije 5 verzija 9 nudi fleksibilni format poruka kao i podršku za MPLS i IPV6. Kod ostalih proizvođača se takođe može naći ovaj protokol samo pod drugim nazivom (Juniper-Jflow, Huawei-NetStream…). Sve ove varijante NetFlow protokola su međusobno kompatibilne. Na slici 8.1 je dat format NetFlow V5 poruke.

<table>
<tr><td colspan="4">source IP address</td></tr>
<tr><td colspan="4">destination IP address</td></tr>
<tr><td colspan="4">next hop IP address</td></tr>
<tr><td colspan="2">input interface index</td><td colspan="2">output interface index</td></tr>
<tr><td colspan="4">packets</td></tr>
<tr><td colspan="4">bytes</td></tr>
<tr><td colspan="4">start time of flow</td></tr>
<tr><td colspan="4">end time of flow</td></tr>
<tr><td colspan="2">source port</td><td colspan="2">destination port</td></tr>
<tr><td>pad</td><td>TCP flags</td><td>IP protocol</td><td>TOS</td></tr>
<tr><td colspan="2">source AS</td><td colspan="2">destination AS</td></tr>
<tr><td>src netmask length</td><td>dst netmask length</td><td colspan="2">padding</td></tr>
</table>

Slika 8.1 - Primer NetFlow V5 formata poruke

Usled potrebe za univerzalnim standrardom, od strane IETF organizacije definisan je IPFIX protokol kao univerzalni protokol za eksport prikupljene statistike saobraćaja.

8.2 Princip rada sistema

Kada se na uređaju pokrene NetFlow protokol, počinje da se prikuplja statistika za sav saobraćaj koji prolazi kroz uređaj. Statistika se zatim periodično eksportuje ka serveru (kolektoru) gde je pokrenuta aplikacija koja prima i vrši obradu tih podataka prema zadatim kriterijumima. Kao rezultat analize se obično prikazuju grafici i tabele sa rezultatima i iz njih se lako mogu uvideti problemi koji su se javili. Kod nekih aplikacija postoji mogućnost automatskog detektovanja problema (napada) u mreži.

Rezultati ovakve analize nam pružaju sledeće informacije:

- Informacije o ukupnom prenetom saobraćaju izmedu pojedinih subneta. (Bytes, Packets, Flows)
- Informacije o ukupnom prenetom In/Out saobraćaju na pojedinim interfejsima eksportera.
- Informacije o ukupnom prenetom saobraćaju na nivou protokola, servisa, hosta.
- Informacije o hostovima kojima se pristupalo iz spoljašne mreže.
- Detekcija odbačenog saobraćaja (Saobraćaj koji su odbacile ACL, Loše rutiranje…..).
- Predikciju ponašanja saobraćaja u budućnosti.

Na ovaj način se mogu detektovati:

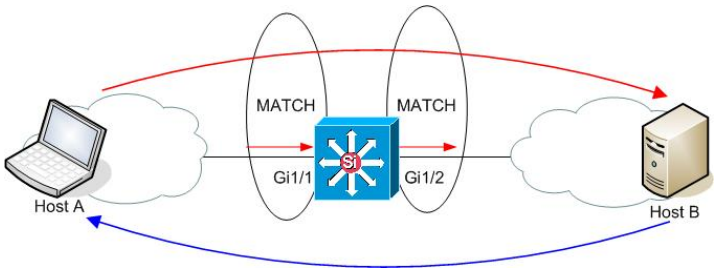
- Pojava Virusa u mreži. (Velika količina saobraćaja se generiše u OUT smeru, ili ka DNS ili MAIL serverima)
- Pojava DoS napada.
- Zloupotreba protoka. (youtube, facebook, torrent….)
- Pristup zabranjenim sajtovima.
- Pokušaji napada/pristupa zaštićenim mrežnim uređajima.
- Pronalazak otvorenih portova u mreži.
- “Top Talker” korisnici.

8.3 Lokacija kolektora u mreži

Lokacija kolektora koji prikuplja NetFlow statistiku zavisi od same arhitekture mreže. Količina NetFlow podataka koju mrežni uređaji eksportuju direktno zavisi od količine saobraćaja koja prolazi kroz taj uređaj (eksporter). Empirijski se pokazuje da procenat NetFlow saobraćaja ne prelazi 1% od ukupnog saobraćaja u mreži, tako da ne postoji problem “udaljenosti” servera (kolektora) od mrežnog uređaja koji eksportuje podatke (eksportera). Bitniji parametri su dostupnost i sigurnost servera. Fizička lokacija servera se obično vezuje za centralno čvorište zato što većina glavnog sobraćaja prolazi kroz njega. Preporučuje se postavljanje servera u odvojeni Vlan (Menadžment Vlan) i postavljanje zaštite u vidu firewall-a na server. U slučaju otkaza pojedinih mrežnih uređaja bitno je da NetFlow server bude dostupan za prikupljanje i analizu saobraćaja.

