Predavanje 1

Kako znamo je li problem sa hardverom ili softverom?
Uglavnom, ako se počne podizati operativni sistem, najvjerovatnije je onda problem sa softverom, jer ako postoji hardverski problem koji se može otkriti tokom paljenja računara, on bi trebao spriječiti pokretanje operativnog sistema.
Šta znači da su naši podaci sigurni/nesigurni?
Ako je nešto pravilima zabranjeno, sve što narušava ta pravila je narušavanje sigurnosti.
Domenska imena - ima ih reda 100 miliona.
Administrator operativno upravlja računarskom mrežom.
Administracija računarskih mreža nije samo administrativni problem nego i inženjerski(otkrivamo i rješavamo probleme). Većina usluga se radi za zajednicu korisnika.
Pretpostavimo da smo mi zaduženi za novu mrežu, prvo treba izabrati hardver(računari, akrivna mrežna oprema, ruteri, svičevi, acces pointi) zatim na taj hardver treba izabrati i instalirati softver.
Kompletan taj sistem koriste korisnici i dobar dio posla administratora je podrška korisnicima. Treba povremeno raditi dijagnostiku – provjera šta se dešava u mreži, šta ne radi. Cilj mreže je da ima funkcionalnu ulogu za korisnike.
Hardver je fizička stvar, ima interakciju sa okolinom. Hardveru moramo pružiti odgovarajuće uvjete, inače neće raditi. Hardver ograničava softver. Softver nema fizičke interakcije.
Ono za šta je mreža namijenjena zavisi od njene svrhe. Svrha određuje prioritet u radu administratora mreže. Ono što služi osnovnoj funkciji sistema ima prioritet.
Treba imati znanja, ukoliko nešto ne znamo, ne treba „čačkati". Administrator uglavnom može pristupiti privatnim i poslovnim podacima korisnika. Postavlja se pitanje kako to spriječiti (npr. banke svojim uposlenicima daju povoljne kredite). Može se spriječiti na razne načine: prijetnjama, molbama, finim ponašanjem i sl.
Da bi se definisalo šta administrator smije, može, za šta se koristi sistem – postoji sistemska politika.
Izazovi: Dizajn logičke i efikasne mreže, Priključivanje velikog broja računara sa mogućnošću budućeg lakog ažuriranja i proširenja, Utvrđivanje potrebnih usluga, Planiranje i realizacija odgovarajuće sigurnosti, Stvaranje ugodnog okruženja za korisnike, Upravljanje znanjem
Šta je cilj?
Generalno mreža treba da podrži veliki broj računara i da bude proširiva(skalabilnost).
Treba znati šta su dobri izvori informacija.
Operativni sistemi i aplikativni softver imaju bugove. Administratori najčešće koriste gotov tuđi softver čijem izvornom kodu nemaju pristup. Treba se snaći u gotovom softveru u kojem ne možemo otkloniti bugove. Mora se naći rješenje koje zaobilazi taj bug.
Sistemska administracija kreće od politike – odluke o tome što želimo i kako treba da bude s obzirom na to što možemo priuštiti.
-Predvidljivost – administrator treba da teži predvidljivom sistemu koji je osnova pozdanosti.
-Skalabilnost – skalabilni sistemi mogu rasti u skladu s politikom, oni se ponašaju predvidljivo, čak i kad se povećavaju.
Treba da imamo sistem za koji znamo kako će se u različitim situacijama ponašati. Treba odbacivati stara znanja i sticati nova. Vlasnik firme definiše šta su prioriteti. Računarska mreža i usluge koje pruža imaju svrhu (poslovna, obrazovna..) koja rukovodi postupke i odluke administratora.

Predavanje 2

Sistem kojim upravljamo tj. računarska mreža se sastoji od korisničkih uređaja (tableti, računari, mobiteli).Ti uređaji se međusobno i sa ostatkom svijeta povezuju pomoću mreže(kablovi, uređaji koji omogućavaju to povezivanje). Zadnja komponenta su korisnici. Hardver je osjetljiv. Zašto treba gasiti uređaje prije nego što ih izvučemo iz struje? Da se ne bi oštetio neki dio. Kad ga ugasimo uredno se završi kompletan proces. Operativni sistem uglavnom drži informacije u kešu, kada ga ugasimo sve se to upiše na disk. Možemo oštetiti konektore ako pogrešno ih ubacujemo. Statički elektricitet može oštetiti hardver.
Uticaj okoline na hardver – munje (zaštita od visokih napona), napajanje (UPS-nešto kao akumulator). Računari su osjetljivi na loše uslove. Kada im je vruće pregriju se i počinju lošije raditi. Visoka vlažnost je korozija, niska vlažnost je statički elektricitet. Toplota, hladnoća i vlažnost – klimatizacija.
SATA je serijska konekcija, a PATA je paralelna. Kako je serijski brži od paralelnog? Jednostavniji, dovoljno brzo možemo slati. SSD su brži od tradicionalnih diskova. Prvi SSD diskovi su bili USB stikovi. Ako imamo dva diska, SSD i tradicionalni. Na SSD disk operativni sistem i aplikacije, a na drugi podatke.
Opretivni sistemi - upravljanje uređajima, datotečni sistem. Omogućava komunkaciju sa korisnicima. Savremeni OS – više zadataka istovremeno, više korisnika. Unix(oidni) sistemi – Linux, MAC OS, iOS, Android. Windows ima sisteme koji su namijenjeni za desktop i serversku distribuciju. Razlika je svrha. Ako ce biti desktop ne treba nam dns server, mail server. Ako ce biti server, ne treba nam grafičko okruženje. Kućni računar nije bio višekorisnički. Kada je počelo više ljudi koristiti jedan računar, javila se potreba da se odvoje podaci i da se zaštite.
Višekorisniči sistemi – ograničavaju šta obični kornsik može. Postoji privilegovani korsnik. Na windowsu se zove administrator, na unixoidnim root. To su korisnici koji imaju sva prava sistema. Oni služe da pripreme okruženje za druge korisnike. Ne bi trebalo da se računar koristi pod prijavom privilegovanog korisnika. Zašto? Jer privilegovani korisnik nema ograničenja. Napravimo grešku, nešto obrišemo, pokrenemo zlonamjerni softver. To što radimo imat će posljedicu na sve korisnike sistema. Ako smo prijavljeni kao obični korisnik, sve greške, sav zlonamjerni softver će uticati na nas kao jednog korisnika. Kad smo prijavljeni kao administrator i kad hoćemo da instaliramo nešto pojavi se poruka, upozorenje da može imati posljedice. Na unixoidnim sistemima se koristi

sudo(superuser do). Princip minimalnih privilegija – Svaki korisnik treba da ima onoliko prava koliko mu je neophodno da obavlja svoje poslove, ni manje ni više. Ne prijavljivati se kao privilegovani korisnik, osim ako to nije neophodno. Datotečni sistem omogućava da bite na disku organizujemo organizujemo u bajte. Da ne predstavljaju niz bita bez značenja, nego organizovane bite koji predstavljaju neki sadržaj. Kroz datotečni sistem se upravlja pravima pristupa. Unixoidni datotečni sistemi. Uglavnom su hijerarhijski organizovani – kao stablo. Prava pristupa – unixoidni datotečni sistemi imaju implementirana prava pristupa. Windows datotečni sistemi – particije(nezavisni diskovi A:,B:,C:...). Organizacija je također hijerarhijska. Kod windowsa ekstenzija datoteke je bitna.

