

Retele de calculatoare – Informatica anul 3 (2019-2020)

Note de Laborator
Retele de calculatoare

Specializare: Informatica anul 3

Contact:
retelecdsd@gmail.com
<http://www.cdscd.ro>

Comunicatii de
Date si
Sisteme
Distribuite



<http://www.cdscd.ro>

Laborator 2

1. Obiective:

- Intelegerea rolului protocoalelor in retelele de calculatoare
- Identificarea nivelelor modelelor OSI si TCP/IP.
- Analiza conectivitatii si traficului dintr-o retea folosind utilitare si programe specializate
- Programarea in Python/ Aplicatii de retea
- Introducere **Riverbed Modeler Academic Edition** (versiune actuala a Opnet-ului - **Optimized Network Application and Network Performance**) – mediu de simulare a retelelor de calculatoare (**Varianta C++**: OMNeT++ Network Simulation Framework
<http://www.omnetpp.org/>)

2. Consideratii teoretice

2.1. Protocoale de comunicatie. Modelul TCP/IP (Transmission Control Protocol/Internet Protocol)

Pentru ca pachetele de date sa parcurga drumul de la sursa la destinatie intr-o retea, este important ca oricare dintre dispozitivele de retea sa “vorbeasca aceeași limbă” ... protocol. Astfel, un **protocol de comunicatie** corespunde unui **set de reguli care determina formatul si transmitia datelor, controland aspecte legate de :**

- **“Constructia” rețelei.**
- **Modul de conectare a calculatoarelor/hosturilor in retea.**
- **Formatul si transmiterea datelor.**
- **Rezolvarea erorilor, etc**

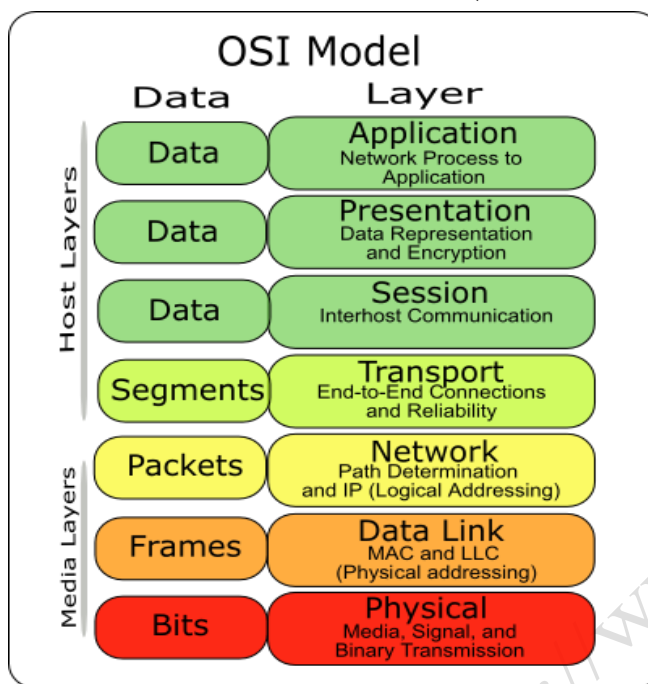
Protocoalele sunt create si mentinute de diferite comitete sau organizatii cum ar fi: Institute of Electrical and Electronic Engineers (**IEEE**), American National Standards Institute (**ANSI**), International Organization for Standardization (**ISO**), etc.

In Internet standardul tehnic, implementat software, il reprezinta suita de protocoale **TCP/IP** (Transmission Control Protocol/Internet Protocol). Acesta este dezvoltat ca un **standard deschis** putand fi folosit in mod liber.

Modelul TCP/IP (model simplificator!!!!) cuprinde 4 niveluri (layers-straturi) de ierarhizare (fata de cele 7 ale modelului OSI-Open System Interconnection):

Modelul OSI	Modelul TCP/IP	Protocoale
Application	Application	Telnet, SSH SMTP, POP, IMAP FTP, TFTP, NFS HTTP DNS
Presentation		
Session		
Transport	Transport	TCP, UDP
Network	Internet	IP, ICMP, ARP, RARP
Data Link	Network Access	Internet, Ethernet, FDDI, ATM SLIP, PPP ARP, RARP
Physical		

Retele de calculatoare – Informatica anul 3 (2019-2020)



- **Nivelul Acces Retea (Network Access)**

Gestionează conexiunea la mediul fizic al rețelei indiferent de tehnologia folosită. Include nivelul Legatură de Date (Data Link) și Fizic (Physical) al modelului OSI.

- **Nivelul Internet (Internet)**

Asigură rutarea pachetelor de date la destinație determinând cel mai bun drum și comutarea de pachete. Protocolul determinant de pe acest nivel este Internet Protocol (IP).

- **Nivelul Transport (Transport)**

Oferă servicii de transport între punctul sursă și punctul destinație. De asemenea, asigură controlul fluxului de date, corectarea erorilor și calitatea serviciilor. Cele două protocoale de pe acest nivel sunt: Transmission Control Protocol (TCP) și User Datagram Protocol (UDP). TCP este un protocol orientat pe conexiune, garantându-se recepția informației la destinație așa cum a fost transmisă. Se asigură astfel o comunicare stabilă și fără erori. Spre deosebire de TCP, protocolul UDP nu necesită stabilirea unei conexiuni cu destinatarul, fiind un protocol neorientat pe conexiune.

- **Nivelul Aplicație (Application)**

Asigură reprezentarea corectă a datelor. Acest nivel include nivelele Sesiune (Session), Prezentare (Presentation), și Aplicație (Application) ale modelului OSI (Open System Interconnection). Există o serie de protocoale la acest nivel:

- Telnet, SSH (Secure Shell) (conexiune remote nesigură/sigură)
- Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), Internet Message Access Protocol (transmiterea și recepționarea mesajelor)
- File Transfer Protocol (FTP); Trivial FTP (TFTP) (transferul de fișiere)
- Hyper Text Transfer Protocol (HTTP) pentru www,
- Domain Name System (DNS) pentru rezolvarea numelor de domeniu, etc. Obs: Fiecare din aceste protocoale are asociat un număr de port de comunicație (0-1023; 1024-49151; 49152-65535)

Retele de calculatoare – Informatica anul 3 (2019-2020)

2.2. Comenzi Windows/Unix

Windows Command Reference: <http://www.gatepoint.ch/cmdreferenz//index.html>

2.2.1. Comanda ping

Unix

NUME

ping - trimite pachete ICMP ECHO_REQUEST catre sisteme din retea

SINOPTICA

ping [-**dfnqrR**] [-**c** numar] [-**i** interval] [-**l** preincarcare] [-**p** model]

DESCRIERE

Ping utilizeaza datagrame obligatorii *ECHO_REQUEST* ale protocolului *ICMP* pentru a obtine datagrame *ICMP ECHO_RESPONSE* de la o gazda sau de la o pasarela. Datagramele *ECHO_REQUEST* ("ping-uri") au un antet IP si *ICMP*, urmat de o structura "timeval" si de un numar arbitrar de octeti "pad" utilizati pentru a umple pachetul. Optiunile posibile sint urmatoarele:

-c numar

Se opreste dupa trimiterea (si receptionarea) de *numar* pachete *ECHO_RESPONSE*.

-d

Seteaza optiunea *SO_DEBUG* pentru socket-ul ce este folosit.

-f

Transmisie in masa de pachete ping (flood ping). Emite pachete cu viteza cu care se intorc inapoi sau de 100 de ori pe secunda, care oricum este mult. Pentru fiecare pachet *ECHO_REQUEST* trimis este afisat un punct ".", in timp ce pentru fiecare pachet *ECHO_REPLY* receptionat este tiparit un caracter Backspace. Aceasta determina o afisare rapida a marimii de pachete pierdute. Numai root poate utiliza aceasta optiune. *Acesta actiune poate fi foarte deranjanta intr-o retea si trebuie utilizata cu multa grija.*

-i interval

Asteapta *interval* secunde *dupa transmisia fiecarui pachet*. Implicit se asteapta o secunda. Aceasta optiune este incompatibila cu optiunea **-f**.

-l preincarcare

Daca este specificat *preincarcare*, **ping** trimite pachete cit poate de rapid, inainte de a intra in regimul normal de lucru. Numai root poate utiliza aceasta optiune.

-n

Numai rezultate numerice. Nu se va incerca transformarea numelor simbolice pentru adresele gazdelor.

-p model

Puteti specifica pina la 16 octeti "pad" pentru a umple pachetul de trimis. Aceasta este utila pentru diagnosticarea problemelor de retea ce depind de structura datelor. De exemplu, *-p ff* va determina umplerea pachetului numai cu biti de 1.

Retele de calculatoare – Informatica anul 3 (2019-2020)

-q

Afisare sumara. Nu este afisat nimic, cu exceptia liniilor sumar de la executia si de la sfirsitul ping-ului.

-R

Inregistreaza ruta. Include in pachetul *ECHO_REQUEST* optiunea *RECORD_ROUTE* si afiseaza buffer-ul de rutare la pachetele raspuns. De notat ca antetul IP este suficient numai pentru 9 asemenea rute. Multe gazde ignora sau rejecteaza o asemenea optiune.

-r

Ignora tabelele normale de rutare si trimite pachetul direct la gazda atasata la retea. Daca gazda nu este direct atasata la retea este generata o eroare. Aceasta optiune poate fi utilizata pentru a trimite ping la o interfata locala care nu are nici o ruta catre ea (de exemplu dupa ce interfata a fost scoasa de sub controlul lui *routed(8)*).

-s *marime_pachet*

Specifica numarul de octeti de date de trimis. Implicit este 56, care se va transla intr-un pachet *ICMP* de 64 de octeti atunci cind se combina cu 8 octeti din datele antetului *ICMP*.

-v

Afisare detaliata. Sint afisate si pachetele *ICMP* altele decit cele *ECHO_RESPONSE*.

Cind se utilizeaza **ping** pentru izolarea defectelor, el ar trebui rulat mai intii pe gazda locala pentru a verifica faptul ca interfata de retea locala este activa si functioneaza corect. Dupa aceea, se poate trimite ping catre gazde si pasarele din ce in ce mai distante. Sint calculate timpul dus-intors si statisticile de pierderi. Daca sint receptionate pachete duplicate, ele nu sint incluse in calculul pierderilor, dar totusi timpul dus-intors este considerat in calculul timpilor dus-intors minim/mediu/maxim. In momentul in care s-a terminat numarul de pachete trimise (si receptionate) sau programul s-a terminat cu semnalul *SIGINT*, este afisat un sumar al rezultatelor.

