TEHNIČKA ŠKOLA RUĐERA BOŠKOVIĆA
Zagreb, Getaldićeva 4

Nastavni predmet	DIJAGNOSTIKA I ODRŽAVANJE INFORMACIJSKIH SUSTAVA
Naslov jedinice	Vježba 1: Praćenje i analiza mrežnog prometa

CILJ VJEŽBE

Učenik će znati samostalno pratiti i analizirati mrežni promet te koristiti naredbe ping i nslookup u dijagnostici problema u radu mreže.

IZVOĐENJE VJEŽBE

1) Naredba *ping*

Kad se pojavi problem u radu neke mrežne aplikacije, obično se prvo provjerava postojanje povezanosti na mrežnom sloju. Jednostavno rečeno, potrebno je ustanoviti prolaze li uopće IP paketi od jednog do drugog računala između kojih se pojavio problem u komunikaciji. Upravo u tu svrhu koristi se naredba *ping*.
Naredba *ping* omogućava ispitivanje povezanosti između računala na kojem se naredba koristi i bilo kojeg od ostalih računala i čvorova u mreži.

Sintaksa naredbe:
`ping <adresa ili ime odredišnog računala>`

Ova naredba šalje upit prema navedenom odredišnom računalu te na taj upit odredišno računalo odgovara. Ukoliko naredba *ping* primi odgovor, ona ga ispiše i korisnik ima informaciju da je odredišno računalo dostupno. U slučaju da se ne primi odgovor, postoji problem povezanosti između dotičnih računala.

1) U komandnoj liniji računala, isprobajte naredbu *ping*. U bilježnicu ispišite sadržaj ekrana.
2) Koji je naziv odredišnog računala i njegova IP adresa?
3) Koja je veličina paketa koji se šalje?
4) Koliko je upita poslano? Sadrže li svi iste podatke? Ako ne, koji je razlog?
5) Koja je vrijednost TTL? Što ona predstavlja?
6) Uz pomoć naredbe -?, proučite i zapišite opcije.
7) Utvrdite i objasnite što se događa pri slanju paketa koji u TTL polju ima vrijednost 3, a odredišno računalo je udaljeno više od 3 skoka.
8) Pokrenite alat Wireshark i sučelje na kojem želite pratiti mrežni promet (mrežna kartica računala).
9) U komandnoj liniji upišite `ping www.google.com`
10) Zaustavite praćenje prometa.
11) Koji protokoli se javljaju u pojedinim paketima? Koja je njihova zadaća?
12) Na kojem se protokolu temelji naredba *ping*?
13) Zašto se u uhvaćenom prometu javlja protokol DNS?

14) Na isti način provjerite dostupnost pojedinih računala u laboratoriju. Detaljno analizirajte uhvaćeni slijed paketa koji je generirala naredba *ping*. Utvrdite koji su sve protokoli iskorišteni kao posljedica izvođenja naredbe *ping* i koji je odnos među njima (tj. koje druge protokole svaki pojedini protokol koristi). Zapišite svoja zapažanja.
15) Isprobajte naredbu dodavanjem parametra **-t**. Kako sada radi *ping*? Pratite promet pomoću Wiresharka te objasnite i zapišite rezultate.
16) Isprobajte naredbu dodavanjem parametra **-a**. Kako sada radi *ping*? Pratite promet pomoću Wiresharka te objasnite i zapišite rezultate.
17) Isprobajte naredbu dodavanjem parametra **-n**. Kako sada radi *ping*? Pratite promet pomoću Wiresharka te objasnite i zapišite rezultate.
18) Isprobajte naredbu dodavanjem parametra **-l** (npr. 10000). Kako sada radi *ping*? Pratite promet pomoću Wiresharka te objasnite i zapišite rezultate.
19) Isprobajte naredbu dodavanjem parametra **-i**. Kako sada radi *ping*? Koliko je skokova potrebno za dohvatiti www.google.com? Pratite promet pomoću Wiresharka te objasnite i zapišite rezultate.
20) Postoji li način da se iz primljenog paketa očita put kojim je paket prošao kroz mrežu?

2) Naredba nslookup

Naredba *nslookup* očitava DNS zapis i omogućuje nam da dobijemo IP adresu na osnovu imena domene ili ime domene na osnovu IP adrese.
Budući da se ovi podaci nalaze u DNS serverima naredba *nslookup* je u stvari upit DNS serveru za ove podatke.

Sintaksa naredbe:
`nslookup [-dodatna opcija=X] [računalo/poslužitelj]`

1) U komandnoj liniji računala, isprobajte naredbu *nslookup*. U bilježnicu ispišite sadržaj ekrana. Uz pomoć alata Wireshark, proučite promet koji se odvija tijekom upita. Koji protokoli se javljaju? Posebno proučite pakete vezane za protokol DNS.
2) Naredbu ? iskoristite na dva načina:
   - nslookup ?
   - nslookup [enter]
     > ?

   Proučite i zapišite opcije koje se nude u oba slučaja.
3) Zatražite odgovor za IP adresu vašeg računala. U bilježnicu zapišite rezultate. Pratite promet pomoću Wiresharka i objasnite rezultate.
4) Zatražite DNS odgovor za neke poznatije domene, npr. www.google.com. Koji odgovor ste dobili? Pokušajte zaključiti zašto je odgovor takav.
   Pratite promet pomoću Wiresharka i objasnite rezultate. Objasnite značenje pojedinih informacija u odgovoru.
5) Uz pomoć dodatne opcije `querytype=SOA`, saznajte koji je nadležni DNS poslužitelj za www.google.com. Iskoristite tu informaciju kako biste dobili autoritativni odgovor na nslookup upit za www.google.com (`nslookup -querytype=soa ime.posluzitelja`).
   Pratite promet pomoću Wiresharka i objasnite rezultate. Objasnite značenje pojedinih informacija u odgovoru.
6) Uz pomoć dodatne opcije `querytype=PTR`, saznajte ime poslužitelja na temelju IP adrese. (npr. 8.8.4.4)

3) Naredba Tracert

Paketi od jednog do drugog računala putuju mrežom, preko niza drugih računala.
Naredba *tracert* pokazuje vrijeme putovanja paketa do svakog pojedinog uređaja kroz koji je paket prošao na putu do odredišta. Na ovaj način, možemo ustanoviti točno mjesto gdje dolazi do greške.