Sve što se dešava na OSu, svaki program koji se pokrene je proces. Procesi mogu biti oni koji se izvršavaju u pozadini, koji nemaju direktnu interakciju sa korisnikom, i imaju oni foreground procesi, koji imaju direktnu interakciju sa korisnikom. Ti se procesi izvršavaju pod prijavom korisnika koji ih je pokrenuo. Svaki ima svoj ID. Ako jedan proces pokrene drugi, onda je jedan roditelj, a jedan dijete. Ako se roditelj proces prestane izvršavati, onda je dijete zombi proces. Varijable okruženja su definisane varijable kojima svi programi mogu da pristupe.

Računarska mreža

Mreža je povezana skupina autonomnih računara. Svaki od čvorova u mreži, od uređaja u mreži je nezavisan uređaj. To što je povezan u mrežu daje mu dodatnu funkcionalnost da razmjenjuje informacije. Da bi mogli komunicirati, mora biti neki medij preko koga komuniciramo. Dva su načina, kroz kablove, dakle neki fizički medij, ili bezično (elektromagnetni talasi). Prednost kablova je da su bolje zaštićeni od vanjskih uticaja i veći je domet. Prednost bežičnog prenosa je da je jednostavnije i jeftinije. Ethernet je dominantan žičani protokol. Drugi dominantan protokol je bežični wifi 802.11.

U URLu se nalazi domensko ime, aplikacija je uradila poziv DNSu i došla do IP adrese. Operativnom sistemu kaže evo ti poruka koju treba da pošalješ, IP adresa na koju treba da pošalješ i port. Port je adresa aplikacije na tom računaru. IP adresa služi da se dođe do odredišnog računara, a port da se zna kojoj aplikaciji na toj računaru. OS prvo doda TCP ili UDP zaglavlje. U tom zaglavlju se nalazi odredišni port aplikacije. Dodaje se IP adresa odredišta. Šta se dalje dešava sa tim paketom? OS taj paket šalje NIC-u (network interface card), ona mora dodati DataLink zaglavlje. Ona što dobije od IP, na to dodaje svoje zaglavlje koje sadrži MAC adresu.

Šta radi switch kad dobije paket. Ako dolazi paket koji ide na MAC adresu 2. Switch ima tabelu u kojoj piše MAC adresa i interfejs(port). Switch dobije paket, nađe MAC adresu odredišnu i nađe interfejs na koji treba da proslijedi paket i tu je switch završio. Sve je to uredu dok se taj računar nalazi u istoj mreži. Šta ako se adresa nalazi u drugoj mreži, npr. facebook? Naš switch ne zna MAC adresu facebook-a jer nije u toj mreži. Šta se dešava kad šaljemo paket na facebook, znači kad nije u lokalnoj mreži?

Šta radi ARP zahtjev? Daje MAC adresu za neku IP adresu. ARP zahtjev se šalje kao broadcast. Switch šalje na sve svoje interfejse. Ali pošto facebook nije u našoj mreži, neće dobiti taj zahtjev. Treba nam defaultni gateway. Postoji IP adresa, kao defaultni gateway. Defaultni gateway je čvor preko kojeg možemo pristupiti uređajima koji nisu u našoj mreži. Da bi mogli poslati nešto defaultnom gatewayu, on mora biti povezan na switch. Default gateway je najčešće ruter. Ruter je uređaj koji odvaja/spaja dvije mreže. Switch dobije paket na IP adresu. Switch ne zna IP adrese nego MAC adrese. Switch dobije paket, pročita tabelu, ako ima preslikavanje, proslijedi na taj interfejs. Ako dobije neki paket na MAC adresu koju nema u tabeli, ili na broadcast adresu, šalje na sve uređaje. Moramo nekako naznačiti da je poruka za ruter, tj. za facebook ali preko rutera. Moramo poslati paket na MAC adresu rutera. MAC adresu ćemo dobiti pomoću ARP-a. ARP se pošalje na broadcast adresu, ruter se javi da je njegova, i zapamtit će njegovu MAC adresu, te se paket vrati do računara koji dobija informaciju koji je default gateway i njegovu MAC adresu, te šalje paket na njegovu IP adresu.

Kad podešavamo parametre, imamo IP adresu, default gateway, subnet maska i DNS server. Subnet maska nam govori koliko je bita IP adrese fiksirano. Računari koji imaju istu subnet masku, i toliko bita jednakih se nalaze u istoj podmreži i mogu direktno komunicirati. Ako tražimo neki računar u lokalnoj mreži, stavljamo MAC adresu tog računara. Pomoću subnet maske provjeravamo da li je neki računar u njegovo podmreži. Ukoliko su fiksirani biti jednaki, onda su u istoj podmreži. Osnovna namjena subnet maske je da pomogne da se odredi da li je neki računar u istoj podmreži. Dva računara su u istoj podmreži ako imaju istu subnet masku i toliko prvih bita jednakih. Ako šaljemo na odredište u lokalnoj mreži, on će napravit ARP upit za adresu iz te mreže, računar dobije upit i vrati odgovor. I u tom slučaju će poslati paket u kom će pisati MAC adresa tog računara. To što je uređaj dobio paket, ne znači da je paket za njega. Može biti poslan na broadcast adresu. On prvo treba da provjeri da li je paket za njega. Pogleda MAC adresu, ako je njegova gleda IP adresu. Ako je i ona njegova, paket je za njega i dalje ga raspakuje, provjeri port i proslijedi aplikaciji. Šta ako je IP adresa izvan lokalne mreže? Kome treba poslati paket? Poslat će zahtjev za MAC adresu default gatewaya. Kako pravi paket? Piše se MAC adresa default gateway-a, a IP adresa odredišta. Paket dolazi do switcha, switch vidi da je MAC adresa DG-a i prosljeđuje paket DG-u. DG će vidjet da je MAC adresa prijemnika vidjet njegova, kad raspakuje vidjet će da nije njegova IP adresa. DG kad dobije paket, skine zaglavlje, ne zanima ga ostatak, nego samo IP zaglavlje. Šta dalje radi ruter? Ruter radi dvije stvari. Jedna je usmjeravanje, odnosno prosljeđivanje, treba da odredi na koji interfejs da proslijedi paket. Ruter ne radi sa MAC adresama, nego sa IP adresama. Ruter ima tabelu rutiranja. Kad se i kako formira ta tabela. Ruter ima tabelu rutiranja, ona kaže sve mreže do kojih se može doći, i preko kojih mreža. Rutiranje bi trebalo kroz jedan proces da bilo koja adresa koja se otkuca, da ruter zna kojim putem treba poslati paket. Postoji defaultna ruta, sve što ne znaš šta će, proslijedi na neki tamo interfejs. Svaki ruter bi trebao da zna sve, ali obično imaju u tabeli rute do rutera koji su dio njegove mreže. U ruter, u trenutku kad dođe paket već ima izračunatu rutu. Svaki ruter kad se upali, definišemo IP adrese i interfesje, i kažemo koji protokol rutiranja koristi. Ruter kad se upali, pošalje poruke drugim ruterima u mreži, razmijene informacije, ko do koga može doći. Nakon toga ruter ima tabelu rutiranja. Mi samo podesimo interfejse, i tabela rutiranja se automatski formira.

