Laborator nr 2

Auditarea utilizând comenzi Linux

La ora actuală este o tendință de a neglija comenzile clasice ale linuxului în detrimentul unor instrumente mai complexe mai sofisticate care au de multe ori și o interfață grafică. Totuși sunt situații în care auditarea trebuie realizată de pe dispozitive cu resurse reduse (cum ar fi microcontrolerele) sau se dorește utilizarea unui sistem de operare minimal (de exemplu o imagine în docker). În aceste condiții este necesar ca orice expert în domeniu să stăpânească fără probleme și aceste comenzi de bază.

1. Comenzi simple pentru analiza comportamentului și funcționării rețelei:

Packet InterNet Groper sau ping după cum este cunoscută comanda este o comandă care permite verificarea existenței ca activă (live) a unei stații în rețeaua locală sau internațională. El reprezintă de fapt utilizarea principiului radarului numai că acest lucru se realizează cu ajutorul unui pachet ICMP trimis și reprimit. Astfel se pot măsura timpii de întârziere (latența) unei comunicații cu respectivul nod aflat în test, timpul de viață al pachetului TTL

Suportă următorii parametri:

/? Lists command syntax options.
-t Pings the specified host until stopped with Ctrl+C. ping -t is also known as the ping of death. It can be used as a denial-of-service (DoS) attack to cause a target machine to crash.
-a rezolvă (dacă este posibil) numele adreselor prin care se trece)
-n contor se specifică explicit un număr de pachete de test la alegere
-r contor realizează o înregistrare a căii (numai pt IPV4) are valoare maximă 9 (pentru un număr mai mare de noduri se utilizează traceroute sau program dezvoltat special)
-s count marcaje temporale pentru duratele de la un nod la altul (numai pe IPV4)
-i TTL cu valoare maximă 255

ping www.yahoo.com
PING atsv2-fp-shed.wg1.b.yahoo.com (87.248.98.7) 56(84) bytes of data.
64 bytes from media-router-fp1.prod1.media.vip.ir2.yahoo.com (87.248.98.7): icmp_seq=1 ttl=48 time=59.1 ms

Ifconfig este deja înlocuită din diverse motive inclusiv de eficiență și securitate cu un subset de parametri de comandă echivalente ale comenzii ip și anume ip a (ip addr), ip link, ip -s (ip -stats). În consecință vom discuta comanda ip.Aceasta este utilizată pentru următoarele scopuri:

- găsirea interfețelor de comunicație configurate în sistemul curent
- aflarea stării interfeței IP
- configurarea buclei local de testare (loop-back) pentru Ethernet și alate interfețe IP
- pornirea sau oprirea funcționării unei anumite interfețe.
- Afișarea intrărilor din cache-ul ARP sau NDISC.
- asocierea, ștergerea, inițializarea rețelelor IP, a rutelor, a unor subrețele precum și ale altor informații pentru interfața IP.

- afișarea și gestionarea stării tuturor rețelelor active
- furnizarea informațiilor despre adresele multicast
- ștergerea sau inițializarea unei întrări în tabela de intrare
- afișarea obiectelor vecine cum ar fi cache ARP, invalidarea cache ARP, adăugarea unei intrări în cache-ul ARP și multe altele.
- găsirea unei căi către o adresă anume
- modificarea stării interfeței

După cum se observă această comandă este un integrator pentru majoritatea comenzilor specifice configurării parametrilor interfețelor de comunicare ale calculatorului gazdă și nu numai. Comanda suportă trei abordări generice prezentate mai jos

ip OBIECT COMANDA

ip [opțiuni] OBIECT COMANDĂ

ip OBIECT help

Obiectul referit în cadrul exemplelor generice de comandă poate fi ales într-o formă completă sau prescurtată din posibilitățile prezentate în tabelul de mai jos.