U LINUX-u naredba je traceroute.

Sintaksa naredbe:
`tracert [-dodatna opcija] [računalo/poslužitelj]`

1) U komandnoj liniji računala, isprobajte naredbu *tracert*. U bilježnicu ispišite sadržaj ekrana.
2) Pokrenite alat Wireshark i sučelje na kojem želite pratiti mrežni promet (mrežna kartica računala).
3) U komandnoj liniji upišite tracert www.google.com
4) Zaustavite praćenje prometa.
5) Koji protokoli se javljaju u pojedinim paketima? Koja je njihova zadaća?
6) Na kojem protokolu se temelji naredba *tracert*?
7) Isprobajte naredbu dodavanjem parametra **-d.** Kako sada radi *tracert*? Pratite promet pomoću Wiresharka i zapišite rezultate.
8) Isprobajte naredbu dodavanjem parametra **-w** (npr. 20). Kako sada radi *tracert*? Pratite promet pomoću Wiresharka i zapišite rezultate.
9) Isprobajte naredbu dodavanjem parametra **-h** (npr. 10). Kako sada radi *tracert*? Pratite promet pomoću Wiresharka i zapišite rezultate.

4) Naredba Netstat

Prikazuje aktivne TCP veze, portove na kojima računalo sluša, Ethernet statistike, IP tablice usmjeravanja, IPv4 statistike (za IP, ICMP, TCP i UDP protokole) i IPv6 statistike (za IPv6, ICMPv6, TCP preko IPv6 , i UDP preko IPv6 protokola). Kada se koristi se bez parametara, netstat prikazuje aktivne TCP konekcije.

Sintaksa naredbe:
`netstat [dodatna_opcija]`

1) U komandnoj liniji računala, isprobajte naredbu *netstat /?* U bilježnicu ispišite sadržaj ekrana.
2) U komandnoj liniji računala, isprobajte naredbu *`netstat -e -s`* Za koje sve protokole je prikazana statistika
3) U komandnoj liniji računala, isprobajte naredbu *`netstat -s -p tcp`* i naredbu *`netstat -s -p udp`* U bilježnicu zapišite i objasnite rezultate. Objasnite značenje pojedinih informacija.
4) U komandnoj liniji računala, isprobajte naredbu *`netstat -n -o`* U bilježnicu zapišite i objasnite rezultate. Objasnite značenje pojedinih informacija.
5) U komandnoj liniji računala, isprobajte naredbu *`netstat -r`* U bilježnicu zapišite i objasnite rezultate. Objasnite značenje pojedinih informacija.

6) Naredba Pathping

Pruža informacije o latenciji mreže i gubitku na skokovima između uređaja koji se nalaze između izvora i odredišta. Naredba šalje više echo zahtjeva svakom usmjerivaču između izvora i odredišta tijekom vremenskog razdoblja, a zatim izračunava rezultate na temelju paketa koji se vraćaju iz svakog usmjerivača.
Budući da *pathping* prikazuje stupanj gubitka paketa u bilo kojem zadanom routeru ili vezi, može se odrediti koji usmjerivači ili podmreže mogu imati mrežnih problema.
Pathping izvodi ekvivalent *tracert* naredbe identificiranjem koji usmjerivači su na putanji, tada šalje pingove periodički na sve usmjeritelje u određenom vremenskom razdoblju i izračunava statistiku na temelju broja koji se vraća iz svakog od njih.

Sintaksa naredbe:
`pathping [-dodatna_opcija] [računalo/poslužitelj]`

1) U komandnoj liniji računala, isprobajte naredbu *pathping* U bilježnicu ispišite sadržaj ekrana.
2) Pokrenite alat Wireshark i sučelje na kojem želite pratiti mrežni promet (mrežna kartica računala).
3) U komandnoj liniji upišite pathping www.google.com
4) Zaustavite praćenje prometa.
5) Koji protokoli se javljaju u pojedinim paketima? Koja je njihova zadaća?
6) Na kojem protokolu se temelji naredba *pathping*?
7) Isprobajte naredbu dodavanjem parametra **-n.** Kako sada radi *pathping*? Pratite promet pomoću Wiresharka i zapišite rezultate.
8) Isprobajte naredbu dodavanjem parametra **-p** (npr. 40). Kako sada radi *pathping*? Pratite promet pomoću Wiresharka i zapišite rezultate.

Nakon obavljenih zadataka u ovoj vježbi učenik će znati samostalno (ili uz manju pomoć zabilješki):

- pratiti i analizirati promet na vezi sa programom za praćenje protokola
- koristiti naredbe ping, nslookup, tracert, netstat i pathping s dodatnim opcijama prilikom iščitavanja informacija o mreži

Provjera znanja:

1. Bilješke i točni odgovori na pitanja iz vježbe – 3 boda
2. Točni odgovori i objašnjenje na postavljena pitanja – 3 boda

2 b – nedovoljan , 3 b – dovoljan, 4 b – dobar, 5 b – vrlo dobar, 6 b - odličan