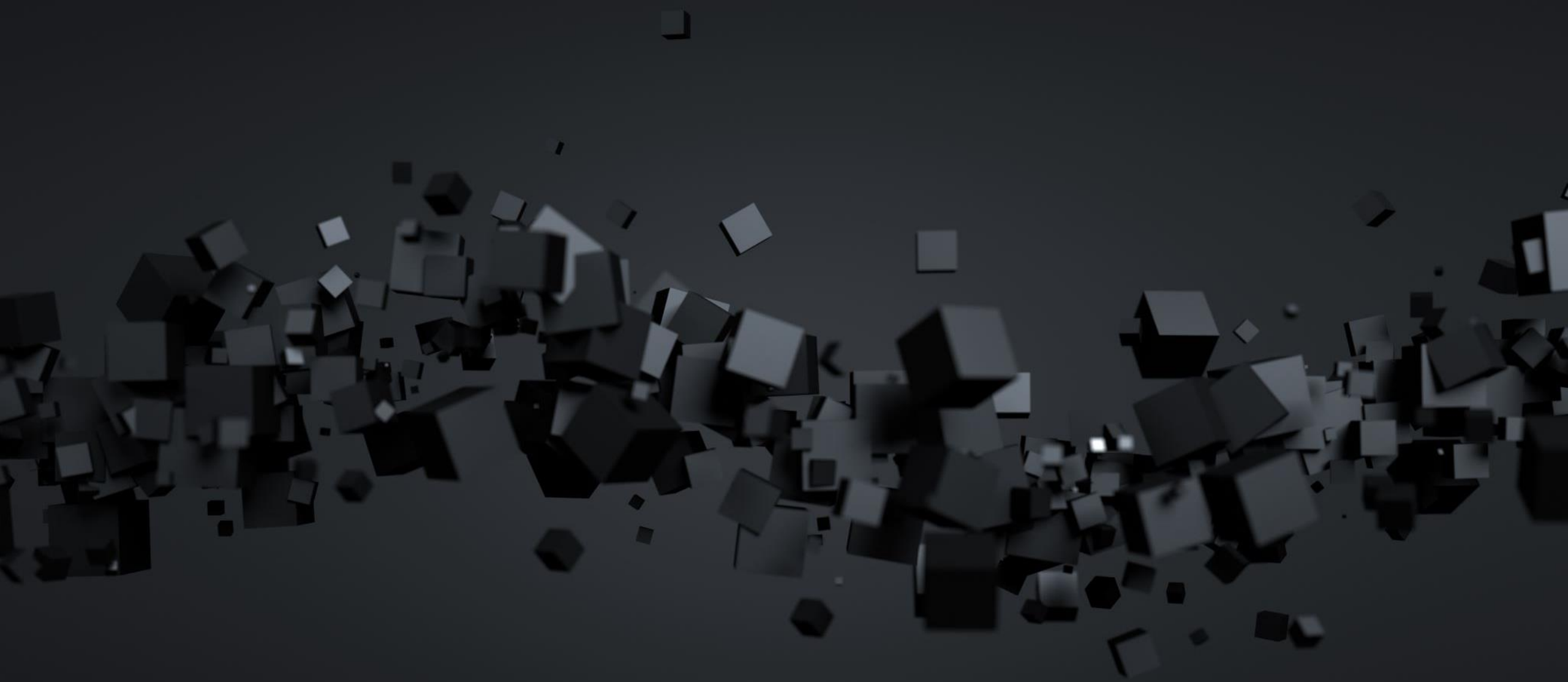


Omrežna varnost

Osnove računalniškega mreženja

Računalniško omrežje - skupina računalnikov, ki uporabljajo nabor skupnih komunikacijskih protokolov prek digitalnih medsebojnih povezav za skupno rabo virov, ki se nahajajo na omrežnih vozliščih ali, ki jih ta vozlišča zagotavljajo

Medsebojne povezave med vozlišči nastajajo iz širokega spektra telekomunikacijskih omrežnih tehnologij, ki temeljijo na fizično žičnih, optičnih in brezžičnih radiofrekvenčnih metodah, ki so lahko razporejene v različnih omrežnih topologijah

Osnove računalniškega mreženja

Vozlišča računalniškega omrežja – so lahko osebni računalniki, strežniki, mrežna strojna oprema ali gostitelje za splošno uporabo