Daca **ping** nu primeste nici un raspuns la pachetele trimise el se va termina cu codul de retur 1. La aparitia unei erori returneaza valoarea 2. In celelalte cazuri genereaza un cod de retur 0. Acest lucru permite sa determinati daca o gazda este in functiune sau nu, numai prin analiza codului de retur.

Acest program are scopul de a fi utilizat in testarea, administrarea si masurarea retelelor. Din cauza incarcarii pe care o genereaza in retea, este de nedorit sa utilizati **ping** in timpul operatiilor normale sau din scripturi automatizate.

DETALIILE PACHETULUI ICMP

Un antet IP fara optiuni are 20 octeti. Un pachet *ICMP ECHO_REQUEST* contine 8 octeti aditionali pe linga cei din antetul *ICMP*, urmati de un numar arbitrar de date. Cind este data optiunea *marime_pachet*, aceasta indica marimea blocului de date suplimentare (implicit este 56). Astfel, cantitatea de date dintr-un antet de pachet IP de tipul *ICMP ECHO_REPLY* va fi intotdeauna cu 8 octeti mai mare decit spatiul cerut (antetul *ICMP*).

Daca spatiul de date este cel putin de 8 octeti, **ping** utilizeaza primi 8 octeti pentru a include marcajul de timp pe care il utilizeaza la calculul timpilor dus-intors. Daca spatiul este mai mic decit aceasta valoare, nu vor mai fi calculati acesti timpi.

PACHETE ERONATE SI DUPLICATE

Ping va raporta pachetele eronate si duplicate. Pachetele duplicate nu ar trebui sa apara

Retele de calculatoare – Informatica anul 3 (2019-2020)

niciodata si se poate intimpla sa fie cauzate de retransmisii necorespunzatoare la nivelul legatura de date. Duplicatale pot apare in multe situatii si sint rareori (daca sint) un semn bun. Oricum, prezenta pachetelor duplicate la nivelele inferioare nu poate fi intotdeauna un motiv de alarmare.

Pachetele eronate sint in mod evident o cauza serioasa de alarma si indica module hardware defecte undeva pe calea parcursa de pachetele **ping** (in retea sau in gazde).

LUCRUL CU DIFERITE MODELE DE DATE

Nivelul (inter)retea ar trebui sa nu trateze niciodata pachetele in mod diferit, in functie de informatiile continute in zona de date. Din pacate, se stie ca aceste probleme apar pe furis in retea si ramin nedetectate perioade lungi de timp. In multe cazuri, un model particular care are probleme este unul care nu are suficiente ``tranzitii'', ca de exemplu toti bitii unu sau toti zero, sau un model exact la limita, adica aproape toti bitii sa fie zero. Nu este suficient sa specificati un model de date cu toti bitii zero (de exemplu) in linia de comanda, deoarece modelul care ne intereseaza este la nivelul legatura de date si relatia intre ceea ce introduceti dumneavoastra si ceea ce trimit controler-ele de retea poate fi complicata.

Aceasta inseamna ca daca aveti probleme dependente de date s-ar putea sa fie nevoie sa faceti o gramada de teste pentru a determina defectul. Daca sinteti norocos, s-ar putea intimpla sa gasiti un fisier pe care nu il puteti transmite prin retea sau a carui transmisie dureaza mai mult decit a altor fisiere similare ca lungime. Puteti cauta modele repetate in acest fisier, pe care le puteti testa utilizind optiunea **-p** a programului **ping**.

DETALII TTL

Valoarea *TTL* a unui pachet IP reprezinta numarul maxim de rutere IP pe care le poate parcurge pachetul inainte de a fi rejectat. In practica curenta este de asteptat ca fiecare ruter din Internet sa decrementeza cimpul *TTL* cu exact o unitate.

Specificatia protocoalelor TCP/IP recomanda ca cimpul *TTL* al pachetelor TCP sa fie setat la 60, dar multe sisteme utilizeaza valori mai mici (BSD 4.3 utilizeaza 30, BSD 4.2 utilizeaza 15).

Valoarea maxima a acestui cimp este 255 si cele mai multe sisteme Unix seteaza cimpul *TTL* al pachetelor *ICMP ECHO_REQUEST* la 255. Din acest motiv veti observa ca puteti sa dati ``ping" la unele gazde, dar nu puteti sa le contactati cu **telnet(1)** sau **ftp(1)**.

In operare normala ping afiseaza valoarea *TTL* din pachetele pe care le receptioneaza. Cind un sistem distant primeste un pachet ping, el poate face unul din trei lucruri, cu cimpul *TTL* din pachetul de raspuns:

Nu il modifica

Aceasta este ce fac sistemele Berkeley Unix inainte de versiunea BSD 4.3 tahoe. In acest caz valoarea *TTL* din pachetul receptionat va fi 255 minus numarul de rutere din calea dus-intors.

Il seteaza la 255

Aceasta este ce fac sistemele Berkeley Unix curente. In acest caz valoarea *TTL* din pachetul receptionat va fi 255 minus numarul de rutere din calea de la sistemul distant la gazda care primeste cererea *ping*.

Il seteaza la o alta valoare

Unele sisteme utilizeaza aceeasi valoare atit pentru pachetele *ICMP* cit si pentru pachetele TCP, de exemplu 30 sau 60. Altele s-ar putea sa utilizeze cu totul alte valori.

Retele de calculatoare – Informatica anul 3 (2019-2020)

ERORI

Multe gazde si pasarele ignora optiunea *RECORD_ROUTE*.

Lungimea maxima a antetului IP este prea mica pentru optiuni ca *RECORD_ROUTE*, astfel incit aceasta sa fie complet utila. Oricum, nu se poate face mai mult.

In general, nu este recomandata transmiterea de ping in masa si ping-ul in masa pe adresa de difuziune trebuie facut numai in conditii foarte bine controlate.

ping

ping prescurtare de la Packet InterNet Groper, este o comanda folosita pentru a verifica daca pachetele de date ajung la o adresa (destinatie) fara erori.

Sintaxa pentru sisteme Windows este:

ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] destination-list

destination-list este numele domeniului (de exemplu univ-ovidius.ro) sau adresa IP.

-t	Pings the specified host until stopped To see statistics and continue - type Control-Break To stop - type Control-C
-a	Resolve addresses to hostnames
-n count	Number of echo requests to send
-l size	Send buffer size
-f	Set Don't Fragment flag in packet
-i TTL	Time To Live
-v TOS	Type Of Service
-r count	Record route for count hops
-s count	Timestamp for count hops
-j host-list	Loose source route along host-list
-k host-list	Strict source route along host-list
-w timeout	Timeout in milliseconds to wait for each reply

Exemplu: dintr-o fereastră CLI (Start -> Run -> tastati: cmd -> OK) tastati:

ping www.univ-ovidius.ro

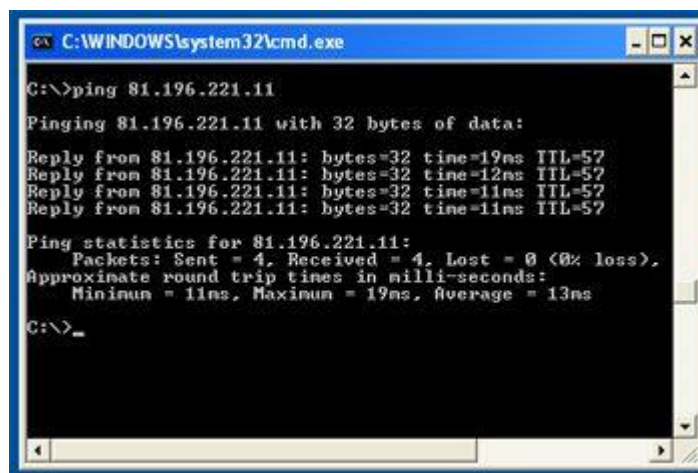
■ **TTL (Time To Live)** este un camp de 8 biti din header-ul IP si este continut de al 9-lea octet din cei 20.

Campul TTL este stabilit de cel care trimite datagrama si este decrementat de fiecare host (echipament activ de retea) aflat in ruta catre destinatie. Daca acest camp ajunge la 0 inainte ca datagrama sa ajunga la destinatie datagrama va fi stearsa si se va genera o eroare ICMP (11 - Time Exceeded) care va fi trimisa inapoi trimitatorului. Scopul campului TTL este de a evita situatia in care o datagrama nelivrata continua sa circule prin Internet.

Retele de calculatoare – Informatica anul 3 (2019-2020)

TTL reply este valoarea afisata ca raspuns la executarea comenzii ping.

Exemplu: daca intre noi si destinatie sunt 7 routere si valoarea originala pentru TTL este 64 vom primi raspunsul $64 - (7 * 1) = 57$ (vezi imaginea de mai jos).



```
C:\WINDOWS\system32\cmd.exe
C:\>ping 81.196.221.11

Pinging 81.196.221.11 with 32 bytes of data:

Reply from 81.196.221.11: bytes=32 time=19ms TTL=57
Reply from 81.196.221.11: bytes=32 time=12ms TTL=57
Reply from 81.196.221.11: bytes=32 time=11ms TTL=57
Reply from 81.196.221.11: bytes=32 time=11ms TTL=57

Ping statistics for 81.196.221.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 19ms, Average = 13ms

C:\>_
```

Pentru aflarea **propriului TTL** se da comanda **ping localhost**. Pentru calculatoare care ruleaza versiuni mai vechi de Windows rezultatul va fi 32, iar pentru versiuni noi va fi 128.

Din valoarea TTL a pachetelor de date receptionate putem intui sistemul de operare rulat pe calculatorul destinatie (Windows sau Unix). Aceasta valoare nu ne ofera o informatie sigura si completa asupra sistemului de operare ci doar orientativa.

