Verkkojen välinen liikenne

S-38.188 Tietoliikenneverkot
15.10.1997

Luennon aiheet

- Internet Protocol (IP)
- IPng eli IPv6
- Internetin nimipalvelu
- Muut verkkoprotokollat

Internet Protocol (IP, DoD IP)

- nykyisin käytössä versio 4 (RFC 791, 1981)
- toimii verkkokerroksella
- sähkepohjainen
  - tarjoaa best-effort -palvelun
- 32-bittinen osoite
  - sisältää verkkonumeron
  - alunperin jako A, B ja C-luokkiin
  - nykyään aliverkon koko voidaan melko vapaasti valita (CIDR)

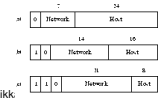
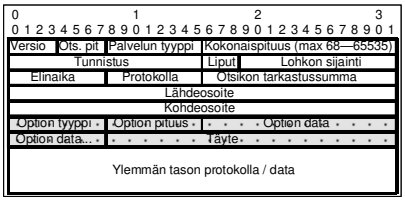


Figure 5.10

IP - paketti



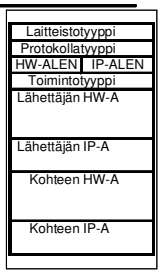
Pakettien lohkominen

- Paketin maksimikoko vaihtelee verkoissa
  - PPP (ld): 296, x.25: 576, eth: 1500, FDDI: 4352, ATM Classical IP: 9168, 16Mb TR: 17914, Hyperchannel: 65535
  - isommat paketit tehokkaimpia
- Lohkominen:
  - joka yhteydellä, kasaus jokaisessa reitittimessä
    - » viive, hukkuneet paketin osat, muistitarve
  - vain tarvittaessa pienemmiksi, kasaus kohdekoneessa
    - » käytössä IP:ssä

Figure 5.8

Liikennöinti samassa verkossa

- Vastapuolen MAC-osotteen selvittäminen: Address Resolution Protocol
  - lähettää levitysviestinä ARP-kyselyn
    - » muut koneet oppivat
  - kone vastaa joko kohde- tai levitysviestinä
  - mikäli ei käyttöä, poistuvat vähitellen (~15 min)
- Reverse ARP
  - oman IP-osotteen selvittäminen



Liikennöinti toiseen verkkoon

- Tunnistetaan verkkomaskin perustella
  - reititystaulut koneissa
    - » yleensä yksi “default gateway”
    - » lähetetään reitittimen MAC osotteeseen
  - proxy arp
- Reititin päättää taulukon perusteella kohteen
  - staattinen konfigurointi
    - » ei vikasietoinen
  - reititysprotokolla päivittää taulukkoa
    - » reitittimet vaihtavat määrävälein taulukoitaan
    - » turvallisuus?

Internet control message protocol

- Pakollinen osa kaikkia IP-toteutuksia
  - virheistä tiedottaminen
  - saavutettavuustestaus, suorituskykymittaus
  - ruuhkanhallinta
  - reitin muutos, aliverkkomaski
- sovellukset
  - ping - kohteen saavutettavuus, viive
  - traceroute - reitti kohteeseen
    - » lähettää UDP-paketin, vastauksena ICMP

IP:n päällä käytettävät protokollat

- TCP - luotettava tavuvirta
- UDP - sähkepalvelu
- GGP, BGP, EGP, OSPF, RIP, ISIS - reititystieto
- VINES - Banyan Vines mikroverkko
- ISO-IP - ISO Internet Protocol, ISO-TP4 - ISO Transport Protocol Class 4

IP: tulevaisuuden vaatimukset

- nykyään palvelee “tietokoneyhteisöä”: nykyisin Internettin liittyneiden verkkojen määrä kaksinkertaistuu vuosittain
- kasvun seuraava vaihe jakautuu useille markkinoille
  - liikkuvat informaatiovälineet
    - » langattomat (radio/infrapuna) verkot
  - verkkoviihde
    - » tilausvideo, pelit
  - laitteiden ohjaus
    - » kotiautomatio

IP->IPng

- väistämätöntä 3-7 seuraavan vuoden aikana
- reititys ja osotteistus
  - IPv4:ää tekohengitetty Classless Inter-Domain Routing
    - » C-luokan verkkoja annettu operaattoreille nipuissa
  - verkot loppuvat
  - tuki liikkuville laitteille
- siirtyminen helpompaa niin kauan kuin osoitteet ja verkot riittävät
- edellytykset: IPv4 ja IPng toimivat yhdessä, joustava siirtyminen
  - taaksepäin yhteensopiva (vrt x86-prosessorit)
- Turvallisuuden parantaminen

