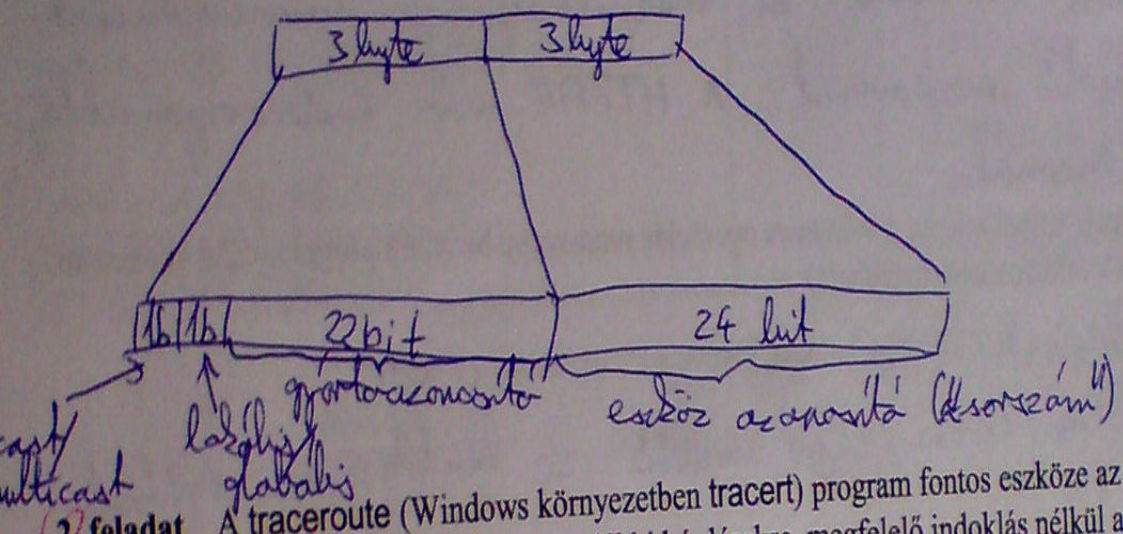
0	17	1
18	24	2
25	31	3
32	38	4
39	46	5

1. feladat Ismertesse az Ethernet címek szerkezetét, a címek típusait! (4 pont)

Az ethernet címek 48 bitesek.



2. feladat A traceroute (Windows környezetben tracert) program fontos eszköze az IP alapú hálózatokban előforduló egyes hibák meghatározásának. Válaszoljon az alábbi kérdésekre, megfelelő indoklás nélkül a válaszok nem fogadhatók el!

a) Mit tesz lehetővé a traceroute? (1 pont)

Egy útvonal feldertését két állomás között, illetve a köztes állomások címének és válaszidejének megismerését.

b) Az IP fejrész milyen mezőjét és hogyan használja a traceroute a működése során? (2 pont) 1p

TTL (time to live): a célállomás címét pingelő folyamatosan növekvő TTL értékek mellett, így a válaszban az adott hálózaton lévő állomás címét kapjuk meg.

c) Mi történik, ha a traceroute által megszólított állomás ki van kapcsolva, vagy az általa üzemeltetett tűzfal beállítása miatt nem válaszol a traceroute által küldött csomagokra? (1 pont) 0,5 p

Az állomáshoz küldött ping timeout-tal ("*") válasszal.

d) A traceroute működése során milyen további TCP/IP protokollokat használ a rendszer? (1 pont)

ethernet, felette IP, felette ICMP (Internet Control Message Protocol)

NÉV: .. .. Neptunkód: .....

3. feladat Válaszoljon az alábbi kérdésekre! Indoklás nélkül a válaszok nem fogadhatók el!

a) Milyen megoldások léteznek a HTTP-ben arra, hogy a felhasználó információkat küldjön paraméterként a szerveren futó programoknak, és ezek a megoldások milyen formában teszik lehetővé a paraméterátadást? (2 pont)

(2) GET: a request url mezőjében küldi az adatot
POST: a request HTTP fejlécben küldi az adatokat

b) Milyen beépített megoldások teszik lehetővé a HTTP-ben felhasználók azonosítását, és azok milyen formában viszik át a felhasználó által megadott felhasználói adatokat (felhasználó név és jelszó)? (2 pont)

(2) HTTP basic: a 401-es üzenetre a kliens válaszában elküldi az adatokat base64 kódolásban (titkosítatlanul)
digest: a 401-es üzenetre válaszként csak az adatok MD5 hash-ét küldi el.

c) Biztonságosak a HTTP beépített felhasználói azonosítást végző módszerei, ha egy harmadik fél le tudja hallgatni (pl. Wiresharkkal) a felhasználó és a szerver közötti kommunikációt? (1 pont)

(0) a HTTP nem titkosít, harmadik fél lehallgathatja a kommunikációt bármilyen hálózatfigyelő programmal. A HTTPS már biztonságosabb, mert SSL-t használ.