In tabelul urmator sunt date valorile TTL pentru diferite platforme:

OS	VERSION	PLATFORM	TTL
-----	-----	-----	---
DC-OSx	1.1-95	Pyramid/NILE	30
Windows	9x/NT	Intel	32
NetApp	OnTap	5.1.2-5.2.2	54
HPJetDirect	HP_Printer		59
AIX	4.3.x	IBM/RS	60
AIX	4.2.x	IBM/RS	60
Cisco	11.2	7507	60
DigitalUnix	4.0	Alpha	60
IRI	X6.x	SGI	60
OS390	2.6	IBM/S390	60
Reliant	5.43	Pyramid/RM1000	60
FreeBSD	3.x	Intel	64
JetDirect	G.07.x	J3113A	64
Linux	2.2.x	Intel	64
OpenBSD	2.x	Intel	64
OS/400	R4.4	AS/400	64
SCO	R5	Compaq	64
Solaris	8	Intel/Sparc	64
FTX (UNIX)	3.3	STRATUS	64
Unisys	x	Mainframe	64
Netware	4.11	Intel	128
Windows	9x/NT	Intel	128
Windows	2000	Intel	128
Cisco	12.0	2514	255
Solaris	2.x	Intel/Sparc	255

Retele de calculatoare – Informatica anul 3 (2019-2020)

Obs: Windows <http://subinsb.com/default-device-ttl-values>

■ Administratorul de retea poate afla daca unul din clientii sai foloseste un router pentru partajarea conexiunii de retea.

Pentru aceasta se da comanda ping catre respectivul client. Daca valoarea TTL returnata este mai mica cu o unitate decat valoarea uzuala (64 sau 128) atunci clientul foloseste un router inaintea calculatorului.

Pentru a contracara acest lucru putem seta routerul sa nu raspunda la comanda ping dinspre WAN ("Discard ping from WAN" sau "Block WAN request"), astfel administratorul nu va mai primi o valoare TTL din care sa poata interpreta existenta routerului.

2.2.2. Comanda tracert

Numarul de routere aflat intre noi si destinatie se poate afla folosind comanda **tracert**. Rezultatul ofera adresele IP sau numele routerelor tranzitate.

Sintaxa pentru sisteme Windows este:

tracert [-d][-h maximum hops][-j host_list][-w timeout] target_name

target_name este numele domeniului (de exemplu alfa99.ro) sau adresa IP.

-d	Do not resolve addresses to hostname
-h maximum_hops	Maximum number of hops to search for target
-j host-list	Loose source route along host-list
-w timeout	Wait timeout miliseconds for each reply

Exemplu: dintr-o fereastră DOS (Start -> Run -> tastati: cmd -> OK) tastati:
tracert 10.9.85.17

2.2.3. Comanda NETSTAT

Comanda netstat poate fi folosită pentru a afișa informații detaliate despre conexiunile dumneavoastră și despre porturile folosite. Cea mai importantă funcție a sa este de a arăta ce porturi comunică date și care sunt deschise și gata de a „asculta”.

- Tipăriți netstat în command prompt. Comanda va afișa toate conexiunile active dintre sistemul dumneavoastră și orice alt sistem din rețea sau la internet.

- Tipăriți netstat /a pentru a afișa toate conexiunile curente împreună cu toate porturile deschise și care ascultă.

- Tipăriți netstat /o pentru a afișa ID-ul proceselor cărora le sunt asociate conexiunile curente. Vă ajută mult la identificarea aplicațiilor nedorite care rulează pe sistemul dumneavoastră.

2.2.4. Comanda TASKLIST

Retele de calculatoare – Informatica anul 3 (2019-2020)

Comanda vă arată procesele care rulează în acel moment pe sistemul dumneavoastră, împreună cu ID-ul acestora. Programul poate fi configurat să arate mai mult decât standardul Task Manager din Windows XP. După ce ați rulat nestat, ați văzut că, în lista ID-urilor proceselor, vi s-au oferit anumite coduri formate din cifre. Pentru a afla cărei aplicații îi corespunde fiecare cod, rulați tasklist.

2.2.5. Comanda PATHPING

Această comandă combină alte două comenzi: PING și TRACERT într-una singură. În modul de folosire implicit, pathping va lista la început numărul de hopuri (numărul de pași între diferitele rutere sau servere de rețea) necesare pentru a atinge destinația dumneavoastră IP sau URL, apoi va da ping fiecărui pas din rută de 100 de ori oferindu-vă o idee clară despre viteza conexiunii dintre sistemul dumneavoastră și țintă, precum și despre legăturile slabe din rețea.

2.3. Utilitare de rețea

Obs. Toate utilitarele de mai jos se rulează din linia de comandă (start; run; cmd)

2.3.1. In Windows (XP/ 7///10)

Toate utilitarele din tabelul care urmează se găsesc, alături de multe altele, în directorul `c:/windows/system32`.

nume	scurta descriere
arp	Vizualizarea și manipularea tabelelor de corespondență adIP -> adMAC menținute de entitatea ARP.
finger	Obținerea de informații despre utilizatori internet (identificați prin email) de la un server "finger".
ftp	Trimiterea și primirea de fișiere de pe sisteme distanțate prin protocolul FTP.
ipconfig	Afisează setările interfețelor de rețea ale calculatorului.
net	Obținerea de informații despre diferite aspecte ale organizării specifice Windows ale rețelei (de exemplu grupuri de lucru). Una dintre facilitățile interesante este că permite trimiterea de mesaje scurte către alte calculatoare din rețea care apar ca mici ferestre de dialog.
netstat	Afisează starea entităților TCP și UDP.
nslookup	Interogarea a diverse servere DNS (<i>Domain Name Server</i>)
ping / ping6	Măsurarea timpului dus întors până la diverse stații prin intermediul unor pachete ICMP peste IPv4, respectiv peste IPv6.
telnet	Conectarea distanțată la alte sisteme. Vezi <code>ssh</code> din Linux.
tracert / tracert6	Explorează calea (ruterile) urmate până la o anumită stație.
winchat	Chat simplu între două calculatoare (cu interfață grafică).

- <http://www.windowsnetworking.com/kbase/WindowsTips/WindowsServer2008/AdminTips/Network/NetworkCommand-LineUtilitiesinWindows.html>
- http://whirlpool.net.au/wiki/windows_nw_diag_cmds
- <http://www.windowcentral.com/how-manage-wireless-networks-using-command-prompt-windows-10>

Retele de calculatoare – Informatica anul 3 (2019-2020)

- <https://support.microsoft.com/en-us/help/10741/windows-10-fix-network-connection-issues>

2.3.2. In Unix/Linux (RedHat/Fedora Core etc)

In Linux informatii detaliate despre diverse comenzi se pot afla folosind `man` sau `info`. Daca stiti cam ce face o comanda dar nu va aduceti aminte exact cum se numea folositi `apropos`.

nume	scurta descriere
dig	Interogarea a diverse servere DNS (<i>Domain Name Server</i>)
ftp	Trimiterea si primirea de fisiere de pe sisteme distante prin protocolul FTP.
ifconfig	Afiseaza setarile interfetelor de retea ale calculatorului.
ping	Masurarea timpului dus intors pana la diverse statii.
telnet	Conectarea distanta la alte sisteme. Folositi ssh in loc de telnet.
traceroute	Exploreaza calea (rutele) urmate pana la o anumita statie.
ssh	Conectarea distanta sigura (cu autentificare/criptare) la alte sisteme.

- <http://www.tecmint.com/linux-network-configuration-and-troubleshooting-commands/>
- <http://www.tecmint.com/20-advanced-commands-for-linux-experts/>
- <http://www.slackbook.org/html/basic-network-commands.html>
- <http://www.unix.com/shell-programming-and-scripting/85519-links-all-networking-commands-linux.html>

ARP este folosit pentru a converti adresa Internet Protocol (IP) in corespondenta sa fizica, adresa de retea. ARP este un protocol low-level, operand in Layer2 din modelul OSI.

ARP este de obicei implementat chiar in driverele sistemelor de operare din cadrul retelelor, este gasit de obicei in retele Ethernet (desi este implementat si pentru ATM, Token Ring si alte tipuri de retele). In RFC 826 este documentat design'ul initial si implementarea ARP.

Ce face ARP?

Fiecare adaptor ethernet (placa de retea) este produs cu o adresa fizica inscrisa in cadrul hardware'ului sau, numita Media Access Control - MAC address. Fiecare producator are grija ca aceasta adresa de 6bytes sa fie unica si Ethernet se bazeaza pe unicitatea acestor identificatori pentru a livra fiecare mesaj. In momentul in care un device incearca sa trimita ceva catre un alt device din retea prin Ethernet, in primul rand trebuie sa determine adresa MAC a tintei. Aceste mapari IP-to-MAC sunt derivate dintr-un cache ARP aflat in cadrul fiecarui device. Daca adresa IP nu apare in cache'ul device'uli, acesta nu poate trimite un mesaj catre "tinta" sa. El trebuie mai intai sa broadcast o cerere ARP in subnetul local, host'ul cu IP'ul respectiv va trimite un ARP reply ca raspuns al broadcastului, permitand in acest fel device'ul care vrea sa trimita mesajul sa updateze cache'ul si sa inceapa trimiterea efectiva a mesajului.

Se poate determina IP-ul pe baza adresei MAC?

- ARP este un *feature built-in* in IP, scopul sau este de a traduce (translata) adrese IP in adrese MAC...ARP nu a fost conceput pentru a determina o adresa IP pe baza unei adrese MAC cunoscute, desi in anumite conditii acest lucru este posibil.
- Cea mai simpla metoda este aceea de a face o scanare a intregii retele si de a folosi un utilitar pentru a analiza datele si a gasi tinta. In cazul unei retele mari (sau foarte mari) acest lucru poate dura foarte mult timp si poate fi complet ineficient.

Retele de calculatoare – Informatica anul 3 (2019-2020)

- O metoda mai eleganta este de a cauta adresa IP fie in cache-ul ARP din statia locala, fie in cache-ul tinut de router (in unele cazuri chiar de switch-uri, desi poate fi foarte "delicat"). In Windows daca tastati (intr-un cmd evident) "arp -a" veti vedea o lista cu toate aceste corespondente IP-MAC. Numarul acestor conexiuni depinde foarte mult de cum este configurata masina.
- Majoritatea router-elor permit acces la cache-urile ARP printr-o interfata Web de administrare. Acestea vor arata adresele IP si MAC al fiecarui device conectat la retea. In general, in cazul conexiunilor intre retele, adresele MAC vor corespunde unui router si nu unui device...adica daca in cache-ul routerului exista si IP-uri - MAC-uri din alte retele, ele nu sunt valide, MAC-ul fiind al routerului retelei externe, nu al statiei din retea respectiva.
- In unele corporatii sunt folosite programe software care mapeaza toate corespondentele MAC-IP. Aceste programe sunt instalate pe fiecare statie si ele trimit datele catre o baza centrala, folosindu-se de Simple Network Management Protocol (SNMP). In aceasta baza centrale sunt stocate corespondentele IP-MAC pentru fiecare device din retea.

