

# ISP0040 1. laboratoorse töö teoreetilised alused:

## 1. Üldine kirjeldus

Antud laboritöö eesmärgiks on anda praktilisi oskusi Etherneti standardil põhinevate LAN (Local Area Network) arvutivõrkude projekteerimisest ja koostamisest SOHO (Small Office Home Office) skaalas. Töö käigus tuleb tudengeil koostada lihtsad arvutivõrgud erinevate skeemide alusel ja häälestada võrgus olevad arvutid ja lisaseadmed (ruuter) vastavalt labori ülesannetele.

## 2. Kasutatavad seadmed:

- 3 personaalarvutit Windows XP operatsioonisüsteemiga
- ruuter (sobilik kasutamiseks SOHO võrkudes)
- ühenduskaablid

## 3. Ülesanded

Laboritöö ülesanded on kasvava keerukusega. Iga järgnev ülesanne eeldab eelmise ülesande lahendamist ja vastavate teadmiste omandamist. Laboritöö edukaks sooritamiseks peab tudeng oskama vastata järgnevatele küsimustele:

1. Mis on Ethernet otse- ja ristkaabli erinevus ja kus neid kasutatakse?
2. Mis on IP (Internet Protocol) aadress? Milleks on seda vaja?
3. Kuidas saab muuta WinXP operatsioonisüsteemiga arvutis võrguseadistusi?
4. Kuidas ja milleks kasutatakse WinXP võrgudiagnostika baasutiliite “ping” ja “ipconfig”?
5. Milline on DHCP (Dynamic Host Configuration Protocol) serveri töö üldine põhimõte?
6. Mis on NAT (Network Address Translation) ja kuidas see töötab?
7. Mis on veebiserver? Kuidas see töötab? Milleks on veebiserverit vaja?
8. Mis on ruuter ja milleks seda kasutatakse? Kuidas ruuterit häälestada, taaskäivitada (restart) ja alglähtestada (reset)?

## 4. Lühikokkuvõtte toereetilisest alustest. Täpsem info iga lõigu kohta on leitav loengu- ja muudest materjalidest.

### 4.1. Ethernet LAN

Ethernet LAN on standard, mis on kasutusel väikses füüsilise ulatusega võrkudes. Standard defineerib võrkude ISO/OSI 7 kihilisel mudelis 2 madalamat kihti (1, 2)

### 4.2. Võrguadapter (võrgukaart)

Seade, mis võimaldab ühendada arvuti arvutivõrku. Antud laboris on tegemist PC arvuti sisese võrgukaardiga, mis paikneb arvuti korpuse sees ühendatuna emaplaadi PCI siinile. Ethernet standardile vastavate võrgukaartide ühiseks tunnuseks on reeglina väline liides Ethernet võrgukaablitele. Laboris kasutame keerupaari võrgukaableid. Selleks, et arvutis kasutatav operatsioonisüsteem saaks võrgukaarti kasutada on tavaliselt vaja võrgukaardi ohjurprogramme (draivereid) konkreetse operatsioonisüsteemi tarbeks. Laboris kasutatavatel arvutitele on need juba paigaldatud.

### 4.3. Võrgukaabel

Ethernet võrkudes on põhiliselt kasutusel 3 tüüpi võrgukaableid. Ajalooliselt vanimad neist on

