

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE
BEOGRAD

MASTER STUDIJE

STUDIJSKI PROGRAM:
SAVREMENE INFORMACIONE TEHNOLOGIJE

MASTER RAD

KRIPTOGRAFSKI ASPEKTI ZAŠTITE MREŽE ZA UPRAVLJANJE TELEKOMUNIKACIONIM SISTEMIMA

MENTOR:
Prof. dr Mladen Veinović

STUDENT:
Branislav Veljković
Br. indeksa:
410162/2010

BEOGRAD, 2015. GODINE

SAŽETAK

Razvoj telekomunikacionih mreža i njihova složenost su svakim danom sve izraženiji. Mreže za upravljanje telekomunikacionim sistemima predstavljaju jedan od uslova za uspešnu upotrebu i funkcionisanje savremenih telekomunikacionih sistema. Podaci koje se prenose mrežama za upravljanje su izuzetno osetljivi na napade od strane neovlašćenih lica. Sistem za zaštitu mreže za upravljanje mora da obezbedi zaštitu protoka informacija kroz mrežu za upravljanje na svim njenim nivoima.
U ovom radu je razmatran koncept centralizovanog nadzora i upravljanja heterogenim telekomunikacionim mrežama kroz uvođenje mreže za upravljanje. Razmatran je pojam kriptografije i izvršena je analiza simetričnih, asimetričnih i hibridnih kriptoloških algoritama. Izvršeno je razmatranje savremenih kriptografskih protokola sa posebnim osvrtom na IPSec – Internet Security Protocol. Izvršena je analiza procesa upravljanja kriptografskim ključevima. Izvršen je osvrt na procese koje treba realizovati prilikom uvođenja sistema zaštite mreže za upravljanje telekomunikacionim sistemima u rad.
Cilj ovog rada je sticanje predstave o značaju zaštite mreže za upravljanje telekomunikacionim sistemom i osnovnim principima organizovanja i uvođenja sistema za zaštitu u operativnu upotrebu.

Ključne reči: mreža za upravljanje, kriptografija, kriptografski sistem, algoritam, ključ, IPSec.

ABSTRACT

The development of telecommunications networks and their complexity are growing every day. Network management system of telecommunications networks represent one of the main conditions for the successful use and operational functionality of modern telecommunication systems. The data to be transmitted by the network management system are highly sensitive to attacks by unauthorized persons. Cryptographic protection system of the network management must ensure the protection of information flow through the network management system.at all its levels.
This study examined the concept of centralized control and management of heterogeneous telecommunication networks through the introduction of network management. It examined the concept of cryptography and analyzed the symmetric, asymmetric and hybrid cryptographic algorithms. This study examined modern cryptographic protocols with special reference to the IPSec - Internet Protocol Security. This study analyzed the process of managing cryptographic keys.This study conducted a review of the processes to be implemented when introducing cryptographic protection system of network management system of telecommunications networks in operational use.
The aim of this research is to get the show on the importance of network management system, telecommunications and basic principles of organization and introduction of a system for cryptographic protection in operational use.

Keywords: network management system, cryptography, cryptographic system, algorithm, key, IPSec

SPISAK SLIKA

Slika 2.1. Osnovni model telekomunikacionog sistema ..... - 10 -
Slika 2.2. OSI referentni model ..... - 14 -
Slika 2.3. OSI i TCP/IP referentni model ..... - 16 -
Slika 3.1. Odnos TMN-a i telekomunikacione mreže ..... - 18 -
Slika 3.2. Funkcionalni blokovi TMN-a ..... - 19 -
Slika 3.3. Primer upotrebe refrentnih tačaka između funkcionalnih blokova TMN - 20 -
Slika 3.4. Primer fizičke arhitekture TMN ..... - 22 -
Slika 3.5. Objekat upravljanja ..... - 23 -
Slika 3.6. Prikaz odnosa između menadžera, agenata i objekata upravljanja ..... - 23 -
Slika 3.7. Hijerarhijska upravljačka piramida ..... - 24 -
Slika 4.1. SNMP operacionalni model ..... - 30 -
Slika 4.2. Sastavni činioci SNMP arhitekture ..... - 31 -
Slika 4.3. Management Information Base (MIB) ..... - 32 -
Slika 4.4. Primer MIB strukture stabla ..... - 33 -
Slika 4.5. Struktura RMON MIB stabla ..... - 35 -
Slika 4.6. Odnos RMON1 i RMON 2 i OSI modela ..... - 36 -
Slika 5.1. Osnovni model CMIP/CMIS mreže ..... - 38 -
Slika 5.2. Format SNMPv1 paketa ..... - 40 -
Slika 5.3. Format SNMPv2 paketa ..... - 41 -
Slika 5.4. Format SNMPv3 paketa ..... - 42 -
Slika 6.1. Struktura umbrella sistema ..... - 48 -
Slika 6.2. Struktura TIS-a ..... - 49 -
Slika 7.1. Primer Cezarove šifre ..... - 53 -
Slika 7.2. Nemački uređaj za šifrovanje Enigma ..... - 54 -
Slika 7.3. Šenonov model tajnog komuniciranja ..... - 55 -
Slika 8.1. Tipovi zaštite komunikacija ..... - 57 -
Slika 8.2. Model simetričnog kriptografskog algoritma ..... - 59 -
Slika 8.3. Algoritam DES ..... - 60 -
Slika 8.4 Operacije u jednoj rundi DES ..... - 61 -
Slika 8.5 AES operacija ByteSub ..... - 63 -
Slika 8.6 AES operacija ShiftRows ..... - 63 -
Slika 8.7 AES operacija MixColumns ..... - 63 -
Slika 8.8 AES operacija AddRoundKey ..... - 64 -
Slika 8.9 Model asimetričnog kriptografskog algoritma ..... - 65 -
Slika 8.10 Potpisivanje elektronskog dokumenta i verifikacija ..... - 67 -
Slika 8.11 Postupak šifrovanja pomoću PGP algoritma ..... - 69 -
Slika 9.1 Prikaz paketa prilikom transportnog režima rada ..... - 72 -
Slika 9.2 Prikaz paketa prilikom tunelskog režima rada ..... - 72 -
Slika 9.3 AH zaglavlje ..... - 73 -

Slika 9.4 AH protokol u IP paket ..... - 73 -
Slika 9.5 ESP paket ..... - 74 -
Slika 9.6 ESP u IP paketu ..... - 75 -
Slika 10.1. Faze kriptološkog ključa ..... - 76 -
Slika 10.2 Proces razmene ključeva pomoću KDC-a ..... - 79 -
Slika 10.3 Proces razmene ključeva pomoću Needham-Schroeder protokola ..... - 81 -
Slika 10.4 Proces razmene ključeva pomoću Diffie-Hellman protokola ..... - 82 -
Slika 11.1 Model mreže za upravljanje telekomunikacionim sistemom ..... - 85 -
Slika 11.2 Princip povezivanja sistema SUNCE-M ..... - 86 -
Slika 11.3 Princip povezivanja sistema SUNCE+ ..... - 87 -
Slika 11.4 Model sistema za zaštitu ..... - 90 -

SADRŽAJ

UVOD ..... - 7 -

1 METODOLOGIJA NAUČNOG ISTRAŽIVANJA ..... - 8 -

1.1 Predmet istraživanja ..... - 8 -
1.2 Ciljevi i zadaci istraživanja ..... - 8 -
1.3 Istraživačke hipoteze ..... - 8 -
1.4 Metode istraživanja i tok istraživačkog procesa ..... - 9 -

2 TELEKOMUNIKACIONE MREŽE ..... - 10 -

2.1 Osnovne tehnologije telekomunikacionih mreža i sistema ..... - 10 -
2.2 Vrste telekomunikacionih mreža ..... - 12 -
2.3 Referentni modeli telekomunikacionih mreža ..... - 13 -
2.3.1 OSI (Open Systems Interconnection) referentni model ..... - 14 -
2.3.2 TCP/IP (Transmission Control Protocol/Internet Protocol) ..... - 15 -

3 MREŽE ZA UPRAVLJANJE - *TELECOMMUNICATION MANAGEMENT NETWORK* – TMN ..... - 17 -

3.1 Uvod u mreže za upravljanje - Telecommunication Management Network - TMN ..... - 18 -
3.2 Funkcionalna arhitektura ..... - 19 -
3.2.1 TMN referentne tačke ..... - 20 -
3.3 Fizička arhitektura ..... - 21 -
3.4 Informaciona arhitektura ..... - 22 -
3.5 Logička arhitektura ..... - 24 -
3.6 Upravljačke oblasti TMN-a ..... - 25 -
3.6.1 Upravljanje greškama ..... - 26 -
3.6.2 Upravljanje konfiguracijom ..... - 26 -
3.6.3 Upravljanje naplatom ..... - 27 -
3.6.4 Upravljanje performansama ..... - 27 -
3.6.5 Upravljanje bezbednošću ..... - 27 -

4 SIMPLE NETWORK MANAGEMENT PROTOCOL – SNMP ARHITEKTURA MREŽA ZA UPRAVLJANJE ..... - 28 -

4.1 Osnovni model SNMP arhitekture mreže za upraljanje ..... - 29 -
4.2 Sastavni činioci SNMP arhitekture mreže za upraljanje ..... - 30 -
4.2.1 Struktura upravljačkih informacija - Structure of Management Information (SMI) ..... - 31 -
4.2.2 Baza podataka upravljačkih informacija - Management Information Base (MIB) ..... - 31 -
4.2.3 SNMP protokol ..... - 33 -
4.2.4 Zaštita i administracija - Security and Administration ..... - 34 -
4.3 Remote Network Monitoring - RMON ..... - 35 -

5 PROTOKOLI MREŽA ZA UPRAVLJANJE ..... - 37 -
5.1 Common Management Information Protocol – CMIP ..... - 37 -
5.2 Simple Network Management Protocol – SNMP ..... - 39 -
5.2.1 SNMPv1 ..... - 39 -
5.2.2 SNMPv2 ..... - 41 -
5.2.3 SNMPv3 ..... - 42 -
5.3 Poređenje SNMP i CMIP ..... - 43 -
5.3.1 Prednosti SNMP protokola ..... - 43 -
5.3.2 Prednosti CMIP protokola ..... - 43 -
6 PROCES UVOĐENJA MREŽE ZA UPRAVLJANJE ..... - 45 -
6.1 Osnovni činioci procesa uvođenja mreže za upravljanje ..... - 46 -
6.1.1 Sagledavanje činioca koji opisuju mrežu za upravljanje ..... - 46 -
6.1.2 Izgrada projekta mreže za upravljanje ..... - 47 -
6.1.3 Realizacija izrađenog projekta mreže za upravljanje ..... - 47 -
6.1.4 Eksploatacija mreže za upravljanje ..... - 47 -
6.2 Aplikacija za mrežu za upravljanje ..... - 47 -
6.3 Sistem za upravljanje poslovnim tokovima-Workflow management system- 49 -
7 KRIPTOGRAFIJA U SAVREMENIM TELEKOMUNIKACIONIM SISTEMIMA- 51 -
7.1 Pojam i cilj kriptografije ..... - 51 -
7.2 Kratak istorijski pregled kriptografije ..... - 53 -
7.3 Osnovni pojmovi u kriptografiji ..... - 54 -
7.4 Analiza napada i pretnji ..... - 56 -
8 KRIPTOLOŠKI ALGORITMI ..... - 57 -
8.1 Simetrični kriptografski algoritmi ..... - 58 -
8.1.1 DES algoritam ..... - 59 -
8.1.2 3DES algoritam ..... - 62 -
8.1.3 AES algoritam ..... - 62 -
8.1.4 Prednosti i mane simetričnih kriptografskih algoritama ..... - 64 -
8.2 Asimetrični kriptografski algoritmi ..... - 65 -
8.2.1 Rivest-Shamir-Adleman (RSA) asimetrični kriptološki algoritam ..... - 66 -
8.2.2 Digitalni potpis ..... - 67 -
8.2.3 Prednosti i mane asimetričnih kriptoloških algoritama ..... - 68 -
8.3 Hibridni kriptografski algoritmi ..... - 68 -
9 INTERNET PROTOCOL SECURITY - IPSec ..... - 70 -
9.1 Osnovni koncept IPSec ..... - 70 -
9.2 Režimi rada IPSec-a ..... - 71 -
9.3 Zaglavlje za autentifikaciju – AH (*Authentication Header*) ..... - 72 -
9.4 Enkapsulirani šifrovani podaci – ESP (Encapsulating Security Payload) - 74 -
9.5 Zaglavlje za razmenu ključeva – IKE (Internet Key Exchange) ..... - 75 -

10 UPRAVLJANJE KRIPTOGRAFSKIM KLJUČEVIMA ..... - 76 -
10.1 Generisanje ključa ..... - 77 -
10.2 Distribucija ključeva ..... - 77 -
10.2.1 Distribucija ključeva u simetričnim kriptografskim algoritmima ..... - 78 -
10.2.2 Distribucija ključeva u asimetričnim kriptografskim sistemima ..... - 78 -
10.3 Zamena i uništenje ključeva ..... - 78 -
10.4 Sistemi za razmenu kriptografskih ključeva ..... - 79 -
10.4.1 Centar za distribuciju ključeva - KDC ..... - 79 -
10.4.2 Needham-Schroeder algoritam za razmenu ključeva ..... - 80 -
10.4.3 Diffie-Hellman algoritam za razmenu ključeva ..... - 82 -
11 IMPLEMENTACIJA KRIPTOGRAFSKOG SISTEMA U MREŽU ZA UPRAVLJANJE TELEKOMUNIKACIONIM SISTEMOM ..... - 84 -
11.1 Analiza karakteristika mreže za upravljanje ..... - 84 -
11.1.1 Model mreže za upravljanje telekomunikacionim sistemom ..... - 85 -
11.1.2 Karakteristike sistema za upravljanje ..... - 86 -
11.2 Zahtevi sistema za zaštitu ..... - 88 -
11.3 Izrada projekta sistema za zaštitu ..... - 89 -
11.3.1 Model sistema za zaštitu ..... - 89 -
11.3.2 Realizacija izrađenog projekta mreže za upravljanje ..... - 91 -
11.3.3 Eksploatacija mreže za upravljanje ..... - 92 -
ZAKLJUČAK ..... - 93 -
LITERATURA ..... - 94 -

UVOD

Savremene komunikacione mreže su usled stalnih naučnih otkrića iz oblasti telekomunikacija i informatike, praćenih brzim razvojem opreme, sve složenije u pogledu veličine i različitosti prisutne opreme. Istovremeno osnovni zahtevi savremenih komunikacionih mreža jesu visoka raspoloživost, pouzdanost i kvalitet telekomunikacionih usluga. Da bi opreater sistema bio u mogućnosti da uspesno odgovori svim zahtevima korisnika mora mu se obezbediti stalni uvid u mrežu i mogućnost brzog reagovanja prilikom prekida, kvarova i pada kvaliteta pružene usluge. Rešenje ovog problema možemo pronaći kroz uvođenje mreže za upravljanje.

Osnovni koncept mreže za upravljanje je da uspostavi interkonekciju između različitih vrsta operativnih sistema i telekomunikacione i informatičke opreme radi razmene upravljčkih informacija uz korišćenje dogovorene arhitekture sa standardizovanim interfejsima uključujući i protokole i poruke. Da bi se elementi mreže za upravljanje povezali u jedinstvenu funkcionalnu celinu potrebno je formirati zasebnu računarsku mrežu sa svim njenim LAN i WAN elementima.

Podaci koji se prenose kroz mrežu za upravljanje telekomunikacionim sistemima predstavljaju interesantan cilj za potencijalne napadače. Prodorom u mrežu za upravljanje napadaču su dostupni svi podaci o kapacitetima mreže, realizovanim servisima i podaci o korisnicima servisa. Prodor u mrežu podrazumeva da se napadaču stvara mogućnost da prisluškuje saobraćaj u mreži koji mu je interesantan, da preusmerava i onemogućuje servise u telekomunikacionoj mreži i da na kraju i onemogući rad kompletne mreže. Osetljivost mreže za upravljanje na eventualne napade od strane neovlašćenih lica zahteva da se saobraćaj, koji ide van mreže nesigurnim spojnim putevima zaštiti.

Rešenje ovog problema možemo pronaći kroz uvođenje sistema za zaštitu mreže za upravljanje telekomunikacionim sistemom. Upotreba sistema za zaštitu omogućava nesmetanu komunikaciju između elemenata mreže za upravljanje zaštićenu od zloupotrebe od lica koja nisu ovlašćena da imaju uvid i da koriste te podatke.

Sistem za zaštitu mora da bude formiran na najboljim iskustvima i savremenim teorijskim postavkama iz oblasti kriptografije. Sistem za zaštitu treba da ponudi rešenje koje je transparentno za krajnje korisnike i jednostavno primenljivo. Pored toga sistem za zaštitu ne sme da naruši performanse mreže za upravljanje i onemogući ispunjene njene namene.

1 METODOLOGIJA NAUČNOG ISTRAŽIVANJA

1.1 Predmet istraživanja

Predmet istraživanja u ovom radu jeste kripotografska zaštita mreže za upravljanje telekomunkacionim sistemom, odnosno da se prikaže neophodnost zaštite podataka u mreži za upravljanje i način na koji se može ostvariti zaštita podataka u mreži za upravljanje telekomunikacionim sistemom.

1.2 Ciljevi i zadaci istraživanja

Naučni cilj ovog rada je sistematizacija znanja o mrežama za upravljanje, kriptografiji i načinom zaštite podataka u telekomunikacionim mrežama, odnosno da se definiše opšti model sistema za zaštitu mreže za upravljanje heterogenim telekomunikacionim mrežama koji bi bio primenljiv na različite sisteme uz uvažavanje specifičnosti istih.
Na nivou naučnog opisa moguće je sagledati: osnovne pojmove i vrste mreža za upravljanje, osnovne pojmove o kriptografiji u savremenim telekomunikacionim sistemima, kriptografske algoritme, kriptografske protokole, proces upravljanja kriptografskim ključevima, kao i proces implementacije sistema za zaštitu u telekomunikacioni sistem.
Na nivou naučne klasifikacije moguće je utvrditi: karakteristike mreže za upravljanje, zahteve sistema za zaštitu i njegove karakteristike, odnosno model sistema za zaštitu mreže za upravljanje telekomunikaconim sistemima.

Društveni cilj ovog rada proizilazi iz njegove praktične primenljivosti i ogleda se u povećanju sigurnosti i bezbednosti protoka podataka i informacija kroz mrežu za upravljanje telekomunikacionim sistemom i povećanju raspoloživosti telekomunikacionog sistema i servisa i usluga koje se obezbeđuju za potrebe krajnjih korisnika.

1.3 Istraživačke hipoteze

Opšta hipoteza pri izradi ovog rada je bila:

Analizom karakteristika i načina funkcionisanja mreža za upravljanje telekomunikacionim sistemom i karakteristika i mogućnosti kritografije u savremenim telekomunikacionim sistemima moguće je doći do modela sistema za zaštitu mreže za upravljanje telekomunikacionim sistemom.

Radne hipoteze pri izradi ovog rada su bile sledeće:

- Razvojem telekomunikacionih mreža i mrežnih servisa javlja se potreba za mrežom za upravljanje telekomunikacionim sistemom
- Važnost informacija i podataka u mreži za upravljanje telekomunikacionim sistemom zahteva postojanje sistema za zaštitu informacija i podataka u mreži za upravljanje
- Analizom karakteristika i zahteva mreže za upravljanje telekomunikacionim sistemom moguće je identifikovati zahteve sistema za zaštitu
- Raznovrsnost opreme u okviru mreže za upravljanje usložnjava izbor adekvatnog sistema za zaštitu
- Ne postoji idealno rešenje za zaštitu mreže za upravljanje telekomunikacionim sistemom, već svako od njih ima prednosti ali i ograničenja i funkcionalne nedostatke

1.4 Metode istraživanja i tok istraživačkog procesa

Metode koju se koristili pri izradi ovog rada su sledeće:

- metoda deskripcije je, kao metoda opisivanja činjenica, predmeta i procesa prisutna u celom radu.
- metoda analize je, kao metoda dolaženja da zaključaka rasčlanjivanjem složenijih elemenata pojmova, sudova i zaključaka na njihove jednostavnije delove, korišćena prilikom objašnjavanja osnovnih pojmova i funkcionalnih delova: TMN i SNMP arhitekture za upravljanje mrežom, kriptografskih algoritama, kriptografskih protokola i sistema za razmenu kriptografskih ključeva.
- metoda sinteze je, kao metoda koja od jednostavnijh delova teži ka grupisanju u složeniji pojam, sud i zaključak, korišćena prilikom objašnjavanja zahteva za proces za uvođenje mreže za upravljanje sa upravljačkom aplikacijom i sistemom za upravljanje poslovnim tokovima i prilikom objašnjavanja zahteva za implementaciju kriptografskog sistema u mrežu za upravljanje telekomunikacionim sistemom.
- komparativna metoda je, kao metoda koja služi za upoređivanje sličnih činjenica, pojmova i procesa i utvrđivanja sličnosti i razlika između njih, korišćena pri objašnjavanju: arhitektura za upravljanje mrežom i protokola koji se najčešće koriste u mrežama za upravljanje, kritografskih algoritama, kritografskih protokola i sistema za razmenu kriptografskih ključeva.

2 TELEKOMUNIKACIONE MREŽE

Komunikacija predstavlja jednu od osnovnih ljudskih potreba bez koje je teško zamisliti postojanje ljudske vrste. Kroz komunikaciju ljudi izražavaju svoje misli, emocije, osećanja, namere drugim ljudima. Komunikacija nam služi i za razmenu informacija, koje mogu biti lične, društvene ili poslovne prirode. Da bi došlo do komunikacije između ljudi, koji nisu neposredno jedan pored drugog, koristimo razne oblike kominikacije: razgovor preko telefona, slanje e-maila, slanje video poruka, audio-video konferencije i slično. Da bi svi ovi oblici komunikacije bili mogući pored krajnje terminalne opreme potrebna je da postoji komunikacijska mreža.

„Elektronska komunikaciona mreža predstavlja sisteme prenosa i, tamo gde je to primenjeno, uređaje za komutaciju i usmeravanje i druge resurse, uključujući pasivne mrežne elemente, koji omogućavaju prenos pomoću žičnih, radio, optičkih ili drugih elektromagnetnih sredstava, uključujući satelitske mreže, fiksne (sa komutacijom kola i paketa, uključujući Internet) i mobilne mreže, energetske kablovske sisteme, u delu koji se koristi za prenos signala, mreže koje se koriste za distribuciji i emitovanje medijskih sadržaja, bez obzira na vrstu podataka i informacija koje se prenose.“(1)

Telekomunikaciona mreža predstavlja skup terminalne opreme i spojnih puteva u cilju ostvarivanja komunikacije između učesnika koji koriste tu terminalnu opremu, a radi prenosa informacija. Ona je namenjena da se kroz nju obavi proces slanja, propagacije i prijema analognih ili digitalnih signala preko fizičkog spojnog puta.

2.1 Osnovne tehnologije telekomunikacionih mreža i sistema

Tri neophodne tehnologije za ostvarivanje komunikacije kroz mrežu su prenos (transmision), komutacija (switching) i signalizacija (signaling).(2)

a) Prenos (transmision)

Prenos podrazumeva proces slanja, propagacije i prijema analognih ili digitalnih signala preko fizičkog spojnog puta između krajnjih tačaka sistema ili mreže. Osnovni model prenosnog sistema dat je na slici broj 2.1.



Slika 2.1. Osnovni model telekomunikacionog sistema

Predajnik je sklop koji je namenjen da izvorni signal od korisnika pretvori u predajni signal prilagođen karakteristikama koje odgovaraju spojnom spojnom putu.
Spojni put je prenosni medijum koji se koristi za prenos signala od predajnika do prijemnika.

Prenosni medijumi su podeljeni na:

- **bakarni kablovi** – koriste se uglavnom u pristupnoj ravni i namenjeni su za LAN i telefonske mreže. Uz korišćenje xDSL tehnologije (ADSL, ADSL2/2+, SDSL , SHDSL i VDSL) mogu se koristiti i za povezivanje opreme na udaljenosti do nekoliko kilometara
- **optički kablovi** – predstavljaju dominantan medij za prenos i po podatku iz 2004. godine nešto više od 80% telekomunikacionog saobraćaja u transportnoj mreži realizuje putem optičkih vlakana. Namenjeni su prenos telekomunikacionog saobraćaja velikog kapaciteta putem svetlosti. Na predajnoj strani se vrši modulacija električnog signala izvorom svetlosti i tako modulisani svetlosni signal putuje do predajne strane preko optičkog vlakana. Na predajnoj strani se vrši proces demodulacije i ponovnog dobijanja električnog iz svetlosnog signala. Dominantni standard optičkog prenosa u svetu je SDH/SONET sa već sada prisutnim prenosom od STM-256 (OC-768) što odgovara prenosu od 40GB/s. U mrežama koje nisu konekciono orjentisane i koje služe za paketski prenos u upotrebi je 10-gigabitni Ethernet, dok su potrebe dovele do 100-gigabitnog Etherneta, što je posebno značajan podatak ako se zna da su mreže nove generacije (Next Generation Network - NGN) bazirane na Internet protokolu. Razvojem uskopojasnih optičkih predajnika (narrowband optical transmitters) i optičkih filtara stekli su se uslovi za povećanje kapaciteta prenosa tehnikom multipleksiranja po talasnim dužinama - DWDM (Dense Wavelenght Division Multiplexing). DWDM tehnika omogućila je da se preko jednog optičkog vlakna prenosi od nekoliko kanala do nekoliko desetina ili stotina kanala, tako što svaki od njih koristi različitu talasnu dužinu. Time su omogućile brzine prenosa signala reda veličine 1 Tb/s. Optički kablovi se pored korišćenja u transportnoj ravni sve više koriste i u pristupnoj ravni kroz FTTx tehnologiju (Fiber to the x = H (home), B (building), C (curb)).(3)
- **radio talasi** – koji omogućavaju komunikaciju korišćenjem elektromagnetnih talasa na frekvencijama izvan spektra vidljivog ljudskom oku. Primeri ovakvih komunikacija su mobilna telefonija, satelitske veze, radio-relejne veze, digitalna televizija (DVB - Digital Video Broadcasting), bežične – wireless 802.11 a/b/g/n mreže, WiMax (Worldwide Interoperability for Microwave Access) mreže, TETRA (Terrestrial Trunked Radio) mreže. Kroz navedene primere radio komunikacija vidi se da je ovakav vid komunikacije prisutan u transportnoj i pristupnoj ravni. Prednost ovih veza je što su najekonomičnije rešenje, jer ne zahtevaju postojanje kablovske infrastrukture za njihovu realizaciju. Mana radio veza je nedostatak frekvencija u radio spektru.

Prijemnik je sklop koji je namenjen da signal koji je došao sa spojnog puta pretvori u signal koji je odgovarajući za upotrebu korisniku na prijemnoj strani.

b) Komutacija (switching)

Komutacija podrazumeva proces preusmeravanja signala kroz komutatore (switch) u mreži radi prenosa informacije od korisnika na predajnoj do korisnika na prijemnoj strani.

Postoje dve vrste prenosa podataka komutacijom:

- **prenos podataka komutacijom veze (circurit switching)** u kojoj se veza između dva korisnka odvija kanalom dodeljenim nakon uspostave veze. U sistemima sa komutacijom veze postoje tri faze: uspostava veze, razmena podataka i raskidanje veze. Za vreme trajanja komunkacije druga dva učesnika ne mogu da koriste isti kanal po kome se već odvija razmena podataka, čime se smanjuje efikasnost telekomunikacionog sistema, što predstavlja negativnu osobinu ovog načina komutacije. Pozitivnu stranu ovakog načina komutacije predstavljaju činjenice da nakon uspostave veze, a tokom razmene podataka, nema dodatnog adresiranja i celokupan propusni opseg dodeljenog kanala je dostupan za prenos podataka maksimalnom brzinom sa minimalnim kašnjenjem. Primeri mreža sa komutacijom veze su: javna telefonska mreža (PSTN – Public Switched Telephone Network), ISDN (Integrated Services Digital Network), X.21 mreže.
- **prenos podataka komutacijom paketa (packet switching)** u kojoj se prenos poruke odvija slanjem paketa između dva korisnika kroz mrežu. U sistemima sa komutacijom paketa postoje tri glavne aktivnosti: podela podataka u pakete na predajnoj strani, slanje paketa kroz mrežu nezavisno jedan od drugoga i sastavljanje orginalne poruke od dobijenih paketa na prijemnoj strani. Paketi od zavisnosti od protokola koji se koristi sadrže razne parametre (adresu pošiljoca, adresu primaoca, dužinu paketa, broj paketa na koliko je poruka podeljena, redni broj određenog paketa, prioritet i sl.). Paketi se kroz mrežu preusmeravaju preko rutera, koji predstavljaju uređaje namenjene da vrše preusmeravanje paketa kroz mrežu na najbolje moguće putanje uz korišćenje tabele rutiranja i adresa pošiljoca i primaoca iz zaglavlja paketa. Pozitivna strana ovakvog načina komutacije je da telekomunikacioni kanal po kojem se vrši slanje paketa mogu istovremeno da koriste i drugi učesnici u mreži u pauzama između poslatih paketa što znači da je efikasnost veća. Negativna strana je da je brzina prenosa manja, jer se smanjuje propusni opseg kanala usled većeg broja učesnika koji ga koriste. Kvalitet usluge je moguće povećati korišćenjem posebne vrste vrste prenosa podataka komutacijom paketa koja se naziva prenos podataka virtualnom vezom (virtual circuit). Prilikom prenosa podataka virtuelnom vezom vrši se prenos podataka kroz mrežu po tačno utvrđenoj putanji. Prenos podataka komutacijom paketa je zastupljena u sledećim tehnologijama: X.25, Frame Relay, ATM (Asynchronous Transfer Mode) , TCP/IP (Transmission Control Protocol/Internet Protocol), MPLS (Multiprotocol Label Switching).

c) Signalizacija (signaling)

Signalizacija predstavlja mehanizam koji podrazumeva razmenu signala namenjenih za uspostavu veze, održavanje veze, prenos informacija, kontrolu veze i raskidanje veze.

2.2 Vrste telekomunikacionih mreža

Podela telekomunikacionih mreža se može izvršiti na puno načina u zavisnosti od ogranizacije mreže, opreme od koje se mreža sastoji, namene zbog koje je

napravljena, tehnologija koje su primenjene u realizaciji iste i drugih parametara koji mrežu mogu da okarekterišu na osnovu svojih specifičnosti.

Prema vrsti različite opreme koja je zastupljena mreže delimo na:

- Homogene – predstavljaju mreže u kojima je pretežno zastupljena samo jedna vrsta uređaja
- Heterogene – predstavljaju mreže u kojima je zastupljeno više različitih tipova uređaje od različitih proizvođača opreme

Prema načinu interkonekcije sa drugim mrežama mreže delimo na:

- Zatvorene – koje predstavljaju zatvorene mreže koje se ne povezuju sa drugim mrežama
- Otvorene – koje predstavljaju mreže koje su otvorene za povezivanje sa drugim mrežama i koje omogućuju *outsourcing*-a servisa (poput usluga call centra, e-mail servisa i sl.) i pristupa spoljnim korisnicima

Prema nameni telekomunikacione mreže delimo na:

- Javne telekomunikacione mreže – koje predstavljaju javne mreže za pružanje telekomunikacionih uslova koje su svima dostupne na osnovu unapred udređenih uslova za korišćenje. Primer ovakve vrste mreže predstavljaju javne telefonske mreže fiksne i mobilne telefonije, Internet i sl.
- Privatne telekomunikacione mreže – koje predstvljaju mreže zatvorenog tipa dostupne samo pripadnicima organizacije koja poseduje mrežu, kao i određenom broju fizičkih i pravnih lica koja imaju posebno obodbrenje za korišćenje mreže. Primer ovakve vrste mreže predstavljaju mreže državnih institucija, kao što su vlada, vojska i policija, mreže posebnih državnih i privatnih preduzeća. Karakteristika ove vrste mreža je da se akcenat polaže na poverljivost podataka i sistem zaštite mreže.

Posebnu vrstu podele čini podela na:

- Telekomunikacione mreže sa tradicionalnim načinom prenosa informacija kao što su SDH/SONET optički i radio-relejni sistemi prenosa, javne telefonske mreže PSTN, ISDN mreže
- Računarske mreže zasnovane na prenosu podataka komutacijom paketa uz korišćenje TCP/IP protokola. Primer ovakve mreža predstavljaju Interernet i računarske mreže različitih organizacija organizovane kao LAN ili WAN mreže. Računarske mreža predstavlja skup računara povezanih u jednu celinu, bez obzira na njihovu lokaciju, uz korišćenje raznih vrsta spojnih puteva i sistema prenosa, u cilju njihove komunikacije i razmene podataka.

2.3 Referentni modeli telekomunikacionih mreža

Protokol podrazumeva skup pravila koja definišu komunikacione funkcije sa namenom da obezbede učenicima u komunikaciji da šalju, primaju i interpretiraju razmenjene informacije.
Referentni model predstavlja skicu kako komunikacija treba da se odvija. Ovaj model predstavlja sve procese potrebne za uspešnu komunikaciju i deli ih u logičke grupe pod

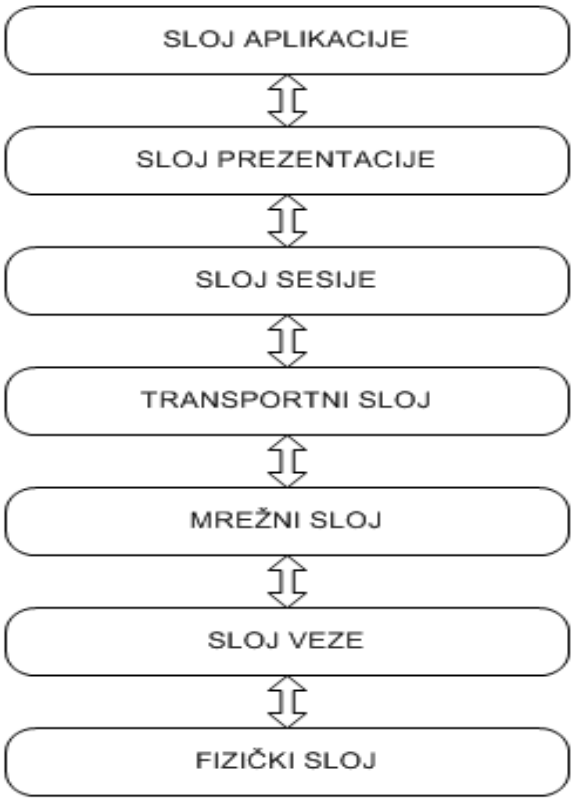
nazivom slojevi. Sloj predstavlja skup konceptualno sličnih funkcija koja obezbeđuje servis višim slojevima i dobija servise od nižih slojeva.

Postoje dva referentna modela koja su danas u upotrebi:

- OSI (Open Systems Intrconnection) referentni model
- TCP/IP (Transmission Control Protocol/Internet Protocol) referentni model

2.3.1 OSI (Open Systems Interconnection) referentni model

OSI (Open Systems Interconnection) referentni model je razvijen od stane ISO (International Standardization Organization) i objavljen je 1984. godine. OSI referentni model uspostavlja osnovni okvir za usaglašavanje standarda za međusobno povezivanje sistema. OSI model ima sedam slojeva (slika 2.2). Svaki nivo obavlja tačno definisani skup funkcija potrebnih za komunikaciju sa drugim sistemima, pri tome se oslanjajući na servise koje mu nude nivoi nižeg reda. Viši slojevi zaduženi su za aplikacije, servise i aktivnosti. Niži slojevi su zaduženi za prenos informacija. Ovakav pristup obezbjeđuje modularnost i nadogradnju.



Slika 2.2. OSI referentni model

Slojevi OSI referentnog modela su sledeći:

1) **Fizički sloj (Physical layer)**

   Fizički sloj je namenjen da binarne brojeve pretvori u signale i da predaje i prima te signale preko spojnog puta (bakani kablovi, optički kablovi, radio talasi), odnosno za prenos toka bitova između mrežnih elemenata. Standardi

fizčkog sloja definišu: električne i mehaničke karakteristike spojnog puta, mehaničke karakteristike konektora (materijal, dimenziju, pinout), pretvaranje bitova u signale i obrnuto i definisanje kontrolnih signala.

2) Sloj veze (Link layer)

Sloj veze je namenjen za ispravan prenos podataka, korišćenjem algoritama za detekciju i ispravljanje grešaka čime omogućava pravilno funkcionisanje višeg nivoa. Osnovna jedinica protokola koja se formira na ovom sloju je frejm (frame).

3) Mrežni sloj (Network layer)

Mrežni sloj je namenjen da obezbedi prenos podataka u vidu paketa preko različitih vrsta mreža izborom primarnog i sekundarnog (alternativnog) puta ili uspostavljanjem virtuelnog kola. Osnovna jedinica protokola koja se formira na ovom sloju je paket (packet). Osnovne radnje koje se odvijaju na ovom sloju su: adresiranje, enkapsulacije segmenata u pakete, rutiranje i dekapsulacija paketu u segmente.

4) Transportni sloj (Transport layer)

Transportni sloj je namenjen da obezbedi transparentan i pouzdan prenos podataka između krajnjih učesnika. Osnovna jedinica protokola koja se formira na ovom sloju je segment (segment). Transportni nivo obavlja funkciju optimizacije mrežnog servisa i pružanje odgovarajućeg kvaliteta servisa, kontrolu protoka segmentacije.

5) Sloj sesije (Session layer)

Sloj sesije je namenjen za uspostavljanje logičke veze između dva krajnja učesnika. Ovaj sloj poseduje mehanizme za kontrolu i organizaciju dijaloga između sloja prezentacije između dva krajnja korisnika, tako da dijalog bude nezavisan od prekida veze nižih nivoa.

6) Sloj prezentacije (Presentation layer)

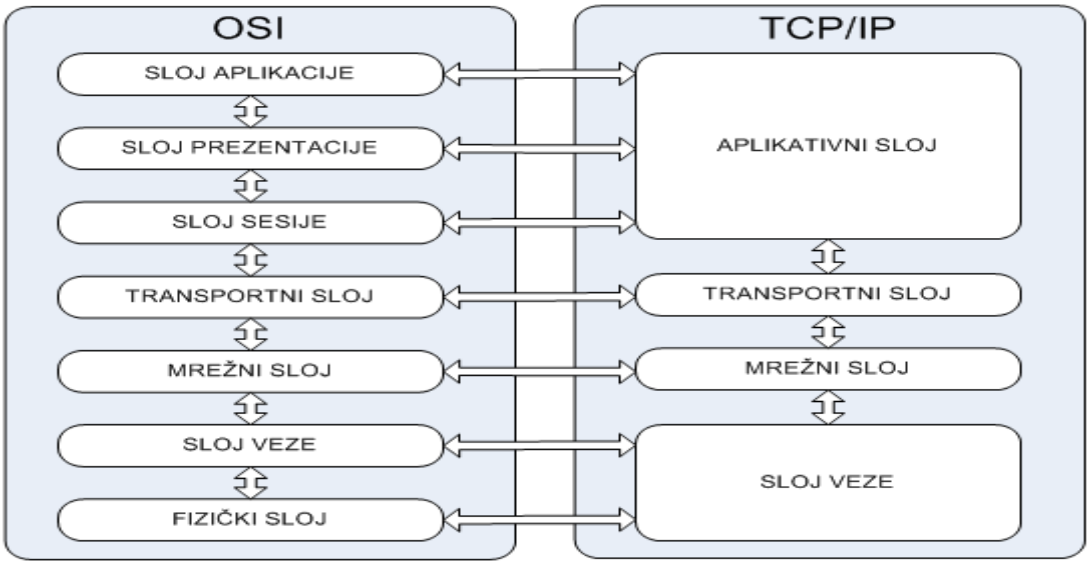
Sloj prezentacije je namenjen da formatira podatke tako da budu razumljivi za obe strane u komunikaciji.