2.4. Wireshark (<http://www.wireshark.org/download.html>) – este un *packet sniffer* (network protocol analyzer). Programul permite examinarea traficului dintr-o retea, sau capturarea si salvarea traficului intr-un fisier. Pentru fiecare pachet capturat, programul afiseaza informatii detaliate. **Wireshark** include un limbaj propriu pentru definirea expresiilor de filtrare si permite reconstruirea unei sesiuni TCP pe baza pachetelor capturate.

2.5. RIVERBED – MODELER ACADEMIC EDITION

2.5.1. Introducere

Riverbed Modeler Academic Edition (versiune actuala a Opnet-ului - **Optimized Network Application and Network Performance**) – mediu de simulare a retelelor de calculatoare furnizează software de management pentru aplicații și rețele, care oferă soluții pentru:

- Proiectarea retelelor si planificarea capacității acestora
- Modelare și simulare pentru rețele și aplicații
- Managementul configurării rețelelor
- Managementul performanțelor aplicațiilor

Academic Edition Account Signup

https://rpmapps.riverbed.com/ae/4dcgi/SIGNUP_NewUser

Some of the restricted capabilities in Riverbed Modeler Academic Edition

<https://supportkb.riverbed.com/support/index?page=content&id=S24443>

Download Software

If you do not already have the Modeler Academic Edition installer, you may download it here. You may also review the system requirements for installing and running Modeler Academic Edition.

https://rpmapps.riverbed.com/ae/4dcgi/DOWNLOAD_HOME

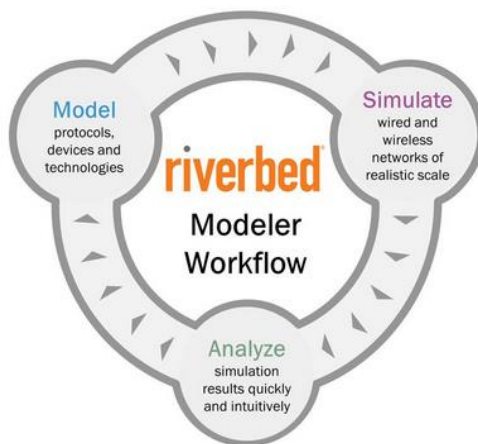
License Activation

After installation, run the software. It will guide your through the product activation process. In special cases you may need to access the license activation site directly.

Riverbed oferă o versiune academică (**Modeler Academic Edition**) - include modele standard pentru protocoale și echipamentele disponibile în tehnologia IT (disponibile, dupa instalare, în subdirectoare).

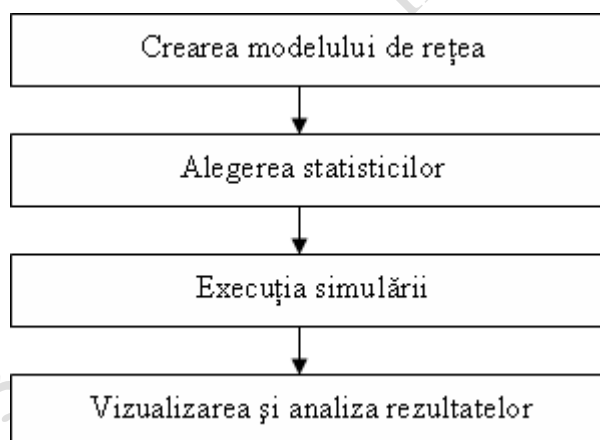
Retele de calculatoare – Informatica anul 3 (2019-2020)

Scopul acestui material introductiv este de a învăța folosirea caracteristicilor Modeler Academic Edition pentru a proiecta și analiza rețele, având în vedere (SI !!!!) **proiectul de curs** pe care fiecare student îl va finaliza, conform temei nominale care va fi data la cursul 4. În proiectul de curs se vor adopta modele de rețea care permit analiza unei probleme, se vor extrage informațiile statistice relevante problemei și se vor analiza rezultatele obținute.



2.5.2. Modeler Academic Edition

Etapele de lucru:



Modeler Academic Edition: Etapele de lucru pentru simularea și analiza unei rețele

Obs: O statistica este o caracteristica numerica a unui esantion (Anexa 3, pag.79, Lab2)

- **Statistica** este stiinta colectarii, clasificarii, prezentarii, interpretarii datelor numerice si a folosirii acestora pentru a formula concluzii si a lua decizii.
- **Statistica descriptiva** (Descriptive Statistics) se ocupa cu colectarea, clasificarea si prezentarea datelor numerice.
- **Statistica inferentiala** (Inferential Statistics) se ocupa cu interpretarea datelor oferite de statistica descriptiva si cu folosirea acestora pentru a formula concluzii si lua decizii.

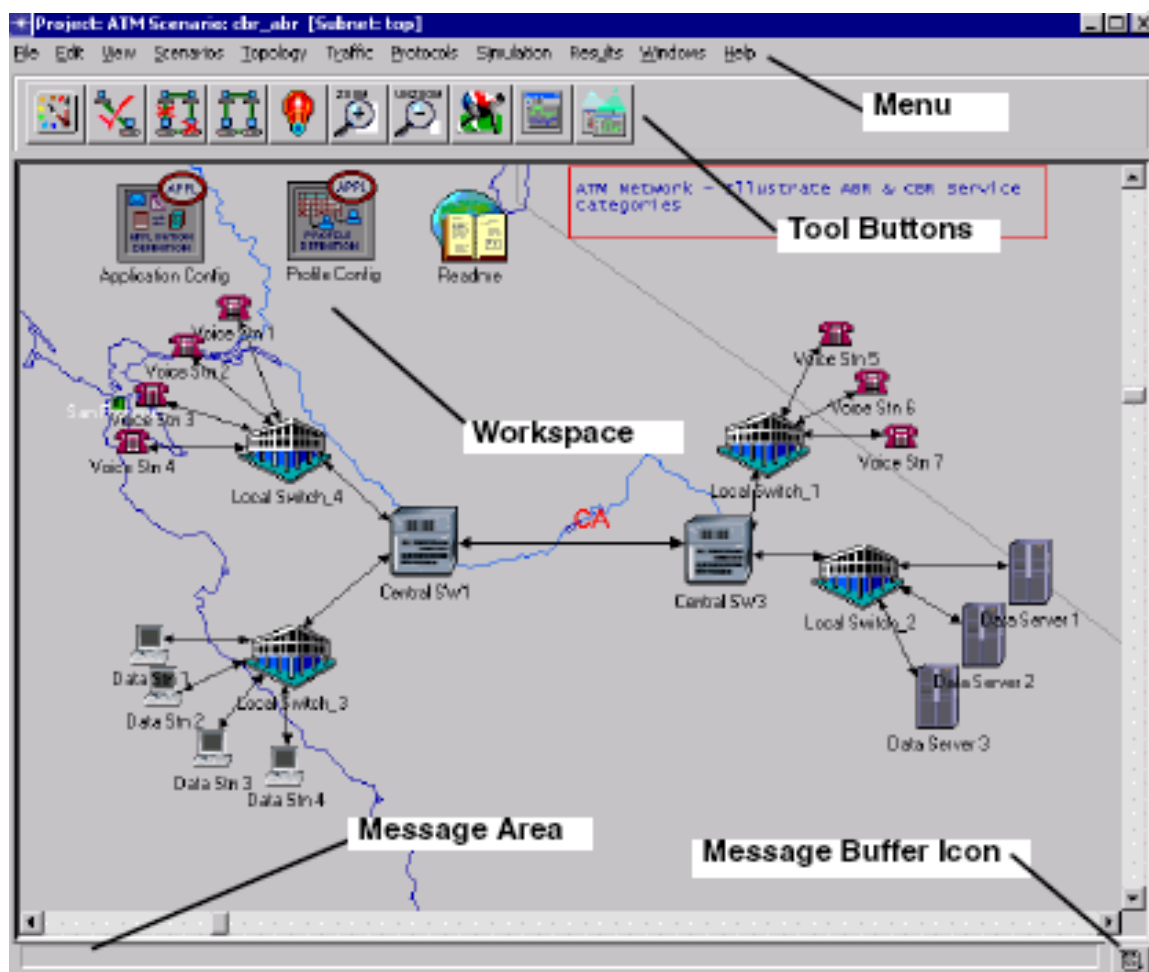
Modeler Academic Edition dispune de un *Project Editor* care permite crearea modelului de rețea folosind modele din biblioteca standard, alegerea statisticilor care urmează a fi colectate pentru fiecare obiect al rețelei sau pentru întreaga rețea. De asemenea poate fi executată o simulare și pot fi vizualizate rezultatele obținute prin simularea rețelei.

Retele de calculatoare – Informatica anul 3 (2019-2020)

Când se deschide un proiect existent, *Project Editor Window* pune în evidență: **Menu, Tool Buttons, Workspace, Message Area, Message Buffer Icon.**

Menu Bar organizează toate operațiile editorului. Numărul și tipul operațiilor accesibile depind de modulele folosite. Operațiile editorului referitoare la context sunt accesibile prin folosirea butonului din dreapta al *mouse-ului*

O parte din operațiile comune, care sunt accesibile prin *Menu Bar*, pot fi accesate și prin *Tool Buttons*. Semnificația acestor butoane, prezentate și în fig.3, se prezintă în tabelul 1.



Project Editor Window



Butoane folosite în *Project Editor*

Tabelul 1. Semnificația butoanelor din *Project Editor*

1. <i>Open object palette</i>	6. <i>Zoom</i>
2. <i>Check link consistency</i>	7. <i>Restore</i>
3. <i>Fail Selected objects</i>	8. <i>Configure discrete event simulation</i>
4. <i>Recover selected objects</i>	9. <i>View simulation results</i>
5. <i>Return to parent subnet</i>	10. <i>Hide or show all graphs</i>

Retele de calculatoare – Informatica anul 3 (2019-2020)

Workspace este spațiul de lucru din partea centrală a ferestrei editorului, care este folosit pentru crearea modelului rețelei, selectarea și deplasarea obiectelor rețelei, alegerea operațiilor specifice conextului.

Message Area, plasată în partea de jos a ferestrei, furnizează informații despre starea *tool-ului*.

Message Buffer Window, plasata în partea de jos în stânga, permite accesul la o listă de mesaje, notificări, atenționări.

