



Сингидунум

UNIVERZITET SINGIDUNUM
Departman za postdiplomske studije
Savremene informacione tehnologije

Internet exchange point

MASTER RAD

Mentor:
Doc. dr Marko Šarac

Kandidat:
Stefan Radovanović
2014/410514

Beograd, 2017.

Abstrakt: Internet današnjice se sastoji od preko 50000 mreža koje su pod kontrolom privatnih lica. Zajedno, ove mreže pružaju mogućnost globalnog povezivanja. Da bi povezanost u današnjem svetu, u startu bila moguća, ove mnogobrojne mreže moraju međusobno da komuniciraju. Upravo tu dolazimo do pojma Internet exchange point (IXP), preko kojeg dobijamo tehničke mogućnosti da se mreže “sretnu” i razmene podatke. Cilj mi je da u ovom naučnom radu kroz naučnu i eksperimentalnu fazu predstavim koliko se naše doba oslanja na Internet exchange point-ove.

Ključne reči: internet exchange point; internet; ISP.

Sadržaj

1. Metodologija

- 1.1. Uvodne napomene
- 1.2. Predmet istraživanja
- 1.3. Hipoteza
- 1.4. Ciljevi istraživanja
- 1.5. Naučne metode

2. Uvod

- 2.1. Šta je internet?
- 2.2. Definicija Interneta
- 2.3. Istorija Interneta
- 2.4. Internet danas u svetu i u Srbiji
- 2.5. Povezivanje na Internet
- 2.6. Mrežni napadi
 - 2.6.1. Browser attacks
 - 2.6.2. Brute force attacks
 - 2.6.3. SSL attacks
 - 2.6.4. Scans
 - 2.6.5. DNS attacks
 - 2.6.6. Backdoor attacks
 - 2.6.7. Botnet attacks
 - 2.6.8. Distributed denial-of-service (DDoS) attack
- 2.7. Odbrane od napada
 - 2.7.1. Blackholing
 - 2.7.2. Selective blackholing
 - 2.7.3. Scrubbing
 - 2.7.4. Traffic engineering
 - 2.7.5. Local filtering

3. Forme i oblici mrežnog interneta

- 3.1. Tehničke osnove i principi rada Interneta – protokol TCP/IP

- 3.2. OSI struktura Interneta
- 3.3. Protokol rutiranja
 - 3.3.1. Routing Information Protocol (RIP)
 - 3.3.2. Open Shortest Path First (OSPF)
 - 3.3.3. Intermediate System to Intermediate System (IS-IS)
 - 3.3.4. Enhanced Interior Gateway Routing Protocol (EIGRP)
 - 3.3.5. Border Gateway Protocol (BGP)
- 3.4. Autonomni system
- 4. IXP – Internet Exchange Point
 - 4.1. Tehničke karakteristike i analize
 - 4.2. Ekonomoska benefit Internet Exchange Point-a
 - 4.3. Trend rasta Internet Exchange Point-a
 - 4.4. Evropski i Američki modeli IXP-a
 - 4.5. Analiza postojećih Internet Exchange Point-ova
- 5. Pokretanje novog IXP-a
 - 5.1. Izazovi na početku
 - 5.2. Institucionalni i operativni modeli za IXP
 - 5.3. Lokacija
 - 5.4. IXP Oprema i Usluge
 - 5.5. Osoblje IXP-a
 - 5.6. IXP Website
 - 5.7. IXP i Internet zajednice

1. Metodologija

1.1 Uvodne napomene

U ovom radu predstavljeni su uređaji za razmenu Internet saobraćaja (IXP) između Internet servis provajdera (ISP). Razvoj, način funkcionisanja i poređenje sa starijim tehnološkim rešenjima bitni su za razumevanje cele mreže koje danas nazivamo Internetom.

1.2 Predmet istraživanja

Predmet ovog istraživanja jeste da se utvrde prednosti, ali i mane ove tehnologije, kao i mogućnosti za razvoj postojećih IXP-eva.

1.3 Hipoteza

IXP su nastali zbog potrebe da se smanji Internet saobraćaj koji saobraća od manjih ka većim Internet servis provajderima. Internet exchange point-ovi predstavljaju zajedničko mesto gde Internet servis provajderi mogu da razmene Internet saobraćaj između autonomnih mrežnih sistema.

1.4 Ciljevi istraživanja

Istraživanje i definisanje razvoja IXP-eva, budućnost i evolucija uređaja, kao i cele postojeće Internet mreže. Upoznavanje korisnika sa uređajima za razmenu Internet saobraćaja, kao i tendencija ka daljem uspostavljanju i razvoju.

1.5 Naučne metode

Pri izradi ovog rada korišćene su osnovne naučne metode deskripcije, indukcije, dedukcije, analize, sinteze i generalizacije.

Metoda deskripcije je korišćena pri objašnjavanju osnovnih pojmova i sistema funkcionisanja.

U teorijskim segmentima su primenjene metode analize, indukcije i dedukcije, dok su u izvođenju zaključaka korišćene metode sinteze i generalizacije.

2.Uvod

2.1. Šta je internet?

Pojam Internet znači, mreža unutar mreže, ili interkonekcija između više računara. Internet je globalna mreža. Strukturno postoje male mreže koje se međusobno vezuju, i time čine ovu strukturu.

Internet je globalni, svetski sistem umreženih računarskih mreža koji je promenio način prenosa podataka. Početak funkcionisanja interneta 1969. godine, poklapa se sa vremenom nastanka mreže računara pod kontrolom Ministarstva odbrane SAD, koja je nazvana ARPANET.

Danas, Internet povezuje milijarde računara širom sveta i predstavlja mrežu raznorodnih uređaja, ne samo računarskih već i komunikacionih, multimedijalnih, senzorskih, mernih itd.

Internet takođe predstavlja rezultat društvenog napretka, u širem naučnom, kulturno-umetničkom, političkom i svakom drugom pogledu i nije samo proizvod tehnološkog napretka, koji se neminovno proširio na sve oblike poslovanja.

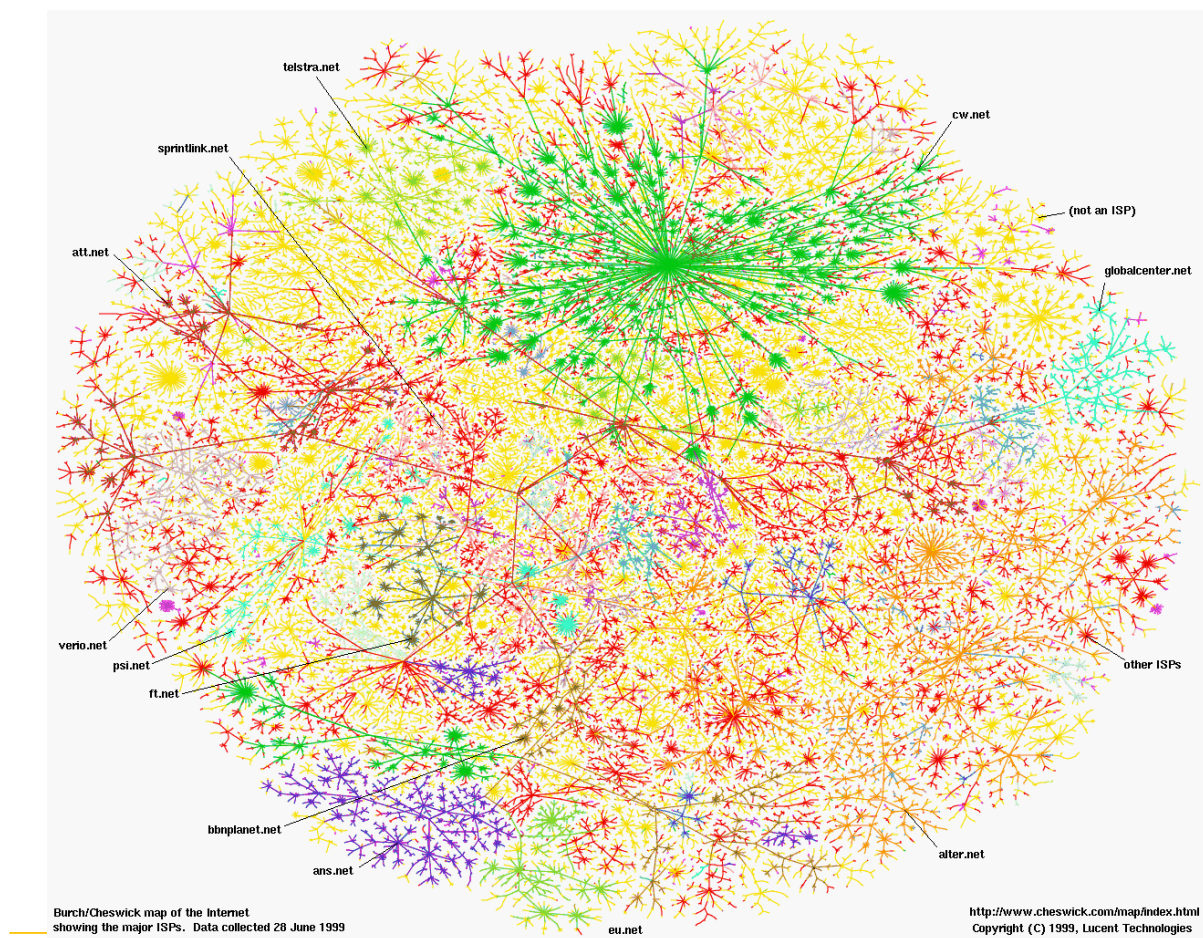
I pored navedenih prednosti, tek posle skoro 30 godina, Internet se nametnuo kao savremeno tehnološko sredstvo, inovacija koja bez prekida unapređuje društvo i ekonomiju. Internet je postao javno dostupno dobro, u vidu globalne mreže za prenos paketnih podataka, koja povezuje računare i računarske mreže korišćenjem internet protokola (IP). To je "mreža svih mreža" koja se sastoji od desetina miliona kućnih, akademskih, poslovnih i vladinih mreža koje međusobno razmenjuju informacije i usluge kao što su elektronska pošta, „razgovor”, prenos datoteka, povezane stranice i dokumente „World Wide Web“-a.

2.2 Definicija Interneta

Postoji mnogo različitih definicija Interneta. Po nekima je “mreže svih mreža”, dok neki Internet nazivaju “globalnom svetskom mrežom”. Najuniverzalnija definicija opisuje Internet na sledeći način: ” Internet je globalna mreža računara svih vrsta koja smišljeno i logički objedinjuje hiljade različitih računarskih mreža širom sveta, koje koriste iste tehničke standarde kako bi se ostvarila međusobna komunikacija”. Ova mreža omogućava mnoštvo različitih usluga i to je svrstava u INFORMACIONI SISTEM.

Ukoliko kućni računar ili neku lokalnu mrežu povežemo sa modemom preko otičkog kabla ili telefonske linije prema provajderu, odnosno davaocu Internet usluge, bićemo u mogućnosti da pristupimo na takozvanu “svetsku mrežu” i time budemo deo Interneta.

Internet se bazira na slobodnoj kooperativnoj osnovi uz obavezno poštovanje tehničkih pravila i standarda kako bi se ostvarila prisutnost i vidljivost na mreži. Internet ne pripada ni jednoj korporaciji i ne postoji centralna vlast koja njime upravlja. Postoji društvo koje je preuzelo bitnu ulogu i bavi se preporukama tehničkih sadržaja. To društvo se naziva Internet društvo (Internet Society) sa sedištem u Fairfax-u, Virginia, USA. Još jedna od bitnih stavki kojom se bave jeste i komunikacija između vladinih ustanova sa pojedinim zemljama kao i nevladinim institucijama, odnosno univerzitetima i kompanijama.



2.3 Istorija interneta

Rand Korporacija se smatra najsitaknutijim predstavnikom korporacija orjentisanih ka hladnom ratu. Jedan od glavnih problema sa kojim se ova korporacija suočila jeste kako da američka vlada komunicira posle nuklearnog rata. Pre više od pedeset godina imali su potrebu za mrežom pomoću koje mogu da izdaju naređenja, ali da ih i kontrolišu. Mreža je trebalo da

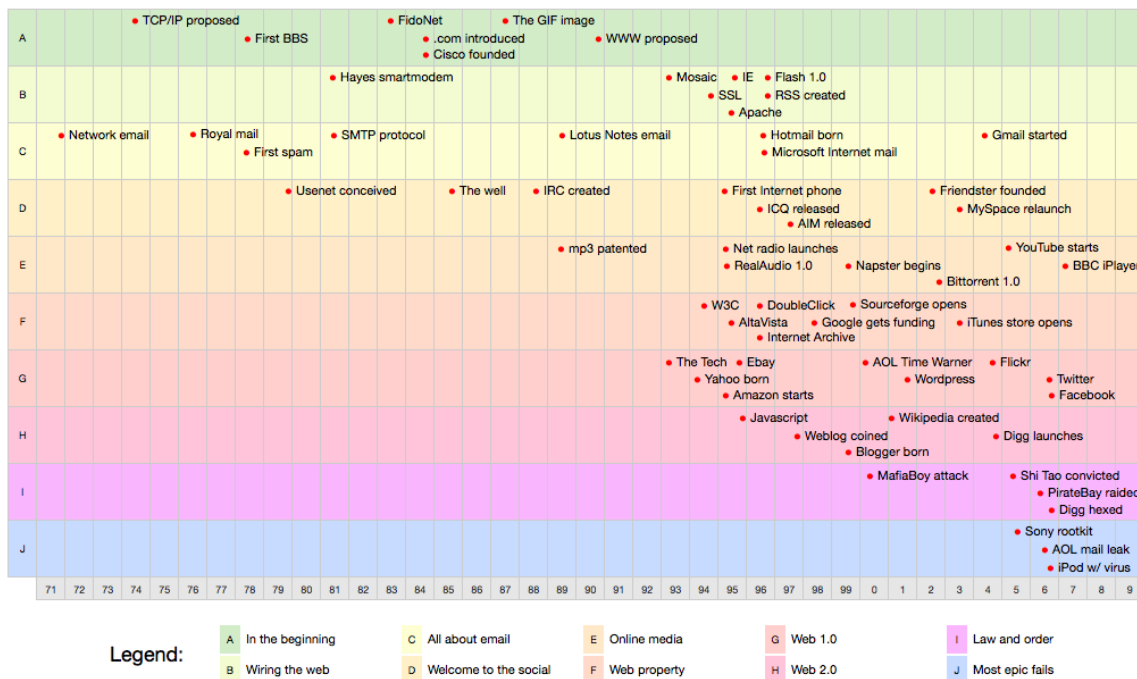
poveže gradove, države i baze. Problem sa kojim su se suočavali jeste da odgonetnu kako da posle nuklearnih napada mreža ostane zaštićena. Pokušavali su da nađu rešenje kako da prekidači i žice posle napada ne budu uništeni i ostanu upotrebljivi. Rand je dugo pokušavao da odgonetne kako bi mreža mogla da opstane, koja bi centralna mreža bila očigledna meta neprijatelja i kako bi sama mreža bila kontrolisana. Predstavnik kompanije Paul Boran je 1969. godine ispred korporacije i posle dugotrajnog rada u strogoj tajnosti izneo rešenje. Po njegovoj teoriji mreža ne bi trebala da ima "centralnu vlast"[2]. Ona od samog početka mora biti stvorena tako da "radi u krpama".

Principi na kojim je bila bazirana teorija su bili krajnje jednostavni. Kretalo se od pretpostavke da je mreža nepouzdana konstantno, u svako doba. Napravljena je tako da transcendentalno prolazi kroz sopstvenu nepouzdanost. U mreži, svi čvorovi bi bili međusobno jednakog statusa. Svaki od čvorova bi imao mogućnost da stvara, prenosi i prima poruke. Te poruke bi bile podeljene u pakete, a svaki paket zasebno bi bio adresiran. Paketi bi se kretali sa određenog čvora, a završavali bi se na drugom, predviđenom za odredište. Svaki od paketa kroz mrežu bi putovao individualno, a specifičan pređen put bi bio nevažan. U ovoj postavci bitan je samo rezultat. Poruka bi se prebacivala sa čvora na čvor sve dok ne dospe na odredište. Ukoliko bi deo mreže bio uništen ne bi predstavljalo problem jer bi paketi bili preneseni do odredišta pomoću preostalih čvorova. Ovakava postavka mreže može se smatrati neefikasnom, međutim ukoliko uporedimo sa nekim drugim postojećim sistemom, kao što je npr. telefonski, može se zaključiti da je izdržljiv.

Tačan trenutak nastajanja Interneta je nepoznat, odnosno ni najbolji poznavaoći istorije informatike se ne mogu usaglasiti kada je u pitanju ta tema. Postoje oni koji tvrde da je zaslužan dr. Leonard Klajnrok. Po toj teoriji dr. Klajnrok je 1961.godine na MIT univerzitetu prvi put objavio rad koji se bazirao na packet-switching tehnologiji. Postoje i oni koji se zalažu za teoriju u kojoj je Internet rođen 1969. godine kada je Ministarstvo odbrane SAD-a, odabralo Advanced Research Project Agency Network, poznatiju kao ARPANET. Njima je on poslužio za istraživanje i razvoj komunikacija i komandne mreže koja bi mogla preživeti napade, a posebno nuklearne.

Sedamdesete godine se smatraju jednim od najplodnijih kada su upitanju otkrića vezana za razvoj Interneta. Tih godina je došlo i do odvajanja ARPANET-a iz vojnog eksperimenta, pa je postao dostupan za javne istraživačke projekte.

Top significant moments from the Internet history



Created by João Bordalo, based on the work of builderau.com.au, some rights reserved

Vremenski dijagram najvažnijih trenutaka u razvoju interneta

Američki univerziteti u Los Angelesu, Stanfordu i univerzitet Kalifornije u Santa Barbari kao i Univerzitet Jute bili su od 1969. godine pikopčani na ARPANET. U tom trenutku mreža je koristila 50 kbit/s mrežna kola. Danas se ARPANET smatra pretečom današnjeg Interneta, iako je u mnogo čemu bio ograničen.

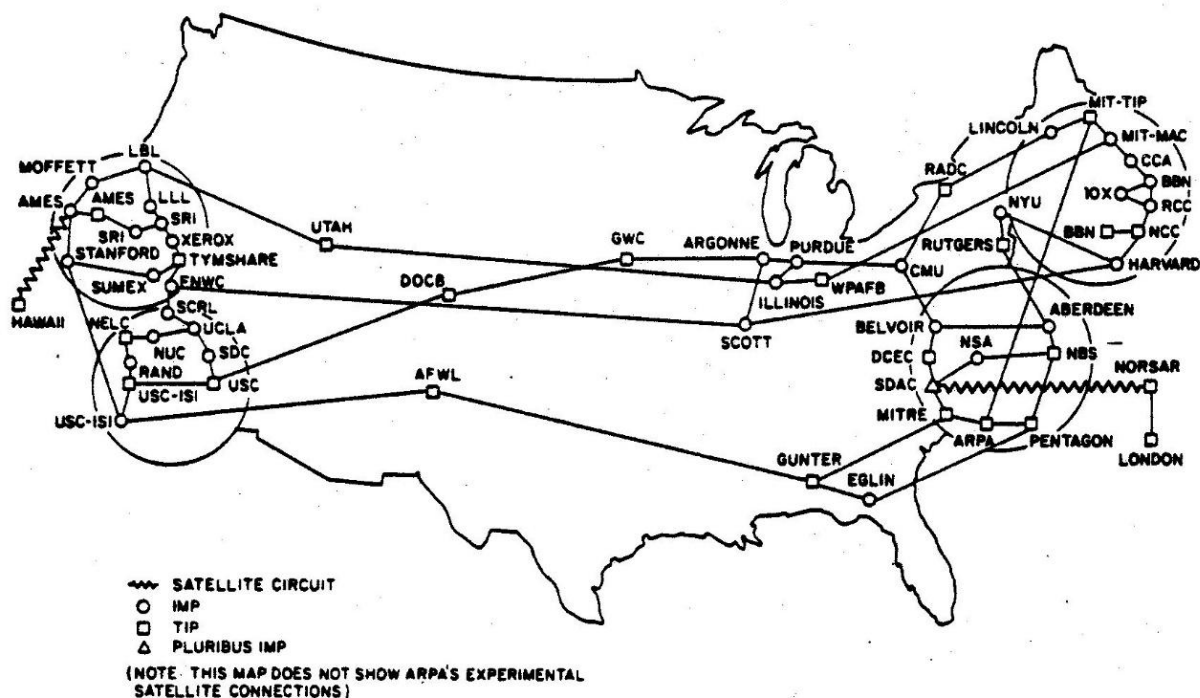
Mreža koju sačinjavaju manje i veće mreže povezane bakarnim, optičkim i drugim kablovima, a koja za komunikaciju koristi IP, Internet Protokol i globalno je dostupna naziva se INTERNET.

Američka Nacionalna Naučna Fondacija (NSF) napravila je univerzitetsku mrežu 1.januara 1983. godine. Na taj način je nastala prva Internet mreža. NSF je kasnije prerastao u NSFNet, a Internet je nastavio da se razvija velikom brzinom. TCP/IP Internet protokoli su doprineli razviju i omogućili da radi preko već postojećih mreža kao što su npr. telefonske žice. Ipak navažniji trenutak je prelazak tadašnje mreže sa NCP-a (Network Control Protocol) na TCP/IP (Transmission Control Protocol / Internet Protocol) 1983. godine. Stvaraoci ovog protokola su Vinton Cerf i Robert Kan.

Stanandardi koji omogućavaju komunikaciju računara putem mreže nazivaju se protokoli. Godine 1983. manje od 1000 računara bilo je vezano za ARPANET i koristilo zastarelu verziju Network Control Protocola. Ovaj protocol, iako je imao ograničenja, mogao

je da bude upotrebljiv u manjim mrežama. Mana sa kojom su se suočavali korisnici jeste u tome što nije bio dovoljno fleksibilan. Kako su do izražaja dolazile nove potrebe, opširniji pristup komunikacionom protokolu, došlo je do stvaranja novih, komplikovanih mreža.