Obiect	**Formă prescurtată**	**Scopul**
link	l	Dispozitiv de rețea
address	a addr	Adresă protocol (IP sau IPv6) pe un dispozitiv
addrlabel	addrl	Configurarea etichetei pentru selectarea adresei protocol.
neighbour	n neigh	Intrare în cache ARP sau NDISC.
route	r	Intrare în tabela de rutare.
rule	ru	Regulă în baza de date cu politici de rutare
maddress	m maddr	Adresă multicast
mroute	mr	Intrare în cache-ul de rutare multicast
tunnel	t	Tunel peste IP.
xfrm	x	Framework pentru protocolul IPsec.

Dacă se doresc informații despre un obiect se pot folosi comenzile de ajutor în următoarea manieră:

ip OBIECT help

ip OBIECT h

ip a help

ip r help

Să prezentăm câteva exemple simple de utilizare:

- afișarea tuturor informațiilor despre toate interfețele de comunicare se face cu:

ip a

Sau

ip addr

Dacă vreaun numai cele care utilizează numai IPV4
ip -4 a
Dacă vreau numai informații specifice despre o anumită interfață de rețea
ip a show eth0
ip a list eth0
ip a show dev eth0
Sau pot afișa numai interfețele active cu
ip link ls up
Pentru adăugarea unei adrese IP pentru o interfață anume:
Generic ip a add {ip_addr/mask} dev {interface}
De exemplu pentru a asocia adresa 192.168.1.200/255.255.255.0 la eth0:
ip a add 192.168.1.200/255.255.255.0 dev eth0
sau
ip a add 192.168.1.200/24 dev eth0
Adăugarea unei adrese de broadcast la o interfață nu este realizată implicit de comandă. Acest lucru trebuie specificat explicit utilizând următoarele sintaxe alternative.
ip addr add brd {ADDDRESS-HERE} dev {interface}
ip addr add broadcast {ADDDRESS-HERE} dev {interface}
ip addr add broadcast 172.20.10.255 dev dummy0
Este permisă de asemenea utilizarea simbolurilor speciale cum ar fi +/- în locul adresei de broadcast prin setarea sau resetarea biților care descriu interfața. În exemplul următor se stabilește adresa 192.168.1.50 cu masca de rețea 255.255.255.0 (/24) care are broadcast standard și eticheta “eth0A” către interfața eth0:
ip addr add 192.168.1.50/24 brd + dev eth0 label eth0Home
Se poate face o referire circulară inclusiv către loop-back-ul sistemului
ip addr add 127.0.0.1/8 dev lo brd + scope host
Se poate elimina sau șterge o adresă de IP asociată unei interfețe anume, comanda are următoarea sintaxă:
ip a del {ipv6_addr_OR_ipv4_addr} dev {interface}
Dacă , de exemplu, dorim să ștergem 192.168.1.200/24 de la eth0:
ip a del 192.168.1.200/24 dev eth0
Golirea condiționată (flush) unei adrese IP. Deși se poate adresă cu uadresă sunt situații în care dorim să procesăm toate stațiile dintr-un segment de rețea. De exemplu toate adresle dintr-o rețea privată 192.168.2.0/24 pot fi simultan șterse cu:
ip -s -s a f to 192.168.2.0/24
Dacă de exemplu doresc să dezactivez toate adresele IP pentru toate interfețele pot da:
ip -4 addr flush label "ppp*"
La fel și pentru interfețele etc:
ip -4 addr flush label "eth*"
Pentru pornirea sau oprirea din funcționare a unei interfețe se va folosi următoarea sintaxă
ip link set dev {DEVICE} {up|down}
De exemplu pentru a opri eth1

ip link set dev eth1 down
iar pentru a o porni
ip link set dev eth1 up
Dacă se dorește modificarea explicită a dimensiunii cozii de transmisie txqueuelen pentru un dispozitiv se poate folosi:
ip link set txqueuelen {NUMBER} dev {DEVICE}
De exemplu dacă vreau sa modific valoarea lui txqueuelen de la 1000 la 10000 pentru eth0:
ip link set txqueuelen 10000 dev eth0
ip a list eth0
Se poate modifica inclusiv maximum transmision units sau MTU
ip link set mtu {NUMBER} dev {DEVICE}
De exemplu pentru a schimba MTU pentru eth0 la 9000:
ip link set mtu 9000 dev eth0
și verificăm că s-a schimbat cu:
ip a list eth0
Pentru afișarea cache neighbour/arp:
ip n show
ip neigh show
Ultimul câmp al rezultatului va afișa starea procesului detecției disponibilității vecinului pentru fiecare intrare și poate fi:

STALE - atunci când vecinul este funcțional dar probabil nu există o cale către el deci kernel-ul va încerca să verifice acest lucru la prima transmisie.