2.6. Aplicații de rețea în [Python](https://www.python.org/) (<https://www.python.org/>)

- [Python intro](#)
- [Programare Python](#)
- [Byte-of-python](#)

3. Partea practica

3.1. Strangerea de informatii privind conexiunea, numele calculatorului, adresa MAC si configurările TCP/IP de rețea.

```
C:\> C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\admin>ipconfig ?
Error: unrecognized or incomplete command line.
USAGE:
    ipconfig [/? | /all | /renew [adapter] | /release [adapter] |
            /flushdns | /displaydns | /registerdns |
            /showclassid adapter |
            /setclassid adapter [classid] ]
where
    adapter          Connection name
                    <wildcard characters * and ? allowed, see examples>

Options:
    /?              Display this help message
    /all            Display full configuration information.
    /release        Release the IP address for the specified adapter.
    /renew          Renew the IP address for the specified adapter.
    /flushdns       Purges the DNS Resolver cache.
    /registerdns    Refreshes all DHCP leases and re-registers DNS names
    /displaydns     Display the contents of the DNS Resolver Cache.
    /showclassid   Displays all the dhcp class IDs allowed for adapter.
    /setclassid    Modifies the dhcp class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

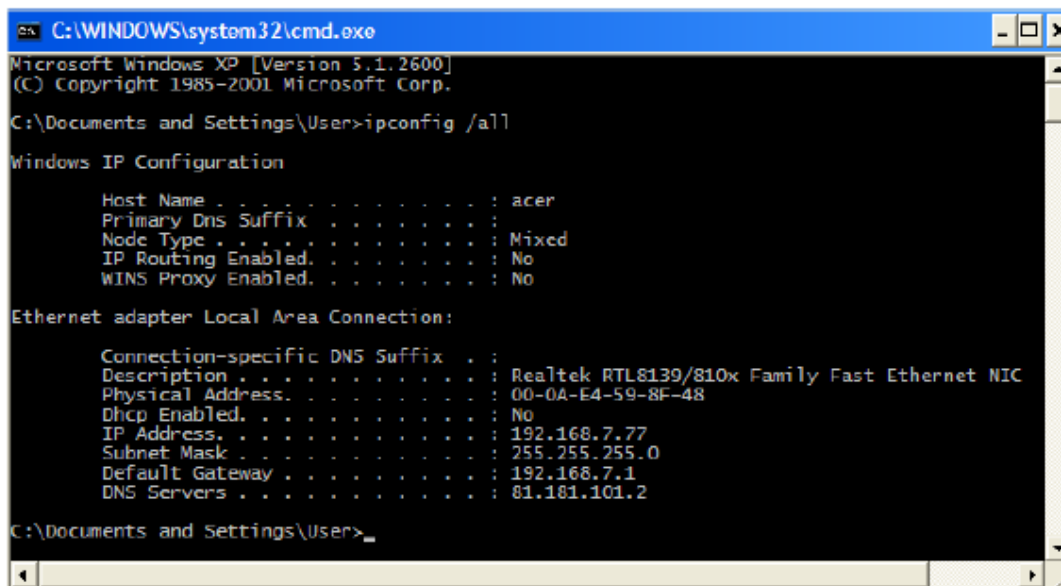
For Setclassid, if no ClassId is specified, then the ClassId is removed.

Examples:
> ipconfig          ... Show information.
> ipconfig /all     ... Show detailed information
> ipconfig /renew    ... renew all adapters
> ipconfig /renew EL* ... renew any connection that has its
                    name starting with EL
> ipconfig /release *Con* ... release all matching connections,
                    eg. "Local Area Connection 1" or
                    "Local Area Connection 2"
```


Retele de calculatoare – Informatica anul 3 (2019-2020)

Pentru aflarea acestor informatii se alege (pe o statie Windows) : **Start > Run**. In campul *Open* al ferestrei **Run**, se introduce comada **cmd**. In acest moment se deschide fereastra de comanda, dupa care se tasteaza comanda **ipconfig /all**. Figura de mai jos reprezinta configurariile IP detaliate, rezultatul ultimei comenzi:

3.2.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\User>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : acer
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Mixed
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

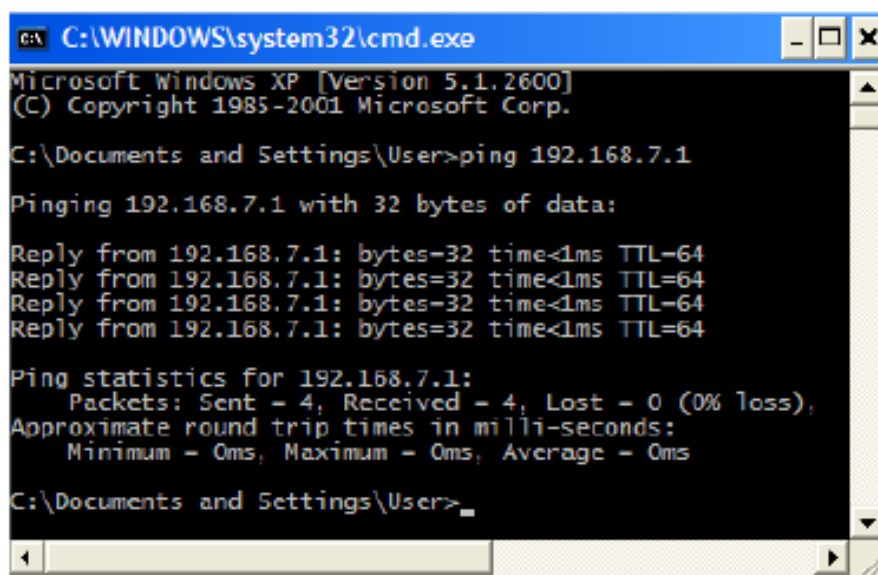
    Connection-specific DNS Suffix . :
    Description . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC
    Physical Address. . . . . : 00-0A-E4-S9-8F-48
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 192.168.7.77
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.7.1
    DNS Servers . . . . . : 81.161.101.2

C:\Documents and Settings\User>
```

Testarea conectivitatii in retea, a configurarii corecte TCP/IP si a functiei de transmitere/receptie a interfetei de retea (NIC).

Utilitarul folosit este utilitarul *ping*. Poate fi folosit pentru masurarea timpului dus-intors a pachetelor IP trimise catre o statie din retea. El transmite pachete ICMP de tip 8 (Echo Request). Statia care primeste aceste pachete raspunde cu un pachet ICMP de tip 0 (Echo Reply). Intervalul scurs intre trimiterea unui “Echo Request” si primirea unui “Echo Reply” este afisat de *ping*. Protocolul ICMP (Internet Control Message Protocol) este inclus in orice implementare TCP/IP.

Testarea stivei de protocoale TCP/IP si a functiei de transmitere/receptie a NIC-ului de face testand adresa interna de *loopback* (127.0.0.1).



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\User>ping 192.168.7.1

Pinging 192.168.7.1 with 32 bytes of data:

Reply from 192.168.7.1: bytes=32 time<1ms TTL=64
Reply from 192.168.7.1: bytes=32 time<1ms TTL=64
Reply from 192.168.7.1: bytes=32 time<1ms TTL=64
Reply from 192.168.7.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\User>
```

3.3. Determinarea traseului parcurs de un pachet la destinatie.

Utilitarul folosit este *tracert* . Acest utilitar este similar cu *ping*, si transmite pachete de tip ICMP unei statii din retea, dar care retine tot traseul parcurs de pachete pana la destinatie, masurand timpii parcursi pana la sosirea

Retele de calculatoare – Informatica anul 3 (2019-2020)

raspunsurilor de la ruterele intermediare. Astfel, acest program este foarte util pentru detectarea cauzelor pierderii unor pachete.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\User>tracert 192.168.7.1

Tracing route to 192.168.7.1 over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    192.168.7.1
Trace complete.

C:\Documents and Settings\User>tracert 81.181.101.162

Tracing route to 81.181.101.162 over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    81.181.101.162
Trace complete.

C:\Documents and Settings\User>tracert 81.181.101.2

Tracing route to mail.etc.upt.ro [81.181.101.2]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    192.168.7.1
  2  <1 ms    <1 ms    <1 ms    mail.etc.upt.ro [81.181.101.2]
Trace complete.

C:\Documents and Settings\User>_
```

3.4. Monitorizarea conexiunilor in retea, afisarea tabelii de rutare a sistemului si statisticilor interfetei de retea (NIC).

Utilitarul utilizat este *netstat*. Testati urmatoarele optiuni : *-a*, *-n*, *-b*, *-r*, *-e*.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\User>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP    acer:smtp               acer:0                  LISTENING
TCP    acer:finger              acer:0                  LISTENING
TCP    acer:http                acer:0                  LISTENING
TCP    acer:106                 acer:0                  LISTENING
TCP    acer:pop3                acer:0                  LISTENING
TCP    acer:epmap               acer:0                  LISTENING
TCP    acer:ldap                acer:0                  LISTENING
TCP    acer:microsoft-ds        acer:0                  LISTENING
TCP    acer:3306                acer:0                  LISTENING
TCP    acer:5106                acer:0                  LISTENING
TCP    acer:5107                acer:0                  LISTENING
TCP    acer:5108                acer:0                  LISTENING
TCP    acer:8888                acer:0                  LISTENING
TCP    acer:1052                localhost:1053          ESTABLISHED
TCP    acer:1053                localhost:1052          ESTABLISHED
TCP    acer:10025               acer:0                  LISTENING
TCP    acer:10110               acer:0                  LISTENING
TCP    acer:netbios-ssn         acer:0                  LISTENING
TCP    acer:1128                81.181.101.162:22      ESTABLISHED
UDP    acer:microsoft-ds        *:
UDP    acer:isakmp              *:
UDP    acer:1065                *:
UDP    acer:4500                *:
UDP    acer:ntp                 *:
UDP    acer:1055                *:
UDP    acer:1123                *:
UDP    acer:1900                *:
UDP    acer:ntp                 *:
UDP    acer:netbios-ns          *:
UDP    acer:netbios-dgm         *:
UDP    acer:1900                *:

C:\Documents and Settings\User>
```


Retele de calculatoare – Informatica anul 3 (2019-2020)

