# Lucrarea 1: Utilitare pentru analiza

# pachetelor si testarea functionarii retelelor TCP/IP

**Obiectivul acestei lucrari este prezentarea celor mai comune aplicatii utilizate in analiza si**

**testarea functionarii retelelor Internet. De asemenea, sunt studiate tehnicile aplicate**

**pentru functionarea acestor aplicatii.**

• **tcpdump**

• **ping**

• **arping**

• **traceroute**

**Captura de trafic: tcpdump**

Aplicatia **tcpdump** este utilizata pentru a realiza captura pachetelor de date transferate

prin retea, in urmatoarele cazuri: proiectarea retelei/protocoalelor, verificarea functionarii

unor servicii de retea pentru diagnoza, monitorizarea si realizarea de statistici de trafic.

Pachetele capturate pot fi afisate selectiv in mod text pe consola terminal sau salvate intrun

fisier. Alternativ, iesirea aplicatiei tcpdump poate fi prelucrata in vederea construirii

de grafice de trafic (ex. utilizand aplicatia **mrpr**).

Aplicatia tcpdump preia din retea pachetele capturate prin intermediul interfetei OSI de

nivel 2, corespunzatoare unei interfete locale de retea. In figura de mai jos se prezinta

modul de integrare al aplicatiei tcpdump in sistemul de comunicatie Linux. Interfata

aplicatiei tcpdump cu sistemul Linux este de tip API, fiind implementata prin intermediul

bibliotecii de functii de captura specializate, numita **pcap**.

****

In mod implicit, captura pachetelor se face in modul promiscuos. Acest mod de captura

presupune interceptarea tuturor pachetelor indiferent daca sunt, sau nu, adresate hostului

pe care aplicatia tcpdump ruleaza. Pentru captura pachetelor in modul promiscuos

aplicatia tcpdump trebuie sa fie executata cu drepturi de root (din cauza ca informatiile

care sunt capturare in mod neautorizat pot determina un risc de securitate ridicat pentru

retea).

****

Asa cum se poate remarca in figura de mai sus, aplicatia tcpdump interpreteaza orice

camp specific nivelelor OSI 2,3 si 4 cu scopul de a fi afisat intr-un format uman.

Comanda pentru executarea aplicatiei tcpdump are urmatoarea sintaxa generala:

**#tcpdump [optiuni] [expresie\_de\_filtrare]**

**Ex. 1: specificarea interfetei de retea**

Sa se realizeze o captura a traficului de pachete transferat de o entitate de retea cu mai multe interfete de retea, mai intai pe interfata eth0.

**#tcpdump –i eth0**

**Ex. 2: dezactivarea utilizarii serviciului DNS**

Sa se realizeze o captura a traficului de pachete transferat de o entitate de retea pe interfata eth0, cu afisarea adreselor Ip in format zecimal cu punct.

**#tcpdump –n**

**Ex. 3: afisarea antetului de nivel de legatura de date**

**#tcpdump –e**

**Ex. 4: afisarea detaliata a capturii**

**#tcpdump –vv**

**Ex. 5: salvarea in fisier a capturii**

Sa se realizeze o captura sis a se salveze in scopul consultarii ei ulterioare.

**#tcpdump –w filename**

**Ex. 6: citirea unei capture salvate in fisier**

Sa se afiseze pe ecran continutul capturii salvate la exercitiul anterior.

**#tcpdump –r filename**

**Ex. 7: filtrarea pachetelor capturate dupa adresa IP a sursei**

Sa se realizeze o captura care contine numai pachete transmise de entitatea de retea locala.

**#tcpdump –n src host 141.85.168.x**

**Ex. 8: filtrarea pachetelor capturate dupa adresa Ip a destinatiei**

Sa se realizeze o captura care contine pachetele transmise de entitatea de reta locala numai catre o anumita destnatie.

**#tcpdump –n dst host 141.85.168.1**

**Ex. 9: filtrarea pachetelor capturate dupa parametrul protocol**

Se vor captura numai pachetele de date care contin un antet de tip TCP/ARP.

**#tcpdump –n tcp**

**#tcpdump –n arp**

**Ex. 10: filtrarea pachetelor capturate dupa portul destinatie**

Se vor captura numai pachetele care sunt adresate serviciului web.

**#tcpdump –n tcp dst port 80**

**Testarea conectivitatii cu determinarea parametrilor de performanta ai**

**acesteia: ping (Packet InterNet Groper)**

Aplicatia **ping** este utilizata in principal pentru realizarea testelor functionale de

conectivitate si de testare a disponibilitatii destinatiei. In plus, ping raporteaza un set

minimal de parametrii de performanta a conectivitatii (ex. RTT, pachete pierdute), dintre

sursa S si destinatia D.

Aceasta aplicatie utilizeaza serviciul ICMP-ECHO pentru a realiza un dialog

REQUEST-REPLY. Testul poate fi realizat cu una sau mai multe destinatii simultan. De

regula, serviciul ICMP-ECHO este implementat in stiva TCP/IP a tuturor sistemelor de

comunicatie din retea (i.e hosturi, rutere, servere). Serviciul ICMP-ECHO a fost proiectat

special pentru realizarea unor astfel de teste de retea. In figura de mai jos este prezentata

functionarea serviciului ICMP-ECHO si a aplicatiei ping:



Astfel, entitatea S, genereaza mesaje “ICMP-ECHO REQUEST” catre entitatea D cu rata

determinata de valoarea prestabilita a parametrului **i**. Valoarea parametrului **i** reprezinta

intervalul de timp dintre doua transmisii consecutive. La receptia fiecarui mesaj trimis de

S, entitatea D raspunde cu mesajul “ICMP-ECHO REPLY”.

