MREZE 2 ISPITNA PITANJA

1. DIO

1. **Objasni osnovnu logiku HTTP protokola kao i razliku izmedju perzistentne i neperzistentne varijante?**

HTTP (Hypertext transfer protocol) Web-ov protokol aplikativnog sloja, stateless organizovan po klijent-server modelu gdje klijent zahtjeva, prima i prikazuje Web objekte a server salje objekte kao odgovor na primljeni zahtjev. Klijent inicira TCP konekciju na portu 80, server je prihvaca, razmjenjuju se HTTP poruke i TCP konekcija se zatvara. HTTP se zasnva na mehanizmu da je svaki objekat na Web-u (HTML dokument, slika, video) adresiran preko URL-a. U toku parsiranja html odgovora klijent moze naici na dodatni broj referenci.

Ako je u pitanju nonperistant HTTP klijent ce za svaku referencu morati ponovo zahtjevati konekciju, cekati da se ona odobri, poslati zahtjev i ceakti odgovor nakon cega se raskida konekcija i to ce se desiti onoliko puta koliko referenci je pronasao dok u slucaju persistant HTTP-a konekcija ostaje otvorena pa se poruke istih klijent/server ucesnika salju u okviru jedne sesije sto znaci da klijent salje novi zahtjev cim u toku parsiranja oktrije novu referencu (ne mora ponovo uspostavljati konekciju jer nije ni prekidana) cime se dosta stedi na vremenu (trosi samo 1 dodatni RTT za prenos svih objekata referisanih web stranicom) za razliku od nonpersistant HTTP-a koji zahtjeva 2 dodatna RTT po SVAKOM objektu sto uzrokuje OS opterecenje za svaku TCP konekciju.(cesto pretrazivaci otvore paralelne TCP veze da se sto brze dobave objekti).

2. **Sta je zadatak web proxy servera? Zasto je uvedena i kako radi komanda za uslovni pristup web sadrzajima?**

Proxy server je rjesenje kojim se tezi rasterecenju originalnih servera, smanjenju saobracaja ka globalnoj mrezi i unapredjenju performansi Interneta na nacin da uredjaji kada traze neki dokument se prvo obracaju lokalnom proxy serveru (kojeg instalira ISP, univerzitet i sl.) koji u sebi ima kesirane dokumetne iz ranijih potrazivanja pa ako je trazeni objekat vec u cache-u proxy ga odma isporucuje (ne izlazi se dalje u mrezu) a ako ga nema obraca se originalnom serveru koji mu ga isporucuje, on taj objekat skladisti kod sebe ako ga neko bude opet trazio i naravno klijentu dostavlja dokument koji je od proxy-ja u pocetku i trazen. Proxy se ponasa i kao server (kada se desi cache hit) i kao klijent (cache miss pa onda on od originalnog servera trazi dokument)

Komanda za uslovni pristup (Conditional Get) je nastala kao posljedica toga sto je sadrzaj Web stranica promjenjiv pa se ne zna da li se na proxy-ju nalazi vremenski zadovoljavajuca ili zastarjela kopija dokumenta pa proxy server u svome zahtjevu za neki dokument navodi da mu se posalje nova verzija dokumetna ako je modifikovan nakon datuma navedenog u zahtjevu, ako odgovor izostane znaci da je kopija dokumenta na proxy-ju bila validna a ako originalni server otkrije da on ima noviju verziju od navedenog salje je proxy serverui a on je usvaja.

3. **Sta je to DNS, hijerarhija DNS?**

DNS(Domain Name System) je distribuirana baza podatka implementirana hijaerarhijskim skupom name server-a. Upotreba ovog sistema se odvija po istoimenom DNS apliaktivnom protokolu koji definise komunikaciju izmedju uredjaja i name servera zarad razrjesenja referenci oko imena. DNS za unesen hostname (znakovni oblik) prevede u IP adresu (radi i obrnuto). Pruza mogucnost reimenovanja host racunara (ima primarno kanonicno ali i alias ime), reimenovanje mail servera kao i mogucnost raspodjele opterecenja (umnozavanje Web servera i vezivanje skupa IP adresa za jedno kanonicko ime – jedan od primjera bi bila logika da preusmjerava na najblizi web server iz tog skupa IP adresa).

DNS serveri se organizuju hijerarhijski: najvisi nivo su DNS Root serveri, nize se nalze com, org i edu DNS serveri koji se opet granaju na nize DNS servere.i u sustini postuju pravilo ako visi DNS server ne poznaje mapiranje pristupa nizem DNS serveru.

Npr kada klijent trazi www.facebook.com obraca se root serveru da nadje com DNS server na kome ce traziti dalje facebook.com DNS server na kome ce pak traziti IP adresu od www.facebook.com.

4. **Izmedju prenosa bita i simbola stoji sledeca relacija:**

   1.)bps=baud * br_simbola

   2) bps=baud / br_simbola

   3) baud=bps* broj_simbola (Mislim ovaj nisam sig.)