Ruter dalje šalje paket za rutu prema facebooku. Šta će uraditi sa paketom. Ima paket u kome oiše IP adresa odredišta, i sadržaj paketa. Ruter stavlja MAC adresu sljedećeg rutera. Ponovo se šalje ARP zahtjev. Ruter ima u svojoj tabeli IP adresu tog rutera, tj. next hop. Saobraćaj koji ide od jednog rutera do drugog rutera, je isti kao od računara do rutera. U sljedećem ruteru se dešava

isto, skida zaglavlje, stavlja svoje zaglavlje i šalje dalje. Kada dođe do posljednjeg rutera, šta će se desit? Skine zaglavlje, piše IP facebooka i njegov sadržaj. Šta će ruter uraditi? Pošto je facebook direktno vezan na ruter, u tabeli piše IP adresa facebooka, i za next hop piše da je direktno vezan. Pravi ARP upit na IP adresu facebooka, i dobija MAC adresu i šalje paket. Provjeri se MAC adresa, IP adresa zatim port, te se tom portu proslijedi taj zahtjev.Zašto nam treba IP adresa pošiljaoca? Da bi se vratio odgovor. Subnet maska služi da pošiljaoc odredi da li je odredište u njegovoj podmreži. Default gateway moramo imati ukoliko nisu svi računari u lokalnoj mreži. To je IP adresa preko koje šaljemo pakete za računare koji nisu u lokalnoj mreži. Put kojim je došao paket se ne pamti. U konfiguraciji računara piše njegova IP adresa, Default gatewaym subnet maska i adresa DNS servera. DNS je usluga koja omogućava pretvaranje domenskih imena u IP adresu. Kakva je razlika ako nam je kao DNS server podešen etf-ovski, a šta ako je google-ov. Razlog za google je pouzdanost.
Šta je NAT? Ukoliko imamo računar A, i šaljemo paket na adresu facebooka,kad izađe iz lokalne mreže, on dobija IP adresu vanjskog interfejska rutera. To se radi jer su adrese u podmreži privatne. IP adrese bi trebale biti jedinstvene, ali nema dovoljno IP adresa, pa su određene klase adresa. Privatne se adrese mnogu ponavljati u više lokalnih mreža, a na internet izlaze sa javnom IP adresom. Jedna ideja NATa je da se štede IP adrese, a druga je zaštita. Ako pošaljemo paket do facebooka, njegov odgovor ide na adresu vanjskog interfejsa rutera. Kako ruter zna za koga je paket. Ruter napravi tabelu u kojoj treba da bude pošiljalac, primalac. Paket dolazi sa neke IP adrese i porta. Zapamti se IP adresa i port primaoca. Port primaoca služi da znamo kojoj aplikaciji je poslan paket. Port pošiljaoca služi da znamo koja aplikacija šalje paket. NAT pamti i informacije o pošiljaocu (IP adresu i port). Zamijenit ću IP adresu pošiljaoca sa adresom vanjskog interfejsa, ali mijenjam i port. Stavlja se neki random broj. Kad dođe paket sa računara A sa porta 30000, da mu se npr 10002. Kad se vrati paket, ako ide na 10002, znači da je došao sa facebooka za računar A na port 30000.

Predavanje 3.