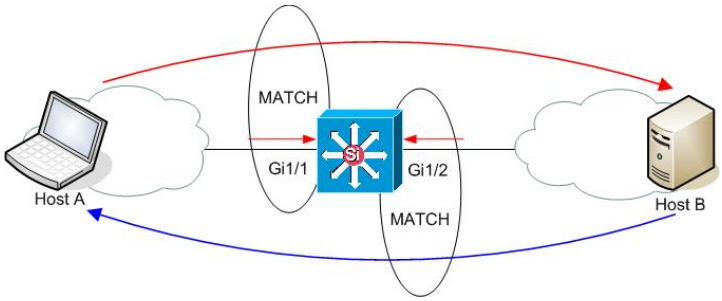
8.4 Konfigurisanje NetFlow eksportera

Konfigurisanje eksporta NetFlow statistike na uređajima zavisi od karakteristika samih uređaja ali i od arhitekture mreže. Na slici 8.2 je dat primer nepravilnog konfigurisanja NetFlow eksporta.



Slika 8.2 - Nepravilno konfigurisan eksport NetFlow statistike

Na slici se vidi da je na interfejsima Gi1/1 i Gi1/2 konfigurisano prikupljanje Netflow statistike i to na Gi1/1 interfejsu u IN smeru a na Gi1/2 interfejsu u OUT smeru. Sa slike se vidi da će jedan flow, koji prolazi od tačke A do tačke B, biti dva puta obrađen i eksportovan ka NetFlow kolektoru. U drugom slučaju komunikacija od tačke B do tačke A neće biti obuhvaćena statistikom. Usled toga će se dobiti pogrešna informacija o ovom saobraćaju (dupliraće se vrednosti i to samo u jednom smeru). Obično na uređajima postoji mogućnost eksporta NetFlow statistike koju je moguće podešavati na nivou interfejsa, i to u jednom od dva smera, ulaznom (in/ingress) smeru ili izlaznom (out/egress) smeru. Neki uređaji imaju mogućnost eksporta i u ulaznom i u izlaznom smeru istovremeno. Na slici 2.2 je dat prikaz ispravno konfigurisanog eksporta na centralnom uređaju. Na interfejsima Gi1/1 i Gi1/2 je konfigurisan netflow eksport samo u IN smeru.



Slika 8.3 - Ispravno podešen NetFlow eksport

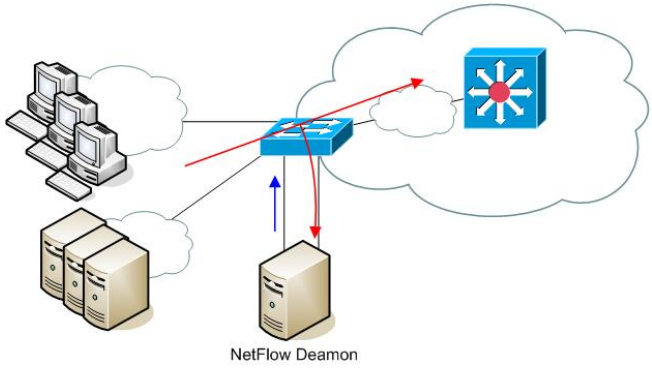
Sada će se eksportovati informacija o saobraćaju u smeru od tečke A do tačke B (Eksport sa Gi1/1 interfejsa koji se vrši za saobraćaj u IN smeru) i eksportovaće se informacija od hosta B do hosta A (Eksport sa Gi1/2 interfejsa koji se vrši za saobraćaj u IN smeru). U ovom slučaju nema dupliranja eksportovane statistike. Sa ove slike se vidi da je moguće pokrenuti NetFlow eksport na centralnom uređaju i na taj način pokriti celu mrežu. Sav saobraćaj koji prođe kroz centralni ruter će biti eksportovan ka NetFlow kolektoru. Jedini saobraćaj koji se neće detektovati je onaj koji ne prolazi kroz centralni ruter. Na slici 2.3 je dat primer situacije kada se statistika o jedom delu saobraćaja ne eksportuje.

8.5 Indirektna rešenja prikupljanje NetFlow statistike

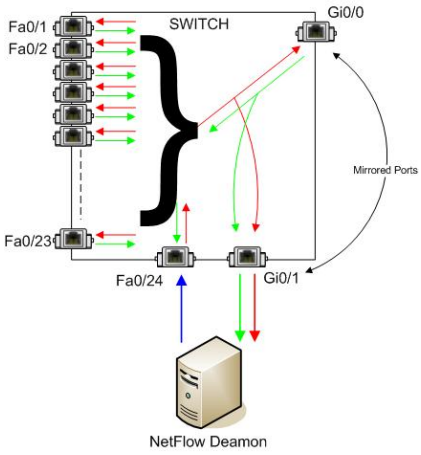
Podrška za NetFlow protokol je obično implementirana u ruterske platforme. Većina svičeva ne podržava netflow protokol, osim pojedinih L3 svičeva (cisco6500, cisco4500...).

U slučaju kada se javlja potreba za analizom saobraćaja, a sami mrežni uređaji ne podržavaju NetFlow protokol, moguće je na indirektan način sakupiti te informacije.

Na slici 8.4 je prikazana ovakva situacija.

