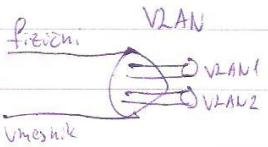
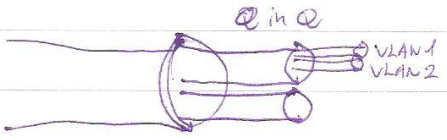
Omrežja

1) Ethernet:

→ 22 protokol, Plug and play, visoke hitrosti prenosa, različne tehnologije prenos
→ Omogoča PoE, VLAN (tuneli navidezni), protokoli za preprečevanje zank
→ Enotna velikost okvirja: 1500 oktetov tovor + 18 oktetov vežija
↳ glava: dest. MAC, source MAC; polnilnik bitov za tovor
→ Slaba nezivljivost, konvergance, enostavno poplavljanje MAC tabel, nizka cena vmesnikov; nerejen za multicast - nekavna prilagojenost
→ MAC - 48 bit v HEX; 24 bitov kopi proizvajalec, druga polovica je spremenljiva
→ stikalo dela MAC tabelo (MAC/vmesnik)

• VLAN:
→ virtualizacija ETH omrežij; neodvisnost od fizične topologije omogoča ločitev uporabnikov. Naredimo lahko logično topologijo.
→ Vsak VLAN ima svoj ID, omejeno na 4094
→ statično/dinamično dodeljevanje VLAN vmesnikov
→ en fizični vmesnik lahko pripada enemu VLAN, večim ali delaje v načinu "trunk": V glavi ETH se doda VLAN informacija (4 okteti) → 802.1Q
→ virtualni tunelski mehanizem:





• Zaščita:
→ Fizični sloj SDH
→ Povezavni: STP, Rapit STP, Link Aggregation

STP:
→ preprečevanje zank, max 7 vozlišč, slaba konvergenca ~30-50 sec. Določimo root stikalo (preko privilegiet), na podlagi cene poti postavimo virtualno eno pot v blokad

da prikinemo krog.

→Root in Designated port

→Da pridem v stanje forwarding čakam do 50 sec, da se stikala zmenijo za poti. Signalizacija poteka preko BPDU sporočil

RSTP: rapid spanning tree prot.

→porti v enakih vlogah kot pri STP

→čas konvergence ~1s

→ročna nastavitev robnih portov: uporabnikov, to se avtomatsko postavi v stanje forwarding

→omogoča dvosmerno komunikacijo med stikali (zahteve-potrditve)

MSTP:

→omogoča razširitve RSTP na VLAN omrežje

Link Aggregation:

→omogoča navidezno združevanje več fizičnih vmesnikov, da deluje kot ena sama navidezna povezava (LAG) 802.3ad

→konvergenca pod 0,5 sec

QoS v Eth:

→V delu glave Eth okvirja v polju za VLAN je 3 bit prostor za dodeljevanje prioritete. Komunikacije, ki zahtevajo najmanjše zakasnitve imajo najvišjo prioriteto (IPTV, VoIP) tako se na omrežnih stičiščih zagotavlja kvaliteta storitev.

Varnost:

→Napadi MAC, ARP, DHCP, STP

Metro-eth:

⇒ ETH kot transportna tech, ETH kot storitev

\+ enostavno omogoča multicast, IPTV, VLAN, visoka hitrost prenosa

\- manjša zanesljivost kupnam SDH, počasna konvergenca, sluba

nezširljivost, varnost, omejeno št. vnosov v MAC

MEF model → standardizirani eth vmesniki UNI

↓ → omogoča logično povezljivost med dvema ali več vmesniki EVC

EVC omogoča povezavo med končnima točkama

→ UNI-Client, UNI-Network

→ Funkcije EVC:

- povezovanje dveh ali več vmesnikov
- preprečevanje prenosa podatkov med dvema različnima EVC

→ Pravila:

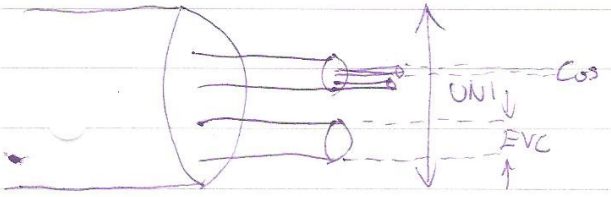
- okvir nesme priti nazaj na izvorni UNI
- poslani ETH okvir mora ~~biti~~ ostati nespremenjen

