



Verkkoyhteydet ja turvallisuus

S-38.188 Tietoliikenneverkot
Markus Peuhkuri

Luennon aiheet

- ◆ Etäyhteydet
 - WWW-palvelimet
 - OVT-yhteydet
- ◆ Järjestelmien suojaus
 - ongelmat
 - ratkaisukeinot

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

2

Yhdistämistekniikat



- ◆ Valintaiset yhteydet
 - POTS (0,3 — 56 kbit/s)
 - Datex (1,2 — 9,6 kbit/s)
 - Diginet (1,2 — 64 kbit/s)
 - ISDN (BRI: 64; 128 kbit/s PRI: n*64 kbit/s; n<=30)
 - radioverkot (0,3 — 14,4 kbit/s)
- ◆ Kiinteät yhteydet
 - galvaaninen yhteys (19,2 — 2048 kbit/s)
 - piirikytentäinen yhteys (n*64 kbit/s)
 - pakettiverkko [x.25/x.32] (1,2 kbit/s — 2048 kbit/s)
 - kehysvälitteinen verkko (64 kbit/s — 2 Mbit/s)
 - soluvälitteinen verkko (2 Mbit/s —)

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

3

Valintaiset yhteydet



- ◆ Puhelinverkko (0,3 — 56 kbit/s)
 - tarjoaa 3,1 kHz:n (300 — 3400 Hz) taajuuskaistan
 - datasiirtoon käytettävä modeemia
 - » maksimissaan 33 kbit/s molempiin suuntiin
 - » riippuva yhteyden laadusta
 - voidaan tehostaa pakkauksella (1,5 - 2 x)
 - yhteydenotto ei 100 % luotettava
 - kytkentäaika pitkäkö (15 — 30 s)
 - saatavissa kaikkialle, maailmanlaajuiset yhteydet
 - peruskustannukset edulliset
 - käyttökustannus yhteyssajan perusteella

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

4

Valintaiset yhteydet...



- ◆ Datex (1,2 — 9,6 kbit/s)
 - nopea kytkentä, pohjoismainen
 - aloitusmaksu + kk-maksu + yhteyden luominen + yhteysaika
- ◆ Diginet (1,2 — 64 kbit/s)
 - digitaalisen puhelinverkon avulla toteutettu datasiirtopalvelu
 - kehitetty "ISDN:ää odotellessa"

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

5

Valintaiset yhteydet/ISDN



- ◆ Integrated Services Digital Network
 - perusliittymä (2B+D, Basic Rate Interface)
 - » 2*64 kbit/s data, 16 kbit/s merkinanto
 - järjestelmäliittymä (30B+D, Primary Rate Interface)
 - » 30*64 kbit/s data, 64 kbit/s merkinanto
 - tukee eri palveluja (esim 3.1 kHz puhe ja 64 kbit/s digitaalinen yhteys)
 - tieto tyypistä (puhe/data) välittyy verkossa:
 - » modeemien kättelyvaihe jää pois
 - » kytkeytyminen nopeaa (0,3 — 3 s)
 - » mahdollistaa paremmin tarvemukaisen yhteyden muodostuksen

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

6

...ISDN

- useita yhteyksiä voidaan ryhmitellä nopeammaksi yhteydeksi
- peruskustannuksiltaan POTS:a kalliimpi
 - » liittymismaksu ja kk-maksu suurempia
 - » päätelaitteet merkittävästi kalliimpia
- data-liikennöinti kalliimpaa
 - » ulkomaanyhteydet 5-20 % kalliimpia

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

7

Valintaiset yhteydet.../radioverkot

- ♦ analogiset verkot (NMT, ARP, VHF-verkot)
 - puheen siirtoon tarkoitetuissa verkoissa voidaan käyttää valintaisen puheliverkon modeemeja
 - radiotien häiriöt poikkeavat langallisista yhteyksistä
 - virheenkorjauskehyksen oltava pienempi [MNP10]
 - DMS-modeemi NMT-verkossa (600 bit/s)
 - NMT-yhteydet toimivat noin 7200 bit/s
 - tiedon pakkaus ja sala

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

8

Radioverkot

- ♦ digitaaliset verkot (GSM)
 - läpinäkyvä/ei-läpinäkyvä siirto
 - nopeus maksimissaan 9,6 kbit/s [12 kbit/s]
 - analogisiin modeemeihin modeemipankin kautta
 - ISDN-yhteydet V.110-sovituksella