Baud – broj prenesenih simbola u sekundi gdje 1 simbol kodira N bita a bps je broj prenesenih bita u sekundi

5. **Sta je hub i zasto ima ogranicenje?**

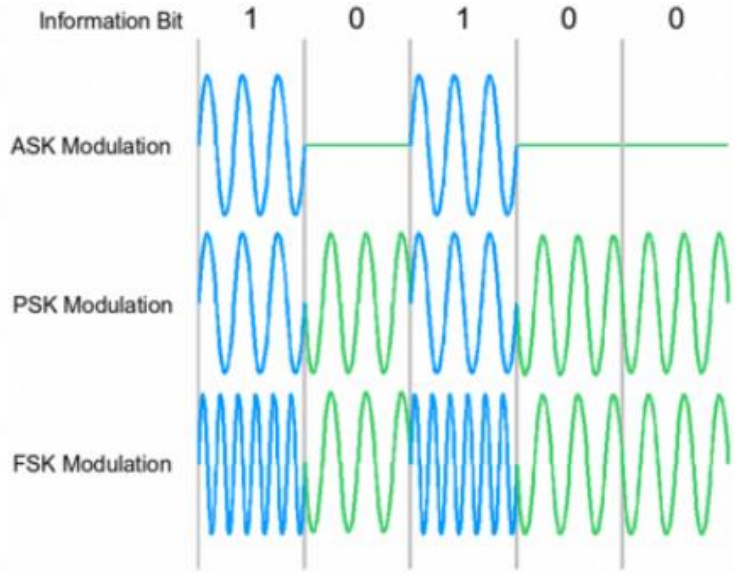
Repeater, Hub je osnovni uredjaj u mrezi koji funkcionise na fizickom nivou OSI ref. modela. On prima okvir, regenerise preamble, pojacava signal i salje ga dalje (ali na sve svoje izlaze jer

nije inteligentan da zna ko mu se na kom portu nalazi) te ne kontrolise niti broadcast niti kolizione domene niti vodi racuna o protokolima nivoa mreze. Ograniceni su zbog toga sto ne otkrivaju kolizije, zadrzavaju jedan kolizioni domen i zakrcuju mrezu (zbog broadcast nacina slanja).

6. Navedi i objasni osnovne vrste digitalne modulacije

Postoje tri osnovna tipa digitalne modulacije a to su:

- ASK (Amplitude Shift Keying) – 0 i 1 se razlikuju po amplitudi
- PSK (Phase Shift Keying) - 0 i 1 se razlikuju po faznom uglu
- FSK (Frequency Shift Keying) – 0 i 1 se razlikuju po frekvenciji

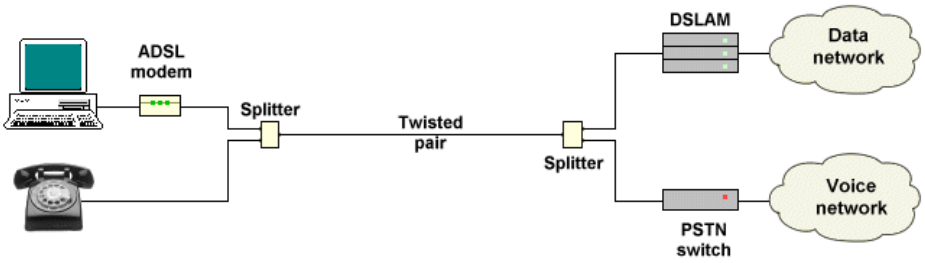


Pored navedenih 1 bit-nih modulacija postoje i modulacije koje koriste vise bita po simbolu.

7. xDSL

Tehnologije sirokopojasnog prenosa preko digitalne pretplatnicke linije (DSL- digital subscrieber line) bez ometanja osnovne telefonske usluge na istoj bakarnoj parici. xDSL koristi frekvencije iznad opsega potrebnog za rad telefona. Ima vise razlicitih verzija koje se razlikuju po brzini i uslugama. Odnos upload/downlaod je takav da je upload uglavnom sporiji.

Na korisnickoj strani ovakve veze se nalaze Spliter, DSL modem, ruter dok se u telefonskoj centrali nalze Spliter, DSLAM.



Spliter razdvaja TF DATA kanale dok je DSLAM mrezni uredjaj koji prosledjuje IP pakete u oba pravca.

Aktuelne varijante xDSL tehnologije su ADSL(najpopularnija), VDSL, VDSL2. Primjenjivost zavisi od odstojanja od optike/centrale, ukupan prenosni opseg se dijeli na 256 kanala po 4 kHZ od kojih je 32 za upload te svaki kanal nezavisno prenosi podatke. Koristi se N-QAM modulacija koja se adaptira prema uslovima prenosa (nivou suma) u svakom od pod-opsega. Razlicit je broj bita po simbolu u razlicitim kanalima (N nije isto za sve kanale).