DELAY – un pachet a fost trimis către un vecin aflat in STALE și kernelul așteaptă să primească confirmarea.

REACHABLE – vecinul precum și comunicarea cu el sunt funcționale.

Pentru adăugarea unei noi intrări ARP se va utiliza:
ip neigh add {IP-HERE} lladdr {MAC/LLADDRESS} dev {DEVICE} nud {STATE}
Și un exemplu unde se va adăuga un ARP permanent către vecinul 192.168.1.5 utilizând interfața eth0:
ip neigh add 192.168.1.5 lladdr 00:1a:30:38:a8:00 dev eth0 nud perm
În această sunt utilizați o serie de termeni al cărui înțeles se găsește în tabloul de mai jos.

Stare neighbour (nud)	Înțeles
permanent	Intrarea neighbour este considerată implicit ca fiind permanent validă și poate fi eliminată numai de către administrator
noarp	Intrarea neighbour este validă. Nu se va face nicio încercarea de verificare a acesteia.
stale	Intrarea neighbour este validă dar există suspiciuni. Utilizarea acestei opțiuni la ip neigh nu va schimba starea vecinului dacă aceasta a fost validp iar comanda nu conține și instrucțiuni de modificare a adresei.
reachable	Intrarea neighbour este validă până la expirarea timpului prestabilit.

Ștergerea unei intrări ARP
Următoarea sintaxă poate fi utilizată pentru a șterge sau invalida o intrare ARP pentru vecinul 192.168.1.5 pe dispozitivul eth1:
ip neigh del {IPAddress} dev {DEVICE}
ip neigh del 192.168.1.5 dev eth1
Pentru schimbarea stării vecinului neighbour 192.168.1.100 de pe interfața eth1
ip neigh chg 192.168.1.100 dev eth1 nud reachable
Golirea unei intrări ARP
Mai jos se dă sintaxa pentru golirea condiționată a tabelelor pentru neighbour/arp tables
ip -s -s n f {IPAddress}
Și un exemplu
ip -s -s n f 192.168.1.5
sau
ip -s -s n flush 192.168.1.5
Cu această comandă se poate realiza și gestionarea tabelei de rutare inclusiv manipularea tablelei de rutare de la nivelul kernelului. Pentru afișarea tablei vom folosi:
ip r
ip r list
ip route list
ip r list [options]
ip route
Afișarea rutei pentru 192.168.1.0/24:
ip r list 192.168.1.0/24
Pentru adăugarea unei noi rute sintaxa va fi:
ip route add {NETWORK/MASK} via {GATEWAYIP}
ip route add {NETWORK/MASK} dev {DEVICE}
ip route add default {NETWORK/MASK} dev {DEVICE}
ip route add default {NETWORK/MASK} via {GATEWAYIP}
Și un exemplu de adăugare a unei căi catre rețeaua 192.168.1.0/24 utilizând poarta (gateway) 192.168.1.254
ip route add 192.168.1.0/24 via 192.168.1.254
Pentru a dirija tot traficul prin gateway-ul următor utilizând interfața eth0
ip route add 192.168.1.0/24 dev eth0
Ștergerea unei rute
Dacă doresc să șterg o poartă
ip route del default
În acest exemplu se va șterge calea creată în exemplul anterior
ip route del 192.168.1.0/24 dev eth0
Dacă se dorește schimbarea adresi MAC pentru placa de rețea numită NIC
NIC="eno1" ## <-- NUmele meu ##
ip link show $NIC
ip link set dev $NIC down
stabilirea unei noi adrese MAC
ip link set dev $NIC address XX:YY:ZZ:AA:BB:CC
ip link set dev $NIC up

Deoarece în multe din exemplele din Internet este des folosită comanda ifconfig mai jos se găsește un tabel cu exemple de utilizare cu ajutorul comenzii ip.