Vinton Cerf je izjavio jednom prilikom: "Stvorili smo protokol koji će se koristiti i u velikim mrežama, sa velikim brojem računara, protokol koji će nositi Internet budućnosti, što znači, da mora biti fleksibilan, kako bi različite mreže mogle funkcionisati u zajedničkom okruženju". Tada je postalo jasno da će INTERNET postati jedna velika, globalna mreža sačinjena od mnoštva manjih mreža. Ipak prelazak na TCP/IP protokol nisu svi podržali. Neki su smatrali da se prihvate neki drugi protokoli, a najviše su navijali za upotrebu Open System Interconnection Protocola. ARPANET je pre zvaničnog prelaska na TCP/IP nekoliko puta isključivao NCP prenos podataka, kako bi pokazao da se on može isključivati po želji korisnika mreže.

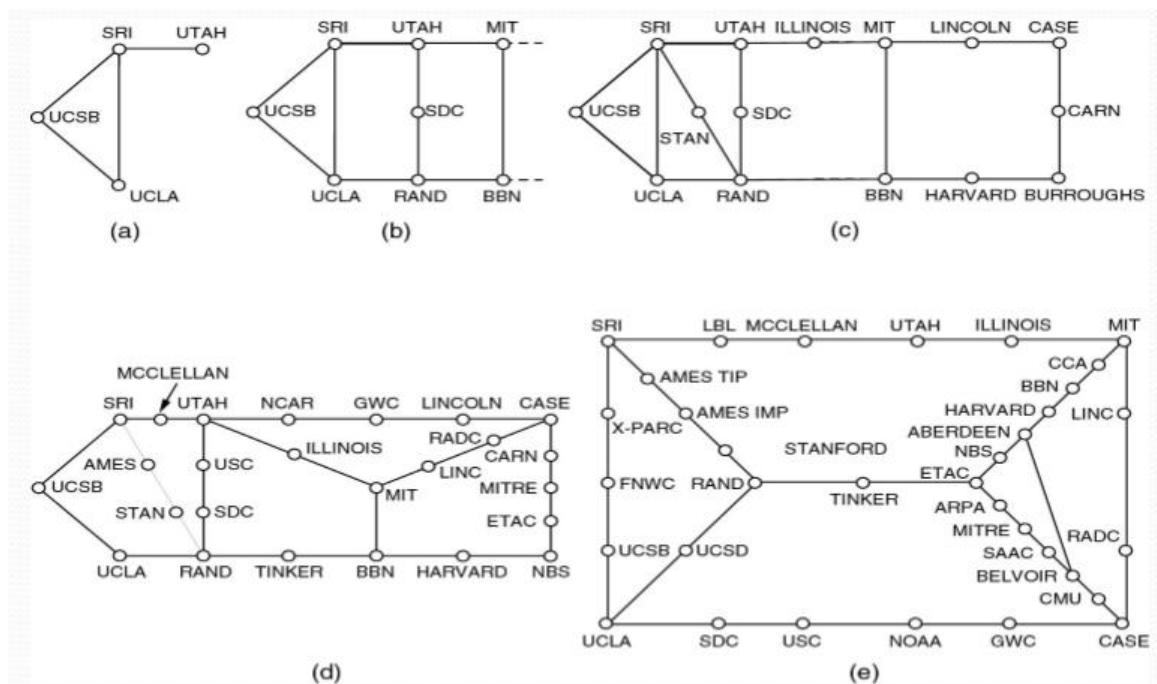


Dijagram ARPANET u Sjedinjenim Američkim Državama

Stvaraoci TCP/IP protokola Vinton Cerf i Robert Kan, na stvaranju novog protokola počeli su da rade i pre 1983. godine, tačnije 10 godina ranije, javila se ideja o novom protokolu. Razvijali su ideje i usavršavali ih. Implementacija TCP/IP-a u operativne sisteme trajala je oko 5 godina, dok se uporedo pripremao i usavršavao novi protokol koji će promeniti sve.

Devedesetih godina dvadesetog veka došlo je do predstavljanja novog protokola svetu. CERN u Švajcarskoj je 1991. godine predstavio Web sajt. Tri godine pre toga je Tim Berners-Lee počeo stvaranje HTMLa, HTTPa, a zatim i prve Web stranice. 1994. godine naglo raste interes javnosti za Internet, koji je do tog trenutka bio samo akademsko/tehničke prirode.

Kako je interesovanje raslo, tako se sve brže integrisao broj javnih računarskih mreža 1990. godina. Integracija je omogućila nesmetan rast mreže i slobodu protokola. Po statistikama, do 2008. godine, pokazano je da oko 1,46 milijardi ljudi koristi Internet u celim svetu.



Razvoj ARPANET-a: (a) Decembar 1969. (b) Jul 1970. (c) April 1972. (e) Septembar 1972.

Ideja o decentralizovanoj i neuništivoj mreži, koja prenosi pakete, bila je prisutna tokom 60-tih godina i u drugim korporacijama kao što su Rand, MIT i UCLA. U Velikoj Britaniji u nacionalnoj laboratoriji za fiziku prvi put su testirali mrežu 1968. godine. Posle toga je istupila Pentagonova agencija za razvojne istražne projekte koja je odlučila da investira u jedan od većih projekata u SAD-u. Novo istraživanje je bilo zasnovano na ideji da čvorovi mreže treba da budu superkompjuteri velike brzine. Pod superkompjuterima u to vreme su se smatrale mašine koje su bile retke i skupe, kojima je rad na dobroj mreži bio osnova. Za cilj su imali dobrobit nacije i razvoj projekata i istraživanja. Jedan takav superkompjuter je instaliran u Kalifornijski UCLA Univerzitet u Los Angelesu u jesen 1969. godine. Iste godine u decembru na novonastaloj mreži je bilo četiri kompjutera koje su nazvali ARPANET. Podaci su mogli da se prebacuju na određenu liniju za brz prenos. Uspeli su čak da budu programirani sa daljine, odnosno sa drugih kompjutera. Zahvaljujući ARPANET-u, bilo je moguće deliti i razmenjivati informacije preko kompjutera sa velike daljine. Ipak ono što se najviše prenosilo bile su uglavnom razne vesti i poruke lične prirode. Istraživači su ga koristili kako bi sarađivali na različitim projektima. Svaki korisnik je imao svoju adresu i elektronsku poštu kako bi mogao da razmenjuje poruke.

NCP Network Control Protocol predstavljao je originalni standard za komunikaciju u ARPANET-u. Kako je vreme prolazilo razvijala se i tehnika, pa je NCP prevaziđen i zamenjen novim boljim standardom, danas poznatim kao TCP/IP Transmission Control Protocol. TCP/IP protocol, poruke pretvara u ogranke paketa na izvoru, razlaže i ponovo spaja u poruku na odredištu. Ovaj protocol se bavi adresiranjem i obezbeđivanjem paketa koji

putuju preko čvorova i preko mreža sa više standarda. U te standard spadaju Ethernet, FDDI i X.25. Od 1977. godine TCP/IP protocol, koristile su i druge mreže da se povežu na ARPANET. Sve do 1983. godine ARPANET je čvrsto kontrolisan, a kasnije se i razdvojio pa je deo ARPANET-a, koji je ostao vezan za vojsku postao MILNET. Ipak TCP/IP ih je sve povezivao.

Naglo širenje raznih mreža računara koje su se povezivale na globalnu mrežu kreće nakon 1970. godine. Internet je postajao sve jednostavniji, a korišćenje protokola TCP/IP postaje uobičajno. Tada je mreža koja se sve više širila, dobila zvaničan naziv INTERNET.

Povezivanje na Internet za sve građane postaje jeftino i dostupno, negde čak i besplatno. Svaki čvor je bio nezavisan a samim tim je sebi mogao da omogući samofinansiranje i sve neophodne tehničke uslove.

Sredinom osamdesetih godina mreži se priključuje Nacionalna Fondacija Nauke (National Science Foundation). Tada Internet postaje bitan kao institucijalizovana naučna osnova. Dalje se nastavlja razvoj i ubrzano širenje "mreže svih mreža". Priključivanje NSFNET bilo je od velike važnosti i predstavljalo je veliki iskorak ka novim tehničkim dostignućima. Imao je novije, brže i bolje superkompjutere, a konstantno je napredovao, širio se i obnavljao. Trend priključivanja INTERNETU prate i druge vladine agencije, pa dolazi do priključenja mreži i Nacionalnog Instituta za zdravlje i vladinog ogranaka za energiju. Među prvima koji su se povezali je i NASA.

Kako se mreža širila došlo je i do odvajanja čvorova na osnovne vrste. Nekoliko američkih i neki od stranih kompjutera izabrali su da se prepoznaju po geografskoj poziciji, a preostali su se grupisali u 6 osnovnih Internet domena: GOV, MIL, EDU, COM, ORG i NET. Kada se govori o GOV, MIL, EDU domenima, mora se spomenuti da su oni vezani za vojne i obrazovne institucije. ORG obuhvata sve ostale neprofitne organizacije.

Do zvaničnog gašenja ARPANET-a došlo je 1989. godine. Njegove funkcije su nastavile da se poboljšavaju i dovele su do stvaranja globalne mreže. Korišćenje navedenih standarda te godine je koristilo više desetina kompjutera iz 42 zemlje sveta. Internet je naročito postao popularan među naučnicima i bio je korišćen kao jedan od najvažnijih instrumenata dvadesetog veka. Tokom devedesetih godina Internet se širio ubrzano. Kada se pogleda statistika dolazimo do zaključka da se širio brže od mobilnih telefona. Svakog meseca u toku prošle godine rastao je za skoro 20%. Ekspanziju doživljava i uvođenjem u osnovne i srednje škole, fakultete i biblioteke kao i u komercijalni sektor.

Ljudi uglavnom žele da budu deo Interneta zbog slobode. Slobode govora i pristupa informacijama. U modernom svetu Internet predstavlja funkcionalnu anarhiju. Ne postoji cenzura, šefovi, akcionari ili bilo koje ograničenje. svaki kompjuter se može obratiti drugom kao sebi ravnom sve dok poštuje pravila TCP/IP protokola.

Ipak ljudi po svojim potrebama spojeni u grupe imaju drugačije zahteve i potrebe. Ljudi koji Internet koriste za posao očekuju čvršći finansijski nivo, vlada želi da je

regulisaniji, akademski građani materijale bitne za istraživanja. Zbog različitih potreba i očekivanja Internet danas opstaje u blagodarno anarhičnim uslovima. Danas i naši kućni računari predstavljaju jedan Internet čvor.

Nekada se Internetu pristupalo uglavnom pomoću računara i korišćenjem telefonske linije. Moglo se pristupiti uglavnom formiranim grupama NETNEWS-a gde se mogla koristiti sopstvena email adresa.

Internet je postao sve pristupačniji i jeftiniji krajem devedesetih i početkom dvehiljaditih godina. Korišćenje je postalo jednostavnije, a TCP/IP sistem omogućio je korišćenje prostora za razvoj kvalitetnijeg pristupa korisnicima.

2.4 Internet danas u svetu i u Srbiji

Mreža u kojoj se može koristiti niz usluga, a širom sveta povezuje milione računara jeste Internet. Predstavlja jednu informatičku mrežu koja nije u ničijem vlasništvu pojedinačno. Zasniva se na velikom broju lokalnih sistema koji imaju različitu svrhu i veličinu, a međusobno su povezani u jednu veliku mrežu. Cilj je da preko više različitih i odvojenih puteva se stigne do odredišta. Podatak se može razložiti na pojedinačne delove – pakete, a paketi mogu na različite načine, odnosno različitim putanjama stizati na odredište.

Kada se govori o brzini Interneta, moramo biti svesni da se ona povećava iz dana u dan. Danas, u razvijenim zemljama informacije se razmenjuju brzinom oko 50MB/s dok je nekada je protok bio najviše 10KB/s. Danas je primetan uticaj Interneta na društvo i sve više se radi na sigurnosti i povećanju brzine. Većinom, lokalne mreže (LAN-ovi) dizajniraju se tako da brzina između ključnih mrežnih uređaja ima brzinu od 10GB/s. Ovakav dizajn čini osnovu lokalne mreže – backbone.

Internet u Srbiji je počeo da se razvija posle Dejtonskog sporazuma 1995. godine. Koji je Internet provajder prvi počeo sa radom je jako teško odrediti. Trenutno u Srbiji postoji preko 250 firmi koje se bave Internet uslugama. Kao sam početak, vezuje se za kraj osamdesetih godina povezivanjem Univerziteta u Beogradu na tadašnju Evropsku Akademsku Mrežu (EARN). Zbog rata koji je zadesio ove prostore devedesetih godina veza je bila prekinuta. Internet komunikacija je nastavljena 1995.godine. Tih godina je komunikacija išla preko kablova do Mađarske. U tom period mreža je bila izložena čestim kvarovima i podložna interferencijama. U Srbiji Internet je tek 2000. godine doživeo ekspanziju. Danas u Srbiji kompjuter poseduje 65,8% domaćinstava, odnosno 1,4% više nego predhodne godine. Statistika je bazirana na istraživanju sprovedenom 2016. godine od strane Republičkog zavoda za statistiku o upotrebi informaciono-komunikacionih tehnologija.

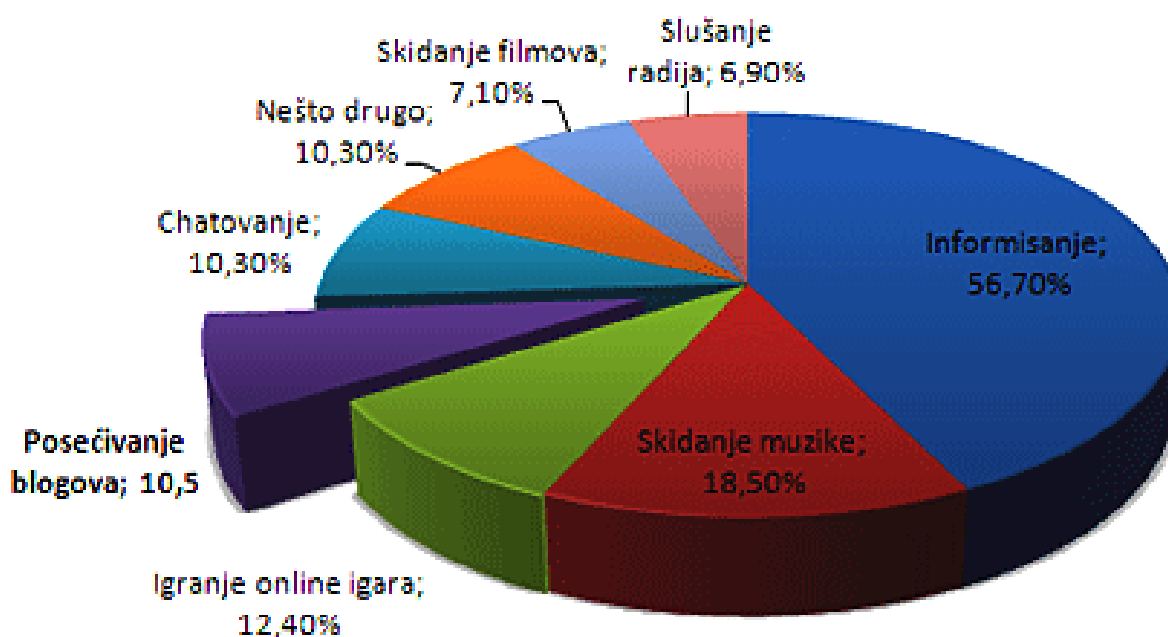
Statistika još pokazuje da je zastupljenost Internet priključka najveća u Beogradu, a iznosi 73,1%, dok je u Vojvodini 68,7%. Centralna Srbiji po toj statistici ima oko 57,9% Internet priključaka. Internet priključke uglavnom poseduju domaćinstva čiji je mesečni prihod veći od 600 evra (94,7%), dok učešće domaćinstava sa prihodom do 300 evra iznosi svega 46,1%.

Kada se gleda vrsta priključka DSL (ADSL) ima 45,5% od ukupnog broja korisnika, dok kablovski Internet poseduje 45,3%. Broj onih koji imaju modemsku konekciju iznosi 1,2%.

Širokopoljnu (broadband) Internet konekciju u Srbiji ima 57,8% domaćinstava. To predstavlja 1,8% više nego prošle godine. Zastupljenost ove vrste konekcije najveća je u Beogradu (68,5%), zatim u Vojvodini (61,0%), dok je najmanja u centralnoj Srbiji (50,4%).

Po prikazanoj statistici više od 2,6 miliona ljudi koristi računar svakog dana, a više od 2,4 miliona svakodnevno koristi Internet. Najviše se Internet koristi za komunikaciju putem emaila (70,4%). Na drugom mestu su čitanje i preuzimanje novina, kada se govori o sadržaju koji se na Internetu pretražuju. I u novije vreme velika pažnja se posveđuje društvenim mrežama kao što su Facebook i Twitter. Po statistici, čak 68% Internet se koristi za pristupanje ovim mrežama. Najmanje se koristi za preuzimanje softvera - 27,9%, traženje posla 24,3% i učešće na profesionalnim mrežama -17,4%.

Rezultati su pokazali da preko više od 900.000 ljudi u Srbiji u poslednjih godinu dana koristi Internet za kupovinu ili poručivanje robe. U odnosu na prošlu godinu zabeležen je rast od 300.000 korisnika.



Dijagram korišćenja Interneta u Srbiji

2.5. Povezivanje na Internet

Internet je velika mreža internih mreža, povezanih za tu svrhu dizajniranim uređajima, na krajevima na kojima su krajnji korisnici. Zahtevi za povezivanje korisnikovog računara s Internetom su:

- Fizička povezanost - mrežna kartica, mrežni uređaji (mreža, zvezda...)
- Logička povezanost - protokoli (najčešće broadcast i tokenpassing)
- Aplikacije - prikazuju informacije (Internet explorer, Outlook...)
- Komponente mrežnog sistema dele se u tri grupe:
- Uređaji krajnjeg korisnika (End-user devices) - računar, server...
- Mrežni uređaji (Networking devices) - router, switch, hub, bridge...
- Spojni vodovi (Cabling) - bakarni, optički, bežični...

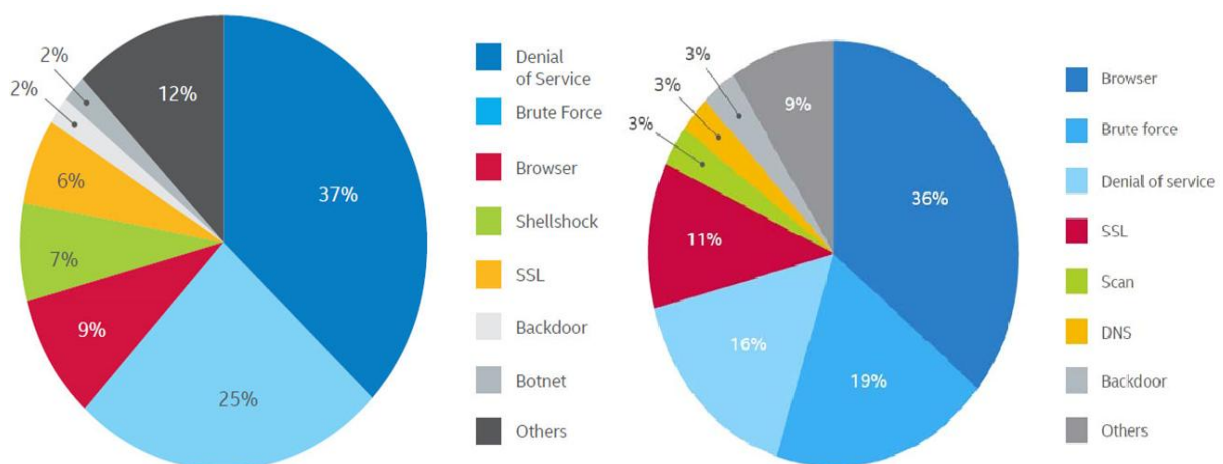
Uređaji krajnjeg korisnika omogućavaju korisniku korišćenje raznoraznih aplikacija, radi korišćenja raznih usluga Interneta, a mrežni uređaji omogućavaju razmenu informacija između uređaja korisnika preko spojnih vodova različitih vrsta.

Fizička konekcija za mrežu ostvaruje se spajanjem sa specijalno dizajniranom karticom, koja se stavlja u računar i omogućava modemska ili Ethernet komunikaciju. Dobro je da ove kartice za navedenu radnju imaju vlastiti procesor kako bi se što manje opteretio procesor računara. Sve su češći slučajevi da su obe funkcije implementirane na matičnoj ploči računara, što nije dobro jer su to obično jeftiniji sklopovi. U profesionalne namene se ugrađuje kvalitetna NIC kartica u PC računar i isključuje integrisana na matičnoj ploči.

Logička konekcija za mrežu koristi standarde nazvane protokoli. Protokol je kao što smo do sada definisali, formalni skup pravila i konvencija s kojima se u radu koriste mrežni uređaji. Veza prema Internetu može se ostvariti korišćenjem više vrsta protokola, ali je TCP/IP skup protokola osnova današnjeg Interneta. Mrežni uređaji povezuju korisničke uređaje, pa i same mreže, u jedinstvenu funkcionalnu celinu.

2.6 Mrežni napadi

Kriminalci biraju, iz raznovrsne liste, neke od metoda mrežnih napada, kako bi napali mala preduzeća[10]. Neki tipovi su češći, pa imajući to u vidu lakše se biraju odbrambeni prioriteti.



Metode mrežnog napada iz 2015. (levo) i 2016. (desno)

2.6.1 Browser attacks

Napadi preko browser-a ciljaju krajnje korisnike koje surfuju Internetom. Oni pokušavaju da prevare surfere da preuzmu malware koji su preruseni kao softverske aplikacije.

Sajber kriminalci takođe ciljaju popularne operativne sisteme i aplikacije korišćenjem exploit-a, koji može da bude deo podataka ili niz komandi koje iskorišćavaju ranjivosti u sistemu.