1. **Od cega se sastoji Web stranica?**

Web stranica se sastoji od objekata (to moze biti HTML file, JPEG image, Java applet, audio file itd.) a definisana je osnovnim HTML fajlom koji sadrzi na reference vise objekata gdje se svaki objekat adresira pomocu URL.

2. **Protokoli za pristup e- posti**

Ovi protokoli ne sluze za slanje e poste nego za njeno preuzimanje sa servera.

POP (Post Office Protocol) funkcionise na nacin da se agent prvo autorizuje pa se onda preuzima e mail. Koristi download & delete rezim sto znaci da korisnik ne moze ponovo da procita skinuti mail ako promjeni racunar. Protokol je stateless izmedju sesija tj one su medjusobno nezavisne,

IMAP (Internet Mail Access protocol) pruza nesto vise mogucnosti nego POP (kompleksniji je) te poruke ostaju na serveru. Dozvoljava korisnicima da sami organizuju svoje poruke u foldere zbog cega on vodi racuna o korisnicima (nije stateless).

HTTP se takodje moze koristiti za pristup postanskom sanducetu na serveru (gmail, Hotmail, Yhoo!)

3. **Exponential backoff sta oznacava**

Exponential backoff je postupak u CSMA/CD algoritmu po kome Ethernet adapter ceka kada se desi kolizija. Takvo cekanje se realizuje tako sto adapter produzuje suspenziju pri pojavi uzastopnih kolizija na nacin da ako je m-ta uzastopna kolizija, bira se slucajan broj iz K opsega $\{0,1,2,...,2^m - 1\}$ te se ceka K*512*bit_time gdje je bit_time vrijeme potrebno za slanje jednog bita.

4. Proces filtriranja i prosledjivanja kod switch-a

Za razliku od hub-a koji ne zna ko mu je na kom portu pa primljeni ethernet okvir salje na sve portove switch je pametniji i on ispituje MAC adresu dolaznog okvira i selektivno ga usmjerava na jedan od svojih izlaza (portova) koji je vezan za tu MAC adresu (zna koja MAC adresa mu se nalazi nakacena na koji port).

Metode kojim se odlucuje kome se prosledjuje okvir su:

- Store and Forward je spor ali pouzdan metod u kome se cio okvir smjesta u buffer switch-a uz provjeru FCS-a (Frame Chechsum) te se samo validni okviri prosledjuju a nevalidni odbacuju
- Cut trough – brz ali nepouzdan metod koji analizira samo 6 prvih bajta okvira kako bi doznao MAC adresu odredista te nema validacije vec se prosledjuju svi pristigli okviri pa i oni osteceni (jer se ne zna da su osteceni jer je samo procitao MAC)
- Fragment free – je metod kompromisa izmedju ove dva metoda gdje se okvir prosledjuje nakon prijema prva 64 bajta bez validacije. Rizik prosledjivanja nevalidnih okvira se smanjuje jer su nevalidni okviri najcesce kraci od 64 bajta te se oni odbacuju.

Kako switch zna gje mu je ko? Pa odrzava Switch tabelu u kojoj se za svaku MAC adresu nalazi njoj odgovarajuci port i vremenski okvir (TTL). Ta tabela se popunjava u toku rada te switch polako „uci“ gdje je ko pa u slucaju kada mu stigne neki okvir on odma zabiljezi podatke od posiljaoca, pogleda ko je primalac ako zna na kojem portu je destMAC on samo tamo i prosledi (osim u slucaju kada je odrediste na istom portu sa koga je stigao frejm – tada se odbacuje) a ako ne zna, salje na sve portove sem na onaj sa koga je frejm stigao.

5. Objasni ideju virtuelnih lokalnih mreza, kako se formiraju i sta obezbjedjuju

Ideja jeste da se unutar jedne LAN mreze (gledano sa fizickog aspekta) moze konfigurisati N virtuelnih (logickih) mreza. U sustini VLAN je skup cvorova grupisanih u jedan broadcast domen koji je zasnovan na logickoj organizaciji ne na fizickim lokacijama. Switch-evi se programski konfigurisu i za svaki VLAN odrzavaju tabelu adresa i tabelu prosledjivanja (jednostavna konfiguracija VLAN-a samo grupisemo koji portovi su u kom VLAN-u nema

potrebe za nikakvom fizickom reorganizacijom) Broadcast domen LAN mreza se prekidao pomocu rutera a broadcast VLAN mreza se prekida preko switch-a. Ovakvom organizacijom se postize to da uredjaji iz jednog VLAN-a ne vide saobracaj iz drugih VLAN-ova. Ovo rjesenje je zgodno za rukovanje saobracajem (zbog podjele na vise broadcast domena).

Za kreiranje VLAN-a je potreban switch kome se unesu parametri za VLAN ali ako zelimo komuniakciju izmedju VLAN-ova to vec zahtjeva upotrebu rutera jer switch to ne umije.