koaksiaalkaablid. Enimlevinud kaablitüüp on keerupaari kaabel, mis sisaldab 4 erineva sammuga kokku keeratud juhtme paari (kokku 8 juhet). Kasutatakse veel ka optilisi kaableid. Standardis lubatud keerupaari kaablisegmendi suurim pikkus on 100m ning ühenduseks kasutatakse 8 kontaktiga RJ45 standardile vastavaid pistikuid. Võrguseadmetes ja arvutite võrgukaartides on vastavalt RJ45 pesad. On defineeritud kaks standardit pistikute ja kaabli omavaheliseks ühenduseks: TIA-568A ja TIA-568B. Full-duplex režiimis 10 ja 100 Mbps kiirusega võrkudes on 4-st paarist kasutusel 2: üks paar signaali saatmiseks, teine vastuvõtuks. Kui arvuti võrgukaart on kaabli abil ühendatud mõne võrguseadmega (hub, switch), siis kasutatakse võrgukaablit kus mõlemad otsad on ühendatud kas TIA-568A või TIA-568B skeemi järgi (otsekaablit). Kui aga ühendatakse kaks võrguseadet omavahel või kaks arvu tit omavahel, siis kasutatakse kaablit kus erinevad otsad on ühendatud erinevate (A ja B) standardite järgi (ristkaablit). Enamik tänapäevaseid võrguseadmeid (switch, hub) omavad automaatset kaablituvastamise mehhanismi ja töötavad edukalt nii rist- kui otsekaablitega.

#### 4.4. IP address

IP võimaldab koostada võrgu, mis koosneb väiksematest osavõrkudest mis on omavahel ühendatud lüüsidega (gateway). Internet ongi näide sellisest võrkude võrgust, kus kõigis alamvõrkudes on kasutusel IP. IP aadress on võrgusõlme (arvuti või võrguseadme) unikaalne identifikaator terves võrgus. IP aadressi pikkus on 4 baiti e. 32 bitti. See võimaldab kasutada kokku  $2^{32}=4\,294\,967\,296$  erinevat aadressi. Tänapäeval jääb veidi üle 4-st miljardist aadressist väheks ja igale IP võrku toetavale seadmele ei jätku unikaalset aadressi. IP aadress on jagatud kaheks osaks: võrguosa ja võrgus oleva seadme osa. Võrguosa suuruse määrab alamvõrgu mask (subnet mask). Kahendsüsteemi kujul alamvõrgu maski väärtusega 1 bitikohad on võrguaadressi bitikohad. Kahendsüsteemi kujul alamvõrgu maski väärtusega 0 bitikohad on seadme aadressi bitikohad. Ühes võrgus (kui IP aadressi võrguosa on sama) saavad arvutid ja võrguseadmed suhelda vahetult. Erinevate võrkude vahel info liikumiseks saadetakse pakett algul kindlale „oma“ võrgu arvutile või seadmele – lüüsile (gateway), mis siis omakorda saadab paketi edasi vajalikku sihtvõrku. IP aadress, kus kõik seadmeosa bitid on 0, on võrguaadress. IP aadress, kus kõik seadmeosa bitid on 1, on võrgu leviaadress (broadcast). Kui IP võrku pole plaanis ühendada interneti ega teiste IP võrkudega, siis võib seadmetel kasutada suvalisi IP aadresse. Laboriülesannete puhul tuleb võrk ühendada internetiga ja siis on lubatud kasutada vaid neid IP aadresse mis kuuluvad privaatsete IP aadressite hulka (Tabel 1).

Klass	Alamvõrgu mask	Aadressvahemik
A	255.0.0.0 (/8)	10.0.0.0 kuni 10.255.255.255
B	255.255.0.0 (/16)	172.16.0.0 kuni 172.31.255.255
C	255.255.255.0 (/24)	192.168.0.0 kuni 192.168.255.255

Tabel 1: Privaatsete IP aadressite vahemik

#### 4.5. Ruuter

Seade või arvuti, mis on füüsiliselt ühendatud kahe IP võrguga ja võimaldab piianguteta või piirangutega liiklust ühest võrgust teise. Laboris kasutatavat ruuterit võib käsitleda kui kahe võrguliidesega (LAN ja WAN liidesed) arvutit. LAN liideses on ruuterisse sisse ehitatud 4 pordine switch, mille tulemusena saab ruuteri külge ühendada 5 võrgukaablit. 4 neist ühenduvad ruuteri sees tegelikult kõik ühte - LAN liidesesse. Ruuteri tööks on vajalik mõlema liidese IP seadistuste (aadress jms.) korrektne häälestus. Ruuteritel on tavaliselt olemas mingi füüsiline mehhanism püsivara algseadete taastamiseks (reset) ja taaskäivitamiseks (restart). See on iga ruuteri mudeli puhul erinev ja on täpselt kirjas ruuteri kasutusjuhendis.