Jedan od najboljih načina da se izbegnu napadi je da se redovno ažurira veb pretraživač, kao i programi, kao što su Java i Flash. Ovo obezbeđuje da su novootkriveni sigurnosni propusti popravljani pre nego što se mogu eksploatisati.

2.6.2 Brute force attacks

Napad brutalnom silom je kada haker pokušava da dekodira lozinku nasumično pogađajući šifru. Neki napadi traže zadnja vrata, ali napad silom pokušava da razvali ulazna vrata. Automatizovani softver sistemi se često koriste da se pogodi stotine ili hiljade kombinacija lozinki.

Postoji mnogo načina da se odbrani od napada. Jedan od najjednostavnijih je da se zaključa account nakon određenog broja pokušaja. Blokiranje IP adrese posle više neuspeha prijavljivanja je još jedan od načina. Korisnici mogu da se zaštite tako što će često menjati svoje lozinke, a pomoću kombinacije brojeva, slova, simbola i predmeta otežati napadaču da je pogodi.

2.6.3 SSL attacks

Secure Sockets Layer (SSL) uspostavlja šifrovanu vezu između sajta i pretraživača, ili mail server i klijenta pošte. To je standardna bezbednosna tehnologija koja omogućava da se sigurnosne informacije bezbedno dostave.

SSL napad presretne šifrovane podatke pre nego što se mogu kodirati, dajući pristup napadaču osetljivim podacima, uključujući informacije o kreditnoj kartici, lozinci, cookies i druge provere identiteta tokena. Ranjivost je zakrpljena 2014, i SSL 3.0 se smatra zastarelim protokolom.

2.6.4 Scans

Port skeniranje su neprijateljske pretrage na internetu za otvorene portove preko kojih napadači mogu da dobiju pristup računaru. On nije jedan od pravih tipova mrežnih napada, umesto toga oni su obično izviđanja i vide se kao potencijalni predhodnik napada.

Uljez šalje poruku portu, odgovor mu može otkriti status porta i pomaže mu da identifikuje operativni sistem i njegove slabosti, što može pomoći pri pokrenuti budućeg napada.

2.6.5 DNS attacks

Domain name server (DNS) održava direktorijum domena i prevodi ih u IP adrese.

DNS imitiranje je kada se podaci ubace u Domain Name Sistem cache, izazivajući da server vrati netačnu IP adresu, koja preusmerava saobraćaj na alternativni kompjuter po izboru napadača.

DNS otmica je vrsta mrežnog napada koji preusmerava korisnike na lažne veb strane kada pokušavaju da pristupe legitimnim. Mnoge kompanije ne štite DNS jer ne shvataju da je pretnja vektor.

2.6.6 Backdoor attacks

Backdoors su aplikacije koje omogućavaju da se daljinski pristupi računarima. Mnoge backdoor aplikacije su dizajnirane da zaobiđu sistem zaštite od upada.

Backdoor je vrsta napada koji zaobilazi normalnu potvrdu identiteta da bi imao daljinski pristup po volji. Backdoors napadi su ređi i često se koriste kao deo ciljanih napada. U ovim slučajevima backdoor može biti prilagođen i dizajniran da izbegne otkrivanje i obezbedi prikrivenu tačku ulaska.

2.6.7 Botnet attacks

Botnet je grupa otetih/hakovanih računara koji su daljinski kontrolisani od strane jednog ili više zlonamernih hakera.

Napadač koristi botnet za zlonamerne aktivnosti, ili iznajmljuje botnet drugima za obavljanje zlonamerne aktivnosti. Može da se koristi za pokretanja DDoS napada, za slanje spam email, a napadači koriste botnet za njihov prljavi posao.

2.6.8 Distributed denial-of-service (DDoS) attack

Denial of Service (DoS) napad sprečava korisnike da pristupe uslugama ili informacijama. Oni se smatraju uspešnim kada napadač napuni server sa više zahteva nego što server može da obradi.

Distributed Denial-of-Service (DDoS) napad je kada napadač koristi mrežu zombi računara da sabotira određeni sajt ili server. Napad se dešava kada napadač kaže svim zombi računarima da kontaktiraju određeni sajt ili server iznova i iznova. To povećanje obima saobraćaja, opterećuje sajt ili server, i dovodi do toga da bude spor za ostale korisnike, ponekad do te mere da se sajt ili server gasi u potpunosti. Napadi su "distribuirani", jer napadač koristi više računara, da pokrene denial-of-service napada. DDoS napadom se najčešće napadaju IXP i ISP.

2.7 Odbrane od napada

Postoji veliki broj strategija za odbranu od napada i svaka ima svoje mane i vrline. Navešćemo neke od njih.

2.7.1 Blackholing

Blackholing je česta strategija odbrane koja se koristi da se zaustavi DDoS napad blokiranjem dolaznog saobraćaja i preusmeravanjem u crnu rupu (Blackhole). Blackholing odbacuje sav saobraćaj ka ciljanoj IP adresi. Lažni i legitiman saobraćaj se šalju u crnu rupu i ne obrađuju se ni na koji način. Svaki zahtev za pristup se jednostavno baca u prazan prostor i zauvek je izgubljen. DDoS napadi traju u rasponu od nekoliko dana do nekoliko meseci, pa ova strategija predstavlja pravi izazov za IXP. Pitanje je da li pružene usluge mogu sebi da priušte da budu van mreže danima / nedeljama / mesecima?

Usluge koje najviše gube u napadu su:

- Veb sajtovi
- Internet bankarstvo
- Bankomati
- Call-centari
- E-mail

Cela poenta DDoS napada je da se onemogući servis. Kada IXP uzime sav saobraćaj i preusmeri ga u crnu rupu, on time dovrši zadatak hakera.

2.7.2 Selective blackholing

Umesto blackholing-a IP adresa za ceo Internet, može biti korisnije da se promeni BGP rutiranje za određeni raspon adresa, tako da je dostupan samo za delove Interneta. To se obično naziva "selektivni blackholing". Ideja je da mnoge Internet usluge treba da budu dostupne samo u određenom regionu (obično neke zemlje ili kontinent). Na primer, koristeći selektivni blackholing, nemački IXP pod napadom može da izabere da njegov IP-opsega bude blackholed za saobraćaj koji dolazi iz Kine, dok će Evropske IP adrese moći da pristupe ciljanoj adresi. Ova tehnika može zadovoljavajuće da radi i ako napad dolazi iz drugačijeg izvora saobraćaja van redovnog saobraćaja.

2.7.3 Scrubbing

Bolje rešenje od blackholing-a je da se koriste „scrubbing” centri, koji se obično hostuju van IXP mreže, kao usluga. Kada je pod DDoS napadom, IXP preusmerava saobraćaj za taj IP-opseg do centra za filtriranje. Scrubbing centar ima opremu za filtriranje neželjenog saobraćaja, ostavljajući (uglavnom) čist saobraćaj koji se rutira nazad IXP-u. U poređenju sa blackholing-om ovo je bolje rešenje, jer su usluge na ciljanoj IP adresi ostale na raspolaganju. Mana je što su „scrubbing” centri komercijalni i što može dosta da košta. Isto tako, čišćenje saobraćaja nije uvek lako, pa saobraćaj može biti i lažno pozitivan (željeni saobraćaj se filtrira) i lažno negativan (neželjeni saobraćaj se ne filtrira).

2.7.4 Traffic engineering

U okviru većih mreža, moguće je da se stvori "sinkhole" ruter koji samo privlači saobraćaj od IP-opsega pod napadom. Saobraćaj prema svim drugim IP-opsezima biće usmeren na druge rutere. Na ovaj način, IXP je u stanju da izoluje DDOS u određenoj meri objavljivanjem napadnutog IP-opsega u BGP samo na sinkhole ruteru, a u isto vreme zaustavljajući objavljivanje tog IP-opseg na drugim ruterima. Saobraćaj sa Interneta do te destinacije će biti forsiran kroz taj ruter. Ovo može dovesti da dolazeći saobraćaj na tom ruteru bude zasićen, ali saobraćaj na svim ostalim ruterima će teći normalno.

Veliki nedostatak ove metode je da čitav opseg u kome je napadnuta IP adresa (najmanje / 24) može biti zasićen. Zbog toga je ova metoda često poslednje rešenje.

2.7.5 Local filtering

Ako IXP ima dovoljno kapaciteta na svom uplink-u, može da se sprovede lokalno filtriranje. Ovo se može uraditi na razne načine, kao na primer:

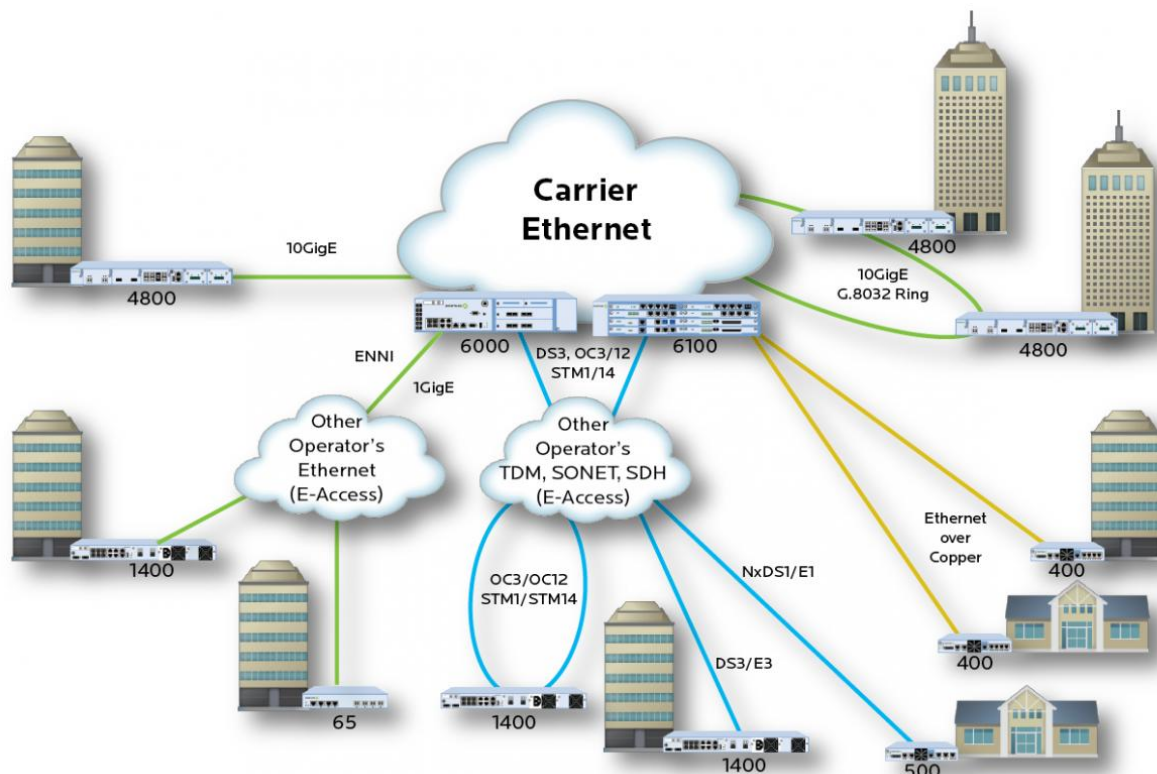
- dodavanje pristupne liste na ruteri, odbacujući karakteristike kao što su adresa izvora ili destinacioni port.
- sprovođenje granice saobraćaja kako bi se smanjila količina saobraćaja na ciljnoj IP adresi
- preusmeravanje saobraćaja preko lokalnih „scrubbing“ kutija koje filtriraju neželjeni saobraćaj
- sprovođenje BGPFlowspec, koji omogućava ruterima da sprovedu i razmene pravila filtriranja koristeći BGP.

3. Forme i oblici mrežnog Interneta

Prvo ćemo raščistiti razliku između tri naizgled slična pojma:

- Intranet - korišćenje tehnologija koja su bazirana na Internetu u okviru organizacije ili kompanije, a u svrhu podrške razmene podataka i informacija
- Internet - svetski sistem umreženih računara, mreža unutar mreže ili interkonekcija između više računara
- Ethernet - dominantna LAN (Local Area Network) tehnologija.

Ethernet se pojavio kao odgovor na sve veći broj upita za brzim LAN tehnologijama. Kada se pojavio Ethernet 1973. godine brzina je bila do 3MB/s, dok je do danas brzina eksponencijalno rasla i trenutno radi na 10GB/s. Okosnica Ethernet-a je pristup više korisnika na zajednički medij po CSMA/CD principu. Specifikacije ove mreže podržavaju različite medije sa različitim propusnostima (Bandwidth – BW) i različite verzije hardvera u odnosu na prvi i drugi sloj OSI modela. Ethernet je realizovan kao otvoreni standard, tj standard koji ne traži zahtev sa licenciranim pravima, koji je od osnivanja 1980. godine uveden od strane kompanije DIX (Digital, Intel, Xerox). Prednosti Ethernet-a su mnoge: jednostavnost i lako rukovanje, pouzdanost u radu, kompatibilnost sa starijim tehnologijama, prihvatljiva sigurnost sistema, mala cena održavanja i mnoge druge.



Ethernet dijagram

Intranet je privatna računarska mreža unutar neke organizacije koja u svom sistemu koristi Internet protokole, koja je mrežno povezana i koja omogućava upotrebu javnih komunikacionih sistema kako bi omogućila zaposlenima unutar te kompanije sigurnu razmenu informacija ili obavljanje nekih radnji vezane za organizaciju. Intranet je moguće napraviti upotrebom istih koncepata i tehnologija kao što je potrebno i za Internet, preciznije kao što su klijenti i serveri koji koriste Internet Protokol (IP). U Intranetu se koriste i drugi Internet Protokoli kao što su HTTP, FTP i E-Mail. Intranet je u suštini privatni oblik Interneta. Funkcije Intraneta su E-Mail, zajedničko korišćenje datoteka, upravljanje informacijama i davanje pristupa informacijama, pretraživanje informacija, upravljanje i održavanje mreže. Velike kompanije dozvoljavaju svojim zaposlenima da izađu na Internet preko Firewall servera. Postoji mogućnost da se dolazni i odlazni paketi skeniraju iz razloga sigurnosti. Kada se deo Intraneta otvori prema kupcima i ostalim ljudima van kompanija, taj deo postaje Extranet. Kompanije mogu uz specijalizovane metode enkripcije/dekripcije i preko ostalih sigurnosnih mera da međusobno povežu Intranet-ove.



Intranet dijagram

3.1 Tehničke osnove i principi rada Interneta – protokol TCP/IP

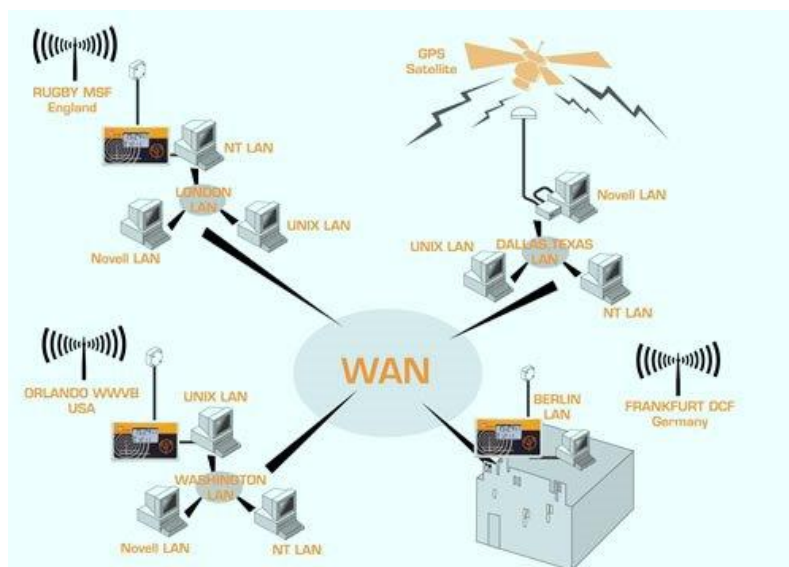
Prvobitna ideja svetske mreže je bila ideja da postoji centralizovani računarski sistem – koncept računarskog centra gde jedan veliki računar opslužuje čitavu organizaciju. Međutim zbog poteškoća u razvoju, prešlo se na vrlo jednostavniji sistem gde računarska mreža funkcioniše kao niz samostalnih računara koji su međusobno povezani, tj. mogu razmenjivati informacije.

Mreža je omogućila deljenje resursa tako da je sve što se nalazi na datoj mreži dostupno svima bez obzira na fizičku udaljenost. Pored toga omogućuje se skalabilnost kroz klijent - server model, komunikacija između udaljenih organizacionih jedinica i razdvojenih klijenata, put do udaljenih informacija finansijske transakcije, razmena multimedijalnih

informacija itd. U suštini radi se o povezivanju više malih lokalnih mreža (LAN) u veće grupe (MAN) i njihovo povezivanje u jedinstveni skup na svetskom nivou između država (WAN). LAN je mreža, obično u privatnom vlasništvu unutar jedne ili nekoliko zgrada čija udaljenost nije veća od nekoliko kilometara. Koristi mrežnu ili zvezdastu topologiju sa brzinom prenosa podataka od 10-1000 Mb/s (1 megabit/sec = 1'000'000 bit/sec).

MAN je veća verzija LAN-a koja koristi sličnu tehnologiju, povezuje više kompanija, ustanova ili gradova i može biti privatna ili javna. Obično koristi DQDB (Distributed Queue Dual Bus) i koncipirana je tako da se sastoji od dva jednosmerna kabla na koje su svi računari povezani što olakšava dizajn mreže.

WAN povezuje geografski veliko područje, državu ili kontinent.

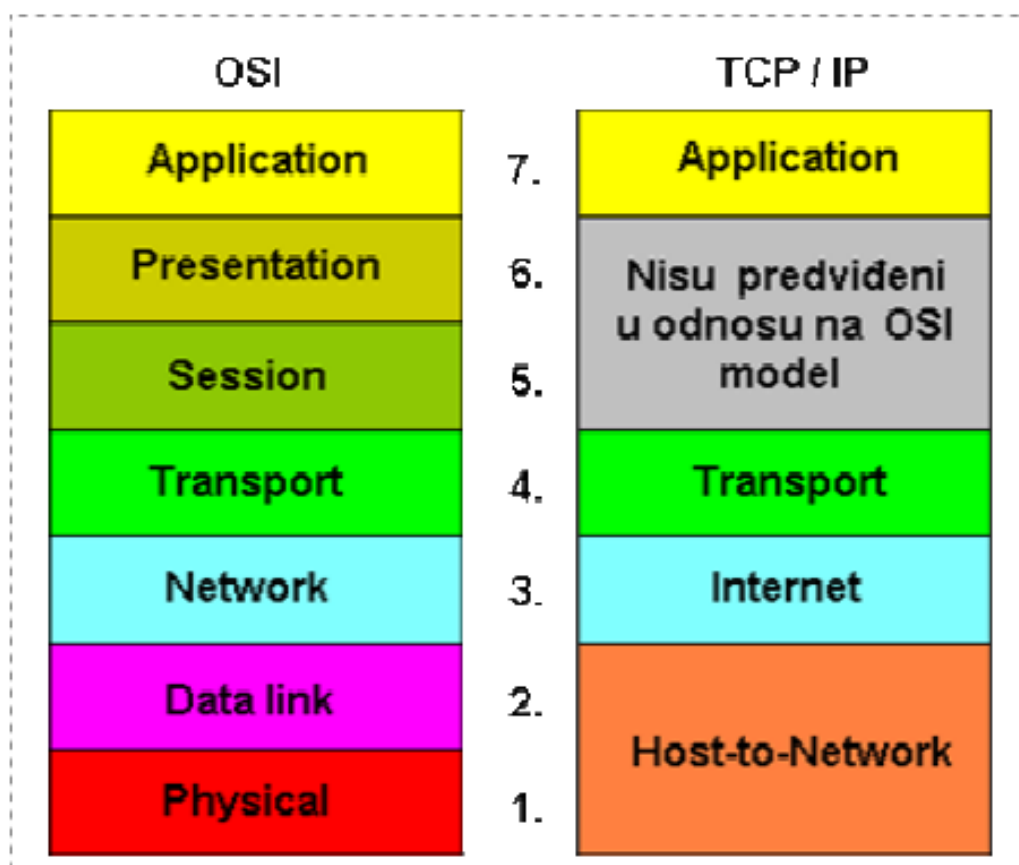


WAN topologija

3.2 OSI struktura Interneta

U prethodnom delu teksta pričali smo uopšteno o mrežama, i većina njih je napravljena kao niz više slojeva ili nivoa. Svaki od tih slojeva je funkcionalan samo kao deo celine, a ne kao samostalna jedinka. Svaka od spomenutih mreža je izgrađena od različitih vrsta nivoa, imena, sadržaja i funkcija slojeva. Jedan od razloga je to što su mreže nastajale u različito vreme i drugačija tehnologija je bila dostupna, što je dovelo do sledećeg problema. Nemogućnost komunikacije različitih mrežnih modela dovela je do problema u usklađivanju njihove međusobne komunikacije. TCP / IP model se zadržao do danas, gde i dalje predstavlja osnovu funkcionisanja Interneta po takozvanom OSI principu.

Sledeća slika pokazuje organizaciju TCP / IP modela po slojevima u odnosu na OSI model:



TCP / IP referentni model u odnosu na OSI model

Svaki nivo ima zadatak da pruži neku vrstu usluge (servisa) za više nivoe, sa ciljem da viši nivoi ne moraju paziti o detaljima ugradnje i implementacije tih usluga. Sloj 'n' na jednom kompjuteru komunicira sa slojem 'n' na drugom pomoću skupa pravila koja se nazivaju protokol.

Sloj domaćin – mreža (Host-to-Network) je sloj gde nije precizno definisan protokol kojim se host vezuje za mrežu. Ovaj sloj koristi MAC adresu za komunikaciju sa drugim slojevima i šalje podatke na mrežni medijum. Podaci su skupovi bit-ova koji se nazivaju frame (okvir).