6. **HTTP 1.0,1.1., 2.0 sta su uveli**

HTTP/1.0 metode: GET (uzmi), POST (postavi, posalji), HEAD (isto kao GET samo trazi od servera da u svom zahtjevu izostavi zahtjevani objekat)

HTTP/1.1 metode: HHTP/1.0 + metode PUT (upload file iz tijela poruke na poljem zadatu URL) i DELTE (brise datoteku oznacenu sa URL poljem)

HTTP/2 je kompleksnije rjesenje koje je uvelo ubrzanje rada i kompresiju.

7. **Objasni funkcionalnost i nacin rada zvjezdastog repetitora (hub-a). Zasto postoji ogranicenje u broju nivoa?**

Hub je u osnovi komprimovana zajednicka magistrala koja koristi UTP ozicenje uz regeneraciju signala (u samom centralnom uredjaju) gdje se biti sa jednog prolaza prosledjuju na sve ostale bez bufferovanja ovira i bez CSMA/CD logike gdje eventualnu koliziju detektuju mrezni adapteri LAN stanica. Stanice povezane na hub vide sve pakete u mrezi (jedan broadcast tomen).

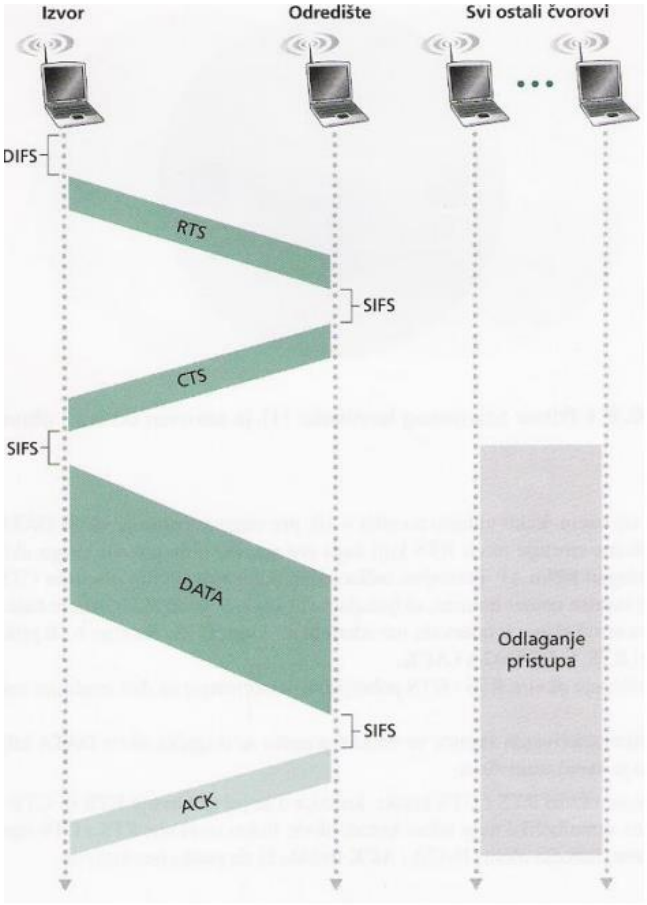
Svaki prolaz (port) omogucava jednom uredjaju da bude prikljucen na zvjezdasti repetitor, zvjezdasti repetitor ne analizira adresu u zaglavlju okvira te nije u mogucnosti da identifikuje na koji prolaz treba da uputi okvir pa ga prosledjuje na sve izlaze (samim tim sto nema bufferovanja i analize nema ni detekcije gresaka u poruci). Zbog toga upravo i postoji ogranicenje u broju nivoa jer su svi uredjaji u jednom broadcast domenu pa bas zbog tog broadcast slanja mreza bi postala nefunkcionalna sa velikim brojem uredjaja, kasnjenje veliko.

---

1. **HTTP/1.1 metodi:**

- Definisu nacin prezentacije podataka iz web stranice
- Obuhvataju prenos fajlova pomocu PUT i DELETE komandi
- Definisu format upita za pristup podacima sa web stranice **(Tacno)**

2. **Kolacici (zaokruzivanje) –** vec objasnjeno u poglavlju sa proxy
3. **Komutatori zaokruzivanje –** vec objanjenji iznad
4. **Zaokruzivanje - rezervacija kanala** - je u sustini takodje CSMA/CA pristup za izbjegavanje kolizije gdje se kanal rezervise tako sto je uveden mehanizam sa dva dodatna paketa, prvo se ceka DIFS period zatim se salje RTS paket kojim se zahtjeva od odredista vrijeme potrebno za prenos gdje odrediste potvrjuje rezervaciju tog vremena nakon koga (tek nakon rezervacije!) krece transport podataka (znamo da smo ekskluzivni na medijumu).



Ova procedura je opciona jer povecava kasnjenje u mrezi.

2.DIO

1. Firewall i aplikacijske barijere, razlike

Razlika je u tome sta koriste kao skup mogucih ogranicenja za restrikciju saobracaja. Standardni firewall filtrira paket za paketom primjenjujuci fiksni skup pravila iz ACL tabele (kod statelles-a), pravila baziranih na osnovu IP, UDP i TCP zaglavlja tj. vrednosti polja zaglavlja. Statefull firewall pored fiksnih kriterijuma baziranim na IP, UDP i TCP zaglavljima takodje kotisti ta zaglavlja da prati „smislenost“ paketa koje filtrira.

