Linnéuniversitetet
Kalmar Växjö

Prestandautvärdering av firmwares baserade på öppen källkod för routrar/brandväggar på MIPS-arkitektur

Jämförelse mellan Open-WRT, DD-WRT och Tomato firmware

Författare: Anton Alm & Joakim Björling
Handledare: Jacob Lindehoff
Examinator: Marcus Wilhelmsson
Termin: VT14
Nivå: G1E
Kurskod: 1DV41E

Abstrakt

Den här undersökningen jämför prestanda hos tre olika firmwares som är baserade på öppen källkod. DD-WRT, Open-WRT samt Tomato Firmware för MIPS-arkitektur. Testerna följer två RFC som beskriver hur en prestandaanalys av ett nätverk ska genomföras.

De sammanfattade resultaten pekar på en vinnare som presterat generellt bättre genom alla tester och det var Tomato firmware. Dessa resultat är hämtade från tre olika tester: genomströmningstest, svarstidstest och test med samtidiga sessioner.

Undersökningen visar också att prestandan rent generellt är väldigt jämlik över alla firmwares i de olika testerna. En viktig aspekt är att det finns ingen överlägsen vinnare, vilket beror på, till exempel, hur konsekventa resultaten varit. Detta hänger även ihop med en möjlig slutsats där firmwaresen presterar olika bra beroende på vilken typ av uppgift det gäller.

Som fortsatt arbete rekommenderas prestanda och funktionsanalys av liknande verktyg som varje firmware innehåller. Även en undersökning gällande gränssnittet för varje firmware skulle vara intressant.

Nyckelord: Prestandautvärdering, MIPS, Öppen källkod, DD-WRT, Open-WRT, Tomato-firmware, Router

Abstract

This investigation compares the performance of three different open-source firmwares. DD-WRT, Open-WRT and Tomato Firmware with MIPS architecture. The test follows two RFC that describes the process of how to perform a performance analysis of network interconnected devices.

The summarized results show a winner which has generally performed better throughout all the tests and this was Tomato firmware. These results are gathered from three different tests, which is throughput, latency and concurrent sessions test.

The survey also shows that the performance in general is very equal across all firmwares in the various tests. An important aspect is that there are no outstanding winner, which depends on for example how consistent the results have been. This also concerns a possible conclusion where the firmwares perform various well depending on the type of task involved.

As further work on this investigation we recommend a performance and function analysis of the tools that the firmware contains. Although a survey of the interface for each firmware would be interesting.

Keywords: Performance evaluation, MIPS, Open-Source, DD-WRT, Open-WRT, Tomato firmware, Router

Innehåll

1 Introduktion

Detta kapitel kommer att behandla bakgrunden till problemet och vad som, med hjälp av undersökningen, kommer att lösas. Vidare kommer även syftet med uppsatsen samt problemformulering att diskuteras. Tidigare forskning kring området kommer även tas upp.

1.1 Inledning

När man köper en router/brandvägg för vanliga konsumenter får man med ett redan inlagt firmware från tillverkaren. I många fall har denna typ av firmware egna funktioner utvecklade av företaget i fråga. Detta kan vara begränsande om man använder sig av flera olika märken. Möjligheten finns då att välja en firmware baserad på öppen källkod som är ett gratisalternativ och ger användaren full kontroll över sin enhet.
Denna uppsats behandlar prestandajämförelser mellan tre olika alternativ av firmware för MIPS-arkitektur baserade på öppen källkod. Dessa tre är Open-WRT, DD-WRT, Tomato Firmware.[1]

Större krav ställs på IT-infrastrukturen i hemmet, det ska vara tillgängligt, snabbt och enkelt. Allt fler saker i hemmet börjar nyttja trådlös nätverksuppkoppling, det kommer då resultera i fler enheter på nätverket som har åtkomst till Internet. Detta ökar attackytan på ditt interna nätverk och nätverkssäkerhet blir en viktig aspekt. Routern kommer spela en större roll än vad den har gjort innan.[2]