- Vozlišča so tudi znana kot gostitelji (hosts)

Označeni so z imeni gostiteljev (host names) in omrežnimi naslovi (network address)

Imena gostiteljev služijo kot nepozabne oznake za vozlišča, ki se redko spremenijo po začetni dodelitvi

Omrežni naslovi služijo za iskanje in prepoznavanje vozlišč s pomočjo komunikacijskih protokolov, kot je internetni protokol (IP)

Osnove računalniškega mreženja

Tipi omrežij

Topologije omrežij

Omrežne naprave

Nivoji komunikacije

Protokoli

IP naslovi

Tipi omrežij

Žična in brezžična omrežja

Zgodnja (pred leta 2008) omrežja so bila pretežno žična

Danes pa je večina omrežij dejansko mešanico žičnega in brezžičnega omrežja

Žična omrežja uporabljajo Ethernet kot protokol za podatkovno povezavo

Žična omrežja

Prednosti

- Ethernetna vrata najdemo v skoraj vseh osebnih računalnikih (PC), večino prenosnikih (pri novejših več ne, sicer obstajajo adapterji).
- So hitrejša od brezžičnih. Hitrosti prenosa podatkov so se občasno povečale s prvotnih 10 megabitov na sekundo na 1 gigabit na sekundo. Večina domačih omrežij uporablja 10-100Mbps.
- So bolj varno kot brezžična

Slabosti

- Uporabiti je treba kabel, ki je lahko težko vodljiv in drag.
- Ni ga mogoče enostavno uporabiti med stavbami.

Brezžična omrežja

Prednosti

- Na splošno lažje nastaviti.
- Uporabljajo se lahko v domačih in javnih omrežjih
- Kabli niso potrebni.
- Lahko se uporabljajo z mobilnimi telefoni in tabličnimi računalniki.

Slabosti

- Na splošno počasnejša kot žična omrežja.
- Omejena z obsegom.
- Odprta za prisluškovanje.
- Ne tako varna, odvisno od nastavitve.

Topologije omrežij

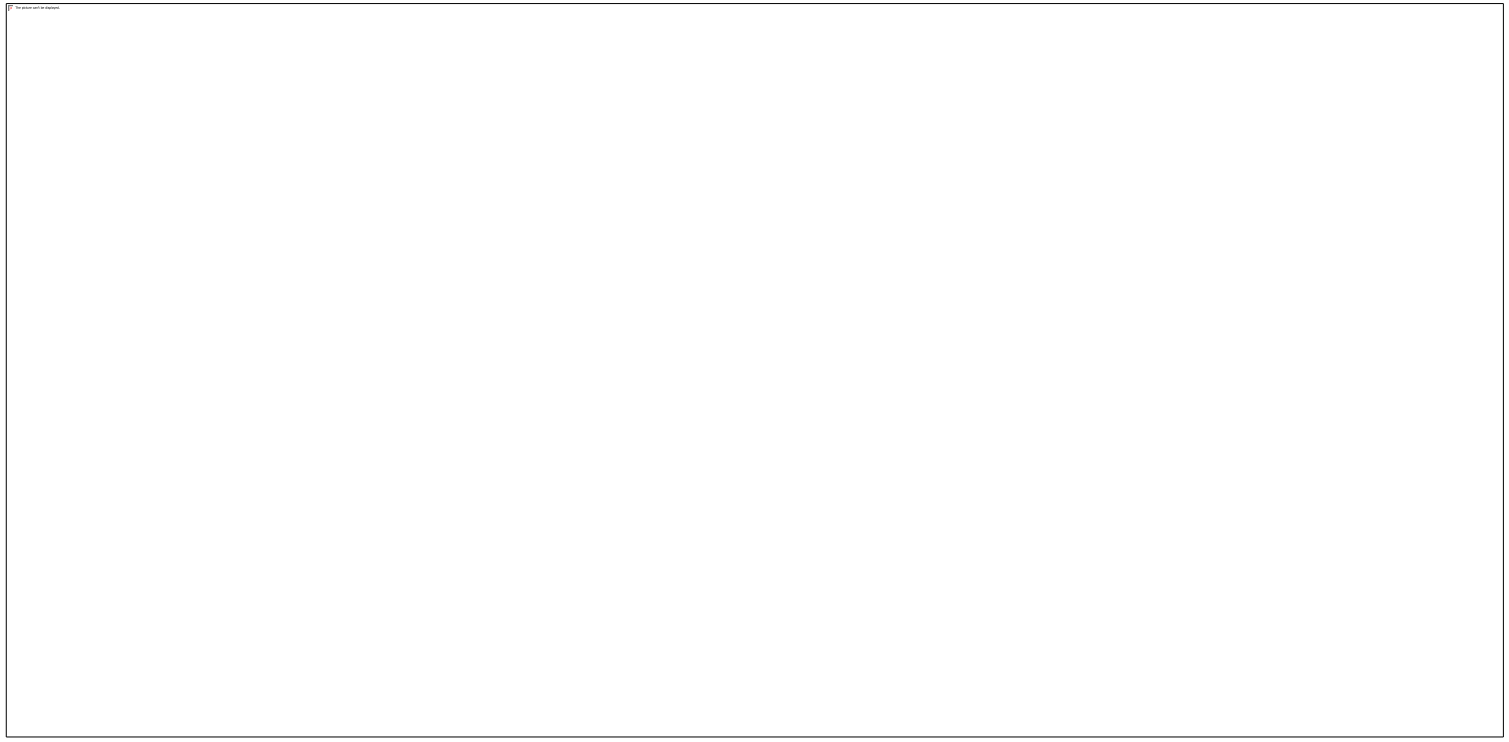
Topologija omrežja je postavitev, vzorec ali organizacijska hierarhija medsebojnega povezovanja omrežnih gostiteljev, v nasprotju z njihovo fizično ali geografsko lokacijo