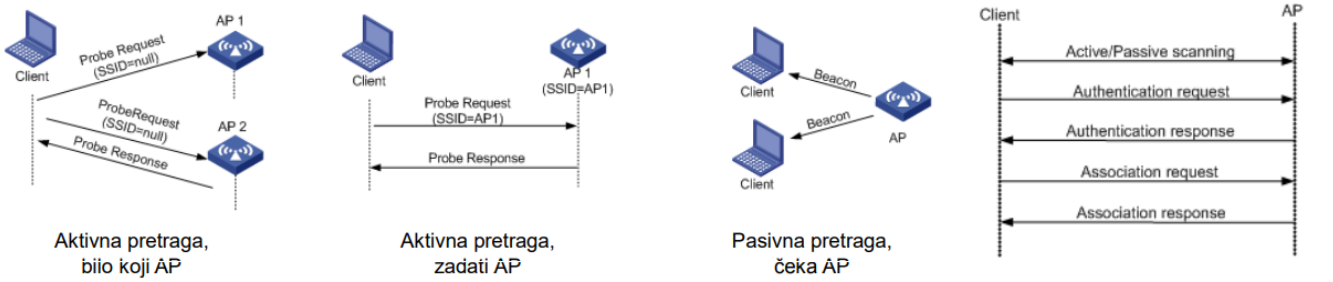
Aplikativne barijere prosiruju taj skup i pored pomenutih zaglavlja vrse filtraciju i na osnovu aplikativnih podataka (npr. dozvoli nekim internim korisnicima da koriste Telnet van loklane mrze.)

2. Objasni prikljucivanje baznim stanicama

Administracijom svaka pristupna racka (AP) dobija svoj SSID (Service Set ID) od jedne ili dvije rijeci kao i svoj opseg za prenos definisan brojem kanala. Jesan BSS moze imati vise AP povezanih komutatorom ako se njima dijeljeni kanali medjusobno ne preklapaju (povecanje propusnosti).

AP periodicno salje okvire za navodjenje (beacon) koji sadrze njen SSID i MAC adresu. Terminalske stanice tako dobijaju mogucnost prijave na osnovu MAC adrese ili lozinke. U toku rada terminal ostatak interneta vidi kao racunar u podmrezi bazne AP stanice.

Proces pridruzivanja klijenta pocinje pretragom raspolozivih WLAN (aktivno –terminal trazi AP, svaki ili prekonfigurisan; pasivno – terminal ceka navodjenje), zatim se autentifikuje nakon cega (ako je uspjesno) pridruzuje i moze poceti komunikacija.



Aktivna pretraga, bilo koji AP | Aktivna pretraga, zadati AP | Pasivna pretraga, čeka AP

3. **Sta je sustina radio prenosa u prosirenom opsegu? Kako se siri spektar signala u DS (Direkt Sequence) tehnici?**

Radio spektar je zajednicki resurs i mora se dijeliti pa od pravilne podjele i upotrebe raspolozivog opsega zavisi i sama uspjesnost komunikacije.

Spread spectrum (resireni spektar) vrsi prenos u opsegu sirem od informacionog te je bitno drugaciji koncept (u odnosu na frekventni i vremenski multipleks) koji je omogucio drasticno veci broj korisnika (dodatak: u frekventnom bi veci broj korisnika iziskivao precizniju podjelu frekventnih opsega sto je tesko izvodivo zbog preklapanja a u vrmenskom bi vrmenski prozori bili neefikasno uski). Prenosni opseg se ne dijeli nego svi koriste isti ali svoj signal raspoznaju zahvaljujuci pseudo slucajnom kodu cime se znacajno povecava otpornost na interferenciju signala (ne koristimo vise frekventnih domena pa da pazimo na preklapanje sa okolinom). Pseudoslucajni algoritam polazeci od pocetne vrednosti (sjeme-seed), deterministicki odredjuje sekvencu kojom se siri ulazni signal te je proizvedena sekvenca statisticki slucajna.

Interferencije izmedju kanala i susjednih celija nema ako obezbjedimo da su im pseudoslucajni kodovi RAZLICITI.

8. **TLS ili TLS zastita na TCP**

SSL obezbjedjuje zastitu na transportnom nivou za sve TCP-aplikacije (npr. izmedju web browser-a i servera za e trgovinu). Pruza sigurnosne usluge autentikacije servera, kripto-zastite podataka kao i opcionu autentikaciju klijenta. SSL. SSL mozemo posmatrati kao sigurnosnu nadogradnju TCP kao da se izmedju aplikacionog i transportnog sloja smjesti SSL podsloj koji je sa aplikacionim slojem povezan preko SSL soketa a sa transportnim TCP soketom.