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

9

Kiinteät yhteydet

- ♦ Galvaaninen yhteys (19,2 — 2048 kbit/s)
 - rakennetaan itse tai vuokrataan kaapeliyhteys
 - käytetään kantataajuusmodeemeja, pitkällä yhteyksillä kantoaalto-modeemeja
 - nopeus laskee etäisyyden kasvaessa
 - yleensä mahdollista vain saman keskuksen alueella (max 10 km)
 - radiolinkit
 - vaatii linkkitason protokollan käyttöä
 - asennusmaksu+kk-hinta

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

10

Ky / piiriyhteydet

- ♦ Piiriyhteydet (n*64 kbit/s)
 - yhteys asiakkaalta kantataajuusmodeemilla (kuten gy) tai nopeammissa yhteyksissä kuidulla pisteeseen, jossa data liitetään PCM-yhteyksiin
 - puhelinverkossa on varattu kiinteät PCM-aikavälit yhteyttä varten
 - kapasiteetti on varattuna vaikei liikennettä olisikaan
 - viive pieni
 - kuten galvaaninen yhteys, mutta laajemmalle alueelle
 - vaatii linkkitason protokollan käyttöä
 - asennusmaksu+kk-hinta

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

11

Ky / pakettiverkko

- ♦ Pakettiverkko (1,2 kbit/s — 2048 kbit/s)
 - yhteys asiakkaalta lähimpään X.25-solmuun piiriyhteydet
 - jokainen solmu vastaa paketin välittämistä eteenpäin
 - » vaatii muistia solmuissa
 - » aiheuttaa viivettä
 - x.32: valintainen yhteys
 - kansainväliset yhteydet laajalle
 - asennusmaksu + kk-hinta + yhteysaika + siirretty tietomäärä

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

12

Verkkojen vaihtoehdot

- ◆ Modeemilinjat puhelinverkossa
 - + yhteydet kaikilta-kaikkiin
 - kaistanleveys, kiinteä kaista, hallinta puutteelline
- ◆ Kiinteät vuokralinjat
 - + eri linjanopeuksia, hallinta eri tasoilla
 - kiinteä kaista (vajaakäyttö), kahden pisteen välinen
- ◆ PCM (E1) multiplexerillä
 - + suuri siirtonopeus (1,5-2Mb/s), useita yhteyksiä samassa liittymässä, hallinta
 - kiinteä kaista, kahden pisteen välinen

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

13

Verkkojen vaihtoehdot

- ◆ ISDN / kytkentäinen data (64k-2Mb/s)
 - + kaistanleveys haluttaessa, eri yhteydet kutsutasolla
 - kiinteä kaista kutsutasolla, huono saatavuus
- ◆ X.25
 - + pakettipohjaisuus hyödyntää kaistanleveyden, yhteydet kaikilta-kaikkiin, virheenkorjaus
 - raskas protokolla hidastaa (< 256 kb/s (2Mb/s)) ja lisää kustannuksia

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

14

Frame Relay

- ◆ Pakettivälitys (-kehys)
 - tilastollinen kanavointi yhteyksillä
 - tukee purskeista liikennettä
- ◆ Virtuaaliyhteydet
 - luotavissa verkonhallinnalla (PVC) / valintaisesti (SVC)
 - kehyksessä yhteystunniste DLCI
- ◆ Määrittelee
 - ANSI: T1.602, T1.606, T1.607-1990, T1S1/91-659, T1.617, T1.618
 - ITU: I.122, Q-922, Q.933
 - pohjautuu ISDN-määrittelyihin
- ◆ Rajapintamäärittely

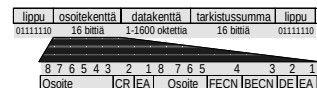
3.12.1997

Markus Peuhkuri / TTK Teletekniikka

15

FR-kehys

- ◆ LAPD-kehystys
 - alkueroin
 - » bitstuffing
 - osoitekenttä
 - » osoite (DLCI)
 - » käsky/vastaus
 - » lisäosoitebitti
 - » ruuhkailmaisu eteen- ja taakse
 - » hylkäysprioriteetti
 - datakenttä
 - tarkiste
 - loppueroin



3.12.1997

Markus Peuhkuri / TTK Teletekniikka

16

Liikenne verkossa

- ◆ Solmut välittävät DLCI-arvojen perusteella
 - paikallisia
- ◆ Kehys on vioittunut
 - ei alku- tai loppuerointa tai alle 5 oktetia välissä
 - ei tasamäärää oketteja (bittejä 8*N)
 - tarkistevirhe
 - osoitekenttä virheellinen tai arvoa ei tueta
 - koko liian suuri (sopimukseen nähden)
- ◆ Vioittunut kehys hylätään
 - ei indikaatiota lähettäjälle / vastaanottajalle