Vechea comandă (depășită)	Se echivalează cu
ifconfig -a	ip a
ifconfig enp6s0 down	ip link set enp6s0 down
ifconfig enp6s0 up	ip link set enp6s0 up
ifconfig enp6s0 192.168.2.24	ip addr add 192.168.2.24/24 dev enp6s0
ifconfig enp6s0 netmask 255.255.255.0	ip addr add 192.168.1.1/24 dev enp6s0
ifconfig enp6s0 mtu 9000	ip link set enp6s0 mtu 9000
ifconfig enp6s0:0 192.168.2.25	ip addr add 192.168.2.25/24 dev enp6s0
netstat	ss
netstat -tulpn	ss -tulpn
netstat -neopa	ss -neopa
netstat -g	ip maddr
route	ip r
route add -net 192.168.2.0 netmask 255.255.255.0 dev enp6s0	ip route add 192.168.2.0/24 dev enp6s0
route add default gw 192.168.2.254	ip route add default via 192.168.2.254
arp -a	ip neigh
arp -v	ip -s neigh
arp -s 192.168.2.33 1:2:3:4:5:6	ip neigh add 192.168.3.33 lladdr 1:2:3:4:5:6 dev enp6s0
arp -i enp6s0 -d 192.168.2.254	ip neigh del 192.168.2.254 dev wlp7s0

NSlookup
Principalul scop al acestei comenzi este să ajute la rezolvarea problemelor specifice DNS. Aceasta poate fi utilizată în două moduri: interactiv și cu parametri. Pentru intrarea în mod interactiv se va lansa comanda de la tastatură și ea va prezenta un prompter. În celălalt caz vom avea de exemplu:
nslookup mail.yahoo.com
Care va extrage informații suplimentare (utilizând reverse DNS)
Dacă se doresc și informații specifice
nslookup qureytype=mx mail.yahoo.com
Evident că trebuie testată pe un server mai puțin protejat deoarece yahoo nu va răspunde unei astfel de comenzi.
Dacă nu se doresc toate informațiile despre nod se poate încerca utilizarea următorilor parametri
HINFO pentru a afla tipul procesorului și sistemul de operare instalat
UNIFO ne dă numele utilizatorului

MB dă numele de domeniu al serverul de poștă electronică
MG ne dă numele unui membru din grupul de poștă electronică
MX dă numele serverului de poștă electronică

Traceroute - ne permite afișarea informațiilor cu privire la nodurile prin care se trece de la punctul de origine până la o adresă anume:
traceroute mail.yahoo.com
Iar dacă se dorește evitarea rezolvarea DNS
traceroute -d mail.yahoo.com

Netstat - de multe ori suntem interesați să știm informații detailate despre toate comunicațiile inițiate de către stația curentă cu exteriorul. Pentru aceasta s-a introdus nestat. Evident că se poate folosi un grep în caz că dorim o informație mai punctuală

Legat de informațiile afișate 0.0.0.0 referă un fel de adresă generică
Testați netstat -sp 0.0.0.0

the 0.0.0.0 is called a por

Sau dati un ip a vedeti adresa locala a stației și dați de exemplu
Netstat -sp 192.168.0.4
Dacă se dorește să identificăm și procesul care comunică vom utiliza
Netstat -nao
Care îi va afișa pid-ul
Pentru cei care stiu deja jucați-vă și cu nmap.

Temă de laborator
- Testați fiecare comandă cu diverse combinații de parametri (când acest lucru este posibil).

Temă pe acasă:
Faceți o analiză completă a subrețelei din cămin (din punct de vedere al fiecăruia dintre voi) - extrageți structura ca un graf cu stațiile detectate active iar pentru fiecare stație realizați o fișă cu privire la cele descoperite din analiza ei. Să nu uiești din subrețeaua voatră că aveți probleme cu nodul. Cei care nu stau în cămin deconectează legătura cu isp-ul și fac analiză pe calculatoarele din rețeau locală (mama, tata, desktop etc)