Tillverkare av routrar gör sitt yttersta för att ge användarna en enkel administration och tillgänglighet av sina produkter, detta kan göra att säkerheten blir bristfällig och att tillverkarna lyckats skapa säkerhetshål.[3]
Ett exempel på detta påträffas i en BBC-artikel där Linksys routrar blivit offer för ett självreplikerande virus eller mask som kallas “The moon”, denna mask tar kontroll över routern och börjar scanna efter andra sårbara system som den kan infektera. Över 23 olika modeller av Linksys routrar beräknas vara sårbara för detta virus. Det som tillät masken att ta sig in och fortsätta sin scanning var en fjärrstyrd hanteringstjänst. En annan attack som nämns i samma artikel är mot Asus routrar, denna attack gjordes av välvilliga hackare som ville påvisa ett säkerhetshål i 10 olika modeller. Detta säkerhetshål upptäcktes genom en tjänst som tillåter användare på nätverket att komma åt hårddiskar på deras lokala datorer genom WiFi. Hackarna lyckades då få åtkomst till dessa hårddiskar externt och lämnade en textfil med instruktioner för att säkra upp routern. Dessa exempel påvisar att genom att göra saker mer lättillgängligt och enkelt att administrera så kan det påverka säkerheten för nätverket.[4]

En annan nackdel med tillverkarnas produkter med låst firmware är att när man ska bygga ut sitt nätverk med enheter och tjänster så kräver det ofta att man bygger upp detta ’ekosystem’ med hjälp av produkter av samma märke. Skulle man välja att blanda märken kan vissa funktioner negligeras samt kan de uppstå kompatibilitetsproblem.[5][6]

Det är inte bara hemmanätverk som kan dra nytta av firmwares baserad på öppen källkod utan även mindre företag. Många mindre företag ligger i gråzonen när det kommer till att investera i nätverksutrustning, det finns dyra enterprise-lösningar och sedan finns det vanliga routrar för hemanvändare.

Funktioner som finns för att underlätta för människor med lägre kompetens inom IT kan agera hinder och utgöra säkerhetshot för en IT-administratör på ett företag. Här är några exempel på typiska funktioner i en konsumentrouter: QoS, föräldrakontroll, gästnätverk, inbyggd mediaserver och lättviktig VPN-support.[5]
Ett exempel på en vanligt förekommande funktion i hemmaroutrar är "UPnP", denna funktion har massor av användningsområden när det kommer till att koppla ihop nätverk för mindre kompetenta personer. Den underlättar konfigurationen genom att göra de inställningarna som krävs automatiskt för att en ny enhet ska bli en del av nätverket. Detta kan då medföra att vissa inställningar som enheten gjort kan utgöra en säkerhetsrisk på ett företag där man inte kan lita på alla människor som är kopplade till det lokala nätverket.[7]

Med hjälp av firmware baserad på öppen källkod kan man fylla detta gap mellan dyr utrustning och konsumentprodukter och ge företag ytterligare ett alternativ som är prisvärt men erbjuder fler alternativ än en standardrouter och dess firmware. Dessa firmwares är mer inriktade mot personer med högre kompetens inom IT-området och ger därför användaren fler alternativ och har tagit säkerheten i aspekt och byggt lösningar för att täppa igen diverse säkerhetshål.[9][32]
Det som framgår från denna rapport kommer vara en sammanställning av tre stycken firmwares baserade på öppen källkod, funktioner samt prestanda kommer att jämnföras för att hjälpa intressenter att hitta vad de söker.

1.2 Tidigare forskning

Tidigare publicerad forskning inom området är väldigt begränsat. Forskning direkt kopplat till ämnet har i skrivande stund ej hittats.