Internet – funkcioniše na principu IP (Internet Protocol) grupa podataka koji se nazivaju packet ili datagram. Grupe podataka su usmeravane optimalnim putem i ostvaruju kontakt, a zatim i komunikaciju između dva udaljena kompjutera. Ruteri koriste protokole koji se nazivaju ruting protokoli (routing protocols), i IP adresu u zaglavlju paketa. Protokoli i IP adresa kao celina omogućavaju protokolu da kreira optimalni put. Internet protokol potpada u routed protokole. U daljem tekstu ćemo opisati slojeve protokola:

Prenosni sloj (Transport layer) – funkcija ovog sloja je prenos podataka među peer procesima između dva kompjutera uz upotrebu TCP protokola (Transmission Control Protocol) ili UDP protokola (User Datagram Protocol). U prenosnom sloju podaci su

grupisani u celine koje se nazivaju segmenti. Zaglavlje ovih protokola nose oznaku ulaza, da bi naredni sloj mogao da zna koja će aplikacija upotrebiti podatke u segmentu. TCP omogućava pouzdanu serijsku komunikaciju, i baza je za više protokola od kojih se zahteva da se podaci prenesu bez greške. Ovo mu omogućava sama definicija protokola zahtevajući potvrdu ispravnog prijema podataka pre slanja narednih podataka. UDP je nepouzdana serijska komunikacija (primer: prenos govora, video snimaka) i ne zahteva potvrdu prijema podataka pre slanja narednih, te je njegova struktura jednostavnija. Koristi se u sistemima gde je pouzdanost manje bitna.

Aplikacijski sloj (Application) – sadrži sve protokole višeg nivoa. U početku je to bio virtuelni terminal (Telnet), prenos datoteka (FTP) i elektronska pošta (SMTP). Posle nekog vremena razvijen je i DNS, NNTP, HTTP. Aplikacijski sloj dozvoljava razmenu podataka među peer procesima dva računara između dve aplikacije iste namene. Radi na principu čitanja port-a iz zaglavlja segmenta, te određena aplikacija uzima njegove podatke i od jednog segmenta kreira razumljiv skup podataka. Dekriptacija ovih podataka uz pomoć aplikacije se vrši u ASCII kodu, MIDI, JPEG, TIFF formatu itd.

Slojevi između sebe nemaju „pravi“ prenos podataka. Sistem funkcioniše tako što se informacije šalju sloju ispod, sve dok informacija ne dođe do najnižeg sloja. Ispod najnižeg sloja se nalazi fizički medij preko kojeg se odvija komunikacija. Skup slojeva i protokola čini mrežnu arhitekturu. Skup protokola čine lista protokola, po jedan za svaki sloj. Internet se iz perspektive mrežnog sloja može posmatrati kao skup međusobno povezanih pod mreža. Ne postoji prava struktura, ali može da se definiše nekoliko glavnih kičmi (backbone) na koje su regionalne mreže povezane.

Na regionalne mreže su zatim povezani LAN univerziteta, kompanija, davaoca internet usluga itd. Internet zapravo na okupu drži protokol mrežnog nivoa IP (Internet Protocol) čiji je zadatak da na najbolji mogući način prenese IP.

UDP (User Data Protocol) protokol omogućava slanje IP datagrama sa dodatim kratkim zaglavljem bez potrebne potvrde da se uspostavi veza. Prenos paketa na medij odvija se posredstvom najnižeg nivoa (sloja) OSI - TCP/IP modela. Mediji za prenos podataka su različiti, ali je gotovo svima zajedničko da se paketu dodaju MAC adrese mrežne kartice ili nekog interface-a (Media Access Control) izvora i odredišta. Navedena struktura zajedno pravi okvir (Frame) podataka koji se serijski razmjenjuje između izvora i odredišta.

3.3 Protokol rutiranja

Protokol rutiranja ([eng.](#) Routing protocol) predstavlja skup pravila kojim ruteri razmenjuju informacije o rutama kojima paket treba da se kreće da bi došao do željene destinacije.

Protokol rutiranja određuje kako ruteri komuniciraju jedni sa drugima, širenjem informacija koje im omogućavaju da izaberu puteve između bilo koja dva čvora na računarskoj mreži. Algoritmi rutiranja utvrđuju konkretan izbor rute. Svaki ruter ima prethodno znanje samo mreže vezane za njega direktno. Protokol rutiranja deli ovu informaciju prvo među prvim susedima, a zatim kroz mrežu. Na ovaj način, ruteri steknu znanje topologije mreže.

Interior gateway protocols (IGPs) razmenjuju informacije rutiranja unutar jednog rutirajućeg domena. Primeri IGP uključuju:

- Open Shortest Path First (OSPF)
- Routing Information Protocol (RIP)
- Intermediate System to Intermediate System (IS-IS)
- Enhanced Interior Gateway Routing Protocol (EIGRP)

Exterior gateway protocols razmenjuju informacije rutiranja između autonomnih sistema. Primeri uključuju:

- Exterior Gateway Protocol (EGP)
- Border Gateway Protocol (BGP)

Stotine različitih mrežnih protokola su stvoreni za podršku komunikaciji između računara i drugih vrsta elektronskih uređaja. Takozvani protokoli rutiranja su porodica mrežnih protokola koji omogućavaju kompjuterskim ruterima da komuniciraju jedni sa drugima i zauzvrat da inteligentno šalju saobraćaj između njihovih mreža.

Svaki mrežni protokol rutiranja obavlja tri osnovne funkcije:

1. Otkriće (discovery) - identifikuju druge rutere na mreži,
2. Upravljanje rutama (route management) - pratiti sve moguće destinacije zajedno sa nekim podacima opisuju put svakog,
3. Određivanje puta (path determination) - pravi dinamičke odluke gde da pošalje svaku mrežnu poruku.

3.3.1 Routing Information Protocol (RIP)

Routing Information Protocol (RIP) je jedan od najstarijih protokola rutiranja još uvek u širokoj upotrebi, ali ima značajna ograničenja, posebno u većim mrežama. Istraživači su razvili Routing Information Protocol 1980. godine za upotrebu na malim ili srednjim Internet mrežama koji su povezavali početni Internet.

RIP koristi skokove (hop) za metriku udaljenosti. Da spreči beskonačne petlje, broj skokova je ograničen na 15, što može da bude ograničenje ako je mreža dovoljno velika. RIP trazi od rutera da emituju celu svoju trenutnu tabelu ruta periodično (30 sekundi po defaultu).

Tradicionalni RIP podržava samo IPv4 mreže, ali novi RIPng standard takođe podržava i IPv6.

3.3.2 Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) je protokol rutiranja razvijen za IP mreže od strane IGP radne grupe Internet Engineering Task Force.

Stvoren je da se prevaziđu neka ograničenja RIP-a uključujući:

- ograničenje od 15 skokova (hops),
- nemogućnost da organizuje mrežu u hijerarhiju rutiranja, važno za upravljanje i performanse na velikim unutrašnjim mrežama,
- značajni skok mrežnog saobraćaja generisan stalnim slanjem pune tabele rutiranja u zakazanim intervalima.

OSPF ima dve primarne karakteristike:

- to da je otvoren protokol. Njegova specifikacija je u javnom domenu ,
- zasnovan je na Shortest Path First (SPF) algoritmu, ponekad poznat kao Dijkstra algoritam.

OSPF se koristi više od RIP u većim mrežama, jer ima efikasniji sistem za komunikaciju između rutera i zato što bolje vlada saobraćajem u većim mrežama.

3.3.3 Intermediate System to Intermediate System (IS-IS)

Intermediate System to Intermediate System (IS-IS) protokol funkcioniše slično kao OSPF. Dok je OSPF postao popularan izbor uopšte, IS-IS ostaje u širokoj upotrebi od strane ISP-a koji su imali koristi od protokola koji može da bude lakše prilagođen njihovim posebnim okruženjima. Za razliku od drugih protokola, IS-IS ne radi preko Internet protokola (IP) i koristi svoju šemu adresiranja.

3.3.4 Enhanced Interior Gateway Routing Protocol (EIGRP)

Cisco je razvio Internet Gateway Routing Protocol (IGRP) 1985. godine kao još jednu alternativu za RIP. EIGRP je razvijen 1992. godine i podržan je samo u Cisco mrežnim uređajima (ruterima). Radi po algoritmu na osnovu vektora udaljenosti.

EIGRP se koristi na rutere da dele rute sa drugim ruterima unutar istog autonomnog sistema. Za razliku od drugih poznatih protokola, kao što su RIP, EIGRP protokol samo šalje inkrementalne ispravke, smanjujući opterećenje na ruteru i količinu podataka koja treba da se prenosi.

EIGRP protokol je dizajniran sa ciljevima lakše konfiguracije i bolje performanse nego OSPF

3.3.5 Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) je u širokoj upotrebi na Internetu, ali obično spolja nego iznutra. Interna upotreba BGP je tipično samo za veoma velike mreže. Na primer, to može da se koristi kao veza između više mreža koje već koriste OSPF, kada je cela mreža prevelika za OSPF sama po sebi. BGP je jedinstven po tome što koristi TCP kao svoj transportni protokol. Internet provajderi (ISP) obično koriste BGP da pridruže svoje mreže zajedno. Osim toga, veće firme ponekad koriste BGP da se udruže nekoliko njihovih internih mreža. BGP uključuje pokazatelje troškova za svaki put, tako da pakete preuzme najefikasniji put. BGP detektuje izmene u tabeli rutiranja i selektivno šalje te promene ka drugim ruterima preko TCP/IP.

Profesionalci smatraju BGP najizazovnijim od svih protokola rutovanja da savladaju zbog svoje kompleksnosti konfiguracije.

Sadašnja verzija BGP je verzija 4 (BGP4).

3.4 Autonomni sistem

Autonomni sistem (AS) predstavlja mrežu, ili kolekciju mreža koje su nadgledane i kontrolisane od strane jednog entiteta ili organizacije.

AS predstavlja heterogenu mrežu tipično nadgledanu od strane velikih korporacija. AS ima više različitih podmreža sa kombinovanom logikom rutiranja i zajedničkim ruting polisama (pravilima po kojima se rutiranje saobraćaja obavlja). Svako podmreži IANA (Engl.

Internet Assigned Numbers Authority) dodeljuje globalno jedinstven 16 karakterni identifikacioni broj poznatiji kao ASN.

Autonomni sistemi su uvedeni kako bi se regulisale organizacije poput Internet servis provajdera (Engl. Internet Service Providers - ISP), edukativne ustanove i državna tela. Ovi sistemi se sastoje od više različitih mreža, ali funkcionišu pod pokroviteljstvom jednog tela radi jednostavnijeg i efikasnijeg upravljanja i nadgledanja. Velike organizacije uglavnom imaju kompleksnu mrežnu infrastrukturu koju čine manje mreže, geografski rasprostranjene ali povezane upotrebom sličnog operativnog okruženja.

Border Gateway Protocol (BGP) predstavlja protokol koji adresira rutiranje paketa između različitih autonomnih sistema kako bi ih spojio. BGP upotrebom ASN-a sa lakoćom identifikuje različite sisteme. Ovo je posebno vazno prilikom rutiranja i upravljanja ruting tabelama za udaljene mreže ili autonomne sisteme oko njihovih granica.

Javni AS ima globalno unikatni broj (ASN), ovaj broj se koristi i za razmenu eksternih ruting informacija (između susednih Autonomnih sistema) i kao identifikator samog AS.

Postoje dva tipa AS brojeva:

- Javni AS brojevi
- Privatni AS brojevi

Javni AS broj je obavezan samo kada AS razmenjuje ruting informacije sa drugim Autonomnim Sistemima putem javnom Interneta. Tacnije, sve putanje koje zapocinju od AS moraju biti vidljive na Internetu.

Privatni AS broj je obavezan ukoliko AS mora komunicirati upotrebom BGP protokola sa jednim provajderom. Iz razloga netransparentnosti komunikacije na Internetu između AS i provajdera, privatni AS ključ se može koristiti u ove svrhe.

4. IXP – Internet Exchange Point

Šta je IXP? Koja je prava definicija za to? Najpribližnije rečeno IXP je javna tačka interkonekcije u koje su umrežene tri ili više mreža ili autonomnih sistema. IXP kada se prevede znači tačka razmene Internet saobraćaja (Internet eXchange Point – IXP).

Internet nije jedan jedinstven entitet, već je skup više nezavisnih mreža. Entiteti kao jedinica u mreži su međusobno povezani klijenti uz pomoć protokola TCP/IP. Najvažnije članice ovog sistema mreža su IXP-evi, tj. Internet eXchange tačke, bez kojih Internet današnjice ne bi funkcionisao efikasno. Razlog je što bi različite mreže koje čine Internet morale da se direktno povežu sa svakom drugom mrežom, kako bi bila moguća razmena informacija. Daleko najjednostavniji oblik mrežne topologije je bilo uvođenje tački koje spajaju više davaoca usluga Interneta (ISP-eva). Kada više od dva davaoca Internet usluga rade u istom području, nezavisni hub obično radi efikasnije kao zajednička interkonekcijska tačka na kojoj se razmenjuje saobraćaj između lokalnih mreža. Sličan princip se koristi u avio-industriji na primeru aerodroma gde avio-kompanije razmenjuju putnike između letova veoma slično načinu na koji mreža razmenjuje podatke preko IXP-eva.

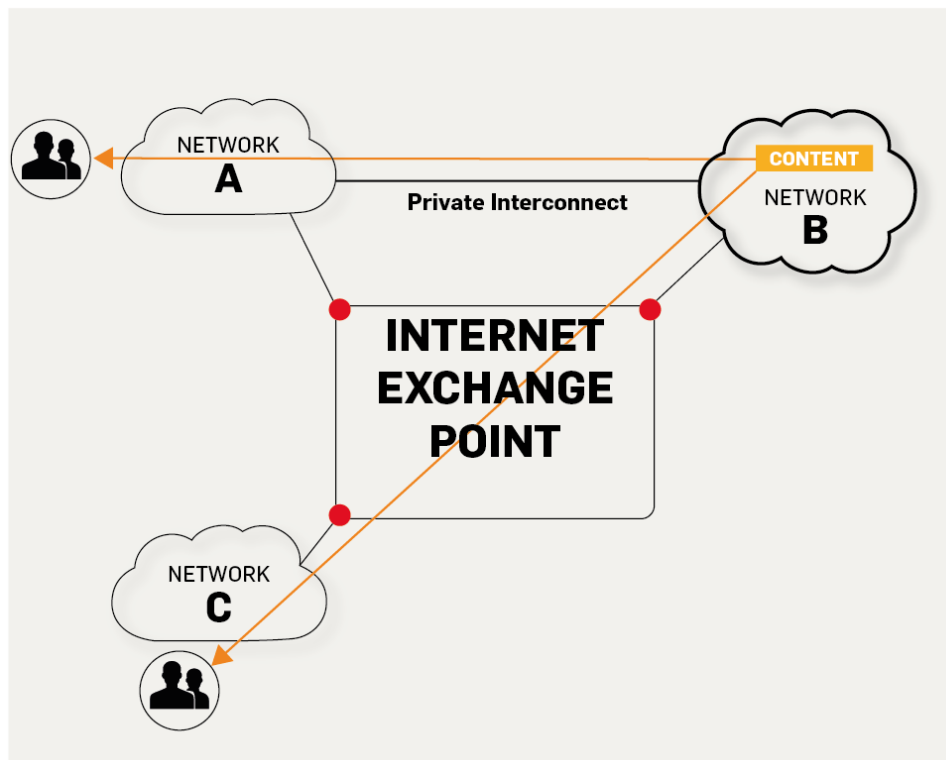
Internet exchange point je fizička lokacija gde se različiti internet provajderi nalaze, da razmene međusobni Internet saobraćaj preko bakarnih ili optičkih kablova koji povezuju njihovu opremu, preko jednog ili više Ethernet switcheva. Prvobitno nastojanje je da se lokalni saobraćaj zadrži na lokalnom nivou[1].

Postoje više vrsta postojećih institucionalnih i operativnih modela koji su usvojeni kako bi se upravljali IXP-evi. Izvršena je kategorizacija na pet tipova:

- Nefitne organizacije,
- Industrijska asocijacija Internet provajdera,
- Profitna organizacija neutralnog operatora,
- Univerzitet ili vladina organizacija,
- Neformalna asocijacija mreža.

Osim u Sjedinjenim Američkim državama, najčešći model IXP-eva je koncipiran kao neprofitna organizacija ili kao industrijska asocijacija Internet provajdera. Komercijalni model koji se koristi u SAD su upravljani od strane specijalizovanih peering centara razmene, ili kompanijama čija je glavna namena upravljanje centrima podataka, kao što su CIX, Any2 i Equinix.

Operativna pravila su relativno uniformna na većini IXP-eva u smislu vrste saobraćaja koji je dozvoljen sa komentarom da lokalni uslovi mogu da reflektuju neke varijacije u vrsti. Da bi povezivanje bilo dozvoljeno, mrežama je traženo da budu priznate od strane legalnih entiteta i da moraju biti licencirane za rad. Svakom entitetu koji želi da razmeni saobraćaj sa ostalim članovima IXP-eva je dopušteno da to uradi.

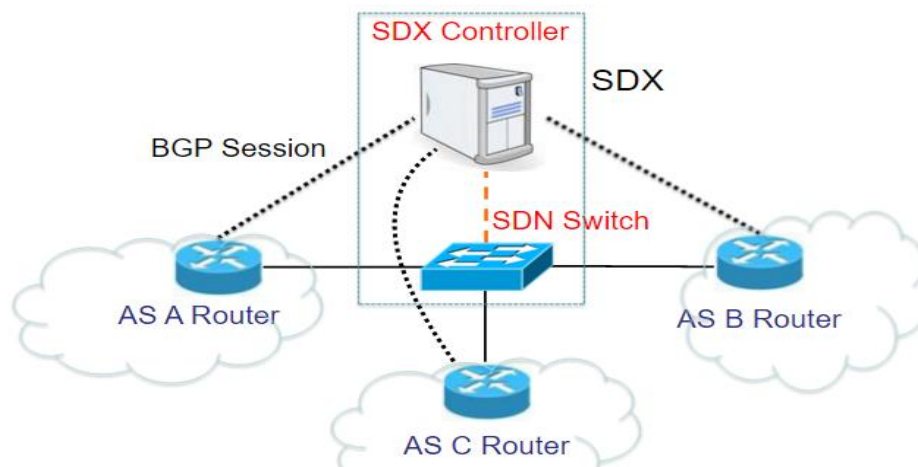


Dijagram Internet Exchange Point-a

Internet Exchange Point-ovi obezbeđuju IP interkonekciju za participante, koristeći Layer 2 ili Layer 3 mrežnu infrastrukturu. Layer 2 se zasniva na upotrebi mrežnog medija kao što je Ethernet. Border Gateway Protocol (BGP) je inter-autonomni sistem (Inter-AS) protokol rutovanja. Najčešće se koristi za olakšavanje razmene podataka i dostupnosti između mreža preko mrežnih medija.

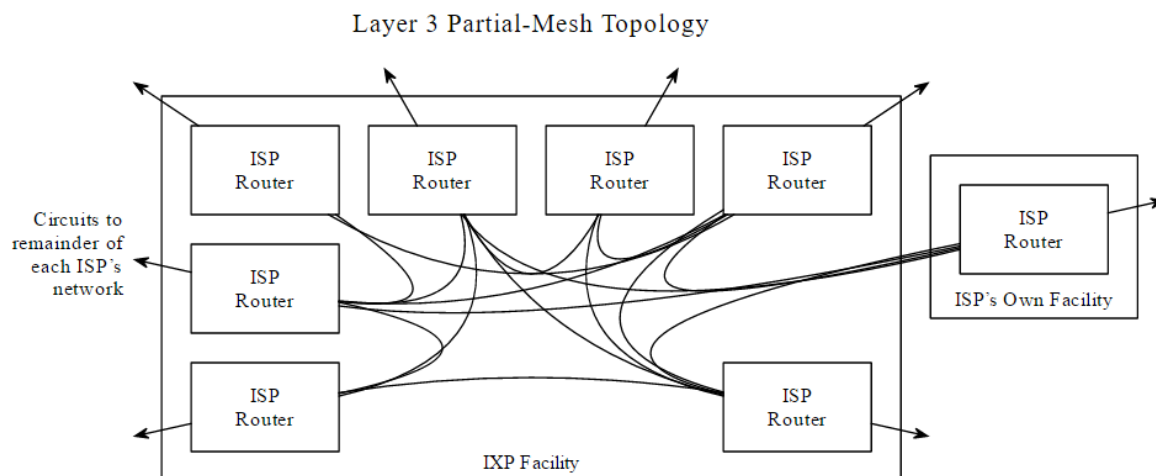
Ranije su bilateralne EBGp sesije bile najkorišćeniji vid prenosa dostupnosti informacije, ali sa povećanjem broja učesnika u velikim IXP-evima, dolazi do guste interkonekcije i moguća je pojava operacionálnih skaliranih problema za participante. Multilateralno povezivanje je metoda interkonekcije BGP predajnih rutera koristeći third-party sistem za posredovanje koji se obično u terminologiji naziva kao route server[7]. Route server je tipično upravlján i održávan od strane IXP operatora. Svaki participant multilateralne interkonekcije naziva se klijent route servera i dužán je da šalje informacije o mrežnoj dostupnosti serveru preko EBGp-a. Sledeći korak u procesu je da route server prosleđuje informaciju svakom klijentu multilateralne interkonekcije u skladu sa konfiguracijom infrastrukture. Iako route server koristi BGP za razmenjivanje informacije o dostupnosti sa svakim od klijenata, on ne prosleđuje saobraćaj podataka, i ne može se nazvati ruterom. Najbolje je da ga posmatramo kao reflektor rute, osim što je konfigurisan da radi preko EBGp umesto Intra-BGP (IBGP) protokola. Potrebna su neka usvanja na BGP protokolu da bi se obezbedio da EBGp ruter operište kao route server.