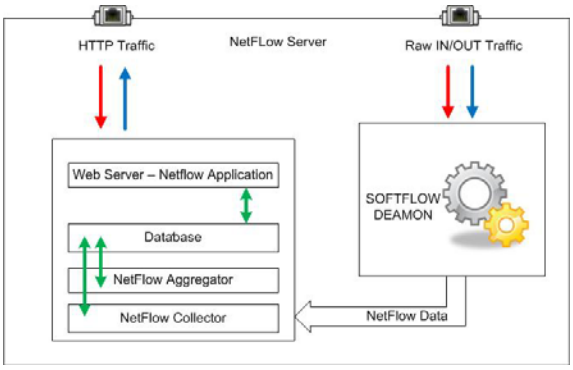


Slika 8.4 - Preusmeravanje saobraćaja ka NetFlow-deamon serveru

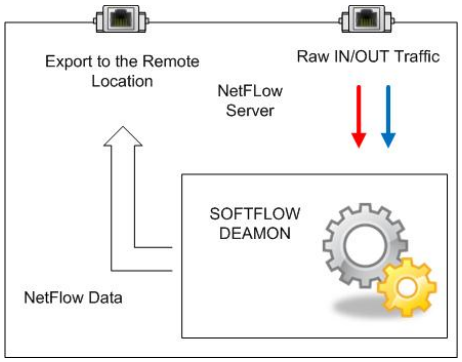


Slika 8.5 - Detaljniji prikaz postavljanja servera i povezivanja (Port Mirroring) portova

Na slikama 8.4 i 8.5 se vidi da je izvršeno preusmeravanje saobraćaja (port mirroring) ka serveru gde je pokrenut NetFlow deamon. Kada se pokrene port mirroring na sviču, interfejs ka kome se sav saobraćaj prosleđuje postaje neupotrebljiv za normalnu komunikaciju između uređaja. On samo prosleduje sav saobraćaj (IN/OUT) sa interfejsa sa kim je urađen port mirroring. Problem je kako eksportovati statistiku ako je interfejs na koji je povezan server sa NetFlow-demonom neupotrebljiv za normalnu komunikaciju. Rešenje je dodavanje još jedne mrežne kartice na server i njeno povezivanje na svič. Na slici 8.5 je plavom strelicom prikazan eksport NetFlow statistike sa druge mrežne kartice sa servera. Ovakvom konfiguracijom je omogućeno da se vrši eksport NetFlow statistike i sa L2 uređaja. Mana je dodatno zauzimanje portova na sviču i potreba za dodatnim serverom. Jedan port na sviču se koristi za primanje kopiranog (mirrored) IN/OUT saobraćaja a drugi za slanje NetFlow statistike. Sada se na serveru može pokrenuti aplikacija koja vrši netflow analizu prikupljenog saobraćaja. Jedan od alata za kreiranje Netflow statistike, IN/OUT saobraćaja na serveru, je ***softflow*** aplikacija. Ona ima mogućnost da eksportuje statistiku lokalno (127.0.0.1) ka kolektoru na samom serveru ili ka kolektoru na udaljenom serveru. Na slikama 8.6 i 8.7 su prikazani primeri kada se Netflow statistika eksportuje lokalno i kada se eksportuje na udaljenu lokaciju gde se nalazi NetFlow kolektor.



Slika 8.6 – Primer kada se NetFlow statistika eksportuje NetFlow kolektoru lokalno



Slika 8.7 – Primer kada se Netflow statistika eksportuje na udaljeni server gde se nalazi NetFlow kolektor

Na ovaj način je moguće izvršiti prikupljanje NetFlow statistike i u situacijama kada uređeaji ne podržavaju NetFlow protokol.

Reference

[1] http://www.net-snmp.org/

[2] http://www.mindrot.org/projects/softflowd/

[3] http://www.cisco.com/en/US/docs/ios/solutions_docs/netflow/nfwhite.html

[4] RFC-1901-1908, SNMP v2c

[5] RFC-3411-3418, SNMP v3

[6] Mauro D., Schmidt K.(July 2001), Essential SNMP.

[7] CentOS SNMP and Syslog manuals

Rečnik

ACL	Access List
AES	Advanced Encryption Standard
CLI	Command Line Interface
CPU	Central Processing Unit
DES	Data Encryption Standard
DNS	Domain Name System
DoS	Denial of Service
FTP	File Transfer Protocol
HMAC-MD5	Hashed Message Authentication Code, Message Digest 5
HMAC-SHA	Hashed Message Authentication Code, Secure Hash Algorithm
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
IPFIX	Internet Protocol Flow Infromation Export
IPv6	Internet Protocol version 6
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NETFLOW	Cisco Proprietary Protocol
NMS	Network Management System
NTP	Network Time Protocol
OID	Object Identifier
OOBM	Out of Band Management
RCP	Remote Copy Protocol
RDP	Remote Desktop Protocol
RFB	Remote Frame Buffering
SCP	Secure Copy
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
SYSLOG	System Logger
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network

VNC	Virtual Network Computing
VPN	Virtual Private Network