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

17

Verkon toiminta

- ◆ Määritely rajapinta
 - verkon sisäinen toteutus voi olla erilainen
 - paikallinen hallinta (DLCI=0)
- ◆ Solmussa
 - tarvittaessa hylkääminen
 - ei muutosta käyttäjädataan
 - muutetaan DLCI:t

DLCI	Käyttö
0	LMI: paikallinen hallinta (linjan testaus & kutsut)
1-15	tulevaisuutta varten
16-991	virtuaaliyhteyksien käytössä
992-1007	kerroksen 2 hallinta
1008-1022	tulevaisuutta varten
1023	hallintaa varten (ylemmät kerrokset)

3.12.1997

Markus Peuhkuri / TTK Teletekniikka

18

Liikenteen sääntely

- ♦ Solmut voivat ruuhkatilanteissa hukata kehyksiä
 - ensin DE-bitillä varustetut
- ♦ Ilmoitus myös päätelaitteelle
 - FECN: tässä suunnassa ruuhkaa
 - » esimerkiksi hidasta kuittausta
 - BECN: vastasuunnassa ruuhkaa
 - » vähennä lähetysnopeutta
 - ei velvoita päätelaitetta

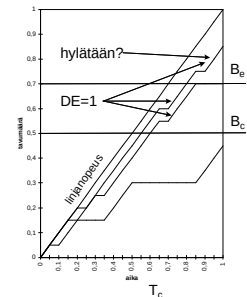
3.12.1997

Markus Peuhkuri / TKK Teletekniikka

19

Ruuhkan hallinta

- ♦ Liikennesopimus
 - $CIR \leq \text{linjanopeus}$ [bit/s]
 - $CIR = B_c / T_c$
 - $B_c + B_e = \text{sallittava purske}$
 - » B_c :n ylittävät kehykset merkitään DE
 - » $B_c + B_e$:n ylittävät: hylätään tai DE



3.12.1997

Markus Peuhkuri / TKK Teletekniikka

20

Kiint.../kehys...

- ♦ Soluvälitteinen verkko [ATM] (2 Mbit/s —)
 - asiakas-asiakas -yhteys ATM-tasolla
 - » lähiverkkoemulointi, MPOA, ...
 - sama tekniikka kuin lähiverkossa
 - tehokas kaistanleveyden käyttö
 - tulevaisuuden tekniikkaa
 - FR-toteutuksia ATM:n päällä

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

21

Lähiverkkojen yhdistäminen

- ♦ Siltaamalla
 - yksinkertaisempi
 - toimii kaikilla protokollilla
 - enemmän liikennettä
- ♦ Reittittämällä
 - toimii reititettävillä protokollilla
 - liikenteen suodatus
 - levitysviestit eivät leviä (kuin hallitusti)
 - varayhteydet ja kuormanjako helpompaa
 - laajoissa verkoissa ainoa vaihtoehto

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

22

WWW-palvelinvaihtoehdot

- ♦ Oma palvelin
 - vaatii kiinteän yhteyden
 - oma ylläpito
 - liitettävyyden yrityksen tietojärjestelmiin
 - » sekä sisäinen että ulkoinen tiedotus
 - » myyntipalvelu, helpdesk
- ♦ Palvelun osto
 - joko palvelintilan vuokraus tai "täyspaketti"
 - liitettävyyden tietojärjestelmään huono (staattinen tieto)
 - turvallinen vaihtoehto
 - pieni panostus, jos tutkitaan mahdollisuuksia

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

23

Yhteydet liikekumppaneihin

- ♦ OVT/EDI
 - kauppa (erit. tukku-) edelläkävänä, kuljetus ja teollisuus imussa
 - pankkiyhteydet merkittävien (2/3 tilisiirroista konekielisiä)
 - oman toiminnan tehostaminen ja asiakassuhteiden kehittäminen
 - » tiedonhallinnan parantaminen ja asiakastytyväisyys
 - » uudet toimintamahdollisuudet, virheiden väheneminen
 - EDIFACT-muunnin oma tai palveluntarjoajan hallinnassa

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

24

Yhteydet liikekumppaneihin

- ♦ Reititinverkot
- ♦ X.25
- ♦ Kiinteät yhteydet
- ♦ Internet
 - joustavin
 - tietoturvaongelmat
 - ovatko muutkaan viestinvälitysjärjestelmät turvallisia?