7) Sloj aplikacije (Application layer)

Sloj aplikacije je najviši nivo OSI referentnog modela namenjen da omogući pristup mreži korisničkim programima – aplikacijama i predstavlja interfejs mreže ka korisniku.

2.3.2 TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP (Transmission Control Protocol/Internet Protocol) je IETF (Internet Engineering Task Force) referentni model, koji obuhvata skup protokola koji se koriste za povezivanje računarskih mreža (TCP i IP su samo dva protokola iz tog skupa, najpoznatiji i najčešće korišćeni iz celog skupa). Ovaj referentni model definiše kako podaci trebaju da se formatiraju, adresiraju, preusmeravaju i dostavljaju na pravo odredište. TCP/IP referentni model ima za razliku od OSI referentnog modela ima samo četiri sloja (slika 2.3.). Tri najviša sloja OSI modela sloj aplikacije, prezentacije i sesije su obuhvaćeni jednim aplikativnim slojem, dok su dva najniža sloja, fizički sloj i sloj veze obuhvaćeni jednim slojem veze.



Slika 2.3. OSI i TCP/IP referentni model

Slojevi TCP/IP referentnog modela su sledeći:

1) Sloj veze (Link layer)

Sloj veze je zadužen za razmenu paketa između dva mrežna sloja između dva različita korisnika na istom linku. Namenjen je da definiše karakteristike prenosnog medija, predstavlja interfejs između sistema i mreže i omogućava prenos frejmova korišćenjem protokola sloja veze između dva rutera. Ovaj Karakteristični protokoli sloja veze su Ethernet, PPP (Point-to-Point Protocol), ATM.

2) Mrežni sloj (Network layer)

Mrežni sloj ili Internet sloj (Internet layer) je namenjen za prenos podataka u vidu paketa između izvorišta i odredišta podataka. Ovaj sloj je ekvivalentan sloju mreže OSI referentnog modela. Dve osnovne funkcije mrežnog sloja su IP adresiranje i rutiranje paketa kroz mrežu. Karakteristični protokoli mrežnog sloja su ICMP (Internet Control Message Protocol) and IGMP (Internet Group Management Protocol).

3) Transportni sloj (Transport layer)

Transportni sloj je namenjen da obezbedi transparentni i pouzdan prenos podataka u formi segmenta između krajnjih učesnika. Ovaj sloj je ekvivalentan transportnom sloju OSI referentnog modela. Karakteristični protokoli mrežnog sloja su TCP (Transmission Control Protocol) i UDP (User Datagram Protocol).

4) Aplikativni sloj (Application layer)

Aplikativni sloj je namenjen da obezbedi komunikaciju između procesa ili aplikacija na odvojenim učesnicima. U TCP/IP referentnom modelu nema slojeva sesije i prezentacije OSI referentnog modela, tako da aplikativni sloj mora da nadomesti njihov nedostatak. Karakteristični protkoli aplikativnog sloja su: File transfer (FTP), SMTP (Simple Mail Transfer Protocol), HTTP (Hypertext Transfer Protocol).

3 MREŽE ZA UPRAVLJANJE - *TELECOMMUNICATION MANAGEMENT NETWORK* – TMN

Upravljanje mrežom – *Network and System Management (NMS)* se u zavisnosti od stanovišta gledanja definiše na razne načine. Upravljanje mrežom se definiše kao izvršenje skupa funkcija neophodnih za kontrolu, planiranje, lociranje, koordiniranje i upravljanje telekomunikacionim ili računarskim mrežama, uključujući i izvršenje funkcija kao što su mrežno planiranje, raspodela frekvencija, definisanje rutiranja saobraćaja u cilju smanjena preopterećenja mreže, distribucija kriptoloških ključeva, upravljane konfiguracijom, upravljanje greškama, upravljanje sigurnošću, upravljanje performansama i upravljanje naplatom.
Prednosti centralizovanog i automatizovanog upravljanja u odnosu na lokalno i ručno upravljanje su sledeće:

- Vreme otkrivanja problema i greške u sistemu je znatno kraće čime se omogućuje da davalac usluge pravovremeno interveniše pre nego korisnik uslugu uoči problem sa kvalitetom usluge
- Donošenje odluke, u procesu planiranja razvoja mreže i korišćenja njenih kapaciteta za postojeće i nove servise i usluge, bazirano je na preciznim pokazateljima o kapacitetima i parametrima mreže. Vreme prikupljanja podataka i donošenje odluke je znatno kraće i daje prednost u odnosu na konkurente.
- Cena održavanja sistema za centralizovano upravljanje u odnosu na cenu ručnog nadzora na svakoj lokaciji u sistemu
- Manji broj ljudi u sistemu čime se smanjuje mogućnost greške usled ljudskog faktora.
- Manji broj ljudi u sistemu prouzrokuje da je lakše pronaći, obučiti i zadržati ljudski kadar za rad u sistemu za upravljanje i održavanje mreže

Kod svih vrsta mreža za upravljanje zastupljena je paradigma o odnosu menadžer – agent (manager – agent). Agent se nalazi u svim uređajima koji su zastupljeni u mreži i ima ulogu da izveštava menadžera o problemima koje uoči u uređaju ili mreži u kojima se nalazi i da prima i izvršava komande koje dobija od menadžera. Agenti omogućavaju da menadžer zna sve o procesima koji se dešavaju u uređajima i da omoguće kontrolu i upravljanje uređajima. Menadžer se nalazi u centru za nadzor i upravljanje i predstavlja inteligenciju koja donosi odluku o procesima koje agenti moraju da izvrše. Menadžer kontroliše rad agenata u mreži, reguliše ulogu i odnose agenata u mreži i izdaje komande agentima koje omogućavaju da mreža funkcioniše bez problema.

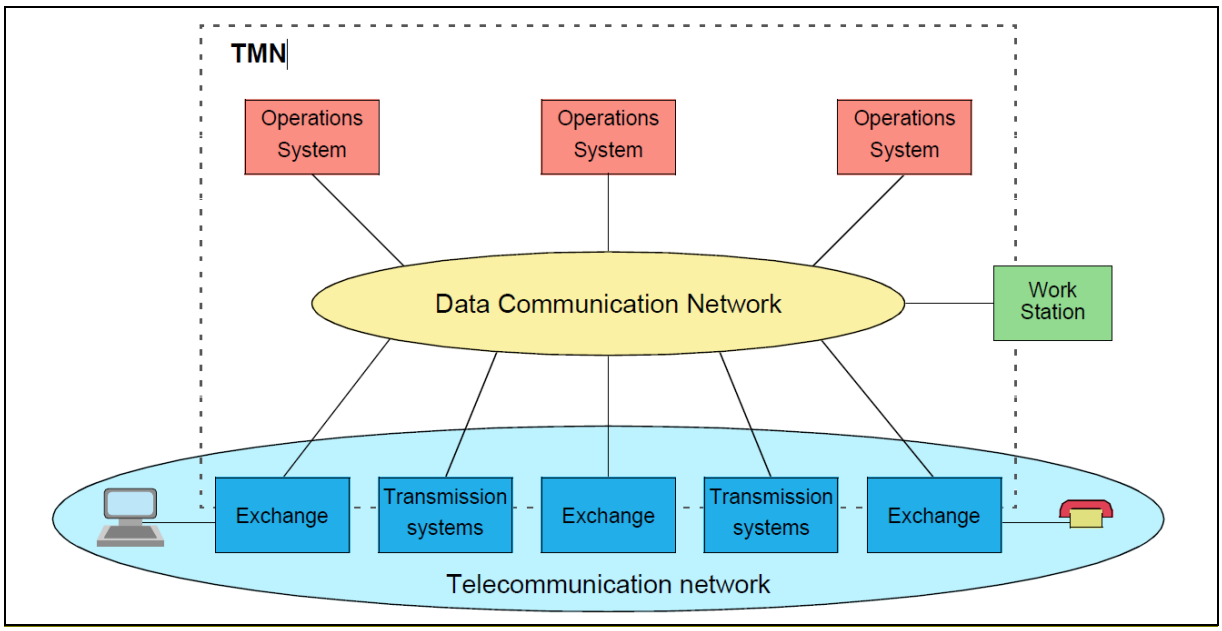
Ljudski faktor koji je pojavljuje u sistemu za upravljanje mrežom predstavlja administrator, koji ima ulogu da prati rad mreže i da preko menadžerske aplikacije izvrši promene u mreži u cilju promene parametara radi uvođenja novih servisa ili otklanja smetnji u radu.

Postoji više predstavljenih arhitektura za upravljanje mrežom od kojih su dve dominantne:

- TMN - *Telecommunication Management Network* – pretežno zastupljena u klasičnim telekomunikacionim mrežama
- SNMP – *Simple Network Management Protocol* – pretežno zastupljena i računarskim mrežama

3.1 Uvod u mreže za upravljanje - Telecommunication Management Network – TMN

TMN je predstavlja arhitekturu za upravljanje mrežom koju je razvio ITU (International Telecommunications Union) i regulisana je serijom standarda M.3000 (4). TMN je namenjen da obezbedi arhitekturu za povezivanje i razmenu informacija između opreativnih sistema i telekomunikacione opreme, u okviru raznovrsnih jednostavnih ili složenih telekomunikacionih mreža, uz korišćenje standardizovane arhitekture sa definisanim interfejsima, protokolima i porukama. TMN mora da obezbedi širok spektar funkcija za upravljanje, koje obuhvataju planiranje, instaliranje, administaciju i održavanje telekomunikacionih mreža i servisa.
TMN predstavlja mrežu za prenos podataka koja prenosi informacije neophodne za upravljanje. U logičkom smislu predstavlja odvojenu mrežu, koja sa telekomunikacionom mrežom ima zajedničke tačke kako bi mogla da je nadzire i da upravlja sa njom. Za potrebe komunikacije između elemenata mreže za upravljanje može se koristiti i mreža koja se nadzire. Primer odnosa između TMN-a i telekomunikacione mreže koja se nadzire dat je u na slici 3.1.



Slika 3.1. Odnos TMN-a i telekomunikacione mreže (5)

Svaki elemenat TMN-a je zadužen za upravljanje određenom grupom uređaja i servisa. Glavni deo TMN-a predstavlja serverska jedinica koja vrši objedinjavanje upravljačkih funkcija, obrađuje ih i prosleđuje na radnu stanicu administratora mreže.
Funkcionalnost TMN-a se ogleda u sledećem:

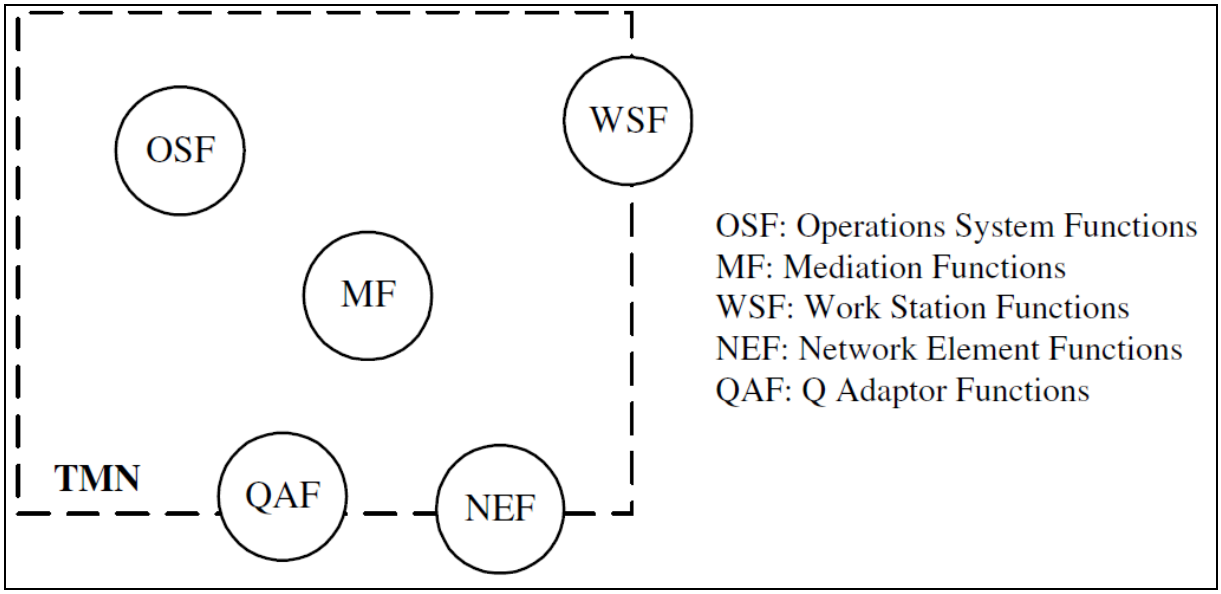
- Mogućnost da informacije iz jednog elementa TMN-a pređu u drugi preko različitih interfejsa
- Mogućnost konvertovanja informacija u različite formate
- Mogućnost prenosa informacija na različite lokacije
- Mogućnost analiza informacija
- Mogućnost različitog prezentovanja informacija
- Obezbeđenje sigurnosti i pouzdanosti informacija

U okviru ITU preporuke M.3010 (5) definisan je osnovni koncept TMN arhitekture za upravljanje mrežom i definisane su četiri oblasti koje se prilikom planiranja i projektovanja TMN-a mogu razmatrati zasebno. Te četiri oblasti TMN-a su prikazane kao:

- Funkcionalna arhitektura
- Fizička arhitektura
- Informaciona arhitektura
- Logička arhitektura

3.2 Funkcionalna arhitektura

Funkcionalna arhitektura TMN-a je predstavljena sa pet funkcionalnih blokova koji predstavljaju elemente koji se mogu naći u mreži za upravljanje. Nije neophodno da se svaki od funkcionalnih blokova nađe u mreži za upravljanje, ali je moguće da se više istih funkcionalnih blokova nađe u istoj mreži za upravljanje. Funkcionalni blokovi TMN-a su prikazani na slici 3.2.



Slika 3.2. Funkcionalni blokovi TMN-a

Način na koji su funkcionalni blokovi prikazani na slici označava da su OSF i MF funkcionalni blokovi, koji se u potpunosti nalaze u okviru TMN-a, prikazuje da su oni kompletno definisani ITU preporukama koje se odnose na TMN. Način na koji su funkcionalni blokovi QAF, NEF i WSF prikazani na obodu TMN-a označava da su samo njihovi delovi obuhvaćeni TMN-a preporukama.

Operations Systems Function (OSF) funkcionalni blok je namenjen da izvršava funkcije oprerativnog sistema u cilju nadgledanja i kontrole upravljačkih funkcija. Služi da inicira upravljačke operacije i prima obaveštenja od ostalih elemenata u mreži. Ovaj funkcionalni blok predstavlja menadžera u relaciji menadžer – agent u okviru mreže za upravljanje.

Network Element Function (NEF) funkcionalni blok predstavlja mrežni element koji se nadzire i kojim se upravlja. U relaciji menadžer – agent u okviru mreže za upravljanje predstavlja agenta. Pored elementa za nadgledanje i upravljanje NEF je i

deo telekomunikacione mreže kojom se upravlja i u tu svrhu ima zadatak da izvršava i telekomunikacione zadatke za koje je namenjen i koje nisu deo TMN-a.

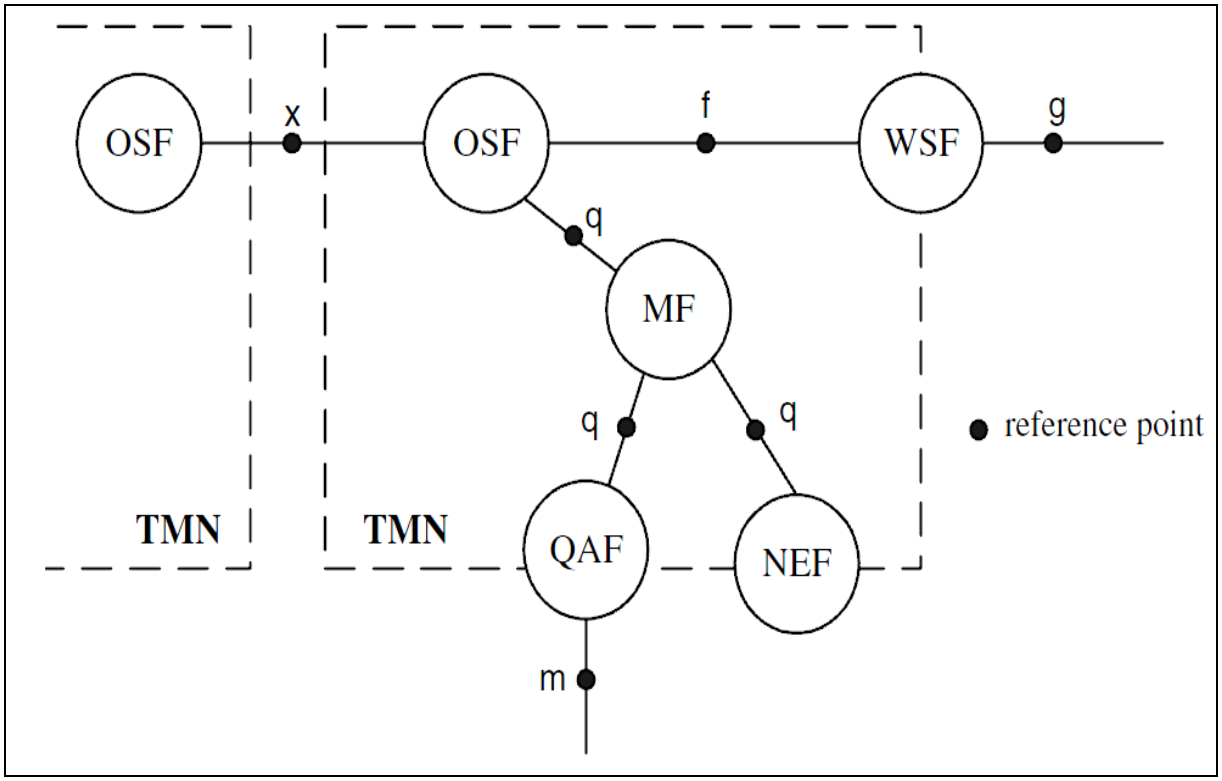
Workstation Function (WSF) funkcionalni blok predstavlja sredstvo za interpretiranje TMN informacija korisnicima upravljačkih informacija. WSF predstavlja interfejs za povezivanje sa čovekom u ulozi administratora i korisnika mreže za upravljanje. Zbog svoje uloge ovaj funkcionalni blok se u vidu radne stanice smatra delom TMN-a, dok je drugim delom sredstvo za rad administratora mreže.

Mediation Function (MF) funkcionalni blok izvršava funkcije posredovanja između OSF funkcionalnih blokova i lokalnih NEF i QAF funkcionalnih blokova. U MF-u se informacije prikupljaju, prilagođavaju, filtriraju i prosleđuju u odgovarajućoj formi ka ostalim funkcionalnim blokovima.

Q Adaptor Function (QAF) funkcionalni blok je namenjen da izvrši povezivanje elemenata TMN-a preko njihovih referentnih tačaka sa elementima koji nisu delovi TMN-a i ne podržavaju standarde TMN referentnih tačaka.

3.2.1 TMN referentne tačke

TMN referentne tačke su namenjene da definišu format i način razmene informacija na mestima dodira funkcionalnih blokova unutar TMN-a i elemenata izvan TMN-a koji su povezani sa elementima unutar TMN-a. Referentna tačka definife granice servisa između funkcionalnih blokova. Na slici 3.3 je prikazan primer upotrebe referentnih tačaka između funkcionalnih blokova TMN-a.



Slika 3.3. Primer upotrebe refrentnih tačaka između funkcionalnih blokova TMN

Prema M.3010 TMN preporukama definisane su tri klase referentnih tačaka:

- **q referentna tačka** za vezu između OSF, QAF, MF i NEF funkcionalnih blokova. Definisane su dve vrste q referentne tačke: q_x (koja služi za vezu između NEF i MF, QAF i MF i MF i MF) i q_3 (koja služi za vezu između NEF i OSF, QAF i OSF, MF i OSF i OSF i OSF).
- **f referentna tačka** za povezivanje MF i OSF sa WFS
- **x referentna tačka** za vezu između OSF dva TMN-a ili za povezivanje OSF TMN-a sa po funkciji ekvilalentnim OSF druge mreže.

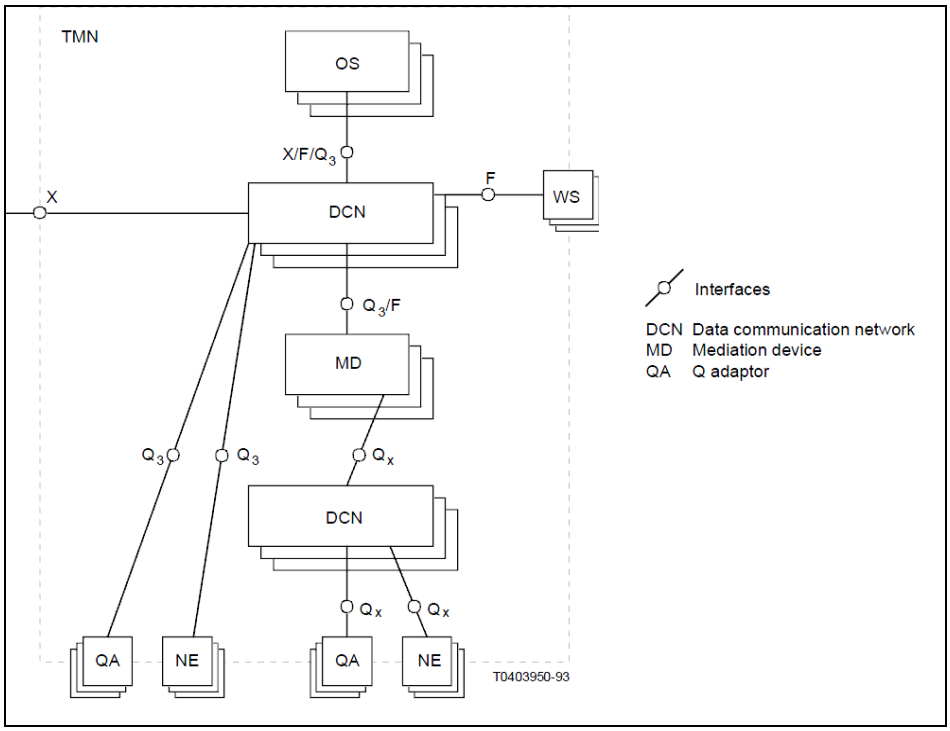
Pored tri klase referentnih tačaka TMN-a, postoje i dve klase referentnih tačaka koje nisu deo TMN-a:

- **g referentna tačka** za povezivanje WFS sa korisnicima
- **m referentna tačka** za povezivanje QAF sa opremom koja nije u pod mrežom za upravljanje u kojoj se QAF nalazi

3.3 Fizička arhitektura

Fizička arhitektura prikazuje kao se TMN funkcionalni blokovi mogu mapirati u fizičke blokove (opremu) i kako se referentne tačke mogu mapirati u intrfejse. Namena fizičke arhitekture je da prikaže način na koji se mogu inplementirati funkcionalni blokovi i referentne tačke. Na slici 3.4 je dat primer fizičke arhitekture mreže za upravljanje sa funkcionalnim blokovima i interfejsima koji se mogu naći u njoj.
Fizički blokovi mreže za upravljanje su sledeći:

- **Operations System (OS) - operacioni sistem** koji obezbeđuje izvršenje funkcije OSF i namenjen je za nadzor i upravljanje mrežom
- **Mediation Device (MD) – posrednički uređaj** koji obezbeđuje izvršenje funkcije MF i namenjen je za nadzor i koristi se u mreži za konverziju interfejsa i formata paketa
- **Network Element (NE) – mrežni element** koji obezbeđuje izvršenje funkcije NEF i sačinjen je od uređaja ili bilo kog dela telekomunkacione mreže koja obavlja funkciju NEF. NE je najčešće komunikacioni uređaj, ali može biti i server koji u mreži obezbeđuje neki od servisa.
- **Workstation (WS) – radna stanica** koja obezbeđuje izvršenje funkcije WSF i namenjen je da omogući pristup administratorima mreži za upravljanje kako bi realizovali svoje funkcije. U mreži za upravljanje može da bude više radnih stanica, ali se organizacijom mreže za upravljanje mora definisati način njihove integracije i prioriteta u mreži, kako bi se sprečile koalizije u mreži
- **Q Adaptor (QA) – Q adapter** koji obezbeđuje izvršenje funkcije QAF i predstavlja uređaj namenjen za povezivanje OS i NE sa elementima koji nisu delovi TMN i ne podržavaju standarde TMN referentnih tačaka.
- **Data Communication Network (DCN) – komunikaciona mreža** koji obezbeđuje izvršenje funkcije DCF (Data Communication Function) i namenjena je isključivo za prenos podataka namenjenih za nadzor i upravljanje mrežom. Može da se realizuje u okviru telekomunkacione mreže koja se nadzire, ali može da se realizuje kao fizički zasebna mreže ili kao VPN u okviru neke druge velike mreže. Mora da podržava protokole koje koristi mreža za upravljanje.



Slika 3.4. Primer fizičke arhitekture TMN

Interfejsi fizičke arhitekture mreže za upravljanje su definisani da bi odgovarali standardnim referentnim tačkama TMN-a kada se ostvaruje fizička konekcija preko njih. Interfejsi TMN-a su sledeći:

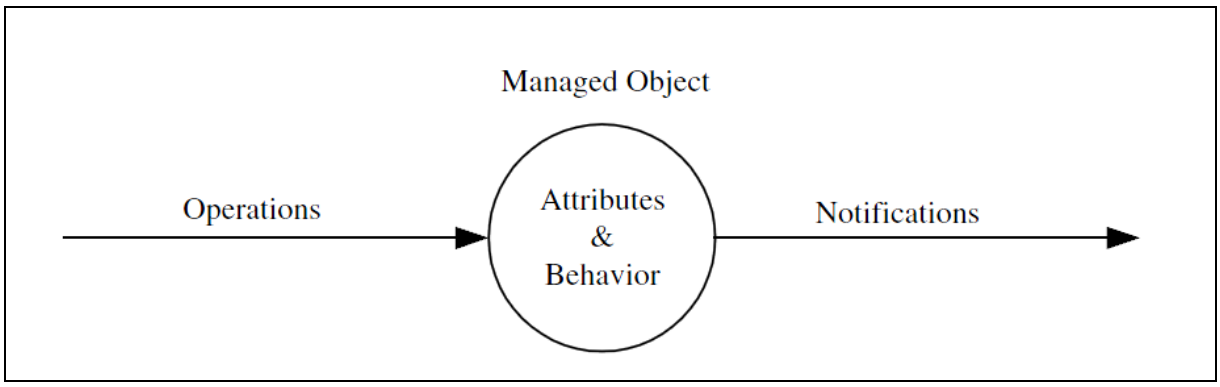
- **Q interfejs** koji je primenjen kod q referentne tačke i postoje dve vrste ovog interfejsa: Qx koji je primenjen kod q_x referentne tačke i Q_3 koji je primenjen kod q_3 referentne tačke. Razlika između ova dva interfejsa se ogleda u informaciji koju se preko njih prenosi. Qx interfejs karakteriše to da primarno prenosi informacije između MD i NE koji su na nju povezani. Q3 interfejs karakteriše da prenosi informacije između OS i elemenata TMN-a koji su direktno povezani na OS:
- **F interfejs** koji je primenjen kod f referentne tačke i namenjen je za povezivanje radne stanice sa elementima TMN-a.
- **X interfejs** koji je primenjen kod x referentne tačke i namenjen je za vezu između dva TMN-a ili za povezivanje sa drugom mrežom za upravljanje koja ima interfejse ekevivalentne TMN intrfejsima. Ova vrsta interfejsa je najosetljivija po pitanju sigurnosti i zaštite podataka.

3.4 Informaciona arhitektura

Informaciona arhitektura objašnjava objektno orjentisani pristup TMN u sklopu upravljanja mrežom. TMN informaciona arhitektura bazirana je na OSI informacionom modelu definisanom u ITU preporuci X.700 (6). Koristeći objektno orjentisani pristup za upravljanje ova arhitektura definiše opremu u telekomunikacionoj mreži kao objekte u mreži za upravljanje koji se nadziru i kojima se upravlja operativnim sistemom za upravljanje.

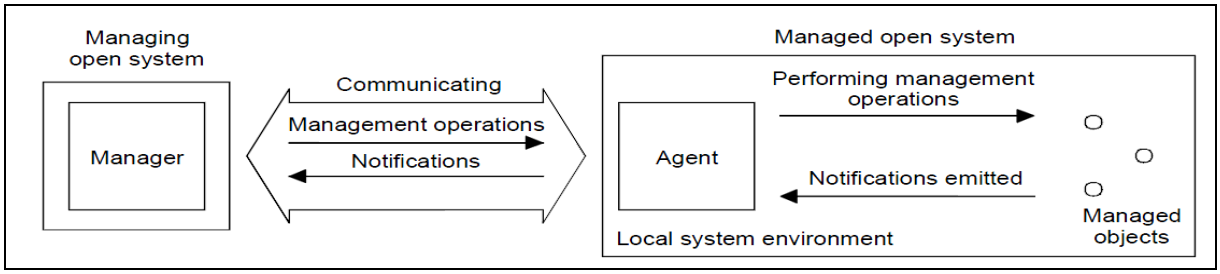
Objekat kojim se upravlja može se definisati sledećim karakteristikama, prikazanim na slici 3.5:

- Svojstva objekta koja prikazuju karakteristike i specifičnosti objekta kojim se upravlja
- Operacije koje su primenjene nad objektom upravljanja i objektu kojem se izdaju zadaci
- Ponašanje kojim se prikazuje način odgovora na zadate operacije
- Obaveštenja koje objekat upravljanja šalje kao izveštaje o izvršenim zadacima i stanjima u kojima se nalazi



Slika 3.5. Objekat upravljanja

TMN arhitektura za upravljanje mrežom pripada vrsti distribuirano orjentisanih mreža upravljanja u pogledu hijerarhije u mreži.. Osnovna odlika ovakog načina upravljanja je da pored menadžera na vrhu postoje menadžeri srednjeg nivo, koji u slučaju gubitka veze sa menadžerima na vrhu, preuzimaju njihovu ulogu i nastavljaju sa upravljanjem agentima koji su vezani u okviru njihovog dela mreže za upravljanje. Ukoliko dođe do gubitka veze između menadžera srednjeg nivoa i agenata, agenti su odgovorni za upravljanje objektom u kojem se nalaze u skladu sa zadacima koji su predefinisani u samim agentima. Odnos između menadžera, agenata i objekata upravljanja prikazan je na slici 3.6.



Slika 3.6. Prikaz odnosa između menadžera, agenata i objekata upravljanja

Komunikacije između menadžera i agenta se sastoji od razmene operacionalnih zadataka, koji potiču sa strane menadžera, i obaveštenja, koja potiču od strane agenta. Komunikacije je realizovana uz korišćenje Common Management Information Services (CMIS) and Common Management Information Protocol(CMIP) definisanih ITU preporukama X.710 (7) i X.711(8). Komunikacija između agenta i objekta

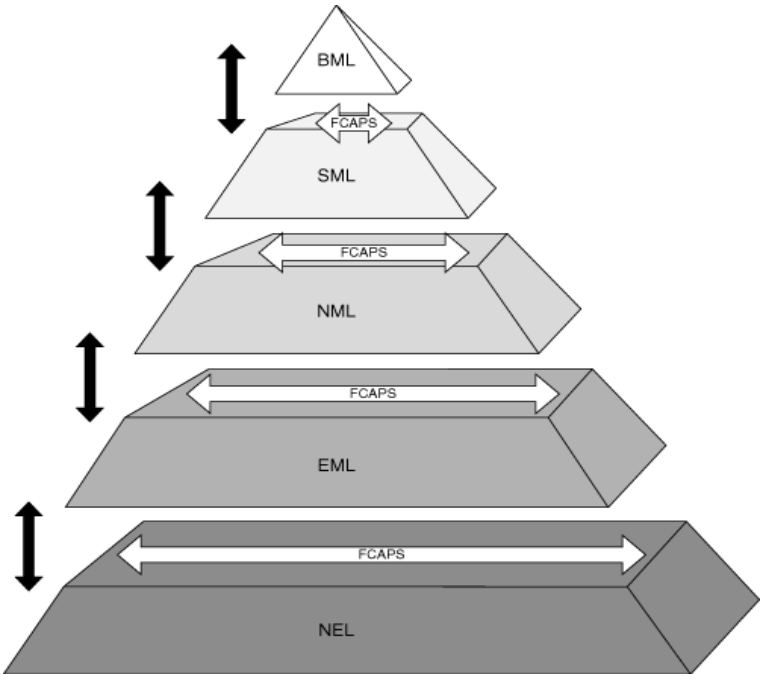
upravljanja se sastoji od operacija za izvršenje zadataka koje šalje agent i povratnih obaveštenja od strane objekta upravljanja. Objekat upravljanja, za razliku od menadžera i agenta, nije deo TMN-a.

3.5 Logička arhitektura

Logička arhitektura (Logical Layer Architecture - LLC) predstavlja logički pogled na delove upravljačkog sistema koji su neophodni da postoje u organizaciji hijerarhije jednog rešenja za upravljanje telekomunikacionom mrežom i servisima i uslugama koje ona pruža. Da bi se pojednostavila kompleksnost upravljanja mrežom neophodno je da se izvrši podela poslova i uspostavi hijerarhija odgovornosti kroz slojeve logičke arhitekture.
Koncept TMN primenjuje više slojeva logičke arhitekture po sledećem:

- sloj upravljanja poslovanjem (*Bussines Management Layer-BML*),
- sloj upravljanja servisima (*Service Management Layer-SML*),
- sloj upravljanja mrežom (*Network Management Layer-NML*),
- sloj upravljanja elementima mreže (*Element Management Layer-EML*),
- sloj mrženih elemenata *(Network Element Layer –NEL).*

Slojevi upravljnja su poređani po opadajućoj hijerarhijskoj piramidi i predstavljeni su na slici 3.7.



Slika 3.7. Hijerarhijska upravljačka piramida

Definicija funkcionalnosti svakog od ovih slojeva nije striktna i zavisi od više faktora kao što su: stategije upravljanja, veličina mreže, složenosti TMN upravljačkih servisa i dr. Generalno logički slojevi upravljanja mogu biti najkraće biti opisati na sledeći način:

- **BML** - omogućuje globalni poslovni pregled i kordinaciju telekomunikacionog operatora. Operacioni sistemi (Operation Systems –OSs) na ovom sloju imaju sledeće zadatke: podršku procesima donošenja odluka za optimalno

investiranje i korišćenje postojećih i novih telekomunikacionih resursa; podršku upravljanju ukupnim budžetom, posebno delom namenjenom održavanju, administriranju i radu mreže/servisa; podršku u pogledu kadrovskih resursa; održavanje i agregaciju podataka o ukupnom poslovanju preduzeća. Fizička realizacija upravljačkog sistema na ovom sloju naziva se Biznis menadžer sistem.

- **SML** - obuhvata aktivnosti na obezbeđivanju servisa krajnjim korisnicima, ukupnom administriranju ovih servisa i korisnika u okviru posmatranog operatora, međusobne odnose između različitih operatora i pružalaca servisa, održavanje statističkih podataka o kvalitetu servisa kao i odnose između različitih servisa. Radi toga ovaj sloj treba da raspolaže podacima o stanju mreže, da pruža podršku planiranju mreže i da izvršava upravljačke servise koje mu postavlja BML. Fizička realizacija funkcionalnosti ovog sloja naziva se Servis menadžer sistem.
- **NML** - obezbeđuje kontrolu rada mreže. To uključuje kontrolu, način povezivanja i koordinaciju svih elemenata mreže (Network Element – NE) unutar mreže ili posmatranog domena mreže, kontrolu uspostavljanja veze sa kraja na kraj, podršku sistemima za rekonfiguraciju mreže, podršku kreiranju mehanizama za otklanjanja greške nakon njene pojave, održavanje mrežnih mogućnosti, održavanje statističkih i drugih podataka o mreži i njenim interakcijama sa višim servisnim slojem. Ovaj sloj takođe ima uvid u podatke o konfiguraciji svih elemenata mreže u posmatranom domenu, kao i informacije o odnosima sa susednim domenima. OS ovog sloja podržava mrežno bazirane TMN aplikacione funkcije radi kontrole raspoloživosti mrežnih kapaciteta i povećanja kvaliteta servisa. Po analogiji sa nadređenim slojevima fizička realizacija upravljačkog sistema naziva se Mrežni menadžer sistem.
- **EML** - direktno upravlja elementima mreže na pojedinačnoj ili grupnoj osnovi, odnosno u okviru jednog EML-a može se naći više elemenata mreže. Najveći deo skupova upravljačkih funkcija kao što su nadzor i kontrola elemenata mreže, lokalizacija greške unutar elemenata mreže, statistika i istorija elementa mreže obavljaju se unutar ovog sloja. U bazi podataka ovog sloja nalaze se podaci o elementima mreže, podaci o ponašanju, obaveštenjima i akcijama svakog elementa mreže, kao i podaci o povezivanju unutar elemenata mreže. Element menadžer je usvojeni naziv za fizičku realizaciju upravljačkog sistema.
- **NEL** - direktno usmeren na fizičke resurse NE. U opštem slučaju NE može obuhvatiti više uređaja od kojih svaki ima svoje resurse (fizičke i logičke). Nova telekomunikaciona oprema dizajnirana je tako da se može direktno kontrolisati od strane TMN-a. NEL prenosi EML informacije o stanju i događajima vezanim za resurse, a od njega prihvata komande za akcije koje sprovodi nad resursima.

3.6 Upravljačke oblasti TMN-a

Rad TMN-a je definisan preporukom ITU M.3400 (9) i odvija se u pet upravljačkih oblastikoje se skraćeno prikazuju akronimom FCAPS (*Fault, Configuration, Accounting, Performance, Security*).

Upravljačke oblasti TMN-a su:

- upravljanje greškama – Fault Management
- upravljanje konfiguracijom – Configuration Management
- upravljanje naplatom – Accounting Management
- upravljanje performansama – Performance Management
- upravljanje bezbednošću – Security Management

3.6.1 Upravljanje greškama

Upravljanje greškama obuhvata aktivnosti rukovanja alarmima, detekcije i izolacije grešaka i aktivnosti u cilju otklanjanja greške i oporavka mreže. Upravljanje greškama pruža mogućnost da se pažljivo posmatraju problematična područja i da se brzo odreaguje kako bi se nesmetano nastavile mrežne operacije. Ovu oblast upravljanja možemo podeliti u šest setova funkcija:

- merenje pouzdanosti, raspoloživosti i opstanka – RAS (Reliability, Availability, Survivability),
- praćenje stanja alarma,
- lokalizacija greške,
- korekcija greške,
- testiranje nakon korekcije greške,
- administracija greške

Obim primene ove oblasti upravljanja zavisi od stabilnosti mreže i mrežnih elemenata. Ukoliko je mreža pouzdana javljaće se manji broja grešaka u sistemu i alarma i samim tim oblast upravljanja greškama biće manje zastupljena, dok je kod nestabilnih sistema, pri velikom broju grešaka i alarma, ova oblast znatno zastupljenija.