Virtuelno je nešto što je prividno, nije stvarno. Virtuelna memorija – memorija koja je prividna programima. Misle da pristupaju ramu, a ustvari pristupaju disku. Virtualne privatne mreže – ako je neki korisnik udaljen, mreža preko koje on komunicira je javna, ali se spaja na privatnu mrežu, stvara se privid privatne mreže, ali je ustvari javna. Većina softvera komunicira sa hardverom preko nekog interfejsa, operativni sistem priča sa harverom preko drivera. Šta je virtuelna mašina? Mi smo operativnom sistemu stvorili privid da postoji računar koji je njemu na raspolaganju, sa memorijom, diskom itd. On je dobio samo dio fizičkog hardvera na kojem postoji. Virtualizacija omogućava da se istovremeno na jednom hardveru izvršava više operativnih sistema i da oni međusobno komuniciraju. Virtualizacija omogućava da u jednom trenutku, na jednom računaru izvršava više operativnih sistema, od kojih svaki misli da se izvršava na posebnom hardveru. Mi možemo imati operativni sistem na jednoj lokaciji, i prebacit ga na drugu lokaciju, tako što samo kopiramo. Virtualnim mašinama možemo podijeliti samo onoliko resursa koliko imamo. Neke stvari se mogu preklapati pod uslovom da se neće sve virtelne mašine izvršavati u isto vrijeme.
Kako to sve radi? Postoji harver(diskovi, ram,CPU, ostali resursi). Na tome se izvršava komad softvera. Postoji i Virtual Machine Manager. Svi upiti OS-a prema hardveru prolaze kroz Virtual Machine Manager. Broj mašina koje možemo podići na nekom računaru određuju resursi i zahtjevi virtuelnih mašina. Ne možemo podići više VM-a nego što imamo resursa. Koja je koristi od VM-a? Troši se manje struje. Virtuelna mašina troši minimalno struje ako se na njoj ništa ne radi. Manje je potrebno hlađenja, manje kablova,manje mrežnih switch-eva i manje fizičkog prostora. Lahko je „premjestiti“ virtuelnu mašinu sa jedne fizičke na drugu lokaciju, svodi se na kopiranje file-ova sa jedne lokacije na drugu. Ako joj porastu potrebe, npr. veći disk, u konfiguracijama se to poveća. U slučaju da se hardver pokvari, prebacimo VM na drugi ispravni hardver. Da bi se to uradilo, postoji virtual machine monitor. Pokretanje virtuelne mašine je kao i pokretanje računara. Mi virtuelizacijom ne možemo stvoriti resurse koje nemamo. Pretvaranje fizičkih resursa u virtuelne fizičke resurse radi Virtual Machine Manager. Mi ne pričamo direktno sa hardverom, nego sa softverom koji priča sa hardverom. Virtuelna mašina je skup datoteka. Jedna je datoteka konfiguracijska. Imamo folder koji se zove kao i VM. Posebna datoteka je hard disk, datoteka koja predstavlja memoriju itd. Virtuelnoj mašini možemo sačuvati stanje. Deep freeze – umjesto da pišemo po pravom hardveru, pišemo u datoteku, te kad se ugasi računar briše se. Virtuelne mašine imaju snapshoot. Tako čuvamo stanje mašine. Zbog toga je lahko prebacivati virtuelnu mašinu, jer je skup datoteka. Napravimo VM, instaliramo softver i ako želimo na 10 računara istu konfiguraciju i samo iskopiramo. Monitor VM obavlja mapiranje virtuelnih i fizičkih resursa.Prilikom kopiranja moramo promjeniti ime servera i IP adresu jer moraju biti različiti. Ako otkaže jedan server, prebacivanje na drugi server je jednostavno. Virtuelnu mašinu možemo premještati bez gašenja. Postoje 2 tipa hipervizora. Tip1-nema i Tip2-ima.
Umrežavanje virtuelnih mašina. Može da nema nikakve mreže, nema komunikacije sa drugim mrežama. NAT je defaultna postavka, taj OS se ponaša kao da između njega i mrežne kartice OSa NAT. On ima puni pristup svemu čemu ima i pristup host operativni sistem, ali paketi prema njemu kad se vraćaju moraju da prođu kroz NAT. Dakle u drugoj je mreži od host OSa. Premošteno (bridged) – ponaša se kao da je zakačen na isti switch kao i host, bukvalno ima se utisak da je iz njega kabl utaknut u switch kao i host pa može komunicirati sa hostom. Njegova IP adresa je dostupna svim računarima unutar mreže. Interna mreža nema izlaz na internet. Mreža samo sa monitorom VM-host only.
Virtuelizacija kontejnerima – izvršava se na OS. Stvara samo izvršno okruženje za aplikacije, a ne kompletan prividni računar ili OS, sve aplikacije u kontejnerima na računaru dijele OS, nema poseban OS za svaku aplikaciju.
Instaliranje operativnog sistema
Prilikom instalacije operatovinog sistema se možda instaliraju neke komponente koje su nepotrebne i koje troše resurse na našem računaru. Računari se dijele po namjeni na serverske i klijentske. Serverski pružaju uslugu većem broju korisnika, a klijentski jednom korisniku. Serverskim računarima ne treba grafičko okruženje. Windows ima strogu podjelu na serverske i klijentske operativne sisteme. Informacije o računaru: ime, ip adresa i subnet maska, ime domena, lokalna vremenska zona... Serverima najčešče mi dajemo IP adresu, ne dobija od DHCP-a, jer IP adresa mora biti uvijek ista, a od DHCP-a se dobije svaki put različita.

Moramo imati jednog privillegovanog korisnika za svaki operativni sistem. Servisi su softveri koji se izvršavaju u pozadini i pružaju odgovarajuću uslugu. Kako aplikacije zovu DNS? Ne komunicira direktno sa DNSom, nego se obraća servisu na računaru, a onda taj servis kontaktira DNS. Svaki od servisa kad se pokrene, troši dio rama na računaru. Instalacija androida – integrisan je tijesno OS sa hardverom, zato ne možemo androit generički instalirati na bilo koji uređaj. Nekad, način da imamo više OS na istom računaru je dual boot. Na različite particije možemo instalirati različite operativne sisteme. Prije pokretanja računara, pokrene se boot manager i koji pita koji OS želimo pokrenuti. Kad se pokrene jedan OS, drugi samo stoji na disku, ne može se pokrenuti.
Kloniranje – omogućava da na lakši način istu instalaciju operativnog sistema i softvera instalira na više računara. Koristi se instalaciona datoteka. Fizička kopija diskova ili particija (promjena IP i imena).
Licenciranje softvera – pravo korištenja i mijenjanja. Striktna kontrola – dolazi u izvršnom obliku, ne možemo mijenjati ni koristiti bez saglasnosti proizvođača (npr. Microsoftov softver). Postoje i liberalne licence sa open source kodom kod kojeg možemo mijenjati, koristiti i sl. Kako se instalira softver? Izvršna verzija ili izvorni kod. Linux ima mogućnost instalacije iz paketa. Većinu softvera bi trebalo instalirati iz paketa Svaka distribucija ima svoju formu paketa. Paket je instalacioni softver koji u sebi ima definisano šta mu sve treba da bi radio, i prilagođen je instalaciji na toj konkretnoj distribuciji. Instalacija iz paketa je prilagođena instalaciji na toj distribuciji. Ako neki softver nema za našu distribuciju linuxa, ili izbačena nova verzija softvera,a nija izbačena u pakete, treba vršiti instalaciju iz izvornog koda. Instaliranje iz izvornog koda se češće radi na linuxu. Instalacija iz izvršnog koda se sastoji iz dva dijela: pravljenje od izvornog koda izvršni kod, drugi dio je da se napravi datoteka, i kad na nju kliknemo da se izvši.Drugi način je da naš file bude dostupan kroz okruženje OSa. Da bi instalirali nešto iz izvornog koda moramo imati razvojno okruženje(kompajler i linker). Standardna instalacija na linuxu ima tri koraka: odemo u folder gdje smo raspakovali softver,
zatim ./configure, make, make install. Ukoliko se jave greške, gleda se prva pa zadnja. Zadnja greška je posljedica prve greške.
Kad upalimo računar šta se dešava?
Kad pritisnemo dugme za paljenje, šalje se signal matičnoj ploči da pokrene proces za paljenje računara. Na matičnoj ploči se nalazi komad trajne memorije, u kojem se nalazi BIOS, on omogućava da se pokrene računar. Prva stvar što uradi je da provjeri na matičnoj ploči koji se nalazi hardver. Provjeri preko sabrinice ko mu se sve javlja. Vrši neke testove da li hardver radi. Ako ne dobije preko sabirnice odgovarajući odgovor, znači da ne radi kako treba. Ako neki dio ne radi, prikaže na ekranu, ako je problem sa grafičkom karticom, onda javlja zvučnim signalima. Bilo kakvo odstupanje od normalnog se ispisuje na ekranu, ili se javlja zvučnim signalima. Ako provjera hardvera prođe uredu, nakon toga pokreće operativni sistem. Gleda sve trajne medije sa kojih može da se pokrene OS. U BIOSu je definisano kojim redom će se pretraživati mediji. Kad pronađe medij onda sa tod medija pokrene boot manager. Ako ima samo jedan operativni sistem, onda pokreće OS. Ako ima više OS-a, onda nudi da izaberemo koji želimo pokrenuti.
Kod linuxa ima init proces koji pokreće sve druge procese. U unixoidnim sistemima postoji run level – definiše programe koji će se pokrenuti: 0 gašenje, 1 jednostruki način rada, 6 ponovno pokretanje, 2-5 višekorisnički, 5 GUI, 3 bez GUIa sa mrežom, 2 bez GUI i mreže. Kod windowsa je definisano u registrima šta će se pokrenti. Safe mode- pokretanje minimalnog broja drajvera. Prilikom pokretanja OSa pokrene se dosta servira. Servis je proces koji se izvršava u pozadini i pruža različite vrste usluga drugim programima ili preko mreže drugim računarima. Spominjali se DNS. Kad web preglednik dobije domensko ime, on pita servis na lokalnom računaru čija je uloga da pita servis koji traži DNS server. Servisi su usluge unutar operativnog sistema. Neki nam trebaju neki nam ne trebaju. Oni koji nam ne trebaju a izvršavaju se troše naše resurse. Automatic – pokreće se automatski, manual – pokreće se ručno, disabled – ne pokreće se.