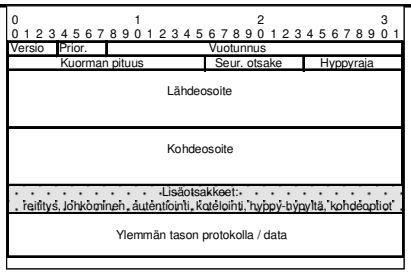
IPng: IPv6

- laajennetut reititys- ja osoituskapasiteetit
  - 32->128 bittiä: enemän hierarkiatasoja, enemän mahdollisia asemia ja yksinkertaisempi konfigurointi
  - jakelulähetysreititys (multicast) skaalattavampi
  - jokulähetys (anycast): lähetetään jollekin useasta
- yksinkertaisempi otsake
  - enemän optionaalista: osoite 4*=>otsake 2*
  - nopeampi käsittely ja kaistanleveyden säästö
- parempi tuki optioille
  - tehokkaampi edelleenohjaus, vähemän rajoituksia ja mahdollisuus uusille
  - järjestys määrätty => nopeampi käsittely

IPng: IPv6...

- palvelun laatu
  - paketit kuuluvat tiettyihin virtoihin, joille pyydetään erityiskäsittelyä, esim tosiaikasovellukset
- tunnistaminen ja yksityisyys
  - mekanismit tunnistamiseen, tiedon eheyteen ja luottamuksellisuuteen ovat peruselementteinä: mukaan kaikkiin toteutuksiin

IPv6 otsake



IPng osoitteistuis

- 128 bittiä
  - $7{,}9*10^{28}$ kertaa IPv4:n osoiteavaruus
  - tehollisia osotteita $8*10^{17}$ — $2*10^{33}$ (1500 — $3*10^{18}$ osoitetta/m^2)
  - nyt 15 %:n käyttö määritelty

Osoitehierrarkiat

- Tarjoajapohjainen
- Maantieteellinen
- Paikallinen (MAC-osotteeseen perustuva)
  - esim. käynnistyksen ajaksi, myös osittaiseen MAC-osotteeseen
- IPv4-osotteita vastaavat
  - sekä IPv6 että IPv4 osaaville
  - vain IPv4
- IPX, NSAP-osotteiden muunnos
- Anycast: ryhmälle reitittimiä
- Jakeluosoite (multicast) laajuusmäärittelyllä

IP v6 osoitteet

	128 bittiä			
	kone			
	n bittiä			128-n bittiä
	aliverkkotunniste			kone
	n bittiä	80-n bittiä		48 bittiä
	tilaajatunniste	aliverkkotunniste		IEEE-802 MAC
	s bittiä	n bittiä	m bittiä	128-s-n-m bittiä
	tilaajatunniste	aluetunniste	aliverkkotunniste	kone
IPv4-osoite	80 bittiä		16 bittiä	32 bittiä
	0000:0000:.....:0000		0000	IPv4-osoite
vain IPv4	80 bittiä		16 bittiä	32 bittiä
	0000:0000:.....:0000		FFFF	IPv4-osoite
linkki	10 bittiä	n bittiä		118-n bittiä
	1111111010	0		ID
yksityinen	10 bittiä	n bittiä	m bittiä	118-n-m bittiä
	1111111011	0	aliverkkotunniste	ID
jakelu	8 bittiä	4 bittiä	4 bittiä	112 bittiä
	11111111	liput	laajuus	ryhmätunniste

IPng reititys

- lähes kuten IPv4 Classless Inter-Domain Routing:llä
- vanhat reititysprotokollat käyttökelpoisia suoraviivaisilla muutoksilla
  - OSPF, RIP, BGP
- uudet ominaisuudet
  - tarjoajan valinta (hinta, suorituskyky...)
  - liikkuvuus (reitti nykyiseen sijaintiin)
  - automaattinen uudelleenosoitteistus (reitti uuteen osoitteeseen)
- perustuvat “Routing”-optioon
  - reitti tallentuu ja vastapuoli lähettää samaa reittiä takaisin