I en liknande publicering vid namn *Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions* jämförs prestanda mellan iptables och Cisco ASA. Skillnaden på det som behandlas i den här undersökningen är att både tester och syfte avser endast två olika typer av brandväggar varav Cisco ej stödjer öppen källkod. [8]

1.3 Problemformulering och syfte

Denna uppsats avser att undersöka firmwares baserade på öppen källkod och dess prestandaförmågor. Arbetet kommer att fokusera på vilken firmware som ger bäst prestanda när det gäller maximal genomströmning av datatrafik, lägst svarstid samt max antal samtidiga sessioner. Genom att analysera resultaten kommer denna uppsats att kunna svara på eventuella frågor gällande prestanda för de olika alternativen.

Ur ett praktiskt perspektiv innebär det att den frågeställning som besvaras i uppsatsen går att, vid val av firmware, motiveras med hjälp av den data som presenteras i uppsatsen. Genom att granska resultatet kommer val av firmware med prestanda som kriterier underlättas väsentligt.

Utbudet på tidigare prestandaanalyser samt allmänna praktiska studier för detta ämne är bristande. Det är svårt att hitta något praktiskt konkret i jämförelser mellan de olika öppen källkod alternativen utan det jämförs för det mesta endast informativt mellan två alternativ. Det finns också en brist på vetenskapliga artiklar inom området och de flesta jämförelser man hittar ligger på Internetforum. Det gör att man ifrågasätter tillförlitligheten samt att materialet är svårare att hitta för en intressent.

2 Teknisk bakgrund

Detta kapitel kommer att förklara de tekniska delar som behandlas i arbetet. Detta för att visa hur undersökningen har genomförts samt vilka verktyg som används. Det som kommer bland annat att förklaras är vad MIPS och firmware är.

2.1 Processorarkitektur

Processorarkitektur är den benämning som används för att förklara hur en processor bearbetar data. Varje arkitektur har sin egna uppsättning med instruktioner. Exempel på arkitekturer är x86, ARM, MIPS, PowerPC, Itanium. Arkitekturen beskriver själva grunden hur en processor beräknar och hanterar data.[28]

2.1.1 MIPS

MIPS (från början en akronym av Microprocessor without Interlocked Pipeline Stages) är en mikroprocessorarkitektur som använder en RISC (Reduced Instruction Set Computer)-baserad instruktionsarkitektur. MIPS-arkiteturen har utvecklats och framställts av MIPS Computer Systems (nuvarande MIPS Technologies). Den första hårdvaran som företaget producerade släpptes Januari 1986 och var en mikroprocessor vid namn R2000. [10]
Denna microprocessor var den första tillgängliga RISC-processorn för företag att köpa och använda sig av i sina system. Dåtidens system byggde på 32-bit medans de nyare anpassats och kör 64-bit.

MIPS används främst i inbäddande system som t.ex. Windows CE-system, routers samt spelkonsoler. Innan 2006 användes de även i ett flertal system från SGI (Silicon Graphics, Inc). MIPS implementationer användes även av företag som Digital Equipment Corporation, NEC, Pyramid Technology, Siemens Nixdorf, Tandem Computers m.fl. i mitten till senare 1990-tal beräknade man att en av tre mikroprocessorer som tillverkades var MIPS-implementationer.[11]

2.2 Firmware

Firmware är en benämning på ett program som innehåller programkod för att styra fysiska komponenter. Firmware är vanligt förekommande i inbyggda system som t.ex. trafikljus och digitalklockor. Firmware lagras vanligtvis på minnen som ej är beroende av ström för att upprätthålla lagring, t.ex. ROM-minnen. Med hjälp av att kunna uppdatera firmware-versionen genom att flasha hårdvaran så kan man förbättra prestanda eller lägga till fler funktioner. Firmware används oftast för sköta de grundläggande operationerna. Utan firmware skulle inte enheter fungera då kommunikation mellan mjukvara och hårdvara skulle vara icke existerande.[12]