## 4.6. NAT

Mehhanism, mis muudab IP paketi päises aadresse ja TCP ning UDP päistes porte vastavalt eeldefineeritud reeglitele. Kasutatakse põhiliselt IP aadressite puuduse leevendamiseks. Enamikel internetiga ühendamiseks kasutatavatel ruuteritel on püsivaras NAT funktsioon mingil kujul realiseeritud. Eristatakse 2 tüüpi NAT funktsiooni lähtudes esimesena muudetavast aadressist: sNAT (source NAT) ja dNAT (destination NAT).

### 4.6.1. sNAT – tihti kasutatakse lihtsalt terminit NAT.

Sel juhul muudab ruuter ühest pordist (laboris LAN) saabuva ja teisest pordist (laboris WAN) väljuva IP paketi (nt. HTTP päring) lähteadressi pärast saabumist võrdseks enda väljasaatva pordi (laboris WAN) IP aadressiga. Siit ka nimi – esimesena muudetakse lähteadressi (source address). Modifitseeritud lähteadressiga pakett saadetakse välja teisest pordist (laboris WAN) ja jõuab sihtpunkti. Sihtpunktis olev adreess vastab teise (vastus)paketiga, kus lähetaadressiks on tema enda aadress, kuid sihtaadressiks hoopis ruuteri, mitte paketi tegeliku allika aadress (sest ruuter muutis esimese paketi lähetaadressi enda omaks ja sinna saadetakse ka vastus). Pakett jõuab ruuteri (laboris WAN) porti. Ruuter, mis avastab (laboris WAN) pordist endale adreseedud paketi leiab enda sisemisest mälust eelneva muutmise kirje ja muudab selle alusel nüüd juba teise paketi sihtaadressi esimese paketi lähteadressiga võrdseks ning saadab paketi välja vastavast (laboris LAN) liidesest. Tulemusena ei „näe“ esimene (laboris LAN võrgus olev) arvuti võrguliikluses mingit anomaaliat. Tema jaoks on ruuteris toimunud sNAT täiesti „läbipaistev“. Paketi sihtpunkt (laboris WAN pordiga ühendatud arvuti) aga „näeb“ et saabuval päringul tulevad vaid ruuteri (laboris WAN) pordi IP aadressilt. Ruuteri „taga“ olevad arvutid (mis on tegelikud päringute allikad) jäävad tänu sNAT mehhanismile täiesti „peidetuks“ ja nn. sisevõrku. Välisvõrgust (laboris WAN pordi küljes olevast võrgust) ei õnnestu sNAT funktsiooniga ruuteri kaudu sisevõrgu arvuteid otse adreseedida.

Kuna esimene aadressi muundamine toimub skeemiga mitu (ükskõik milline sisevõrgu aadress) üheks (üks konkreetne ruuteri välisvõrgu pordi IP aadress) ning sNAT- ja salvestusalgoritm on SOHO ruuteritel tavaliselt fikseeritud, siis ei vaja sNAT tavaliselt erihäälestust (laboris kasutatavas ruuteris pole see võimalik). Piisab vaid sNAT süsteemi lülitamisest häälestusliidese kaudu. Vaikimisi on seadistustes on SOHO ruuteritel sNAT tavaliselt sisse lülitatud.

### 4.6.2. dNAT – tihti kasutatakse terminit „pordi suunamine“ (port forwarding) või virtuaalserver (virtual server)

Toimemehhanism on sarnane sNAT skeemile, kuid erinevusega, et esimesena muudetakse ühel, teatud tingimutele vastaval, paketil sihtaadress ja seejärel saabuval teisel paketil, vastassuunal liikuvast vastusel, lähteadress. Skeem on vajalik, kui soovetakse „näidata“ kasutuses oleva sNAT funktsiooniga ruuteri taga sisevõrgus olevat serverit (nt. veebiserver) välisvõrgu arvutitele. dNAT pöördub välisvõrgu arvuti ruuteri välise IP aadressi poole ja talle tundub, et vastused saabuval samalt aadressilt st. justkui oleks ruuteri asemel mingi server.