SSL komunikacija se odvija u 3 faze sa tim da se nakon zavrsetka prenosa komunikacija zatvara:

- Rukovanje (Handshake) predstavlja autentikaciju servera i razmjenu kljuceva: uspostavlja se standardna TCP sesija uz dogovaranje o tipu enkripcije nakon cega server (Alisa) salje svoj sertifikat, klijent (Bob) kreira glavni kljuc, sifruje ga Alisinim javnim kljucem i salje je Alisi koja ga dekriptuje svojim privatnim kljucem.
- Key Derivation – na osnovu glavnog kljuca (Master Key- MS), Alisa i Bob generisu dva simetricna kljuca za sifrovanje jedan za smjer Alisa ka Bobu a drugi od Boba ka alisi kao i dva MAC kljuca isto za dva smijera. Ovo se radi zbog vece sigurnosti jer se razliciti kljucevi korsite u dva pravca komunikacije.

- Data transfer: TCP strim bajtova se dijeli na blokove od n bajta, za svaki blok se generise MAC kod koji se dodaje na blok pa se sve to sifruje simetricnim kljucem i zajedno sa otvorenim SSL zaglavljem (Tip, Verzija, Duzina) salje

9. Objasni razliku izmedju stateless i statefull sigurnosnih barijera. Koje podatke one koriste?

Stateless paket filteri su filteri bez stanja sto znaci da kao kriterijum filtriranja koriste samo fiksna pravila kada odlucuju da li paket smije proci firewall (kriterijum po portokolu, po ACK-u, portu i sl.) dok statefull filteri pored svakako restriktivne stateless metode ne dozvoljavaju prenos nekih paketa koji su nelogicni na nacin da prati status svake TCP konekcije:

- Uspostava (SYN, SYN+ACK, ACK)
- Prekid (FIN, ACK)
- Odlucuje da li neki od in/out paketa imaju smisla
- Ako nema aktivnosti (po isteku timeout-a) odbacuje neaktivnu vezu i brani dalji saobracaj paketa

Ove barijere koriste podatke iz IP, UDP, TCP zaglavlja.

10. SNMP, kodiranje (prezentacija) podataka u SNMP

SNMP (Simple Network Management Protocol) se sastoji od 4 kljucna dijela:

- Management information base (MIB)(Distribuirana baza mrežnih podataka, potrebnih za upravljanje)
- Structure of Management Information (SMI): (Definicija podataka u MIB(Management Information Base) objektima)
- SNMP protokol (Prenos komandi i podataka između upravljača i agenata, Podaci u sklopu upravljačkih objekata)
- Sigurnost i administracija (Glavna unapređenja u SNMPv3)

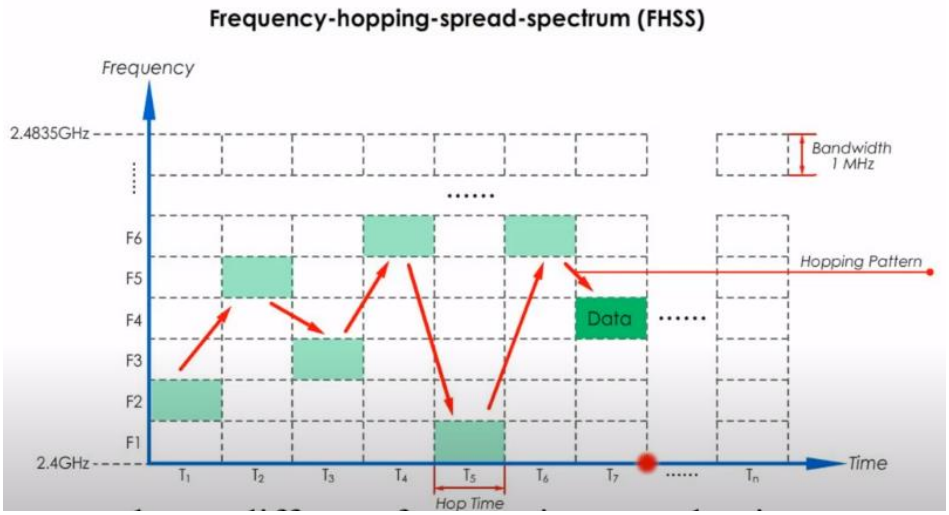
Dodatno: SMI definise sledece: osnovne tipove podataka, OBJEST-TYPE tipove podataka (definise tipove i znacenje podataka jednog upravljanog objekta), MODULE_IDENTITY (grupise vezane objekte u MIB modul).

Problem moze nastati usljed razlicitog formata i konvencije smjestanja podataka izmedju dva host-a (jedan big-endian drugi little, razlicit PACK). Najkorektnije rjesenje je da posiljalac prevodi podatke u foramat nezavisan od obe strane (standardizovan format-primalac zna sta da ocekuje kao prijem) koji se po prijemu prevodi u format primaoca. Koristi se TLV kodiranje

ASN.1 objekata podataka (slicno SMI). Ideja TLV kodiranja jeste slanje podatka koji sam sebe identifikuje tj polje T (Type) opisuje tip podataka(jedan od ASN.1 tipova), L (Length) opisuje duzinu u bajtima dok V (Value) opisuje vrijednost podatka kodirana po ASN.1. standardu.