2.2.1 DD-WRT

DD-WRT är en Linuxbaserad firmware för flera olika typer av trådlösa routrar och inbäddade system som är ett alternativ baserat på öppen källkod. DD-WRT skapades av Sebastian Gottschall och första versionen kom ut 2005 och baserades på en firmware vid namn Sveasoft Alchemy. Version 23 av DD-WRT var den första som baserades på Open-WRT-kärnan.[14]

2.2.2 Tomato Firmware

Tomato är en liten och enkel ersättningsfirmware för routrar med Broadcom-chipset. Det man får är ett nytt och lättbearbetat GUI (Graphical User Interface), en ny

monitorfunktion där man kan kolla bandbreddsanvändningen, mer avancerade funktioner för QoS (Quality of Service), åtkomstrestriktioner, nya trådlösa funktioner som WDS (Wireless Distribution System),“Wireless client modes”, höjer gränsen för maximala anslutningar för P2P (Peer to Peer), tillåter användare att köra skräddarsydda skripts eller använda Telnet/SSH för fjärråtkomst till en resurs där man kan till exempel omprogrammera SES/AOSS knappen, lägger till “Wireless site survey” där man kan se WiFi-grannar, samt fler funktioner.[15]

2.2.3 OpenWRT

Open-WRT är en firmware som bygger på Linuxkärnan och används främst i routrar och inbäddade system. Open-WRT är en firmware baserad på öppen källkod vilket betyder att den är gratis och källkoden finns att tillgå. Genom detta har många andra utvecklare valt att basera sina firmwares på Open-WRT. Ett exempel på detta är DD-WRT. Open-WRT använder sig av opkg vilket är en pakethanterare. I dagsläget finns mer än 2000 paket tillgängliga.[16]

2.3 Open Source

Termen “Open source” refererar till något som kan modifieras då dess uppbyggnad och design är publikt tillgänglig. Ordet kommer ursprungligen från mjukvaruutveckling för datorer men har anammats för flera olika projekt och produkter och har mer eller mindre blivit en livsstil eller policy för företag världen över.[17]

Specifikt för programvara baserad på öppen källkod gentemot “stängd” programvara är att regler kring äganderätt och modifiering av programkoden tillåter mer frihet. Det innebär att vem som helst får modifiera den och publicera som sin egen. Innan du installerar en sådan programvara så måste man acceptera ett licensavtal, precis som man gör med stängd programvara. Det finns dock olika typer av licensering för öppen källkod, vissa säger att du inte själv får ta betalt för en egen version andra tillåter kanske detta. De flesta licenser vill dock att om du modifierar programkoden så har du en skyldighet att dela den nya koden med ursprunglig författare. Det är detta som är fördelen med öppen källkod, man kan räkna med kontinuerlig uppdatering av programvaran då de får in idéer och modifikationer från olika parter som sedan kan tillämpas på originalet. Eftersom flera parter har tillgång till programkoden är chansen större att man hittar eventuella säkerhetshål, detta är också en av anledningarna till varför vissa föredrar licensering av öppen källkod.[17]

2.3.1 Stängd programvara

Med stängd programvara får man acceptera ett licensavtal som förbjuder användaren att göra några som helst modifikationer med programkoden. Denna programkod är endast avsedd för utvecklarna eller företaget, exempel på programvaror under denna licens är Microsoft Word eller Adobe Photoshop. Nackdelar med denna är support och uppdatering inte sker lika frekvent som ett program under till exempel en GNU-licens. En fördel är att uppdateringarna oftast är väl testade och erhåller hög kvalité, detta gör även licenser på öppen källkod men det är ändå svårare att garantera det.[17]

2.4 Router/Brandvägg

En router används för att knyta samman flera stycken nätverk med varandra. Det innebär att den har portar eller “interfaces” som tillhör alla de olika nätverken som är kopplade mot den. När routern får in ett IP-paket från ett nätverk så bryts paketet ner för att undersökas och ta reda på vilken väg den ska gå, se figur 2.1. Destinationen för