Običajno je večina diagramov, ki opisujejo omrežja, razporejena po ustrezni topologiji

Topologija omrežja lahko vpliva na prepustnost, vendar je zanesljivost pogosto bolj kritična

Pri mnogih tehnologijah, kot je recimo Bus, lahko en sam izpad povzroči popolno odpoved omrežja

Na splošno velja, da več kot je medsebojnih povezav, močnejše je omrežje; toda dražje ga je namestiti



Topologije omrežij

Topologije omrežij

Bus network - vsa vozlišča so povezana s skupnim medijem vzdolž tega medija. To je bila postavitev, ki se je uporabljala v prvotnem Ethernetu, imenovanem 10BASE5 in 10BASE2. To je še vedno pogosta topologija na ravni podatkovne povezave, čeprav sodobne različice fizične plasti uporabljajo point-to-point povezave.

Star network - vsa vozlišča so povezana s posebnim osrednjim vozliščem. To je tipična postavitev, ki jo najdemo v brezžičnem LAN-u (Wireless LAN), kjer se vsak brezžični odjemalec poveže z osrednjo brezžično dostopno točko.

Ring network - vsako vozlišče je povezano s svojim levim in desnim sosednjim vozliščem, tako da so vsa vozlišča povezana in lahko vsako vozlišče doseže drugo vozlišče s premikanjem vozlišč levo ali desno.

Mesh network - vsako vozlišče je povezano s poljubnim številom sosedov na tak način, da obstaja vsaj en prehod s katerega koli vozlišča na katero koli drugo.

Fully connected network - vsako vozlišče je povezano z vsakim drugim vozliščem v omrežju.

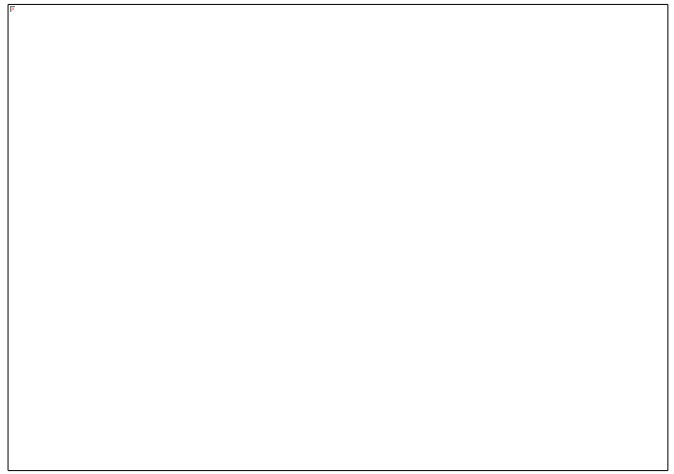
Tree network - vozlišča so razporejena hierarhično.