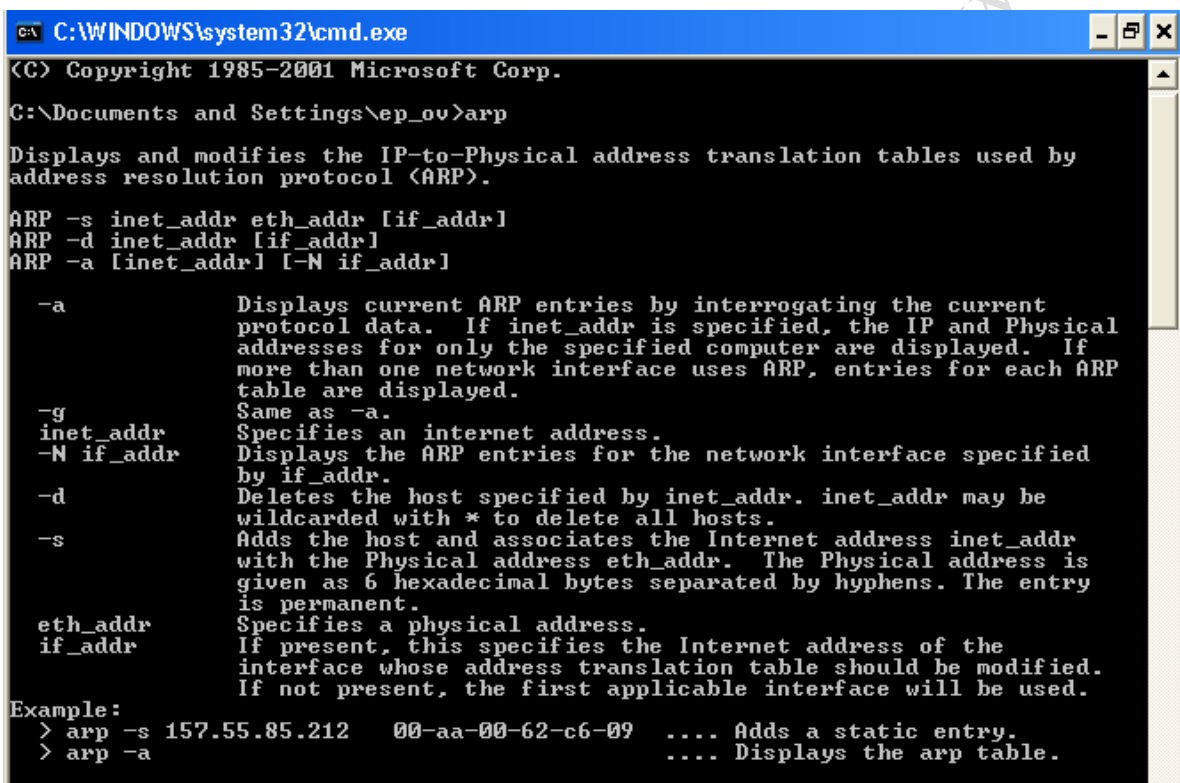
3.5. Comanda TASKLIST

Comanda procesele care rulează în acel moment pe sistem împreună cu ID-ul acestora. Se va rula `tasklist /?` Precum si exemplele din help.

3.6. Comanda PATHPING

În modul de folosire implicit, pathping va lista la început numărul de hopuri (numărul de pași între diferitele rutere sau servere de rețea) necesare pentru a atinge destinația IP sau URL, apoi va da ping fiecărui pas din rută de 100 de ori oferindu-vă o idee clară despre viteza conexiunii dintre sistemul țintă, precum și despre legăturile slabe din rețea. Se va rula comanda cu opțiunile indicate in help (pathping <enter>).

3.7. testare arp



```
C:\WINDOWS\system32\cmd.exe
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ep_ov>arp

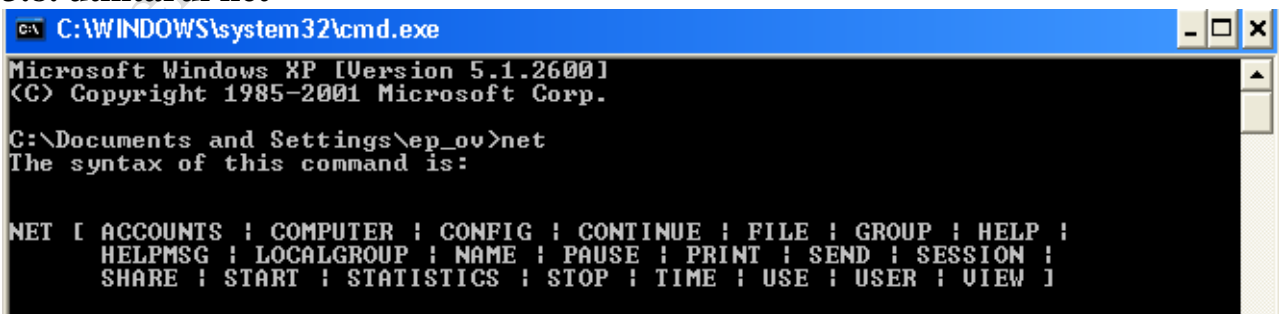
Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

-a          Displays current ARP entries by interrogating the current
            protocol data.  If inet_addr is specified, the IP and Physical
            addresses for only the specified computer are displayed.  If
            more than one network interface uses ARP, entries for each ARP
            table are displayed.
-g          Same as -a.
inet_addr   Specifies an internet address.
-N if_addr  Displays the ARP entries for the network interface specified
            by if_addr.
-d          Deletes the host specified by inet_addr.  inet_addr may be
            wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
            with the Physical address eth_addr.  The Physical address is
            given as 6 hexadecimal bytes separated by hyphens.  The entry
            is permanent.
eth_addr    Specifies a physical address.
if_addr     If present, this specifies the Internet address of the
            interface whose address translation table should be modified.
            If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a          .... Displays the arp table.
```

3.8. utilitarul net



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ep_ov>net
The syntax of this command is:

NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
    HELPMMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |
    SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

Retele de calculatoare – Informatica anul 3 (2019-2020)

3.9. utilitarul netstat

```
C:\Documents and Settings\admin>netstat ?
```

Displays protocol statistics and current TCP/IP network connections.

```
NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]
```

-a	Displays all connections and listening ports.
-b	Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.
-e	Displays Ethernet statistics. This may be combined with the -s option.
-n	Displays addresses and port numbers in numerical form.
-o	Displays the owning process ID associated with each connection.
-p proto	Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s option to display per-protocol statistics, proto may be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-r	Displays the routing table.
-s	Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default.
-v	When used in conjunction with -b, will display sequence of components involved in creating the connection or listening port for all executables.
interval	Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

```
netstat help
```

```
netstat -ns
```

3.10. utilitarul nslookup

```
> ?
Commands:  (identifiers are shown in uppercase, [] means optional)
NAME       - print info about the host/domain NAME using default server
NAME1 NAME2 - as above, but use NAME2 as server
help or ?  - print info on common commands
set OPTION - set an option
all        - print options, current server and host
[no]debug  - print debugging information
[no]d2     - print exhaustive debugging information
[no]defname - append domain name to each query
[no]recurse - ask for recursive answer to query
[no]search - use domain search list
[no]lvc    - always use a virtual circuit
domain=NAME - set default domain name to NAME
srchlist=N1[,N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
root=NAME  - set root server to NAME
retry=X    - set number of retries to X
timeout=X  - set initial time-out interval to X seconds
type=X     - set query type (ex. A,ANY,CNAME,MX,NS,PTR,SOA,SRU)
querytype=X - same as type
class=X    - set query class (ex. IN (Internet), ANY)
[no]lmsxfr - use MS fast zone transfer
ixfrver=X  - current version to use in IXFR transfer request
server NAME - set default server to NAME, using current default server
[no]server NAME - set default server to NAME, using initial server
finger [USER] - finger the optional NAME at the current default host
root         - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
-a          - list canonical names and aliases
-d          - list all records
-t TYPE     - list records of the given type (e.g. A,CNAME,MX,NS,PTR etc.)
view FILE   - sort an 'ls' output file and view it with pg
exit       - exit the program
>
```

Retele de calculatoare – Informatica anul 3 (2019-2020)

3.11. utilitarul ipv6 (windows xp!)/ windows 7, 10:

<https://docs.microsoft.com/en-us/windows/desktop/winsock/using-ipv6-2>

The following command is available on Windows XP with SP1 and later to query and configure IPv6 on a local computer:

- [Netsh.exe](#)

```
C:\Users\EP>netsh interface ipv6 /?
The following commands are available:

Commands in this context:
6to4          - Changes to the 'netsh interface ipv6 6to4' context.
?             - Displays a list of commands.
add           - Adds a configuration entry to a table.
delete        - Deletes a configuration entry from a table.
dump          - Displays a configuration script.
help          - Displays a list of commands.
isatap        - Changes to the 'netsh interface ipv6 isatap' context.
reset         - Reset the IP configurations.
set           - Sets configuration information.
show          - Displays information.

The following sub-contexts are available:
6to4 isatap

To view help for a command, type the command, followed by a space, and then
type ?.
```

Prior to Windows XP with Service Pack 1 (SP1), IPv6 configuration and management used several older command-line tools to configure and manage IPv6. Using these older tools, the IPv6 changes are not permanent and are lost when the computer or the IPv6 protocol was restarted.

The following older commands are available on Windows XP

- [Net.exe](#)
- [Ipv6.exe](#)
- [Ipsec6.exe](#)

How to Ping IPv6 Address from Windows and Linux CLI

<https://linuxide.com/linux-how-to/ping-ipv6-address-windows-linux-cli/>

3.12. ping IPv4 si IPv6

<http://www.ipv6now.com.au/pingme.php>

Ping by Hostname or IP Address

Ping measures the round-trip time for packets between this host and a destination host. This test uses 5 pings over IPv4 and IPv6. A response for both IPv4 and IPv6 means that the host is accessible over both protocols. A result of 'unknown host' means that the host may not be accessible via that protocol.

The results show a summary of the minimum, mean, maximum, and standard deviation of the round-trip times. If you see large variations in the time, or less than five ping responses, there may be congestion or some other problem on the network.

Enter Hostname or IP address

3.13. Studiu de caz: INTRANET de capacitate mică.

În această studiu de caz ne propunem să analizăm o rețea Intranet a unei mici organizații. În mod obișnuit o astfel de rețea este o rețea în topologie **stea**.