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

25

Miksi järjestelmän suojaaminen

- ♦ 80 % **havaitusta** yrityksistä pääsee järjestelmään
- ♦ Keitä te ootte...
 - teinejä, joilla on modeemi (lähinnä elokuvissa)
 - » ilkeävaltaa, tageja
 - omat työntekijät
 - palkkakräkkerit
 - tietokauppiat
 - kilpailijat
 - tiedustelupalvelut

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

26

Millä suojataan

- ♦ Jokainen kone turvallinen
 - käytännössä mahdoton heterogeenisessä ympäristössä
- ♦ Osa koneista turvallisia
 - liikenne tietyille/ltä koneilta estetään
- ♦ Verkon eristäminen
 - kaikki liikenne yhdyskäytävän kautta

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

27

Miksi suojataan

- ♦ Haavoittuvat TCP/IP -palvelut
 - suunniteltu käytettäväksi "turvatussa" ympäristössä: luottaminen tiettyihin osoitteisiin
 - NIS, NFS, SNMP, r-UNIX
- ♦ Salakuuntelun helppous
 - suurin osa liikenteestä salaamatonta
- ♦ Suojauspolitiikan puute
 - pääsy liian avoin
- ♦ Asetusten monimutkaisuus
 - virheet yleisiä

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

28

TCP/IP: ongelmat

- ♦ IP Source Routing
 - testauksarkoituksiin luotu
- ♦ TCP Sequence Number guess
 - useat koneet luovat eri TCP-yhteysten sarjanumerot determinisesti: helpottaa yhteyden kaappausta
- ♦ UDP
 - ei yhteyden luontia: hankalampi seurata
- ♦ ICMP redirect
 - reitityksen muuttaminen eri koneelle

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

29

Ohjelmistot: ongelmat

- ♦ Logiikkavirheet
 - puskurin ylivuotoja, väärää konfiguraatiota oletuksena
- ♦ Troijan hevoset
 - suosituissa ftp-palvelinohjelmassa virhe
 - vapaa ohjelma <=> kaupallinen ohjelma
- ♦ Salakuuntelu usein helppoa
 - pysyvät salasanat: kerran kuunneltu käytettävissä myöhemmin
- ♦ Autentikointi
 - huonot / salakuunnellut salasanat
 - useissa palveluissa koneen tarkkuudella: tietty IP-osoite

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

30

Ohjelmistot: ongelmat

- ◆ Tekeytymisen helppous
 - IP source routing
 - yhteyksien kaappaus
 - koneiden sammuttaminen
 - ei autentikointia: SMTP, NNTP
- ◆ LAN-palvelut, toisiinsa luottavat koneet
 - ylläpidon helpottaminen: NIS, NFS
 - käytön helpottaminen: rlogin
- ◆ Vaikeat konfiguraatio
 - järjestelmät usein konfiguroitu maksimaalisen salliviksi
- ◆ Konepohjainen turvallisuus ei skaalautu

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

31

Puskurin ylivuoto

```
fd=get_config(...
....
FILE *get_config_file(void)
{
    char buf[BZ], *p;
    if (p=getenv("MY_CONFIG")){
        strcpy(p, buf);
    } else {
        p="/etc/my.config";
    }
    return fopen(p, "r");
}
```



```
exec("/bin/sh", "-sh");
```

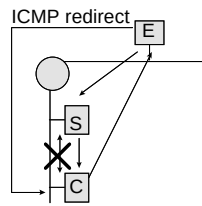
3.12.1997

Markus Peuhkuri / TKK Teletekniikka

32

ICMP redirect

- ◆ Reitiin ilmoittaa sopivamman reitittimen tietyille koneelle
 - useimmat uskovat mitä vain
- ◆ Saadaan lähettämään kaikki k.o. koneelle menevä liikenne toisen koneen kautta
- ◆ Suojautuminen:
 - ei sallita verkon sisään
 - vain k.o. reitin reitittimeltä
 - vain eri verkossa olevalle kohteelle



3.12.1997

Markus Peuhkuri / TKK Teletekniikka

33

Palomuuuri

- ◆ Ei vain joku purkki
- ◆ Turvallisuuspolitiikka
 - määrittää palvelut ja pääsyn niihin
 - yleensä erottaa "turvallisen" ja "turvattoman" osan
- ◆ Perusteet käyttöön
 - haavoittuvien palvelujen suojaaminen
 - hallittu pääsy järjestelmiin
 - keskitetty turvallisuus
 - parempi yksityisyys
 - loki ja tilastot
 - politiikan täytäntöönpano

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

34

Palomuurityypit

- ◆ Pakettisuodin
 - » estää esimerkiksi sisäänsuuntautuvat SYN!ACK-paketit
 - » tietyt protokollat / portit
 - suorituskakyinen
 - ei piilota verkon rakennetta
 - helposti kierrettävissä
 - » pitävä konfigurointi vaikeaa
- ◆ Yhteystason suodin
 - TCP-yhteydet luodaan verkon sisälle ja ulos
 - yhteystason valvonta
 - » kierrettävissä: esimerkiksi irc-yhteydet tunneloidaan telnet-yhteyksille

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

35

Palomuurityypit...

