**ICMP - Windows**

1. **Koliko paketov se dejansko prenese med izvorom in ciljem?**

Med izvorom in ciljem se dejansko izvede **20 prenosov paketov oziroma za vsak request se izvede reply, torej 10 requestov in 10 replyjev**. Opazimo lahko, da je request poslan iz našega izvornega IP naslova 164.8.163.40 na ciljni IP naslov 164.8.8.99 desetkrat. Prav tako je obratno nato poslanih 10 reply paketov. Tukaj je **paketov 20 saj se je ping ukaz izvedel v celoti brek napake, ob napaki pa bi lahko bilo teh paketov manj.**

Število paketov lahko preštejemo ali pa uporabimo orodje “Capture File Properties” in pod Displayed pridobimo število poslanih in prejetih paketov.

A screenshot of a computer

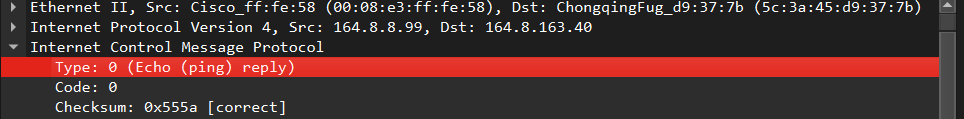
Description automatically generated

1. **Kakšnega tipa so paketi za zahtevo in kakšnega tipa so paketi za odgovor?**

Paketi za **zahtevo (request) so tipa 8 Echo Ping Request, paketi za odgovor (reply) pa so tipa 0 Echo Ping Reply**. To je razvidno iz analize paketov kot je razvidno na sledečih slikah.

A screen shot of a computer

Description automatically generated



1. **Zapišite MAC naslov mrežne kartice, ki se nahaja v ciljnem računalniku.**

MAC naslov mrežne kartice na ciljnem računalniku/strežniku je **00:08:e3:ff:fe:58 oziroma Cisco\_ff:fe:58**, kar pridobimo iz analize prometa kot je razvidno na sliki spodaj. Tu moramo **paziti kateri tip paketa analiziramo** saj je source pri request zahtevi naš računalnik, destination pa ciljni naslov, medtem pa je to ravno obratno ko govorimo o reply zahtevi.

A screenshot of a computer

Description automatically generated

1. **Koliko zlogov se prenaša v polja "Data" in kakšna je vsebina polja?**

V poljih Data se prenaša **32 zlogov oz. 32 bytes**. Vsebina teh je **nepopolna abeceda oz. ASCII sekvenca** in sicer **abcdefghijklmnopqrstuvwabcdefghi.** Ta vsebina je razbrana iz Data analize posameznih paketov, wireshark pa te tudi pretvori iz bitne v nam razumljivo obliko.

A screenshot of a computer

Description automatically generated

**ICMP – Linux**

1. **Koliko paketov se dejansko prenese med izvorom in ciljem?**

Tudi ukaz izveden na Linux sistemu dejansko **izvede 20 prenosov. 10 od teh je requestov in 10 je replyjev.** Za razliko od Windows testa je tu **izvorni naslov drugačen zaradi virtualnega okolja in drugega omrežja**. Izvorni naslov je 172.19.185.220 ter **ciljni ostaja enak pri 164.8.8.99.** Pravtako lahko število paketov preštejemo oz. Uporabimo Capture File Properties kot je razvidno iz slike spodaj.

A screenshot of a computer

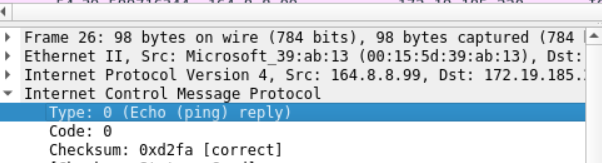
Description automatically generated

1. **Kakšnega tipa so paketi za zahtevo in kakšnega tipa so paketi za odgovor?**

Paketi tudi na Linuxu ostajajo **enakega tipa torej 8 Echo Ping Request za zahtevo ter 0 Echo Ping Reply za odgovor.** To velja saj ne glede na napravo, delovanje po protokolu naj bi ostalo enako oz. Standardno.

A screenshot of a computer

Description automatically generated



1. **Zapišite MAC naslov mrežne kartice, ki se nahaja v ciljnem računalniku.**

Pri MAC naslovu mrežne kartice ciljnega računalnika pa se **pojavi razlika, saj je tu zaradi virtualizacije Linux okolja z Microsoftovim orodjem Hyper-V ciljni MAC naslov vmesnik med virtualko in dejanskim ciljem**. Ta naslov je **00:15:5d:39:ab:13 oz. Microsoft 39:ab:13.** Razlika je tudi v izvornem naslovu, kjer je MAC tudi Microsoftov vmesnik z naslovom 00:15:5d:21:dl:01 oz. Microsoft\_21:dl:01.