Predavanje 4

Klijentski su namijenjeni za jednog korisnika u jednom trenutku, a serverski za više korisnika. Koja je razlika za hardver klijentskih računara i serverskih računara? Kada se pokvari hardver na klijentskom računaru, utiče na jednog korisnika, dok kada se pokvari na serverskom računaru, utiče na više korisnika. Dakle hardver mora biti takav da može raditi 24/7. Kućni računari nisu pravljeni da rade 24 sata. Serverski hardver mora biti pouzdaniji. Da bi kod servera ostvarili traženu pouzdanost, kućište je predviđeno da u njega može stati više komponenti. Serverski hardver je pravljen da se može nadograditi, ugradiv u ormar, proširiv, bolje CPU performanse, bolje I/O performanse, ugrađuju se dodaci za visoku pouzdanost(sve što se može pokvarit dodaje se više). Serveri su nekad pravljeni kao jedan veliki računar, onda se pojavila prva ideja, hajmo uzeti više servera i napraviti konfiguraciju koja pruža izgled jednog servera. Blade serveri – računari manje veličine. Danas, blade serveri su pravljeni da se njih pravi viška. Server soba – ograničen pristup, UPS, klimatizacija, redudantnost, antistatičko okruženje, lak pristup opremi i kablovima, obilježena oprema, zaštita od elementarnih nepogoda. Data centar – pružanje usluga velikom broju korisnika. Postoji više servera. Pouzdanost se povećava kroz redudantnost.
Sve što pišemo na disk, pišemo na particije. Particije su dijelovi diska. Time prenamijenimo taj disk. Veličina particije se prilagođava namjeni. Prvi korak odredimo koliko ćemo particija praviti. Na windowsu mogu biti 4 primarne i ostale su extended. Prvi korak je pravljenje particija. Formatiranje omogućava da se podaci mogu pohranjivati na disk. Datotečni sistem je način kako su datoteke organizovane. Mi prilikom formatiranja uspostavljamo datotečni sistem. Kakva je veza između particija i diskova? Na jednom disku možemo imati više particija. Na windowsu ne možemo vidjeti koja particija je na kojem disku. Kod linuxa imamo hard diskovi i sata ili scsi diskovi, a je prvi disk, b je drugi disk, označava koji je po redu na kontroleru kako su povezani kablom. Treći broj označava particiju. Particije kreću od 0. Kako možemo pristupiti dijeljenom folderu na nekom drugom računaru? Moramo znati IP adresu računara i protokol koji se za to koristi. Računarska mreža je zajednica svih korisnika koji koriste tu mrežu. Sve što radimo mora biti u skladu sa pravilima, politikom i sl. Računari su dio lokalne mreže, koja ima sistemsku politiku koja kaže čemu služi ta mreža. Šta je cilj i kako radi, kako izgleda, šta su čije odgovornosti. Uniformnost – manje razlika i odstupanja o kojim treba voditi računa, veća statička predvidljivost. Raznolikost – raspoređivanje rizika od mogućih problema sa pojedinim komponentama. Isti problem uglavnom ne pogađa različite komponente. Unix je donio ideju distribuiranog modela. Računar može biti i server i klijent. Šta znači

peer to peer? Svi svima pružaju usluge. Ideja je da imamo zajednicu, koja čini mrežu, gdje svaki čvoj konzumira usluge drugih čvorova i pruža usluge drugim čvorovima. Sve usluge koje mreža pruža idu preko nekih servisa. Šta radi web server? Web server poslužuje objekte. DNS server prevodi domenska imena u IP adrese. Serveri kao usluge se na unixu se implementiraju kao procesi koji se izvršava na računaru i pruža neku uslugu. Na windowsu se zovu service, a na unix daemon. Kad reinstaliramo računar, korisnička podešavanja se gube, ali se mogu i sačuvati – repair. Opterećenje sistema zavisi od ljudi. Ljudi generišu opterećenje sistema.
Analiza mreže – kada imamo računarsku mrežu, treba da znamo kako ona radi. Kako otkriti kako izgleda gotova mreža? Način otkrivanja kako je mreža organizovana. Analogija mreže – pitanja. Kako su čvoroci povezani? Kako to otkriti? Hodanjem i gledanjem. Hardver – računari, mrežni uređaji, štampači?, IP adresiranje, lokacija ljučnih mrežnih servisa. Koliko ima računara, kako se zovu i koje su im adrese, kakvi su im procesori, memorija, diskovi, kakav je OS instaliran. Kako otkriti kabliranje, komunikacioni ormarići, mrežna oprema – gdje se nalazi. Koje usluge mreža pruža, ima li peer to peer. Ovo sve mi trebamo zaključiti. Idealna situacija je da tu bude dokumentacija. Alat kojim možemo saznati IP adrese nekih računara je nslookup. Dig – radi isto. Ping, tracert, traceroute, tracepath – alati kojima ispitujemo povezanost mreže, da li paketi od nas putuju do tog uređaja. Ping daje nekoliko informacija: ttl – time to live, time – vrijeme koje je bilo potrebno da ping ode i da se vrati. Govori nam da li paketi mogu od nas da prođu od nas do tog uređaja, druga je koliko vremena treba tim paketima. Tracert – komanda koja ne pokazuje samo da li imamo konekciju sa nekom uređajem, nego IP adrese ili domenska imena svih rutera kroz koje je paket prošao. Možemo da vidimo na kojem dijelu se javila greška, možemo da vidimo kuda putuje paket, pokazuje na kom od linkova između nas i krajnje lokacije ne prolaze paketi. Nmap otkriva mrežne servise, skenira mrežu slanjem paketa na sve portove, ako se neki port javi, na tom portu ima servis.