https://www.studytonight.com/computer-networks/network-topology-type

Omrežne naprave

Poleg fizičnih prenosnih medijev so omrežja zgrajena iz dodatnih osnovnih gradnikov sistema, kot so krmilniki omrežnih vmesnikov (Network Interface Controllers - **NIC**), repetitorji (**repeaters**), zvezdišča (**hubs**), mostovi (**bridges**), stikala (**switches**), usmerjevalniki (**routers**), modemi (**modems**) in požarni zidovi (**firewalls**)

Vsak določen del opreme bo pogosto vseboval več gradnikov, zato lahko opravlja več funkcij



Omrežne naprave

NIC - računalniška strojna oprema, ki poveže računalnik z omrežnim medijem in ima možnost obdelave omrežnih informacij na nizki ravni

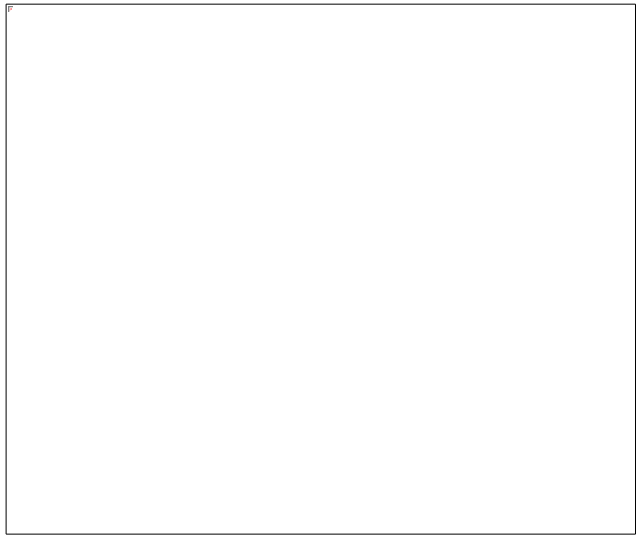
- Ima lahko priključek za sprejem kabla ali anteno za brezžični prenos in sprejem

V omrežjih Ethernet ima vsak NIC edinstven naslov za nadzor dostopa do medijev (MAC) - običajno shranjen v stalnem pomnilniku krmilnika

Da bi se izognili nasprotujočim si naslovom med omrežnimi napravami, Inštitut za inženirje elektrotehnike in elektronike (IEEE) vzdržuje in upravlja edinstvenost naslovov MAC

Velikost naslova Ethernet MAC je šest oktetov (48 bitov). Trije najpomembnejši okteti so rezervirani za identifikacijo proizvajalcev NIC

Proizvajalci samo z dodeljenimi predponami enolično dodelijo tri najmanj pomembne oktete vsakega vmesnika Ethernet, ki ga proizvedejo



Omrežne naprave

Repeaters in Hubs

- Repetitor je elektronska naprava, ki sprejme omrežni signal, ga očisti nepotrebnega hrupa in ga regenerira
- Signal se ponovno odda na višji ravni moči ali na drugo stran ovire, tako da lahko signal prekriva večje razdalje brez poslabšanja
- Repetitorji delujejo na **fizični plasti** modela OSI, vendar še vedno potrebujejo malo časa za regeneracijo signala
- Ethernetni repetitor z več portov je znan kot Ethernet Hub
- Repetitorji in Hubi so v veliki meri zastareli – danes imamo sodobna omrežna stikala

Omrežne naprave

Mostovi (Bridges)

- Delujejo na data link layer (plast 2) modela OSI in povezuje in filtrira promet med dvema mrežnima segmentoma, da tvori enotno omrežje
- Segmentacija omrežij s pomočjo mostov razgradi veliko preobremenjeno omrežje v skupek manjših in učinkovitejših omrežij

Switches

- Naprava, ki posreduje podatke in okvire (frames) podatkov med vrati na podlagi ciljnega naslova MAC v vsakem okviru
- Okvirje posreduje samo na vrata, ki sodelujejo v komunikaciji, medtem ko Hub posreduje na vsa vrata
- Stikala imajo običajno številna vrata, kar olajša topologijo zvezde za naprave in za kaskadno vezavo dodatnih stikal