SDX = SDN + IXP



Dijagram BGP sesije

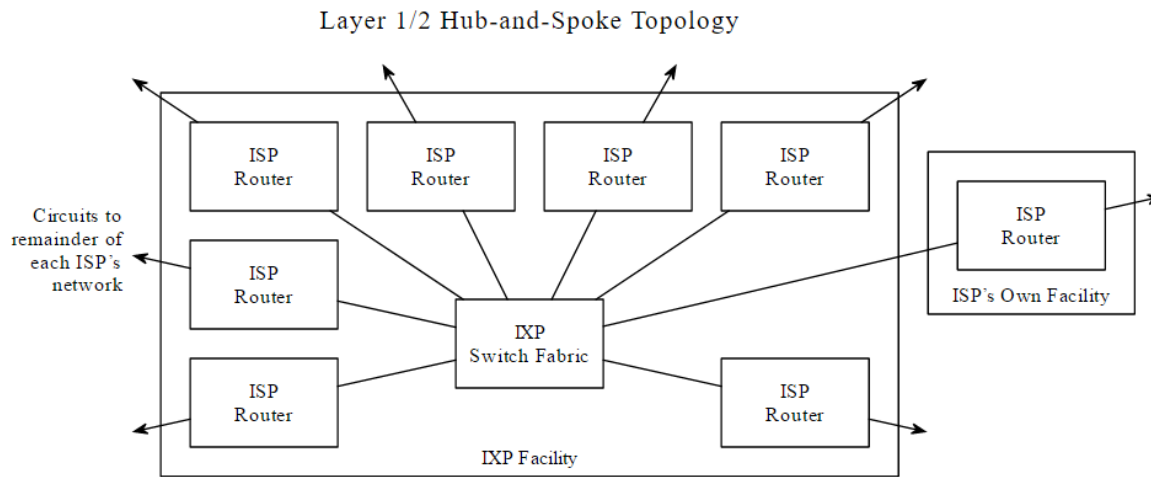
Postoje dva osnovna modela za IXP operacije. Prvi, koji je stariji, je da se sav saobraćaj između participantskih mreža odvija unutar jednog rutera. Ovaj vid se zove Layer 3 IXP. Trenutno model koji je dominantan u svetu je Layer 2 IXP gde svaka mreža dostavlja sopstveni ruter i saobraćaj se razmenjuje preko Etherneta prekidača. Beneficija Layera 3 je da je jeftiniji i jednostavniji za postavljanje, ali pri povećavanju mreže dolazi do problema skalabilnosti i autonomnosti samih članova jer nemaju punu kontrolu peer-ovanja i zavisni su od spoljne konfiguracije svih međusobnih ruta. Layer 3 zahteva da osoblje IXP-a bude bolje tehnički osposobljeno.



Topologija Layer 3 IXP-a

Slovenački IXP (SIX) je hostovan na ARNESu (akademska mreža) i jedan je od primera Layera 2 IXP-eva. Članovi povezuju svoje rutere preko fiber kabla. Uprkos

prvobitnoj investiciji, ovaj model se pokazao kao daleko jeftiniji i bolji pri interkonektovanju članova. Kolokvijalne potrebe su dosta manje, jer nema potrebe za naprednim konfigurisanjem, međutim ovaj model zahteva sigurnu Layer 2 infrastrukturu. Oprema koja se koristi u modelu mora biti podvrgnuta proveravama, jer svaki sigurnosni propust može dovesti celu mrežu u veliki rizik. Procedura je da svi portovi moraju biti podešeni sa odgovarajućim sigurnosnim ulaznim mehanizmima.



Topologija Layera 1/2 IXP-eva

Primarna uloga IXP-eva je omogućavanje povezivanja više mreža direktno ili putem razmene, umesto više „third-party“ mreža. Prednosti direktne komunikacije su cena, latencija i protok. Direktna interkonekcija, izbegava potrebe da podaci putuju ka drugim gradovima, koji su potencijalno na drugim kontinentima, te je samim tim je i sama latencija niža što se tiče razmene podataka[3]. Brzina protoka sa IXP infrastrukturom je najprimetnija u oblastima gde je slabo razvijena infrastruktura sagrađena sa svrhom povezivanja dalekih lokacija. ISP-evi u ovim regionama, kao što je Afrika, moraju da plate između 10 i 100 puta veće troškove za transport podataka nego u Severnoj Americi, Evropi ili Japanu. S'toga ISP-evi iz siromašnih regiona poseduju sporiju i limitiraniju konekciju ka ostatku Interneta. Međutim, konekcija ka lokalnom IXP im omogućava prenos podataka bez limita, troškova, gde je brzina protoka značajno unapređena između korisnika dva susedna ISP-a.

Tipičan IXP se sastoji od jednog ili više mrežnih prekidača, gde se priključuju ISP-evi koji participiraju u lokalnom IXP-u. Pre implementacije priključaka, baza Internet exchange point-ova je bio fiber optički „inter-repeater“ link (FOIRL) čvor ili prsten naziva „Fiber Distributed Data Interface (FDDI)“.

Jedna od najvećih prednosti povezivanja preko IXP-eva je značajno smanjenje latencije. Zahtevi brzine i latencije na raznim servisima koji se baziraju na „Cloud“ arhitekturi se mogu klasifikovati u tri nivoa: bazični, srednji i napredni. Za najnaprednije servise potrebno je posedovati latenciju koja je ispod 100 milisekundi. Zahtevi poput ovoga podižu

primamljivost kreiranju i pristupa IXP-u. Ako je saobraćaj regulisan lokalno, latencija se

BASIC	INTERMEDIATE	ADVANCED
Download: 750 kbps Upload: 250 kbps Latency: 160 ms	Download: 751–2,500 kbps Upload: 252–1,000 kbps Latency: 159–100 ms	Download: >2,500 kbps Upload: >1,500 kbps Latency: <100 ms
Single Player Gaming Text Communications (Email, IM) Stream Basic Video/Music Web Conferencing Web Browsing VoIP (Internet Telephony)	ERP/CRM HD Video Streaming Multiplayer Gaming Online Shopping Social Networking (Multimedia/Interactivity) Video Conferencing	3D Video Streaming HD Video Streaming Stream Super HD Video Connected Education/Medicine Group Video Calling Virtual Office

dramatično smanjuje.

Nivoi sofisticiranosti servisa na Internetu i potrebni uslovi

Visoka latencija, tj kašnjenje signala, značajno utiče na korisničko iskustvo upotrebe Interneta. Proizvođač telekomunikacione opreme „Nokia“ procenjuje da je kašnjenje značajnija stavka od brzine Interneta za servise kao što su VoIP, preuzimanje muzike i igranje preko interneta (NSN 2009). Korisnici postaju sve osetljiviji na kašnjenje i prestaju da koriste aplikacije ako im je potrebno dosta vremena da se pokrenu. Sa druge strane, ako aplikacije zahtevaju manje vremena za start, postoji tendencija porasta zainteresovanosti korisnika ka njima.

Rutovanje IP paketa ka dalekim destinacijama preko dugih kablova implicitno duplira latenciju, jer je potreban povratni put do destinacije. Sa IXP-evima saobraćaj ne mora da putuje do željene destinacije i da se vraća. Kao rezultat toga, korisnici mogu koristiti aplikacije koje ranije nisu mogli zbog visoke latencije.

Redukcija u kašnjenju prilikom rada preko IXP-eva je dokumentovana u raznim istraživanjima. Primer koji ćemo prikazati je kreacija Kenijskog Internet Exchange Point-a (KIXP) gde je latencija smanjena sa 200-600 milisekundi na 2-20ms.

Kako raste zastupljenost IXP-eva, oni vrlo često evoluiraju od jednostavnih servisa za rutovanje na centre za Internet ekspertizu u zemlji. Znanje zaposlenih u ovoj oblasti koje priključuju u samom radu omogućava im i kreaciju adicionalnih servisa u mreži. Dopunjuju i postojeću kritičnu infrastrukturu Interneta kao što je Ipv6, mrežnu bezbednost (CERT kao primer), mobilno peerovanje kao i mnoge druge stvari. Dolazak i povezivanje internet provajdera na Internet Exchange Point-ove se sagledava u više aspekata. Posle investicije dolazi do porasta pristupa Internetu i ova teza je bazirana na nizu istraživanja gde se dolazi do uske korelacije između ekonomskog razvitka i pristupa Internet mreži.

Internet provajderi imaju niže operativne troškove jer je razmena lokalnih podataka daleko jeftinija od IP tranzita. Samim tim, krajnji korisnici plaćaju manju pretplatu internet provajderima. Rezultat smanjenja troškova dovodi do veće kupovina kompjuterskog hardvera i softvera zbog veće iskorišćenosti. Podatak koji je dobijen iz studije u Južnoj Americi je da je ušteda zbog korišćenja IXP-eva u 2013. godini bila 915\$ miliona dolara (Telecom Advisory Services 2013.)

4.1 Tehničke karakteristike i analiza

Internet exchange Point (IXP) je infrastruktura koju koriste Internet provajderi (ISP) za razmenjivanje saobraća između njihovih autonomnih sistema (AS). IXP omogućava internet provajderu interkonekciju sa AS-ovima direktno, tj uspostavljanje direktne veze između njih, kao alternativa korišćenju third-party mreža. IXP igraju krucijalnu ulogu u razvoju Interneta, jer kreiranjem guste mreže interkonekcija po niskoj ceni ohrabruju Internet provajdere da koriste ovu metodu. Neki od provajdera poseduju protok od nekoliko Tbit/s i smatraju se najvažnijim članicama današnjeg Interneta[9].

Opšte je prihvaćeno da je peerovanje na IXP vrlo korisno, gledano sa strane performansi. Na primer, kraći putevi poboljšavaju kašnjenje povratnog puta (Round-trip) i lokalizaciju samog saobraćaja. Međutim, zbog malog broja literature i studija nije posebno naglašeno kolika je ušteda u ceni i performansama prilikom upotrebe IXP-a. Neki od eksperimenata koji su sprovedeni na Italijanskom IXP-u će pokazati koliko je zapravo poboljšanje prilikom upotrebe tačke za razmene podataka.

Nedavne vesti koje ne idu u prilog razvoju IXP-a kao dominantnom načinu umrežavanja interneta su bile da nekoliko velikih internet provajdera otkazuju svoje peerovanje na IXP (De-peering). Svoju odluku su opravdali sa informacijama da mogu efikasnije da upravljaju IP saobraćajem i kvalitetom servisa (QoS).

Studija će pokazati koliko je IXP efektivan u obezbeđivanju da Internet saobraćaj ostane lokalnog karakter tako što će se proveriti preko kojih zemalja je putovala konekcija. Pretohodna stavka je vrlo važna za mnoge države zbog sigurnosti informacija

Kao što je rečeno, studija je fokusirana na Italiju gde se nalaze izvorni AS i ciljni AS koji su i cilj merenja. Najviše je pažnje obraćeno na dva najpopularnija Italijanska IXP-eva: Milanski Internet Exchange (MIX) i Nautilus Mediterranean Exchange Point (NaMeX). U okviru studije je takođe uključeno i tri IXP-a srednje veličine zbog aktivne kontrole BGP „objava“ i prisiljavanja Internet saobraćaja da uzima druge rute za pravilno upoređivanje. Eksperiment se bazirao na merenjima mrežne metrike: vreme povratnog puta (RTT), broj skokova, gubici u paketima itd. Za ovaj sistem merenja je korišćen RIPE Atlas, koristeći sonde koje su isključivo locirane u Italiji kojih trenutno broji oko 150.

Izvedene su dve vrste eksperimenata koje su nazvane, respektivno, Kritični Internet Servisi (CIS) i Selektivne BGP Objave (SBA)[16].

Kritični Internet Servisi (CIS)

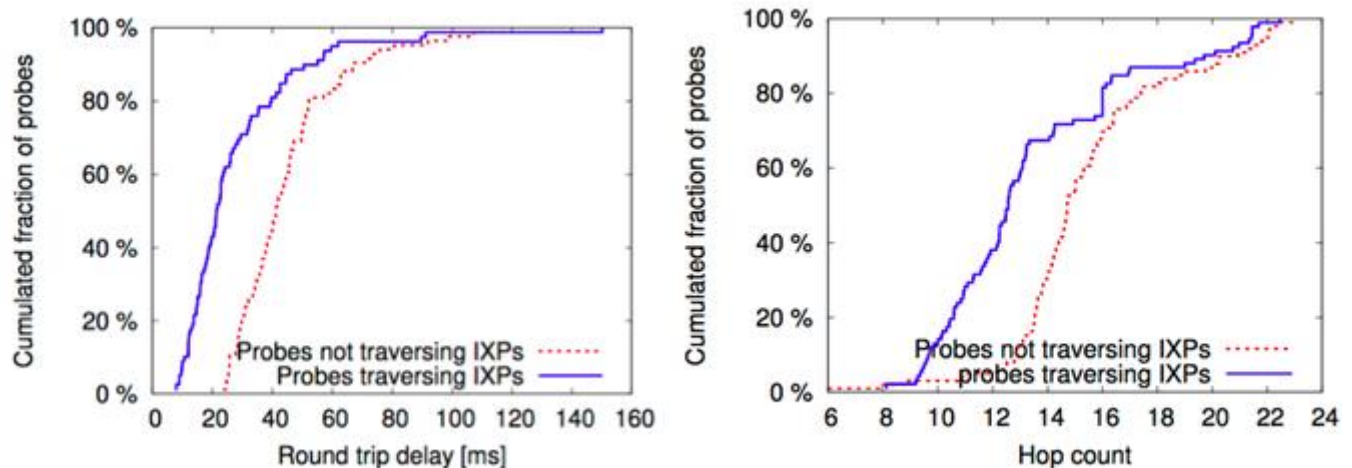
U prvom eksperimentu mrežni eksperimenti su isprojektovani u cilju mogućeg uvida u QoS povezanog sa kritičnim web sajtovima za italijanske klijente. Koncept je bio da se pribavi klasifikacija rezultata u skladu sa razlikom da li je klijent povezan na IXP ili nije. Odabrani su dva seta Internet web stranica koje se mogu smatrati za najznačajnije među italijanskim korisnicima. Prva grupa web sajtova, koja su nazvani „Kritično“ je povezana sa kritičnom infrastrukturom, dok je druga grupa web sajtova „Posećeno“ vezana za popularne sajtove. „Kritično“ se sastoji iz sledećih kategorija: online bankarstvo, osiguravajuće kompanije, javna administracija, webmail provajderi i drugo. Drugi set web sajtova čini 100 najposećenijih italijanskih sajtova prema rangu od strane „Alexa“.

Kritični Internet Servisi (CIS) - Rezultati

Sledeći grafikoni pokazuju RTT za skup podataka od grupe web sajtova „Kritično“, kao i broj skokova za grupu sajtova „Posećeno“. Naziv grafikona je: Kumulativne Distributivne Funkcije (Cumulative Distribution Functions) i pokazuju da za svaku vrednost RTT/Broja skoka, procenat sonde koje imaju istu tu vrednost.

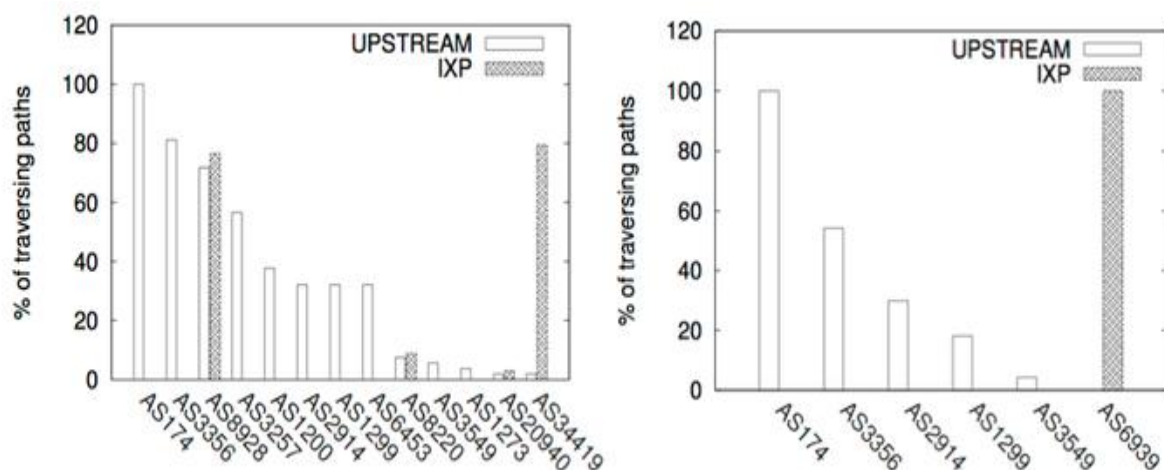
Krive pokazuju da sonde koje putuje preko IXP-eva poseduju bolje indikatore i statistiku. Na primer, RTT za oko 70% sonde koje putuje preko IXP-a iznosi 30ms ili manje, dok samo 20% ima iste performanse za sonde koje ne putuju preko IXP-a.

Konačno, podaci koji su kolektovani u CIS eksperimentu mogu biti analizirani u pogledu bezbednosti kritičnih Web servisa sa njihovim dolaznim Internet saobraćajem. Nedavni slučajevi špijunaže Internet saobraćaja prisililo je vlade da istraže da li je saobraćaj generisan od strane njihovih građana i da li je saobraćaj koji je išao ka kritičnim servisima ostao u potpunosti lokalno duž puta. Jasno je da ako je saobraćaj ostao u zemlji, tj. ako je ostao lokalnog karaktera ne može biti dovoljan garant za bezbednost saobraćaja, ali su vlade vrlo osetljive na ovo pitanje.



RTT za kritične web sajtove (levo) i broj skokova za set najposećenijih sajtova (desno)

Sledeće merenje, koje je izvršeno, je koliko frekventno uz pomoć IXP-a može doći do italijanske destinacije sa lokalnog izvora bez upotrebe tranzita većeg provajdera koji nije iz Italije. Kvantitativno je provereno da li MIX i NaMeX efektivno čuvaju lokalni Internet saobraćaj lokalno.



U skladu sa determinisanjem države gde se nalazi AS kojeg ćemo nazvati X, pitan je RIPEstat servis, koji se bavi Internet merenjima i analizama, za prefikse koje je X objavio i državama čiji ovi prefiksi odgovaraju. Ako su vraćeni prefiksi svi bili asocirani sa istim zemljom, onda možemo da zaključimo da je u tom zemlji lociran X. U drugom slučaju, za određivanje zemlje, potrebno je manuelno uzeti meta podatke iz X, gledajući na primer Web sajt odgovarajućeg provajdera. U većini slučajeva, strani AS se zaobilazi samo kada se upotrebljava ruta većeg provajdera, što potvrđuje koliko je IXP efektivan u prezervaciji lokalnog saobraćaja.

Ovi rezultati se moraju uzeti u obzir vrlo pažljivo zbog 3 razloga:

1. Dva CDF-a su referisana na razjedinjene setove sonde, jer je svaka sonda prošla ili kroz IXP ili ne.

2. RTTovi i brojevi skokova referišu na poslednji skok koji je odgovorio našim merenjima, što vrlo često nije stvarna meta (40/53 za set podataka „Kritično, 59/94 za set podataka „Poseta“).

3. Ruter u IXP-u može odgovoriti na traceroute-u koristeći interfejs koji se ne nalazi na peering LAN-u, što može dovesti do pogrešno zavedene korespondovane traceroute. Podaci sa brojača skokova mogu biti pod uticajem postojanja tunela (primer: transparentnih MPLS tunela).

Konkluzija je da nam grafikoni koje smo naveli da dobijemo prve pozitivne eksperimentalne impresije o uticaju IXP-a. Sledeći eksperiment koji smo izvršili ne sadrži probleme na koje smo ukazali iznad.

Selektivne BGP objave (SBA)

Drugi eksperiment je vezan za analizu alternativnih rutiranja koje uključuje ili IXP ili upstream korišćen od strane italijanskih internet provajdera sa ciljem dolaska na Internet servis. Partnerstvo sa „MC-link“, „Seeweb“ i „Unidata“ internet provajderima, koji spadaju u red provajdera srednje veličine u Italiji je bila preparacija za eksperiment koji je podrazumevao da svakome od navedenih provajdera se dostavlja rezervacija jednog IP subneta i jednog servera sa centrom podataka. Svakom serveru je dodeljena IP adresa koja je proistekla iz rezervisanog IP subneta. Konfiguracija je glasila da tačno rukuje i odgovara zahtevima za ICMP echo sa pingovima i traceroute-ama. Za svakog provajdera se izvršeni opisani koraci u drugačijem vremenskom okviru. Internet provajderi su zamoljeni da naglase predodređenu sekvencu narednih 5 BGP ažuriranja koje se odnose na rezervisane IP subnet-ove. Svako ažuriranje je trajalo 4 sata, sa totalnom sumom od 20 sati po testu. Lista BGP ažuriranja je napravljena sa razlogom selektivnog distribuiranja ruta na različite sub-setove dostupnih ulaza, pridržavajući se šeme:

“UPSTREAM”: objaviti samo ako se prenosi AS-ovi.

“IXPS”: objaviti samo za MIX i NaMeX članove.