3.6.2 Upravljanje konfiguracijom

Upravljanje greškama obuhvata aktivnosti kontrole, upravljanja, identifikacije mrežnih elemenata, dostavljana upravljačkih funkcija ka objektima upravljanja i prikupljnje informacija u suprotnom smeru. Ovu oblast upravljanja možemo podeliti u pet setova funkcija:

- planiranje mreže i mrežnih elemanata,
- instalacija mreže,
- planiranje i ugovaranje servisa,
- konfigurisanje servisa,
- status i kontrola mrežnih elemenata

Obim primene ove oblasti zavisi od namene telekomunikacione mreže kojom se upravlja. Ukoliko se radi o mrežama kod kojih nakon puštanja u rad nema velikih promena i uvođenja novih servisa onda je ova oblast malo primenjena. Upravljanje konfiguracijom postaje znatno primenjena u slučaju da se radi o mrežama koje podložne stalnim izmenama konfiguracije i uvođenja novih servisa.

3.6.3 Upravljanje naplatom

Upravljanje naplatom obuhvata aktivnosti merenja iskorišćenosti mreže i servisa i tarifiranja i naplate za pružene usluge. Ovu oblast upravljanja možemo podeliti u tri seta funkcija:

- merenje iskorišćenosti mreže i servisa,
- tarifiranje i naplata usluga,
- sakupljanje podataka i kontrola poslovanja

Ova oblast ima znatniju primenu kod instituciija koje se bave davanjem servisa i usluga drugim licima u komercijalne svrhe, kao bi ostvarili veću finansijsku dobit i tretirali korisnike u skladu sa njihovim potrebama. Kod institucija koje nisu komercijalnig karatera oblast upravljanja naplatom ima ulogu u pogledu optimizacije sopstvenih troškova.

3.6.4 Upravljanje performansama

Upravljanje performansama obuhvata aktivnosti merenja i izveštavanja administratora o ponašanju telekomunikacione mreže i efikasnosti mreže i mrežnih elemenata. Ovu oblast upravljanja možemo podeliti u četiri seta funkcija:

- kvalitet performansi,
- nadzor performansi,
- kontrola performansi,
- analiza performansi

Ova oblast ima primenu pri prikupljaju i analizi podataka o stanju mreže i kvaliteta servisa (QoS – Quality of Service) pruženih korisnicima u cilju korekcije i dovođenja u stanje kvaliteta u okviru garantovanih graničnih vrednosti za određeni servis ili uslugu.

3.6.5 Upravljanje bezbednošću

Upravljanje bezbednošću obuhvata omogućavanja sigurne komunikacije i detekcije događaja i obaveštenja narušavanja sigurnosnih mera. Ovu oblast upravljanja možemo podeliti u četiri seta funkcija:

- prevencija,
- detekcija,
- oporavak sistema nakon detekcije narušavanja bezbednosti,
- administracija bezbednosti

Ova oblast omogućava funkcije autentifikacije, kontrole pristupa, integritedt i pouzdanost podataka, detekcije neovlašćenog pristupa i korišćenja i oticanja poverljivih podataka. Oblast upravljanja bezbednošću je povezana sa svim ostalim oblastima upravljanja TMN-a i obim posla zavisi od složenosti mreže i zahteva za zaštitom i sigurnošću mreže.

4 SIMPLE NETWORK MANAGEMENT PROTOCOL – SNMP ARHITEKTURA MREŽA ZA UPRAVLJANJE

Simple Network Management Protocol (SNMP) arhitektura mreža za upravljanje je deo veće arhitekture koja se naziva Internet Standard Management Framework i koja je namenjena za nadzor i upravljanje mrežama baziranim na TCP/IP referentnom modelu. SNMP predstavlja Intrenet standard za nadzor i upravljanje uređajima povezanih na Internet ili u okviru zatvorenih Intranet mreža.
Da bi jedna TCP/IP mreža funkiconisala bez problema ili sa problemima koji bi se otklanjali u kratkom vremenskom roku neophodno je administratoru mreže obezbediti nadzor i upravljanje uređajima koji se u njoj nalaze. U početku kada su mreže bile sa malo elemenata administrator je mogao steći uvid u stanje hardvera i softvera elemenata mreže fizičkim praćenjem rada uređaja ili korišćenjem protokla upravljanja nižih slojeva referentnog modela. Ovakva mogućnost nadzora i upravljanja je razvojem opreme u modernim mrežama postala nemoguća. Mreže su se sastojale od velikog broja mrežnih elemenata, geografski raširene na velikom prostoru i često sa različitim tehnologijama na nižim slojevima upravljanja. Zahtevi za nadzorom i upravljanjem ovakvim vrstama mreža uslovile su potrebu za jedinstvenim standardizovanim modelom za nadzor i upravljanje TCP/IP mrežama.
Početkom osamdesetih godina dvadesetog veka više radnih grupa su pokušvale da pronađu rešenje ovog problema, ali zbog različitih vrsta tehnologja zastupljenih u tim grupama nije se doslo da jedinstvenog rešenja. Tri vodeća rešenja su bila:

- *High-level Entity Management System (HEMS) / High-level Entity Management Protocol (HEMP)* definisan preporukama RFC 1021-1024
- *Simple Gateway Monitoring Protocol (SGMP)*, definisan preporukom RFC 1028
- *Common Management Information Protocol* (CMIP), koji je bio deo OSI referentnog modela

Internet Engineering Task Force (IETF) je 1988 objavila preporuku RFC 1052 (10) o razvoju standarda za nadzor i upravljanje TCP/IP mrežama Kako ova preporuka nije standar njen zaključak je bio da se SGMP iskoristi kao osnova za razvoj novog Internet standarda nazvanog *Simple Network Management Protocol (SNMP)*.

Ime SNMP je dvosmisleno i predstavlja:

- SNMP je jedan od protokola u aplikativnom sloju TCP/IP referentnog modela poput SMTP, DHCP ili FTP protokola.
- SNMP je drugi i znatno upotrebljivaniji naziv za Internet Standard Management Framework (ISMF) arhitekturu upravljanja mrežom koja se sastoji od više elemenata od kojih je SNMP protokol samo jedan njen deo.

SNMP arhitektura je orginalno bila namenjena za upravljanje IP mrežama preko in-band IP ulaza, odnosno preko istog intrefejsa koji je namenjen i za slanje i prijem IP saobraćaja. Upravljanje se vršilo konekcijom preko telenet konekcije ili korišćenjem softverskih rešenja baziranih na SNMP-u, kao što je HP's Open View. Da bi se omogućio pristup ruteru ili nekom drugom uređaju u slučaju kada IP saobraćaj ne funkcioniše, odnosno da bi se omogućilo upravljanje opremom koja ne podržava in-band IP ulaz, SNMP je adaptiran i ostvarena je mogućnost upravljanja preko nezavisnih telekomunikacionih kanala i out-of-band IP ulaza.

SMNP arhitektura je zamisljeni kao jednostavan (simple) način nadzora i upravljanja mrežom. U početku je bilo moguće ostvariti zahtevanu jednostavnost, ali se usložnjavanjem mreža i nadogradnjom verzija sastavnih činioca SNMP arhitekture, usložnjavala i sama arhitektura, tako da je SMNP arhitektura za upravljanje mrežom mnogo kompleksnija od sam naziv simple – jednostavan možda ukazuje i predstavlja mnogo više od protokola za protok upravljačkih informacija između delova mreže. Uprkos usložnjavanj SNMP arhitektura je i dalje ostala znatno jednostavnija od ostalih vrsta arhitektura za upravljanje mrežom. Glavni ciljevi SNPM arhitekture upravljanja mrežom su:

- SNMP definise univerzalni način na koji se upravljačka informacija može lako definisati za bilo koji objekat i onda se lako razmeniti između navedenog objekta i opreme zadužene za nadzor i upravljanje mrežom
- SNMP odvaja funkcije definisanja i prenosa upravljačkih informacija od aplikacije namenjene za nadzor i upravljanje mrežom
- SNMP protokol je jednostavan i sastoji se od nekoliko jednostavnih operacija i neophodno ga je kroz nadogradnju održavati sto je moguće jednostavnijim
- Nadogradnja SNMP protokola je moguća bez ometanja kompletne SNMP arhitektura
- Implementacija SNMP-a je jednostavna i jeftina za proizvođače opreme

4.1 Osnovni model SNMP arhitekture mreže za upraljanje

SNMP arhitekturu u pogledu hardverskih komponenti sačinjavaju dva vrste uređaja:

- Mrežna upravljčka stanica - **Network Management Station (NMS)** koje predstavlju tačno definisane mrežne uređaje opremljene softverom za nadzor i upravljanje sa ulogom da realizuju funkciju upravljanja mrežnim elementima. U jednoj mreži može postojati više mrežnih upravljačkih stanica.
- Mrežni elementi **- Managed Nodes** koji predstavljaju uređaje u mreži koji poseduju određeni softver koji omogućava da se njima upravlja od strane mrežnih upravljačkih stanica. Mrežni elementi predstavljju objekte upravljanja.

Na slici 4.1. predstavljen je osnovni SNMP operacionalni model u kome imamo prikazne osnovne entitete u SNMP arhitekturi upravljnja. Kao i kod TMN arhitekture i u slučaju SNMP arhitekture komunikacija se obavlja na relaciji menadžer – agent. Komunikacija od menadzera je u principu realizovana po sistemu tačka – više tačaka, odnosno jedan menadžer komunicira sa više agenata. U suprotnom smeru od agenata ka menadžeru komunikacija se odvija po sistemu tačka – tačka, odnosno jedan agent komunicira samo sa jednim menadžerom.
Dva osnovna entiteta kod SNMP arhitekture mreža za upravljanje su:

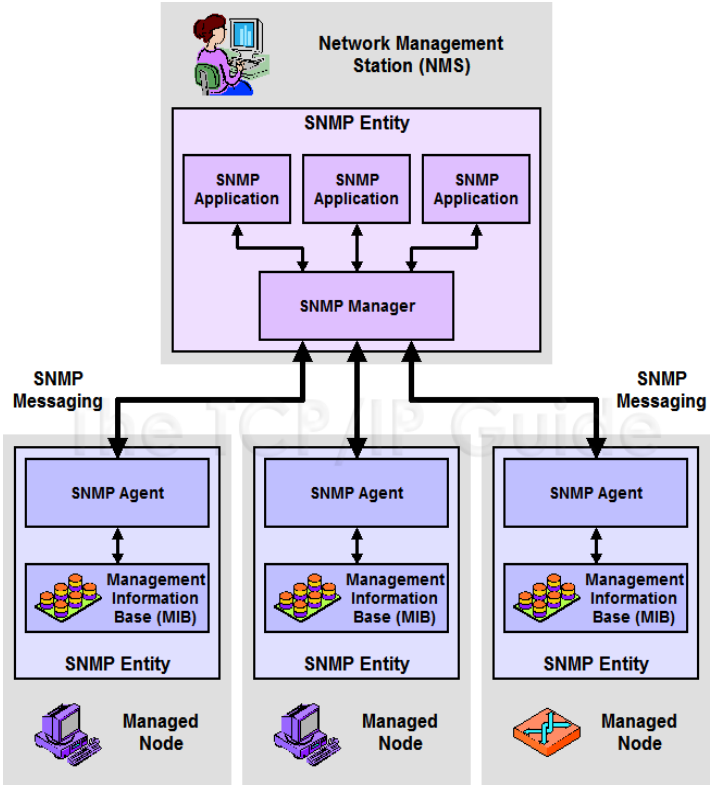
- **SNMP entitet mrežnog elementa**– koji je deo mrežnog elementa odnosno bilo kojeg uređaja u mreži kojim se upravlja i koji poseduje softver koji mu omogućava da se upravlja sa njim. Sastoji se od dva softverska elementa:

  - SNMP agent – koji je predstavlja softverski program koji implementira SNMP protokol i dozvoljava objektu upravljanja da prima komande od mrežne upravljačke stanice i da šalje informacije o stanju i događajima u suprotnom smeru.

- SNMP MIB (Management Information Base) – koja je predstavlja bazu podataka sa informacijama o objektu upravljanja, koje se koriste u svrhu upravljanja istim uz razmenu poruka putem SNMP protokola.

- **SNMP entitet mrežne upravljačke stanice**– koji je obuhvata više hardverskih elemenata u jedanu softversku celinu namenjenu za upravljanje mrežom sastoji se od dva elementa:

  - SNMP menadzer – koji predstavlja softverski program koji implementira SNMP protokol i omogućava mrežnoj upravljačkoj stanici da šalje komande ka objektu upravljanja i da prima informacije o stanju i događajima iz suprotnog smera.
  - SNMP aplikacija – koji je predstavlja jednu ili više aplikacija namenjenih da čoveku, u ulozi administratora, omogući korišćenje SNMP-a za nadzor i upravljanje mrežom.

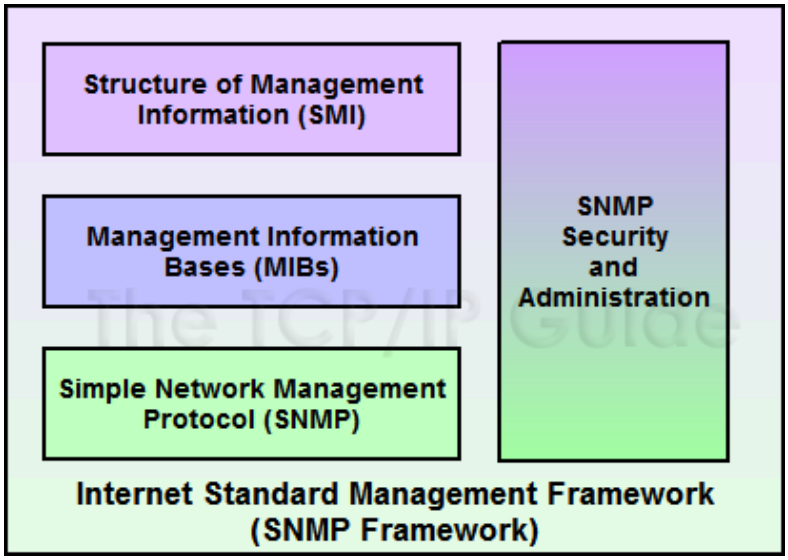


Slika 4.1. SNMP operacionalni model (11)

4.2 Sastavni činioci SNMP arhitekture mreže za upraljanje

Sastavni činioci SNMP arhitekture mreže za upravljanje su, kao što je i prikazano na slici 4.2, sledeći:

- **Struktura upravljačkih informacija - Structure of Management Information (SMI)**
- **Baza podataka upravljačkih informacija - Management Information Bases (MIBs)**
- **SNMP protokol**
- **Zaštita i administracija - Security and Administration**



Slika 4.2. Sastavni činioci SNMP arhitekture (12)

4.2.1 Struktura upravljačkih informacija - Structure of Management Information (SMI)

Struktura upravljačkih informacija - Structure of Management Information (SMI) predstavlja skup pravila kojima se definišu objekti koima se upravlja preko SNMP protokola. SMI predstavlja mehanizam za opisivanje i imenovanje objekata i događaja u cilju upravljanja SNMP protokolom uz korišćenje Abstract Syntax Notation One (ASN.1) standarda. SMI predstavlja lokalnu organizaciju podataka u MIB.
SMI definiše sledeće karakteristike neophodne za upravljanje objektima:

- **Ime objekta** kojima se objekat upravljanja jedinstveno definiše u mreži za upravljanje
- **Sintaksu objekta** kojom se definiše vrsta objekta kojim se upravlja
- **Enkodovanje** kojim se definiše kako se oblikuje informacija, koja se odnosi na određeni objekat upravljanja, za razmenu između elemenata u mreži za upravljanje

SMI je definisan kroz dve vrste:

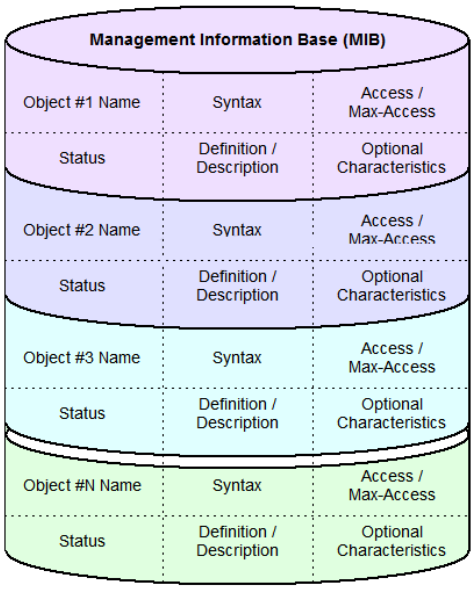
- **SMIv1 –** verzija koja je zastupljena od uvođenja SNMPv1 verzije protokola i omogućava prenos podataka između objekata u mreži pri korišćenju SNMPv1, SNMPv2c i SNMPv3 verzija protokola
- **SMIv2 –** poboljsana verzija koja je zastupljena od uvođenja SNMPv2c verzije protokola i omogućava prenos podataka između objekata u mreži pri koršićenju SNMPv1, SNMPv2c i SNMPv3 verzija protokola

4.2.2 Baza podataka upravljačkih informacija - Management Information Base (MIB)

Baza podataka upravljačkih informacija - Management Information Base (MIB) predstavlja skup promenljivih osobina koje su namenjene da opišu upravljačke karakteristike bilo koje vrste opreme u mreži. Svaka od promenljivih osobina

prikazuje informaciju o komandi upućenoj od strane mrežne upravaljačke stanice ka mrežnim elementima i od obaveštenja koja se šalju od mrežnih elemenata ka mrežnoj upravljačkoj stanici. Svaka zasebna promenljiva osobina se naziva MIB objekt i skup MIB objekata čini jedanu bazu podataka upravljačkih informacija – MIB, sto je prikazano na slici 4.3. MIB predstavlja bazu podataka sa informacijama o objektu upravljanja koje se koriste u svrhu upravljanja istim uz razmenu putem poruka SNMP protokola. Vrednosti stanja zapisanih u MIB svakog elementa u mreži predstavlja trenutno stanje mreže.
MIB objekti mogu da imaju tri načina na osnovu koji se komunicira sa njima:

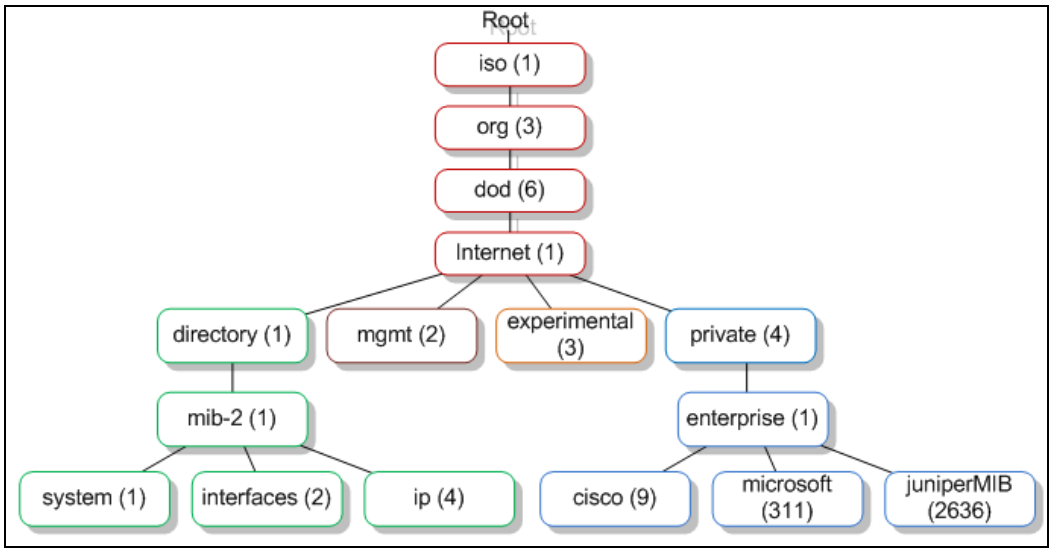
- Read only – koji omogućava samo čitanje podataka MIB objekta
- Write only – koji omogućava samo upis podataka u MIB objekat
- Read-write – koji omogućava i čitanje podataka i upis podataka u MIB objekat



Slika 4.3. Management Information Base (MIB)

U zavisnosti od složenosti hardevera i softvera jednog uređaja MIB se sastoji od više različitih MIB objekata, od kojih postoje i neki novi u odnosu na postojeću opremu. Kako broj MIB objekata nije konačno definisan, ostavljena je mogućnost da se nove vrste MIB objekata definišu novim RFC preporukama. Do sada je definisano više od 100 vrsta MIB objekata.
MIB poseduje razgranatu strukturu stabla koja organizuje MIB objekte upravljanja u logičke kategorije i predstavlja hijerarhijski poredak svih objekata upravljanja i nacina na koji se može doći do njih. Za formiranje strukture stabla koristi se ime objekta - object identifier (OID) koji jedinstveno definiše objekat u MIB hijerearhiji, odnosno u mrezi za upravljanje. OID predstavlja niz brojeva koji su čitljivi samo MIB-u. Objektom koji nema OID ne moze da se upravlja. Na slici 4.4. je dat primer MIB strukture stabla. Da bi se omogućilo da se uspostavi nadzor i upravljanje na relaciji menadžer – agent, odnosno mrežna upravljačka stanica – mrežni element, neophodno je da se u MIB upravljačkim stanicama nalazi potpuno ista MIB mrežnog elementa, jer se samo tako omogućuje praćenje nastalih promena u objektu upravljanja i pravilno smeštanje informacija. Kada se novi element dodaje u mrežu, sadržaj i format

njegove baze podataka mora biti usnimljen u bazu podataka upravljačke stanice, dok je na njemu neophodna instalacija softvera agenta preko koga se uspostavlja funkcija nadzora i upravljanja.



Slika 4.4. Primer MIB strukture stabla

Postoje dve vrste MIB - baza upravljačkih podataka:

- **MIB-I** koja je nastala pojavom prve verzije SNMPv1
- **MIB-II** koja je nastala pojavom druge verzije SNMPv2 i koja je donela poboljšanja u odnosu na prethodnu verziju u vidu dodataka u skladu sa novim operativnim zahtevima, povećanja kompatibilnosti između SMI-a i MIB-a sa SNMP protokolom, poboljšane podrške za objekte koji koriste više protokola I funkcije poboljšanja jasnoće tekstualnog sadržaja MIB-a radi bolje jasnoće i čitljivosti podataka iz baza.

Sadržaj i format MIB-a je standardizovan od strane standarzicionih tela, ali je ostavljena mogućnost proizvođačima opreme da za svoju opremu mogu da dodaju MIB objekte u MIB baze podataka. Primer za to je nadzor temperaturnih uslova u kojoj je smeštena oprema, jer nadzor ovakvog elementa nije definisan u standardnim MIB preporukama, tako da proizvođači čija oprema nadzire navedeni element moraju da izvrše dodavanje objekta u bazu podataka. Svaki proizvođač registruje svoje objekte pod različitim OID. Primeri OID za neke prizvođače su: 1.3.6.1.4.1.311 za Microsoft; 1.3.6.1.4.1.343 za Intel; 1.3.6.1.4.1.2 za IBM; 1.3.6.1.4.1.9 za Cisco.

4.2.3 SNMP protokol

Simple Network Management Protocol (SNMP) je protokol aplikativnog sloja namenjen za razmenu upravljačkih informacija između mrežnih elemenata i mrežne upravljačke stanice. Namenjen je da definiše više vrsta SNMP poruka i način na koji se poruke stvaraju i koriste. Sastoji se od više operacija protokola, koje definišu način razmene upravljačkih informacija između elemenata u mreži upravljanja, i grupe transportnog mapiranja koje definišu način na koji se poruke prenose preko različitih vrsta mreža.

Postoje dva načina komuniciranja između elemanata u mreži upravljanja:

- **Poll-driven** koji predstavlja način komuniciranja u kome onaj element koji želi informaciju mora da je traži, odnosno upravljačka mrežna stanica traži informacije od mrežnih elemenata. Koristi se za redovno prikupljanje informacija o stanju u mreži za upravljanje.
- **Interrupt-driven** koji predstavlja način komuniciranja u kome onaj element kod koga se desi problem obaveštava drugi element o problemu bez zahteva za taj zadatak, odnosno mrežni element obaveštava o problemu mrežnu upravljačku stanicu. Koristi se za trenutnu signalizaciju o nastalom problemu u mreži za upravlaljnje

Komunikacija se između upravljačke mrežne stanice i mrežnih elemenata, odnosno menadzera i agenata obavlja kroz tri vrste operacija:

- **Get** – upravljačka mrežna stanica dobija skalarnu vrednost od mrežnog elementa
- **Set** – upravljačka mrežna stanica ažurira skalarnu vrednost objekta u mrežnom elementu
- **Trap** – mrežni element šalje skalarnu vrednost upravljačkoj mrežnoj stanici bez prethodno traženog upita

Za prenos SNMP paketa koristi se User Datagram Protocol (UDP) protokol kroz portove 161 za set i get pakete i 162 za trap pakete. U OSI referentnom modelu za prenos SNMP paketa koristi se Connectionless Transport Service (CLTS).
Postoje tri verzije SNMP protokola:

1. **SNMPv1** - koja predstavlja prvu verziju protokola iz 1988. godine. Ova verzija protokola je i dalje u širokoj upotrebi pored toga što su objavljene novije poboljšane verzije protokola. Prva verzija protokola uvodi u upotrebu pojmove MIB, SMI i tri vrste operacija get, set i trap. Glavni nedostatak SNMPv1 je zaštita. Ona se zasniva na autentifikaciji prilikom identifikacije menadžera uz korišćenje community string-a koji se šalje u okviru SNMP paketa i koji deluje kao neka vrsta lozinke.
2. **SNMPv2** - koja predstavlja poboljšanu verziju SNMP protokola sa ciljem da ispravi greške prve verzije protokola. Ova verzija uvodi novine u pogledu pobljšane strukture upravljačkih informacija, mogućnosti razmene informacija između dva menadzera u mreži i dve nove operacije koje omogućavaju prenos grupe podataka i slanje trap poruka između dva menadžera. Postoje više verzija SNMP protokola (SNMPv2p, SNMPv2c, SNMPv2u) od kojih je najkorišćenija SNMPv2c verzija.
3. **SNMPv3** - koja predstavlja najnoviju verziju protokola iz 1998. godine koja je je uvela novine u pogledu zaštite SNMP protokola

4.2.4 Zaštita i administracija - Security and Administration

Zaštita i admnistracija predstavljaju četvrti sastavni činilac SNMP arhitekture za upravljanje mrežama koji se prožima kroz tri prethodna činioca i omogućava uspešnu implementaciju i upravljanje SNMP protokolom i uspešno sprovođenje mera zaštite SNMP protokola. Zaštita predstavllja vrlo bitan činilac SNMP protokola zbog činjenice da napadač ukoliko presretne SNMP poruke može da ukrade ili zameni informacije iz SNMP paketa. Ukoliko napadač ukrade informacije to mu omogućava da napravi šemu naše mreža i preuzme daljinsku kontrolu nad bilo kojim delom opreme iz naše

mreže konfigurisane za daljinsko upravljanje. Ukoliko napadač zameni informacije u SNMP porukama može da naruši fukcionisanje mreže i dovede do situacije da se ona ne može koristiti.
SNMPv1 i SNMPv2 verzije protokola su predmet packet sniffing napada, zbog karakteristike da za autentifkaciju koriste community string u vidu otvorenog teksta i usled ne korišćenja tehnika šifrovanja poruka. Pored toga navedene verzije protokola su podložne usled korišćenja UDP protokola napadima u vidu IP spoofing-a kao jednim od načešće korišćenih predstavnika denial-of-service (DoS) napada.
SNMPv3 je kao napredna verzija SNMP protokola uvela dodatne mogućnosti u pogledu zaštite i administracije. SNMPv3 pruža sledeće mogućnosti:

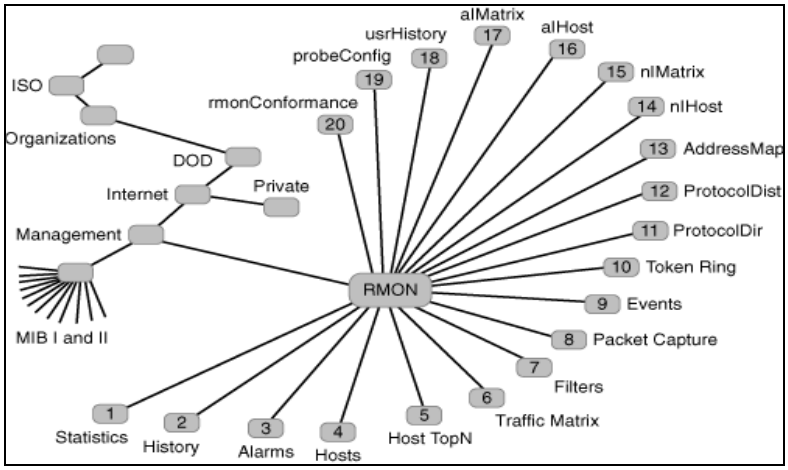
- Šifrovanje – encryption
- Autentifikaciju – authentication
- Zaštitu protiv ponavljanja poruka - protection against playback
- Kontrolu pristupa – access control

Zaštita i administracija u SNPM arhitekturi upravljanja mrežama funkcioniše na mehanizmu koji kontroliše nivo servisa koji pruža određni SNMP enetitet. Mehanizam odbaciju poruke na osnovu odgovora na pitanja:

- Ko šalje poruku? Postupkom autentifikacije se utvrđuje da li je adekvatan pošiljlac poruke
- Koja je operacija zahtevana? Postupkom autorizacije se identifikuje koja je vrsta operacije dozvoljena
- Gde će operacija biti izvršena? Postupkom kontrole pristupa definiše se lista objekata u čijim MIB-ovima se može izvršiti navedena operacija
- Kako je zahtev poslat? Nivoi zaštite razmatraju zahtev na osnovu protokola zaštite korišćenih prilikom slanja zahteva.

4.3 Remote Network Monitoring - RMON

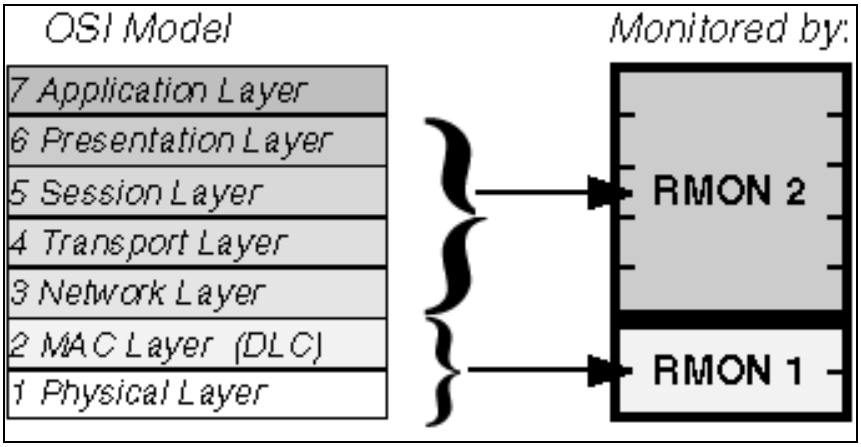
Remote Network Monitoring – RMON predstavlja važan dodatak osnovnom setu SNMP standarda koji definiše bazu podataka upravljačkih informacija za daljinski nadzor – RMON MIB i obezbeđuje najneophodnije podatke o stanju mreže. Na slici 4.5. je data struktura RMON MIB stabla u kome su prikazane MIB grupe koje su definisane u okviru RMON stanadarda.



Slika 4.5. Struktura RMON MIB stabla

Postoje dve verzije RMON standarda:

- **RMON1** koji je prevashodno namenjen za nadzor i analizu stanja lokalnih računarskih mreža (LAN). Namenjen je da vrši nadzor na prva dva sloja OSI modela, odnosno na fizičkom sloju i sloju veze. RMON1 definiše 10 MIB grupa koje se mogu naći u modernoj informatičkoj opremi i vrši nadzor mreže na nivou MAC adresa i niže. Za razliku od SNMP protokola koji je baziran na nadzoru i upravljanju na osnovu stanja u MIB-u nadgledane opreme, RMON se bazira na nadgledanju protoka – flow-based management. Time je RMON baziran na stanju saobraćaja u odnosu na stanje pojedinačne opreme
- **RMON2** predstavlja dodatak prvoj verziji RMON standarda koji omogućava na višim nivoima OSI modela. Odnos RMON1 i RMON2 standarda i OSI referentnog modela dat je na slici 4.6. RMON2 je proširen sa još 10 MIB grupa koje omogućavaju efikasniji nadzor i analizu stanja mreže. Nadzorom na višim slojevima modela protokola RMON2 omogućava nadzor kompletnih komutiranih mreža, jer je u mogućnosti da prati saobraćaj na višim nivoima mreže.



Slika 4.6. Odnos RMON1 i RMON 2 i OSI modela

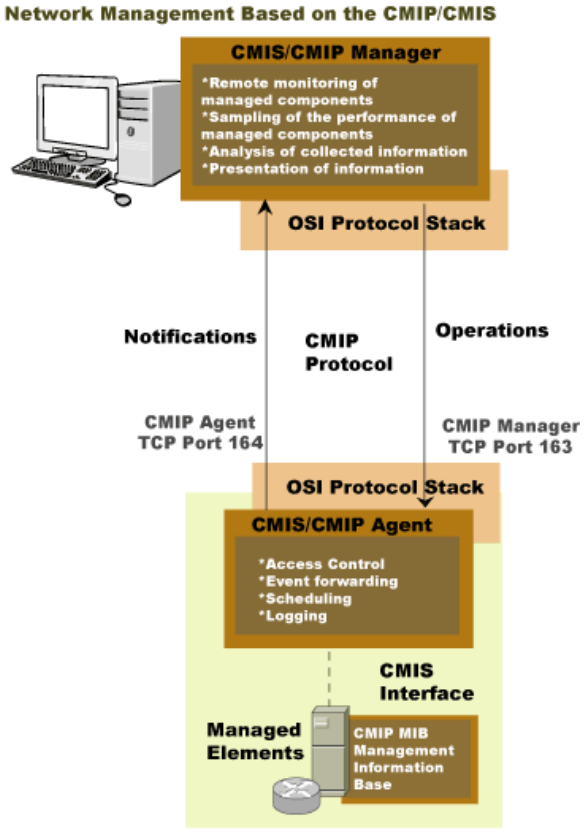
5 PROTOKOLI MREŽA ZA UPRAVLJANJE

Stalnim i brzim razvojem telekomunikacionih mreža raste i potreba za kvalitetnijim i jednostavnijim načinom nadzora i upravljanja mrežama. Kroz razvoj raznih arhitektura za upravljanje mrežama, kao njihov bitan i neodvojivi činilac pojavljuju se i protokoli za upravljanje mrežama. Protokoli definišu način razmene upravljačkih informacija između mrežnih upravljačkih stanica i mrežnih elemenata, odnosno menadžera i agenata u jednoj mreži za upravljanje. Protokoli poseduju posebno definisan način organizacije informacija o elementima u mreži, poseban jezik za razmenu informacija i poseban način dodele imena upravljačkim objektima. Ne postoji jedan standardizovani i idealni protokol za upravljanje mrežama. Svaki od protokola za upravljanje ima svoje prednosti i nedostatke, koje ga čine boljim ili lošijim izborom u odnosnu na konurentni protokol. Odabir pravog protolola zavisi od veličine i potreba mreže kojom se upravalja. Na osnovu toga se donosi odluka da li je bolji izbor kompleksniji, ali pouzdaniji i sigurniji protokol, u odnosu na jednostavniji i lakse primenljiviji, ali nepouzdaniji i nesigurniji protokol.
Postoje više protokola koji se koriste za upravlajnje mrežama od kojih su najdominantniji Simple Network Management Protocol (SNMP) i Common Management Information Protocol (CMIP).

5.1 Common Management Information Protocol – CMIP

Common Management Information Protocol – CMIP predstavlja protokol za upravljanje mrežama razvijen za mreže bazirane na OSI referentnom modelu. Omogućava implementaciju servisa definisanih od strane Common Management Information Services (CMIS) u cilju razmene upravljačkih informacija između mrežnih elemenata kojima se upravlja i aplikacija za upravljanje mrežom. CMIP je definisan ITU-T X.700 serijom preporuka i predstavlja glavnog konkureta IETF SNMP protokolu. Zbog svoje zasnovanosti na OSI referentnom modelu CMIP je tipični predstavnik TMN aplikacije. CMIP je pouzdan protokol jer svoj transportni mehanizam zasniva na connecntion-oriented vrstama prenosa. Pored toga predstavlja i vrlo siguran protokol, jer podržava procese kontrole pristupa, autentifikacije i sigurnosnih logova (security logs). Upravljačke informacije se razmenjuju između mrežnih aplikacija i mrežnih elemenata uz korišćenje upravljačkih objekata (managed objects), koji predstavljaju karakteristiku elementa mreže da može da se nadzire, da se njime upravlja i da izvršava postavljene zadatke.
CMIP ne razmatra funkcionalnost aplikacije za upravljanje mrežom, već samo definiše način razmene upravljačkih informacija u mreži za upravljanje.
CMIS podržava razmenu upravljačkih informacija između elemenata u mreži i definiše servise za dobijanje informacija o mrežnim elementima u cilju kontrole i upravljanja, kao i dobijanja izveštaja o efektima izvršenih akcija nad njima.
CMIP je kao protokol za upravljanje mrežama rasprostranjeniji u telekomunikacionim mrežama, ali su razvijene verzije za upravljanje TCP/IP mrežama. Verzija za upravljanje TCP/IP mrežama se naziva CMOT (CMIP Over TCP). Verzija razvijena za IEEE 802 LAN mreže naziva se CMOL (CMIP Over LLC). Sa razvojem tih verzija predstavlja glavnog kandidata SNMP protokolu.
Upravljački objekti (MOs) kao specifični oblici informacija ili resursi kojima se upravlja predstavljeni uz korišćenje Abstract Syntax Notation One (ASN.1) standarda. Grupa MOs sačinjava Management Information Base (MIB). Uz korišćenje Guidelines for

the Definition of Managed Object (GDMO) koji predstavllja specifičan tehnički jezik kojim se za svaki od MOs definiše klasa, kojom se određuju ponašanje i svojstva objekta. Kod CMIP je posebno važna karakteristika da se nasleđuju osobine viših klasa čiji su oni podsistemi. MOs formiraju bazu podataka koja se u CMIP definiše kao Management Information Tree (MIT). CMIP omogućava da se MOs u MIT menjaju, brišu ili dodaju. CMIP služi da se izazove određena akcija u mrežnom elementu ili da se od mrežnog elementa primi obaveštenje o događaju.
Na slici 5.1 je dat osnovni model mreže bazirane na CMIP/CMIS.