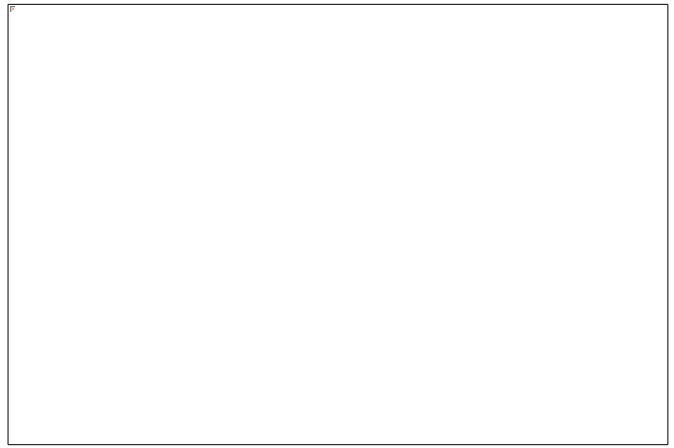
Omrežne naprave

Usmerjevalniki (Routers)

- Naprava, ki posreduje pakete med omrežji z obdelavo informacij o naslavljanju ter usmerjanju, vključenih v paket
- Informacije o usmerjanju se pogosto obdelujejo v povezavi s tabelo za usmerjanje
- Usmerjevalnik s pomočjo usmerjevalne tabele določi, kam naj posreduje pakete

Modemi (Modems)

- Modemi (MOdulator-DEModulator) se uporabljajo za povezovanje omrežnih vozlišč prek žice, ki prvotno niso bila zasnovana za digitalni omrežni promet ali za brezžično povezavo
- V ta namen digitalni signal modulira enega ali več nosilnih signalov, da ustvari analogni signal, ki ga je mogoče prilagoditi tako, da daje zahtevane lastnosti za prenos



Nivoji komunikacije

Omrežje lahko razdelimo na različne ravni ali sloje (layers)

Vsaka raven je odgovorna za določeno funkcijo

OSI uporablja 7-slojni model, **TCP / IP** pa 4-slojni model

Internet Protocol Suite, imenovan tudi **TCP / IP**, je temelj vseh sodobnih mrež

V osnovi, protokol TCP/IP opredeljuje specifikacije naslavljanja, identifikacije in usmerjanja za internetni protokol različice 4 (IPv4) in za IPv6 (naslednjo generacijo protokola z močno razširjeno zmožnostjo naslavljanja)

Nivoji komunikacije – TCP / IP

http://www.steves-internet-guide.com/internet-protocol-suite-explained

Protokoli

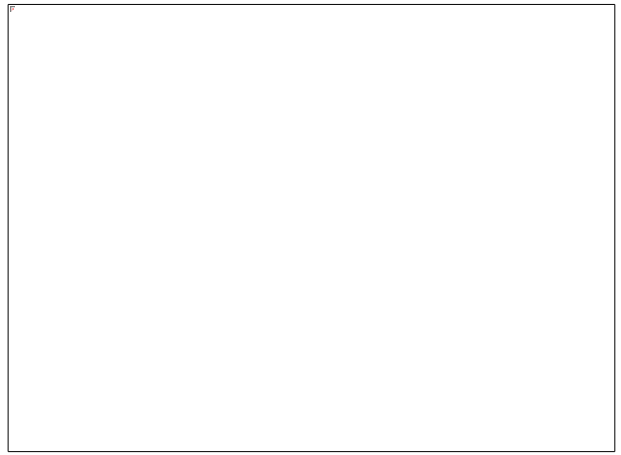
Komunikacijski protokol je sklop pravil za izmenjavo informacij po omrežju

V protokolnem skladu vsak protokol izkoristi storitve protokolarne plasti pod seboj, dokler najnižji sloj ne nadzira strojne opreme, ki pošilja informacije prek medija

Uporaba razporeditve protokolov je danes povsod razširjena na področju računalniških omrežij

Pomemben primer skladov protokolov: HTTP (protokol svetovnega spleta), ki deluje prek TCP prek IP (internetni protokoli) prek IEEE 802.11 (protokol Wi-Fi)

- Uporablja se med brezžičnim usmerjevalnikom in osebnim računalnikom domačega uporabnika, ko uporabnik brska po spletu



Protokoli

Ethernet - dvoslojni protokol / standard, ki pokriva sloj fizične in podatkovne povezave (physical in data link layer)