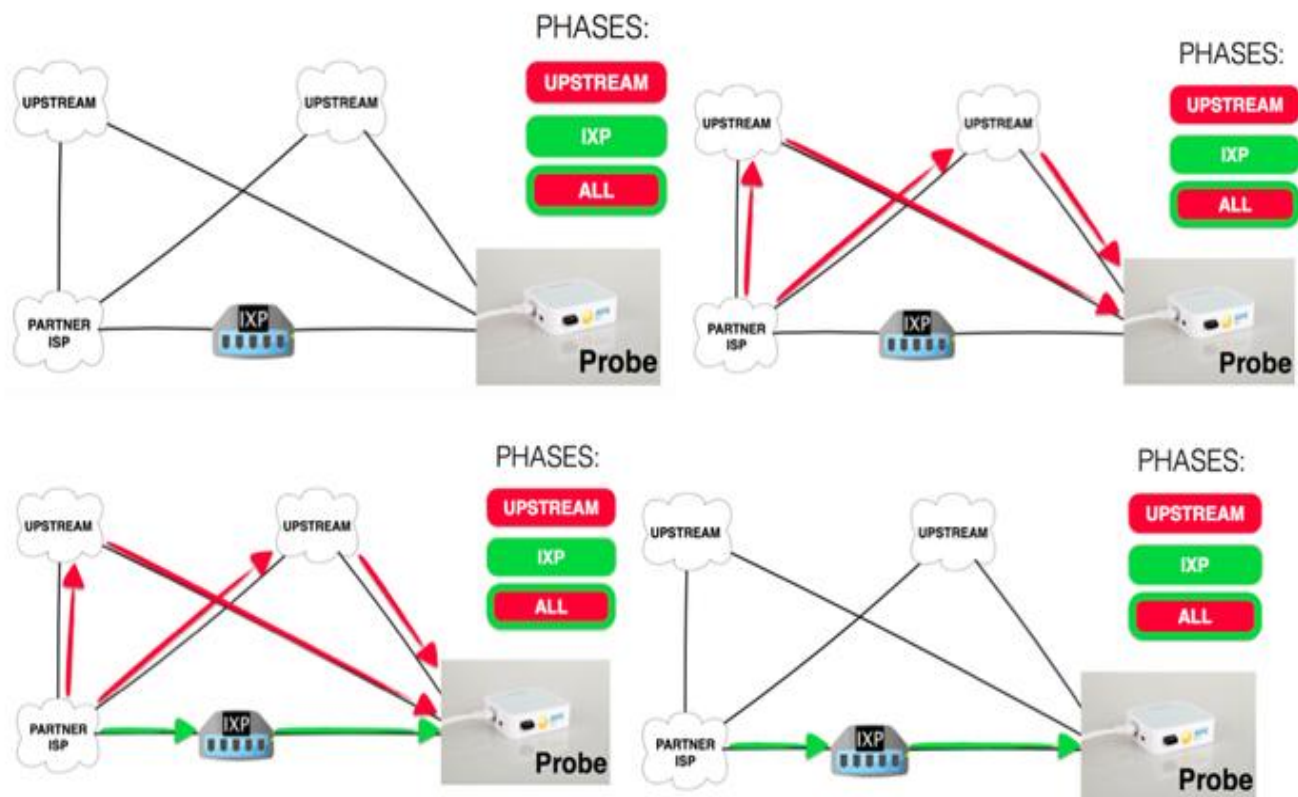
“MIX”: objaviti samo za MIX članove.

“NAMEX”: objaviti samo za NaMeX članove.

“ALL”: objaviti za sve članove.

Faze selektivne BGP objave

Selektivne BGP objave (SBA) – Rezultati:



Za eksperiment SBA, pokrenuli sa odabiranjem sub-setova za sonde koje su mogle da dođu do cilja tokom oba „UPSTREAM“ intervala, i tokom barem jednog „MIX“ i „NAMEX“ intervala. Probe koje su odabrane su nam omogućile da izmerimo razliku izme

Grafici pokazuju zastoј povratnog puta izmeren tokom eksperimenta sa Seeweb-om, broj skokova tokom eksperimenata sa MC-linkom i jitter-a izmerenog u „UniData“-i. Kao primer, prvi grafik se sastoji iz 4 krive koje pokazuju distribuciju prosečnog RTT-a za sve Seeweb mete, u oba slučaja kada je meta pokušavala da se kreće preko IXP-a ili upstream-a. Grafikoni pokazuju da putevi preko IXP-a kao medijuma uvek pokazuju iste ili bolje performanse nego put preko upstream provajdera.

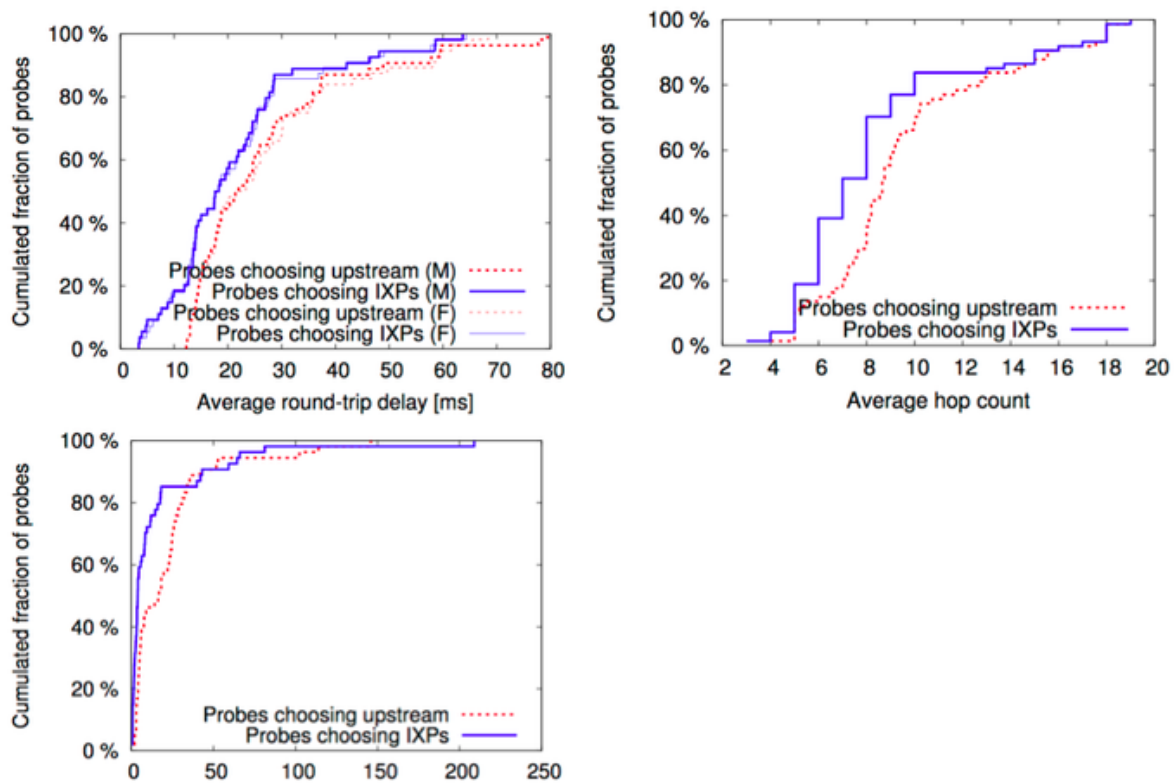
RTT zastoјi tokom eksperimenata sa „Seeweb“-om, broj skokova sa „MC-link“-om i „jitter“ sa „UniDatom,,

Tokom eksperimenta, primetili smo da putanje duž upstreama pokazuju sasvim drugačije vrednosti indikatora performansi. Gledajući prikupljenu traceroutu tokom upstream intervala, otkrili smo rutu za svaku od provajdera i fokusirali analizu za sve njih. Ovo je lista upstream-ova koje smo našli:

MC-link (AS3257, AS12874, AS174, AS3356, AS35612, AS57329)

Seeweb (AS3257, AS174, AS3549, AS3356)

Unidata (AS3257, AS12874, AS16004, AS24796, AS20836)

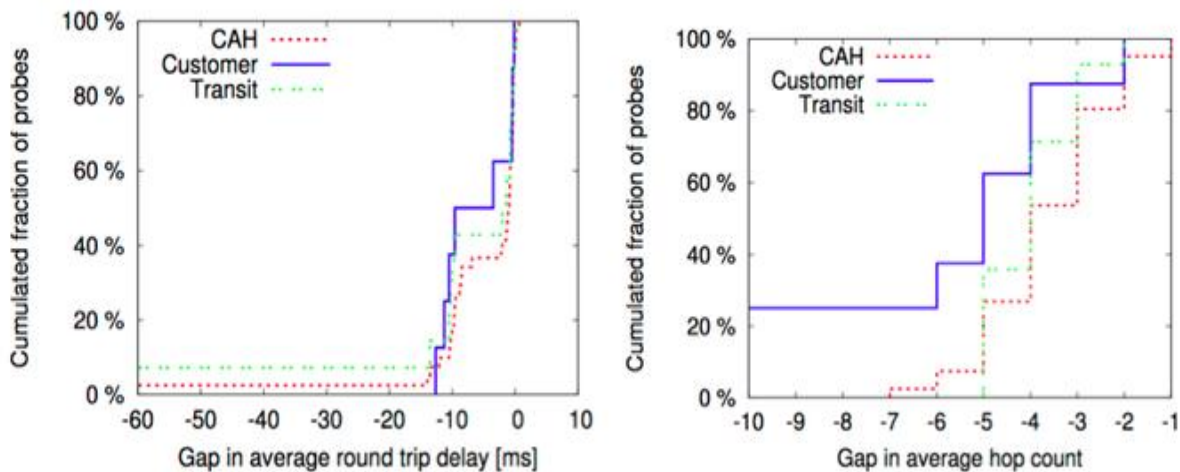


Glavni poređenje IXP-a i upstream-a

AS-ovi su bili raspoređeni u 3 klase:

- 1) Klijenti koji reprezentuje razne organizacije, univerzitete i kompanije itd.
- 2) Tranzitni Internet provajderi koji omogućavaju pristup Internetu i tranzitnim servisima. Krajnji cilj tranzitnih Internet provajdera je da povećaju klijentsku bazu u njihovoj zoni i da smanje troškove korišćenja „upstream“ tranzita pomoću selektivnog peeringa sa ISP-evima.
- 3) Content/Access/Hosting provajderi (CAH) su Internet provajderi koji nude Internet pristup i/ili serverski hosting. Njihovi klijenti su rezidencijalni potrošači ili kompanije bez AS broja, dok su njihovi klijenti za serverski-hosting uglavnom content/service provajderi, takođe bez AS broja.

Sledeća dva grafikona, respektivno, su bazirana na prosečnom RTT i broju skokova koji su se dogodili u SBA eksperimentu na meti Seeseb Milan. Svaki grafikon sadrži tri krive, svaka vezana za jednu AS klasu.



Prosečan RTT (levo) i prosečan broj skokva (desno) za Seeweb Milan tokom SBA eksperimenta

Kriva je CDF koja pokazuje distribuciju performansnih praznina izvedenih iz komparacije indikatora performansi između puteva koji putuju preko IXP-a i puteva koji ih izbegavaju. Klijent je uzet sa klasom manjih mreža i kućnih potrošača. Možemo videti da oni najviše dobijaju od upotrebe IXP-a, tako da se može zaključiti da Internet Exchange Point najviše benefita donose upravo kućnim korisnicima.

4.2 Ekonomoska benefit Internet Exchange Point-a

U ovom odeljku ćemo da obratimo pažnju na mogućnosti ostvarivanja uštede Internet provajdera prilikom pristupanja tačkama razmene Interneta. Pristup IXP-u je atraktivan za provajdera ako je cena razmene saobraćaja lokalno jeftinija od kupovine internacionalnog bandwidth-a (IP tranzita) od strane provajdera višeg ranga za routovanje međunarodnog saobraćaja. Internacionalni bandwidth može da učestvuje u velikoj proporciji u ukupnim troškovima internet provajdera u razvijenim zemljama, tako da se pribegava sve većim upotrebama IXP-eva u datim regionima zbog smanjenja cena, što dovodi do manje cene interneta za krajnjeg korisnika. Finansijska atraktivnost IXP-eva se analizira sa više ulaznih varijabli i faktora. Neki od tih faktora su struktura tržišta i količina lokalnog saobraćaja. Inicijativa za umrežavanjem provajdera postoji ako uzeta teritorija ima dosta saobraćaja koji odlazi van lokalnih okvira jer se time postiže značajna ušteda.

Uzmimo Nemački Internet Exchange (DE-CIX) kao primer za analizu ekonomoske isplativosti. Cena „peerovanja“ je izkalkulisana na osnovu tri poznata parametra. Lokalne,

obližnje i vrlo daleke distance do DE-CIX. Troškovi IP tranzita su procenjeni na 3.50\$ po Mbps i do ovog podatka se došlo kroz razgovore sa više internet provajdera. U troškove „peerovanja“ ulaze i promenljive nadoknade za transport ka IXP-u zavisno od lokacije kao i uobičajenih troškova za 10G port u IXP-u, troškove razmeštaja i amortizaciju rutera.

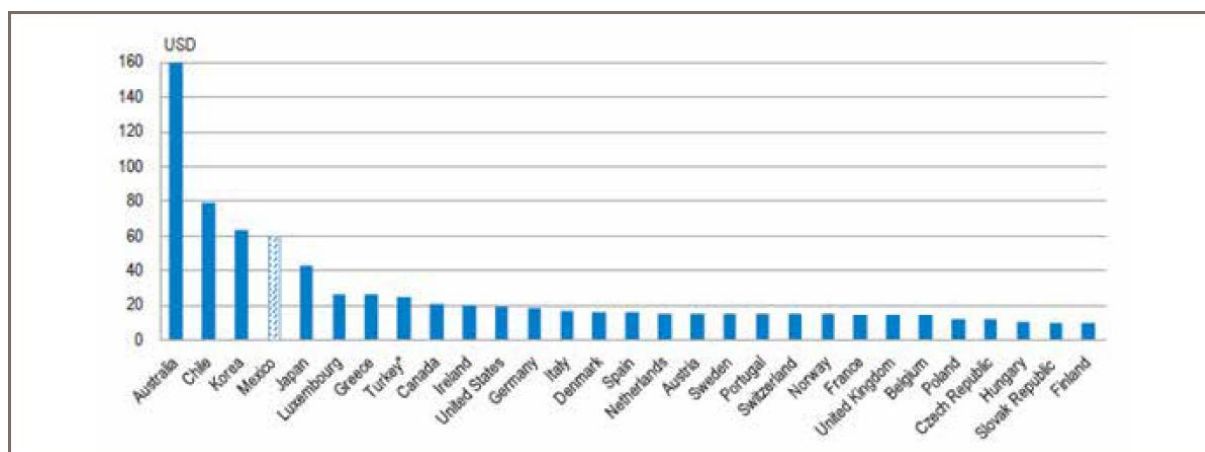
Tabela ispod pokazuje nivo saobraćaja potreban da bi IXP bio jeftinija varijanta od IP tranzita za razne scenarije uzimajući u obzir da je cena IP tranzita 3.50\$ po MbpS. Tačka isplativosti je zavisna od obima i odnosa lokalnog/internacionalnog saobraćaja. Potrebno je dodati da nacionalni fiber kalovi i vodovi koji se nalaze u moru imaju relativno nezavisnu cenu u odnosu na daljinu prenosa, što može uticati na računicu. Dodatno, troškovi „peerovanja“/IXP-a mogu biti dosta niži u razvijenim državama. Tabela će nam pokazati minimalnu cenu upotrebu IXP-a, pod pretpostavkom da je barem 70% 10G portova u upotrebi.

	Far	Near	Local
Transport into IX	\$6,000	\$4,000	\$2,000
Colocation Fees	\$1,000	\$1,000	\$1,000
Peering Fees	\$2,000	\$2,000	\$2,000
Equipment Costs	\$2,000	\$2,000	\$2,000
Total Cost of Peering	\$11,000	\$9,000	\$7,000
IP Transit Price (US\$/Mbps)	\$3.50	\$3.50	\$3.50
Peering Break-even Point (Mbps)	\$3,143	\$2,571	\$2,000
Minimum Cost for Traffic Exchange (US\$/Mbps) (assuming 70% utilization of 10G port)	\$1.57	\$1.29	\$1.00

Tabela troškova IXP-a za DE-CIX

Ključni faktor koji utiče na odluku o pristupanju tački za razmenu podataka je obim saobraćaja. Kako se obim povećava, tako se cena po jedinici smanjuje. Ako internet provajder poseduje dovoljno saobraćaja, onda će peerovanje biti jeftinija opcija nego IP tranzit.

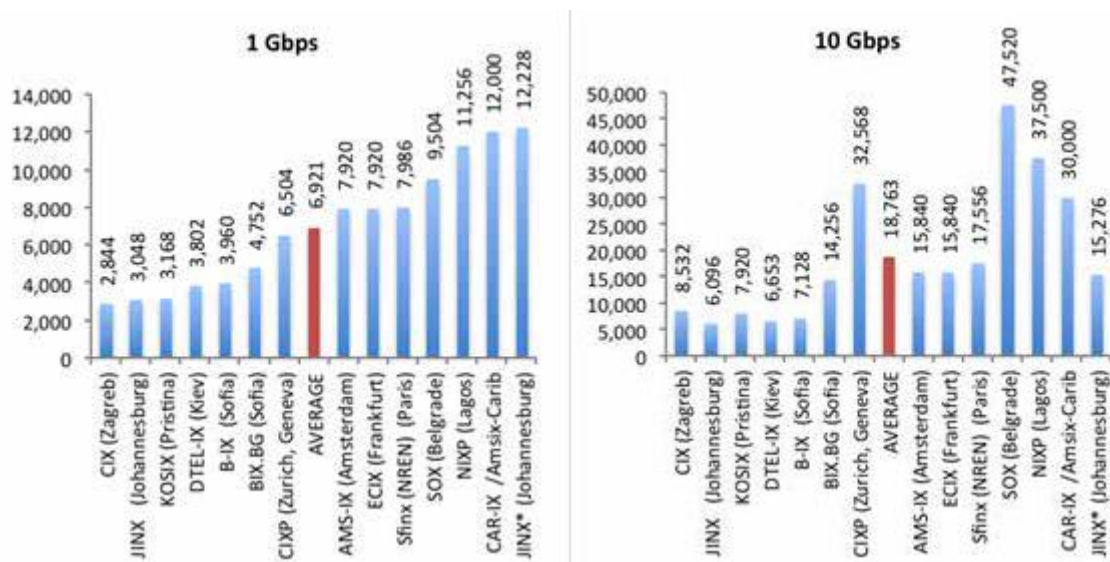
Jedan od parametara za određivanje cene je i geografska pozicija države. Cena IP tranzita je najveća u Australiji zbog udaljenosti od ostatka razvijenog sveta zbog neophodnosti upotrebe morskih vodova kao jedan od razloga.



Grafikon cene IP tranzita u US\$, MpbS/Mesec, 2011.

Bez obzira na institucionalnu instalaciju, čak i IXP-evi koji nisu striktno komercijalni moraju da budu profitabilni da bi mogli da budu funkcionalni. Potrebno je da prihodi budu viši od troškova da bi bilo moguće reinvestirati u mrežu koja je u konstantnom progresu. Servisi koje IXP pruža moraju biti pažljivo procenjeni sa cenom, da bi se obezbedio normalan rad i prirodan rast, pri tome uzimajući u obzir da li se internet provajderima isplati da se pridruže IXP-u kao alternativa troškovima saobraćaja IP tranzita. Operatori tački razmena mogu zaraditi iz plejade varijabilnih i fiksnih troškova. Fiksni troškovi uključuju članarinu na sistem, dok su varijabilni troškovi cena port-a. Poneki operatori zarađuju od pružanja usluga kolokacije, CERT-a i od obezbeđivanja drugih servisa.

Daljim posmatranjem, možemo da vidimo da postoji nekoliko vrsta kapaciteta portova koje IXP-evi nude širom sveta. Manji operatori poseduju funkcionalne portove kapaciteta 10Mbps, dok veći operišu sa kapacitetima do 100Gbps po portu. Cena iznajmljivanja portova raste sa kapacitetom porta, međutim ako se gleda cena koja zavisi „po bitu“ onda dolazimo do konkluzije da su veći portovi značajno jeftiniji. Navešćemo primer 100Gbps porta na Amsterdamskom IXP-u koji košta 10 puta više nego port od 1Gbps. Naplata po Gbps iznosi 64\$ na 100Gbps portu, dok je cena Gbps na portu od 1Gbps jednaka 643\$. Skaliranje je kritično jer marginalni troškovi eksponencijalno opadaju sa porastom u veličini porta.



Troškovi po IXP-evima zavisno od 1Gbps i 100Gbps porta u 2013. godini

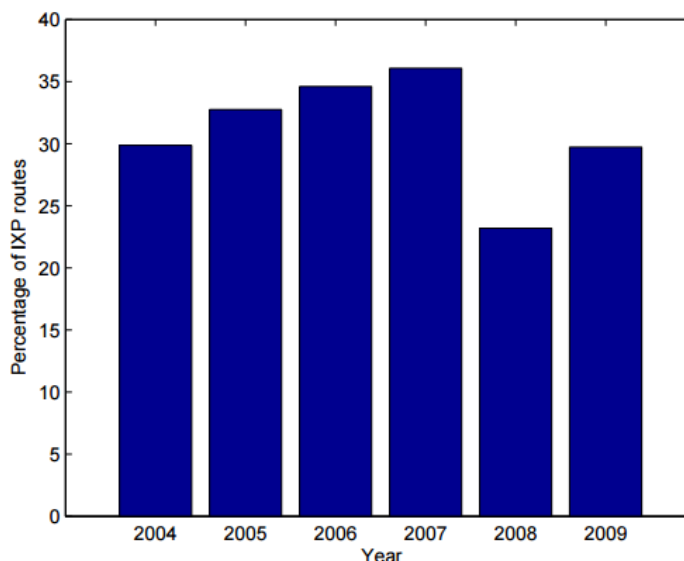
Nivo IXP saobraćaja ne utiče značajno na fiksne i varijabilne cene priključivanja. Tačka razmene podataka u Amsterdamu je najveća koju smo posmatrali u ovom istraživačkom radu i vidimo da cena porta potpada u srednji cenovni rang. Kao što možemo videti i sa grafikona, prosečna cena 1Gbps porta iznosi 6.921\$ godišnje, dok je cena 100Gbps porta 18.763\$ među posmatranim IXP-evima.

Deprecijacija je jedan od najznačajnijih troškova koje IXP operator mora imati u vidu. Uzimajući u obzir tehnološki razvoj, kritično je obezbediti dovoljno fondova za investiciju u hardver, softver i servise. Procene kapitalnih troškova za pokretanje IXP-a variraju. Olakšavajuća okolnost je da organizacije kao što su Cisco, Internet society, Network Startup Resource Center (NSRC) i PCH često doniraju opremu prilikom inicijalnog starta tačke, kao i pri prelaska na viši stepen funkcionisanja. Prilikom istraživanja, procena je da inicijalna investicija iznosi između 40.000-100.000\$ za kreiranje IXP-a. Iznos koji se pokazao da se vrlo brzo vraća investitorima ako postoji dovoljan saobraćaj u tački.