Predavanje 5

DNS služi za pretvaranje domenskih imena u IP adresu. Kada otkucamo web pregledniku www.google.ba šta se desi? Kako se domensko ime pretvara u IP adresu. Provjeri se u mrežnim postavkama koja je adresa DNS servera. Postoji program kojem se browser obrati, on se obrati name serveru koji je definisan u mrežnim postavkama. Name serveru pošalje www.google.com, name server mu vrati IP adresu. DNS resolver je jedan od servisa. Browser se obratio operativnom sistemu i rekao de mi pretvori ovo domensko ime u IP adresu. Name server kome se resolver obraca, on je prvi u hijerarhiji. Kako on zna sve adrese. Kaže bunda ne zna on hehe. Obraća se root dns-u. Kaze bunda naucila na orm-u.
Logično je da name server ne može znati sve adrese. Kad dodamo novi domen, kako cijeli svijet sazna za taj domen. Domenska imena se sastoje od nekoliko nivoa. Na kraju svakoga bi trebala da stoji tačka. Tačka je root domen, pa onda poddomeni. Osnovni su TLD – top level domen. Ima ih oko 1000. 7 osnovnih domena – gtld(com,gov,edu,mil,net,org,arpa). ICANN upravlja domenskim imenima. Ona to radi kroz regionalne registre. RIPE je za Evropu. Kad se dodjeljuju domenska imena i IP adrese, ICANN podijeli na 5 svjetskih regiona, onda RIPE dalje za Evropu. Domenska imena su podjeljena na 2 grupe – generička – njih prodaju komercijalne organizacije. Genericki top domeni su zasnovani na ekonomskoj koristi. Druga grupa domena su CCTLD, country code top level domain. U svakoj zemlji postoji organizacija koja upravlja domenskim imenima ispod domenskog imena koje odgovara zemlji. Kompletan skup domenskih imena izgleda kao stablo. Pravila: ima ograničenje na dužinu ukupnu, ima ograničenje na broj poddomena koji može biti, do nedavno su mogli biti samo znakovi americke tastature, sad može bilo šta. Imamo pitanje za naš ns koji je dobio pitanje za neki server koji se nalazi duboko u hijerarhiji. Pita se root server. Otkud njemu adresa root servera? Kako je resolver došao do adrese dns servera? Piše u mrežnim postavkama. Obično negdje nešto piše, ili je jako jednostavno za saznat. Name server kojem smo se mi obratili, ns je dobio upit, obraca se root ns i da njega pita, međutim treba imati adresu. Pošto je ns komad softvera, u konfiguraciji imaju adrese root ns. Druga varijanta koja može biti da on pored ovoga ima upisan ako ti ne znaš koga da pitam. Ne postoji jedan root server nego ih ima 13. Zovu se A-M, i svaki ima svoju IP adresu. On se obraća nekom od tih 13 root servera. Šta znaju root name serveri? Kad se obratimo root serveru, on ne zna sve. On zna IP adresu servera top level domain-a. Ako mu je psotavljeno pitanje za nesto.ba, on ne zna, ali šalje IP adresu servera ba domene. Svih 13 root servera imaju idetičnu kopiju baze, 13 ih je samo zbog redudantnosti. Ako smo tražili www.etf.unsa.ba šta će nam odgovoriti ns .ba. On šalje adresu sljedećeg ns u hijerarhiji, šalje ip adresu ns od unsa. Pitamo taj ns, on vrati IP adresu ns etf.unsa.ba. Kad njega pitamo, on vrati IP adresu. Ovaj proces konvergira i korak po korak nas vodi do onog što se naziva autoritativni server imena. Preslikavanje domenskih imena u IP adrese zapisuje se samo na jednom mjestu, unutar ns unutar kog se nalaze ta imena.
Znači imamo web browser u kom smo otkucali www.etf.unsa.ba , on se obratio operativnom sistemu, resolveru, koji je onda pročitao IP konfiguraciju, dobio ime DNS servera, dobio dns serveru upit, on se obratio root name serveru, root vratio IP adresu za ba domen, onda se obratio njemu, dobio nazad IP adresu za unsa.ba domen, obratio se njemu, dobio IP adresu za etf.unsa.ba , obratio se njemu i dobio IP adresu za www.etf.unsa.ba.
Postoje 2 vrste upita, rekurzvini i iterativni. Rekurzivni upiti – resolver je pitao dns server i on mu je dao rezultat, to je rekurzivno. Između klijenta (resolvera) i name servera je rekurzivno, i uvijek će mu dati kompletan odgovor. Između root servera i ovog ns je iterativno ponašanje koje kaže da root server neće odgovorit sa konačnom IP adresom, nego mu daje sljedeću IP adresu. Preglednik ima svoj DNS cache, ako ja tražim stranicu i dobijem odgovor, on će neko kraće vrijeme držati to preslikavanje. Resolver također ima cache. Koliko će ns pamtiti neki odgovor? Obično jedan dan. Neautorizovano – nije od autorizovanog servera, nego iz keša.
Dinamički DNS – svaki put DHCP vrati drugačiju IP adresu, a ja hoću nešto da hostam, obraćam se dinamičkom DNSu, traži domensko ime koje se veže za IP adresu koja je trenutna. On zapiše preslikavanje, ali ne treba keširati. Server će da za adrese koje se češće mijenjaju stavit kraći ttl. Ako imamo etf.unsa.ba i hoćemo da otvorimo domen ri.etf.unsa.ba, ri ne mora imati svoj ns. Postoje zone odgovrnosti name servera, zona može biti jedan hijerarhijski nivo ili više njih. Kada dođe upit za ri.etf.unsa.ba, etf.unsa.ba pogleda upit i vidjet će da je definisan kod njega i da će on dati odgovor. Drugi slučaj je da ima IP adresu servera. Ns može biti zadužen za jedan ili više nivoa hijerarhije. Može biti da ri ima svoj server, a da npr tk koristi etf.unsa.ba.