1. Objasni FHSS

FHSS (Frequency Hopping Spread Spectrum) je jedna od tehnika prenosa u rasirenom opsegu gdje se signal prenosi na razlicitim frekvencijama koje se mijenjaju u pseudoslucajnoj sekvenci poznatoj na obe strane (kljucno). Drugacije receno signal ce jedan vremenski period biti unutar jednog frekventnog opsega, narednom u drugom i kada se prate te promjene uocava se kao da signal skakuce iz opsega u opseg gdje se nakon nekog vremena uocava uzorak skakanja tj hopping pattern. Poenta svega ovoga jeste nepredvidivost tj da zlonamjerni napadac presreo paket mora da poznaje hop pattern.



5. IPSec

Predstavlja zastitu IP sloja koja pruza tajnost na mreznom nivou na nacin da predajni racunar sifruje podatke u IP datagramu, pruza mogucnost autentifikacije izvorisne IP adrese. Koriste se dva osnovna protokola Authentication Header (AH) i Encapsulation Security Protocol (ESP) gdje za oba navedena postoji handskahe izvora i odredista gdje se kreira logicki kanal na mreznom nivou koji se naziva security association (SA) koji je jednosmjeran i jedinstveno odredjen sa protokolom (AH ili ESP), source IP address i 32-bit connection ID.

AH omogucuje integritet i autentifikaciju ali ne i povjerljivost a ESP integritet, autentifikaciju i povjerljivost te je sire koriscen od AH.

Veoma je pogodan za zastitu komunikacije izmedju dva udaljena dijala jedne mreze (centrala i kancelarija) te takodje omogucuje sigurnu vezu preko javnog interneta (VPNs) ali je i svojevrsna prevencija „snimi i ponovi“ napada. IP je connectionless a IPSec je connection-oriented. Najznacajnija i najcesce koricena kombinacija je tunelovanje (krajnji ruteri realizuju IPSec funkcionalnost, krajnji racuanri ne moraju) u rezimu ESP.

4. **Kako se zove i kako se izvrsava protokol slanja kod Wi-Fi mreza? Koja je od kljucnih razlika u odnosu na zicni Ethernet?**

Razlika izmedju Ethernet-a i Wi-Fi se u osnovi bazira na rukovanju kolizijama, Ethernet koristi CSMA/CD algoritam gdje detektuje koliziju i suspenduje slanje na slucajan period prije no sto ponovo oslusne sto znaci da se mehanizam zasniva na detekciji kolizije dok se kod Wi-Fi koristi CSMA/CA algoritam koji se zasniva na izbjegavanju (nema detekcije) kolizije te se realizuje na nacin da:

- Postupak slanja se pokrece tek ako je kanal slobodan bar DIFS vrijeme
- Predajnik pokrece brojac (backoff time) na slucajnu vrijednost koja je manja od CW-a (Collision Window) i odbrojava sve dok je kanal slobodan dok se u suprotnom brojac zamrzava.
- Po isteku brojaca smo sigurni da je kanal SIGURNO slobodan pa stanica salje cio okvir i ceka potvrdu
- Izostanak ACK-a inkrementira CW a prijem ACK-a vraca CW na min. vrijednost
- Ako ima jos paketa predajna stranica se vraca na korak 2 (pokretanje brojaca)

Prostije receno, DIFS sprecava da sve spremne stanice zajedno napadnu kanal u istom trenu i izazovu koliziju te ce poceti da salje ona kojoj prvoj istekne backoff brojac (ali stranice koje su medjusobno skrivene mogu da naprave koliziju).

5. **Nabroj i objasni tri osnovna elementa zastite komunikacije izmedju dva ucesnika, Sta se stiti?**

Povjerljivost: Samo posiljalac i primalac mogu da „razumiju“ sadrzaj poruke za sta se koriste metode kripto zastite tako da posiljalac sifruje poruku a primalac desifruje poruku.

Autentikacija: Posiljalac i primalac treba da medjusobno (jedan sa drugim) potvrde identitet

Integritet poruke: posiljalac i primalac nastoje da obezbjede da se poruka ne moze mijenjati (u prenosu ili naknadno) neovlasceno i neprimjeceno.

Pristup i raspolozivost: servisi moraju da budu pristupacni i raspolozivi korisnicima.

6. Objasni sustinu TLS zastite i koji dio TCP segmenta je zasticen

Ima TLS (SSL) vec objasnjen uz napomenu da je cio TCP paket zasticen (I preko racunatog MAC-a pa enkriptovan zajedno sa njim).