4.3 Trend rasta Internet Exchange Point-a

Sve veći broj IXP-eva je prisutan širom sveta koji obezbeđuje efikasniji transport saobraćaja preko Inreneta. Kriva rasta IXP-eva je direktno zavisna od geografske lokacije gde se instalira nova tačna za razmenu podataka. Podatak koji zastupa ovu tezu je da postoji dosta veći broj tačaka u Evropi i Severnoj Americi nego u Aziji i Africi.

Nema sumnje da sa većim brojem uspostavljenih IXP-eva i sa sve umreženijim internet provajderima, saobraćaj koji se reguliše preko tačaka je svake godine značajno veći.



Procenat vidljivih IXP ruta u jednom ciklusu Skitter traceroute-a svakog septembra

Za studiozno pristupanje uticaju IXP rutiranja, moramo kvantifikovati procenat ruta koje prolaze kroz IXP do Interneta. Za potrebe istraživanja, uzeli smo „traceroute“ (tragač ruta) podatke od Skittera za period od 2004 do 2009 godine[5]. Naglasićemo da je Skitter promenio naziv i da je sada poznat pod nazivom Ark. Kompletan ciklus podataka reprezentuje drugačije tačke za Skitter širom planete koje šalje sonde za traganje ruta na standardnu listu destinacija CAIDA gde se zabeležava svaki put kojim prolazi sonda.

Bazirano na dostupnoj listi IXP prefiksa koji je uzet od PCH-a i PeeringDB-a, zadatak istraživanja je traganje za rutama koje poseduje hops-e (skokove) među ovim prefiksima. Zaključujemo da je IXP ruta definisana kao ruta koja se sastoji od barem jednog skoka kroz mrežu sa poznatim IXP prefiksom. Za procenu stanja je potrebno brojati broj IXP ruta preuzetih iz jednog ciklusa i izračunati ukupan broj rutiranja na internetu.

Sa slike se vidi procenat rutiranja preko tačaka za razmenu podataka, gde se dolazi do podatka da ukupno 30% internet saobraćaja funkcioniše preko IXP-eva, osim u 2008. godini gde je primetan pad zbog početka transformacije CAIDA Skitter arhitekture, gde je bio cilj promena na Ark arhitekturu. Rezultat promene je bio da je manje sondi bilo poslato u mrežu pa je samim tim i broj rutiranja bio manji. Međutim, iz drugih izvora zaključujemo da je rast IXP-eva linearan i u sledećim godinama se može očekivati eksponencijalni razvitak, što možemo videti u slici ispod.

Region	Internet Exchange Points			
	Feb 2016	Feb 2017	Net Change	Percent Change
Europe	136	175	+39	+29%
North America	81	94	+13	+16%
Asia-Pacific	75	92	+17	+23%
Latin America	45	72	+27	+60%
Africa	30	42	+12	+40%

Rast protoka saobraća duž IXP-eva po regionama

4.4 Evropski i Američki modeli IXP-a

Evropski IXP Model

Evropski IXP Model poseduje sledeće karakteristike:

- Evropska peering zajednica sa ponosom ističe da su evropski IXPevi neutralni i u pogledu kolokacije i nosioca, što znači da učesnici u Evropi mogu da izaberu koji od potencijalnih kolokacionih provajdera nudi najbolju kombinaciju usluga i cena koje su im potrebne.

- Evropski IXP najčešće nemaju korisnike već članove. Često su oformljene u vidu neprofitnih organizacija (44%) osnovani od strane članova koji su najčešće i prvi IXPevi koji se zakače. Drugi najčešći oblik evropskih IXP organizacija je usluge koje nude akademske organizacije ili organizacije za regionalni razvoj (42%). U oba slučaja, fokus je na pružanju zajedničke vrednosti, podela troškova i postojanje nekog oblika nadgledanja od strane zajednice nad tome što zajednica smatra za svoju organizaciju.

- Evropski IXPevi predvode u pogledu količine javnog peering saobraćaja. Ovi momci su na okosnici i imaju preko 1 Tbps peering saobraćaja.

- Evropski provajderi koalkacije ne dobijaju prihod od kros – konekcija. U ranijim danima, ISPevi su mogli da sprovedu svoje sopstvene unutar - građene kros – konekcije. U

Evropi su 2011. godine Kros – konekcije uglavnom bile jeftine i predstavljale su jednorodne troškove.

- Cene u Evropi za IXP servise uglavnom se formiraju po metodi količine troškova. Ova metoda se koristi u neprofitabilnim formama poslovanja; ako neprofitna organizacija zaradi suviše profita, njen status neprofitne organizacije je ugrožen. Kako trošak peeringa opada, tako je lakše ostalima da opravdaju pridruživanje IXPu, na taj način uvećavaju uštede a istovremeno operateri još više smanjuju cene.

- Kod evropskih IXPeva postoji duga istorija razmene operativnih podataka, trendova rasta, dodatnih usluga, cenovnika, saobraćajnih statistika i statusa korisnika na javnim internet forumima kao što su RIPE, APPRICOT I NANOG.

Ova struktura IXPeva se dokazala istovremeno kao blagoslov i kao kletva. Pomaže u napredovanju IXPa i povećava broj korisnika; pošto osnivači podjednako dele benefirije i troškove, svi oni mogu da vrše pritisak da dovedu dodatne ISPeve u njihov IXP. Ali model “isti cenovnici za celu stukturtru” takođe ograničava korišćenje diskriminatornog određivanja cena koji bi mogao da se koristi da se privuku strateški važne peerove[11]. Ova mogućnost da se obore troškovi peerovanja za bitne ključne peerove je naročito bitna prilikom ranih dana još pre nego što IXP dođe do kritične mase, I vrednost peerovanja je manja nego cene peerovanja.

Američki IXP Model

IXPevi u Americi su najčešće komercijalni i profitabilni. Vode ih kolokacione kompanije koje ih hostuju..

Američki IXP model čini nekoliko karakteristika:

- *Komercijalne IXP kompanije generalno imaju mogućnost da primene diskriminatorne cene kako bi privukli prave igrače, što znači američki IXP može da ponudi besplatni kolokacioni prostor , besplatne switch portove, popuste za kros – konekcije i ostalo za IXPeve koji će pomoći da se dovedu ostali IXPevi u tu strukturu.

- *U Americi se cena određuje po tržišnom modelu. Ovaj model se ogleda na komercijalnoj to jest profitabilnoj formi američkog IXP poslovanja. Profitabilni poslovi teže ka tome da maksimiziraju vrednosti deonice. Rezultat toga je da se američke tačke razmene imaju dosta drugačije cene od evropskih, čije su cene zasnovane na modelu visine troškova.

- *Fokus unutar američkih IXPeva teži ka aktivnostima koje generišu prihode. I ako postoji dosta peeringa, motivisan je generisanjem prihoda.

- *Američki IXPevi imaju korisnike, ne članove. Korisnici plaćaju a ne glasaju. Odluke donosi komercijalni IXP operater a ne zajednica. Izuzetak za pravilo je kada korisnici insistiraju različiti IXPevi rade zajedno.

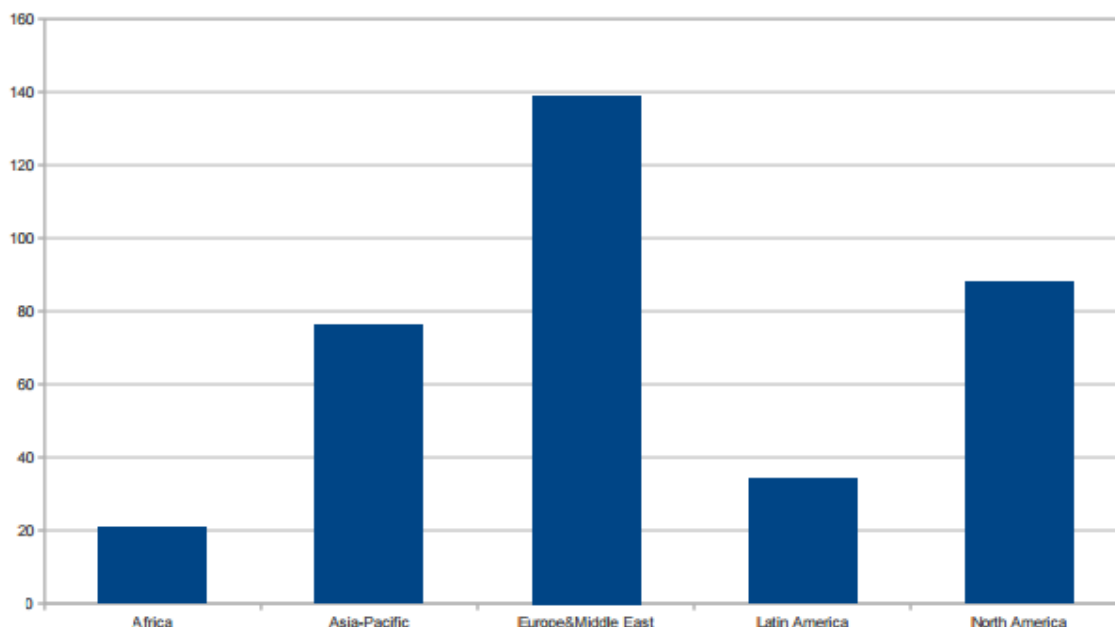
*Količina američkog javnog IXP peering saobraćaja je dosta manja. U Americi postoji mnogo više privatnog peering nego javnog.

4.5 Analiza postojećih Internet Exchange Point-ova

Kao što je prikazano u donjoj tablici, sada je operativno više od 350 IXP. Vodeća je SAD , sa oko 86 IXP-a. Ostale zemlje s više od 10 IXPs su: Australija (11), Brazil (19), Francuska (15), Njemačka (14), Japan (16), Rusija (14), Švedska (12) i Velika Britanija (12).

Kao što se može videti iz ovog popisa, to su uglavnom veće i više gušće naseljene zemlje sa kvalitetnom Internet infrastrukturom, iako postoje neki značajni izostanci na popisu, kao što su Kanada, Kina, Indija i Španija. Uopšteno govoreći potrebno je da bar jedan IXP bude uspostavljen i bude operativan u svakoj zemlji, međutim samo 91 zemlja do sada su uspostavile operativne IXP-eve. Kao što bi se očekivalo zemlje u razvoju zaostaju za ostatkom sveta u uspostavljanju IXP. Afrika je područje s najmanje IXP (samo 21 od 53 zemlje u Africi poseduju ovu tehnologiju danas).

Što se tiče veličine mreža danas se može govoriti o 23 IXP centara sa više od 100 članova u mreži. Oni se u velikoj meri nalaze u Zapadnoj Europi i Severnoj Americi, iako neki od najvećih IXP takođe postoje u nekim gradovima drugih regijama, kao što su: Kejptaun, Hong Kong, Moskva, Sao Paulo, Sidnej, Tokio, i Varšava.



Zastupljenost IXP-eva po kontinentima

U okviru ovog master rada, izvešćemo studiju slučaja u dva najveća IXP-a u Africi, kao i Londonskog Internet Exchange Point-a (LINX) i Serbian Exchange Point-a (SOX). Cilj nam je da pokažemo kako funkcionišu u razvijenim zemljama i zemljama koje su u razvoju.

Nigerijski IXP (IXPN)

„Nigerian Internet Exchange“ (IXPN) koji se nalazi u Nigeriji je počeo sa radom izvan prestonice, u gradu koji se zove Ibadan 2003. godine. Iniciranje je počelo kada su se dva prvobitna člana povezali na 10/100Mbita Ethernet prekidača i na route server. Maksimalni zabeleženi saobraćaj između dva člana, tj dva internet operatera je bio 100Kbit/s. Rane 2005. godine, asocijacija internet provajdera Nigerije (ISPAN) je počela diskusiju na kreiranju IXP-a u Lagosu, glavnom gradu Nigerije. Funkcionisanje bi obezbeđivala asocijacija koja bi postavila nezavisni entitet koji bi regulisao rad. U Novembru te godine, predsednik Nigerije, Olusegun Obasanjo je uspostavio nacionalnu regulatornu jedinicu, Nigerijsku komunikacionu komisiju (NCC) kao garanciju da će Nigerijski nacionalni IXP biti funkcionalan u što kraćem roku. Privremeno upravljačko telo IXPN-a je postavljeno 2007. godine i Nigerijska tačka razmene podataka je pušteno u rad sa 15 inicijalnih članova.

Do danas, broj članova je porastao na 35 i IXP se sastoji od dva operaciona mesta u Lagosu sa dve lokacije u uzamajnoj vezi koje su povezane sa fiber optičkim kablovima. Svaka lokacija poseduje dva „Foundry“ prekidača koji povezuju odvojene peering LAN-ove, gde se obezbeđuje pouzdanost mreže. Primarni peering LAN-a je interpovezan na 1Gbps fiber optičko kolo, dok je sekundarni peering LAN interpovezan na 450 megabitni bežični „backhaul“. Definicija reči „backhaul“ je uzeta iz telekomunikacione mrežne sfera i označava korišćenje komunikacionih sistema za dopremanje podataka od krajnjih korisnika do tačke koja je direktno povezana sa Internetom. Takođe, „wireless backhaul“ može i raditi kao alternativna ruta dopremanja podataka kada je primarni put onemogućen. Na IXPN, dve od tri lokacije poseduju route server. Svi NIX prekidači obezbeđuju 10/100BaseTX prekidački Ethernet i 1000BaseSX Gigabitni Ethernet preko više modova fiber optičke konekcije. Planovi INXP su da se proširi na obližnje gradove u bliskoj budućnosti. Menadžment Nigerijske tačke za razmenu podataka čine 6 direktora i jedan CEO koji čine bord direktora. Tehnički komitet asistira radu osoblja i savetuje bord direktora sa strane tehničkog aspekta INXP-a.

Kenijski IXP (KIXP)

Drugi primer, KIXP Kenija, je opisan na detaljniji način iz razloga što postoji veći broj dostupnih case-study informacija.

KIXP u Najrobiju podržana je od strane Asocijacije Telekomunikacionih Servis Provajdera Kenije (Telecommunication Service Providers Association of Kenya TESPOK),

profesionalne, neprofitne organizacije koja predstavlja interese ISP-ova i ostalih telekomunikacionih servis provajdera Kenije[4]. Nakon posete radionice „Networking Workshop“ za zemlje u razvoju čiji je domaćin bilo Internet Društvo (Internet Society) (ISOC) u Kaliforniji 1999. , jedan od kenijskih internet inženjera posedovao je znanje kako da dizajnira, podesi i održava IXP. Nakon povratka u Keniju, on je podelio te informacije sa svojim kolegama koji su bili istrajni u nameri da uspostave lokalni IXP. Nakon otprilike godinu dana pripremnih radova, koji su uključivali i dizajn i implementaciju tehničkih operacija, modele finansiranja kao i pravni okvir, KIXP je pokrenut u novembru 2000. godine. KIXP nema zasebnu upravljačku strukturu i politika je uspostavljena preko komiteta Kenijske ISP asocijacije (TESPOK). Neposredno nakon lansiranja KIXP, državni telecom operater, Telkom Kenya, uložio je prigovor zajedno sa nacionalnim telom, Communications Commission of Kenya (CCK), argumentujući da KIXP ugrožava ekskluzivni monopol nad internacionalnim saobraćajem koji obezbeđuje Telkom Kenya. U naredne dve nedelje, CCK zaključuje da je za KIXP potrebna licenca i naređuje gašenje sa objašnjenjem da se radi o ilegalnoj telekomunikacionoj radnji. Kao odgovor na CCK-ovu presudu, slučaj je tada predstavljen Apelacionom sudu za Telekomunikacije (Communications Appeals Tribunal) sa jakim tehničkim argumentima koji su pokazivali da je KIXP samo standard, ethernet van sistema (of-the-shelf Ethernet). Ukoliko je potrebno ugasiti KIXP, onda je potrebno ugasiti i svaku kompjutersku mrežu u zemlji s obzirom da su jednaki po arhitekturi i komponentama. Iako je borba Telkom Kenya bila žestoka, hranjena strahom od gubljenja značajnog dela internacionalnih profita od strane IP saobraćaja, kenijski internet provajderi su tvrdili da je KIXP zatvorena grupa korisnika pa je prema tome i legalna po Zakonu o Telekomunikacijama Kenije. Takođe je istaknuto, da lokalna razmena lokalnog internet saobraćaja ne krši internacionalni monopol Telkom Kenije s obzirom da će kompletan internacionalni saobraćaja i dalje ići preko njihovog internacionalnog linka. Nakon skoro godinu dana intenzivnih napora, pritiska javnosti, pravnih pretnji, TESPOK konačno dobija odobrenje od strane CCK u formi licence u novembru 2001. godine.

Bilo je jasno da je Telekom Kenija pogrešno predstavila situaciju, i s obzirom da je cela stvar postala javna, pokrivena i nacionalnim i internacionalnim medijima, bilo je potrebno naći rešenje da se IXP predstavi javnosti u dobrom svetlu. Doneto je rešenje da se otvori kompanija koja se zove KIXP Limited s obzirom da poseduju licencu od strane CCK. Ovo je učinilo Keniju jedinom zemljom koja ima licencu za IXP. KIXP konačno odlazi u prošlost polovinom februara 2002. godine kada je povezano 5 kenijskih ISP-ova. Tokom 2004. godine, odlučeno je od strane članova TESPOK da se uvedu članarine nakon čeka je KIXP postao restriktivan za sve ISP koji nisu licencirani. Ovo je ubrzalo reviziju članstava koja je podigla restrikcije na članstva i smanjila članarinu za 600%. Trenutna članarina je 20000 KSH (oko 330 dolara) mesečno i trenutno je 25 članova priključenih na KIXP (16 ISP-ova, jedna vladina mreža (Kenya Revenue Authority), jedna mreža obrzovne institucije, jedan ccTLD operater, 3 internet Backbone Gateway operatera, jedna Value Added Telecommunication Services Provider i 2 GSM operatera. Jedan od najvećih problema pri uspostavljanju KIXP bio je u vezi sa tim gde da se postavi. Veliki broj opcija je evaluiran, a uključivale su sledeće:

Telkom Kenya je najbolja opcija s obzirom da je on ovlašćeni nacionalni telekom provajder. Još jedan od razloga koji je išao u prilog Telkom Kenya je bila i činjenica da, pored nacionalnog operatera, svi ostali već imaju linkove za njihove mreže. I dodatno, s obzirom da imaju centralnu lokaciju, korisnicima bi bilo mnogo lakše da obezbede fizičku vezu sa IXP, nevezano sa njihovom lokacijom. Međutim, ova opcija se nije mogla uzeti u obzir jer je Telkom Kenya video IXP kao pretnju za svoj rad i odbio zahtev ISP da bude host KIXP.

Univerzitet Najrobi je bio jedna od opcija kao alternativni host za KIXP najviše zbog dinamičnosti korišćenja računara kao i zbog njegove centralne lokacije. Najveća zabrinutost u vezi ove opcije proistekla je zbog pojave čestih studentskih protesta. Pomenuti problem je eliminisao univerzitet kao mogućnost.

Nekoliko internet provajdera koji su imali kancelarije locirane u Najrobiju, ponudili su da budu host za IXP. Izazovi u ovom slučaju su bili: koji ISP izabрати od dva moguća. Činjenica da su mnogi drugi ISP pokazivali visok nivo nezadovoljstva usled čega bi izostalo poverenje u njih kao kompetitore za održavanje IXP bez dobijanja prednosti.

U cilju osiguravanja prihvatljivosti koncepta IXP u Keniji, od ključne važnosti je bilo naglasiti neutralnost objekta i pridobiti pristanak od strane prospektivnih članova na toj lokaciji. Nakon evaluacije svih opcija bez konačne odluke koja zadovoljava sve potencijalne članove, ideja je bila da se iznajmi prostor neutralnog provajdera čija se zgrada nalazi na odgovarajućoj lokaciji. Odlučeno je da se iznajmi prostor od 1500 kvadratnih metara na najvišem spratu zgrade koja je locirana u centru Najrobija. Najveći minus u ovoj ideji bila je cena iznajmljivanja prostora. Kao svaki drugi tip mrežnih podataka ili komunikacione infrastructure, trošak je pao na dve glavne kategorije: podešavanje i operativni troškovi. Troškovi podešavanja su uključili troškove nabavke opreme za jezgro IXP kao i nameštaj za prostorije gde će IXP biti lociran, sa strujom, klimatizacijom, kabineti sa opremom i obezbeđenjem.

Inicijalna oprema je finansirana od strane Cisco Systems donacije kao i uz pomoć malog granta Departmenta za internacionalni razvoj Ujedinjenog Kraljevstva. Ostali troškovi opremanja su pokriveni od strane TESPOK. S obzirom da prostor za KIXP nije bio besplatan, bilo je potrebno naći način da se pokriju operativni troškovi kao što su renta, struja i osiguranje. Mesečne članarine za sve članove koji bi se uključili na KIXP obuhvatao je i pokrivanje navedenih troškova. Veliki broj različitih tehničkih modela je razmatran za IXP Kenije i odlučeno je da bi trebalo da se bazira na principu istog modela koji je korišćen u Hong Kongu – Internet Exchange – dvoslojni Route Reflector IXP. Kao rezultat bilo je da KIXP zgrada sadrži dva Ethernet switcha velike brzine i da svaki KIXP član poseduje opciju da se poveže na oba. Na ovaj način, ukoliko bi jedan switch bio onemogućen, onaj drugi bi mogao da podrži dalje radnje automatski. Jezgro je suplementisano sa dva route reflector-a – posebno konfigurisani ruteri koji prebacuju logiku rutiranja ka svim članovima u KIXP sve dok svi ruteri ne dobiju isti pogled na mrežu. Ovaj dizajn dozvoljava brzu i jednostavnu politiku implementacije u tački razmene koja je osposobljena da podrži i do 48 mreža. Kapacitet se može povećati i do 200 mreža.