Se analizează pentru început o rețea plasată în corpul A - **CorpA**. În continuare se analizează extensia rețelei prin adăugarea unei rețele în topologie **stea** în corpul B - **CorpB**. Se vor construi și testa aceste scenarii și se vor analiza **încărcarea cu trafic (load)** și **întârzierea (delay)** transmiterii pachetelor în cele două etape prevăzute în cele două scenarii.

Small Internetworks

Se vor parcurge „pas cu pas” cele prezentate în tutorialul
[Lab 01 Small Internetworks.pdf](#) (recomandare: TL_01)

„In this tutorial, you will

- Build a network quickly
- Collect statistics about network performance
- Analyze these statistics”

ATENȚIE:

• La punctul 4:

4 Name the project and scenario, as follows:

4.1 Name the project <NUME>_Sm_Int. Exemplu: **MARCULESCU_Sm_Int**

Include your **NAME** in the project name to distinguish it from other versions of this project.

- **Se vor salva în .doc** toate reprezentările grafice obținute în proiectul propriu, conform celor din tutorial, însoțite de denumirile acestora.

Retele de calculatoare – Informatica anul 3 (2019-2020)

- **Se vor interpreta rezultatele obtinute** si, acolo unde tutorialul contine intrebari, se vor oferi raspunsuri argumentate si fundamentate, eventual prin consultarea altor surse (ex. Internet!).

- **Se va tine cont de cele precizate la pagina 26:**

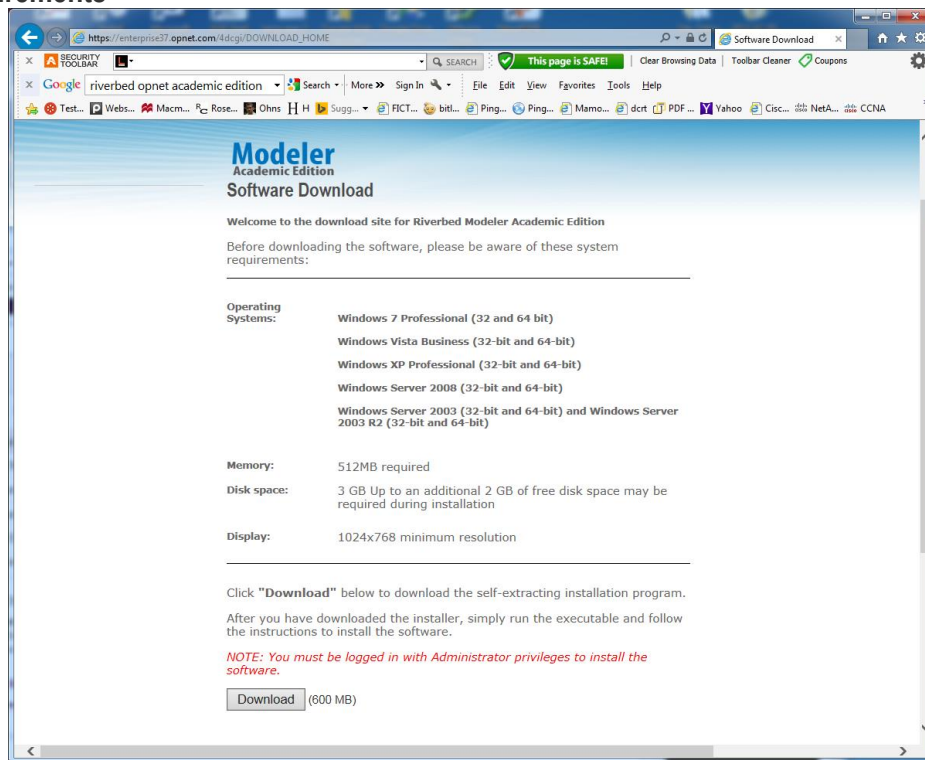
Note—Be sure to delete the **stdmod** setting for the **Network Simulation Repositories** preference when you are finished doing tutorials. To delete the setting, select **Edit > Preferences**, search for **Network Simulation Repositories**, click on the value, and choose **Delete**.

- **Procedure 2-6 (pag. 2-9 → 2-11) din [Lab_01_Small_Internetworks.pdf](#)** nu se va putea executa pe versiunea academica
<https://supportkb.riverbed.com/support/index?page=content&id=S24443>
- **Indicatii f. importante sunt puse la dispozitia cursantilor in [readme_mod_work_dir.pdf](#) si [readme_lab_modeler.pdf](#)**

Anexa: Riverbed Modeler Download Instructions

https://rpmapps.riverbed.com/ae/4dcgi/DOWNLOAD_HOME

1. System Requirements



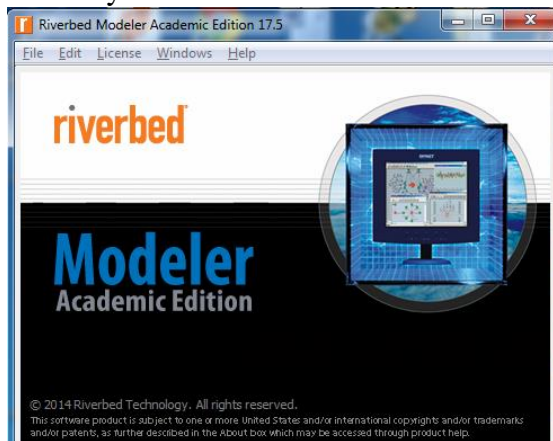
2. Downloading the Software (https://rpmapps.riverbed.com/ae/4dcgi/DOWNLOAD_HOME)
Academic Edition Account Signup: https://rpmapps.riverbed.com/ae/4dcgi/SIGNUP_NewUser

Retele de calculatoare – Informatica anul 3 (2019-2020)

If your computer meets the system requirements, shown above, then download the software from:

https://rpmapps.riverbed.com/ae/4dcgi/DOWNLOAD_HOME

1. **Complete the form (Name; Student; Course: Computer Networks; Organisation: “Ovidius” University, Constantza, Romania; Sponsored Professor: Eugen Petac, Ph.D; etc**
1. You will get an email containing a username and password and a link for downloading the software. Follow the instructions on the website for downloading the software.
2. After downloading the software, double-click on the file,which you just downloaded.
3. Follow the on screen instructions to install the software.
4. Click on **Start/ Riverbed...**Now you should see:



5. Select **License/ License Management** from the menu. Follow the onscreen instructions to activate the product.

https://rpmapps.riverbed.com/ae/4dcgi/REG_TransactionCode

Observatii

1.Atentie (Opnet) – Proiectul creat se salveaza implicit in:

C:\Users\student(NUMÉ user)\op_model\NUMÉ_PROIÉCT

NUMÉ_PROIÉCT *contine proiectul opnet propriu-zis*

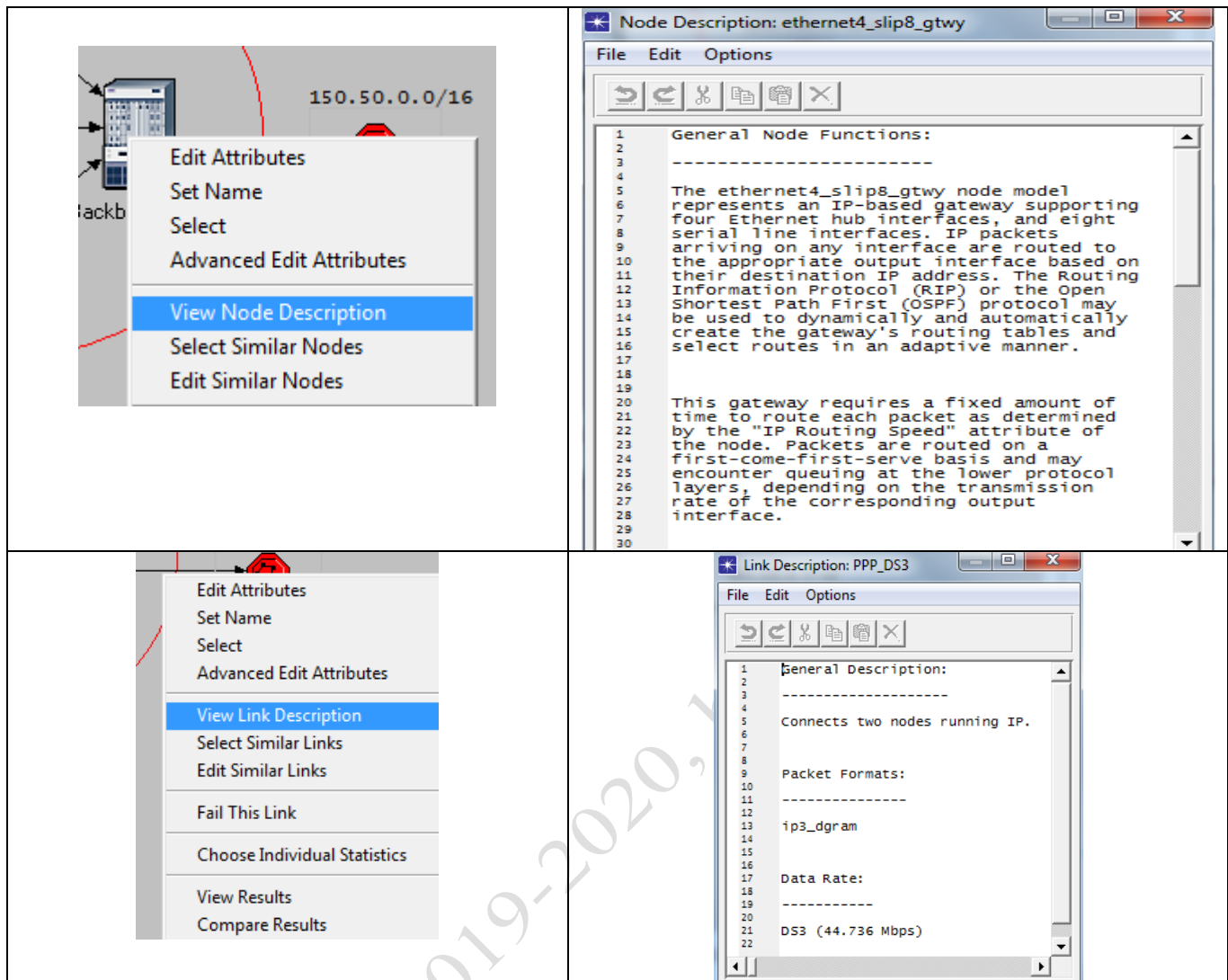
VARIANTA

se arhiveaza intreg folderul **Folder creat mai jos...el contine proiectul opnet propriu-zis**

- In directorul\Studenti\Info3\Nume_Prenume se creează directorul **\L1_Modeler_Nume_Prenume** folosind:
 - **File → New → Folder**
- Se lansează în execuție Modeler.
- Se selectează directorul în care vor fi plasate fişierele proiectului.
 - **File → Model Files → Add Model Directory**
 - Se selectează directorul în care se va lucra (în acest director vor fi salvate fişierele proiectului curent)
 - Se arhiveaza **L1_Modeler_Nume_Prenume**
 -

2. Atentie (Modeler) : Click dreapta pe “obiect” (ex. Router)...”Judec, deci exist!”

Retele de calculatoare – Informatica anul 3 (2019-2020)



3.2. Aplicații de rețea în **Python** (<https://www.python.org/>)

a. Instalare Python

RECOMANDARE: Parcurgerea integrală a următoarelor materiale

- [Python intro](#)
- [Programare Python](#)
- [Byte-of-python](#)

b. Instalare netaddr

Installing from the Python Package Index

The easiest way to install netaddr is to use pip.