→ Tipi povezav:

- E-Line: točka - točka
- E-LAN: multipoint - multipoint
- E-tree: rooted - multipoint

→ Prometni profili: nupodkaji: Class of Service (CoS), EVC ali UNI

- CIR: zajamčena podatkovna hitrost // povprečna generirana hitrost
- CBS: zajamčena velikost izbruha podatkov // količina nalučniku ki jih naročnik lahko pošlje
- EIR: presežena podatkovna hitrost // avg. max. prenešena hitrost ob prezasičeni linji
- EBS: presežena velikost izbruha podatkov // količina ki jih naročnik lahko pošlje v izbruhu v primeru nezasičene linije.



Metar

→parametri za QoS:
- razpoložljivost
- zakasnitev okvirjev
- variacija zakasnitev
- izguba okvirjev

→določanje na podlagi CoS || imamo več tipov storitve glede na CoS

→multipleksiranje: več EVC na en UNI

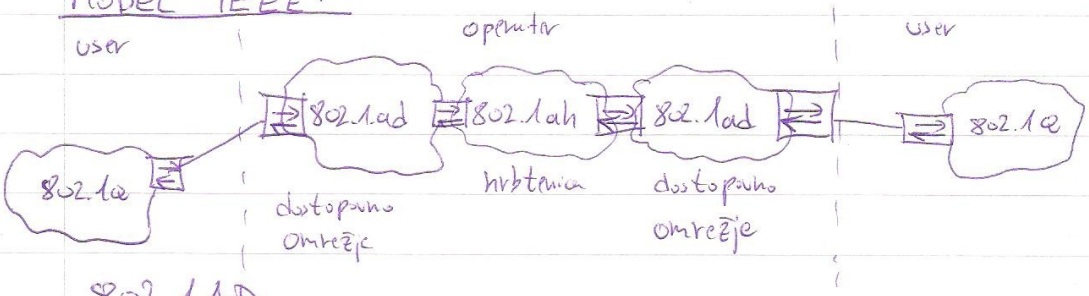
→označevanje VLAN, ločitev prometa uporabnikov. Ohranjevanje CE VLAN ID uporabe podaljšanega LAN omrežja. Q in Q, MAC in MAC

ITU-T model:

→sestavljen iz enakih gradnikov kot MEP

→isti tipi storitev

MODEL IEEE:



802.1AD

→Dvojno označevanje okvirjev: oznaka uporabnika, oznaka operaterja, transparenten prenos uporabniške oznake

→Nov format okvirja v gluki ETH

→transparenten prenos uporabniškega prometa

802.1AH

→Arhitektura in protokoli za povezovanje 802.1AD v hrbtenično omrežje

→koncept MAC in MAC

→dodu indentifikator hrbteničnega omrežja

+enkapsulacija MAC in MAC se izvaja na robu

+nupnive v hrbtenici morjo poznati zgolj UNI MAC naslove

Usmerjanje:

→ Izmenjava podatkov o dosegljivosti, izbira optimalne poti

→ zgradba usmerjevalnega sistema:

- usmerjevalni proces
  - izmenjava usmerjevalnih informacij
  - določitev optimalne poti
  - izvaja se lahko v nerealnem času
- posredovalni proces
  - izbira ustreznega vmesnika
  - posredovanje paketov na izhodni vmesnik
  - izvajati se mora v realnem času

→ poganja usmerjevalne protokole, izmenjava usmerjevalnih informacij, določanje kam poslati diagram (routing), določitev optimalne poti, izgradnja usmerjevalne tabele (RIB - routing info base)

→ posredovanje paketa iz vhodnega na izhodni vmesnik; skozi omrežje obstaja več poti, samo optimalna se zapiše v posredovalno tabelo (FIB); izbira ustreznega izhodnega vmesnika se izvaja po principu ujemanja v največji meri

→ statično usmerjanje:

ročna določitev vmesnikov, admin določa pot.
privzeta pot - pošiljanje vseh paketov, kine najdejo specifične poti gredo na privzeto pot.

→ dinamično usmerjanje:

avtomatična določitev usmerjevalnih poti, uporaba usmerjevalnih protokolov.