Slika 5.1. Osnovni model CMIP/CMIS mreže

Servisi koji se obezbeđuju u CMIP protokolu za upravljajnje mrežnim elementima podeljeni su u tri gupe po sledećem:

- **Upravljački operacionalni servisi**
  - M-CREATE – za kreiranje novog MOs
  - M-DELETE – za brisanje postojećeg MOs
  - M-GET - za slanje zahetva za slanje svojstava MOs
  - M-CANCEL-GET - za poništavanje poslatog zahteva za slanje svojstava MOs
  - M-SET – za postavljanje svojstava u MOs
  - M-ACTION – za slanje zahteva za izvršenje nekog zadatka od strane mrežnog elementa u kome se nalazi MOs
- **Upravljački servisi za obaveštavanje**
  - M-EVENT-REPORT – za slanje obaveštenja o događaju na koji se desio na MOs

- **Upravljački servisi za asocijaciju**
  - M-INITIALIZE – Ostvaruje asocijaciju – povezivanje između dve aplikacije na aplikativnom sloju
  - M-TERMINATE - Prekida uspostavljenu vezu
  - M-ABORT – Prekida vezu u slučaju nestabilnog ponašanja ostvarene veze

5.2 Simple Network Management Protocol – SNMP

Simple Network Management Protocol (SNMP) predstavlja protokol koji je jedan od sastvanih cinioca SNM-aP, odnosno Internet Standard Management Framework (ISMF) arhitekture upravljanja mrežom koji je razvijen od strane Internet Engineering Task Force (IETF) u nameri da se stvori open source standar za upravljanje mrežom. SNMP je protokol aplikativnog sloja namenjen za razmenu upravljačkih informacija između mrežnih elemenata i mrežne upravljačke stanice. Za realizaciju svog zadatka koristi mali broj komandi što mu omogućava jednostavnost navedenu u njegovom nazivu. Jednostavnost se ogleda i u tome što se zasniva na komuniciranju preko UDP protokola i coonectionless komunikacionog kanala. Jednostavnost SNMP omogućila mu je da postane najrasprostranjeniji protokol u mrežama za upravljanje. Standardizacija je SNMP protokolu omogućila široku upotrebu, jer administratori mreže mogu da upravljaju mrežom sastavljenom od opreme različitih proizvođača uz korišćenje jedne aplikacije za nadzor i upravljanje.
Postoje tri verzije SNMP protokola koje su u upotrebi:

- **SNMPv1**
- **SNMPv2**
- **SNMPv3**

5.2.1 SNMPv1

SNMPv1 predstavlja prvu verziju protokola iz 1988. godine objavljene od strane IETF u preporuci RFC 1157 (13). Iako je najstarija verzija ovog protokola ona je i dalje najzastupljenija verzija u upotrebi, koja je tokom dugog vremena korišćenja napredovala od open source do de facto standarda za upravljanje u TCP/IP mrežama.
Komunikacija u SNMPv1 verziji protokola se odvija uz korišćenje pet tipova poruka, odnosno pet PDU (Protocol Data Units) (14):

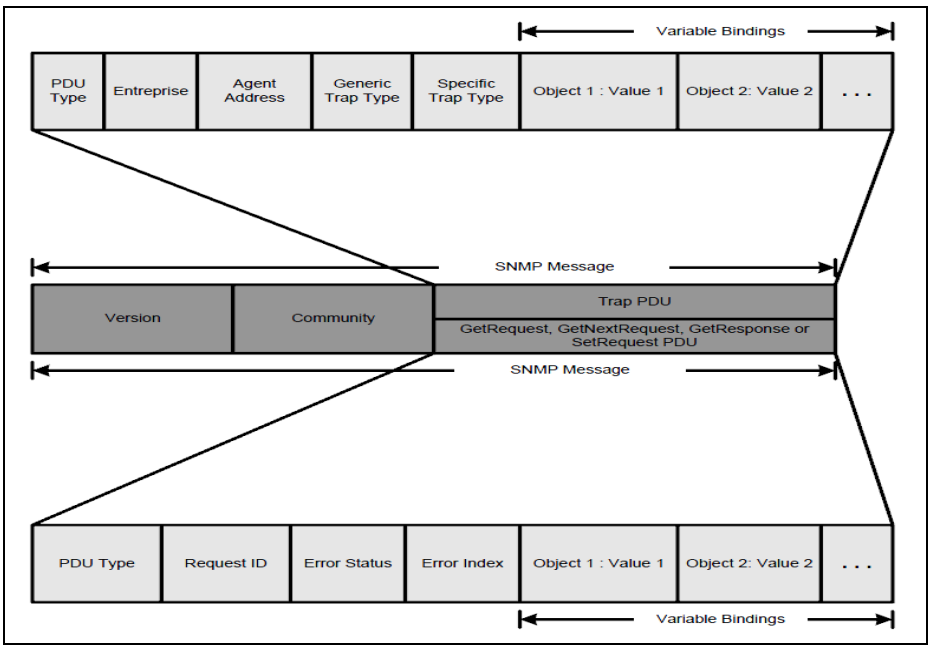
- **GetRequest** – upravljačka mrežna stanica šalje zahtev mrežnom elementu da pošaje vrednosti iz MIB-a. Sobzirom da je svaka predstavljena sa jedinstvenim OID nizom neophodno je da upravljačka mrežna stanica pošalje zahet za svaku vrednost za koju želli da dobije povratnu informaciju.
- **GetNextRequest** - zahtev koji je namenjena traži OID i vrednost MIB-a koja je za jedan broj veći od vrednosti iz prethodnog GetNextRequest zahteva. Ukoliko ne postoji navedena vrednost OID mrežni element odgovara sa vrednošću sledećeg OID-a u MIB stablu. Na ovaj način vrši se provera svih elemenata iste vrste objekata kroz tabelu promenljive dužine.
- **GetResponse –** predstavlja odgovor od mrežnog elementana na GetRequest, GetNextRequest i SetRequest zahteve. Ukoliko je odgovor na Get zahteve onda on predstavlja zahtevane informacije. Ukoliko je odgovor na Set zahteve onda on predstavlja potvrdu da su zahtevane promene izvršene.

- **SetRequest** – predstavlja komandu upravljačke mrežne stanica ka mrežnom elementu da ažurira vrednost objekta u MIB-u
- **Trap** – namenjen je da mrežni element šalje vrednost upravljačkoj mrežnoj stanici bez prethodno traženog upita o promeni definisanog stanja u objektu upravljanja. Trap PDU se sastoji se od OID-a koji je indetifikuje kao trap poruku, informaciju o toke koji je objekat poslao trap poruku i vrednosti u tom MIB objektu. Trap poruke imaju definisane različite nivoe kritičnosti : Critical, Major, Minor, Warning, Marginal, Informational, Normal, Unknown

SNMPv1 omogućeva jednostavan prostupak atentifikacije prilikom identifikacije upravljačke mrežne stanice uz korišćenje community string-a koji se šalje u okviru SNMP paketa. Community string predstavlja lozinku i ukoliko se ona razlikuje od definisane u primljenom paketu paket se odbacuje. Community string se ručno podešava na svim elementima u mreži i šalje se u vidu otvorenog teksta, što predstavlja uzrok niske sigurnosne vrednosti ovog protokola. Postoje tri vrste community string-ova:

- SNMP Read-only community string – koji se koristi prilikom slanja GetRequest i GetNextRequest zahteva
- SNMP Read-Write community string string – koji se koristi prilikom slanja GetRequest i GetNextRequest zahteva, ali i SetRequest zahteva koji omogućava promenu vrednosti u MIB-u
- The SNMP Trap community string – koji se koristi da mrežne elemente organizuje u grupe. Kako SNMP ima mogućnost drugih načina organizacije mrežnih elemenata u grupe kojima se upravlja, njegova primena je retka i koristi se samo kao redundantna mogućnost grupisanja mrežnih elemanata.

SNMP poruke se šalju u okviru SNMP paketa čiji format prikazana na slici 5.2.



Slika 5.2. Format SNMPv1 paketa

Nedostatci SNMPv1 verzije su nedostatak sigurnosti, ograničene funkcije i centralizovan način upravljanja koji ne omogućava uspešno upravljanje velikim i geografski rasprostranjenim mrežama.

5.2.2 SNMPv2

SNMPv2 je novija IETF verzija protokola iz 1993. godine definisane u preporuci RFC 1441 (15), kao i RFC 1452 (16) koja definiše odnos između SNMPv1 SNMPv2. SNMPv2 je napravljena sa namerom da se isprave slabosti iz prve verzije SNMP protokola. U odnosu na SNMPv1 postignuta su sledeća poboljšanja:

- Uvedena je nova i bolja struktura upravljačkih informacija SMIv2
- Omogućena je komunikacija između upravljčkih mrežnih stanica u mreži
- Uvedena su poboljšanja u pogledu sigurnosti u vidu party-based i user-based security načina zaštite, koja nisu kasnije standardizovana kroz SNMPv2c verziju protokola

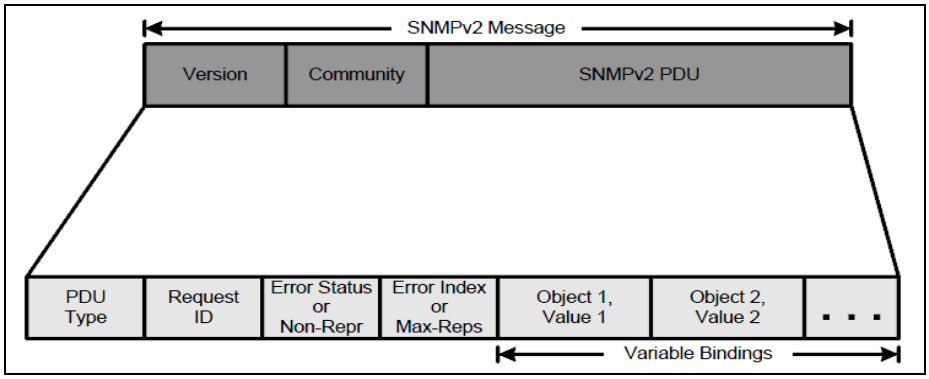
Kao poboljšanje u odnosu na SNMPv1 uvedene su dve nove vrste PDU poruka:

- **GetBulkRequest** – koja kao alternativa za GetNextRequests omogućava prenos veće grupe podataka kao odgovor na jedan zahtev
- **InformRequest** – koje omogućava komunikaciju i slanje trap poruka između upravljačkih mrežnih stanica

Kroz razoj SNMPv2 verzije SNMP protokola razrađeno je više verzija:

- **Party-Based SNMPv2 (SNMPv2p)** – koja je uvedena sa poboljsanjima u vidu SMIv2 struktura upravljačkih informacija i party-based metodom zaštite
- **Community-Based SNMPv2 (SNMPv2c)** – koja predstavlja modifikovanu SNMPv2p verziju protokola da umesto party-based metoda zaštite koristi community string metoda zaštite. Predstavlja najzastupljeniju verziju protokola i pod nazivom SNMPv2 se načešće misli upravo na ovu verziju
- **User-Based SNMPv2 (SNMPv2u)** koja predstavlja modifikovanu SNMPv2c verziju protokola da umesto user-based metodom zaštite umesto community string metoda zaštite

SNMP poruke se šalju u okviru SNMP paketa čiji format prikazan na slici 5.3.



Slika 5.3. Format SNMPv2 paketa

Uzevši u obzir veliki broj različitih verzija SNMPv2 protokola razvijenih od 1993. godine i nemogućnosti odabira prave verzije, većina administratora mreže se

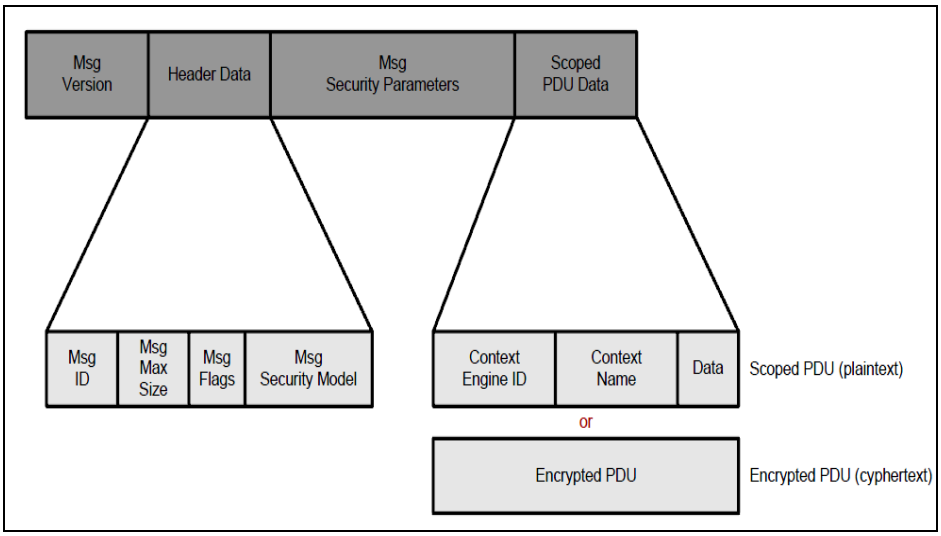
odlučuje za korišćenje SNMPv1 verzije protokola pred svih poboljsanja koje verzija 2 nudi.

5.2.3 SNMPv3

SNMPv3 je najnovija verzija SNMP protokola, koja je objavljenja 1198. godine i opisana je u IETF preporukama od RFC 3410 do RFC 3415 (17), (18), (19), (20), (21) i (22). Ova verzija ne predstavlja zamenu za SNMPv1 i SNMPv2 već predstavlja njihovu nadogradnju u cilju poboljšanja funkcionalnosti i zaštite.(23)
SNMPv3 je doneo sledeća nova rešenja:

- Novi format SNMP poruke
- Novi način autentifikacija za poruke
- Poboljšani sistem zaštite za poruke
- Kontrolu pristupa
- Nastavak podrške za SNMPv2

Zbog modulane strukture SNMP razvoj novije verzije formata poruke ne predstavlja problem i dovoljno je nadograditi postojeći format poruke. Kako SNMPv3 mora da podržava prethodne SNMPv1 i SNMPv2 to se postiže dodavanjem novog SNMPv3 modula u postojeći format poruke.
User-based Security Model (USM), koji je opisan u prepuruci RFC 3414, definiše upotrebu MD5 i hash algoritama u cilju poboljšanja sigurnosti. Ovim novinama se doprinelo integritetu, zaštiti i privatnosti podataka. Postoji podrška u pogledu protokola za autentiikaciju HMAC-MD5-96, HMAC-SHA-96 i opcionalna podrška za protokol šifrovanja CBC-DES.
Kontrola pristupa je omogućena preko View-based Access Control Model (VACM) i opisana je u preporuci RFC 3415. Njome se definiše način vidljivosti podsistema u kopmletnom MIB stablu.
SNMPv3 format poruke je dat na slici 5.4.



Slika 5.4. Format SNMPv3 paketa

5.3 Poređenje SNMP i CMIP

Sličnost između SNMP i CMIP se ogleda u tome da su namenjeni za prenos upravljačkih informacija između elemenata u mreži upravljanja u cilju ostvarivanja funkcija nadzora i upravljanja. Oba protokola predstavljaju funkcionalne celine arhitektura za upravljanje telekomunikacionim mrežama. SNMP je napravljen za korišćenje u TCP/IP mrežama i trenutno predstavlja najdominantniji protokol u toj oblasti. CMIP protokol je kao protokol OSI referentnog modela zastupljen u TMN arhitekturi za upravljanje mrežama i yastupljeniji je u klasočnim telekomunikacionim mrežama.

5.3.1 Prednosti SNMP protokola

Prednosti SNMP protokola se ogledaju u sledećim osobinama:

- **Jednostavnost** – zbog svoje jednostavnosti predstavlja rešenje za upravljanje mrežom koje je lako i brzo primenljivo, što predstavlja naveću prednost u odnosu na CMIP. Jednostavnost kao karakteristika ovog protokola omoguća laku upotrebu u malim i velikim TCP/IP mrežama, i omogućava administratoru jednostavno programiranje osobina koje želi da nadzora i kojima želi da upravlja. Primena ovog protokola doprinosi manjim mrežnim poremećajima prilikom intervencija i promena karakteristika postojeće verzije, odnosno kod prelaska na sledeću verziju softvera.
- **Rasprostrnjenost upotrebe** – zbog toga što je u vreme kada je razvijan predstavljao jedino kvalitetno rešenje mnogi skoro svi proizvođači opreme su implementirali ovaj protokol za potrebe upravljanja opremom
- **Brža implementacija** – implementacija SNMP-a je znatno brža i manje zahtevnija u odnosu na implementaciju CMIP-a, jer se razmena informacija i servisa bazira na nepouzdanom connectionless UDP protokolu, za razliku od CMIP-a koji razmenu informacija i servisa bazira na pouzdanom connection-oriented TCP protokolu. Resursi koje zauzima u okviru mreže, u vidi neophodne širine opsega su znatno manji kod SNMP-a u odnosu na CMIP, što ga čini pogodnijim za opremu sa manjim hardverskim karakeristikama poput radne memorije ili brzine procesora.
- **Proširivost –** zbog svoje jednostavnosti i manjeg uticaja na funkcionisanje mreže nadogradnja opremom opremljene ovim protokolom je znatno jednostavnija, što omogućava lakše proširenje mreže sa novim članovima. Komleksnost CMIP-a čini proces proširenja mreže sa novom opremom znatno složenijim i skupljim procesom, nego što je to slučaj kod SNMP-a, čija je upotreba u finansijskom smislu znatno isplativija.

5.3.2 Prednosti CMIP protokola

Prednosti CMIP protokola se ogledaju u sledećim osobinama:

- **Upotrebljivost upravljačkih informacija** - upravljačke informacije se pored uloge da nose obaveđštenja, mogu iskoristiti izvođenje određenih zadataka, poput obaveštavanja o nemogućnosti pristupa serveru od strane klijenta nakon predefinisanog broja pokušaja, što je kod SNMP-a neizvodljive, jer administrator u tom slučaju mora da vodi računa o broju neuspelih pokušaja i da po dostizanju limita odluči o daljem potezu. Ovo čini mrežu sa CMIP-om

efikasnijom i manje zahtevnijom za rad u pogledu angažovanja administratora mreže.

- **Sigurnost** - predstavlja i vrlo siguran protokol, jer podržava procese kontrole pristupa, autentifikacije i sigurnosnih logova (security logs), što kod SNMP-a nije bilo zastupljeno do pojave SNMPv3, koji još uvek nije u upotrebi kao SNMPv1 i SNMPv2.
- **Veće mogućnosti upotrebe** – u odnosu na SNMP ima veće mogućnosti da omogući upravljačkim informacijama da sa jednim zahtevom izvrši više radnji, što ga čini superiornijim u odnosu na SNMP u pogledu organizacije i izvršenja operacija. Zbog svoje bolje organizacije primenljiviji je u odnosu na SNMP za implementaciju u velikim mrežama.
- **Bolje izveštavanje** – omogućuje slanje boljih izveštaja sa potpunijim i detaljnijim podacima o događajima koji su se desili i time omogućava administratoru i upravljačkoj aplikaciji bolji uvid u stanje mreže i lakši odabir operacije koja treba da se izvrši.
- **Pouzdanost** – zbog korišćenja pouzdanog connection-oriented protokola predstavlja znatno pouzdaniji protokol, što ga čini boljim izborom za državne mreže, kao i mreže velikih telekomunikacionih kompanija gde pouzdanost i kvalitet usluga imaju značajnu ulogu.

6 PROCES UVOĐENJA MREŽE ZA UPRAVLJANJE

U proteklim godinama nadzor i upravljanje heterogenim telekomunikacionim mrežama predstavlja izuzetno izazovan zadatak. Kao ključni problemi u realizaciji upravljanja mrežom javljaju se:

- Usleda velikog obima interakcija između delova opreme u mreži, razmena upravljačkih informacija između upravljačkih mrežnih stanica i mrežnih elemenata je znatno povećana, čime se javlja mogućnost zagušenja u saobraćajnim kanalima telekomunikacione mreže
- Kod upravljanja mrežom korišćenjem centralizovano orjenitisane mreže za upravljanje sa jednom upravljačkom mrežnom stanicom kao jedinim menadžerom u mreži, bez menadžera srednjeg nivao, upravljanje različitim sistemima i servisima postaje nemoguće usled velike količine podataka koje oduzimaju značajni deo mrežnih resursa
- Održavanje skalabilnosti i fleksibilnosti postojeće mreže usled stalnog broja mrežnih elemenata koji se pridodaju mreži za upravljajnje uslovljenih rastom same telekomunikacione mreže usled posvećanih zahteva korisnika

Iz složenosti zadatka za upravljajnjem telekominikacionom mrežom može se zaključiti da je proces uvođenja mreže za upravljanje u jedan telekomunikacioni sistem izuzetno bitan i u isto vreme zahtevan zadatak. Proces uvođenja mreže za upravljanje u jedan telekomunikacioni sistem je deo sistema upravljanja mrežom definisanih u ITU preporuci M.3400 u kojoj su definisani FCAPS upravljačke oblasti koje se moraju definisati i u okviru sistema za upravljanje mrežom.
Proces uvođenja mreže za upravljanje predstavlja aktivnosti koje transformišu ulazne veličine u izlazne veličine uz integraciju rada ljudi, tehnologija i metoda za postizanje zajedničkog krajnjeg cilja. Ulazne veličine su zahtevi za pouzdanom, skalabilnom, fleksibilnom i sigurnom telekomunikacionom mrežom sa visokim kvalitetom pruženih usluga i ljudstvom obučenim da izvršava poslove definisane FCAPS upravljačkim oblastima.
Upravljanje mrežom mora kao krajnji cilj da obezbedi:

- povećan prihod davaocu usluga uz ostvarivanje mogućnosti fokusiranja na poslovanje, kapacitet i mogućnosti mreže, kvalitet usluga i sigurnost mreže
- minimalni finansijski trošak
- predvidiv i fleksibilni rizik

Proces uvođenja mreže za upravljanje da bi bio efikasan mora da sadrži nabojlje prakse u oblasti primene informaciono-komunikacijskih tehnologija. Da bi se zadovoljili ovi uslovi proces mora da bude (24):

- dokumentovan – dostupan svim učesnicima u realizaciji procesa, kao i licima zaduženim za evaluaciju procesa
- prihvatljiv – usklađen sa standardima koji definišu procese upravljanja mrežom
- kontinualno poboljšavan – ponovljiv u cilju poboljšanja procesa upravljanja mrežom
- efiikasan i skalabilan – da se sastoji od nekoliko vitalnih i više trivijalnih rešenja
- efektan – da dovodi do željenjog krajnjeg cilja
- adaptivan – da bude otporan na vanredne događaje

- da obezbeđuje indikatore progresa i okvire – da može da se predstavi kao model
- legalan – da bude usklađena sa zakonskim regulativama

6.1 Osnovni činioci procesa uvođenja mreže za upravljanje

Proces uvođenja mreže za upravljanje se složen proces koji obuhvata sledeće aktivnosti:

- Sagledavanje činioca koji opisuju mrežu za upravljanje
- Izgrada projekta mreže za upravljanje
- Realizacija izrađenog projekta mreže za upravljanje
- Eksploatacija mreže za upravljanje

6.1.1 Sagledavanje činioca koji opisuju mrežu za upravljanje

Osnovni čionici koji utiču na izgled mreže za upravljanje mogu se podeli ti u tri grupe:

- **Tehnički činioci** :

– Vrsta opreme koja se nadzire po funkciji (uređaji za prenos, pristup, komutaciji, tehničko obezbeđenje, napajanje) i vrsti proizvođača
– Vrsta opreme koja će se koristiti u hardeverskom i softverskom smislu za izradu same mreže za upravljanje, koja ustvari predstavlja zasebnu računarsku mrežu
– Način reallizacije mreže u pogledu korišćenja resursa za prenos upravljačkih informacija – in-band i out-band Management

- **Organizacioni činioci** :

– Upravljački slojevi koje će biti prisutnu u mreži (upravljanje poslovanjem, servisima, mrežom, elementima mreže i mreženim elemenatima)
– Izbor arhitekture mreže po orjentaciji u odnosu na mrežne upravljačke stanice (centralizovano i distribuirano orijentisana mreža za upravljanje). Distriburano orjentisana mreža je u predenosti zbog smanjenja količine saobraćaja koji generiše mrežna upravljačka stanica, veća skalabilnost mreže i otklanjanje opasnosti da ispad iz rada mrežne stanice za upravljanje blokira rad kompletne mreže za upravljanje
– Skalablnost i fleksibilnost kapaciteta, odnosno mogućnost proširenja mreže za upravljanje sa dodatnim mrežnim elementima i otpornost na eventualne prekide i zagušenja u komunkacionim kanalima

- **Ekonomski činioci** :

– Cena neophodnih hardverskih i softverskih komponenti za izgradnju mreže za upravljanje
– Cena obuke kadra za održavanje mreže za upravljanje
– Raspoloživost rezervnih delova i način servisiranja instaliranih komponenti

6.1.2 Izgrada projekta mreže za upravljanje

Na osnovu sagledavanja cinioca koji opisuju mrežu za upravljanje pristupa se aktivnosti izrade projekta mreže za upravljanje. Projekat mreže za upravljanje se sastoji iz faze prikupljanja podataka, faze planiranja, izrade prototipa i analize projekta.
Prilikom planiranja mreže za upravljanje neophodno je izvršiti sledeće korake u planiranju:

- Planiranje veličine mreže za upravljanje u odnosu na broj elementa u telekomunikacionoj mreži
- Planiranje rasporeda elemenata mreže za upravljanje u odnosu na izabranu hijerahiju
- Konfiguracija parametara softverskih i hardverskih komponenti
- Planiranje DCN za povezivanje elemenata mreže za upravljanje i razmenu upravljačkih informacija
- Planiranje OSS (Operation Support System) kao nezavisnog softverskog sistema namenjenog za prikupljanje podataka o perormansama sistema, stanju opreme u mreži za upravljanje i upravljanje sistemima za dijagnostiku kvarova
- Planiranje parametara IP mreže (IP adrese, broj porta i propusni opseg)
- Planiranje zaštite i pouzdanosti mreže za upravljanje

6.1.3 Realizacija izrađenog projekta mreže za upravljanje

Nakon faze izrade prototipskog rešenja i faze analize i testiranja prototipa u cilju uočavanja nedostataka pre potpune implemantacije, sledi fizička montaža softverskih i hardverskih komponenti i uvođenje mreže za upravljanje u operativno okruženje. Nakon konačne implementacije mreža za upravljanje mora da demonstrira zahtevane performanse na osnovu usvojenih kriterijuma i propisanih zagarantovanih nivoa performansi.

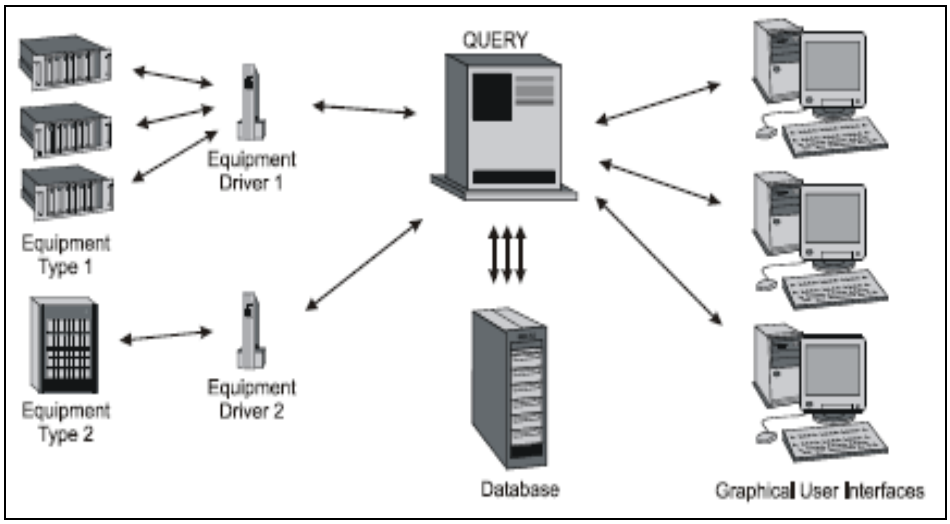
6.1.4 Eksploatacija mreže za upravljanje

Nakon potpune implementacije mreže za upravaljanje sledi korak preuzimanja i eksploatacije mreže od strane korisnika. Korisnik u potpunosti mora biti svestan svih ograničenja zasnovanih na određenoj izabranoj arhitekturi za upravljanje mrežom, na određenoj vrsti mreže za upravljanje u odnosu na orijentaciju u odnosu na upravljačku mrežnu stanicu i na vrsti odabranih softverskih i hardverskih komponenti. Eksploatacija podrazumeva kompletno održavanje funkcionalnosti i performansi mreže za upravljanje.

6.2 Aplikacija za mrežu za upravljanje

Na najvišem nivou mreže za upravljanje u okviru softvera za upravljanje mrežom nalazi se aplikacija za upravljanje mrežom. Aplikacija za upravljanje mrežom je namenjena da vrši nadzor i upravljanje mrežom sa mogućnošću da taj proces upravljanja sprovede ispunjavajući zadatke iz svih pet FCAPS oblasti upravljanja mrežom. Aplikacija u razvijenom sistemu za upravljanje mrežom doprinosi smanjenju

operacionalnih troškova upravljanja, zbog mogućnosti izvršavanja radnji na određenom elementu u mreži sa daljine uz smanjenje broja ljudi angažovanih u sistemu održavanja mreže. Proizvođači telekomunikacione i informatičke opreme uglavnom razvijaju sopstvena softverska rešenja za upravljanje njihovom opremom. Obično ta rešenja nisu kompatibilna i ne mogu da se integrišu u jedinstveni sistem, jer proizvođačima opreme nije u interesu kompatibilnost osim u slučajevima kada su u pitanju sopstveni proizvodi za različite namene. Ključni problem se javlja u načinu korišćenja komunikacionih protokola namenjenih za razmenu upravljačkih informacija. U velikim heterogenim mrežama sa mnoštvom opreme različitih proizvođača postojanje zasebnih aplikacija za upravljanje postaje problem. Rešenje ovog problema predstavalja uvođenje umbrella aplikacije kao sredstva da se prevaziđe nekompatibilnost opreme i omogući upravljanje različitom vrstom opreme od raznih proizvođača opreme. Umbrella aplikacija tretira celi podsistem aplikacija kao jedan homogenizovani sistem i administratori nemaju potreba da znaju šta se dešava na pojedinačnim nižim protoklolima za pojedinačne aplikacije. Podsistem aplikacija proizvodi izlaz za svaki pojedinačni ulaz informacija i prosleđuje ih ka nadređenoj aplikaciji uz primenu sistematičnog procesa indetifikacije, što podrazumeva sofisticiranost procesa i postojanje određene mašinske inteligencije. Povratne informacije ka sistemu koji je ispod umbrella apalikacije moguće je samo u slučaju da u umbrella aplikaciji postoji kompletno znanje o svakom elementu sistema. Prednost umbrella sistema je što omogućava i nadzor infrastrukturne opreme, kao što su napajanje, protivprvovalni sistemi i protivpožarne sistemi.
Na slici 6.1. data je opšta struktura umbrella sistema.



Slika 6.1. Struktura umbrella sistema (25)

Umbrella sistem se sastoji od sledećih elemenata:

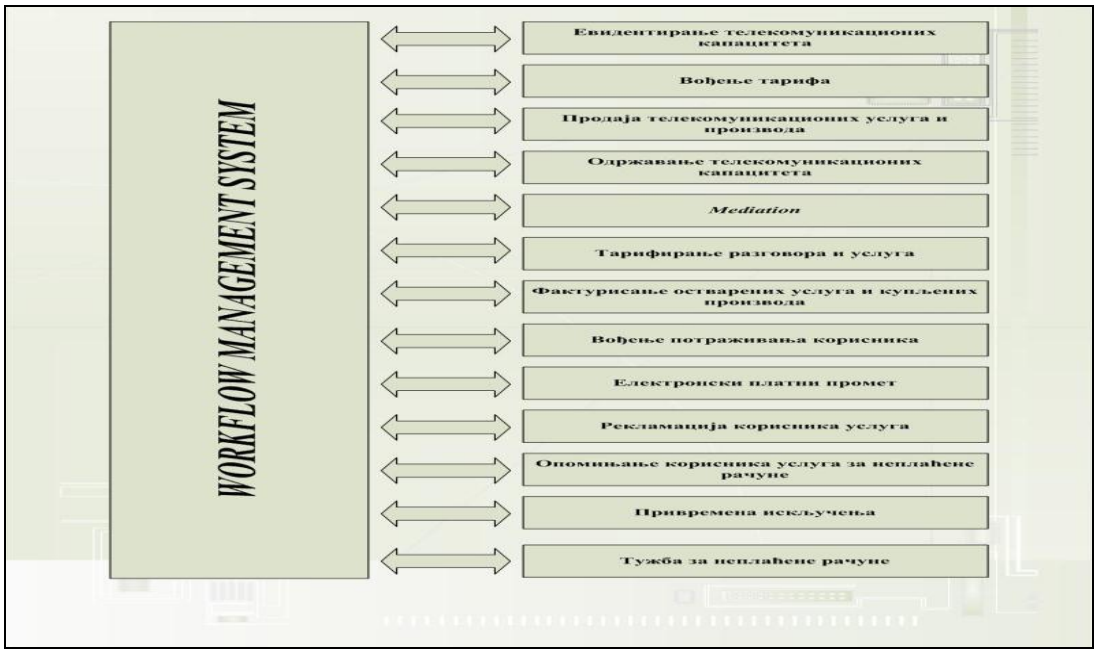
- **Korisnički grafički interfejs** - Graphical User Interface (GUI) koji omogućava administratoru da preko aplikacije sa grafičkom podlogom nadzire I upravlja sistemom
- **Modul drajvera opreme** - Equipment Driver (ED) koji mogućava povezivanje svakog elementa mreže u mrežu za upravljanje. Svaki element u mreži ima svoj ED

- **Centralni modul** – QUERY koji omogućava razmenu upravljačkih informacija između modula drajvera opreme, servera baze podataka i korisničkog grafičkog interfejsa upravljačke aplikacije
- **Server baze podataka** – Database koji vrši prikupljanje i čuvanje svih zapisa o izvršenim akcijama u mreži za upravljanje

Primeri umbrella aplikacija mogu se naći u HP open VIEW i RAD view aplikacijama za upravljanje mrežom, koji predstavljaju dobra rešenja za upravljanje mrežom.

6.3 Sistem za upravljanje poslovnim tokovima- Workflow management system

Jedan od bitnijih podsitema aplikacije za upravljanje mrežom predstavlja sistem upravljanja poslovnim tokovima - Workflow management system. Predstavlja najbitniju komponentu sistema u pogledu organizacije poslovanja upravljanja mrežom kroz pet logičkih oblasti mreže za upravaljanje (upravljanje poslovanjem, upravljanje servisima, upravljnje mrežom, upravljanje elementima mreže i mrženi elementi). Workflow management system upravlja i definiše nizom zadataka da bi se izvršili krajnji ciljevi poslovanja, što u slučaju telekomunikacione mreže podrazumeva pružanje kvalitetne i pouzdane usluge klijentima uz minimalne finasijske troškove i maksimalnu finasijsku dobit. Namenjen je da definiše različite tokove izvršavanja zadataka za različite poslove i procesu u sistemu. Jedan posao prati od početka do kraja, odnosno od kreiranja do realizacije zadatka kroz različite nivoe u hijerahiji preduzeća, tako što prati rad svake pojedinačne grupe koja izvršava specifičan deo posla, aktivira naredni deo sistema da odradi svoj deo posla i pravi izveštaje o realizaciji posla na svim nioima. Omogućava redundantnost svih procesa i praćenje stanja neizvršenih zadataka. Preduzeće može uspešno da funkcioniše ako su svi zadaci precizno i ravnopravno podeljeni po radnim mestima što se omogućava kroz sistem praćenja koje Workflow management system omogućava. Time se doprinosi znatnoj efikasnosti svih elemenata u lancu poslovanja.



Slika 6.2. Struktura TIS-a

Uspostavljajnem toka izvršavanja zadataka povećava se nivo uspešnosti komunikacije između elemenata poslovanja. Napredni sistem izveštavajna omogućava prikupljnje dobro dokumentovanih podataka što omogućava upravljajne promenama i unapređenju sistema. Praćenjem rada svakog pojedinca u sistemu omogućava povećanje njihove efikasnosti, što dovodi do povećanja efikasnosti kompletnog sistema.
Korišćenjem ovog sistema uvek je moguće dati odgovor na pitanje ko šta radi, kada i na koji način. Formalizovanjem poslovnog procesa ne gubi se vreme u odlučivanju šta treba da se uradi, jer se predefiniše učesnik u procesu koji može uspešno da izvrši zadatak.
Primer primene sistema za upravljanje poslovnim tokovima jeste TIS preduzeća ''Telekom Srbija'' a.d. Na slici 6.2 prikazana je struktura TIS-a sa njegovim podsistemima. TIS je realizovan kroz više slojnu arhitekturu sa centralnim delom koji predstavlja Workflow management system, koji predstavlja jezgro na koje se oslanjaju svi ostali podsistemi. Softver je realizovan primenom UDP standarda, sa softverskim komponentama na bazi *Oracle Oracle developer, Java i MS okruženja.*

7 KRIPTOGRAFIJA U SAVREMENIM TELEKOMUNIKACIONIM SISTEMIMA

Savremene komunikacione mreže su usled stalnih naučnih otkrića iz oblasti telekomunikacija i informatike, praćenih brzim razvojem opreme, sve složenije u pogledu veličine i različitosti prisutne opreme. Istovremeno osnovni zahtevi savremenih komunikaconih mreža jesu visoka raspoloživost, pouzdanost i kvalitet telekomunikacionih usluga. Jedna od usluga koja se zahteva jeste i sigurnost i zaštita podataka koji se prenose kroz komunikacione mreže. Odgovor na pitanje zaštite komunikcionih sistema daje kriptografija. Razvojem komunikacionih sistema i performansi komunikacione opreme razvijala se i kriptografija.

7.1 Pojam i cilj kriptografije

Reč kriptografija potiče od grčkih reči κρυπτός (kriptos), što znači skriveno i γράφειν (grafos) što znači pisati. U prevodu kriptografija znači tajno pisanje. Kriptografija predstavlja nauku koja se bavi metodama očuvanja tajnosti podataka. Polje proučavanja kriptografije je široko tako da u stručnoj literaturi imamo puno definicija kriptografije.

Kriptografija je naučno i istraživačko polje u kome se kritografi angažuju u dizajniranju i razvoju kritografskih sistema, koji mogu da zaštite osetljive podatke od hakera, prisluškivača i industrijske šijunaže.(26)

Kriptografija je nauka korišćenja matematike u šifrovanju i dešifrovanju podataka. Kriptografija omogućava skladištenje ili prenos osetljivih informacija kroz nesigurnu mrežu (kao što je Internet) tako da oni ne mogu biti čitljivi ni za koga, osim za primaoca kome su namenjeni.(27)

Kriptografija je proučavanje matematičkih tehnika koje se odnose na aspekte informacija kao što su povreljivost, integritet podataka, autentifikacija i neporecivost. Kriptografija je više skup tehnika nego samo način obezbeđenja informacione zaštite.(28)

Kriptografija je umetnost tajnog pisanja (29)

Na osnovu navedenih definicija može se zaključiti da kriptografija predstavlja nauku, koja se odlikuje svojim jedinstvenim predmetom, jezikom, teorijom i metodama i koja se bavi principima i tehnikama za zaštitu podataka od neautorizovanih osoba. Kritografija obuhvata mnogo procesa kao što su šifrovanje, autentihikacija i generisanje i distribucija ključeva, i umnogome koristi matematiku i matematičke metode u ostvarivanju svog cilja.

Cilj kriptografije jeste da da obezbedi sigurnost podataka kroz obezbeđenje povreljivosti, integriteta, autentifikacije i neporecivosti podataka u svim oblicima komunikacije i kroz sve vrste komunikacionih mreža. Informacije koje se danas razmenjuju kao lične, finansijske, poslovne ili informacije od značaja za funkcionisanje državnih organa i za državnu bezbednost, predstavljaju polje interesovanja za osobe, koje ovu vrstu informacija žele da otkriju i upotrebe ili zloupotrebe u različite svrhe. U cilju zaštite takve vrste podataka od osoba koje nisu autorizovane za njihovu upotrebu, potrebno je sporovesti niz mera i postupak koje nudi kriptografija.