Pre KIXP, sav internet saobraćaj u Keniji bio je razmenjivan na internacionalnom nivou. Ugrubo oko 30% dolaznog saobraćaja bila je ka domaćim destinacijama. Internacionalni protok je u tom trenutku koštao oko 5000 dolara po megabajtu dok je cena lokalnog transfera bila oko 500 do 1000 dolara. Za vreme prve dve nedelje rada KIXP, merenja su pokazala da je latenca redukovana sa prosečnih 1200-2000 milisekunde (putem satelita) na 60-80 milisekunde (putem KIXP). Lokalni saobraćaj je takođe unapređen u poređenju sa 2007. godinom usled povećanja lokalnog sadržaja od digitalizacije nekoliko vladinih servisa i dolazak internacionalnih kompanija, kao što je Google koji sada hostuje njihove servise lokalno.

Celokupan Google saobraćaj (pretrage, mailovi, mape, aplikacije i dokumenti), ide preko KIXP. ISP jedino plaćaju za lokalni saobraćaj i Google plaća za kapacitet od Kenije do njihove mreže u Americi. Usled ograničenog kapaciteta ovlašćenog nacionalnog telekom operatera, većina internet servis provajdera je prešlo na fiber vlakno za povezivanje sa KIXP, što znači da oni imaju veze od velikog broja megabajta po sekundi u okviru razmene. KIXP je implementirao lokalne instance internet F i J root servisa u dodatku na lokalni .com i .net “resolution” servise. Kao rezultat, lokalno organizovan “lookup” zahtev za ove servise nije više imao potrebu da prenosi internacionalne linkove kao odgovor. U 2005. godini, Kenijski mrežni informacioni centar (KENIC) je u liniji sa svojim mandatom počeo da promovise Internet u Keniji i jedna od prvih mera je postavljanje NTP Servera u KIXP-u sa GPS postavkama za integraciju datuma i vremena u kompjuterima. Većina servisnih provajdera su implementirali vremensku sinhronizaciju na svojim sistemima uzimajući kao parameter serversko vreme u drugim zemljama u okruženju. Međutim sinhronizacija nije prenet na krajnje klijente zbog nepouzdanosti konekcije i visokih troškova vezanih za internacionalne linkove. Jedan broj organizacija je koristilo lokalni NTP servis i u te organizacije su spadale vladine agencije, banke, velike državne kompanije i edukacionalne institucije.

Operativan ugovor KIXP-a sa svojim članovima se naziva „Mandatory Multilateral Peering Agreement“, ili skraćeno MLPA koji podrazumeva da je svaki član spojen sa svim ostalim članovima. Trenutno saobraćaj na Kenijskoj tački za razmenu podataka dostiže maksimalno 1Gbps. KIXP objavljuje detaljne informacije o iskorišćenosti interneta i podaci nam daju na uvid da je maksimalna vrednost internet saobraćaja u toku radnog vremena. Izveštaji ove prirode su bitni za operatore IXP-a i internet provajdere da bi mogli da prilagode svoju mrežu za normalno funkcionisanje bez smetnji čak i tokom pikova saobraćaja.

Londonski IXP (LINX)

Londonski Internet Exchange (LINX) je jedan od najvećih svetskih i najduže uspostavljenih centara za razmenu Interneta. Zajednički je u vlasništvu asocijacije čiji su članovi Internet provajderi (ISP). LINX trenutno ima 399 članova u 51 državi, od kojih je većina iz Evrope. Međutim, zbog rasta samog IXP-a veliki broj dolazi iz Severne Amerike, Afrike, Bliskog Istoka, Azije i Okeanije. Prvobitno sama arhitektura je bila zamišljena da članovi mogu biti isključivo ISP-evi, međutim kasnije je restrikcija olabavljena i danas je

veliki opseg mreža priključen na LINX, uključujući i velike kompanije kao što su Google, Yahoo i BBC. Diverzitet servisnih provajdera priključenih na LINX se povećava sa ulaskom specijalista iz kompjuterskih i kockarskih igara, specijalista za ublažavanje DDoS napada, marketing kompanija i mnogih drugih. LINX mreža se sastoji od dve odvojene Ethernet switch platforme koje su locirane na preko 10 mesta duž Velike Britanije. Trenutno je povezano preko 890 portova sa članovima, gde oko 450 članova koristi 10GigE portove sa 1.2TB/s u piku saobraćaja. Za obezbeđivanje redundantne konekcije, korišćeni su barem dva switcha od različitih proizvođača međusobno povezani 10 gigabajtnim Ethernet mrežnim kolima. Za kablove je korišćen optički kabl, i pri tome su kreirana dva odvojena prstena. Fizička obezbeđenost mreže je ostvarena upotrebom različitih puteva gde je to moguće. LINX ne poseduje nijednu od lokacija koje su nabrojane. Svaku od lokacija koju Londonska tačka za razmenu podataka koristi je iznajmljena ili je napravljena forma nepotpunog vlasništva. Menadžment logičke redundanse mreže je održavan od strane mehanizma zaštite baziranog na rapidnoj promeni (EAPS ili MRP). U slučaju gubitka mrežnog segmenta, aktivira se redundantna konekcija u roku od par milisekundi, i time se ponovo uspostavlja konekcija.

Brazilski IXP

Brazil ima veliki broj IXP-a, što je rezultat snažne podrške vlade u kombinaciji sa efikasnom agencijom koja je odgovorna za upravljanje internetom u Brazilu, Comitê Gestor da Internet no Brasil (CGI.br).

CDI ima pristup sredstvima iz registracije .br domena i ima pravni status kao agencija nadležna za promovisanje razvoja Interneta u Brazilu sa predstavnicima iz vlade, privatnog sektora i civilnog društva.

Do 2003. godine, samo tri grada su imali operativni IXP. Skoro 20 gradova u Brazilu imaju više od milion ljudi, tako da je bilo mnogo lokalnog saobraćaja, što je negativno uticalo na troškove i kvalitet usluga. U 2004. godini, CDI pokrenuo je inicijativu da se stvori više IXP-a, poznate kao Ponto de Troca de Tráfego (PTT), u gradovima širom zemlje. Oni su osnovani u saradnji sa različitim mrežnim operaterima (od univerziteta do velikih internet i telekom provajdera).

CGI je odgovoran za administriranje mreže, dok NIC.br obezbeđuje opremu i upravljanje. Ova strategija je pomogla da se smanje troškovi podešavanja i transporta za manje IXP-jeve dok i dalje pružaju neutralnu platformu za razmenu saobraćaja sa većim mrežnim operaterima.

Broj IXP-a je porastao od četiri na 19 između 2006. i 2010. godine i danas ih ukupno ima 24 na različitim lokacijama, koji pokriva 16 od Brazilu 26 država, sa prometom saobraćaja koji dostiže do oko 250Gbps. Naknade se obično ne naplaćuju na učesnika na ovim berzama.

5. Pokretanje novog IXP-a

Nije moguće definisati određeni skup instrukcija za pokretanje IXP; svaki novi IXP suoči će se sa različitim izazovima i radi će pod različitim ekonomskim, tehničkim i pravnim okolnostima.

Pitanja koja treba postaviti pre početka:

- Da li postoji potreba za novim IXP?
- Da li su korisnici spremni za povezivanje i da plate?
- Koja organizacija treba biti postavljena za vođenje IXP-a?
- Kako započeti IXP sa malo ili nimalo novca i rasporedi snažan infrastruktura prvog dana?
- Koje usluge treba voditi?
- Ljudski resursi potrebni za upravljanje ikp?
- Kako da budemo sigurni da će IXP trajati?
- Kako se širiti i dovoditi nove korisnike?

5.1 Izazovi na početku

Najteži deo sa uspostavljanjem IXP-a nije tehnički deo, nego izgradnja zajednice i poverenje.

Takođe, IXP mora biti održiv nakon faze uspostavljanja. Ovo uključuje da ima dovoljno sredstava za rad i unapredjivanje opreme u budućnosti, razvojem tehnologije i rasta saobraćaja. Članovi plaćaju naknadu na osnovu njihove veličine porta , tako da jedna taksa za 1GE port i jedan za 10GE porta. Ovo se ne zasniva na stvarnom saobraćaju, vec na brzini porta.

Novi IXP-jevi su skloni da veruju da je to dobra ideja da ponude besplatne priključke članovima sa velikim sadržajem mrežama kako bi privukli druge članove. Na prvi pogled, ovo možda izgleda kao dobra ideja, ali brzo će se naći stisnuti između vlasnika velikog mrežnog sadržaja i broadband operatera, koji takođe žele svoje port besplatno.

Generalno, bolje je jednako naplatiti i tretira sve jednako. To može učiniti malo teže da IXP krene, ali svakako čini održavanje IXP lakše na duge staze. Većina vlasnika velikih sadržaja takođe podržavaju nove IXP-jeve koji se formiraju u mestima ili regionima u kojima ne postoji IXP.

5.2 Institucionalni i operativni modeli za IXP

Usvojeni su razni institucionalnih modela za rad IXP. Oni spadaju u četiri kategorije:

- Neprofitne industrije udruženja ISP-a
- Operator-neutralne, komercijalne i za-profit preduzeća
- Univerzitetska i vladine agencije
- Neformalne udruženja mreža

Većina evropskih IXP-jeva je izraslo iz nekomercijalnih orgnizacija, kao što su istraživačke organizacije .

Većina afričkih IXP-jeva je osnovano od strane ISP udruženja i univerziteta.

U Sjedinjenim Američkim Državama većina IXP-jeva su komercijalni, a neki komercijalni IXP su se pojavili i u Evropi

IXP Neutralnost:

Mnogi ISP-ovi su izrazili snažna osećanja o značaju neutralnosti IXP-jeva, a većina velikih evropskih IXP-jeva pripisuju svoje uspehe svojoj neutralnosti.

Vlasništvo:

Neutralnost bi mogla biti ugrožena ako ISP član poseduje delove (kao što su oprema, itd) IXP opreme i stiče ih preko druge organizacije.

Mnogi IXP su početi sa donacijama opreme, rack prostora, radnika i druge pomoći - to je deo kooperativne prirode većine početnih IXP. U slučaju donacija, sa sponzorima treba staviti u pisanoj formi prirodu sporazuma za IXP za korišćenje opreme.

5.3 Lokacija

Pored stvaranja zajednice koja će da podrži IXP, drugi važan faktor za uspostavljanje uspešnog IXP-a je njegova lokacija.

Pronalaženje adekvatne lokacije koja je neutralana i jeftina je veoma bitno. Prilikom razmatranja mogućih lokacija, sledeći elementi treba da budu uzeti u račun: prostor, kontrola životne sredine, bezbednost, pouzdanost i redundantno napajanje, pristup zemaljske infrastrukture, kablova, i podrška.

Odlučivanje o lokaciji verovatno će obuhvatiti procenu postojećih objekata koji se mogu koristiti, a zatim u odnosu na potencijalne opcije lokacije na troškove i trud koji su uključeni u formiranje novog samostalnog objekta. U mnogim zemljama, troškovi u vezi sa zakupom prostora, finansijskim sredstvima i platama osoblja mogu biti visoki.

Pored lakšeg pristupa infrastrukturi, data centar takođe treba da obezbedi stabilno napajanje koje vam je potrebno kako bi se osiguralo da imate UPS-eve (Uninterruptible Power Supply) i možda čak i aggregate.

Takođe, proverite da li postoji prostor za rast IXP. Možda počnete samo sa dva Rack-a (ormana), ali ako je IXP uspešan možda će biti potrebno više, a pomeranje IXP je uvek teško.

5.4 IXP Oprema i Usluge

- **Ethernet Switch (Obavezno)**
 - Jezgro svakog IXP-a je Ethernet Switch
 - Ulaganje u opremu koja je najbolja i najviše može da se proširi ako finansije dozvoljavaju.
 - Imati 2 switch-a je uvek dobro, ako to sredstva mogu da dozvole.
- **Adresni prostor (Obavezno)**
 - IXP će zahtevati IP adresni prostor za Peering
- **Route Server (Opciono)**
 - Tokom početnih faza podešavanja, route server obezbeđuje lakoću konfiguracije novih članova
- **Web i Mail Serveri (Opciono)**
- **Transit Router (Opciono)**
- **Route Collector (Opciono)**
 - Takođe se naziva 'looking glass' koji pomaže članovima IXP-a prilikom rešavanja problema. Može se koristiti za prikupljanja ruta za merenja.

Postoji veliki broj osnovnih usluga koje IXP može da ponuditi svojim članovima izvan zajedničkog povezivanja. Ove usluge se razlikuju kod svakog IXP-a i ni na koji način se ne takmiče sa svojim članovima.

Pružaoци drugih usluga, koje nisu mrežni operatori, mogu se povezati u IXP, uključujući i:

- pružaoci keša sadržaja (CDN),

- DNS root serveri,
- country code top-level domain (ccTLD) name server instances,
- vremenski serveri ,
- Looking Glass ili Routeview serveri.

Davaoci ostalih usluga mogu biti privatna preduzeća, nevladine organizacije (NVO), vladine mreže, ili sama IXP operater. Kao i mrežnih operatera, davaoci drugih usluga moraju da instalira i održava svoju opremu u IXP-u i moraju da podržavaju svoje usluge.

5.5 Osoblje IXP-a

Koliko zaposlenih je potrebno jednom IXP-u ?

- 1 do 3 finansijski je održivo (čak i na početku)
 - Nemogućnost da se nadzire 24/7 NOC
 - IXP više zavisi od opreme nego što zavisi od ljudi
- 5+ finansijski održivo samo ako je IXP posobna za pružanje više usluga
 - Sposobnost da se održi kvalitet u korisnička podrška i brzo reakciono vreme u hitnim slučajevima (24/7 NOC)

5.6 IXP Website

U većini slučajeva IXP web strana je njegov prvi kontakt i referentna tačka za sve zainteresovane stranke.

Oni koji dolaze na sajt IXP-a spadaju pod 4 kategorije:

1. Potencijalni IXP učesnici
2. Trenutni IXP članovi
3. Javnost
4. IXP osoblje

Potencijalni IXP učesnici

Najvažnije ciljna grupa. Većina IXP-a je u potrazi za povećanjem njihovog IXP-a sticanjem dodatnih i vrednih učesnika.

Važne informacije za ovu grupu je:

- Ko su sadašnji učesnici IXP-a?
- Iznos saobraćaja koj se razmjenjuje na IXP-u
- Tehnička podešavanja i pravila
- Troškovi priključka

- Postupak povezivanja
- Kontakt informacije i pitanja

Trenutni IXP članovi

Ova grupa će često posećivati sajt IXP-a i važne informacije za ovu grupu uključuju:

- Peering informacije i alati
- Grafikoni upotrebe, statistika, topologija mreže
- 24h kontakt informacije
- Stalne informacije razvoja na IXP-u (novi članovi, planirano održavanje, tehnički sastanci, itd)

Javnost

Istraživači koji su se zainteresovali za Internet i IXP širom sveta.

U principu, oni traže statistike i kretanja saobraćaja koja se razmjenjuju na IXP-u.

Ostale informacije vezane za IXP kao što je IXP godina osnivanja, brend Switch-a koji se koristi, pružene usluge i još mnogo toga.

Pored toga, drugi ne-istraživači mogu biti u potrazi za više informacija, kao što su:

- Šta je IXP?
- Osnovne informacije o IXP-u (istorija)
- Status IXP-a dana

IXP Osoblje

Kako IXP raste web sajt IXP-a postaje korisna alatka za komunikaciju za:

- Tehničko osoblje i inženjere
- Administracija i finansijski menadžment
- Prodaje i marketing
- Nadzor menadžment i izveštavanje

5.7 IXP i Internet zajednice

Zajednice su stvorene da pruže podršku i postoje odlične IXP zajednice. Ispod su navedene neke od IXP zajednica i ostalih “grupa” koje pomažu pri obuci, uvodu, networkingu i tehničkoj podršci.

IXP asocijacije:

Ove asocijacije pružaju obuku, networking i mogućnosti za biznis. Za IXPeve koji su u početku, one pružaju odlično mesto za dobijanje podrške[13]. U principu utvrđen IXP vam

može pomoći tako što blisko sarađuje sa vama. Takođe se možete sastati sa ljudima iz organizacija kao što su [ISOC](#), [PCH](#), i [RIPE](#) koji vam mogu pomoći sa opremom, uživo treningom i ostalim.

- Asia Pacific Internet Exchange Association [APIX](#)
- African Internet Exchange Association [AF-IX](#)
- European Internet Exchange Association [Euro-IX](#)
- Latin-American and Caribbean Internet Exchange Association [LAC-IX](#)

Grupe mrežnih operatera (Network Operator Groups – NOGs):

Sastanci Grupa mrežnih operatera su ključna mesta za dobijanje tehničkog iskustva i obuke, povezivanje sa ekspertima, građenje sopstvene zajednice mreže i poverenja (ljudskog)

- African Network Operator Group: [AFNOG](#)
- Asia Pacific Regional Internet Conference on Operational Technologies: [APRICOT](#)
- Caribbean Network Operator Group: [CaribNOG](#)
- Eurasia Network Operator Group: [ENOG](#)
- Latin-American Network Operator Group: [LACNOG](#)
- Middle East Network Operator Group: [MENOG](#)
- North American Network Operator Group: [NANOG](#)
- South Asian Network Operator Group: [SANOG](#)

Regionalni internet registri (Regional Internet Registry):

Regionalni internet registri alociraju i dodeljuju IP adrese i autonomne sistemske brojeve.

IP adrese i autonomni sistemi brojeva su bitni za građu mreže, rutovanje saobraćaja, i korišćenje ključnih internet protokola kao što je BGP.

- [AfriNIC](#) and [AfriNIC Mailing Lists](#)
- [ARIN](#) and [ARIN Mailing Lists](#)
- [APNIC](#) and [APNIC Mailing Lists](#)
- [LACNIC](#) and [LACNIC Mailing Lists](#)
- [RIPE](#) and [RIPE Mailing Lists](#)

European Internet Exchange Association

European Internet Exchange Association ili Evro-IX je udruženje evropskih IXP-jeva. To je zajednica koja služi evropskim IXP i Internet provajderima. Evro-IXP je deo globalnog IX-F Internet eXchange Federation.

Euro-IX okuplja 80 IXP-jeva širom sveta. Formirana je u maju 2001. godine sa namerom da se razvije, ojača i unapređuje internet (IXP) zajednicu[15]. Jedan broj IXP-jeva

prepoznao je potrebu za razmenu resursa u cilju koordinacije tehničkih standarda, razvitku zajedničkih procedura, učešću i objavi statistike i drugih korisnih informacija. To bi zauzvrat dao svim zainteresovanim stranama bolji uvid u svet IXP-a.

Cilj Euro-IX je da se poveća prisustvo i vidljivost evropskih IXP-a , pomažući im da prošire svoju bazu kupaca/članova:

- Pružajući sve neophodne informacije Internet provajderima (ISP) širom sveta koji žele da se povežu sa evropskom IXP.
- Predstavljajući neutralnost članova IXP na industrijskim događajima širom sveta.
- Omogućavajući IXP-jevima da podele svoje znanje jedni sa drugima putem sastanaka, mailing liste i eb stranica

Internet Exchange Federation (IX-F)

Internet Exchange Federacija (IX-F) deluje kao platforma za spojena udruženja IXP (IXPA). Cilj je da se izgradi globalina IXP zajednica i da se pomogne u razvoju IXP-jeva u u celom svetu[12].

U novembru 2012. godine, na 21. Evro-IX forumu u Stokholmu je potpisan Memorandum o razumevanju (MOR) između APIX (Asia Pacific Internet Exchange Association), LAC-IX (Latin America & Caribbean Internet Exchange Association) and Euro-IX (European Internet Exchange Association), da se formira Internet Ekchange federacija (IX-F). African Internet Exchange Association (Af-IX) pridružuje se IX-F –u 7. oktobra 2014.

Réseaux IP Européens (RIPE)

RIPE (European IP Networks) je nezavisna, neprofitna organizacija koja podržava infrastrukturu Interneta kroz tehničku koordinaciju[14]. Najistaknutija aktivnost je da deluje kao regionalni Internet registar (RIR) obezbeđujući globalne internet resurse i prateće usluge (IPv4, IPv6 i AS brojem) članovima u njihovom servis regionu.

Njihovo članstvo sastoji se uglavnom od Internet provajdera (ISP), telekomunikacionih organizacija i velikih korporacija koje se nalaze u Evropi, na Bliskom Istoku i u delovima Centralne Azije.

Literatura

- [1] <https://www.itu.int/en/wtpf-13/Documents/backgrounder-wtpf-13-ixps-en.pdf>
- [2] <https://www.youtube.com/watch?v=9hIQjrMHTv4>
- [3] https://www.internetsociety.org/sites/default/files/ixps-20090514_0.pdf
- [4] https://www.internetsociety.org/sites/default/files/Global%20IXPToolkit_Collaborative%20Draft_Feb%2024.pdf
- [5] http://etd.fcla.edu/CF/CFE0004802/dissertation_Moh_Final.pdf
- [6] <https://arxiv.org/ftp/arxiv/papers/1307/1307.5264.pdf>
- [7] Juan Camilo Cordona Restrepo, Rade Stanojevic “A history of an internet exchange point” April 2012.
- [8] Internet Traffic Exchange: Market Developments and Policy Challenges (OECD 2012) http://www.oecd-ilibrary.org/scienceand-technology/internet-traffic-exchange_5k918gpt130q-en
- [9] <http://www.eecs.qmul.ac.uk/~steve/papers/ixp-sgcm.pdf>
- [10] <http://www.calyptix.com/top-threats/top-7-network-attack-types>
- [11] http://drpeering.net/a/Internet-Peering-Playbook/Second-Edition/Source/HTML_IPP/chapters/ch12-9-US-vs-European-Internet-Exchange-Point/ch12-9-US-vs-European-Internet-Exchange-Point.html
- [12] <http://www.ix-f.net/about.html>
- [13] <https://www.ixptoolkit.org/content/internet-exchange-points-ixp-and-internet-community>
- [14] <https://www.ripe.net/about-us/what-we-do>
- [15] <https://euro-ix.net/about-euro-ix/>

- [16] https://labs.ripe.net/Members/roberto_di_lallo/is-it-really-worth-peering-at-ixps