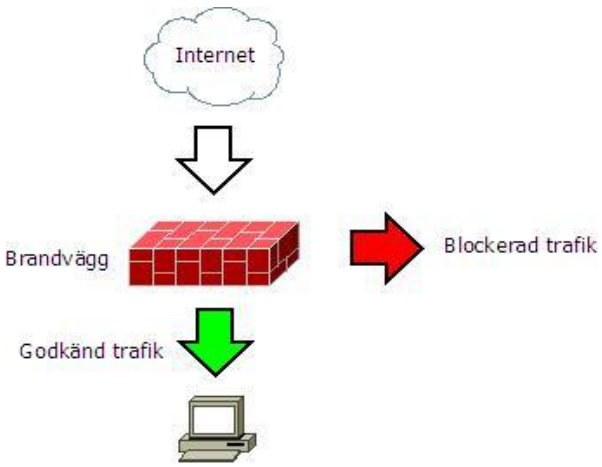
paketet behöver inte vara lokalt på routern utan det kan endast behöva färdas igenom routern. Detta sköter routern med en routingtabell där den har samlat information angående externa nätverk, detta kan göras manuellt eller dynamiskt med hjälp av routingprotokoll.[29]

På detta sätt kopplas miljontals routrar ihop med varandra och skapar "Internet". En router har oftast två olika sorters interface, ett som använts för det lokala nätverket (LAN) och ett som går mot "Internet" (WAN). Detta för att man vill segmentera det interna nätverket från det externa för inte bli utsatt för angrepp från Internet.[30]

Eftersom Internet är såpass stort som det är idag måste man vara förberedd på de olika hot utomstående nätverk och datorer kan skapa. Man har därför utvecklat brandväggar som ett skydd för det interna nätet från hot som kommer från Internet. Den fungerar genom att den applicera ett filter för ingående och utgående trafik på alla interface (portar) där man själv får sätta vilka regler som gäller för olika anslutningar. Eftersom man kan applicera regler på utgående trafik kan man även använda brandväggen som en sorts censur på nätverket, vilket kan komma att spela en roll i säkerhetsaspekten.[31]

Det finns olika typer av brandväggar baserat på hur djupgående de är. Brandväggar som arbetar på lager tre och fyra i OSI-modellen avgör vilken trafik som får passera i genom baserat på källan av adressen, port och protokoll samt destination av paket, port och protokoll. Detta medför ingen säkerhet för att kunna spåra paket och knyta dem till en specifik användare. Detta ökar möjligheten till attacker som spoofing.[18]
I figur 2.1 förklaras funktionen hos en brandvägg.

Brandväggar som arbetar på det sjunde lagret i OSI-modellen kallas för applikationsbrandväggar. Detta betyder att brandväggen kan filtrera trafik för en specifik applikation. En applikationsbrandvägg kommer att öppna alla paket matcha dem mot de regler som är konfigurerade, tillåts ett paket så kommer det att återskapas på nytt och skickas vidare. [19]



Figur 2.1: Förklaring av funktion hos brandvägg

2.5 Linksys WRT54GL

Brandväggen som valdes för prestandatesterna var Linksys WRT54GL. Enheten har följande prestanda:
CPU: Broadcom BCM5352, 200 MHz
RAM: 16 MB
Flashminne: 4 MB
Teknologi: Wireless G
Band: 2.4 GHz
Ethernetportar (Mbit/s): 4x 10/100
[20][21]

2.6 Verktyg

Delen verktyg beskriver de hjälpmedel som används för att kunna utföra arbetet. Verktygen kan delas upp i två olika grupper. En för att generera den test-trafik som används samt en för övervakning och utvärdering av trafik.