Download and install the latest version from PyPI - <http://pypi.python.org/pypi/pip> and run the following command

```
pip install netaddr
```

Retele de calculatoare – Informatica anul 3 (2019-2020)

Installing from a source package

Download the latest release tarball/zip file and extract it to a temporary directory or clone the repository into a local working directory.

Run the setup file from directory:

```
python setup.py install
```

This automatically places the required files in the `lib/site-packages` directory of the Python version you used to run the setup script, may also be part of a virtualenv or similar environment manager.

c. **Aplicatii: Adrese MAC/ MAC addresses** ([Tutorial 2.pdf](#))

4. Tema:

- Toate punctele din sectiunea 3 “partea practica” se vor relua de catre cursanti, folosind etapele de lucru indicate.

- Arhiva cu numele **L2_num+prenume_info3.rar** va contine

a.L1_num+prenume.doc (document .doc): rezultatele experimentale **comenzi insotite de capturi si comentarii**, proiect **Modeler** (pasi intermediari importanti, **rezultate/capturi pentru View node description si View link description** (obs.2 anterioara), **exercitiile rezolvate, raspunsuri la intrebari, rezultate finale, observatii finale**) + **AnalizaConectivitateUOC**

b.L1_num+prenume_Modeler : proiectul **Modeler** (observatia 1 anterioara),

Arhiva cu numele **L2_num+prenume_info3.rar** se va trimite prin e-mail la adresa retelecdsd@gmail.com precizandu-se la **subject: L2_num+prenume_info3**, pana pe data de **16 octombrie 2018, ora 8.00 a.m.** (**Atentie, gmail nu “prea vrea” .rar in .rar** <http://www.makeuseof.com/tag/4-ways-email-attachments-file-extension-blocked/>)

c.L1_num+prenume_Python (.doc pentru aplicatiile Python [Tutorial 2.pdf](#));

RECOMANDARE: [Python intro.pdf](#)

Obs:

Punctaj maxim (Data trimiterii temei)			
<= 16.10.2019	22.10.2019	26.10.2019	30.10.2019
100 pct	80 pct	60 pct	50 pct

Obs. **Studentii “pasionati” (SI) de programare C++**, pot opta (**chiar sunt incurajati !!!**) sa foloseasca SI/ SAU framework-ul Omnet++ www.omnetpp.org/ , cu pastrarea scenariului pentru aplicatie, descris in laborator.

Referinte bibliografice:

<http://www.computerhope.com/issues/ch000444.htm>

<https://www.whatismyip.com/unix-ip-commands/>

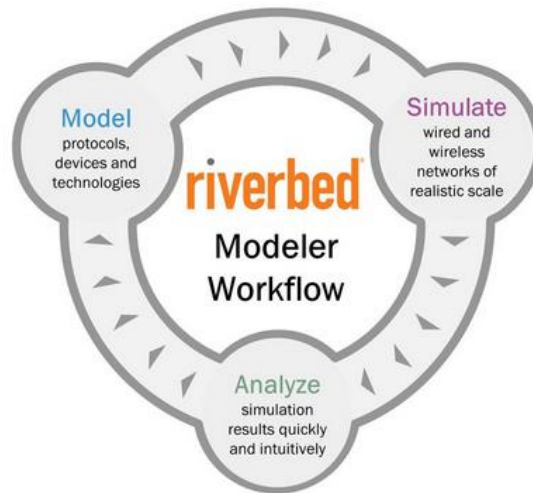
https://rpmapps.riverbed.com/ae/4dcgi/SIGNUP_NewUser

<http://www.cdsd.ro>

<http://www.winsocketdotnetworkprogramming.com/>

Anexa 1:

About Riverbed Modeler Academic Edition



Academic Edition Account Signup

https://rpmapps.riverbed.com/ae/4dcgi/SIGNUP_NewUser

Some of the restricted capabilities in *Riverbed Modeler Academic Edition*

<https://supportkb.riverbed.com/support/index?page=content&id=S24443>

Download Software

If you do not already have the Modeler Academic Edition installer, you may download it here. You may also review the system requirements for installing and running Modeler Academic Edition.

https://rpmapps.riverbed.com/ae/4dcgi/DOWNLOAD_HOME

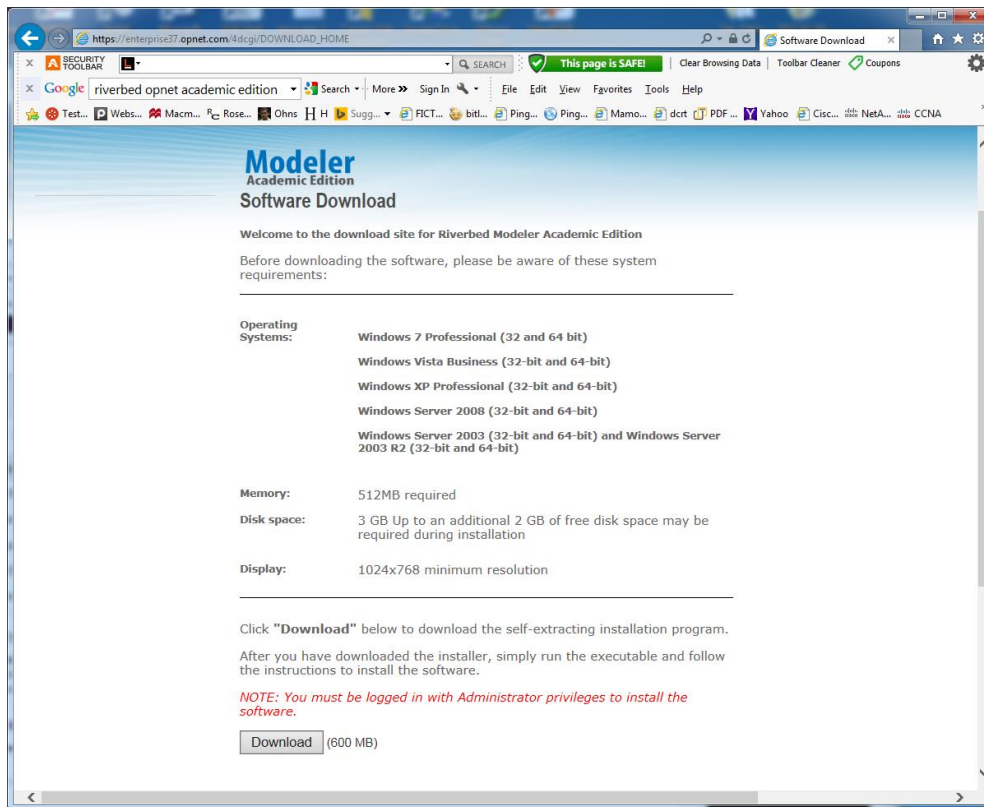
License Activation

After installation, run the software. It will guide you through the product activation process. In special cases you may need to access the license activation site directly.

Riverbed Modeler Academic Edition provides a virtual environment for modeling, analyzing, and predicting the performance of IT infrastructures, including applications, servers, and networking technologies. Based on Riverbed's award-winning Modeler product, Academic Edition is designed to complement specific lab exercises that teach fundamental networking concepts. The commercial version of Modeler has broader capabilities designed to increase network R&D productivity; develop proprietary wireless protocols and technologies; and evaluate enhancements to standards-based protocols. Riverbed software is used by thousands of commercial and government organizations worldwide, and by over 500 universities.

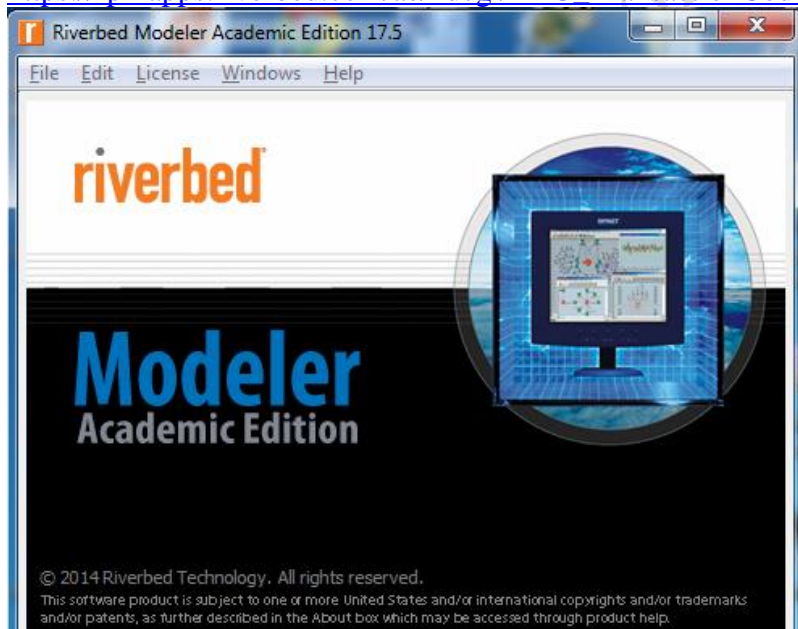
https://rpmapps.riverbed.com/ae/4dcgi/DOWNLOAD_HOME

Retele de calculatoare – Informatica anul 3 (2019-2020)



License Activation

https://rpmapps.riverbed.com/ae/4dcgi/REG_TransactionCode



Retele de calculatoare – Informatica anul 3 (2019-2020)