- ◆ Sovellustason palomuuuri
 - jokaiselle sovellukselle oma yhdyskäytävä
 - » estää sovellusten käytön toisella porttinumerolla
 - » läpinäkyvä sovelluksille
 - palvelimet verkon sisään suuntautuvalle liikenteelle
 - piilottaa verkon sisäisen rakenteen
 - » rekisteröimättämiä osoitteiden käyttö
 - mahdollistaa lisäpalvelut
 - » virussuoja, surffausestot
 - kiertotiet: modeemit, sähköpostiviestit, web-sivut
 - sovellus(versio)riippuva

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

36

Yhteydenotot palomuurin sisään

- ◆ Pääte- tai webyhteydet
 - kertakäyttöiset tai haaste-vastauksalasanat
 - » lista tai PIN-suojattu älykortti
 - » ei suojaa yhteyden kaappaamiselta => salatut yhteydet
- ◆ Tiedostojen siirto
- ◆ Modeemiyhteydet
 - takaisinsoitto autentikoinnin lisäksi
- ◆ Yleiset palvelut mielummin palomuurin ulkopuolelle

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

37

Palomuuuri

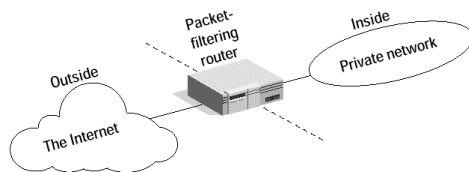
- ◆ Ongelmat
 - vaikeuttaa haluttujen palvelujen käyttöön
 - » sovellusyhdyksyitä ei välttämättä kaikille
 - takaovet olemassa
 - » modeemit
 - pieni suoja organisaation sisältä
 - » osastojen väliset palomuurit

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

38

Pakettisuodin-palomuuuri

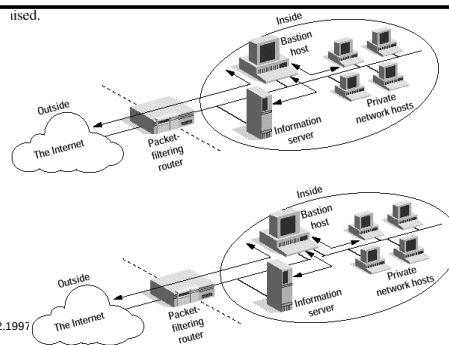


3.12.1997

Markus Peuhkuri / TKK Teletekniikka

39

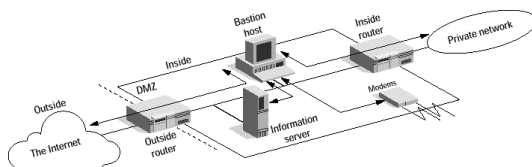
Valvottu kone



3.12.1997

40

Valvottu aliverkko



3.12.1997

Markus Peuhkuri / TKK Teletekniikka

41

Verkkojen yhdistäminen

- ◆ Salattu yhteys palomuurista toiseen
 - toimii vain saman valmistajan laitteiden välillä
 - verkkoon X suuntautuva liikenne ohjataan tunneliin
 - mahdollistaa epäluottettavan verkon käyttämisen yhdistämiseen
- ◆ Etäyhteydet salattuina

3.12.1997

Markus Peuhkuri / TKK Teletekniikka

42



Yhteenveto

- ◆ Ulkoiset liitännät lisäävät verkon arvoa
 - lisäävät turvallisuusriskejä
- ◆ Verkon turvallisuus on yhtä huono kuin huonoin lenkki
 - yhden koneen murtaminen avaa usein pääsyn muihin koneisiin
- ◆ Perussäännöt
 - verkon kriittisten osien ja palveluiden eristäminen
 - varmuuskopiointi
 - pääsyylistojen päivitys ja tarkistus, minimipalvelut
 - ohjelmistojen päivitys
 - salauksen käyttö