Pentru a asigura determinarea corecta a parametrilor de performanta RTT si loss atunci

cand se transmit mai multe mesaje de test incontinuu (**i** < RTT), este utilizat un mecanism

de asociere a mesajelor de tip cerere cu cele de tip raspuns. Acest mecanism consta in:

asignarea de catre S a unui **Id**entificator arbitrar fiecarui mesaj “ICMP-ECHO

REQUEST”, si apoi copierea **Id**entificatorului de catre D in mesajul raspuns “ICMPECHO

REPLY”.

Pentru masurarea parametrului RTT, este aplicata o metoda intuitiva care consta in

realizarea diferentei dintre momentul la care a inceput transmisia mesajului “ICMPECHO

REQUEST” (**t0**) si momentul la care s-a terminat receptia mesajului asociat

“ICMP-ECHO REPLY” (**t1**). Evident, valoarea RTT astfel determinata este dependenta

direct de timpul de procesare de catre entitatea D (**tproc**), dar si de durata de transmisie

data de mediul de comunicatie intre S si D (prin **tS-D trs + tD-S**

**trs**).

Comanda pentru executarea aplicatiei ping are urmatoarea sintaxa generala:

**ping [optiuni] <adresa\_IP> | <nume\_de\_domeniu>**

**Ex. 1: testarea unicast a conectivitatii IP**

Sa se testeze continuu conectivitatea dintre entitatea de retea locala si server.

**#ping 141.85.168.134**

**Ex. 2: dezactivarea utilizarii serviciului DNS**

Sa se testeze functionalitatea cu afisarea adreselor IP in format zecimal cu punct.

**#ping –n 141.85.43.134**

**Ex. 3: realizarea unui numar predefinit de teste**

**#ping –c 5 141.85.43.134**

**Ex. 4: configurarea intervalului de timp intre doua teste consecutive**

Sa se configureze o perioada pentru transmiterea mesajelor de test de 3 secunde.

**#ping –i 3 141.85.43.134**

**Ex. 5: testarea conectivitatii cu rata maxima.**

**#ping –f 141.85.43.134**

**Ex. 6: stabilirea numarului de octeti a mesajelor de test.**

Pentru testarea unei retele se cere sa se genereze mesaje de test de lungime de 100 octeti.

**#ping –s 92 141.85.43.134**

**Ex. 7: determinarea rutei mesajelor de test.**

**#ping –R 141.85.168.7**

**Detectarea coliziunilor de adrese in reteaua LAN: arping**

Ca si aplicatia ping, **arping** poate fi utilizata pentru testarea disponibilitatii unei entitati

de retea si a conectivitatii cu determinarea parametrilor de performanta asociati (RTT si

loss), in ambele moduri de operare (vezi mai jos). In plus, arping ofera un mijloc pentru

detectarea coliziunilor de adrese de nivel OSI L2 si L3, care pot apare intr-o retea de tip

LAN.

Aceasta aplicatie poate utiliza serviciul ARP sau ICMP-ECHO pentru a realiza un dialog

“ARP REQUEST-REPLY”, respectiv “ICMP-ECHO REQUEST–REPLY” cu o anumita

destinatie sau cu mai multe destinatii. De regula, toate sistemele de comunicatie TCP/IP

implementeaza aceste doua servicii.

Mesaje de test generate si descrierea functionarii:



**Ex. 1: determinarea adresei MAC si testarea conectivitatii ARP.**

Sa se determine adresa MAC a unei entitati D si parametrii RTT, intarziere si pierderi care caracterizeaza calitatea comunicatiei la un moment dat, dintre entitatea de retea locala si acea entitate D. Se cunoaste IPD=141.85.168.7

**#arping –v 141.85.168.7**

Mesajele de test ICMP generate si descrierea functionarii:



**Ex. 2: identificarea IP aunei entitati pe baza adresei MAC.**

Sa se determine adresa IP a unei entitati D si parametrii RTT, intarziere si pierderi care caracterizeaza calitatea comunicatiei, la un moment dat, dintre entitatea de retea locala si acea entitate D. Se cunoaste adresa MACD=MAC

**#arping <MM:MM:AA:AA:CC:CC>**

**Ex. 3: identificarea unei coliziuni de adrese MAC.**

Sa se determine daca exista doua statii cu aceasi adresa MAC la un moment dat. Se cunoaste adresa MACD=MAC

**#arping <MM:MM:AA:AA:CC:CC>**

**Aplicatia traceroute**

Descrierea functionarii si mesajele de test generate



**Ex. 1: determinarea rutelor mesajelor de test.**

Sa se determine pentru o retea calea pe care sunt derijate pachetele de date.

**#traceroute 141.85.254.16**

**Ex. 2: dezactivare utilizarii serviciului DNS.**

Sa se testeze functionalitatea cu afisarea adreselor IP in format zecimal cu punct.

**#traceroute –n 141.85.254.16**

**Ex. 3: configurarea intervalului de timp intre doua mesaje de test consecutive.**

Sa se genereze mesaje de test cu perioada de 1000 de milisecunde.

**#traceroute –z 141.85.254.16**

**Verificarea conectivitatii**

Administrarea unei retele implica in primul rand testarea conectivitatii fizice intre gazde:

* Testarea NIC-ului (adresei fizice a placii de retea)

**ifconfig/ipconfig**

* Verificarea conectivitatii via adresa IP

**ping x.x.x.x.**

* Verificarea continutului cache-ului ARP :**arp**
* Verificarea conectivitatii via adresa simbolica:

**ping host**

* Testarea rutei dintre gazde

**traceroute host**

* Testarea serviciilor software