A screenshot of a computer

Description automatically generated

1. **Koliko zlogov se prenaša v polja "Data" in kakšna je vsebina polja?**

Tudi **v velikosti vsebine oz. števila zlogov je razlika, saj se pri Linuxu namesto 32 zlogov prenese 40 zlogov oz. bytov, kar je zanimivo saj se ta ne ujema z statistiko razbrano v konzolnem oknu ob izvedbi ukaza ping.** V konzoli lahko opazimo, da je bilo **poslanih 64 zlogov v vsakem od paketov. Razlika o velikosti paketa je zaradi privzete nastavitve velikosti, ki pa je za oba OS različna, razen če to ročno spremenimo.**

Razlika je tudi v vsebini sami, kjer lahko razvidimo da vsebina niso več črke abecede ampak **druga sekvenca ASCII** kodiranja **----------------!”#$%&’()\*+,-./01234567.**

A screen shot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Komentirajte razlike in podobnosti med izvedbo ukaza *ping* na sistemu Windows in Linux. Razlike utemeljite.**

Z izvedbo ukazov ping na obeh operacijskih sistemih smo opazili kar nekaj razlik in podobnosti, ki so bile že omenjene malo višje. Te podobnosti pa bomo še izpostavili in utemeljili.

* **Količina prenešenih paketov med izvorom in ciljem:**

Ker smo v samem ukazu ping **definirali število paketov**, ki jih želimo poslati na ciljni naslov oz. domeno **z zastavicama -n in -c in to omejili na 10 paketov** se je med naslovoma **preneslo 20 paketov**, saj **vsak paket, ki smo ga poslali (request) je pridobil odgovor (reply).** Če bi prišlo do napake bi bilo teh paketov najverjetneje manj, hkrati pa, če bi izvedli ping ukaz brez omejitve bi pošiljali pakete dokler pošiljanja ne bi ročno ustavili ali pa bi se ta izvedel le štirikrat, odvisno od OS.

* **MAC naslov ciljne naprave:**

Prva vidna razlika med Windows in Linux operacijskim sistemom se je pojavila pri MAC naslovih. Tu smo **zaradi virtualnega okolja** opazili, da je **ciljni tako kot izvorni MAC naslov drugačen**. Ker smo za gostenje virtualnega okolja uporabili Microsoftovo Hyper-V za virtualizacijo smo opazili, da se med izvorom in ciljem pojavita **“vmesnika” oz. virtualna MAC naslova namesto dejanskih MAC naslovov naše in ciljne naprave.** Pomembno pa je izpostaviti, da je to zaradi virtualnega okolja, **če istočasno zajamemo promet na napravi, ki gosti virtualno okolje opazimo, da ICMP promet, ki je bil izveden znotraj virtualke dejansko potuje skozi gostiteljsko napravo do cilja zato je tudi ciljni IP naslov znotraj virtualke enak, čeprav se razlikuje v MAC naslovu**, saj je promet posredovan iz virtualke na gostiteljsko napravo in nato do ciljnega MAC naslova, ki pa je enak kot tisti na Windowsu.

A screenshot of a computer

Description automatically generated

* **Tip prejetih in poslanih paketov:**

Ugotovili smo, da **ne glede na okolje (Linux ali Windows) bosta tipa paketov vedno enaka.** To je zaradi ICMP protokola, ki deluje kot standard in bo zato enak ne glede na naprava oz. okolje na katerem se izvaja. **Tip za zahteve je 8 Echo Ping Request ter tip za odgovore je 0 Echo Ping Reply**.

* **Število zlogov in vsebina paketov:**

Tudi tukaj se pojavi razlika tako kot v številu zlogov, kot tudi v vsebini posameznih paketov. **Na Windowsu ukaz ping posreduje deset 32 bytnih zahtev in pridobi deset 32 bytnih odgovorov. Medtem pa na Linuxu ukaz ping posreduje deset 64 bytnih zahtev in prejme deset 64 bytnih odgovorov**. To velja, če gledamo samo na konzolni izpis, ki vsebuje poleg same vsebine še ostale podatke o samem paketu – glava (header). Velikost paketov lahko **omejimo z zastavico -s (size) primarno pa velja da na Windowsu se prenašajo 32 bytni paketi, na Linuxu pa 64 oz. 58 bytni paketi.** Zato lahko sklepamo, da **Wireshark analizira te pakete z neko omejitvijo oz. najverjetneje skrči vsebino in ohrani le pomembne podatke**.