HTTP (protokol za prenos hiperteksta) – osnova današnjega spleta

SMTP, POP3, IMap4 - to so e-poštni protokoli

TCP (Transmission control protocol) - se uporablja za zagotavljanje zanesljive, varne in celovite povezave

- Podobno kot pri telefonski povezavi - najprej moramo vzpostaviti povezavo s klicanjem številke, ko se povezava vzpostavi imamo imate dvosmerni komunikacijski kanal.
- Nato nadaljujete z govorom in ko končate, prekinete povezavo.
- S TCP nastavite povezavo **s trosmernim rokovanjem (3-way handshake)**

UDP (User Datagram Protocol) – je protokol brez povezave in ne zagotavlja dostave – Fire and forget

- Podobno kot pri e-pošti ali navadni pošti
- Z e-pošto ali pisnim sporočilom pošljete svoje sporočilo, vendar ne veste, ali je bilo to sporočilo prejeto ali ne

IP (Internet Protocol) - to je glavni omrežni protokol. Obstajata dve različici IP (IPv4 in IPV6)

ARP (Adress Resolution Protocol) - prevede naslov IP v MAC ali fizični naslov (omrežja IP4)

IP naslovi

Internet Protocol address (naslov IP) je številčna „nalepka“, dodeljena vsaki napravi (npr. računalniku, tiskalniku, mobilni napravi), ki sodeluje v računalniškem omrežju, ki za komunikacijo uporablja internetni protokol

IPv4 je v uporabi od začetka interneta in je uveden po internetu in domačih / poslovnih omrežjih

IPv4 za naslavljanje uporablja 32 bitov, vendar so zaradi hitre rasti interneta vsi naslovi IPv4 dodeljeni (od leta 2013)

Tehnike, kot je **NAT** (Network Address Translation), so podaljšale življenjsko dobo IPv4 z omogočanjem uporabe zasebnih naslovov IP znotraj omrežij

IP naslovi

Vendar bo sčasoma IPv4 nadomeščen z IPV6, ki za naslov uporablja 128 bitov, zato lahko sprejme veliko več gostiteljev (računalniki / naprave).

Uvajanje IPv6 prek interneta se dogaja počasi, IPv4 pa bo z nami še vrsto let, zlasti v domačih in majhnih pisarniških omrežjih.

Naslovi IP so logični naslovi in jih dodeli skrbnik omrežja ali pa jih je mogoče samodejno dodeliti (z uporabo DHCP)

