Tallinna Tehnikaülikool

12.01.2000

Eksamitöö

aines

Kommunikatsioonivõrgud (rakenduslik käsitlus)

IDK3070

Erki Suurjaak
970772
LAP52

Tallinn 2000

I Referaat

Tehtud teemal "TCP/IP protokollil baseeruvad rünnakud võrguseadmete vastu". Esitatud.

II HTML-lehekülg

Asub aadressil http://www.lap.ttu.ee/erki/

III Ligipääsumeetod IEEE 802.3 CSMA/CD. Kollisioonide avastamine ja vältimine. Võrgu läbilaskevõime võrdlus CSMA/CD ja markeriga siini korral.

IEEE 802.3 CSMA/CD (Carrier Sense Multiple Access with Collision Detect) on leviedastusega (*broadcast network*) - kõik jaamad kuulevad kõiki sõnumeid. Võrk on ühisressurss - kui jaam tahab midagi saata, siis ta kõigepealt kuulab liini peal, kas keegi midagi saadab. Kui hetkel saadab, siis ta ootab mingi teatud ajavahemiku ja püüab uuesti saata. Kui hetkel keegi ei saada, siis on võrguressurss ("eeter" - sellest ka meetodi üldlevinud nimetus EtherNet) vaba ja jaam saadab oma informatsiooni ära. Kui aga juhtub, et kaks jaama tahavad korraga midagi saata, korraga kuulavad "eetrit" ja kuulevad, et on vaba ning saadavad oma informatsiooni ühel ajal ära, siis tekib kollisioon. Kollisioone avastatakse nii, et jaam, kes informatsiooni saadab, samal ajal ka kuulab, mis "eetris" toimub ja kui "eetrist" tuleb mingi muu asi kui see, mis tema sinna saatis, siis saadab ta "eetrisse" "loba" (*jabber*), et ka teised saatvad jaamad saaksid aru, et on toimunud kollisioon. "Loba" saadab välja see jaam, kes on kollisioonile kõige lähemal. Pärast kollisiooni teket ootavad kõik infot edastanud jaamad mõne aja (juhusliku aja) ja siis püüavad uuesti. Kui siis jälle kollisioon tuleb, siis ootavad jälle mõne aja, aga seekord juba pikema, ja proovivad uuesti. Oodatavad ajavahemikud suurenevad eksponentsiaalselt.

IEEE 802.3-l on mitu võimalikku füüsilise kihi varianti :

- 10Base5 - signaliseerimismeetod : põhiribas; ühe segmendi maksimaalne pikkus : 500 m; kasutatav kaabel : 50Ω jäme koaksiaalkaabel; võrgu topoloogia : siin..
- 10Base2 - signaliseerimismeetod : põhiribas; ühe segmendi maksimaalne pikkus : 185 m; kasutatav kaabel : 50Ω peenike koaksiaalkaabel; võrgu topoloogia : siin..
- 1Base5 - signaliseerimismeetod : põhiribas; ühe segmendi maksimaalne pikkus : 250 m; kasutatav kaabel : varjeta bifilaarkaabel (üldiselt tuntud keerupaarina) ; võrgu topoloogia : täht..
- 10BaseT - signaliseerimismeetod : põhiribas; ühe segmendi maksimaalne pikkus : 100 m; kasutatav kaabel : varjeta bifilaarkaabel (üldiselt tuntud keerupaarina) ; võrgu topoloogia : täht..

- 10Broad36 - signaliseerimismeetod : lairibas; ühe segmendi maksimaalne pikkus : 1800 m; kasutatav kaabel : 75Ω koaksiaalkaabel; võrgu topoloogia : täht.

Kõikidel nendel, välja arvatud 1Base5-l, on maksimaalne edastuskiirus 10 Mbit/s (1Base5 - 1 Mbit/s).

Võrdlus markeriga siiniga (Token Bus).