Zona je skup domenskih imena na koje neki name server ima zapisane odgovore. On za neki poddomen može imati IP adresu svih domenskih imena koji pripadaju tom poddomenu ili adresu name servera kome se može obratiti za IP adrese iz tog domena. Kad naš autoritativni ns odgovori, postoji tačno definisani formati kako izgleda odgovor. Tu piše domensko ime, ttl – vrijeme koliko dugo treba keširati odgovor, klasa, tip zapisa. Najvažniji zapisi su zapisi tipa A, A zapis pretvara domensko ime u IP adresu, postoji AAAA – pretvara domensko ime u IPv6 adresu. Baza je teksutalna datoteka u kojoj pišu zapisi. CNAME – nadimci, zamjenska imena. Može biti više domenskih imena za jednu IP adresu.
BIND – podržava da imamo 2 servera, master i slave server, ažuriramo podatke na masteru, automatski se ažurira na slave. Ima jedan direktorij named ili dna, unutar njega master ili slave, unutar njega datoteka koja se naziva kao domen (mora biti istog naziva kao i domen). Postoji reverzni dns upit gdje pretvaramo IP adresu u domensko ime. Datoteka koja pokazuje na samog sebe, named.cache datoteka u kojoj se nalaze adrese root name servera i named.conf koja definiše gdje se šta nalazi. named.conf je neka konfiguraciona datoteka koja u principu kaže kako se zove zona i gdje se nalale root serveri, gdje se nalate podaci o localhostu, o reverznom mapitanju. named.cache je file koji je učitan prilikom pokretanja bind softvera i u kome piše domensko ime, A zapis, koja je IP adresa na kojoj se nalazi taj root ns i koliki je njegov ttl. Način na koji možemo dodati poddomen u domen jeste ustvari: ako ja imam domen etf.unsa.ba i ako je ri napravio svoj name server, dodajemo u datoteku ri i name server. Ako neko pita za taj poddomen, vraća se IP adresa, ali moramo imati i IP adresu, pa moramo i to imati u zapisima.

Predavanje 6

Active directory – neka vrsta baze podataka u kojoj se vodi evidencija o korisnicima domena, računarima, grupama, o svim podacima koji su vezani za domen. Active directory je nekakav zapis o svemu što se nalazi u domenu. LDAP – lightweight directory access protocol. Na osnovu čega google pravi listu stranica – kako zna da je neka stranica relevantna za ono što se pretražuje? Pravi se evidencija ključnih riječi, rečenica i sl. i vrati se u bazu. Kakva je razlika između imenika i baze podataka? Baza podataka je sve u šta se stavljaju podaci.Ako imamo telefonski imenik, imamo jednu tabelu, ime, broj telefona i pretražujemo. Active directory je imenik svih sadržaja koji se nalaze u domenu, korisnike, podatke o korisnicima. Postoji posebna klasa softvera koji su namjenjeni prije svega za pretraživanje i rijetko ažuriranje. Zašto su imenici korisni? Sve aplikacije da ne bi održavale svoj imenik, ako se bilo šta od podataka promjeni o nama, drži se sve u jednom imeniku, i time se olakšava rad. Imenici služe kao repozitoriji podataka, relativno su jednostavni, najčešće su kao jedna tabela. LDAP je protokol, ali obično se i imenik zove LDAP. Active directory je imenik kojem se prostupa putem LDAP prtokola. Kako zapravo izgleda imenik? Ima nešto što se naziva directory information tree. To je zapravo stablo koje predstavlja sve unose u imenik pri čemu jedan unos u imenik je jedan distinguisheg name – jedinostveno ime koje tačno definiše u stablu jedan list. Sastoji se od niza relativno razlučivih imena. www.etf.unsa.ba ba je jedan RDN, onda unsa, pa etf...
Za ime objekta, tj. posljednju stavku u hijerarhiji je naziv CN-common name, organizaciona jedinica – ou, organizacija – o , country – c. LDAP ne propisuje koliko ima nivoa i kako se zovu te stvari. Neke standardne koje se koriste: c,o,ou,cn... DN služi zapravo da adresiramo pojedini unos u imenik, to je njegova adresa. A unutar njega se nalaze podaci koje smo unijeli za taj objekat, to su atributi. DN je adresa unosa u imenik. Stablo definiše sve unose u imenik, kako izlgeda hijerarhija, od kojih se RDN sastoji, i kakva je struktura. Šema definiše sve vrste objekata koji se mogu pohraniti u imenik. Ako želimo da unesemo neki unos, šema specificira šta je sve potrebno unijeti. Šema definiše klasu objekata. Objekat je unos u imenik. Za svaki objekat se definišu atributi, svi atributi koji mogu biti definisati, neki su obavezni neki ne i da li je ta klasa naslijeđena ili ne. Mogu se definisati koji su dozvoljeni ili nedozvoljeni. Atributi mogu imati višestruke vrijednosti. Za svaki objekat treba definisati naziv, opis, tip, vrijednost, maksimalna dužina i obično ima identifikator. Postoje unaprijed definisani atributi. Način zapisivanja, način razmjene podataka je LDAP data interchange format. Prva linija definiše dn, tj. lokaciju objekta unutar stabla i onda nabrajamo sve atribute. LDAP usluge – pretraga, promjena unosa, može se koristiti za potvrđivanje identiteta, može čuvati korisničke lozinke. LDAP server osluškuje na portu 389, prima pakete. Prilikom pretrage upit treba da kaže odakle krećemo, može biti od korjena od početka, ili npr od unsa.ba. Scope – da li pretražujemo sve do kraja, samo na tom nivou... Veličina – ako će odgovor imati 100 zapisa, da li vracamo 100 ili manje, vrijeme – koliko dugo može trajati upit, koje atribute tražimo, da li će vraćati samo anzive atributa ili i vrijednosti i onda filter – omogućava da suzimo pretragu na ono što nas zanima. Rezultati pretrage je zapis – disiguished name i svi atributi. Klijent ce otvoriti konekciju, potrvrditi identitet, uraditi neku pretragu i onda zatvoriti konekciju. Pretraga vrati pokazivač na podatke. Active directory je misrosoftova izvedba imenika LDAP. Služi za pohranjivanje informacija i konfiguracija. Može se napraviti neka grupna politika koja se primjenjuje na sve što se nalazi u domenu.Kroz activy directory se provjerava da li imamo pravo da se prijavimo, i nakon što se prijavimo čemu imamo pravo prisupa. Active directory služi da se pohrani sve što ima u domenu. Cilj je da se olakša administracija u smislu da se sa jednog mjesta radi administracija svega. Open standards – LDAP, koristi DNS za imenovanje i lociranje servira. Ako nam ne radi dns, active directory ne radi, kerberos – koristi se za potvrđivanje identiteta. Kako izgleda AD? Osnovna jedinica AD-a je domen. Unutar domena imamo organizacione jedinice koje mogu biti hijerarhijski organizovane, i unutar organizacionih jedinica može biti bilo šta(ljudi, grupe, računari, drugi resursi). Domeni mogu biti organizovani na različite načine, u stablo i u šumu. Inicijalno, u AD-u su se upisivali korisnici, grupe korisnika i računari. Kasnije je dodano praktično bilo šta: distribucione liste i sistemske politike. Također, AD omogućava da u njega pohranimo bilo šta. Kompletna struktura AD-a je opsiana u šemi koja govori koje tipoce objekata imamo, koji su njihovi atributi i unutar atributa kakvi su tipovi podataka. Jedna šema se primjenjuje unutar svih domena koji čine organizaciju. Domen je dio koji se odnosi na jednu lokaciju, jednu organizaciju. Osnovni gradicni element. Pošto je AD baza podatak ili skup podataka, fizički on se nalazi na kontolerima domena. Unutar domena se mogu praviti organizacione jedinice. organizaciona jedinica omogućava da možemo imati strukturu u domenu. Organizacione jedinice mogu biti hijerarhijski organizovane unutat nekog domena u stablo. Šuma nastaje kada se dva domena stave u root, oni predstavljaju dva različita prostora imena. Domeni nude još da logička i fizička struktura ne moraju biti identične. Fizička struktura