SOHO väikevõrkudes pole dNAT tavaliselt vajalik ja on seetõttu enamikel ruuteritel vaikeväärtusena välja lülitatud. Sisse lülitamiseks vajab teenus eraldi seadistust, sest esimene sihtaadressi muutus pole ühene – üks ruuteri väline IP aadress võib transleeruda (vastavalt seatud reeglitele) suvalise sisevõrgu arvuti IP aadressiks.

## 4.7. Tulemüür

Filter, mis piirab sisse- ja väljaminevat võrguliiklust võrguseadme või arvuti võrguliideses. Kasutatakse ebasobiva liikluse kõrvaldamiseks, eesmärgiga säästa filtri taga oleva seadme resursse, pakkuda turvalisust või piirata ligipääsu.

## 4.8. DHCP

Protokoll, mis defineerib automaatse IP seadete edastamise. IP seadeid DHCP klientprogrammidele jagab DHCP server. Laboris kasutatavates ruuterites on DHCP serveri funktsioon sisse ehitatud. Ruuteri seadistusliidese kaudu saab DHCP serveri tööd häälestada.

## 4.9. DNS (Domain Name System)

Mehhanism, mis seab numbrilisele IP aadressile vastavusse loetava nime. Nime ja IP aadressi vastavust „teab“ DNS server. Kui mõni arvuti või võrguseade pöördub nimelise aadressi poole, siis esiteks pärib see seade DNS serverist nimelisele aadressiel vastava IP aadressi ja pöördub seejärel juba õigele IP aadressile. DNS serverite koormuse vähendamise huvides salvestavad DNS päringu teele jäävad DNS serverid ja klientseadmed DNS kirjeid ajutiselt kohalikku mällu (DNS cache).

## 4.10. Veebiserver

Programm või seade, mis kuulab ja oskab vastata HTTP (Hyper-Text Transfer Protocol) päringutele ja mis tavaliselt vahendab ligipääsu failisüsteemile või seadme sisemistele resurssidele üle HTTP. Laboris kasutame Apache veebiserverit, mille dokumentide juurkataloog (document\_root) on vaikumisi kataloogis „E:\Program Files\Apache Software Foundation\Apache2.2\htdocs“

## 4.11. WinXP operatioonisüsteemi võrguhäälestuste asukoht

WinXP võrguliideste nimiekirja asukoht on leitav järgnevalt:

Start -> Control Panel -> Network Connections

Võrguliidese parameetrite seadistuseks tuleb vajutada paremat nuppu vastava liidese nime peal ja valida lühimenüüst valik „properties“. Avanenud aknast tuleb valida TCP/IP rida ja seejärel vajutada nupule „properties“. Automaatse seadistuse valik tähendab DHCP kasutamist.

Varuavariandina rakendatakse APIPA aadressi määramise skeemi.

## 4.12. WinXP IP võrguseadete silumise baasutiliidid „ping“ ja „ipconfig“

WinXP operatioonisüsteemi koosseisus on mitmeid võrgu häälestuse muutmise ja silumise utiliite. „ipconfig“ võimaldab vaadata kehtivaid IP võrguseadeid ja neid uuendada. Kasutamiseks tuleb käsureale sisestada käsk „ipconfig“. Rohkem infot saab ,kui lisada käsule järgi võti „/all“. Käsk „ping <ip\_aadress>“ saadab võrgusõlmele aadressiga <ip\_aadress> ICMP (Internet Control Message Protocol) tüüp 8 (Echo Request) paketi ja näitab vastuse – ICMP tüüp 0 (Echo Reply) paketi saabumiseks kulunud aega. Kui vastust teatud aja jooksul ei saabu, siis võib järeldada, et vähemalt üks kahest paketist ei jõudnud adreessaadini ja IP tasemel side kahe võrgusõlme vahel puudub.