IPng palvelun laatu

- vuotunnus “satunnainen”
  - mahdollistaa erikoispalvelujen tarjoamisen
  - voidaan käyttää reitityksen ja vuonvarauksen tehostamiseen
- prioriteetti
  - 15–8: realiaikasovellukset
    - » 8: pakettien hukkuminen ei vakavaa (laatuvideo)
    - » 15: paras mahdollinen (pieninopeuksinen ääni)
  - 7–0: ruuhkaohjattu liikenne (TCP)
    - » hallinnalle (reititys, SNMP) korkein prioriteetti (7)
    - » interaktiivinen käyttö (6), interaktiivinen siirto (4)
    - » valvomaton siirto (2), “täyte”liikenne (1)

IPng turvallisuus

- Tunnistaminen ja eheys
  - käyttää “IPng Authentication Header”-osaketta
  - suojaa “tekeytymiseltä”
  - ylemmillä kerroksilla ei ole ollut hyvää suojaa
- Eheys ja luottamuksellisuus
  - käyttää “IPng Encapsulating Security Header”
  - ei sidoksissa yhteen salausalgoritmiin
- Ongelmana (USA:n) vientikiellot, patentit ja viranomaisten politiikka
  - vahva salaus kielletty tai rajoitettu Ranskassa, Belgiassa ja Englannissa

IPng:hen siirtyminen

- Vaiheittainen siirtyminen
  - pienet riippuvuudet (DNS)
  - osotteita ei ole välttämätöntä muuttaa
- Pienet kustannukset
  - IPv4-osotteita voidaan käyttää (::123.45.67.89)
  - alkuvaiheessa laitteet kaksineuvoisia (::00FF:123.45.67.89)
  - IPv6 kapselointi IPv4-paketteihin
  - IPv4-liikenteen reitittäminen vain-IPv6 verkossa suunniteltu (siirtymän viimevaihe)
  - paikallisia laitteita (esim kirjoittimet) ei tarvitse koskaan päivittää

Nimipalvelu

- Numerot
  - vaikeasti muistettavia
  - koneille helppoja käsitellä (kiinteämittaisina)
- Kuvaavat nimet helpompia ihmisille
- Litteä nimiavaruus
  - ei rakennetta nimissä
- Hierrarkinen nimiavaruus
  - nimet muodostavat puumaisen rakenteen
- 80-luvun puoliväliin kaikki Internetin koneet yhtenä tiedostona
  - keskitetty ylläpito, lähetettiin sähköpostitse jokaiselle ylläpitäjälle

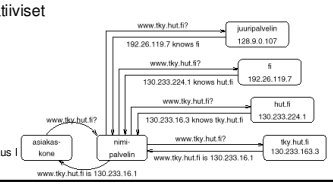
DNS

- Hierrarkinen
  - jaettu hallinnollisesti itsenäisiin osa-alueisiin
  - kaksi tai useampi nimipalvelin joka alueella
- Tietokanta
  - <nimi, arvo, tyyppi, luokka, elinikä>
  - tyyppi: miten nimi-arvo tulkitaan
  - luokka: tyyppien määrittelijä (IN)
  - elinikä: kuinka kauan tietue on voimassa

A	1	a host address
NS	2	an authoritative name server
CNAME	5	the canonical name for an alias
SOA	6	marks the start of a zone of authority
WKS	11	a well known service description
PTR	12	a domain name pointer
HINFO	13	host information
MX	15	mail exchange
TXT	16	text strings
RP	17	for Responsible Person
GPOS	27	Geographical Position
AAAA	28	IP6 Address
*	255	A request for all records

Nimen selvittäminen

- Ohjelma kysyy käyttöjärjestelmän kirjastolta
- Kirjasto omalta nimipalvelimelta
- Oma nimipalvelin lähtee selvittämään niin ylhäältä kuin tarpeen
  - saa joko kysytyn vastauksen tai tiedon “kuka tietää“
  - tallentaa kyselyjen vastaukset
    - » myös negatiiviset



Nimen valitseminen

- Päätason maatunnisteet (ISO3166)
  - USA: com, org, net, gov, mil
- Kunkin päätason hallinnoija jakaa organisaatiotunnisteet
  - Suomi: THK, tietokantaa ylläpitää Eunet
- Organisaation sisällä vapaa: litteä tai hierrarkinen
  - esimerkiksi osastoittain
- Koneiden nimeäminen
  - palveluiden mukaan (mail, news, ftp, www,….)
  - teeman mukaan (planeetat, alkuaineet,…)
  - organisatorisesti (hyflt12, lk-hp-1,..)
  - käyttäjän mukaan (erkkipc, ...)