Ciljevi kriptografije dati su u skraćenici **CIA (C**onfidentiality**, I**ntegrity i **A**vailability) i predstavljeni su kao:

- **Poverljivost** (Confidentiality) – predstavlja zahtev da se spreči otkrivanje sadržaja poruka od strane neovlašćenih lica
- **Intrgritet** (Integrity) – predstavlja zahtev da se spreči neautorizovana promena podataka od strane neovlašćenih lica
- **Raspoloživost** (Availability) – predstavlja zahtev da podaci budu raspoloživi, odnosno dostupni svim korisnicima sistema na način kako je to predviđeno.

Sigurnosni servisi predstavljaju uslugu koja povećava sigurnost sistema. Da bi se sigurnosni servisi sproveli, oni podrazumevaju upotrebu jednog ili više sigurnosnih mehanizama, koji predstavljaju tehnologije, pravila ili procedure namenjenih za detekciju i sprečavanje napada na kriptografski sistem, odnosno njegov oporavak nakon napada. U ITU-T X.800 preporuci sigurnosni servis definiše se kao servis koji je omogućen protokolom određenog nivoa referentnog modela i koji omogućava adekvatnu zaštitu komunikacionog sistema ili podataka koji se tim sistemom prenose.(30) U IETF RFC 2828 definiše se sigurnosni servis kao procesni ili komunikacioni servis koji je omogućen od strane sistema da pruži odgovarajuću zaštitu resursima sistema, sigurnosni sitemi su implemetirani sigurnosnim politikama i sigurnosnim mehanizmima.(31)

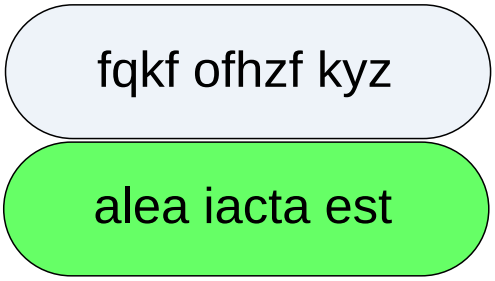
Prema ITU-T X.800 preporuci sigurnosni servisi su svrstani u pet kategorija:

- **Autentifikacija** (*engl. authentication*) – predstavlja sigurnosni servis kojim se dokazuje identitet korisnika i sistema koji šalje poruku. Autentifikacijom se potvrđuje orginalnost poruka i sprečava se mogućnost lažnog predstavljanja. Realizuje se sigurnosnim mehanizmima kao što su: šifrovanje, digitalni potis, vremenski pečat i slično.
- **Poverljivost ili tajnost podataka** (*engl. data confidentiality*) – predstavlja sigurnosni servis kojim se vrši zaštita podataka od neovlašćenih lica. Realizuje se raznim sigurnosnim mehanizmima od fizičke zaštite do šifrovanja.
- **Neporicljivost poruka** (*engl. non-repudation*) – predstavlja sigurnosni servis kojim se sprečava lažno poricanje slanja određenje poruke, kao i mogućnost da primalac poruke izmeni sadržaj poruke i tvrdi da je taku poruku primio. Realizuje se sigurnosnim mehanizmom digitalnim potpisom.
- **Integritet podataka** *(engl. data integrity*), – predstavlja sigurnosni servis kojim se obezbeđuje integritet i tačnost poruke, odnosno onemogućava izmena, uništenje ili lažno generisanje poruke od strane neovlašćenog lica. Realizuje se sigurnosnim mehanizmima kao što su : Heš (*engl. Hash*) funkcija, kontrolne sume, logovanja i razni kodovi.
- **Autorizacija i kontrola pristupa** (*engl. authorization and access control*) – predstavlja sigurnosni servis kojim se reguliše odnos između korisnika i resursa mreže, odnosno vrši se provera pristupa određenim podacima za korisnika. Realizuje se postavljanjem privilegija kojim se definiše pravo pristupa podacima.

Kriptografija omogućava realizaciju sigurnosnih servisa putem niza sigurnosnih mehanizama radi sprečavanja varanje, zloupotrebe podataka i ostalih zlonamernih aktivnosti do kojih može doći ukoliko neovlašćena lica dođu u posed određenih podataka.

7.2 Kratak istorijski pregled kriptografije

Savremene sredstva komunikacije omogućila su veliku brzinu razmene podataka i informacija, kao i količinu podataka koji se razmenjuju kroz komunikacione mreže. Rasprostranjenost komunikacionih mreža minimizira značaj geografske udaljenosti između učesnika u razmeni podataka. Globalizacija savremenih komunikacionih mreža čini mrežu pristupačnijom za neautoriyovani pristup a podatke i informacije koji se razmenjuju komunikacionim mrežama ranjivijim na razne vrste napada. Kriptografija omogućava da se vrši zaštita podataka kroz nezaštićenu komunikacionu mrežu i da podaci sa kraja na kraj komunikacionog kanala dolaze nepromenjeni i zaštićeni od uticaja neovlašćenih lica.
Kriptografija, iako su njena upotreba i značaj postali sve veći razvojem komunikacionih mreža, datira još iz davnih vremena kada su ljudi počeli da komuniciraju između sebe i kada je bilo značajno da njihova komunikacija ostane sakrivena. Prvi oblici razmene podataka predstavljaju pisma, koja su bila namenjena da se prenese informacija na daljinu. Kako su pisma, kao sredstva komunikacije, najpre korišćena u državne i vojne svrhe bilo je neophodno da se sadržaj pisama zaštiti od od osoba koje nisu imale privilegije da budu upoznate sa sadržajem poruke.
Kriptografija ima dugu i interesantnu istoriju. Po nekim mišljenjima ka početak kritografije mogu se uzeti hijeroglifi koje su korišćeni u Egiptu pre oko 4000 godina. Hijeroglifi, koji su u osnovi male slike stvari i pojava, nisu imali ulogu skrivanja teksta, ali kako je mali broj ljudi znao njihovo značenje, sadržaj koji su njima predstavljani ostali su nepoznati za veći broj ljudi. Prvi koji je uspeo da dešifruje fonetski niz hijeroglifa bio je arheolog Žan Fransoa Šampolion 1822. godine.
Kao primer kriptografije 400 godine p.n.e. kod Spartanaca imamo upotrebu štapa, koji se naziva skital, na koji su namotavali list papirusa sa porukom. Da bi poruka bila dešifrovana skital je morao da bude iste debljine kod svih koji su trebali da znaju sadržaj poruke.
Rimski imperator Julije Cezar bio je jedan od prvih velikih vojskovođa koji je koristio šifrovane poruke u komunikaciji sa svojim vojskovođama. Šifrovanje je vršeno tako što je svakom slovu alfabeta dodeljivano slovo koje je od njega bilo udaljeno za tri pozicije sa desne strane. Primer Cezarove šifre dat je na slici broj 7.1 na kojoj je šifrovana čuvena Cezarova izjava: „Kocka je bačena“ („Alea iacta est“)



Slika 7.1. Primer Cezarove šifre

Do pojave prvih električnih i mehaničkih uređaja, koji su se koristili za šifrovanje, postojao je niz sistema za šifrovanje pomoću parira i olovke, koji su se zasnivali na supstituciji (zamena slova sa nekim drugim znakom) i transpoziciji (zamena redosleda slova u tekstu). Pojavom prvih električnih i mehaničkih uređaja za šifrovanje potupak šifrovanja se podiže na viši nivo. što omogućava bolju zaštitu poruke i teže razbijanje šifre. Pored niza uređaja iz tog doba najpoznatiji je Enigma.

Enigma je uređaj koji je izumeo nemački inženjer Artur Šerbijus i koja je korišćena od strane nemačke vojske u Drugom svetskom ratu. Ova elektromehanička mašina koja je izgledom podećala na pisaći mašinu (prikazana na slici broj 7.2), koristila je principe spojenih rotora i razvodne ploče i njen rad se zasnivao na supstituciji znakova, koristeći i aritmetičku i mapirajuću supstituciju. Korišćenjem Enigme nemačka vojska je uspešno šifrovala poruke koje su se razmenjivale na različitim nivoim komandovanja i zahvaljujući tome imala je značajne uspehe na bojnom polju.



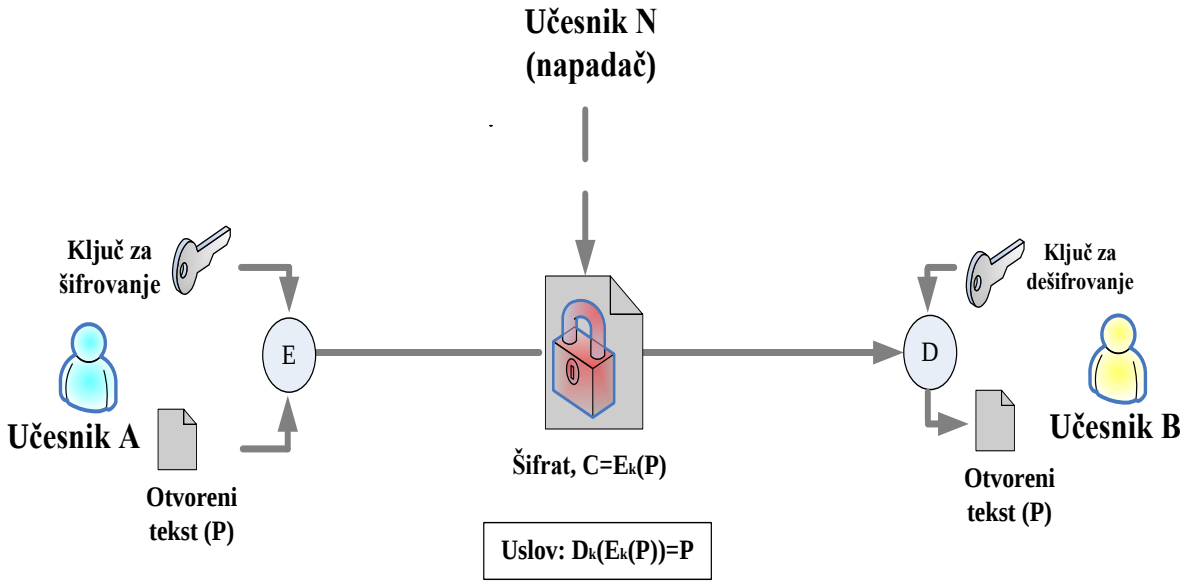
Slika 7.2. Nemački uređaj za šifrovanje Enigma

Grupa engleskih naučnika na čelu sa Alanom Tjuringom, radeći na postojećim saznanjima poljskog matematičara Marijana Rejevskog, uspela je da napravi uređaj koji je omogućavao otrkrivanje dnevnog ključa, odnosno dešifovanje poruka šifrovanih Enigmom i time stvori uslove savezničkim snagama da na vreme usmere svoja borbena dejstva u skladu sa dobijenim informacijama.
Pojavom računara dolazi do naglog razvoja kriptografije, jer sa postojanjem naprava koje mogu da obavljaju nekoliko miliona operacija u sekundi mogućnost otkrivanja sifre za manje vremena postaje sve veća. Razvoj mogućnosti za otkrivanje šifara podstiče stvaranje novih, komplikovanijih i sigurnijih šifarskih sistema, odnosno razvoj kriptografije.

7.3 Osnovni pojmovi u kriptografiji

Osnovne elemente kriptografskog sistema moguće je videti na Šenonovom modelu tajnog komuniciranja, koji je prikazan na slici 7.3. U ovom modelu razlikujemo učesnike u komunikaciji pošiljoca poruke i primaoca poruke (označeni kao osoba A i osoba B) i napadača koji pokušava da dodje do tajnog podatka.
Poruka koja se treba šifrovati predstavlja **otvoreni tekst** (*engl. plaintext*) i označena je sa P. Poruka se tranformiše pomoću određene funkcije koja je definisana parametrima zadatim ključem (označen sa K). Ova procedura transformacije otvorenog teksta u šifrovane podatke naziva se **šifrovanje** (označeno sa E). Šifrovanje se realizuje po određenom kriptografskom algoritmu uz upotrebu **kriptografskog ključa** (**ključ** šifrovanja), koji je predstavlja binarnu sekvencu veće dužine sa osobinama slučajnog niza i nezavisnu vrednost u procesu šifrovanja. Rezultat šifrovanja naziva se **šifrat** (označeno sa C), odnosno Ek(P)=C. Šifrat kao digitalni signal šalje se na prijemnu stranu kroz komunikacioni kanal i u zavisnosti od

upotrebljenog algoritma za šifrovanje poruke može biti iste ili različite dužine od orginalne poruke. Na drugoj strani komunikaciong kanala, odnosno na prijemnoj strani, šifrat se tranformiše pomoću određene funkcije koja je definisana parametrima zadatim ključem (označen sa K). Ova procedura transformacije šifrovanih podataka u otvoren tekst naziva se **dešifrovanje** (označeno sa E). Rezultat dešifrovanja je otvoreni tekst, odnosno Dk(C)=P, i ošto je cilj dešifrovanja da se dobije otvoreni tekst mora da da se zadovolji uslov Dk(Ek(P))=P.



Slika 7.3. Šenonov model tajnog komuniciranja

Cilj napadača jeste da dodje do sifrovane poruke i da određenim tehnikama dođe do otkrivenog sadržaja poruke. Nauka koja se bavi razbijanjem šifri, odnosno otkrivanjem sadržaja poruke iz šifrata, a bez poznavanja kriptografskog ključa naziva se **kritoanaliza**, a lice koje se bavi metodama za razbijanje šifri je **kriptoanalitičar**.
Na osnovu prikazanog modela kriptografskog sistema zaključujemo da je za proces sifrovanja i dešifrovanja potrebno raspolagati određenim kriptografskim algoritmom i kriptografskim ključem. Pored toga zaključujemo i da je neophodno da obe strane komunikacije moraju posedovati isti kriptografski ključ, tako da je neophodno obezbediti i tajnu distribuciju ključa do svih učesnika u komunikaciji.

Kriptografski algoritam predstavlja skup pravila koji se koristi za šifrovanje i dešifrovanje. Kriptografski algoritam funkcioniše u kombinaciji sa kritografskim ključem. Snaga kriptozaštite podataka zavisi od snage kriptografskog algoritma i tajnosti kriptografskog ključa.

Za funkcionisanje kriptografskog sistema pored kriptografskih algoritama i ključeva neophodni su i kriptografski protokoli. **Kriptografski protokoli** predstavljaju skup pravila koja razumeju i poštuju sve strane u komunikaciji radi definisanja komunikacionog okvira između strana u komunikaciji, odnosno definisanja algoritma, ključa i drugih kriptoloških parametara, a u cilju obezbeđenja usluga poverljivosti, integriteta i neporecivosti.

7.4 Analiza napada i pretnji

Napadi predstavlja pokušaj napadača da uđe u sistem ili preuzme kokntrolu nad sistemom korišćenjem raznih metoda, u nameri da dođe do osetljivih podataka radi uništenja ili promene, da nanese štetu sistemu ili da onemogući pristup sistemu drugim korisnicima. Osnovne mete napada predstavljaju mrežni uređaji, komunikacioni kanali i krajnji korisnici. Napadi na podatke koji se prenose telekomunikacionom mrežom mogu se podeliti u dve osnovne grupe:

- **pasivni napadi** – podrazumevaju napade koji se odnose na prisluškivanje i nadgledanje podataka bez njihove izmene. Ovim napadima se na relativno jednostavan način dolazi do potrebnih podataka. Pasivni napadi se teže otkrivaju od aktivnih napada jer ne dolazi do promene poruka
- **aktivni napadi** – podrazumevanju napade koji se odnose na promenu toka ili sadržaja poruke. Obuhvatajau modifikacije paketa podataka koji se kreću putem mreže, slanje lažnih paketa, prekidi toka. Aktivni napadi su komplikovaniji od pasivnih napada o lakše se otkrivaju.

Napadi na kriptografski system obuhvataju napade namenjene za razbijanje šifri, dekodiranje, zaobilaženje sistema autentifikacije I razotkrivanjem kriptografskih protokola I predstavljaju tehnike kriptoanalize. Kriptoanaliza je naučna disciplina koja proučava postupke otkrivanja otvorenog teksta bez poznavanja ključa, te postupke otkrivanja ključa uz poznavanje otvorenih i/ili šifrovanih tekstova, ili uz poznavanje nekih informacija o otvorenim i/ili šifrovanim tekstovima.

Razlicite tehnike kriptoanalize nazivaju se napadi koji mogu biti:

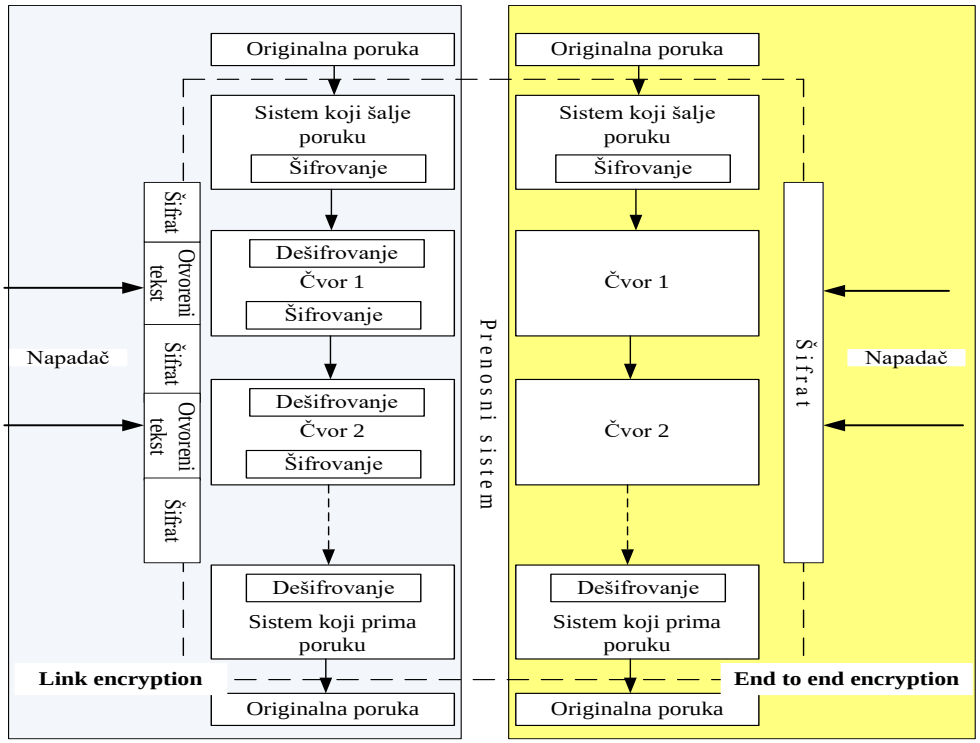
- napad poznatim šifrovanim tekstom – kada kriptoanalitičar ima primenjeni kriptografski algoritam i šifrovane tekstove šifrovane tim algoritmom
- napad poznatim otvorenim tekstom – kada kriptoanalitičar ima deo šifrovanog teksta i odgovarajući otvoreni tekst tih šifrovanih delova.
- napad odabranim otvorenim tekstom – kada kriptoanalitičar ima deo šifrovanog teksta i odgovarajući otvoreni tekst tih šifrovanih delova i kada pored toga kriptoanalitičar bira otvoreni tekst koji će biti šifrovan
- napad odabranim šifrovanim tekstom – kada kriptoanalitičar ima odabrani šifrovani tekst i na neki način ga dešifruje da dobije odgovarajući otvoreni tekst.

Napadi i pretnje na mrežu za upravljaje telekomunikacionim sistemom ogledaju se u težnji napadača da primenom pasivnih i aktivnih napada dođe do podataka koji se nalaze u bazama podataka mreže za upravljanje, da izvrši promenu podataka i određena preusmeravanja telekomuniakcionih kapaciteta u skladu sa svojim potrebama, ili da resurse telekomunikacionih sistema učini preopterećenim i na taj način nedostupnim korisnicima usluga. Motiv za takvu vrstu napada mogu biti različite prirode u zavisnosti od namene telekomunikacionog sistema, od ličnih interesa, preko dobijanja finansijske dobiti, špijunaže diplomatskih i vojnih organizacija, industrijske špijunaže do napada za potrebe terosrističkih i pobunjeničkih napada.

8 KRIPTOLOŠKI ALGORITMI

Savremeni komunikacione mreže teže da svojim korisnicima usluga pruže zaštićeni prenos podataka, u cilju zaštite ličnih i poslovnih tajni od neovlašćenih osoba. Zaštita podataka u komunikaciji između dve učesničke strane podrazumeva formiranje zaštićenog komunikacionog kanala. U zavisnosti koji deo komunikacionog kanala se štiti postoje dve vrste zaštite (slika 8.1):

- **zaštita linkova (*link encryption*)** – podrazumeva zaštitu kompletnog saobraćaja na linkovima realizovanim između dve tačke. Ovom vrstom zaštite šifrovanje se realizuje na prvom i drugom sloju OSI referentnog modela i onemogućava praćenje rutiranja saobraćaja od strane naopadača. Na svakom realizovanom linku koji se štiti koristi se poseban ključ. Ova vrsta zaštite jednostavniju distribuciju kriptoloških ključeva i transparentnost sistema za korisnike komunikacione mreže, ali zbog mogućnosti ugrožavanja bezbednosti sistema ukoliko u mrežnim čvorovima dođe do preusmeravanja na nezaštićene linkove, svi linkovi se moraju zaštititi što povećava finansijske izdatke za realizaciju i održavanje zaštite sistema
- **zaštita sa kraja na kraj (end to end *encryption*)** – podrazumeva za štitu na kompletnom putu između dve tačke u komunikaciji. Ovom vrstom zaštite šifrovanje se vrši na svim nivoima OSI referentnog modela. Prilikom šifrovanja ne šifruju se servisne informacije i zaglavlja poruka, što napadaču omogućava da stekne uvid u rutiranje i izvrši analizu saobraća, što mu omogućava lakši postupak kriptoanalize. Prednost ove vrste zaštite je što se podaci dešifruju samo na krajnjim tačkama komunikacije.



Slika 8.1. Tipovi zaštite komunikacija

Kombinacija ove dve vrste zaštite predstavljala bi nabolje rešenje jer bi time prednosti ove vrste zaštite bile iskorišćene, dok bi se nedostaci neutralizovali. Zaštita informacija predstavlja jedan od osnovnih uslova u savremenim poslovnim, a sve

više i personalnim, komunikacionim uslugama koje pružaju davaoci uluga komunikacija. Kriptografija predstavlja osnov za obezbeđenje zaštite podataka, odnosno glavin uslova da podaci prilikom prenosa komunikacionim mrežama budu tajni. Da bi se postigla tajnost podataka neophodno je realizovati proces šifrovanja podataka. Moderno šifrovajne podrazumeva proces matematičkih tansformacija, koje poruke u vidu numeričkih elemenata transformišu iz razumljivih u potpuno nerazumljive poruke, i obrnuto u procesu dešifrovanja. Skup pravila koji se koristi za realizaciju ovih matematičkih transformacija prilikom šifrovanja i dešifrovanja jesu kriptografski algoritmi. Za realizaciju šifrovanja i dešifrovanja pored postojanja kriptografskog algoritma neophodno je i postojanje kriptografskog ključa.

Kriptografski algoritami zasnovani na ključu mogu se podeliti u tri vrste:

- Simetrični kriptografski algoritmi
- Asimetrični kriptografski algoritmi
- Hibridni kriptografski algoritmi

Da bi se obezbedila što bolja zaštita podataka kriptografski algoritam mora da obezbedi sledeđe uslove:

- vreme potrebno za probijanje algoritma mora da bude duže od vremena koje je potrebno da podaci budu tajni
- cena probijanja algoritma mora da bude veća od cene šifrovanih podataka
- broj šifrovanih podataka sa jednim ključem mora da bude manji od broja potrebnih podataka da se sloritam probije

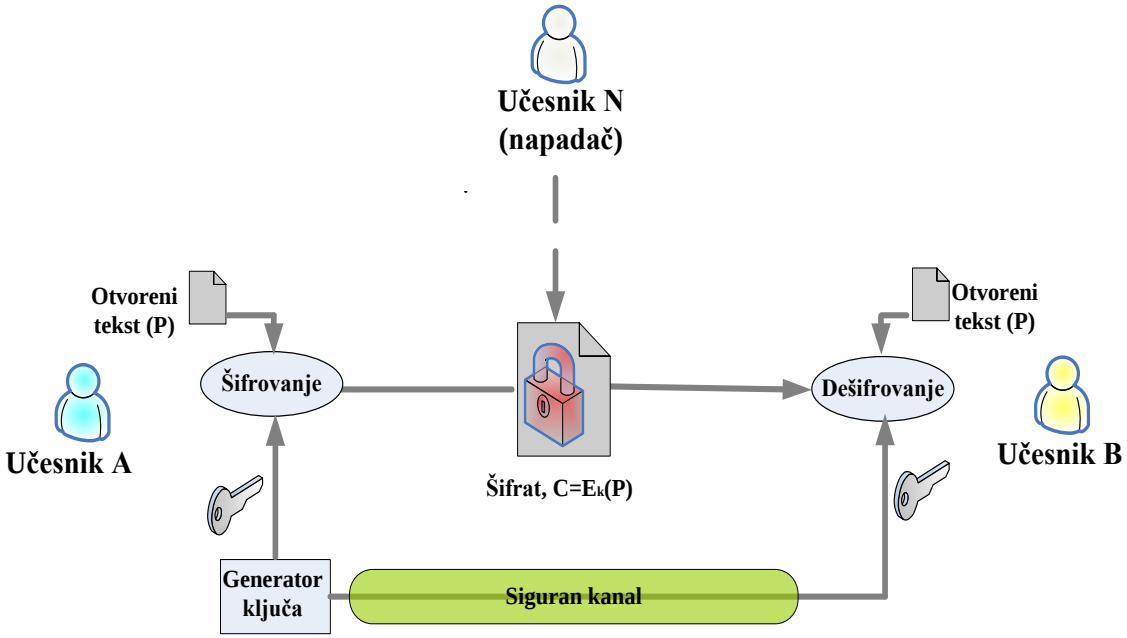
Jedan od uslova kojem se teži prilikom izrade kriptografskog aloritma jeste i da su proces šifrovanja i dešifrovanja inverzni, čime se postiže kopatibilnost operacija šifrovanja i dešifrovanja, a vreme izvršavanja tih operacija se skraćuje.
Moderni kriptografski algoritmi, zasnivaju se kao i stari kriptografski sistemi na postupcima supstitucije i transpozicije, ali je zbog razvoja računarske tehnike proces šifrovanja i dešifrovanja daleko složeniji i brži u odnosu na šifrovaje sa mehaničkim uređajima

8.1 Simetrični kriptografski algoritmi

Simetrični kriptografski algoritmi predstavljaju vrstu kriptografskih algoritama koji za šifrovanje i dešifrovanje koriste isti ključ. Na slici 8.2 je prikazan model simetričnog algoritma. Otvoreni tekst od strane pošljaoca poruke nezaštićenim komunikacionim kanalom treba da bude poslata primaocu, najpre dolazi u blok za šifrovanje. U ovom bloku se uz korišćenje kriptografskog algoritma i kriptološkog ključa dobijenog iz generatora ključa vrši šifrovanje i nastaje šifrat.

Na prijemnoj strani šifrat najpre dolazi u blok za dešifrovanje gde se uz korišćenje kriptografskog algoritma i kriptološkog ključa dobijenog iz generatora ključa vrši dešifrovanje i kao rezultat se ponovo dobija otvoreni tekst poruke koji se nakon toga distribuira primaocu.

Ukoliko napadač dođe u posed šifrata isti može dešifrovati i u upoznati se sa sadržajem poruke ukoliko dođe u posed kriptološkog ključa. Iz tog razloga ključe se nikad ne prenosi nezaštićenim komunikacionim kanalima, već se taj prenos obavlja u tajnosti i preko zaštićenih komunikacionih kanala.



Slika 8.2. Model simetričnog kriptografskog algoritma

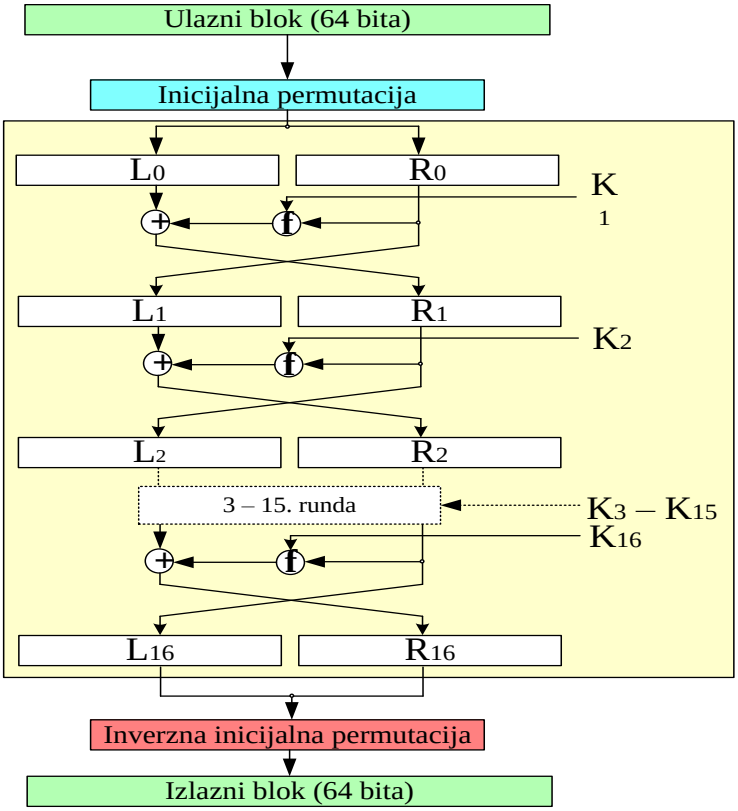
Simetrični kriptografski algoritmi se mogu svrstati u dve grupe:

- **sekvencijalni simetrični kriptografski algoritmi** – predstavljaju algoritme zasnovane na generatorima pseudeslučajnih nizova za čiju se inicijalizaciju koris tajni ključ relativno male dužine. Generisani pseudoslučajni niz ima statističke karakteristike slične karakteristikama pravih slučajnih nizova, sa tim što se pseudoslučajni nizovi ponavljaju posle odgovarajuće periode vremena dugog trajanja. Najčešće se realizuju hardverski i pogodni su za korišćenje u uslovima prenosa lošijeg kvaliteta, jer nemaju propagaciju greške.
- **blokovski simetrični kriptografski algoritmi** – predstavljaju algoritme koji prilikom šifrovanja vrši podela otvorenog teksta na blokove fiksne i zadate dužine (34,126, 192, 256) u bitovima, koji se nakon toga nezavisno šifruju

Najpoznatiji simetrični kriptografski algoritmi su: DES, 3DES, DES-CBC, IDEA, RC5, RC6, AES i drugi.

8.1.1 DES algoritam

Data Encryption Standard (DES) predstavlja jedan od najpoznatijih simetričnih kriptografskih algoritama. Nastao je sedamdesetih godina prošloga veka od strane IBM, a na inicijativu američkog Nacionalnog biro za standarde (engl. *National Bureau of Standards* - NBS) koji pokrenuo je program za zaštitu računarskih i komunikacionih podataka. DES je razvijen od strane IBM i predstavlja simetrični i blokovski orjentisan algoritam i zasnovan je na Feistelovoj šifri, kao i gotovo svi simetrični blokovski algoritmi koji su danas u upotrebi koriste ideju koju je uveo Horst Feistel 1973. godine. Jedna od glavnih ideja je alternativna upotreba supstitucija i transpozicija. DES je prihvaćen kao standard i uveden u operativnu upotrebu 1976. godine.



Slika 8.3. Algoritam DES

Prilikom dizajna DEA-a uvedena su dva principa:

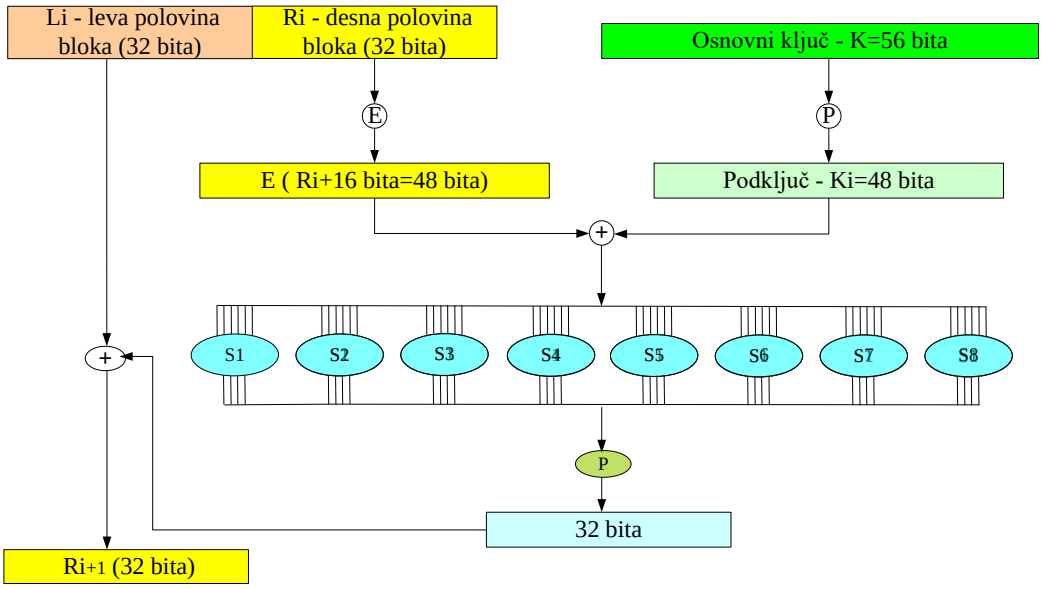
- **princip konfuzije** – prema kome šifrat treba da zavisi od otvorenog teksta i ključa na složen način
- **princip difuzije** – prema kome svaki bit šifrata treba da je u funkciji svih bitova otvorenog teksta i svih bitova ključa

Pored ova dva principa prisutan je i lavinski efekat koji podrazumeva da male promene ulaza treba da izazovu velike promene izlaza. Kod DES-a promena jednog bita ključa ili jednog bita od 64 bita otvorenog teksta 50% bita bloka šifrata.

Dužina ključa je 64 bita, od kojih 8 bitova ključa odbacuje, tako da je efektivna dužina ključa 56 bita. Kako je dužina ključa 56 bita ukupan broj mogućih ključeva je 2^{56}. U ovom algoritmu postoje tri osnovna koraka: inicijalna permutacija (IP), 16 rundi obrade podataka (proširenje, XOR sa podključem, supstitucija), završna inverzna permutacija (IP^{-1}).

Prvi korak DES algoritma (slika 8.3) jeste inicijalna permutaciju (IP). U ovom koraku se bitovi ulaznog bloka dužine 64 bita permutuju nekom permutacijom IP, prema unapred određenoj tablici. Nakon toga se ulazni blok podeli na dva dela od po 32 bita i formira se levi Li i desni Ri blok.

Nakon toga sledi 16 rundi obrade podataka zasnovanih na Fejstelovoj mreži (slika 8.4). Nad desnim blokom se obavlja funkcija F(Ri,Ki), gde je Ri desnih 32 bita, a Ki je 48-bitni ključ koji se generiše iz zadatag tajnog ključa šifrovanja.



Slika 8.4 Operacije u jednoj rundi DES

Nad desnom polovinom podataka Ri se u E-kutiji vrši permutacija proširenja (expansion permutation), pri čemu se proširuje desna polovina podataka (u svakoj rundi) time što menja redosled bitova i ponavlja određene bitove. Svrha permutacije proširenja je da desnu polovinu dovede na veličinu ključa i da se dobije duži rezultat koji može da se komprimuje za vreme operacije supstitucije.
Posle proširenja desna polovina podataka se kombinuje sa 48 bitova pomerenog i permutovanog ključa pomoću operacije XOR, šalje kroz 8 S-kutija (supstitution boxes) gde se vrši supstitucija. Svaka S-kutija ima 6-bitni ulaz i 4-bitni izlaz, a postoji 8 S-kutija u koje ulazi osam 6-bitnih podblokova ulaznog 48-bitnog bloka. Svaka S-kutija ima 4 reda i 16 kolona. Ulazni bitovi definišu jedan element u S-kutiji na način da se kombinuju 1. i 6. bit i daju 2-bitni broj (od 0 do 3) koji odgovara jednom redu tabele, a kombinovani 2-5 ulazni bit daju 4-bitni broj (od 0 do 15) koji odgovara jednoj koloni tabele. Broj na datoj poziciji S-kutije (dobijenoj ukrštanjem) predstavlja izlazni 4-bitni podblok. Osam S-kutija daje osam 4-bitnih blokova čijom se kombinacijom dobija izlazni 32-bitni blok. Supstitucija pomoću S-kutija predstavlja najznačajniji je korak DES-a jer je jedina nelinearna operacija u algoritmu zbog čega se njegova sigurnost, najviše zasniva na ovoj operaciji.
Nakon koraka supstitucije sledi permutacija pomoću P-kutije, koja predstavlja pravu permutaciju, bez komprimovanja ili proširenja. Permutacijom ulaznog 32-bitnog bloka dobija se izlazni blok iste dužine.
Ovim postupkom se završava f funkcija u jednoj rundi i vrednost dobijena operacijom XOR između vrednosti funkcije F i levih 32 bita podataka, postaje Ri + 1, tj. desnih 32 bita za sledeći korak iteracije. Li + 1 za slijedeći korak je Ri.
Može se zaključiti da DES algoritam u današnje doba ima ograničenje zbog 56-bitne dužine ključa, koja mu u doba savremene računarske tehnike ne pruža veliku sigurnost tako da se ređe koristi. Napad na DES algoritam i dalje se zasniva na isprobavanju svih mogućih kombinacija kojih ima 2^{56} (7.2×10^{16}). Majkal Viner je 1993. godine pokazao da je uz određena finansijska ulaganja moguće napraviti hardver za razbijanje DES algoritma za 35 sati sa budzetom od 100.000 dolara, za 3.5 sata sa budzetom od 1 milion dolara i za 21 minut sa budzetom od 10 miliona dolara.

Vrednost DES algoritma ima pre svega veliku istorijski vrednost, jer predstavlja prvi značajniji algoritam svoje vrste i predstavlja pokretač za razvoj savremene kriptografije sa simetričnim algoritmima.

8.1.2 3DES algoritam

Trostruki DES algoritam (Triple DES) je šifarski standard koji je imao namenu da pojača standardni DES algoritam. Ovaj algoritam je baziran na DES algoritmu i koristi koristi 2 ili 3 različita DES ključa. Prvi ključ se koristi za šifrovanje bloka podataka izvorne poruke, nakon čega se ta šifrovana poruka dešifruje drugim ključemi i na kraju se nova šifrovana poruka ponovo šifruje trećim ili opet prvim ključem. Ovim se povečava broj kombinacija koje bi eventualni napadač morao da isproba otkrio ključ. Ovaj unapređeni DES algoritam se najčešće koristi kod aplikacija koje se koriste na internetu i jos uvek je popularan, ali će mu se popularnost i zastupljenost u sistemima smanjivati usavršavanje AES algoritma. 3DES rešava problem povećanja dužine ključa, ali je znatno sporiji od standardnog DES algoritma i to najmanje dva puta.To je i jedan od razloga zašto je raspisan konkurs za AES kriptološki algoritam.