2.6.1 Web Bench

Web Bench är ett verktyg för att testa prestanda på webbservrar eller proxyservrar. Verktyget simulerar flertal klienter som använder sig av HTTP-förfrågningar mot den server man vill testa. Detta test är inte riktigt realistiskt utan pressar servern med många anrop samtidigt för att se vad den klarar av.[22]

2.6.2 iperf

Iperf är ett verktyg för att mäta maximal TCP-bandbredd och även UDP-strömmar som man kan konfigurera manuellt. Programvaran består av en klient och en server där servern ger resultat av testet som initieras av klienten. Servern kan rapportera bandbredd, fördröjning, asynkrona strömmar och antal förlorade datagrams. Klienten kan använda sig av diverse parametrar för att reglera trafikflödet och kunna påverka resultatet.[13]

2.6.3 Apache HTTP Server

Apache är en webbserver för HTTP/1.1 baserad på öppen källkod. Den är snabb och enkel med verktyg för att installera eller programmera egna moduler. Apache är den populäraste webbservern och kördes på 54,2% av alla aktiva webbsidor enligt en undersökning gjord juni 2013.[24]

Apache kan köras på dom flesta moderna operativsystem samt äldre. Windows, OSX, Linux och Unix har alla stöd för Apache.[24]

2.6.4 Ubuntu ping

ICMP (Internet Control Message Protocol) är ett IP-protokoll som används i kontrollsammanhang. ICMP fungerar genom att en förfrågan görs mot en annan enhet som kan ta emot IP-trafik, denna enhet svarar sedan på förfrågan (Reply). När den enhet som skapade förfrågan får ett svar räknas svarstiden ut och man vet nu att enheten fungerar korrekt över ett IP-nätverk. ICMP kan också använda flera olika typer av data och information när man använder protokollet, dessa är: ”Echo Reply”, ”Destination Unreachable”, ”Source Quench”, ”Redirect”, ”Echo”, ”Time Exceeded”, ”Parameter Problem”, ”Timestamp”, ”Timestamp Reply”, ”Information Request” och ”Information Reply”.[32]

2.7 Maximal genomströmning

När man pratar om maximal genomströmning inom nätverk och brandväggar syftar det på den mängd data som en enhet kan processera utan att börja tappa frames.
Den data som skickas över nätverk som t.ex. Internet är uppbyggd av frames och dessa innehåller information. När en frame kommer in till en brandvägg så konsumeras resurser av hårdvaran för att bearbeta varje frame. I IETF RFC 1242 förklaras definitionen av "throughput" eller maximal genomströmning som följande: "The maximum rate at which none of the offered frames are dropped by the device"[25]

2.8 Samtidiga sessioner

När en användare ansluter till en resurs, t.ex. en webbserver bakom en brandvägg, skapas en session mellan användaren och resursen som i sin tur brandväggen måste hålla koll på. Detta kräver resurser som t.ex. minne och processorkraft. När antalet sessioner stiger så allokeras mer minne och mer processorkraft krävs för att kunna hålla reda på sessionerna. Detta är en viktig aspekt när man skall utvärdera en brandväggs prestanda.[26]

2.9 Svarstid

Data som skickas över nätverk passerar oftast genom en rad olika nätverksenheter. Detta innebär att datan som skickas måste i sin tur bearbetas av varje enhet för att kunna fatta beslut om vad skall göras med datan. Detta kommer att skapa en fördröjning vid varje enhet som datan passerar.
Den hårdvara och de firmwares som testerna utförs på använder sig av en teknologi kallad store-and-forward vilket innebär att enheten måste först ta emot hela paketet och ladda in det i systemminnet för att sedan kunna skicka vidare det. Ju större paket som kommer in desto längre blir svarstiden.[27][25]

3 Metod

Detta kapitel behandlar arbetets tillvägagångssätt genom att beskriva miljön, ansats, hantering av mätverktyg samt praktiskt genomförande. Kapitlet kommer även behandla de åtgärder som vidtagits för att säkerställa ett tillförlitligt resultat. För att förtydliga den miljö som använts i testerna kommer även topologin illustreras.