IP-liikenteen vaiheet

- Nimikysely
  - ARP-kysely nimipalvelijan tai (oletus)reitittimen osotteelle
  - nimikysely nimipalvelijalta
    - » mahdollisesti vastaus vaatii kyselyjä
- IP-datagrammin lähettäminen
  - ARP-kysely kohdekoneen tai (oletus)reitittimen osotteelle
- Ylempien protokollien yhteyden luominen

ISO-protokollat

- palvelumäärittely (⇳)
  - mitä palveluja protokolla tarjoaa ylöspäin ja mitä palveluja se voi käyttää
  - request, confirm, indication, response
- protokollamäärittely (⇔)
  - määrittää Protocol Data Unit:n vertaisolioiden kanssa keskusteluun
  - Service Access Point määrittää kunkin kerroksen palvelunsaajan

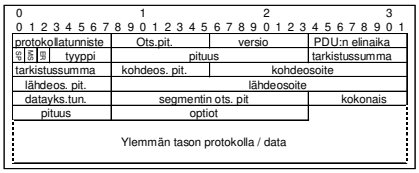
ISO protokollan määrittely

- määritellään kaikki
  - tulevat tapahtumat
  - tilat
  - lähtevät tapahtumat ja toiminnot
  - tilamuuttujat ja määritteet
- luodaan laajennettu tapahtuma-tila -taulukko
  - ainoastaan määritellyt tapahtumat laillisia

Nykytila / Tuleva tapahtuma	S_0	S_1	S_2	…	S_N	
IE_1 … IE_x						Tulevat tapahtumat (yläpuolelta: palvelupyynnöt)
IE_{x+1} … IE_y						Tulevat tapahtumat (alapuolelta: esim data vastaanotettu)
IE_{y+1} … IE_z						Paikalliset tapahtumat (esim ajastimet)

ISO Internet Protocol (ISO IP)

- Connectionless Network Protocol/Service
  - Network Service Access Point



ISO Esitystapakerros

- ASN.1 (abstract syntax notation number one)
  - koodaus- ja purkurutiinit
  - UNIVERSAL: esim kokononaisluvut
  - CONTEXT-SPECIFIC
  - APPLICATION
  - PRIVATE
  - rakenteet
    - » UNIVERSAL SEQUENCE
    - » SEQUENCE OF
    - » SET
    - » SET OF
    - » CHOISE

ASN.1

- Formaali määrittely, josta voidaan tuottaa koodia
- Koodaus
  - Tunniste
    - » luokka
    - » rakenne
    - » tyyppi
  - Pituus
  - Sisältö

Novell Internet Packet Exchange (IPX)

- perustuu Xerox Network Services:n Internet Datagram Protocol:aan
  - verkko.kone.portti-osoite
  - voi käyttää useita eri kehysmuotoja
    - » raaka 802.3 (ilman LLC-kehystä)
    - » LLC-paketointi (oma DSAP/SSAP-koodi)
    - » SNAP-kehystys (Sub-Network Access Protocol: Ethernet-kehystys LLC-kehyksessä)
- tarjoaa yhteydettömän sähkepohjaisen liikenteen (kuten DoD IP)
- reititettävä protokolla
  - Point-to-Point protokollaa kaksipisteyhteyksillä
  - IPX-pakettien "tunnelointi" IP-paketteihin IP-verkkojen yli

Network [Basic] Input/Output System

- palvelurajapinta IBM PC-koneissa
  - verkkoliikennöinnistä IBM:n dokumenttiin 6322916: "Technical Reference PC Network"
- siirtomedian suhteen joustava
  - TCP/IP, DECnet, DLC, XNS, ISO TP4, IPX...
- perustuu nimiin (16 tavua)
  - litteä nimiavaruus
  - reititys vaatii usein lisä-älyä reitittimeen
- "yksinkertaisin" siirtomedia NetBIOS Extended User Interface
  - reititys ei mahdollista

Yhteenveto

- IP merkittävin verkkoprotokolla
  - koeteltu skaalautuvuus
  - uusi versio tulossa
- Muilla omat käyttösovelluksensa
  - parempi turvallisuus (ehkä)
  - eri protokollien sekakäyttö kuormittaa
  - laajasta skaalautuvuudesta ei kokemuksia