Token Bus (IEEE 802.4) implementeeritakse EtherNetiga sarnaselt - ka seal on jaamad siini peal, ainult et korraldus on teistsugune. Võrk ei ole enam suvaliselt kasutatav ressurss, "eetriaega" antakse jaamadele kindla süsteemi järgi - mööda võrku ringleb ringi marker (*token*) ja ainult see, kelle valduses marker hetkel on, võib saata. Seega jääb täiesti ära probleem, mis CSMA/CD-d kummitab - kollisioonid. Kollisioone ei tule, sest mööda võrku ringleb ainult üks marker. Loomulikult, kui võrgus on mingi "pahatahtlik" jaam, kes võrguliiklust tahtlikult häirib, siis selle vastu aitab ainult võrguadministraatori vahelesegamine.

Markeriga siini korral on maksimaalne läbilaskevõime 10 Mbit/s, AGA see on alati saavutatav (see tegelikult sõltub konkreetsest implementatsioonist. Näiteks arcnetis on 2.5 Mbit/s, kuid, jällegi, konstantselt). IEEE 802.3-l on maksimaalne läbilaskevõime küll 10 Mbit/s, aga see pole reaalsetes tingimustes peaaegu kunagi saavutatav. Kui segmendi peal vähegi rohkem jaamu on, mis kõik ka töötavad, siis edastuskiirus läheb kiiresti väiksemaks. Üks lahendus ongi võrk segmenteerida - jaotada võrk väiksematesse osadesse, nii et ühest segmendist lähevad paketid välja ainult siis, kui nende sihtjaam ei asu selles segmendis. See parandab võrgu läbilaskevõimet.

IEEE 802.3 sobib võrkudesse, kus liiklus toimub sporaadiliselt ja on üksikud tipptunnid.

IV Kommutaatorid (switches). Kommuteeritava ja jaotatava sidekanali erinevus. Virtuaalsed kohtvõrgud VLAN. VPN - Virtual Private Network. Süsteemi Privador lühikirjeldus.

Kommutaator on seade, mis ühendab kaht endaga kõrvuti olevat jaama. Kahe jaama vahel luuakse sideliin, mis läbib kommutaatorit ja selle ühenduse ajaks on kommutaator reserveeritud. Saab luua kommutaatorite võrgu, nii et võrku ühendatud jaamad saavad omavahel luua sidekanaleid ja kommunikeeruda.

Jaotatav sidekanal on näiteks kohtvõrk - kõik jaamad ripuvad ühe kaabli küljes ja eetriaeg on siis ressurss, mida mingil viisil jaamade vahel jaotatakse (näiteks IEEE 802.3 - CSMA/CD, IEEE 802.4 - Token Bus, IEEE 802.5 - Token Ring). Jaotatavas ressursis on üldjuhul igal jaamal unikaalne identifikaator, ühel hetkel tohib eetriaega kasutada ainult üks jaam ja kõik kuulevad iga saadet.

Kommuteeritav sidekanal - kanal on kahe jaama vahel privaatne, teisi seal pole. Sõltuvalt liinist võib saata kas korraga üks (*half duplex, simplex*) või mõlemad (*full duplex*). Näiteks POTS (Plain Old Telephone System) on kommuteeritav - kahe telefoni vahel luuakse ühenduse ajaks kommutaatorite abil sideliin, mida kasutavad ainult nemad.

Jaotatava sidekanali puhul aga kanalit ei reserveerita. Võib olla implementeeritud kahel viisil - kas datagrammide edastus - jaama X poolt saadetav

info jagatakse pakettidesse ja saadetakse mööda võrku mingit moodi kohale (iga pakett võib kohale jõuda erinevat teed pidi) - või virtuaalne kanal - ühenduse loomisel tekitatakse A ja B vahele virtuaalne kanal, mida mööda siis kõik saadetavad paketid liiguvad. Kanalis kasutatud punkte ei reserveerita - samal ajal võivad neid kasutada ka teised jaamad, mis oma virtuaalkanalis pakette vahetavad.