7. Sustina radio prenosa (Frequency Hop)

Sustina radio prenosa jeste to da se vazduh iskoristi kao medijum za prostiranje elektormagnetnih talasa – neogranicen medijum . Osnovne osobine (domet, prostiranje) radio prenosa direktno zavise od frekvencije radio talasa. Raspolozivi frekventni opseg se dijeli u opsege i kanale. Komunikacioni uredjaji se razvijaju za rad u ograniceniom opsegu. Podjela spektra je tehnicko ali i politicko pitanje te posotoje tijela na svjetskom nivou koja propisuju opsege i njihovu primjenu.Radio talasi putuju kroz vazuh ili vakuum u svim pravcima a na povrsinama kao sto su jonosfera ili tlo dolazi do refleksije. Sama informacija se prenosi sistemskim mijenjanjem neke osobine radio talasa kao sto je aplituda frekvencija ili faza (odatle proizlaze razlicite tehnike modulacije). Pijem signala podrazumjeva prihvat indukovanog signala sa antene koji se po tom demodulise. Kvalitet prijema direktno zavisi od kolicine energije radio talasa uhvacene preko radio prijemnika.

Problem slabljenja ili izoblicavanja je najcesce smanjenje jacine signala (gubitak signala usljed povecanja udaljenosti, apsorbcija od strane nekih materijala, prepreke i sumovi), smetnje od strane drugih izvora (interferencija sa uredjajima u okolini tj. problem skrivenog terminala), zamucivanje signala usljed odbijanja o razlicite objekate ili zemlju pa radio talasi na odrediste stizu putanjama razlicite duzine.

Frequency Hopping je objasnjen vec iznad.

6. Malware napadi i tipovi

Malware je neprijateljski invazivni program koji ometa normalan rad racunara te se cesto samostalno sire i repliciraju preko zarazene mreze zombi racuanra (botnet). Javljaju se u razlicitim formama:

- Virus (infekcija zahtjeva aktivnu radnju korisnika npr. da otvori fajl u prilogu mail-a, replicira se zapisom na lokalnom racunaru i dalje se siri preko mreze)
- Worm (za razliku od virusa infekcija je pasivna, aktivira se sam po prijemu na napadnuti racunar i replicira se sam dalje)
- Trojanski konj (skriveni dio nekog legitimnog softvera)

- Spyware (spijunira i snima razlicite akcije korisnika)

Spoljni napadi su napadi sa nekog drugog racunara u mrezi i najcesce se ogledaju u:

- Spam-u – slanje brojnjih nezeljenih poruka
- DoS onemogucava uslugu na nacin da napadaci preuzimaju mrezne resurse (zlonamjerni racunari konstantno spamuju server sa zahtjevima za uslugu) i time ih cine nedostupnim za legitimne korisnike. Ne moze se sprijeciti jer je ranjivost sama koncepcija pruzanja usluga u klijent-server modelu.

Packet sniffing je tehnika prisluskivanja saobracaja unutar dijeljeni ethernet i wireless mreza gdje racunar u mrezi moze primiti sve pakete i snimiti sadrzaj (sto mu korsiti ako sadrzaj nije enkriptovan).

IP spoofing je slanje paketa sa laznom source adresom (predstavljanje kao neko drugi).

---

1. **Sirenje spektra (zaokruzivanje)**
   Odgovor: pseudoslucajan kod, pogledaj Frequency Hopping.

2. **Podjela spektra u kodnom prostoru:**
   1) Zahtjeva punu sinhronizaciju svih radio ucesnika
   2) Koristi deterministicki odredjen pseudoslucajan kod **Odgovor**: (Druga formulacija prethodnog pitanja, tacno)
   3) Obezbjedjuje potpuno potiskivanje nezeljenog signala
3. **Oznaci ispravne tvrdnje:**
   1) algoritmi simetricne kriptografije koriste pretezno jednosmjerne funkcije
   2) MAC kod za autentifikaciju poruke se racuna pomocu hash funkcija **(Tacno)**
   3)Autentifikacija korisnika je najpouzdanije pomocu nonce broja R i javnog kljuca
4. **Oznaci ispravne tvrdnje:**

1) 802.11 mreze koriste modifikovan AES algoritam za kriptovanje saobracaja **(Tacno)**

2) WEP zastiti prethodi distribucija dijeljenog simetricnog kljuca Ks

3) Slabost WEP algoritma je uzrokovana ponavljanjem inicijalizacionog vektora IV **(Tacno)**

7. **Broadcast domen kontrolisu ruter i wlan switch – zaokruzivanje** (Nez sta je bilo ponudjeno al vjerovatno je oko toga da svi uredjaji nize od Internet sloja ne prekidaju

broadcast domen pri tome se misli na mostove, switcheve, hubove jedino su ruteri koji su na Internet sloju ti koji prekidaju broadcast domen. Izuzetak je jedino switch u kontekstu VLAN-ova gdje on tada organizuje svaki VLAN kao poseban broadcast domen a inace ne). A sto se tice kolizionih domena brigde, switch i sve ostalo „inteligentnije“ prekida kolizione domene dok uredjaji tipa hub to ne rade.