govori gdje se nešto nalazi. Jedan domen se može nalaziti na više lokacija, na jednoj lokaciji možemo imati više domena. Server u domenu može biti member server ili domain controler. Domain controller je onaj računar na kom se nalazi baza podataka. Moramo imati DNS da bi radio AD. Kerberos je standard, omogućava potvrđivanje identiteta na domenu.

Predavanje 7

Za instalaciju web servera treba proći kroz neku proceduru. Treba odlučiti na kojem računaru ćemo instalirati web server. Ova odluja je vezana za lokaciju u mreži, da li nam treba server koji se nalazi kod nas, da li su većina korisnika lokalni ili su negdje drugo. Moramo odabrati lokaciju datoteka na računaru. Da li će pristup biti po stanadrdnom portu, ko će imati prava pristupa. Onda treba da izaberemo sofvter. Kad smo završili instalaciju, treba podesit neke stvari. U datoteci /etc/services su definisana preslikavanja preslikavanja između usluge i porta na kojem se ona nalazi. Apache koristi httpd.conf datoteku. Konfiguracijska datoteka može biti podijeljena na više datoteka. Jedna od konfiguracija koje mijenjamo je server root – gdje se nalaze konfiguracijske datoteke. Da bi neki servis rezervisao port koji je manji od 1024 na unixoiodnim sistemima, on mora biti root, odnosno mora biti privilegovani korisnik. Perzistentne konekcije – web klijent pita web server odgovara, nakon toga web server pretpostavlja da ce klijent imati još upita. Web server treba da se konfiguriše da to podržava, definiše se MaxKeepAliveRequests – koliko zahtjeva se dozvoljava. Server nakon što odgovori čeka, mora postojati vrijeme nakon kojeg će zaključiti da klijent više nema zahtjeva – KeepAliveTimeout. Prava pristupa – inicjalno niko nema pristup nicemu unutar servera. Uloga web servera je da poslužuje objekte. Web preglednik bi trebao da u get zahtjevu anvede koji objekat želi, dakle putanja i naziv objekta. DirectoryIndex – definiše se naziv objekta ako u zahtjevu nije definisan objekat nego samo putanja. Kako preglednik zna da otvori bilo kakav file? Mime types.
Server u odgovoru šalje content type. Kako server zna koja datoteka se čime otvara. U konfiguraciji servera postoji mime.types datoteka. On za ekstenziju čita type. Web preglednik interpretira datoteku na osnovu content type-a koji je došao u odgovoru.

Načini umrežavanja

Između ostalog tokom instalacije VM moramo odabrati način umrežavanja VM. Možemo izabrati **rad bez mreže**, **NAT** (defaultno podešavanje)
Podešavanje na nivoujedne VM (jednog OSa) – sve uz pretpostavku da je instaliran npr. Virtual Box. -
Sada pored standardnog Ethernet adaptera postoji i Virtual Box adapter koji ima svoju IP adresu. Ta IP adresa će biti adresa gateway-a za VM kojima je mreža podešena da bude NAT. Virtual Box adapter je iza NATa i ima mogućnost pristupa bilo čemu, ali se izvana neće vidjeti. Paketi koji se šalju od strane guest-ova prvo dolaze do Virtal Box adaptera, koji će uzeti podatke koji pripadaju TCP/IP sloju i sve će se resendati preko host računara.
Premošteno – bridged – uglavnom VM ima isti pristup mreži kao i host. VM se ponaša kao da je i ona prikopčana na isti svič kao i host. VM može dobiti IP adresu na isti način kao što je dobio i host, ali ne i ostale parametre. Tako da i host i VM moraju komunicirati preko sviča, odnosno vrijede sva pravila kao i za „standardnu“ lokalnu mrežu.
Internal network – uglavnom kao da su sve VM u jednoj mreži. Ovdje se mreža odnosi na komunikaciju između VM na istom hostu. Sve što se može postići sa internal networkom, može i sa bridge-om, samo što je internal network **sigurniji**. VMe komuniciraju privatno, bez omogućavanja pristupa za host.
Host only – **Mreža samo sa monitorom VM** – u principu mreža u kojoj se nalazi VM i host OS. Host only je **hibrid brige-a i internal network-a.** Kao kod bridge-a VMe mogu komunicirati između sebe i sa hostom ukoliko su priključene na svič. Sa druge strane kao internal network služi kao mreža koja je namijenjena samo za VMe i host OS, „outside world“ se ne može priključiti na ovoj mreži.

Internal network

- The host can’t access the guests
- Guests can’t access the host
- Guests can’t access the internet

NAT

- Internet access
- Guests can’t access each other or the host

Nat network

- Guests can access each other
- Internet access

Bridged

- Guests can access each other
- Host can access guests and guests can access the host. Anyone on the host network can access the guests
- Same access to internet as the host has

Host-only

- Guests can access each other
- No internet access