→posredovalne funkcije (router - posredovalni procesi)

- sprejema paket na vhodu
- dekapsulacija paketa do L3, preverjanje CRC v glavi IP, zmanjšanje TTL ponoven izračun CRC, enkapsulacija datagrama IP
- določanje optimalne poti (posredovanje UNICAST / MULTICAST)
- prenos na ustrezen izhodni vmesnik
- po potrebi: fragmentacija, razvrščevanje paketov

→usmerjevalne tabele: vsak protokol in usmerjevalnik vzdržuje svojo in posredovano usmerjevalno tabelo. V sebi vnose, prek katerih fizičnih vmesnikov mora router posredovati paket na cilj

→izbira optimalne poti: po seštevku metrik posameznih kosov poti

→Lastnosti usmerjevalnih algoritmov: hitra konvergenca, preprost, robusten

→Distance vector (RIP): BGP

- usmerjevalne info. se posredujejo samo sosedom
- vsak pozna samo svoje sosede in ceno do njih
- počasna konvergenca
- pombi zelo mal. CPU in RAM

→Link-State: OSPF, IS-IS

- usmerjevalne informacije se posredujejo vsem v omrežje, routerji poznajo celotno topologijo omrežja.
- oglašujejo samo spremembe v routing tables
- omogočajo boljšo razširljivost

→BGP

- interior in exterior iBGP, eBGP
- izboljšana verzija distance vector
- pot se določi na osnovi ciljnega omrežja-metrike.
- omogoča brezrazredno usmerjanje med domenami
- celotna route tabela se izmenja po inicializaciji, nakndno se oglašujejo spremembe.

IP/MPLS

- vzameno vse prednosti IP in ATM
- koncept label na IP kontrolni ravnini
- tehnologija ni vezana na nobeno specifično L1/L2 tehnologijo

→ ločiti usmerjevalne in posredovalne funkcije
posredovalni mehanizem je zamenjava label

→ glava MPLS: kratek identifikator fiksne dolžine, doda se pred IP datagram. Labela je polje v glavi MPLS

→ Label-switching-Path LSP – enosmeren tunel skozi MPLS omrežje

→ FEC (Forwarding Equivalence Class) - skupina paketov, obravnavanih na enak način

→ Usmerjevalnik LSR: operacije: vstavitev, zamenjava, odstranitev glave MPLS

→ zamenjava glave MPLS: vhodni vmesnik in labela določata:
- operacije vstavi, zamenja, odstrani
- izhodni vmesnik in izhodno labelo

→ Labela ima lokalen pomen med dvema routerjema, omogočen je sklad tabel

→ Omrežje MPLS vpelje povezavno usmerjen princip v sicer nepovezavno usmerjeno omrežje

→ Signalizacija:
- LDP - Label Distribution Protocol
sporočila: "discovery_message" za odkrivanje novih sosedov
"hello" se pošilja vsem sosedom (UDP), nadaljnje komunikacija poteka po TCP
"session message", "advertisment message"

→ MPLS zadosti potrebam po:
- navidezna zasebna omrežja
- zaščitni mehanizmi
- kakovost storitev
- prometni inženiring

Aleta

Paketna Stikala:

- je omrežni element, ki posreduje protokolne podatkovne enote med vhodi in izhodi stikala.
- omrežje sestavljeno iz paketnih stikal izvaja paketno komutacijo
- ETH stikala, router, ATM stikala, ...
- Fiksna velikost paketov: enostavna stikala, težavna določitev opt. velikosti
- Variabilna velikost: zapleteno stikalo, manj potreb po segmentaciji, prez velikosti dogovora
- Majhni paketi: dobro statistično multipleksiranje, manjše zakasnitve, velika režija za majhen tovor, veliko kontrolnega prometa, veliko procesiranja
- Veliki paketi: Enostavno procesiranje, slabo MUX, zakasnitve, dobro razmerje telo/glava, neučinkovit pri prenosu kontrolnih informacij

(router) - Zgradba: kontrolna ravnina (tabele routing), podatkovna (usmerja), upravljalska

- Imajo distribuiran operacijski sistem
- Zgradba paketnega stikala: O/I vrata, vodilo, izravnalnik, Schedula, Classifier
- Vhodno čakanje HoL: teoretično za velikost 2x2 je prepustnost omejena na 58,6% oz. na 75% za večja stikala
- Izhodno čakanje: Možna 100% čakalna vrsta na izhod ~~čaka~~ stikalne matrike
- Navidezno izhodno čakanje: Ločene čakalne vrste za vsak izhod možna 100% prepustnost
- Zmedi čakanja v čakalnih vrstah se lahko zmanjšajo prometa spremenijo. Zmedi zamašitev je lahko del podatkov izgubljen. Zmedi čakalnih vrst prihaja do zakasnitev, tudi neenakomernih - potresavanje zakasnitev.