8.1.3 AES algoritam

Prestankom sigurnosti u jačinu DES algoritma razvila se potreba za novim kriptološkim algoritmom. Američki prestao NIST (engl. The National Institute of standards and Technology) raspisuje 1997. godine javni konkurs za novi kriptološki standard. Uslovi konkursa zahtevali su da standard zadovoljva sledeće karakteristike:

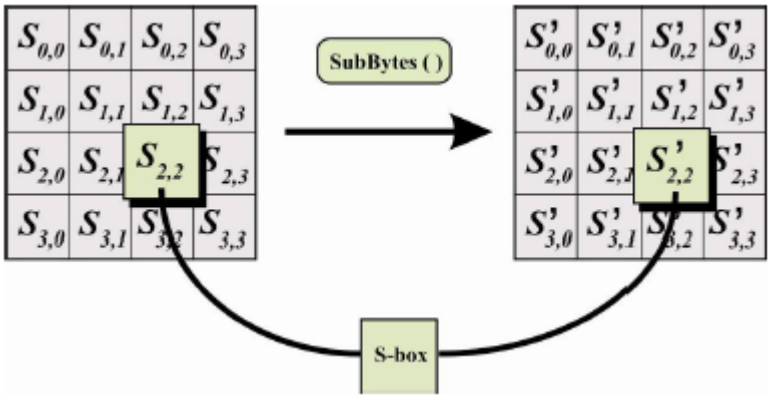
- da bude simetrični blokovski algoritmi sa javnim kodom,
- da podržava veličine bloka od minimalno 128 bita i
- da podržava veličine ključa od 128, 192 i 256 bita.

Pobednik konkursa algoritam RIJNDAEL, belgijskih kriptografa Joana Daemena i Vincenta Rijmena, koji je modifikovan 2000. godine i nazvan AES (Advanced Encryption Standard) i od novembra 2001. godine postaje zvanična zamena za DES. AES predstavlja algoritam sa dužinom bloka otvorenog teksta 128, 192 i 256 bitova. Dužina ključa je promenljiva i može biti 128, 192 i 256 bitova. U zavisnosti od dužine ključa i veličine bloka broj rundi je promenljiv i kreće se od 10 do 16 rundi.

Nakon formiranja matrice stanja koja se formira na osnovu dvodimenzionalne matrice ulaznih brojeva nastale od grupa nastalih od početnih blokova otvorenog teksta (na primer za 128-bitni ulazni blok otvorenog teksta formiraju se 4 grupe od po 4 bajta).

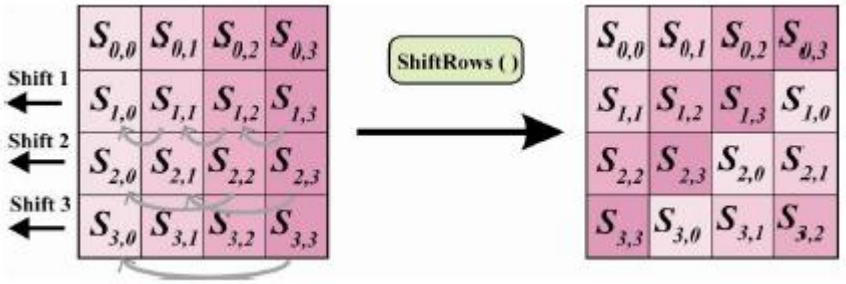
Nakon toga se u svakoj rundi koriste četiri funkcije:

- nelinearni sloj (*ByteSub*)
- sloj linearnog mešanja (*ShiftRow*)
- nelinearni sloj (*MixColumns*)
- dodatni sloj ključa (*AddRoundKey*)



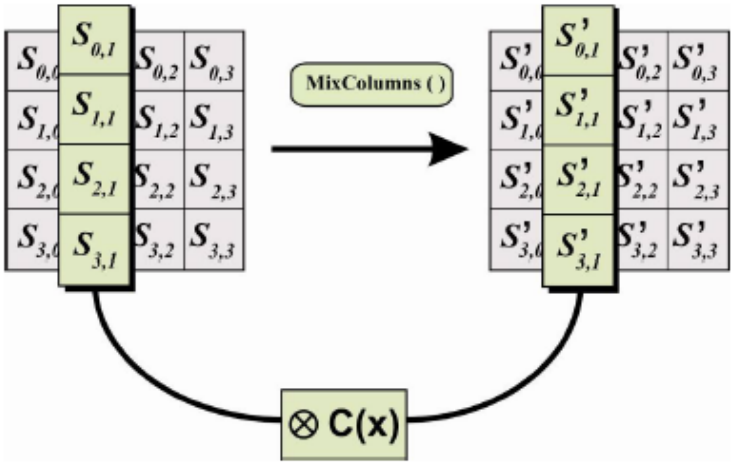
Slika 8.5 AES operacija ByteSub

Zamena bajtova (*ByteSub*), prikazana na slici 8.5, predstavlja operaciju supstitucije koja se obavlja nad svakim bajtom iz matrice stanja tako što se svaki element menja sa elementom iz pomoćne lookup tabele odnosno S-box-a.



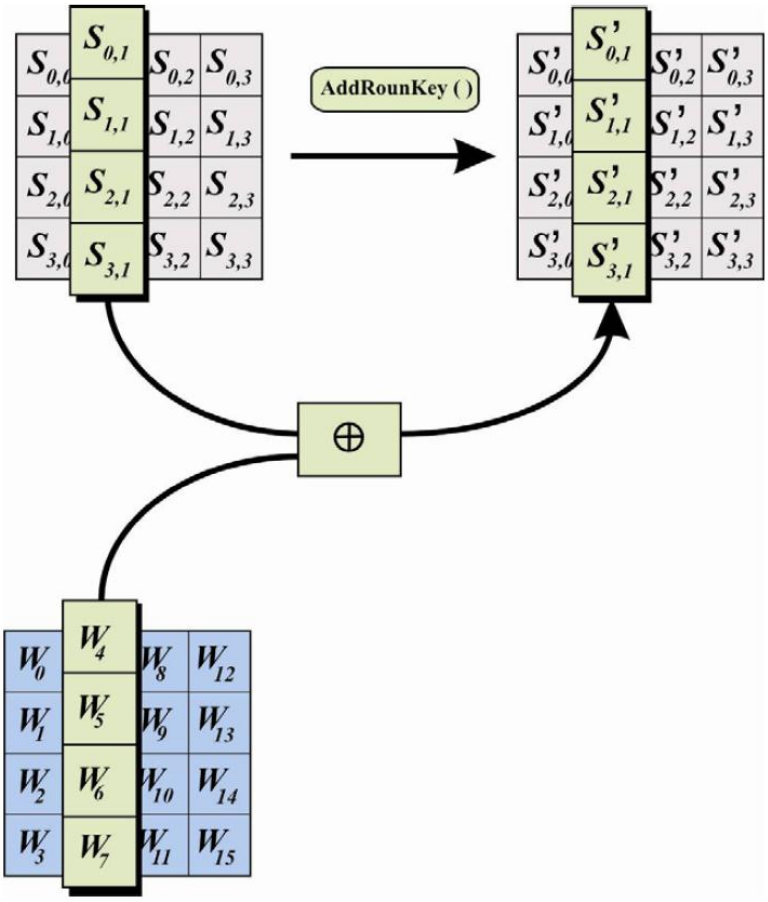
Slika 8.6 AES operacija ShiftRows

Pomeranje bajtova (*ShiftRows*), prikazano na slici 8.6, predstavlja operaciju pomeranja elemenata (bajtova) u okviru kolona za određeni broj pozicija. Prilikom pomeranja prva kolona ostaje nepromenjena, dok se svaka sledeća kružno se pomera i to: druga kolona za po jedno mesto ulevo, treća za po dva mesta ulevo i dalje po istom principu.



Slika 8.7 AES operacija MixColumns

Mešanje podataka u kolonama (*MixColumns*), prikazano na slici 8.7, predstalja operaciju kojom se primenjuje korišćenje određene linearne transformacije nad svakom kolonom iz matrice stanja.



Slika 8.8 AES operacija AddRoundKey

Dodavanje podključa (*AddRoundKey*), prikazano na slici 8.8, predstavlja operaciju se odnosi na XOR operaciju nad matricom stanja i matricom ključeva.

AES predstavlja iterativnu blokovsku šifru, koji nije Fejstel šifra. AES operacije da bi se dešifrovale moraju biti povratne i AES algoritam ima složenu matematičku stukturu. Te njegove karakteristike ga čine ga otpornim na napade. AES je prilično brz algoritam i implementiran je na mnogim procesorima i pametnim karticama.

8.1.4 Prednosti i mane simetričnih kriptografskih algoritama

Osnovne prednosti simetričnih kriptografskih algoritama su:

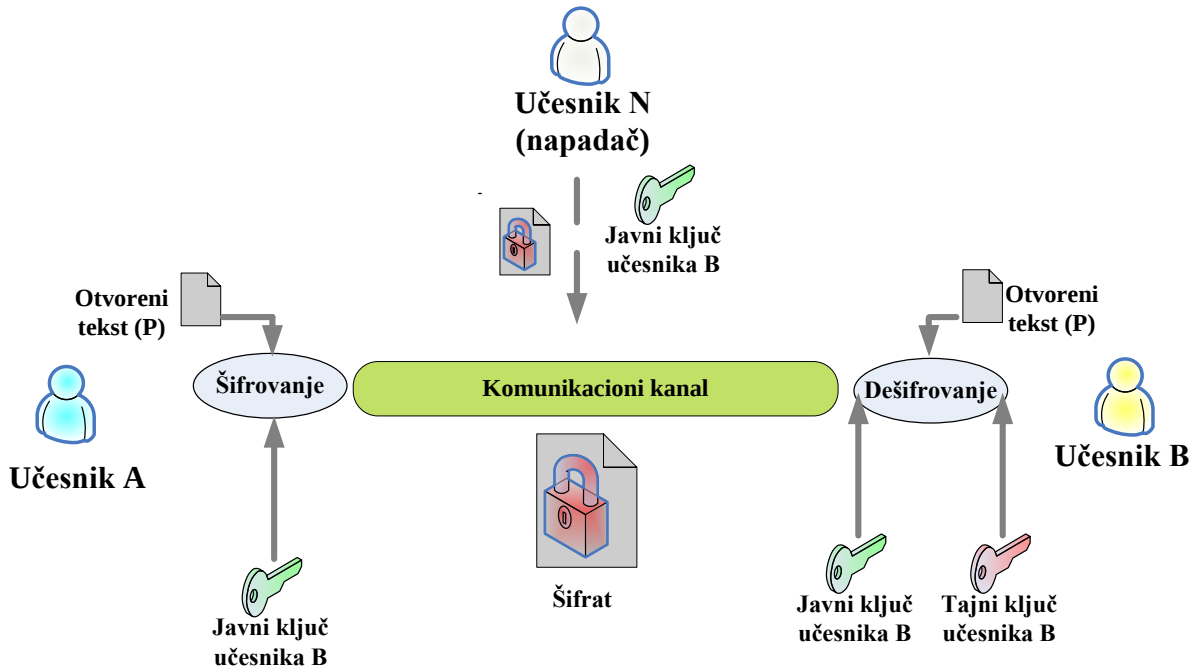
- Visoka efikasnost što se ogleda u kratkom vremenu šifrovanja poruka.
- Kratko vreme šifrovanja poruka prizilazi iz upotrebe kratkih ključeva pa se zbog toga ova vrsta algoritama koristi za šifrovanje poruka velike dužine.

Osnovne nedostaci simetričnih kriptografskih algoritama su:

- distribucija ključeva jer oba korisnika u komunikaciji moraju imati isti ključ a često su fizički razdvojeni na velikim udaljenostima. Da bi razmenili ključeve moraju da dodju u neposredan kontakt ili moraju da koriste neki zaštićen kanal da bi sigurno razmenili ključeve a taj zaštićen kanal praktično ne postoji
- veliki broj potrebnih ključeva jer ako imamo N ljudi koji žele da koriste ovu metodu kriptovanja, to zahteva N(N – 1)/2 simetričnih ključeva. Na 1000 korisnika potrebno je 499500 ključeva.

8.2 Asimetrični kriptografski algoritmi

Asimetrični kriptografski algoritmi predstavljaju vrstu kriptografskih algoritama koji za šifrovanje i dešifrovanje koriste dva različita ključa. U asimetričnoj kritografiji koja se naziva i kritografija sa javnim ključem postoje dva kluča – javni i privatni ključ. Privatni ključ se čuva u tajnosti, a javni može biti pružen mogućim pošiljaocima ili potpuno pušten u javnost. Na slici 8.9 je prikazan model asimetričnog algoritma. Otvoreni tekst od strane pošljaoca poruke učesnika A nezaštićenim kounikacionim kanalom treba da bude poslata primaocu učesniku B. Napadač je učesnik N koja želi da neovlašćeno dođe do podataka. Učesnik A prilikom slanja poruke šifruje poruku javnim ključem učesnika B, koji je javan i poznat je svima, čak i učesniku N. Učesnik B po prijemu šifrata koji je šifrovan javnim ključem učesnika B dešifruje šifrat svojim privatnim ključem. Ova dva ključa su matematički povezani, ali privatni ne može biti otkriven preko javnog.



Slika 8.9 Model asimetričnog kriptografskog algoritma

Na ovaj način poruka je zaštićena od trećeg lica koji je prilikom presretanja šifrovane poruke onemogućen u njenom dešifrovanju jer mu je za to potreban ključ koji se čuva u tajnosti kod ciljnog sagovornika. Glavne mane ovog kriptovanja su njegova sporost i neprikladnost za šifrovanje velikih količina podataka. Takođe, ostaje otvoreno

pitanje autentičnosti poruke, odnosno kako da učesnik B bude sigurna da je poruku koju je primio stvarno poslao učesnik A. Najčešće se koriste sledeći asimetrični algoritmi: RSA (eng. Rivest-Shamir-Adleman), Diffie-Hellman, ElGamal, Eliptic Curves, Rabin i drugi.
Pored uobičajenog kriptovanja poslatih poruka i razmenu ključeva, asimetrična kriptografija se koristi i za digitalne potpise: određena poruka može biti potpisana privatnim ključem, a svi koji je prime mogu, pomoću javnog ključa, utvrditi da li je poruka poslata od pravog učesnika i da li je nepromenjena.

8.2.1 Rivest-Shamir-Adleman (RSA) asimetrični kriptološki algoritam

Rivest-Shamir-Adleman (RSA) asimetrični kriptološki algoritam nastao je 1977. godine na MIT (Massachusetts Institute of Technology) univerzitetu od strane tvoraca algoritma Ronalda Rivesta (Ron Rivest), Leonarda Ejdlmana (Leonard Adleman) i Adi Šamira (Adi Shamir), tako da naziv aloritma RSA predstavlja akronim njihovih prezimena.
RSA algoritam je asimetrični kriptografski algoritam što znači da ima dva ključa i to javni za šifrovanje i privatni za dešifrovanje. U RSA algoritmu ključnu ulogu imaju veliki prosti brojevi i sigurnost RSA se zasniva na složenosti faktorizacije velikih brojeva. Smatra se da je određivanje orginalne poruke na osnovi šifrata i ključa za šifrovanje ekvivalantno faktorizaciji proizvoda dva velika prosta broja.
Postupak razmene poruka u RSA algoritmu se obavlja u tri koraka:

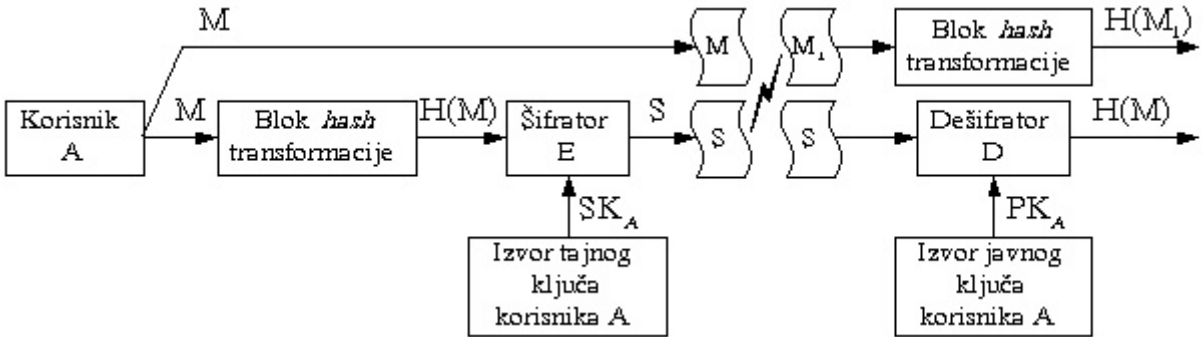
- Prvi korak u RSA algoritmu predstavlja generisanje kljuceva. Tajni ključ predstavlja uređeni par brojeva (N,d). Javni ključ je takođe uređeni par brojeva (N,e). Treba uočiti da je broj N zajednički za oba ključa. Prvo je potrebno izabrati dva prosta broja p i q i izračunati N po formuli N = p x q. Nakon toga se izabira e (mora biti manje od N) tako da e i proizvod (p – 1)(q – 1) budu uzajamno prosti (da nemaju zajedničkog delitelja osim 1). Zatim se određuje broj d tako da zadovoljava jednačinu (e x d) mod [(p – 1)(q – 1)] = 1.
  U datom primeru za izabrane proste brojeve p = 2357 i q = 2551 izračunavaju se N = p x q = 6012707, (p – 1)(q – 1) = 6007800, bira se slučajni broj e = 3113390 i izračunava se d = 3674911.
- Drugi korak u RSA algoritmu predstavlja šifrovanje koje se vrši pomoću jednačine C=Pe mod N, gde je P izvorni tekst koji je prikazan u obliku broja, C broj koji predstavlja šifrovani tekst i brojevi e i N su komponente javnog ključa.
- Treći korak u RSA algoritmu predstavlja šifrovanje koje se vrši pomoću jednačine P = Cd mod N, gde je P izvorni tekst koji je prikazan u obliku broja, C broj koji predstavlja šifrovani tekst i brojevi N i d su komponente tajnog ključa.

Da bi se izvršilo određivanje originalne poruke na osnovu šifrovane poruke i javnog ključa to je ekvivalentno faktorizaciji proizvoda dva velika prosta broja. Ukoliko bi neka osoba C faktorisala broj N i iz toga pronašla proizvod (p – 1)(q – 1) ne može doći u posed broja e, zato što on nema zajedničkog delitelja sa brojem N. Pošto je broj N veoma veliki faktorizacija je skoro nemoguća.
Problemi koji se javljaju u korišćenju RSA aloritama odnose se brzinu šifrovanja i dešifrovanja ovim alogoritmom. Na polju kriptoanalize algoritmi za faktorizaciju su svakim danom sve napredniji tako da, s obzirom na činjenicu da povećanje bezbednosti zahteva povećanje dužine ključa, jer je vreme potrebno za šifrovanje i dešifrovanje proporcionalno trećem stepenu dužine ključa, brzinske karakteristike RSA algoritma su sve lošije. Merenjem performansi RSA algoritma utvrđeno je da je

RSA algoritam 1500 puta sporiji od DES algoritma.(32) Smatra se da je danas 512-bitni RSA algoritam nedovoljan za bezbedno šifrovanje, ali se pretpostavlja se da će 1024-bitni RSA biti bezbedan još petnaestak godina.

8.2.2 Digitalni potpis

Digitalni potpis (*engl. Digital Signature*) predstavlja postupak kojim se određeni segment bloka podataka, ili standardizovane poruke, kriptografski obeležava potpisnikovim tajnim parametrom. Na rešenjima asimetričnih kriptografskim sistema nazira se i tehnika digitalnog potpisa. Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja poruke ili integritet podataka (dokaz da poruka nije promenjena na putu od pošiljaoca do primaoca), kao i da osigura garanciju identiteta pošiljaoca poruke. Osnovu digitalnog potpisa čini sadržaj same poruke. Pošiljaoc primenom određenih kriptografskih algoritama prvo od svoje poruke koja je proizvoljne dužine stvara zapis fiksne dužine (npr. 512 ili 1024 bita) koji u potpunosti oslikava sadržaj poruke. To prakticno znači da svaka promena u sadržaju poruke dovodi do promene potpisa. Ovako dobijen zapis on dalje šifruje svojim tajnim ključem i tako formira digitalni potpis koji se šalje zajedno porukom. Na osnovu digitalnog potpisa primaoca dokumenta može da utvrdi identitet potpisnika dokumenta i obezbeđuje da potpisnik dokumenta ne može da porekne potpisivanje potpisanog dokumenta. Na slici 8.10 predstavljen je postupak potpisivanja elektronskog dokumenta i verifikacija.
Digitalni potpis se može predstaviti izrazom : Digitalni potpis = E(H(M), SA), gdje je I H funkcija sažetka (Hash funkcija), SA tajni ključ potpisnika,E funkcija šifrovanja. Digitalno potpisani dokument se sastoji iz M - digitalnog dokumenta koji se potpisuje i H(M) - otiska digitalnog dokumenta.



Slika 8.10 Potpisivanje elektronskog dokumenta i verifikacija

Postupak kreiranja digitalnog potpisa se sastoji iz dve faze:

- primenom odgovarajuće kriptografske kompresione funkcije (MD5 HASH) određuje se otisak poruke (message digest)
- potpisnik poruke sifruje dobijeni otisak svojim tajnim (privatnim) ključem primjenom odgovarajućeg asimetričnog algoritma (RSA). Šifrovani otisak poruke predstavlja njen digitalni potpis i pridružuje joj se.

Postupak verifkacije digitalnog postupka sastoji se iz 3 faze:

- iz dobijene poruke izdvaja se digitalni potpis i dešifruje se javnim ključem pošiljaoca

- primalac kreira otisak informacionog dela dobijene poruke identičnim postupkom kao na predajnoj strani
- vrši se poređenje i ako je dobijeni otisak poruke identčan sa dešifrovanim otiskom verifiacija je uspešna.

Za kreiranje digitalnog potpisa, danas se najčešće koriste dva sistema: RSA (Rivest,Shamir i Adelman) i DSS (Digital Signature Standard). RSA je asimetrični kriptosistem koji omogućava i kriptografsku zaštitu tajnosti i digitalno potpisivanje dokumenta, dok je DSS namenjen isključivo za digitalno potpisivanje.

8.2.3 Prednosti i mane asimetričnih kriptoloških algoritama

Osnovne prednosti asimetričnih kriptografskih algoritama su:

- rešavanje problema deljenja ključa, koji se javlja kod simetričnih kriptografskih algoritama, gde se ključ razmenjuje između dva učesnika i ne može se koristiti ukoliko jedan od dva učesnika želi da komuniacira sa trećom osobom. Kod asimetričnih kriptografskih algoritama svaki učesnik kreira po dva ključa, jedan privatni (tajni) koji čuva kod sebe, i drugi javni koji se razmenjuje sa drugima. Svaki od entiteta je nezavistan i svoj par ključeva može koristiti u komunikaciji sa bilo kojim učesnicima.
- veliko smanjenje broja ukupno potrebnih ključeva. U sistemu u kome komunicira 1000 korisnika, potrebno je samo 2000 ključeva, dok bi u slučaju korišćenja simetričnog šifrovanja bilo potrebno 499500 ključeva.

Osnovni nedostaci asimetričnih kriptografskih algoritama su:

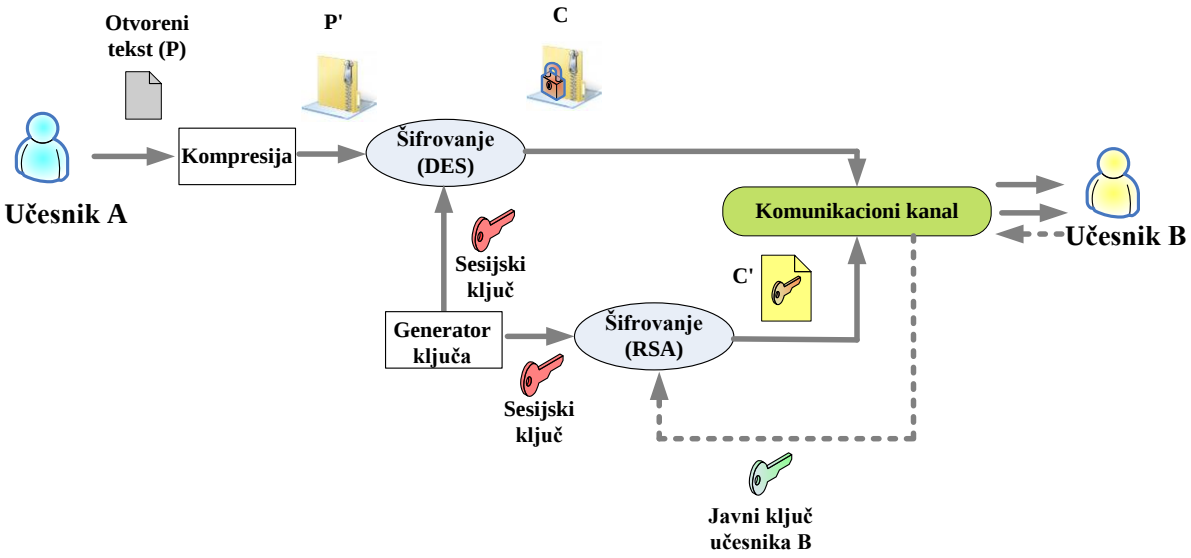
- kompleksnost algoritama koji se koriste prilikom šifrovanja jer algoritmi zbog povećanja bezbednosti koriste velike ključeve prilikom rada i vreme potrebno za šifrovanje asimetričnim kriptografskim algoritmima je veliko. Zbog toga asimetrični kriptološki algoritmi se ne preporučuju za rad sa velikim izvornim podacima i mnogo su efikasniji u radu sa kratkim porukama. Zbog svoje složenosti ova vrsta algoritama nije pogodna za hardversku implementaciju.
- komunikacija između dve strane i javni ključ moraju verifikovati kako ne bi došlo do lažnog predstavljanja os strane neke treće osobe i oticanje podataka

8.3 Hibridni kriptografski algoritmi

Analizom prednosti i nedostataka simetričnih i asimetričnih kriptografskih algoritama može se zaključiti da je najbolje kombinovati prednosti oba kriptografska sistema. Kombinacijom simetričnih i asimetričnih kriptografskih algoritama nastaju hibridni kriptološki algoritmi.
Primer hibridnog sistema predstavlja sistem, koji je 1991. godine formirao Fil Zimerman (*Phill Zimmerman*), pod nazivom PGP (*engl. Pretty Good Privacy*). PGP predstavlja hibridni sistem koji je za svoj rad koristi najbolje osobine simetričnih i asimetričnih kritoloških sistema. Simetrični kriptološki sistemi su brži od asimetričnih, ali problem predstavlja sigurnost distribucije ključa. Ta sigurnost se postiže primenom asimetičnih kriptoloških sistema. Komabinacijom ova dva sistema dobija se brzo šifrovanje sa sigurnim prenosom ključa. Ključ se prenosi šifrovan tako da ga samo osaoba koja ima tajni ključ može dešifrovati.

Princip rada PGP se ogleda u postupku da se poruka prvo šifruje upotrebom ključa (sesijski ključ - session key), a zatim se taj ključ zajedno sa šifrovanom porukom pakuje i ponovo šifruje sa javnim ključem osobe kojoj se šalje poruka. Postupak dešifrovanja cele poruke se ostvaruje obrnutim redosledom operacija tako što osoba koja je primila poruku prvo dešifruje istu sa svojim tajnim kljucem, pronalazi zapakovani sesijski ključ i koristi ga da bi pročitala izvornu poruku. Za generisanje sesijskog ključa koristi se generator pseudo-slučajnog broja u kombinaciji sa raznim korisnikovim unosima u toku procesa generisanja. Sesijski ključ ima jednokratnu upotrebu, jer se koristi da bi se podaci šifrovali simetričnom enkripcijom. PGP zatim šifruje samo privremeni ključ asimetričnom enkripcijom i pridružuje šifrovanim podacima, a ne celu, velika poruka i time se postižu dobre performanse celog sistema.

Na slici 8.11 prikazan je postupak šifrovanja pomoću PGP algoritma. Učesnik A pre slanja poruke P prvo vrši kompresiju pomoću neke od metoda za kompresiju podataka, jer se na taj način ubrzava vreme slanja poruke čime se istovremeno i dobija na zaštiti poruke. Na taj način kompresovana poruka P'se šifruje pomoću nekog od simetričnih algoritama (DES, 3DES ili slično) i sesijskog ključa i na taj način se dobija šifrovana poruka C. Zatim se vrši šifrovanje sesijskog ključa pomoću nekog od asimetričnih algoritama (RSA, ElGamal ili Diffie-Hellman) i javnog ključa učesnika B. Tako nastaje šifrovana poruka C' koja se šalje učesniku B zajedno sa porukom C.



Slika 8.11 Postupak šifrovanja pomoću PGP algoritma

Proces dešifrovanja se obavlja obrnutim redosledom radnji od procesa šifrovanja. Kada primi šifrovanu poruku učesnik B upotrebljava svoj tajni ključ i dešifuje poruku koja sadrži sesijski ključ. Korišćenjem sesijskog ključa učesnik B dešifruje šifrovanu poruku poruku i zatim dekompresuje poruku radi dobijanja izvorne poruke.

PGP aloritam nudi nekoliko stepeni zaštite: niski (koristi 512-bitni ključ), visoki (koristi 768-bitni ključ) i vojni (koristi 1024-bitni ključ. U cilju dokazivanja autentičnosti PGP nudi mogućnost potpisivanja poslatih dokumenata.

9 INTERNET PROTOCOL SECURITY - IPSec

Protokol je skup pravila i konvencija koji definiše komunikacioni okvir između dva ili više učesnika u komunikaciji, koji mogu biti krajnji korisnici, procesi ili računarski sistemi, definišu se skupom pravila koji se naziva protokol. Ukoliko u u komunikaciji deo poruke šifrovan, taj protokol se može smatrati kriptografskim. Kriptografski protokoli se upotrebljavaju za uspostavljanje sigurne komunikacije preko nepouzdanih globalnih mreža i distribuiranih sistema. Dakle, kriptografski protokoli su protokoli koji se oslanjaju na kriptografske metode zaštite kako bi pojedincima i kompanijama obezbedili osnovne sigurnosne usluge poverljivosti, integriteta i neporecivosti.(33) Kriptografskim protokolima se vrši izbor algoritma šifrovanja i dešifrovanja, vrši se izbor ključeva i dogovaraju drugi kriptografski parametri. Protokoli moraju obezbediti osnovne sigurnosne usluge poverljivosti, neporecivosti i integriteta kao i mehanizme za proveru identiteta, autorizaciju i upravljanje ključevima (što uključuje generisanje, čuvanje i razmenu ključeva).

Protokoli pružaju sigurnost na različitim slojevima TCP/IP referentnog modela i zaštita se u odnosu na to može podeliti na:

- zaštita na mrežnom sloju - koja se obezbeđuje se između mrežnih čvorova pri čemu se vrši zaštita IP paketa. Zaštita IP paketa se ostvaruje primenom kriptografskih algoritama (simetrični i asimetrični algoritmi za kriptovanje, heš funkcije, digitalni potpis i drugi). Prednost ovakvog načina ostvarivanja sigurnosti sastoji se u smanjenoj razmeni ključeva jer svi transportni protokoli i aplikacije sada dele infrastrukturu upravljanja ključem koju obezbeđuje mrežni sloj. Prednost predstavljaju i manje potrebe za promenama aplikacija. Najpoznatiji kriptografski protokol na ovom nivou je IPSec protokol.
- zaštita na transportnom sloju – koja se ostvaruje zaštitom tajnosti podataka primenom simetričnih kriptografskih algoritama i proverama identiteta (digitalni potpis, heš funkcije, digitalni sertifikati) strana koje komuniciraju. Prednost ovakvog načina ostvarivanja sigurnosti jeste činjenica da nije potrebno modifikovati svaku aplikaciju. Najpoznatiji kriptografski protokoli koji se koriste na ovom sloju su: SSL, SSH, TLS i WTLS.
- zaštita na aplikacionom sloju – koja se ostvaruje primenom tehnologija poput digitalnog potpisa i zaštita podataka primenom simetričnih kriptografskih algoritama. Prednost ovakvog načina ostvarivanja sigurnosti sastoji se u tome što aplikacija može da se proširi bez oslanjanja na sigurnosne servise koje obezbeđuje operativni sistem. Najpoznatiji kriptografski protokoli koji se primenjuju na ovom sloju su: S/MIME, Kerberos, PGP, i drugi.

9.1 Osnovni koncept IPSec

Potreba za zaštitom podataka dok se transportuju kroz nezaštićenu mrežu je razvojem komunikacionih mreža postajala sve veća. Razvojem Interneta kao globalne nezašićene mreže razvile su se i mogućnosti koje ona pruža za povezivanje i komunikaciju na svim nivoima i za različite potrebe: lične, poslovne, državne i bezbednosne. Upravo taj široki spektar mogućnosti je iskorišćen da Internet mreža postane jedna od najbitnijih komunikacionih mreža i stvorila se potreba za razvojem načina da se prenos podataka kroz ovu mreži zaštiti. Prvobitno IPSec standard je definisan IETF referentnim preporuka RFC 1825 – RFC 1829 koji su oljavljeni 1985. godine. U kasnijem periodu protokol je unapređivan i doživeo je veliki broj promena.

Zadnja verzija protokola je iz decembra 2005. godine i definisan je IETF referentnim preporukama RFC 4301 – RFC 4309. IPSec (Internet Protokol security) je standard i skup protokola (optimalno za IPv4, a obavezan za IPv6) koji obuhvata mehanizme za zaštitu prenosa na mrežnom nivou OSI i TSP/IP referntnih modela šifrovanjem i / ili autentifikacijom IP paketa. IPSec je obavezan za IPv6 a optimalno se korisi za IPv4. IPSec je zadržao kompatibilnost sa postojećim IP protololom što omogućava transparentnost mrežne opreme zasnosvane na IP protokolu, tako da samo dva krajnja učesnika u mreži moraju imati podršku za komunikaciju IPSec protokolom, dok mrežna oprema, kao što su ruteri i svičevi, ne moraju da imaju ovakvu podršku.

IPSec je namenjena da obezbedi sigurnu komunikaciju kroz komunikacione mreže zasnovane na IP protokolu. Za zaštiti poverljivosti, integriteta, autentičnosti i neporecivosti prenošenih podataka, IPSec koristi tri podprotokola, koja se razlikuju po vrsti zaglavlja i podataka i to (34):

- zaglavlje za autentifikaciju – AH (*Authentication Header*)
- enkapsulirani šifrovani podaci – ESP (*Encapsulating Security Payload*)
- zaglavlje za razmenu ključeva – IKE (*Internet Key Exchange*)

Referentne preporuke IETF foruma mogu se podeliti u grupe koje definišu:

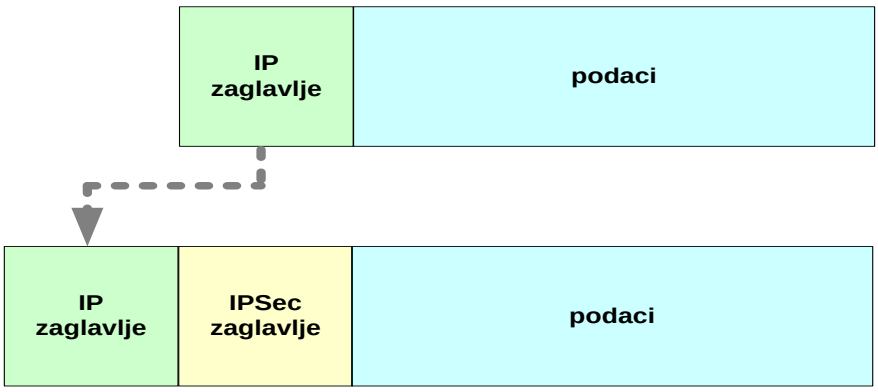
- arhitekturu – pokrivaju osnovni koncept, sigurnosne zahteve, definicije i mehanizme koji definiši IPSec tehnologiju. Trenutna preporuka je RFC 4301 - Security Architecture for the Internet Protocol.
- zaglavlje za autentifikaciju – AH (*Authentication Header*) – pokrivaju AH zaglavlje za obezbeđenje autentifikacije. Trenutna preporuka je RFC 4302 - IP Authentication
- enkapsulirani šifrovani podaci – ESP (*Encapsulating Security Payload*) – pokrivaju ESP zaglavlje za obezbeđenje šifrovanja i kombinaciju šifrovanja i autentifikacije - Trenutna preporuka je RFC 4303 - IP Encapsulating Security Payload (ESP).
- zaglavlje za razmenu ključeva – IKE (*Internet Key Exchange*) – pokrivaju pitanja upravljanja ključevima u IPSec protololu. Osnovna preporuka je RFC 5996 - Internet Key Exchange (IKEv2) Protocol, ali ima puno povezanih RFC preporuka (35)

9.2 Režimi rada IPSec-a

IPSec nezavisno od toga koji vrstu zaštite koriristi može raditi u dva: transportni (*engl. transport mode*) i tunelovanje (*engl. tunnel mode*).

Transportni rezim rada omogućava sifrovanje samo podataka dok IP zaglavlja ostaju u orginalnom obliku, kao otvoreni tekst. Na slici 9.1 je prikazan izgled paketa prilikom transportnog režima rada.

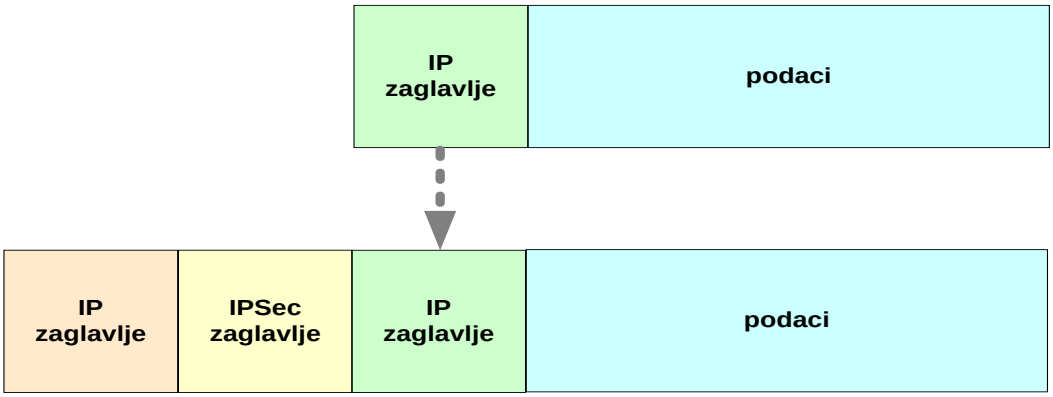
Ovaj režim rada se koristi za komunikaciju kraj-kraj između dva učesnika u komunikaciji (npr. klijent i server ili dve radne stanice). Zaglavlja viših slojeva referentnog modela su šifrovana i mogućnost pregledanja paketa je ograničena.



Slika 9.1 Prikaz paketa prilikom transportnog režima rada

Prednost ovog režima rada je to što se svakom paketu dodaje svega nekoliko okteta. U ovom načinu rada, uređaji (ruteri) mogu na javnoj mreži videti adrese izvorišta i odredišta poruka, što potencijalnom napadaču delimično omogućava da analizira mrežni saobraćaj.

Tunelski režim rada (tunelovanje) je namenjeno za rezim rada koji podrazumeva da se cop IP paket enkapsulira u navi IP paket. Na slici 9.2 je prikazan izgled paketa prilikom tunelskog režima rada. Ovaj režim rada se koristi za komunikaciju kada se nekoliko učesnika ili cela jedna lokalna mreža sakriva se iza jednog čvora te je kao takva nevidljiva ostatku mreže, a samim tim i zaštićena od napada.