IP naslovi – Javni in zasebni

Tako IPv4 kot IPV6 imata javni in zasebni obseg naslovov

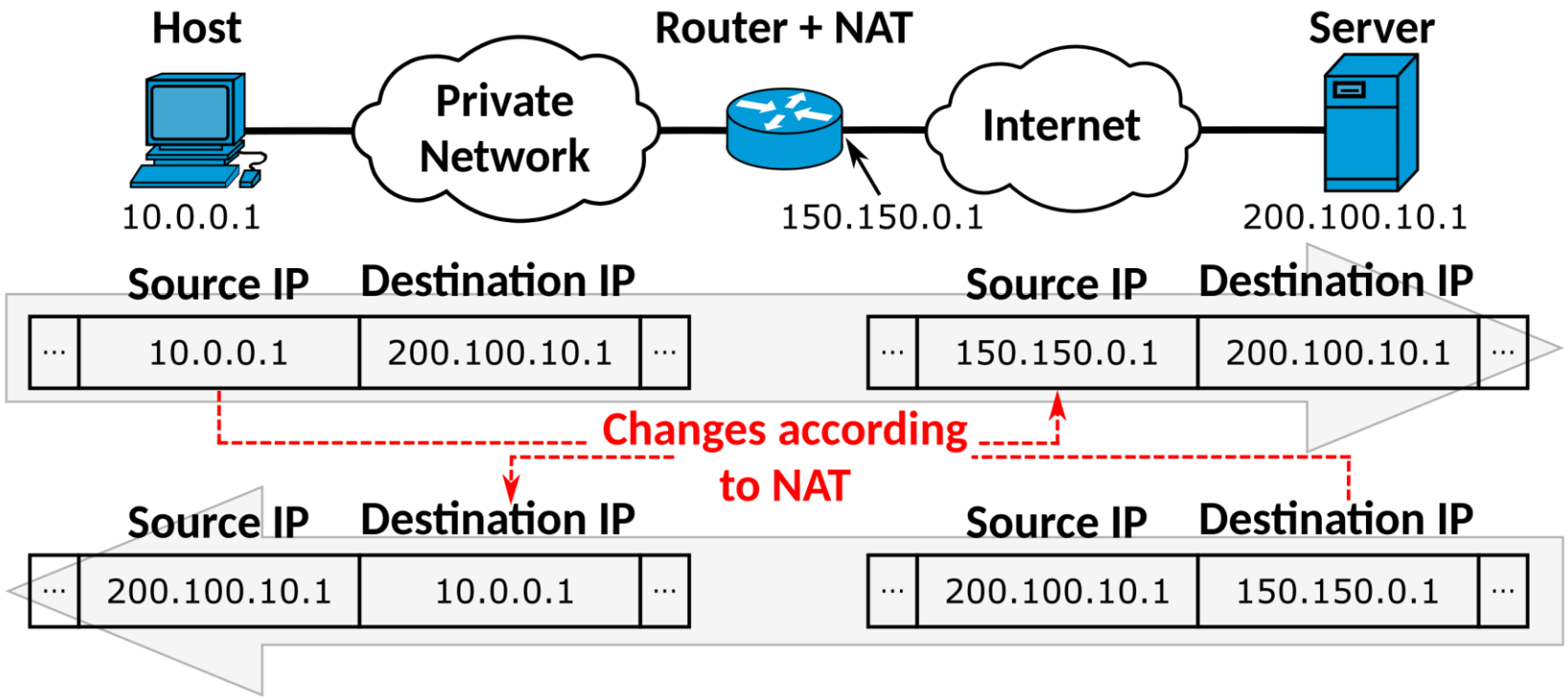
Zasebni naslovi se uporabljajo za domača / poslovna omrežja, naslovi pa niso usmerljivi po internetu, torej ne potujejo po internetu

Za IP4 se zasebni naslovi začnejo z 10.x.x.x ali 192.168.x.x ali 172.16.x.x

Javni naslovi so dostopni kjer koli na internetu in so usmerljivi

https://stevessmarthomeguide.com/internal-external-ip-addresses/

NAT – Network Address Translation



https://commons.wikimedia.org/w/index.php?curid=86017447

Napadi na omrežja

Omrežni napad lahko definiramo kot katero koli metodo, postopek ali sredstvo, ki se uporablja za zlonamerni poskus ogrožanja omrežne varnosti

Varnost omrežja je postopek preprečevanja omrežnih napadov v določeni omrežni infrastrukturi

Na osnovi tehnik in metod, ki jih napadalec uporablja lahko razlikujemo, ali je napad aktiven kibernetski napad, napad pasivnega tipa ali kombinacija obeh

Napadi na omrežja

Aktivni napad je izkoriščanje omrežja, v katerem napadalec poskuša spremeniti podatke na cilju ali podatke na poti do cilja

Aktivni omrežni napadi so pogosto agresivni, očitni napadi, ki jih žrtve takoj zaznajo, ko se zgodijo

Aktivni napadi so zelo zlonamerni in pogosto zaklenejo uporabnike, uničijo pomnilnik ali datoteke ali prisilno pridobijo dostop do ciljanega sistema ali omrežja

Napadi na omrežja

Pasivni napad je omrežni napad, pri katerem se sistem spremlja in včasih skenira glede odprtih vrat in ranljivosti, vendar ne vpliva na sistemske vire

Namen pasivnega napada je torej dostop do računalniškega sistema ali omrežja in zbiranje podatkov brez zaznavanja

Tako omrežna varnost vključuje izvajanje različnih tehnik strojne in programske opreme, ki so potrebne za zaščito osnovne omrežne arhitekture

Z ustrezno varnostjo omrežja lahko zaznate nastajajoče grožnje, preden se vdrejo v vaše omrežje

Napadi na omrežja

Passive

- Network
- Wiretapping
- Port scanner
- Idle scan
- Encryption
- Traffic analysis

Active:

- Virus
- Eavesdropping
- Data modification
- Denial-of-service attack
- DNS spoofing
- Man in the middle
- ARP poisoning
- VLAN hopping
- Smurf attack
- Buffer overflow
- Heap overflow
- Format string attack
- SQL injection
- Phishing
- Cross-site scripting
- CSRF
- Cyber-attack

Napadi na omrežja – najbolj pogosti

Data theft: imenuje se tudi eksfiltracija podatkov, ko napadalec z nepooblaščenim dostopom pridobi zasebne podatke iz omrežja. Napadalci pogosto uporabljajo ukradene podatke za prijavo za branje zaščitenih datotek ali krajo podatkov, medtem ko se ti prenašajo med dvema omrežnima napravama.