4. feladat Az alábbi hálózati problémák esetén milyen a Windows operációs rendszerbe beépített programokkal keresné meg a hiba okát, és miért? (Indoklás nélkül a válaszok nem fogadhatók el.)

a) A számítógépen egyáltalán nem működik a TCP/IP alapú hálózat, kivéve a localhost-ot. (1 pont)

(1) ipconfig /all → megnézném, jól van-e beállítva a hálózat

b) A gépen csak IP címmel érhető el a többi gép, domain névvel nem. (1 pont)

(1) nslookup → megnézném, működik-e a DNS
VAGY ping <DNS szerver címe> → elérhető-e a DNS szerver?

c) A teljes hálózat időnként nem működik, a weblapok nem letölthetőek, a VoIP akadozik. (2 pont)

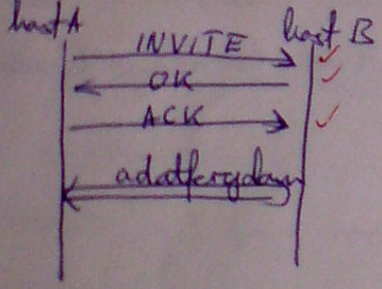
(2) netstat -noa → valaki foglalja-e a 80-as portot?
ping <default gateway> → elérhető-e a default gateway?

d) Bizonyos szerverek időnként nem működnek, a weblapok nem letölthetőek, a VoIP akadozik. (1 pont)

(1) megpingelném a problémás szervereket, tracert-vel megnézném a közelebbi állomások válaszidejét.

5. feladat VoIP

a) Vázolja fel egy SIP kapcsolat felépítését két telefon között! (2 pont)



(de OK előtt B→A adhat egy TRYING ✓ üzenetet is, ha a válaszidő > 200 ms)

2

NÉV: ..... Neptunkód:

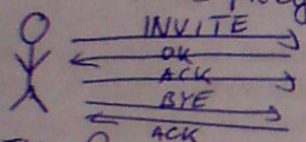
b) Az alább látható INVITE üzenethez jelölje meg azt az üzenetet, amelyik azzal egy kommunikációban szerepelhetett. A VoIP kapcsolatban a *sip:pityu@152.66.254.209* és a *sip:ph@152.66.254.228* felek vettek részt. Több jó válasz esetében jelölje meg mindet! (2 pont)