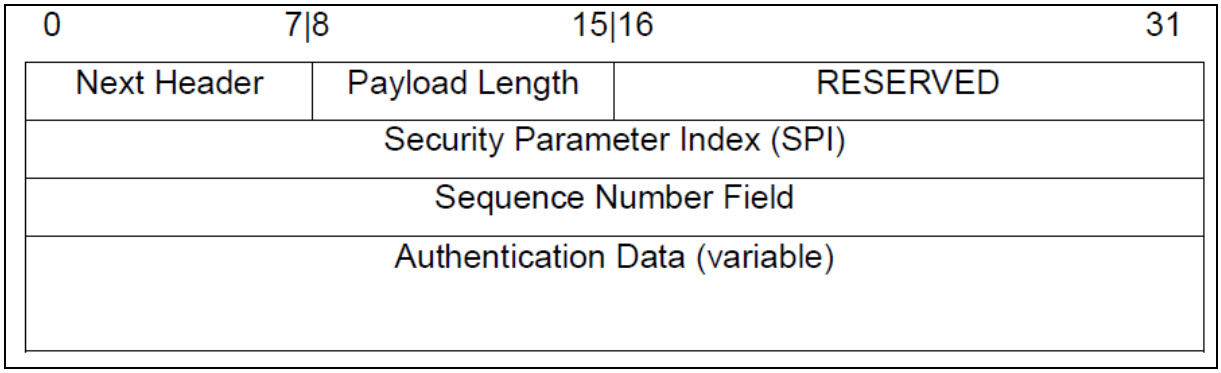
Slika 9.2 Prikaz paketa prilikom tunelskog režima rada

Tunel se sastoji od klijenta i servera koji su tako konfigurisani da koriste IPSec tunelovanje i unapred dogovorene mehanizme za enkapsulaciju i šifrovanje kompletnih IP paketa, što obezbeđuje potpuno siguran prenos preko javnih ili privatnih mreža. Šifrovani podaci se spajaju sa odgovarajućim nešifrovanim IP zaglavljima, formirajući tako IP pakete koji se na kraju tunela dešifriraju i oblikuju u IP pakete namenjene krajnjem odredištu. Prednost ovog režima rada je što onemogućava analizu saobraćaja, dok mu je mana povećanje dužine paketa zbog dodatnog zaglavlja.

9.3 Zaglavlje za autentifikaciju – AH (*Authentication Header*)

AH (Authentication Header) zaglavlje u okviru IPSec je je projektovano da garantuje autentičnost i integritet paketa podataka koji se prenose. Pored toga AH protokol omogućava I zaštitu od ponovljenih slanja istih datagrama. Ovaj protokol korišćenjem neke heš funkcija formira sažetak koji umeće u AH zaglavlje, koje se se kasnije doda

na odgovarajuću lokaciju u paketu, zavisno koji se režim rada koristi (transportni ili tunelski). Na slici 9.3 je prikazano AH zaglavlje.

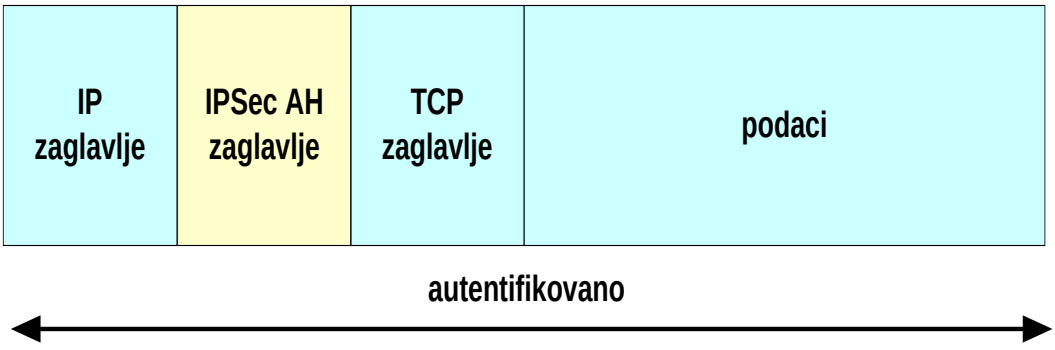


Slika 9.3 AH zaglavlje

Značenje pojedinih polja u okviru AH je sledeće:

- sledeće zaglavlje (*Next Header*) – označava protokol koji se koristi za prenos podataka (TCP ili UDP)
- dužina punjena (*Payload Length*) – polje koje definiše dužinu AH
- rezervisano (*Reserved)* – polje koje se još uvek ne koristi (svi bitovi se ostavljaju na nulu)
- skup sigurnosnih paketa (*Security Parameters Index - SPI*) – polje koje sadrži kombinacije sigurnosnih parametara
- redni broj (*Sequence Number)* – redni broj paketa, a koristi se za zaštitu od "replay" napada (radi se o napadima koji se zasnivaju na uzastopnom slanju istih paketa)
- podaci za proveru identiteta (*Authentication Data*) – polje se koristi za umetanje sažetka poruke u cilju autentifikacije

Prilikom upotrebe AH protokola nema šifrovanje tako da ovaj protokol ne obezbeđuje tajnost poruke. Na slici 9.4 prikazan je AH protokol u IP paketu.

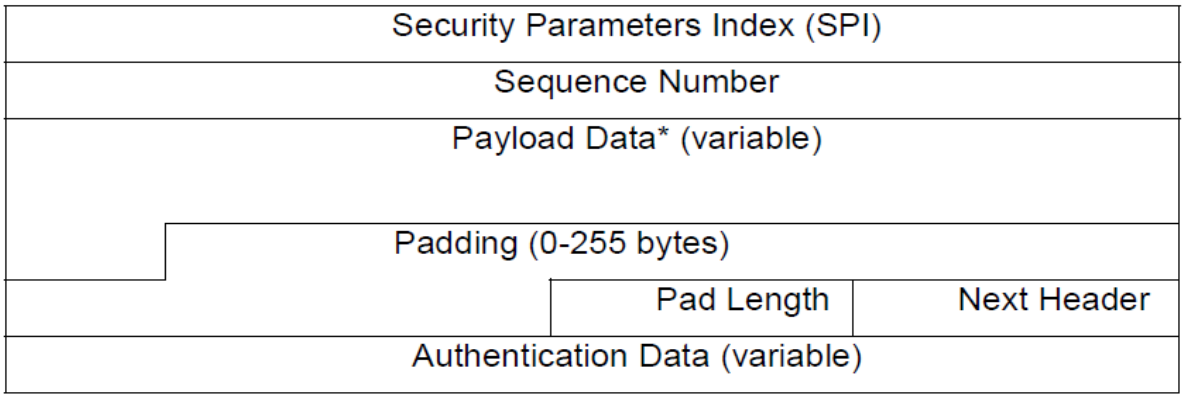


Slika 9.4 AH protokol u IP paket

Kao što se na slici vidi AH u transportnom režimu rada obezbeđuje proveru identiteta, integritet i neporecivost celog IP paketa.

9.4 Enkapsulirani šifrovani podaci – ESP (Encapsulating Security Payload)

Enkapsulirani šifrovani podaci ESP (*Encapsulating Security Payload*) protokol se koristi kada je potrebno očuvati tajnost poruka koje se prenose. Za stvaranje ESP polja podataka koriste se simetrični kriptografski sistemi u sprezi sa metodom digitalnog potpisa. Za minimalni nivo zaštite predložen je 56-bit DES algorita.Na slici 9.5 prikazan je ESP paket.



Slika 9.5 ESP paket

Značenje pojedinih polja u okviru AH je sledeće:

- sledeće zaglavlje (*Next Header*) – označava protokol koji se koristi za prenos podataka (TCP ili UDP)
- skup sigurnosnih parametara (*Security Parameters Index - SPI*) - kombinacija sigurnosnih parametara slično kao i kod AH
- redni broj (*Sequence Number*) - redni broj paketa, koristi se za zaštitu od “replay“ napada
- podaci (*Payload*) – podaci koji se šalju
- dopune (*Padding*) – koristi se za popunu podataka do veličine celog bloka (32 bita).
- dužina dopune (*Padding Length*) – polje označava dužinu Padding polja
- sledeće zaglavlje (*Next Header*) – označava protokol koji se koristi za prenos podataka (TCP ili UDP)
- podaci za proveru identiteta (*Authentication Data*) – polje koje sadrži podatke potrebne za autentifikaciju entiteta i poruke.

Na slici 9.6 prikazan je ESP u IP paketu.



Slika 9.6 ESP u IP paketu

ESP sadrži dva polja: ESP zaglavlje (*ESP heder*) i ESP dopuna (*ESP trailer*). ESP zaglavlje se umeće odmah nakon IP zaglavlja IP poruke a ESP dopuna (veličine 32 bita) se umeće neposredno ispred podataka za autentifikaciju koji se nalaze na kraju poruke.

9.5 Zaglavlje za razmenu ključeva – IKE (Internet Key Exchange)

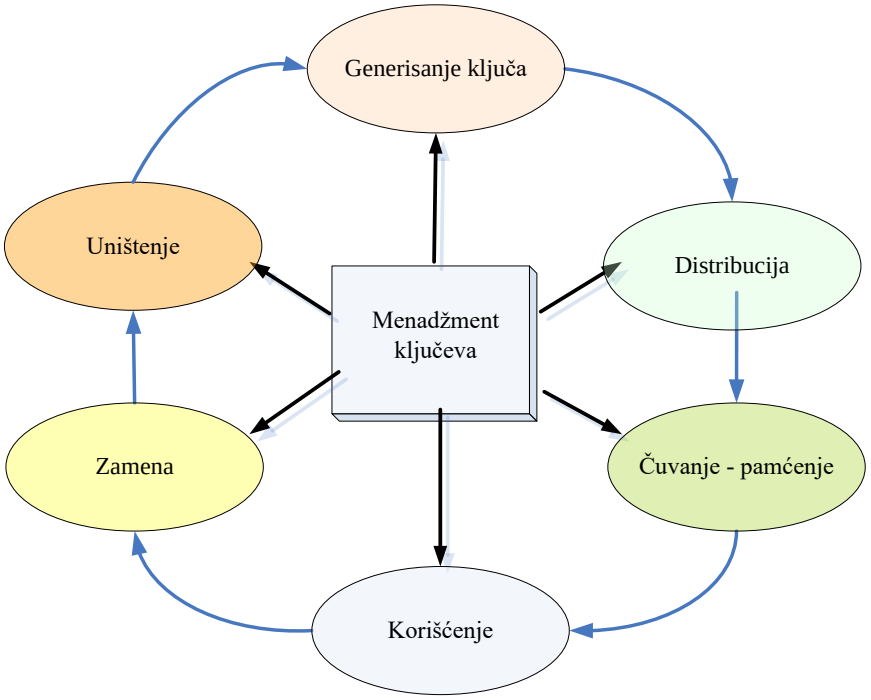
Zaglavlje za razmenu ključeva – IKE (Internet Key Exchange) se koristi u potprotokolu za razmenu ključeva i služi za dogovaranje bezbednosnih parametara IPSec komunikacije i razmenu simetričnih ključeva. Skup pravila koji definiše razmenu ključeva i koje će strane u komunikaciji koristiti za zaštitu međusobnog saobraćajaje je servis bezbednosne asocijacije SA (engl. Security Association). SA sadrži sve sigurnosne parametre potrebne za siguran transport IPSec paketa kroz mrežu. SA su uvek jednosmerne, odnosno koriste se za zaštitu paketa u jednom smeru. Ukoliko je potrebno zaštititi saobraćaj u oba smera, potrebno je posedovati dve SA, i to po jedna na svakoj strani. SA se čuvaju u okviru SA baze podataka SADB (SA Data Base). Skup pravila se čuva u SP (Security Policy). Parametri koji čine SA su: 32-bitni sigurnosni parametar SPI, tip IPSec protokola (AH ili ESP) i izvorna IP adresa.

Sve komunikacije IKE protokola podrazumevaju dve poruke. To su zahtev i odgovor koji se naziva razmenom. Pouzdanost komunikacije je zaduženje strane koja šalje zahtev i ukoliko ne dobije odgovor u određenom vremenskom roku strana koja šalje zahtev dužna je da zahtev ponovi ili prekine konekciju. Prvi par poruka pri uspstavljanju konekcije služi za utvrđivanje parametara zaštićene komunikacije, vremensku sinhronizaciju o razmenu Diffie-Hellman vrednosti. Drugi par poruka razmenjuje identitete učesnika, potvrđuje poznavanje deljene tajne i uspostavlja zaštićenu vezu. Uobičajno se za IKE komunikaciju koristi UDP port (500) i s obzirom da UDP protokol ne nudi pouzdan prenos podataka sam IKE protokol sadrži funkcije za prepoznavanje i rešavanje gubitka paketa, višestruku isporuku istog paketa i falsifikovajne paketa.

Šifarski ključ koji se ugovori IKE protokolom ograničen je vremenskim periodom i količinom podataka koja se šifruje, Nakon isteka jednog od ograničenja konekcija se prekida i ukoliko je potrebno nastaviti sa razmenom podataka uspostavlja se nova zaštićena konekcija.

10 UPRAVLJANJE KRIPTOGRAFSKIM KLJUČEVIMA

Kriptografski ključ predstavlja jedan od najosetljivijih elementata u procesu šifrovanja i dešifrovanja. Ukolliko napadač dođe u posed ključa lakom može da dešifruje šifrat i dođe do optvorenog sadržaja poruke. Upravo zbog toga upravljanje kriptološkim ključevima predstavlja jedan od najbitnijih zadataka u savremenoj kriptografiji. Iako proces kriranja kriptoloških aloritama predstavlja izuzetno težak proces, generisanje kriptografskih ključeva i održavanje njihove tajnosti je još teže. Da bi zaštita jednog šifarskog sistema bila uspešna upravljanje ključevima mora biti što kvalitetnije.
Zadatak procesa upravljanja ključevima jeste generisanje, distribucija i čuvanje ključeva. Od trenutka kada ključ bude generisan do trenutka dok ne bude uništen on mora ostati tajan. U praksi napadač će pre napasti sistem za upravljanje ključevima nego što će pokušati da otkrije zakonitosti po kojima kriptografski algoritam funkcioniše. Upravljanje kriptološkim ključevima se sastoji od 6 faza koje su prikazane na slici 10.1.



Slika 10.1. Faze kriptološkog ključa

Upravljanje kriptološkim ključevima se realizuje kroz:

- Generisanje ključa,
- Dstribuciju ključa do svih učesnika u komunikaciji,
- Čuvanje ključeva,
- Korišćenje ključa,
- Zamena ključa (redovna ili uslučaju deskreditacije ključa koji je uradu)
- Uništenje ključa nakon isteka i u slučaju opasnosti ili eventualno arhiviranje.

10.1 Generisanje ključa

Generisanje ključeva predstavlja početnu fazu u životu jednog kriptološkog ključa. U ovoj fazi upravljanja ključevima dolazi do nastanka ključa. Prilikom generisanja ključeva važan korak predstavlja izbor samog generatora i vliku pažnju treba posvetiti njegovim osobinama i potencijalnim slabostima koje napadač može upotrebiti pri pokušaju razotkrivanja ključa.
Uz pomoć statističkih testova za određivanje osobine generisanog ključa može se zaključiti da većina generatora ne poseduje apsolutnu sigurnost, tj. niz brojeva koje generiše nije slučajan već pseudoslučajan. Pošto ne postoje univerzalni testovi čiji prolaz garantuje da je neki generator potpuno pouzdan, generatori pseudoslučajnih brojeva se konstruišu na osnovu matematičke analize njihovih strukturalnih osobina. Glavni uslov za postizanje sigurnosti generatora jeste dovoljno veliki period. Ulaz u generator mora biti tako odabran da ga je praktično nemoguće otkriti nekom metodom pogađanja. Ovim se omogućava generisanje vrlo velikog broja pseudoslučajnih nizova brojeva koje je nemoguće analizirati u realnom vremenu. Ovako dobijeni nizovi se mogu upotrebiti kao kriptološki ključevi. Ovakvi generatori slučajnih brojeva kod kojih je uz poznavanje algoritma i nepoznavanje početnih uslova nemoguće predvideti niz generisanih brojeva zovu se generatori kriptografskih sigurnih pseudoslučajnih brojeva CSPRNG (Cryptographically secure pseudorandom number generator).(36)
Jedna od najvažnijih karakteristika koja se mora imati u vidu je dužina ključa. Broj mogućih kombinacija za ključ dužine 64 bita je 2^{64}, dok porastom dužine znatno se povećava broj kombinacija koje treba ispitati, a sa time se povećava i vreme potrebno napadaču da realizuje proce kriptoanalize, odnosno povećava se vreme za koje je šifrat siguran. Danas se razvojem računarske snage vrlo lako dolazi do procesora velike brzine tako da je otkrivanje ključeva male dužine, kao što je DES algoritam sa ključem od 56 bita, realna mogućnost i zavisi od želje u finansijskih mogućnosti napadača da dođe do ključa. U okviru RSA algoritma minimalni zahtevi za sigurnost ključa podrazumevaju da je dužina ključa najmanje 512 bita kod istog algoritma, do se za optimalnu dužinu ključa smatra dužina od 1024 bita.

10.2 Distribucija ključeva

Distribucija ključeva predstavlja drugu fazu u procesu upravljanja ključevima, kojom se realizuje dostavljanje ključeva do učesnika koji se nalaze na različitim lokacijama pa je sledeći korak njihova distribucija do učesnika. Prilikom dostavljanja ključa do drugih učesnika po pravilu to dostavljanje se vrši nezaštićenim putem. Da bi ključ ostao siguran, odnosno da ne bi došao u posed osobe koja ne treba da ga poseduje, potrebno je da se ključevi na odredište dostave tajnim kanalom. Da bi ključevi mogli da se koriste treba da budu prenešeni u univerzalnom i za učesnike razumljivom formatu.
Bez obzira koliko je u teoriji kriptografski algoritam siguran, povrljivost njegovog mehanizma može ugroziti problem distribucije ključeva. Pitanje distribucije ključeva može se činiti trivijalnim, ali on je za pouzdan kriptološki sistem najslabija karika. Za dešifrovanje poruke strana B mora posedovati validnu kopiju alata koji je strana A koristila za šifrovanje, ali i ključ kojim je poruka šifrovana. U procesu razmene podataka u bezbednosnom okruženju dve osobe se moraju pouzdati u treću, osobu C, koja će im dostaviti ključ, koji u ovom slučaju postaje slaba karika u lancu bezbednosti. (37)

Način funkcionisanja simetričnih i asimetričnih kritografskih algoritama zahteva različitu upotrebu ključeva, a samim tim i različite načine distribucije ključeva do odredišta što prouzrojuje i različite probleme koji se javljaju prilikom distribucije.

10.2.1 Distribucija ključeva u simetričnim kriptografskim algoritmima

Simetrični kritografski algoritmi pdrazumevaju da obe strane u komunikaciju poseduju isti ključ što predstavlja veliki problem u distribuciji ključeva, posebno ako je broj učesnika veliki. Da bi svaki od učesnika u komunikaciji imao zagarantovanu tajnost komunikacije onda svaki od učesnika u grupi od N korisnika mora da poseduje N-1 ključeva za komunikaciju sa ostalim korisnicima, što dovodi je ukupno potrebno N(N-1)/2 ključeva. Za grupu od 100 korisnika ukupan broj potrebnih ključeva bi bio 4950, a svaki korisnik bi morao da poseduje 99 ključeva. Za grupu od 1000 korisnika ukupan broj potrebnih ključeva bi bio 499500, a svaki korisnik bi morao da poseduje 999 ključeva. Ored velikog broja ključeva koi je nophodan za sve komunikacije i velikog broja ključeva koje jedan učesnik u komunikaciji mora da procesuira, neophodno je obezbediti sigurnu komunikacionu liniju za prenos svih ključeva.

10.2.2 Distribucija ključeva u asimetričnim kriptografskim sistemima

Prednost asimetričnih kriptografskih sistema je da svako može imati svačiji ključ, odnosno da ne postoji potreba za razmenom tajnih ključeva.Ukoliko osoba A želi da pošalje poruku osobi B, potrebno je da zna samo javni ključ osobe B.
Tehnike distribucije ključeva asimetričnim kriptografskim sistemima mogu se realizovati kroz javno objavljivanje ključeva, kroz javno dostupan direktorijum, preko autoriteta za javne ključeve (Public-Key Authority) i korišćenjem sertifikata.(38)
Problem se javlja da prilikom objavljivanja javnog ključa jedne od osoba u komunikaciji, na primer osoba A. Napadač u vidu osobe C tada može da uhvati ključ i da pošalje svoj javni ključ imitirajući osobu B. Nakon toga osoba A prihvata podmetniuti ključ i pomoću koga šifruje poruku i šalje je osobi B. Osoba C umesto osobe B prihvata šifrat i svojim tajnim ključem ga dešifruje i dolazi do sadržaja poruke. Na osnovu ovog primera može se zaključiti da je distribucija ključeva u asimetričnim kriptografskim sistemima složen i bezbednosno osetljiv proces i da je veoma bitno da učesnici koji komuniciraju ili razmenjuju poruke potvrde identitete jedan drugom.

10.3 Zamena i uništenje ključeva

Zamena ključa predstavlja aktivnost zamene i stavljanja ključa van upotrebe. Razlog promene ključa može biti redovna zamena ili zamena usled sumnje da je ključ otkriven.
Redovna zamena ključa podrazumeva redovno obnavljanje ključa i ovim postupkom se znatno smanjuje mogućnost otkrivanja ključa. Pravilo o frekvenciji zamene ključeva ne postoji, ali nije preporučljivo korišćenje jednog ključa u dužem vremenskom periodu, jer mera uspešnosti napada direktno zavisi od vremena i truda napadača na otkrivanju ključa, odnosno o količini informacija koje je prikupio o nekom sistemu. Redovna zamena je planska aktivnost i za upravljanje rokom važnosti ključa odgovorno je sertifikaciono telo.
Ukoliko se zamena vrši usled sumnje da je ključ otkriven potrebno je izvršiti zamenu u što kraćem vremenskom roku.

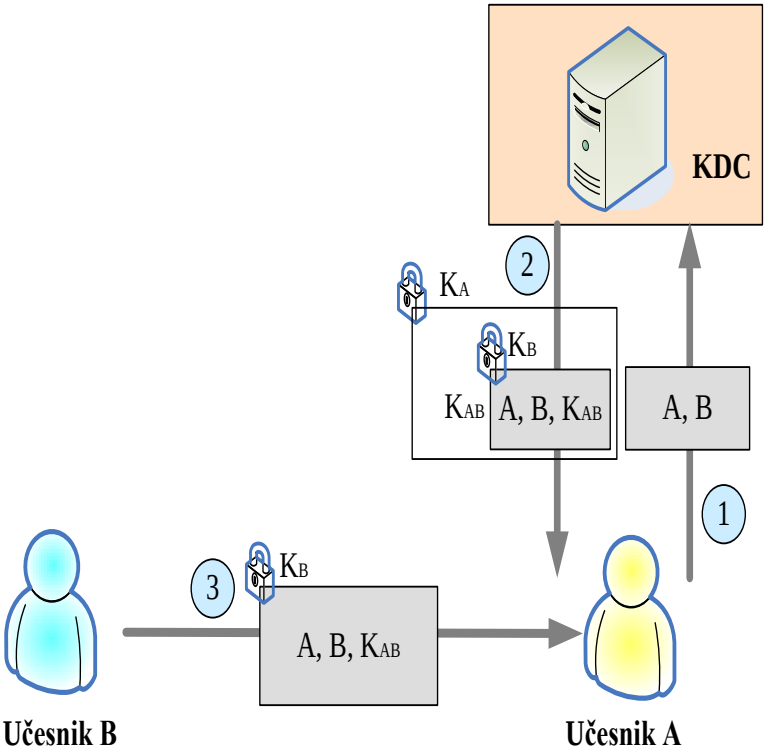
Nakon isteka roka važenja ili usled oštećenja ključevi se obavezno uništavaju a podaci o uništenju ključeva se čuvaju.

10.4 Sistemi za razmenu kriptografskih ključeva

U zavisnosti od vrste kriptografskog sistema postoje različiti sistemi za razmenu kriptografskih ključeva. U ovom radu su ukratko objašnjena četiri sistema za razmenu kriptografskih ključeva: Key Distribution Center (KDC), Diffie-Hellman, Needham-Schroeder i X.509.

10.4.1 Centar za distribuciju ključeva - KDC

Slanje ključeva preko nezaštićenih kounikacionih kanala podrazumevalo je I ugrožavanje njihove bezbenosti. Zato se uvek težilo da se razmena ključeva vrži preko sigurne komunikacionog kanala. Prilikom izvršenja sigurne razmene ključeva između dva učesnika u simetričnom sistemu mogu se koristiti razni protokoli koji se zasnivaju na postojanju trećeg entiteta od poverenja koji se naziva centar za distribuciju ključeva ili Key Distribution Center (KDC).
Uloga KDC-a je da putem sigurnog kanala svakom učesniku obezbedi simetrični ključ za komunikaciju sa bilo kojim učesnikom u mreži. Uslov za to je da svi učesnici poseduju tajni simetrični ključ za komunikaciju sa KDC za čiju distribuciju se razvijaju posebni protokoli, a u određenim situacijama se preuzimaju fizički. Implementacijom KDC-a, pored bezbednosnih, rešava se i veoma izražen problem skalabilnosti mreže. Proces razmene ključeva pomoću KDC je prikazana na slici 10.2.



Slika 10.2 Proces razmene ključeva pomoću KDC-a

Postupak razmene ključa se obično obavlja u nekoliko koraka:

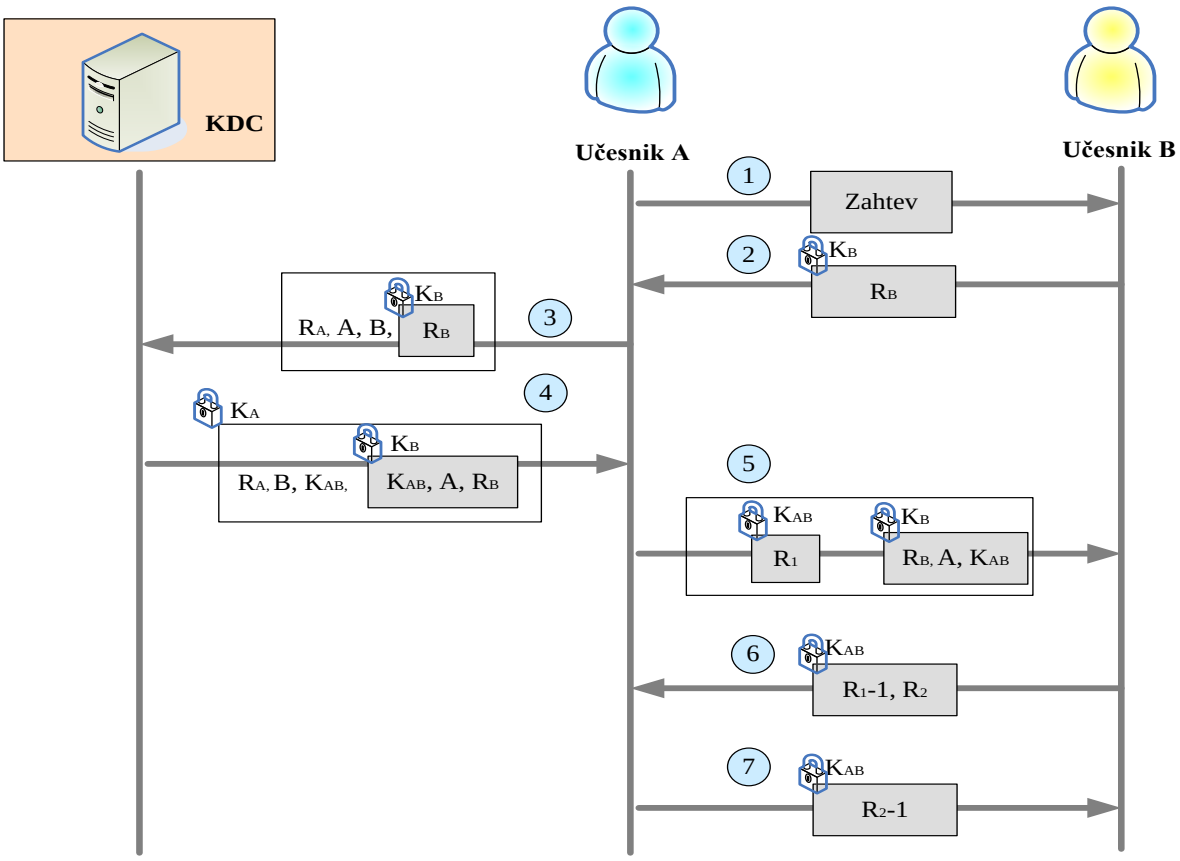
- u prvom koraku učesnik A pošalje poruku KDC-u sa zahtevom da želi da upostavi komunikaciju sa učesnikom B, radi kreiranja zajedničkog sesijskog ključa K_{AB}. Poruka koju je poslao učesnik a sadrži podatke o identitetu učesnika A i identitetu učesnika B i ova poruka nije šifrovana.
- u drugom koraku KDC prima poruku i nakon toga kreira takozvani tiket koji je namenjen učesniku B. Pošto KDC zna tajni ključ učesnika B, koristi ga kako bi šifrovao pomenuti tiket. Kreirani tiket sadrži identitete učesnika A i B i zajednički ključ K_{AB}. Ovako kreiran tiket pakuje se zajedno sa zajedničkim ključem za jednu sesiju K_{AB}, šifruje se sa ključem K_A i na kraju se šalje učesniku A, kao poruka. Nakon prijema poruke učesnik A dešifruje poruku, a zatim otpakuje zajednički ključ K_{AB}. Pošto nema ključ K_B učesnik A ne može da otpakuje tiket koji je namenjen učesniku B.
- u trećem koraku učesnik A prosleđuje tiket učesniku B. Učesnik B prima tiket, otpakuje ga i pamti ključ K_{AB}, jer mu je neophodan radi razmene poruka sa učesnikom A
- Učesnici A i B nakon trećeg koraka mogu razmeniti podatke korišćenjem ključa K_{AB} kao ključa za one-time sesiju.

Način organizacije i funkcionisanja KDC-a se definiđe u zavisnosti od karakteristika telekomunikacionu mrežu u kojoj obavlja svoju ulogu i zavisi od topologije mreže, broja učesnika i frekvencije saobraćaja. Za veće telekomunikacione mreže može se realizovati kroz distributivnu hijerarhiju sa više distributivnih centara na različitim hijerarjihskim nivoima od koji svaki opslužuje po jedan deo mreže.

10.4.2 Needham-Schroeder algoritam za razmenu ključeva

Needham-Schroeder protokol, razvijen od strane Rodzera Nidama (*Roger Needham) i Majkla Šredera (Michael Schroeder), kao algoritam* za razmenu ključeva predstavlja jedan od osnovnih protokola za formiranje sesijskih ključeva putem KDC-a na osnovu koga su nastali mnogi drugi protokoli i predstavlja odlično rešenje po pitanju sigurnosti. Namena ovog protokola je da korišćnjem javnih ključeva omogući autentifikaciju između dva učesnika u komunikaciji uz korišćenje trećeg usčesnika kao entiteta od poverenja odnosno KDC. Prema poslednjoj verziji ovog protokola koriste se četiri slučajna broja: R_A, R_B, R_1 i R_2 za svaki sesijski ključ.

Na slici 10.3 prikazana je razmena ključa pomoću Needham-Schroeder protokola.



Slika 10.3 Proces razmene ključeva pomoću Needham-Schroeder protokola

Proces razmene ključeva pomoću Needham-Schroeder protokola sastoji se od sledećih sedam koraka:

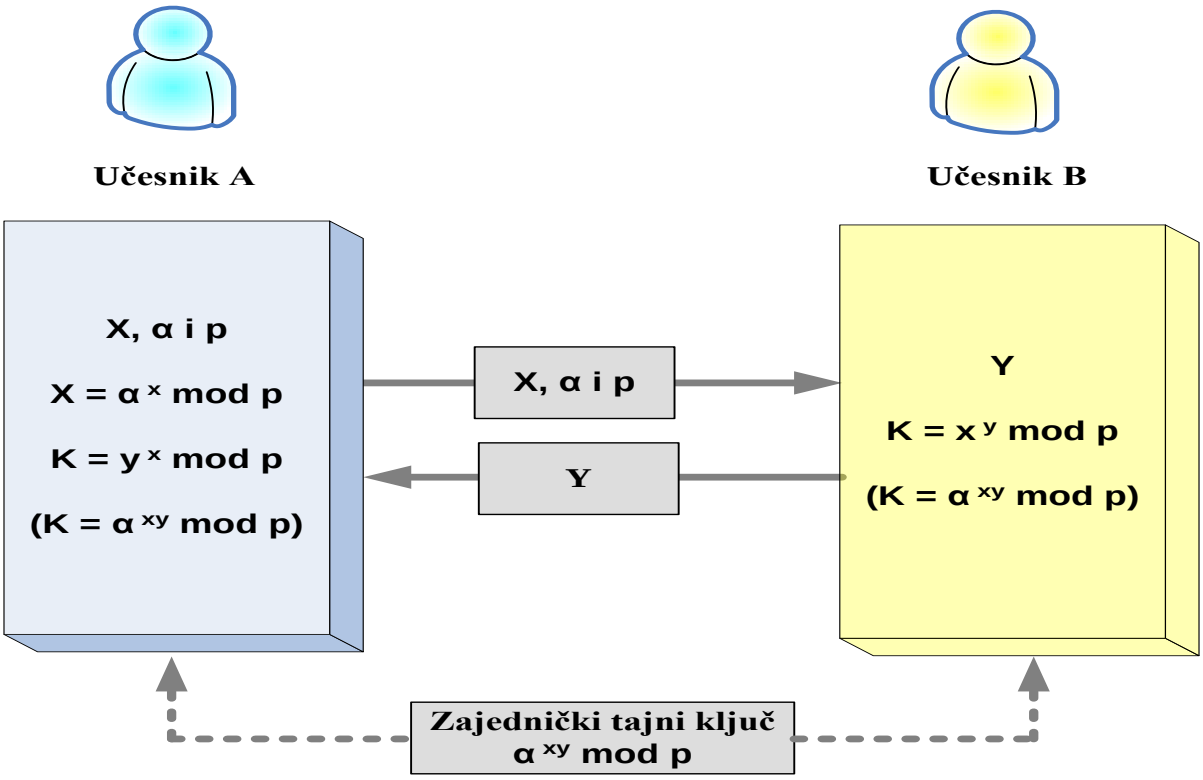
- u prvom koraku učesnik A šalje svoj identitet učesniku B kako bi saopštio učesnikui B da želi komunikaciju sa njim.
- u drugom koraku učesnik B šifruje, pomoću svog tajnog ključa KB, predhodno generisani broj R_B koji namenjuje KDC-u, ali ga šalje učesniku A. Kada primi poruku, učesnik A će proslediti poruku do KDC-a u cilju dokazivanja da je učesnik koji komunicira sa učesnikom B jedini koji će komunicirati sa KDC, odnosno da nije napadač.
- u trećem koraku učesnik A šalje ka KDC-u poruka koju sadrži slučajan broj R_A, identitet učesnika A, identitet učesnika B i šifrovani broj R_B. Ova poruka nije šifrovana i predstavlja zahtev učesnika A koji je namenjen KDC-u u cilju obezbeđivanja tajnog sesijskog ključa K_{AB} za obavljanje sigurne razmene podataka između učesnika A i B.
- u četvrtom koraku KDC vraća učesniku A poruku koja sadrži broj RA, identitet učesnika B, sesijski ključ K_{AB} i šifrovani tiket koji je namenjen učesniku B. Ovaj tiket je šifrovan tajnim ključem učesnika B, a sadrži sesijski ključ K_{AB}, identitet učesnika A i broj koji je predhodno generisao učesnik B, R_B. Ovim postupkom je učesnik A dobio odziv od KDC-a koji sadrži sve neophodne podatke za bezbednu komunikaciju sa učesnikom B.

- u petom koraku učesnik A prosleđuje učesniku B tiket dobijen od KDC-a i novi broj R_1 u cilju prozivanja I verifikacije učesnika B.
- u šestom koraku učesnik B odgovara na poziv učesnika A slanjem šifrovanog boja R_{1-1} i pozivom učesnika A brojem R_2. Ako učesnik A nakon dešifrovanja primljene poruke dobije očekivani broj R_{1-1}, to znači da je identitet učesnika B verifikovan, jer je učesnik koji je poslao ovu poruku bio u stanju da primenom K_B dođe do K_{AB}, što može samo učesnika B.
- u sedmom koraku učesnik A ponovo odgovara na poziv slanjem šifrovanog (pomoću ključa K_{AB}) broja R_{2-1}. Ovom porukom učesnik A obaveštava učesnika B da je primio verifikaciju i istovremeno verifikuje sebe učesniku B (39).

10.4.3 Diffie-Hellman algoritam za razmenu ključeva

Diffie-Hellman algoritam predstavlja prvi algoritam za razmenu javnih ključeva koji su 1976. godine razvili Vitfild Difi (*Whitfield Diffie*) I Martin Helman (*Martin Hellman*). U svojoj primeni koristi dva ključa, jedan javni i jedan tajni. Pošiljo pri komunikaciji sa primaocem šifruje poruku sa svojim tajnim ključem i javnim ključem primaoca. Primaoc dešifruje primljenu poruku korišćenjem svog tajnog ključa i javnog ključa pošiljaoca. Ova šema se zasniva nateţini izračunljivosti logoritamske funkcije za eksponente koji su prosti brojevi, to jest zasniva se na problemu diskretnog logoritma.

Primer Diffie-Hellman algoritama za razmenu ključeva prikazan je na slici 10.4.



Slika 10.4 Proces razmene ključeva pomoću Diffie-Hellman protokola

Proces razmene ključeva pomoću Diffie-Hellman protokola realizuje se u sledećim koracima:

- u cilju razmene tajnog ključa sa učesnikom B, učesnik A šalje poruku α. Celobrojnu vrednost x iz skupa brojeva {1,2,…,p - 1} generiše metodom izbora slučajnog broja. Vrednost x koristi za šifrovanje poruke pomoću formule: $X = \alpha^x \bmod p$
- Ovako formiran podatak X se šalje do učesnika B.
- Kada učesnik B primi poruku i sazna X, α i p , on na osnovu slučajnog izbora generiše broj y i pomoću njega računa vrednost Y po formuli: $Y = \alpha^y \bmod p$
- Ovako dobijenu funkciju šalje nazad učesniku *A*.
- Istovremeno na osnovu podataka koje je dobio od učesnika *A* i broja *y* (koji je sam generisao) računa vrednost ključa *K* po formuli: $K = x^y \bmod p$
- Kako je i učesnik *A* dobio vrednost *Y* može izračunati vrednost ključa *K* po formuli: $K = y^X \bmod p$

Prilikom primene Diffie-Hellman protokola za razmenu ključeva postoje ozbiljni problemi koji se ogledaju u njegovoj osetljivosti na „čovek u sredini“ (man-in-the-middle), gde napadač može da se predstavi kao druga strana za oba učesnika i obmanjivanjem dođe do simetričnih ključeva, a da učesnici ne primete problem. Da bi se sprečila ova vrsta napada potrebno je prilikom korišćenja Diffie-Hellman protokola koristiti mehanizam atentifikacije, koji bi u ovom slučaju opdrazumevao obostranu autentifikaciju.