3.1 Vetenskaplig ansats

Uppsatsen har genomförts med hjälp av en induktiv metod. Detta innebär att de resultat som har framkommit genom olika tester har studerats och utifrån det så har en slutsats dragits. Undersökningen har även givit ett kvantitativt resultat då de mätningar och tester som gjorts gett olika värden. Dessa värden har därefter analyserats för att sedan presenteras under resultatdelen i uppsatsen. I den här uppsatsen innebär detta att information om svarstid, maximal genomströmning av trafik samt maximalt antal ansluta användare samlas in för att studeras och dra slutsatser.

3.2 Datainsamling

Primär- och sekundärkällor är det två sätt som används för att samla in data, detta enligt Patel och Davidsson. Data som enkäter och direkta tester är primärkälla och data som samlats in av andra personer är sekundärdata. Man kan spara tid genom att använda sig av sekundärdata då det är andra personer som samlat in datan. [37]

Vi har baserat vårt val av datainsamlingstekniker genom dokumentstudier där vi har jämfört verktyget mot testernas ändamål och kommit fram till om de är tillräckliga. Denna metod visade sig vara den mest effektiv då vi baserade våra val på Internetartiklar och rekommendationer. Valen av verktyg och metoder har också influerats av en liknande prestanda analys som fick tillfredställande resultat.

Några av de andra vanligaste datainsamlingsteknikerna kontrollerades och valdes sen bort. Enkätundersökningar valdes bort då tid inte fanns och att vi ansåg att denna metod inte kommer att ge oss tillräckligt med information och att det skulle vara svårt att hitta intressenter för enkäten. Resurser för att föra intervjuer för att få information fanns inte. Observation genom egna tester av teknikerna kändes inte nödvändiga då tillräckligt mycket dokumentation gick att hitta för att helt basera våra beslut på dokumentstudier. Rapportens tekniker har influerats av en prestanda analys mellan “Iptables” och “Cisco ASA” där man kunde se resultatet samt de genomförda stegen för testerna[33].

3.2.1 Motivering av verktyg

Web Bench är med som ett av verktygen i rapporten då det är välkänt och finns gott om dokumentation. Det är ett av dem mest välkända verktygen inom dess område och uppfyller ändamålen för denna rapport. Användandet av verktyget för rapportens prestandatester är även influerat av en liknande prestandaanalys.[33]

Iperf valdes som verktyg då det är ett känt verktyg för att mäta bandbredd. Det betyder att det är väl testat och har bra support på diverse forum. Verktyget har levererat tillfredställande resultat för flera examensuppsatser och det hade allt som behövdes för prestandatesterna i denna rapport.[34][35]

Ping valdes då problem uppstod med andra planerade verktyg. Överlag uppfyller Ubuntus ping-verktyg allt som testet behövde och fungerade tillfredställande. Detta verktyg är också ett säkert val då det är väl testat och ger stabila resultat.[32]

Linksys WRT54GL är routern som valdes för rapportens prestandatester. Just denna modell valdes då den är en av de vanligaste och kändaste samt mest prisvärda MIPS-router som stödjer firmwares baserade på öppen källkod. Den valdes även för att det fanns begränsningar i resurserna som fanns att tillgå.[38]

3.2.2 Urval

Testerna som utförts i undersökningarna är maximal genomströmning, svarstid samt samtidiga sessioner. Dessa undersökningar bygger på de motiveringar och rekommendationer som finns i RFC 1242. Eftersom undersökningarna är specifika behövs ej urval göras på resultatet. [25]

3.3 Genomförande

Denna rubrik kommer beröra själva genomförandet av prestandatesterna i rapporten. Här kommer inte slutgiltiga resultat att presenteras.

3.3.1 Installation av firmware

Installation och byte av firmware är en stor del av den praktiska biten i rapporten, därför valdes denna enkla guide som en kort förklaring.