INVITE

```
INVITE sip:ph@152.66.254.228 SIP/2.0
From: <sip:pityu@152.66.254.209>
To: <sip:ph@152.66.254.228>
Via: SIP/2.0/UDP 152.66.254.209
Contact: <sip:pityu@152.66.254.209>
Call-ID: 143
CSeq: 1 INVITE
Content-Type: application/sdp
Content-Length: 119
Max-Forwards: 70

v=0
o=- 4 0 IN IP4 152.66.254.209
s=-
t=0 0
c=IN IP4 152.66.254.209
m=audio 8500 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

(nincs proxy)



PITYU @ ...209 PH @ ...228

C és D üzenet helyes!

A)
```
ACK sip:ph@152.66.254.228 SIP/2.0
From: <sip:pityu@152.66.254.209>
To: <sip:ph@152.66.244.228>
Via: SIP/2.0/UDP 152.66.254.228
Call-ID:143
CSeq: 101 ACK
Content-Length: 0
Max-Forwards: 70
```

B)
```
BYE sip:pityu@152.66.254.209 SIP/2.0
Via: SIP/2.0/UDP 152.66.254.228
From: <sip:ph@152.66.254.228>
To: <sip:pityu@152.66.254.209>
Call-ID: 144
CSeq: 101 BYE
Max-Forwards: 70
Content-Length: 0
```

√ C)
```
BYE sip:pityu@152.66.254.209 SIP/2.0
Via:SIP/2.0/UDP 152.66.254.228
From: <sip:ph@152.66.254.228>
To: <sip:pityu@152.66.254.209>
Call-ID: 143
CSeq: 101 BYE
Max-Forwards: 70
Content-Length: 0
```

√ D)
```
ACK sip:ph@152.66.254.228 SIP/2.0
From: <sip:pityu@152.66.254.209>
To: <sip:ph@152.66.244.228>
Via: SIP/2.0/UDP 152.66.254.209
Call-ID: 143
CSeq: 101 ACK
Content-Length: 0
Max-Forwards: 70
```

1

c) Egy LAN-on a SIP URI-jukkal megadott két fél közötti beszédforgalmat szeretnénk lehallgatni. Hogyan tudná kiválogatni az RTP csomagok közül azokat, amelyek a megadott két felhasználó közötti beszédkapcsolat részét képezik? Mit gondol, a kinyerhető adatok alapján vissza tudná állítani az elhangzott beszélgetést? Indokolja! *(2 pont)* 1,5

Megfigyelném a SIP INVITE utáni ACK csomagot → innen indul a kommunikáció
a SIP BYE üzenettel zárul a kommunikáció
a kettő között zajlik a forgalom (RTP csomagok)

A SIP üzenetből a hanganyagra vonatkozó minden többlet információ kinyerhető. Amennyiben az átvitel nincs titkosítva, a beszélgetés egyszerűen elvégezhető.

6. feladat Sávszélesség számolása

a) Mekkora a PCM A-law kódoló által igényel sávszélesség az IP szinten, ha 20 ms-os időhossz csomagolás technikát alkalmazunk? És UDP szinten? A kódolóról tudjuk, hogy 64 kbps sebességgel működik, azaz 0,125 ms-ként 1 bytos mintákat készít. *(2 pont)* 2

IP fejléc	UDP fejléc	RTP fejléc
20 byte	8 byte	12 byte

$\frac{1000\,ms}{20\,ms} = 50$ csomag/sec

IP: 50 db · 40 byte header = 16 kbit/sec
összes: 64 kbit adat + 16 kbit header = 80 kbit/sec

UDP: 50 db · 20 byte header = 8 kbit/sec
összes: 64 kbit adat + 8 kbit header = 72 kbit/sec

b) Egy ismeretlen beszédkódolóról azt tudjuk, hogy 8 kbps sebességgel működik. Kiszámoltuk UDP szinten a sávszélesség igényét, ami 16 kbps-nek adódott. Mekkora a beszédforgalom sávszélesség igénye az IP szinten? *(1 pont)* 1

16 kbps − 8 kbps = 8 kbps header overhead

Mivel az IP header kétszer akkora → IP szinten 16 kbps header overhead lesz.

Tehát 8 kbps adat + 16 kbps header = 24 kbps forgalom összesen. ✓

NÉV: ..... Neptunkód:

7. feladat Biztonsági entitások azonosítása a Windowsban

a) Mire szolgál a SID a Windowsban? Hogyan épül fel egy felhasználó és egy csoport SID-je? Miben különbözik egy általunk létrehozott felhasználó és a Mindenki csoport SID-je? (4 pont)

1 A SID a felhasználót azonosító ID. A csoport SID is. Így néz ki:
(1-2-5-xxxxxxx) A felhasználó SID=a csoport SID + 1
(1-2-5-xxxxxxx - 1000) Az általunk létrehozott felhasználók általában 1000-től kezdődnek.

b) Egy külső merevlemez egy könyvtárára beállítjuk, hogy csak a saját felhasználónk legyen joga hozzá. Rákötve a merevlemezt egy másik gépre, azon nem tudjuk megnyitni az adott könyvtárat, holott a második gépen is ugyanaz a felhasználónk és jelszavunk, mint az elsőn. Miért? (2 pont)

1 A két gépen különböznek a SID, a felhasználót pedig ez azonosítja.
Az ACL-ben csak felhasználóhoz és nem csoporthoz állítjuk a hozzáférést, emiatt nem működik.

8. feladat Igazak vagy hamisak az alábbi kérdések? (Karikázza be az IGEN vagy a NEM szót!)
(Helyes válasz=**1 pont**, hiányzó válasz=**0 pont**, **hibás válasz= -1 pont**.)

0 a) IGAZ HAMIS A winlogon.exe az első felhasználói módú folyamat, ami elindul egy Windowsban.

1 b) (IGAZ) HAMIS Windowsban a gépen lévő felhasználónevek és jelszavak a rendszerleíró adatbázisban tárolódnak.

1 c) (IGAZ) HAMIS A Local System felhasználó még az Administrator felhasználónál is több joggal rendelkezik alapértelmezés szerint.

1 d) IGAZ (HAMIS) Windowson minden futó folyamathoz pontosan egy darab hozzáférési token tartozik.

9. feladat Milyen UNIX naplófájlokat ismer, és mik találhatók bennük? (Elég hármat felsorolni.) (4 pont)

0

10. feladat Mit eredményez a "ps -ef | grep root" UNIX parancs? (4 pont)

A ps -ef kilistázza a folyamatokat és hogy ki indította őket (kinek a nevében futnak).
4 Ezután a grep root kiszűri azokat a sorokat (folyamatokat), amelyek nevében "root" szerepel vagy a tulajdonosának neve "root".

~~Jó esetben tehát a root neve alatt futó folyamatokat listázza ki.~~