11 IMPLEMENTACIJA KRIPTOGRAFSKOG SISTEMA U MREŽU ZA UPRAVLJANJE TELEKOMUNIKACIONIM SISTEMOM

Implementacija kriptografskog sistema u mrežu za upravljanje telekomunikacionim sistemom proces koji se sastoji iz više koraka. Prvi korak predstavlja definisanje projekta, odnosno obima i granica projekta i formiranje tima za njegovu ralizaciju. Sledeći predstavlja analiza karakteristika mreže za upravljanje, na osnovu koje se stiče zaključak kakvu vrstu zaštite bi trebalo implementirati i kakvi su zahtevi za opremom i načinom konfiguracije mreže i opreme. Nakon sagledavanje neohodnih činjenica sledi proces planiranja sistema zaštite. Planiranje kao složena funkcija ima za cilj da svojim odlukama usmerava sistem zaštite prema budućnosti. Zbog toga treba da sagleda i vizije, ciljeve, strategije i planove razvoja mreže za upravljanje telekomunikacionim sistemom. Planiranje se sastoji iz tri faze: predviđanje, odlučivanje i izrada plana. Predviđanjem treba da se uvide tendencije razvoja telekomunikacionog sistema i mreže za upravljanje tim sistemom. Odluka treba da bude proaktivna, odnosno da ne bude samo odgovor na sadašnju situaciju već da predstavlja i osnov za buduće unapređenje sistema zaštite, odnosno da budu prevencija budućih problema. Planovi moraju da budu izrađeni precizno sa jasno definisanim fazama implementacije šifarskog sitstema. Nakon planiranje vrši se izrada modela prototipa sistema zaštite i isti se testira. Na osnovu testiranje vrši se revizija i otklanjanje nedostataka nakon čega se vrši integracija sistema zaštite u mrežu za upravljanje telekomunikacionim sistemima.
Podaci koji se prenose kroz mrežu za upravljanje telekomunikacionim sistemima predstavljaju interesantan cilj za potencijalne napadače. Prodorom u mrežu za upravljanje napadaču su sostupni svi podaci o kapacitetima mreže, realizovanim servisima i podaci o korisnicima servisa. Prodor u mrežu podrazumeva da se napadaču stvara mogućnost da prisluškuje saobraćaj u mreži koji mu je interesantan, da preusmerava i onemogućuje servise u telekomunikacionoj mreži i da na kraju i onemogući rad kompletne mreže. Osetljivost mreže za upravljanje na eventualne napade od strane neovlašćenih lica zahteva da se saobraćaj koji ide van mreže nesigurnim spojnim putevima zaštiti.
Ovom prilikom nije analizirana telekomunikaciona mreža niti zahtevi za sistem za zaštitu telekomunikacione mreže.
Proces uvođenja sistema za zaštitu mreže za upravljanje je složen proces koji obuhvata sledeće aktivnosti:

- Sagledavanje činioca koji opisuju mrežu za upravljanje (analiza karakteristika mreže za upravljanje i zahtevi sistema za zaštitu)
- Izgrada projekta sistema za zaštitu
- Realizacija izrađenog projekta sistema za zaštitu
- Eksploatacija sistema za zaštitu

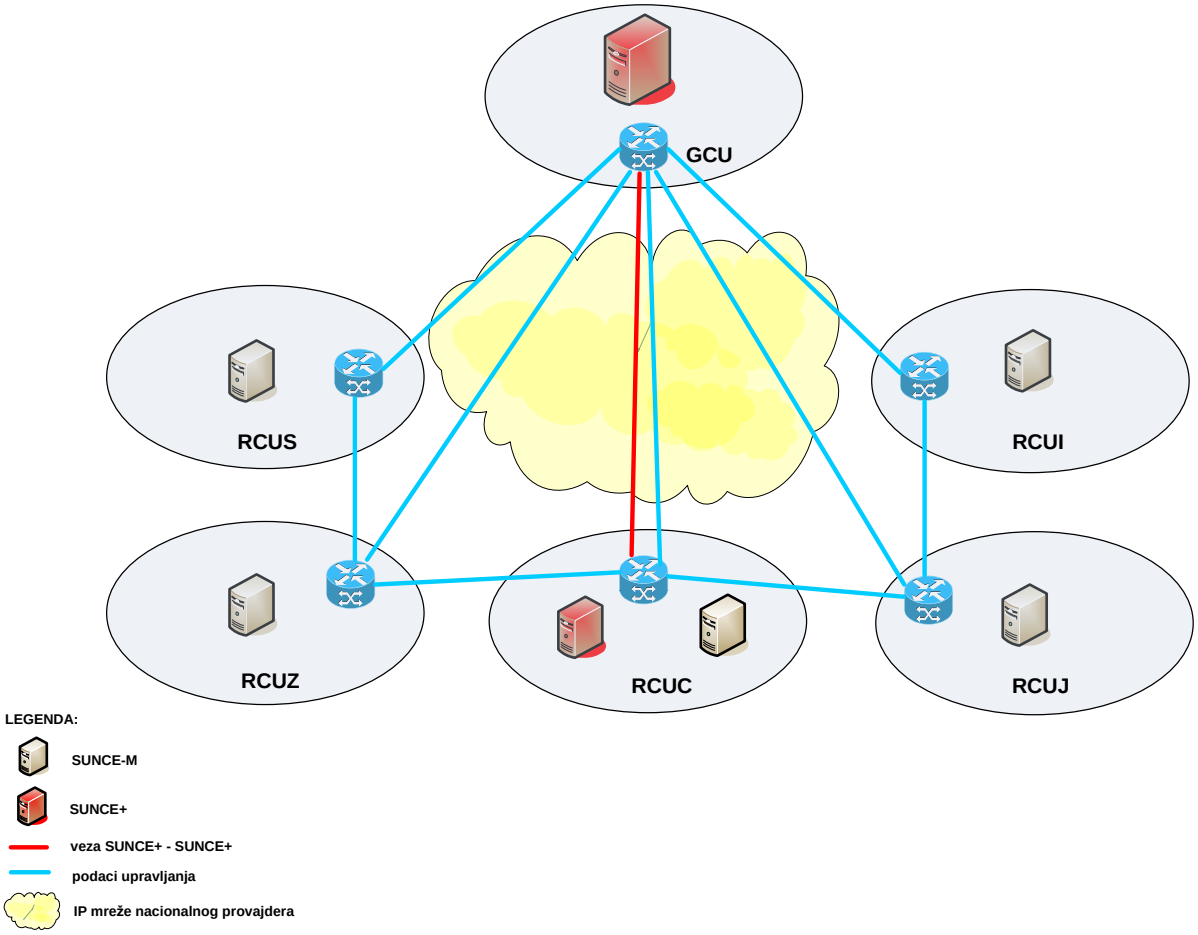
11.1 Analiza karakteristika mreže za upravljanje

Analiza karakteristika mreže za upravljanje telekomunikacionim sistemom je bitna faza u procesu projektovanja sistema zaštite, jer mora da pruži sve neophodne

podatke projektantima, kao bi projektovani sistem zaštite odgovori svim zahtevima i bezbednosnim izazovima nakon integracije u mrežu za upravljanje.

11.1.1 Model mreže za upravljanje telekomunikacionim sistemom

Model mreže za upravljanje telekomunikacionim sistemom će biti iskorišćen da se na njemu izvrši analiza karakteristika mreže za upravljanje, da se iznesu zahtevi za potrebnim sistemom zaštite i opremom koja se može iskoristiti za realizaciju sistema zaštite. Mreža za upravljanje telekomunikacionim sistemom, koja je prikazana na slici 11.1. predstavlja mrežu za upravljanje sa distribuiranom arhitekturom.



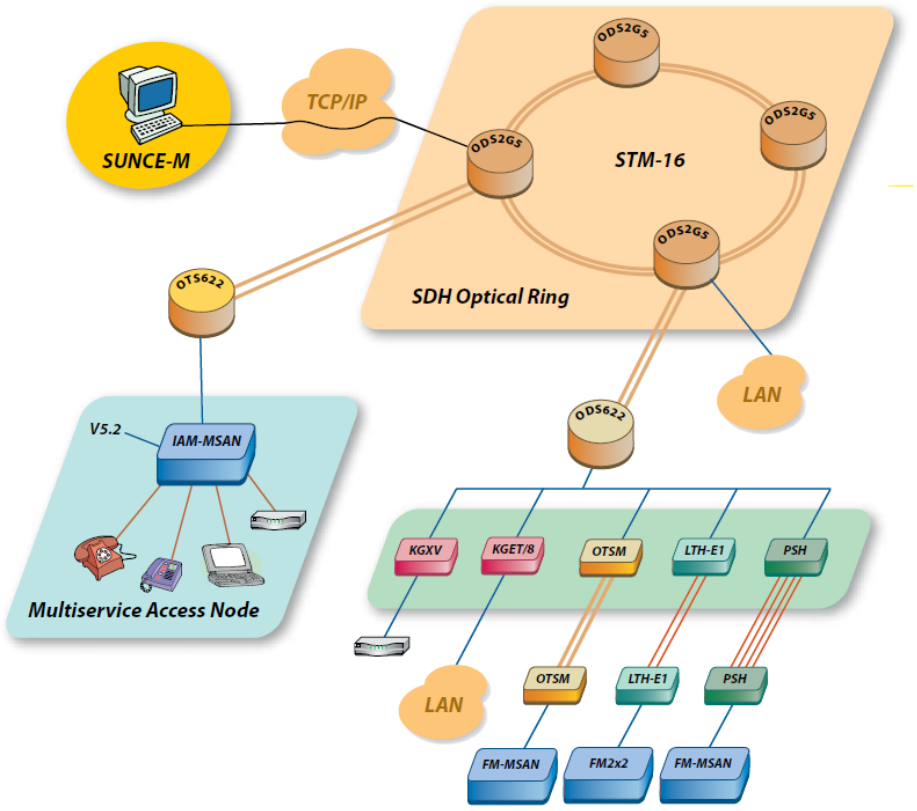
Slika 11.1 Model mreže za upravljanje telekomunikacionim sistemom

Sastoji se glavnog centra za za upravljanje (GCU) i pet regionalnih centara za upravljanje: regionalni centar za upravljanje istok (RCUI), regionalni centar za upravljanje jug (RCUJ), regionalni centar za upravljanje zapad (RCUZ), regionalni centar za upravljanje sever (RCUS) i regionalni centar za upravljanje centar (RCUC). Svaki regionalni centar je zadužen za upravljanje određenim delom telekomunikacione opreme i na njima bi se nalazio sistem za upravljanje domaćeg proizvođača „Iritel" a.d. Beograd SUNCE-M. Glavni centar za upravljenje je zadužen za upravljnje celokupnom mrežom i na njemu se nalazi sistem za upravljanje, isog proizvođača, SUNCE+. U okviru RCUC se nalazi rezervni sistem za upravljanje

SUNCE+, koji ima iste podatke kao i SUNCE+na GCU i služi kao rezerva u slučaju njegovog ispada iz rada. Pored sistema za upravljanje na centrima za upravljanje nalazi se mrežna oprema, ruteri i svičevi, koji služe za realizaciju IP mreže za upravljanje. Mreža je realizovana ka out-of-band mreža koja obezbeđuje stalno dodeljenje kanale za realizaciju saobraćaja za upravljanje mrežom. Saobraćaj koji se realizuje između centara za upravljanje je baziran na IP protolkolu i realizovan je preko IP mreže nacionalnog provajdera.

11.1.2 Karakteristike sistema za upravljanje

Sistem za upravljanje domaćeg proizvođača „Iritel" a.d. Beograd SUNCE-M predstavlja sistem za upravljanje Iritelovim SDH i PDH uređajima i omogućava prikaz od cele mreže do funkcionalnog bloka na jedinici (40). Na slici 11.2 je prikazan princip povezivanja sistema SUNCE-M.



Slika 11.2 Princip povezivanja sistema SUNCE-M

Osnovne osobine sistema za upravljanje SUNCE-M su:

- neprekidan prikaz kompletne mreže i parametara vezanih za ispravanost rada njenih elemenata
- promena topologije mreže i konfiguracije pojedinačnog elementa iz centra za upravljanje
- omogućava TMN (Telecommunications Management Network) funkcije upravljanja greškom, konfiguracijom, performansama i sigurnošću

- u TMN funkcionalnoj arhitekturi nalazi se na sloju upravljanja mrežom (Network Management Layer) i sloju upravljanja elementom (Element Management Layer)
- računar koji ima ulogu centra za upravljanje mrežom povezuje se sa jednim od uređaja iz mreže pomoću Ethernet 10baseT ili RS232 serijskog interfejsa (F interfejs)
- može da se integriše u sistem upravljanja mrežom SUNCE+
- svaki mrežni element je opremljen sa sistemskom jedinicom za upravljanje koja komunicira sa sistemom SUNCE-M.

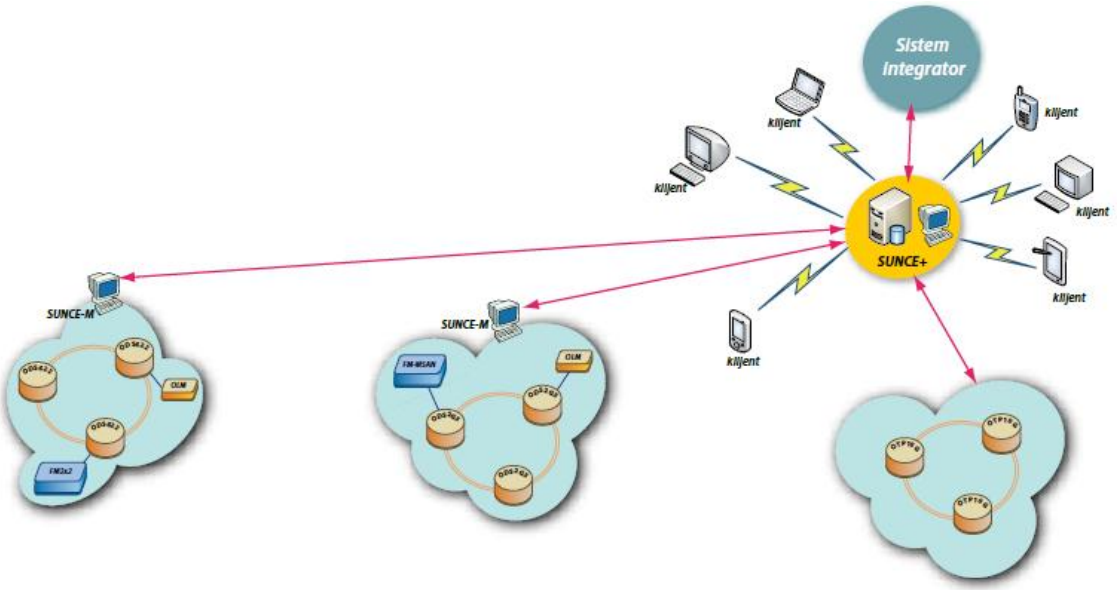
Upravljanje sigurnošću koje omogućava SUNCE-M obuhvata:

- dodeljivanje korisničkih naloga kojima se ograničava pristup opcijama u sistemu
- autorizacija pristupa putem korisničkog imena i lozinke
- administracija korisnika sistema - dodavanje, brisanje i promena podataka
- pregled istorije rada korisnika (log fajlovi, filtriranje)

Sistem za upravljanje domaćeg proizvođača „Iritel" a.d. Beograd SUNCE+ predstavlja sistem za upravljanje Iritelovim SDH i PDH uređajima i omogućava:

- neprekidni hijerarhijski nadzor složenih mreža, podmreža,stanica i uređaja
- praćenje kvaliteta i raspoloživosti mreža i servisa
- alat za eksploataciju i održavanje, bitan za projektovanje mreža
- evolucioni redizajn sistema upravljanja mrežom
- integraciju sa OSS/BSS sistemom

Na slici 11.3 je prikazan princip povezivanja sistema SUNCE+



Slika 11.3 Princip povezivanja sistema SUNCE+

Osnovne osobine sistema za upravljanje SUNCE+ su:

- podržana integracija svih tipova uređaja IRITEL
- integracija svih elemenata u mreži ili njihovog podskupa
- topologija mreže u obliku hijerarhijskog stabla, od nivoa podmreže do stanice i elemenata u njoj
- omogućava brzu detekciju problema na resursima mreže čime se popravlja kvalitet servisa
- klijent-server arhitektura omogućava istovremeni višekorisnički pristup
- distribuirana hardverska platforma
- direktan pristup elementima mreže korišćenjem sistema SUNCE-M
- softverski sistem SUNCE+ raspoređen je na više računara, prema broju i složenosti podređenih SUNCE-M sistema
- automatski prelaz rada sa glavne na rezervnu bazu podataka
- ugrađena dijagnostika omogućava brzu i pouzdanu lokalizaciju smetnje
- pristup sa bilo kog sistema sa Web čitačem putem lokalne mreže ili virtuelne privatne mreže
- implementacija FCAPS modela funkcija upravljanja (Fault, Configuration, Accounting, Performance, Security)
- praćenje trenutnog stanja mreže, kao i istorije njenog ponašanja
- praćenje akcija korisnika sistema SUNCE+

Povezivanje sistema za upravljanje i meržne opreme realizovano je linkovima brzine prenosa 2 MB/s.

11.2 Zahtevi sistema za zaštitu

Na osnovu iznete analize karakteristika mreže za upravljanje telekomunikacionim sistemom u može se zaključiti da je potrebno ralaizovati zaštitu komunikacije izmežu sistema za upravljanje koji se nalaze u glavnom i regionalnim centrima za upravljanje, a koja se realizuje kroz nezaštićenu mrežu nacionalnog provajdera.
Prilikom definisanja zahteva mora se obratiti pažnja da se u potpunosti ispoštuje zakonska regulativa koja definiše pitanje zaštite informacija. Rešenje mora ispunjavati sve zahteve kriptografije, odnosno da budu realizovani svi sigurnosni servisi. Brzina prenosa i kašnjenje informacije moraju da budu u dozvoljenim granicama.
Zahtevi za kripografskim alogitmima i ključevima su sledeći:

- realizovati zaštitu korišćenjem IPSec protokola u tunelskom režimu rada
- primeniti sopstveni simetrični kriptografski algoritam koji razviti modifikacijom AES algoritma
- obezbediti što veći uticaj na algoritam i ključeve od strane korisnika sistema zaštite

- primeniti ključ dužine 128 bita sa tendencijom povećanja na veće dužine a za početak na dužinu 256 bita
- obezbediti čuvanje algoritma u potpunoj tajnosti
- obezbediti potpunu tajnost ključa
- upravljanje realizovati posredstvom centra za upravljanje
- realizovati jednostavno i transparentno rešenje za korisnike

Na osnovu iznetog potrebno je ispitati tržište i izvršiti nabavku opreme koja će omogućiti zaštitu sa IPSec protokolom u tunelskom režimu rada sa algoritmima i ključevima u skladu sa zahtevima.

11.3 Izrada projekta sistema za zaštitu

Projektovanje sistema zaštite je složen proces kojim se u skladu sa analizom mreže za upravljanje i na osnovu zahteva za sistemom zaštite iznalazi optimalno rešenje za zaštitu mreže za upravljanje. Projektovanje obuhvata izradu modela sistema za zaštitu, testiranje modela i otklanjanje nedostataka i implemetaciju sistema zaštite.
Projekat mreže za upravljanje se sastoji iz faze prikupljanja podataka, faze planiranja, izrade prototipa i analize projekta.
Prilikom planiranja mreže za upravljanje neophodno je izvršiti sledeće korake u planiranju:

- Planiranje veličine sistema za zaštitu u odnosu na broj elementa u mreži za upravljanje
- Planiranje rasporeda elemenata sistema za zaštitu
- Konfiguracija parametara softverskih i hardverskih komponenti
- Izbor kriptografsko algoritma
- Određivanje dužine ključeva
- Određivanje načina upravljanjem ključevima
- Izbor kriptoloških uređaja
- Verifikaciono testiranje

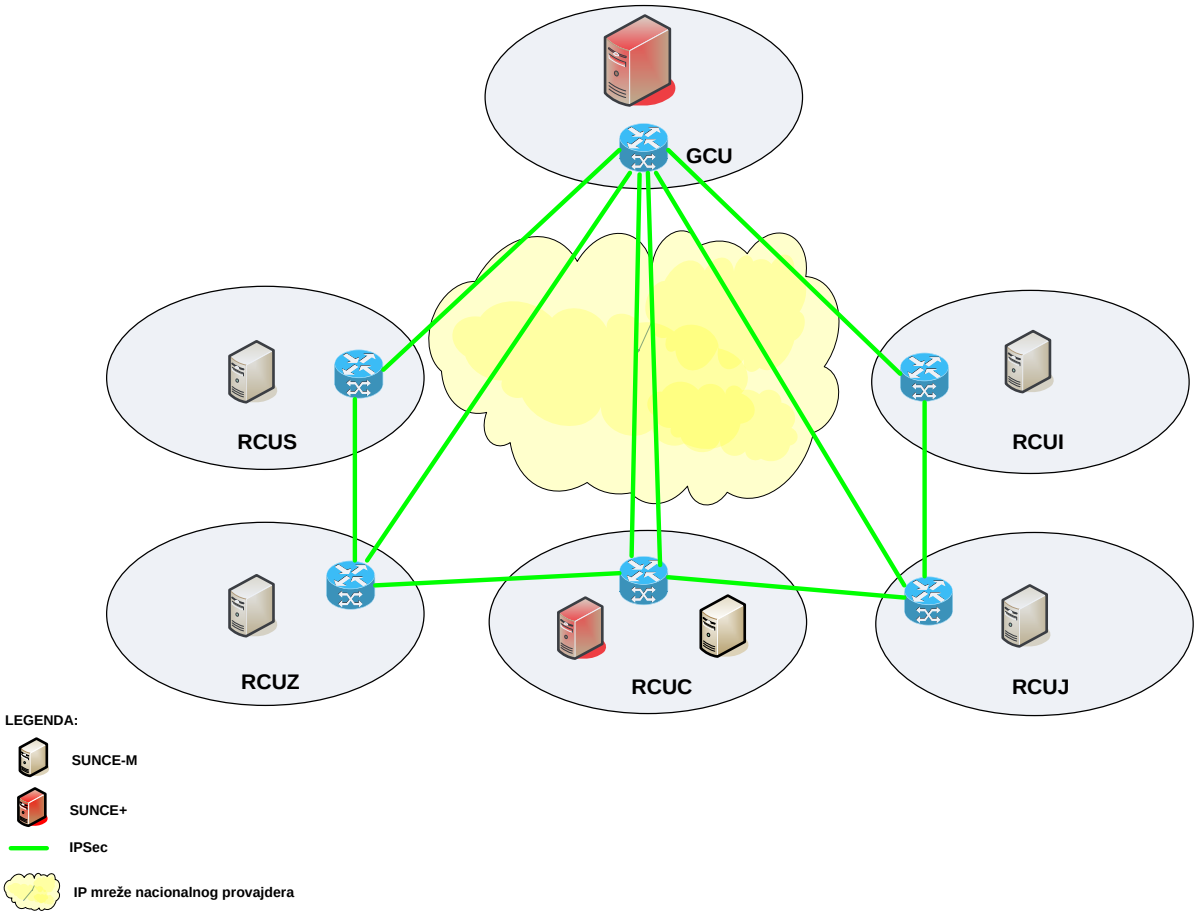
11.3.1 Model sistema za zaštitu

Rezultat projekta treba bude prototip sistema za zaštitu u vidu modela sistema za zaštitu, na kojem bi se izvršila neophodna ispitivanja sistema za zaštitu radi uočavanje nedostataka sistema i njihovaog otklanjanja pre realizacije izrađenog projekta.

Pod modelom sistema za zaštitu podrazumeva se skup opreme i procedura kojima se obezbeđuje zaštita mreže za upravljanje telekomunikacionim sistemom. Model u konkretnom slučaju mora da odredi način realizacije zaštite, algoritme i ključeve koje treba koristiti i način upravljanja ključevima. Model sistema zaštite mreže za upravlanje prikazan je na slici 11.4.

Mreža za upravljanje realizovana je povezivanjem sistema za upravljanje SUNCE-M i SUNCE+ preko IP mreže nacionalnog provajdera. Komunikaciona mreža koja se koristi za komunikaciju između sistema za upravljanje je nezaštićena, a time ostavlja otvorene mogućnosti da bude predmet napada od strane neolašćenih lica. Mreža za upravljanje u osnovi predstavlja računarsku mrežu koja je izložena svim vrstama

napada koji se mogu primenuti na računarske mreže. Nivo tajnosti podataka koji se razmenjuju kroz mrežu za upravljanje i moguća šteta koja može nastati kao rezultat napada od strane neovlašćeni lica zahtevaju razvoj sistema zaštite za mrežu za upravljanje.



Slika 11.4 Model sistema za zaštitu

U profesionalnim sistemima zaštite korišćenje sopstvenog algoritma u simetričnim šifarskim sistemima i tajnost simetričnih šifarskih ključeva jesu osnova garancije bezbednosti. Kao dodatna garancija i preduslov za mogućnost realne procene nivoa sigurnosti rešenja jeste i upotreba pouzdanih nosećih softverskih komponenti čiji je izvorni kod dostupan.(41)

Izbor kriptografsko algoritma je predstavlja korak u projektovanju kojim se na osnovu zahtevanog nivoa zaštite, komunikacionih karakteristika mreže za i pravljanje i raspoloživih finansijskih sredstava vrši odabir kriptografskog algoritma koji će biti korišćen u projektovanom sistemu zaštite. Imajući u vidu karakteristike kriptografskih algoritama za postizanje bolje zaštite i zbog neophodne efikasnosti koju mreža za upravljanje zahteva, imajući u vidu da seu promene stanja telekomuniakcionog sistema brze i da reakcija administratora mreže mora da bude brza, simetrični kriptografski algoritmi predstavljaju bolji izbor. S obzirom na korišćene IPSec protokola za zaštitu izbor simetričnog algoritma se svodi na AES simetrični algoritam. Radi obezbeđenja veće tajnosti i sigurnosti sistema potrebno je razviti sopstveni

algoritam na bazi AES algoritma. Projektom je potrebno planirati i vreme potrebno za razvoj sopstvenog algoritma. Kasnijom ekspoatacijom razvijenog algoritma potrebno je pratiti njegovu sigrnost i konstantno ga unapređivati.

Određivanje dužine ključa predstavlja naredni korak u projektovanju kojim se na osnovu stepena tajnosti odataka koji se štite, vremena aktuelnosti tih odatak i resursa napadače kojima može da ugrozi mrežu za upravljanje, određuje dužina ključa. Ovo je važan korak u procesu projektovanja jer izbor dužine ključa ima direktan uticaj na sigurnost kompletnog sistema zaštite. Aktuelnost podataka u mreži za upravljanje je konstantna, jer su podaci koji se nalaze u okviru mreže podaci koji se očitavaju direktno sa uređaja i iz baza podataka. S obzirom na brze promene u mreži za upravljanje kašnjenje podataka, koje bi nastalo kao posledica tromosti sistema za zaštitu, moralo bi da se svede na minimalnu granicu, što iziskuje pronalaženje optimalne dužine ključa, koja mora da zadovolji uslove mreže za upravljanje i uslove sistema za zašitu. Resursi napadača su uglavnom nepoznati tako da se prilikom ovog faktora koji utiče na izbor dužine ključa, radi na osnovu pretpostavki. Napadi na dužinu ključa predstavljaju napade “grubom silom” i realizuju se ispitivanje svih mogućih ključeva i uspeh otkrivanja ključa zavisi od procesorske moći napadača.Na osnovu ovih činioca i izabranog algoritma rešenje bi bilo u upotrebi ključeva sa izborom početne dužine od 128, sa tendencijom povećanja na veće dužine a za početak na dužinu 256 bita.

Način upravljanja ključevima predstavlja bitan segment u funkcionisanju sitema zaštine. Izbor pravilnog načina upravljanja ključevima otežava mogučnost otkrivanja ključeva od strane napadača. U skladu sa savremenim rešenjima koja se nude na tržištu koja upravljanje ključevima treba da bude centralizovano sa što manjim uticajem lokanih učesnika na proces upravljanja.

Izbor kriptoloških uređaja predstavlja korak projektovanja koji pofrazumeva izbor adekvatnog uređaja a u skladu sa zahtevima koje postavljaju izabrani algoritam, dužina ključa i način upravljanja ključevima. Potrebno je definisati karakteristike uređaja koji treba da se nabave, da se raspiše konkurs za dostavljanje ponude i da se u određenom vremenskom periodu, koji mora sa se definiše projektom, izvrše verifikaciona ispitivanja. Na tim verifikacionim ispitivanjima ispitale bi se karakteristike uređaja koji su ponuđeni od strane ponuđača i donela bi se odluka koje uređaje treba nabaviti. Prilikom nabavke uređaka je dan od bitnih faktora predstavlja i količina finansija kojima se raspolaže kako za nabavku uređaja, tako za realizaciju kompletnog projekta sistema za zaštitu.

Na osnovu stanja na tržištu, zahteva koji postavlja sistem za zaštitu i dosadašnjih iskustava za realizaciju ovog sistema najpogodniji su uređaji inostranih firmi CISCO (iz SAD) (42) i Crypto AG (Švajcarska) (43). Od domaćih proizvođača opremu koja bi se mogla iskoristiti za realizaciju projekta uz određene dodatne dorade mogla bi da ponudi firma Iritel a.d. Beograd.

11.3.2 Realizacija izrađenog projekta mreže za upravljanje

Nakon faze izrade prototipskog rešenja i faze analize i testiranja prototipa u cilju uočavanja nedostataka pre potpune implemantacije, sledi fizička realizacija projekta, odnosno montaža softverskih i hardverskih komponenti i uvođenje sistema za zaštitu mreže za upravljanje u operativno okruženje. Pre uvođena u operativnu upotrebu

mora se raelizovati obuka sa licima, koja će biti zadužena za rad i održavanje implementiranom sistema. Nakon konačne implementacije sistem za zaštitu mreže za upravljanje mora da demonstrira zahtevane performanse za sigurnošću mreže za upravljanje.

11.3.3 Eksploatacija mreže za upravljanje

Nakon potpune implementacije sistema za zaštitu sledi korak preuzimanja i eksploatacije sistema za zaštitu od strane korisnika. Korisnik u potpunosti mora biti svestan svih ograničenja zasnovanih na određenom izabranom sistemu zaštite I da stalnim praćenjem performansi sistema sagledava moguće nedostatke I na iste pravovremeno reaguje koako ne bi došlo do narušavanja bezbednsti mreže za upravljanje telekomunikacionim sistemima.

ZAKLJUČAK

Moderne telekomunikacione mreže svakim danom postaju veće, brže i sa kvalitetnijim servisima. Da bi jedna telekomunikaciona mreža bila funkcionalna neophodno je da postoji pouzdani sistem za upravljanje tom mrežom. Sa unapređenjem mreža javljaja se problem da su one istovremeno kompleksnije, zahtevnije i teže za upravljanje. Sofisticiranije mreže traže sofisticiranije načine za upravljanje. Da bi jedno rešenje mreže za upravljanje bilo uspešno mora da zadovolji brojne uslove od kojih su najnačajniji da mreža za upravljanje bude skalabilna, fleksibilna, pouzdana, sigurna i da omogućava upravljanje kvalitetom servisa.

Glavni cilj mreže za upravljanje jeste da omogući da telekomunikaciona mreža bude funkcionalna sa kvalitetnom i pouzdanom uslugom pruženom korisnicima, sa mogućnošću za stalno proširenje i uvođenje novih servisa i usluga, uz brz povratak uloženih sredstava i stvaranja mogućnosti za povećanje finansijske dobiti pružaocima usluga.

Upravljanje telekomunikacionim sistemom je mnogo više od samog nadzora i upravljanja elementima u mreži i podrazumeva poslovni proces, koji se sastoji od više nivoa i koji da bi uspešno funkcionisao, mora da se njime upravlja sistemom za upravljanje poslovnim procesima, kako bi se kroz izvršavanje pojedinačnih zadataka došlo do ispunjenja postavljenog cilja.

Informacija predstavlja vitalni interes. Razvoj informacione tehnologije uključuje i razvoj sigurnosnih problema. Kada god je u pitanju osetljiva informacija prisutan je i rizik koji mora da se eliminiše. Kada je u pitanju bezbednost informacija samo je perfekcija dovoljno dobra. Svaka konekcija na javnu mrežu ostavlja vrata za napad. Moderno telekomunikaciono društvo je moderno rizično društvo u pogledu količine razmene podataka nezaštićenih od neovlašćenog pristupa.

Osetljivost informacija koje se prenose mrežom za upravljanje iziskuju uvođenje kvalitetne zaštite kako se ne bi narušila tajnost informacija. Zaštitom podataka bavi se kriptogfija, nauka o zaštiti podataka sa dugom tradicijom. Današnja kriptografija je visoko razvijena matematička nauka čija upotreba omogućava moderan pristup zaštiti informacija.

Osnovne pretpostavke za uspešno projektovanje sistema za zaštitu čine ispunjenje tri preduslova da projektovano rešenje bude: transparentno je za krajnje korisnike i jednostavno primenljivo, da koristi sopstveni algoritam za šifrovanje i koristi pouzdane noseće komponente sa dostupnim izvornim kodom.

Glavni cilj sistema za zaštitu mreže za upravljanje jeste da zaštiti protok informacija od napada neovlašćenih lica, i da pri tome ne degradira performanse mreže za upravljanje kako joj ne bi ugrozio realizaciju njene osnovne namene

Tendencija daljeg razvoja sistema za dešifrovanje pokazuje da nijedan algoritam niti ključ ne mogu biti dovoljno snažni da bi bili potpuno sigurni da vremenom neće doći do otkrivanja. Zbog toga je potrebno neprekidno pratiti i unapređivati kriptografski algoritam kao osnovni element sistema zaštite, a sam sistem zaštite shavatiti kao neprekidan proces kojim se teži dostizanju višeg stepena zaštite.

LITERATURA

(1) Narodna skupština (2010), Zakon o elektroskim komunikacijama, Službeni glasnik Republike srbije, Beograd, str. 3

(2) Tarmo Anttalainen (2003), Introduction to Telecommunications Network Engineering - 2nd ed.Artech House, Boston, USA, str 20

(3) Vivek Alwayn (2004), Optical Network Design and Implementation, Cisco Press, Indianapolis, USA, str. 3

(4) M.3000 Overview of TMN Recommendations (2000), ITU-T, Geneva, Switzerland

(5) M.3010 Principles for a telecommunications management network (2000), ITU-T, Geneva, Switzerland

(6) X.700 Management framework for Open Systems Interconnection (OSI) for CCITT applications (1999), ITU-T, Geneva, Switzerland

(7) X.710 Information technology – Open Systems Interconnection – Common Management Information service (1997), ITU-T, Geneva, Switzerland

(8) X.711 Information technology – Open Systems Interconnection – Common management information protocol: Specification (1997), ITU-T, Geneva, Switzerland

(9) M.3400 TMN management functions (2000), ITU-T, Geneva, Switzerland

(10) Vinton G. Cerf (1988),RFC1052 IAB recommendations for the development of Internet network management standards, IETF, USA

(11) Jianguo Ding (2010), Advances in Network Management, Auerbach Publications - Taylor & Francis Group, Boca Raton, USA, str. 59

(12) Charles M. Kozierok (2005), The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference , No Strach Press, San Francisco, USA, str. 1076

(13) Jeffrey D. Case, M. Fedor, M.L. Schoffstall, J. Davin (1990), RFC1157 Simple Network Management Protocol (SNMP), IETF, USA

(14) Matthew G. Naugle (1998), Illustrated TCP/IP, Wiley Computer Publishing, John Wiley & Sons Inc., New Jersey, USA, str. 652

(15) Jeffrey Case, K. McCloghrie, M. Rose, S. Waldbusser (1993), RFC 1441 Introduction to version 2 of the Internet-standard Network Management Framework, IETF, USA

(16) Jeffrey Case, K. McCloghrie, M. Rose, S. Waldbusser (1993), RFC 1442 Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2), IETF, USA

(17) J. Case, R. Mundy, D. Partain, B. Stewart(2002), RFC 3410 Introduction and Applicability Statements for Internet-Standard Management Framework, IETF, USA

(18) D. Harrington, R. Presuhn, B. Wijnen(2002), RFC 3411 An Architecture for Describing Simple Network Management Protocol(SNMP) Management Frameworks, IETF, USA

(19) J. Case, D. Harrington, R. Presuhn, B. Wijnen (2002), RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) , IETF, USA

(20) D. Levi,P. Meyer, B. Stewart (2002), RFC 3413 Simple Network Management Protocol (SNMP) Applications, IETF, USA

(21) B. Wijnen (2002), RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) U. Blumenthal, IETF, USA

(22) B. Wijnen, R. Presuhn, K. McCloghrie (2002), RFC 3415 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), IETF, USA

(23) Regis J. Bates (2002), Broadband telecommunications handbook, McGraw-Hill Professional, New York, USA, str 559

(24) Gojko Grubor (2010),Kvalitet i stabilnost poslovnih procesa.ppt, Univerzitet Singidunum, Beograd, Srbija

(25) K. P. Csányi, L. T. Kóczy, and D. Tikk (2004) Intelligent Solutions for Umbrella Systems in Telecommunication Supervision Systems, International Journal of Information Technology (IJIT), str. 122

(26) Tom Sheldon (2000), Encyclopedia od Networking and Telecommunications, Mc Graw Hill, USA, str. 273

(27) Tom Sheldon (2003), An Introduction to Cryptography, PGP Corporation, USA, str. 11

(28) A. Menezes, P. van Oorschot, S. Vanstone (2000), Handbook of Applied Cryptography, CRC Press Inc., USA, str. 4

(29) David Bishop (2003), Introduction to cryptography with Java applets, Jones and Bartlett Publishers, Inc, USA, str. V

(30) X.800 Security architecture for Open Systems Interconnection for CCITT applications: Recommendation (1991), ITU-T, Geneva, Switzerland

(31) R. Shirez (2000), RFC 2828 Internet Security Glossary, IETF, USA

(32) Mladen Veinović, Saša Adamović (2013), Kriptologija 1 – Osnov za analizu i sintezu šifarskih sistema, Univrzitet Singidunum, Beograd, Srbija, str. 84

(33) Dragan Pleskonjić, Nemanja Maček, Borislav Đorđević, Marko Carić (2007), Sigurnost računarskih sistema i mreža, Mikro knjiga, Beograd,174 strana

(34) Milan Milosavljević, Saša Adamović (2013), Kriptologija 2, Univrzitet Singidunum, Beograd, Srbija, str. 104

(35) William Stalings, Cryptography and Network Security Principles and Practices, 6th edition (2014), Pearson Education, Inc., New Jersey, USA, str. 630

(36) Mladen Veinović, Miroslav Ćajić, Bogdan Brkić (2011), Upravljanje kriptološkim ključevima, 8. Naučni skup sa međunarodnim učešćem Sinergija 2011, Bijeljina, Republika Srpska

(37) Mladen Veinović, Miroslav Ćajić, Bogdan Brkić (2010), Analiza sistema za distribuciju kriptografskih ključeva, 18. Telekomunikacioni forum TELFOR 2010, Beograd, Srbija

(38) Mladen Veinović, Miroslav Ćajić, Bogdan Brkić (2011), Upravljanje kriptološkim ključevima, 8. Naučni skup sa međunarodnim učešćem Sinergija 2011, Bijeljina, Republika Srpska

(39) Roger M. Needham, Michael D. Schroeder (1978), Using encryption for authentication in large networks of computers, Communications of ACM, 1978., str. 993-998

(40) http://www.iritel.com/index.php/sr-YU/proizvodi/sistemi-prenosa (pristupljeno 08.09.2015. godine)

(41) Mladen Veinović, Aleksandar Jevremović(2006), IPsec – analiza uticaja algoritma za šifrovanje na saobraćaju LAN mrežama, 14. Telekomunikacioni forum TELFOR 2006, Beograd, Srbija

(42) http://www.cisco.com/c/en/us/products/security/index.html (pristupljeno 20.09.2015. godine)

(43) http://www.crypto.ch/en/products-and-services (pristupljeno 20.09.2015. godine)