Virtuaalne kohtvõrk (VLAN) käitub võrgusiseste jaamade jaoks täpselt nagu tavaline kohtvõrk (LAN). Tegelikkuses võib iga kohtvõrku lülitatud jaam olla teistest jaamadest tuhandete kilomeetrite kaugusel. Informatsiooni edastuse seisukohalt sellel mingit tähtsust ei ole. Üks meetod virtuaalse kohtvõrgu implementeerimiseks on Virtual Private Network (VPN). VPNi korral seotakse mitmed erinevates kohtades asuvad kohtvõrgud üheks suuremaks kohtvõrguks, kasutades jaamadevaheliseks sidekanaliks Internetti. Kogu side, mis kohtvõrkude vahel toimub, on privaatne, s.o. krüpteeritud.

Üks meetod VPNi implementeerimiseks on AS Cybernetica poolt pakutav süsteem Privador. Privadori korral ühendatakse iga kohtvõrk Internetti krüptomüüriga, mistõttu kohtvõrkude vahel toimuv kommunikatsioon on võõrastele jaamadele mittearusaadav. Kui veel tahetakse, et kohtvõrkudel oleks ka vaba pääs Internetti, siis pannakse ühes kohtvõrgus püsti tulemüür kohtvõrgu ja Interneti vahel (tulemüüri võib täpselt nii konfigureerida, nagu asutuse turvapoliitika nõuab). Oletame, et tulemüür asub kohtvõrgus X. Kui nüüd kohtvõrku Y kuuluv jaam A tahab Internetis mingi jaamaga suhelda, siis ta saadab oma informatsiooni välja. Informatsioon krüpteeritakse krüptomüüris, saadetakse üle Interneti kuni võrgu X krüptomüürini, see dekrüpteerib selle ja saadab kohtvõrku X. Seal jõuab see informatsioon tulemüürini, kes nähes, et informatsiooni sihtaadress on on väljaspool virtuaalset kohtvõrku, saadab selle Internetti (kui see muidugi on lubatud). Kõikide kasutatavate TCP/IP kliendirakenduste jaoks on see toiming ja üldse süsteemi Privador komponendid täiesti läbipaistvad.

V Protokolli ARP (Address Resolution Protocol) - funktsioon ja koht Interneti protokollivirnas.

ARP on meetod IP-protokolli pookimiseks EtherNeti peale. IP-protokollis on jaamade aadressid 32-bitised (IPv4 järgi, varsti tuleb peale IPng), EtherNetis aga jaamade (või õigemini võrgukaartide) aadressid 48-bitised. Seega tuleb seada sisse mingi tabel, kus on igale vajalikule IP-aadressile vastavusse seatud MAC-aadress (EtherNeti aadress). Kui jaam A tahab saata sõnumit jaamale B, aga ta teab ainult tema IP-aadressi, siis ta saadab võrku leviaadressiga paketi (*broadcast*), mis sisaldab B IP-aadressi ja palvet saada B MAC-aadress. Kõik jaamad, mis selle paketi said, võrdlevad oma IP-aadressi paketis oleva IP-aadressiga ja kui need kattuvad, siis antud jaam on jaam B ja ta saadab A-le vastuse, millest A siis saab B MAC-aadressi teada.

Jaamad säilitavad teadasaadud vastavused ARP cache'is, sest iga paketi saatmiseks pole mõtet *broadcast*-i teha. Neid vastavusi ei hoita seal igavesti - sest need võivad muutuda.

ARP-ile vastandprotokolliks on RARP (Reverse Address Resolution Protocol). Seda kasutatakse siis, kui olukord on vastupidine - teada on MAC-aadress, aga on vaja ka IP-aadressi. Siis on käitumine täiesti analoogne, ainult selle vahega, et *broadcast*-paketis on MAC-aadress ja küsitakse IP-aadressi.