Prav tako se pojavi razlika v sami vsebini paketov. Do te razlike pride zaradi **razlike med operacijskima sistemoma Windows in Linux in načinom pošiljanja vsebine. Windows v paket po privzetem vključi ASCII znake od specifičnega znaka dalje ter s tem zajame večji del abecede, medtem ko Linux vključi neko drugo sekvenco, ki pa se lahko razlikuje med distribucijami Linuxa. Pri tem pa še vedno uporabi ASCII** kodiranje. Te razlike načeloma ne vplivajo na delovanje oz. povzročijo razlik v hitrosti pinganja, lahko pa v samem ukazu **določimo kaj želimo vključiti v ping ukaz z zastavico -p.**

Ugotovimo lahko, da čeprav se med operacijskimi sistemi pojavijo razlike, pa samo delovanje protokola oz. ukaza protokola ICMP vrača bolj kot ne iste rezultate.

**HTTP**

1. **Zapišite IP naslov vašega računalnika, IP naslov strežnika in različico HTTP protokola.**Promet je potekal **med IP naslovom 192.168.0.32, ki predstavlja našo napravo, ter IP naslovom strežnika, ki pa je 45.33.7.16.** Ta naslova razberemo iz analize prometa, kjer Source predstavlja izvor Destination pa cilj, pr item pa moremo paziti, da gledamo pravilno zahtevo saj sta zahteva in odgovor obratna.

**A screenshot of a computer

Description automatically generated**

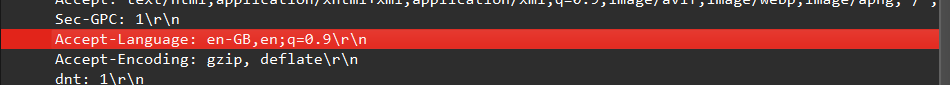
Pri tem pa se je uporabil **protocol HTTP in sicer verzija HTTP 1.1**, kar razberemo iz opisa Hypertext Transfer Protocol zavihka pod Request Version.

**A screen shot of a computer

Description automatically generated**

1. **V katerih jezikih želi vaš spletni brskalnik sprejeti vsebino spletne strani? Kako se imenuje polje protokola HTTP v katerem so definirani jeziki?**

Naš spletni brskalnik želi sprejeti vsebino spletne strain **v angleškem jeziku, kar je definirano v sami HTTP zahtevi** poslani na spletni strežnik. To razberemo iz **polja Accept-Language**, ki navaja da je sprejemljiv jezik oz. locale **en-GB**.

****

1. **Koliko zlogov je bilo prenešenih na vaš računalnik *(vsebina HTML strani, CSS, JavaScript, Flash, slike, ...)*? Koliko časa *(v sekundah)* je preteklo od prve zahteve vašega spletnega brskalnika do zadnje prenešene vsebine iz spletnega strežnika?**

Na našo napravo je bilo **prenešenih 131024 bytov oz. zlogov vsebine**. Ta vsebina je **prispela v 363 paketih, za prenos pa je bilo potrebnih 21.851 sekund**. Tu je **pomembno, da ob analizi uporabimo ustrezen filter in sicer http.response.code == 200**, kar nam bo vrnilo **samo pakete, ki so bili prenešeni na našo napravo** in ne paketov, ki so bili poslani kot zahteva na spletni strežnik.

A screenshot of a computer

Description automatically generated

1. **Kakšne statusne kode in koliko le-teh je vrnil spletni strežnik?**

Spletni strežnik je **vrnil le statusno kodo 200 OK, saj so se vsi zahtevani paketi prenesli uspešno.** Če bi prišlo do napake bi dobili še kakšno drugo statusno kodo. Teh statusnih kod je bilo v našem primeru **toliko kot je bilo odgovorov na zahtevo torej 363**. Te statusne kode pa lahko razberemo iz stolpca Info, kot je razvidno na sledeči sliki.

A screenshot of a computer

Description automatically generated

1. **Tvorite graf poteka prometa *(flow graph)* za protokol HTTP in pokomentirajte stanje.**

Kot je razvidno iz grafa prometa je promet **potekal samo med dvema IP naslovoma** saj se med zajemom prometa ni izvajal drug HTTP promet. Ta dva naslova sta **192.168.0.32 ter 45.33.7.16.** Sam **promet se je začel z prvo HTTP zahtevo, ki je od strežnika zahtevala html datoteko**, katero je po **11.84 sekundah pridobila** ter **uporabila za izvedbo ostalega prometa**, ki temelji na vseh povezavah prisotnih v tistem html dokumentu. Prav tako lahko opazimo da se je **PORT oz. vrata spreminjal le z naše strani, medtem ko je ta ostal na portu 80 na strežniški strani.** To je zaradi tega ker smo stran obiskali **preko http protokola, ki pa za delovanje uporablja port 80**.

**A screenshot of a computer

Description automatically generated**

**RAČUNANJE**

A piece of paper with writing on it

Description automatically generated