IPv6:

- naslovni prostor 2^{128} v HEX.
→ unicast, multicast, anycast
→ ne podpira fragmentacije, minimalni MTU = 1280
→ protokol Neighbour discovery nadomešča ARP izvaja ICMPv6
→ integriran IPsec, fiksna dolžina glave - 40 B, manj polj
→ izboljšuje QoS z flow label v glavi

UNICAST:
→ imamo samo globalne naslove:
- global routing prefix 48 bitov
- subnet ID: 16 bitov
- Interface ID: 64 bit
→ link-local naslovi se uporabljajo v procesu Neighbour-discovery
FE80::/10, interface ID se generira iz MAC

MULTICAST:
FF::/8
→ solicited node naslov: FF02: : 1FF: (24 bitov iz globalnega IPv6)
→ Dodeljevanje naslovov:
- DHCPv6
- zadnjih 64 bitov je ali izračunanih iz MAC ali naključnih MD5
→ Loopback: ::1
→ Izračun MTU: Izvorna naprava pošlje paket privzete velikosti, če kakšen vmes ne zmore take velikosti, vrne ICMPv6 paket "Packet too big", nato izvorna naprava pošlje MTU ustrezne velikosti
→ PING v6 - dela ICMPv6 z echo Request in echo Reply
→ TTL je sedaj Hop LIMIT

Aleksa

IPv6 routing:

- RIPng
  - za metriko uporablja število hopov
  - za oglaševanje sosedom uporablja multicast naslov FF02::9
  - uporablja UDP
- OSPF
  - definicije "area" vsaj 0 je privzeta
  - za IPv6 je nadgradnja OSPFv2 in OSPF v3
  - tipi paketov: Hello, DBD, LSR, LSU, LSA
  - ~~za delovanje~~ uporablja multicast naslove: FF02::5 za vse OSPF routerje
    FF02::6 za DR usmerjevalnike
- BGP:
  - za IPv6 razširitev za oglaševanje IPv6 in za prav MPLS/VPN simulacije

Kriptiranje:

- kriptografija kriptoanaliza
- Simetrični postopki:
  - uporablja se samo en ključ, enak za enkripcijo in dekripcijo
  - vsak ključ mora biti drugačen, težave z varno izmenjavo ključa
  - prednost je hitrost
  - DES, 3DES, AES
- Asimetrični postopki:
  - Enkripcijski in dekripcijski ključa sta različna
  - ključa sta enolično povezana, če poznamo javni ključ je praktično nemogoče izračunati zasebnega
  - Vsak posameznik ima svoj par ključev
  - Diffie-Hellman, RSA, eliptične krivulje
  - enostavna izmenjava ključev, kompleksnost algoritmov, linearno naraščanje ključev, počasnost, problem generiranja naključnih praštevil

- Lastnosti javnih ključev:
  - javno dostopen, ponavadi objavljen v javnem imeniku
  - vedno je povezan z določeno osebo/terminalom/aplikacijo, lastnikom para ključev
- Lastnosti zasebnih ključev
  - ima ga samo lastnik, ki je odgovoren skrbeti za varno hranjenje
  - vedno je povezan z osebo/terminalom, lastnikom para ključev

→ Hibridni postopki
- za enkripcijo se uporablja 3DES, AES, za izmenjavo pa asimetrični

→ Zgoščevalni postopki: MD5, SHA-1
- poljubno dolg niz znakov preslika v blok konstantne dolžine, ki lahko predstavlja "prstni odtis"
- iz povzetka je nemogoče dobiti original (one way hash function)
- Mehanizem Hash MAC zagotavlja celovitost podatkov

→ Elektronski podpis:
- omogoča overjanje, celovitost, nezatajljivost, čas nastanka dokumenta, digitalni podpis nam ne zagotavlja zasebnosti podatkov
- pri digitalnem podpisovanju uporabimo postopek asimetričnega šifriranja ravno v obratni smeri.