Insider Threat: kot že ime pove, notranje grožnje prihajajo od zaposlenih v organizaciji. Ti zaposleni uporabljajo svoj dostop za vdor v omrežje in pridobivanje občutljivih ali zasebnih informacij o podjetju.

Malware Attacks: napad zlonamerne programske opreme se zgodi, ko zlonamerna koda (zlonamerna programska oprema) v omrežno napravo vstavi neželeno in nepooblaščeno programsko opremo. Zlonamerna programska oprema se lahko zlahka širi iz ene naprave v drugo, zato se je zelo težko popolnoma znebiti.

Password attacks: vsak napad, ki vključuje nekoga, ki poskuša nezakonito uporabiti geslo, se šteje kot napad z geslom. Heker lahko dobi dostop bodisi z ugibanjem, krajo ali zlomom gesla (krekanje).

Social Engineering: Ti napadi uporabljajo prevare in laži, da druge prepričajo, naj se odrečejo zasebnim podatkom (na primer geslo za račun) ali kršijo varnostne protokole. Napadi na področju socialnega inženiringa so pogosto usmerjeni na ljudi, ki niso podkovani s področja tehnike, lahko pa tudi na osebje tehnične podpore z lažnimi prošnjami za pomoč.

Omrežna varnost – varnostne rešitve

Protivirusna programska oprema: Protivirusno programsko opremo lahko namestite v vse omrežne naprave. Redno ga je treba posodabljati, da bi lahko odpravili morebitne težave ali ranljivosti.

Enkripcija: šifriranje je postopek kodiranja podatkov do nerazumljivosti: Le pooblaščene stranke imajo dešifrirni ključ (geslo). Tako tudi, če nepooblaščeni uporabnik podatke prestreže ali vidi, jih ne more prebrati.

Požarni zidovi: Požarni zidovi so programska oprema, strojna naprava ali kombinacija obeh, ki preprečuje vstop nezaželenega prometa v omrežje. Lahko jih konfigurirate tako, da blokirajo samo sumljiv ali nepooblaščen promet, hkrati pa omogočajo dostop do zakonitih zahtev.

Multi-Factor Authentication: večfaktorska overitev je preprosta: uporabniki morajo za prijavo v račun navesti dva ločena načina identifikacije (na primer vtipkati geslo in nato vnesti številčno kodo, ki je bila poslana na drugo napravo). Uporabniki bi morali uporabiti edinstvene poverilnice iz dveh od treh kategorij - nekaj, kar **veste**, nekaj, kar **imate**, in nekaj, kar **ste** - da bo večfaktorska overitev v celoti učinkovita.

Segmentacija omrežja: segmentacija omrežja vključuje razčlenitev večjega omrežja na različna podomrežja ali segmente. Če je katero od podomrežij ogroženo, ostanejo ostale nedotaknjene, ker obstajajo neodvisno drug od drugega.

Omrežna varnost – varnostne rešitve

Navidezna zasebna omrežja (Virtual Private Network - VPN) – navidezno zasebno omrežje šifrira povezavo od končne točke do omrežja, pogosto prek interneta. Na ta način preverja pristnost komunikacije med napravo in varnim omrežjem ter ustvarja varen, šifriran "tunel" po odprtem internetu.

Upoštevanje najboljše prakse glede ustvarjanja gesel – to je osnovno načelo, vendar je upoštevanje najboljših praks glede gesla preprost in zelo učinkovit način za vzdrževanje omrežne varnosti. Veliko ljudi ustvari gesla, ki niso močna, ponovno uporabijo prejšnja gesla in ne uporabljajo enoličnih gesel za vsak svoj račun.

Preizkušanje varnosti omrežja – nikoli ne smemo domnevati, da je naše omrežje popolnoma varno.