→ Digitalna potrdila: (certifikati)
- zagotavljajo verodostojnost javnih ključev
- vsebujejo: javni ključ, podatke o lastniku, podpis izdajatelja, ostale parametre
- overitelj-izdajatelj (CA) je ustanova, pooblaščena za izdajanje dig. potrdil
- zagotavlja: šifriranje podatkov, digitalno podpisovanje dokumentov
- Infrastruktura javnih ključev: (PKI)
  - določa: vrsto storitve, postopke ugotavljanja identitete, algoritme za upravljanje s ključi, overitelja (CA ali RA)
  - storitve: overjanje in preklic certifikatu, registracija javnega ključa in izbira ključa, ugotavljanje istovetnosti entitet

IPsec:

- na omrežnem sloju
- v IPv6 je integriran v verzijo, vgrajuje se v produkte za IPv4
- TCP/IP ne podpira varnostnih mehanizmov
- zagotavlja zaščito podatkov na omrežnem sloju; protokol je transparenten za uporabnika in aplikacije, temelji na znanih kriptografskih mehanizmih, dosežen nivo varnosti naj bo odvisen samo od kriptografskih mehanizmov.
- ključna aplikacija za IPsec so danes navidezna zasebna omrežja
- Nudi: avtentikacijo, nadzor dostopa, zaščito pred podtikanjem IP datagramov, zaupnost, celovitost, kompresijo
- Varnostna protokola AH in ESP
- Varna zveza:
  - Je enosmerna logična povezava med dvema IPsec napravama, če želimo dvosmerno komunikacijo, se vzpostavita dve zvezi
  - Tunelski in transportni način
- Ročno ali <u>avtomatsko upravljanje varnih povezav</u>:
  - s protokolom IKE, namenjen za vzpostavitev, vzdrževanje, prekinitev zveze
  - delovanje v dveh fazah.
    1. FAZA vzpostavitev zveze IKE: izmenjava ključev ... (dvosmerna)
    2. FAZA vzpostavitev seje IPsec (enosmerne povezave); protokol AH, ESP...

  IKEv2: Podpira avtentikacijo
- NAT protokol

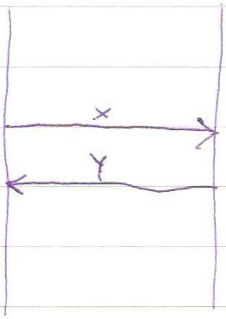
DODATEK

Diffie-Hellman

g...

- A ∈ prastal $(1, \dots, p-2)$ ali naključno izbrano
- B ∈ $(1, \dots, p-2)$

- javni ključ: $X = g^A \bmod p$
- $Y = g^B \bmod p$



- kriptirni ključ $k = Y^A \bmod p$
- $k = X^B \bmod p$

TLS - povezava med dvema aplikacijama (tunel)
IPsec - povezava med dvema napravama. (tunel)

Enosmerna funkcija

$$X = g^A \bmod P$$

- P... končna množica $\mathbb{P}$ števil med vključno 0 in P-1 ; oziroma nad končnim ali Galoisovim poljem GF(P)!
- g... primitivni element polja GF(P), če je z zgornjo enačbo mogoče izmžiti vse nenične elemente polja. To pomeni da z vsemi možnimi čistopisi A dobimo vse možne šifropise X.
- $A = \sum_{0}^{n-1} c_m \cdot 2^m$, n... dolžina sporočila, $c_m = \{0,1\}$

↳ sledi: $X = \prod_{0}^{n-1} K_m^{c_m} \bmod \mathbb{P}$; $K_m = g^{2^m}$

$K_0 = g$

$K_{m+1} = K_m^2 \bmod N$

Izmenjava ključev:

- ~~A izbere~~ Dogovor o izberi g in P, ki sta javna, dostopna v javni bazi podatkov
- A: izbere naključno število $X_A < P$:

$$Y_A = g^{X_A} \bmod P$$ in ga pošlje B

- B: izbere naključno število $X_B < P$:

$$Y_B = g^{X_B} \bmod P$$ in ga pošlje A

- A sedaj lahko izračuna ključ:

$$Y_{AB} = g^{X_A \cdot X_B} \bmod P = Y_A^{X_B} \bmod P = Y_B^{X_A} \bmod N$$

- Y_{AB} je sedaj ključ za komunikacijo (AES)!