Innan tester påbörjas måste firmware installeras, denna rapport behandlar endast processen för Linksys WRT54GL då det är olika för varje router. Den behandlar även endast installationen av en av de tre olika firmware som ska köras i tester, notera att man bör kolla upp modellen på routern då vissa firmwares har olika versioner beroende på modell.

För att installera till exempel DD-WRT börjar man med att hitta rätt firmware version på utvecklarnas hemsida.

Navigera sedan till routerns webbgränssnitt, som ligger på IP adressen 192.168.1.1 som standard för Linksys WRT54GL. En inloggning kommer sedan att krävas, som standard är användarnamnet satt till “root” och lösenordet till “admin”. Väl inne i webbgränssnittet navigera till “Administration” där väljer man “Firmware Upgrade”. Lokalisera sedan den “.bin” som är den nya firmware-filen, genom Browse-knappen. När rätt fil valts trycker man på Upgrade-knappen för att påbörja uppgraderingen.

3.3.2 Genomströmningstest

Genomströmningstestet består av SERVER1 som med verktyget Iperf genererar trafik mot SERVER2. SERVER1 som har iperf installerat som tjänst är inkopplad på LAN-sidan av routern. SERVER2 som har iperf installerat är inkopplad på WAN-sidan av routern.

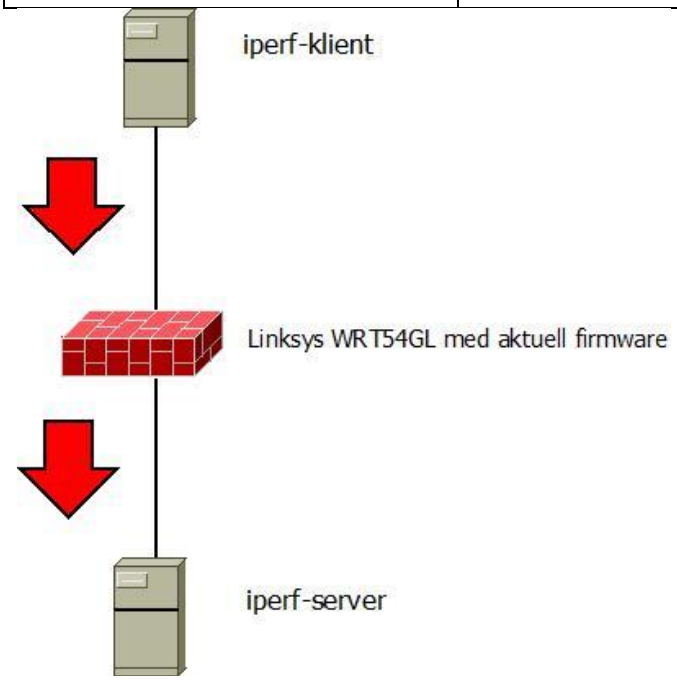
Testet för genomströmning utfördes genom att fem stycken tester genomfördes för varje firmware. Varje test bestod av att under en period på 10 sekunder skickade iperf-klienten största möjliga mängd data till iperf-servern. Mellan varje test var det ett uppehåll på en minut för att försäkra sig om att enheten har bearbetat alla paket. Alla tester använde sig av protokollet TCP, där ett standardvärde på fönsterstorleken var 85 KB. När de fem testerna utförts så registrerades det resultat med högst genomströmning och fördes in i statistiken. I figur 3.1 kan topologin för testet ses.

Följande kommando användes på SERVER 1 som agerade klient:
iperf -c 192.168.2.101 -t 10
Detta kommando skickar så mycket data den kan under 10 sekunder till SERVER 2. Eftersom det inte finns någon parameter i detta exempel som talar om hur många bytes som ska skickas så kommer den skicka som mycket som möjligt under 10 sekunder. Detta innebär att man får ut maximal genomströmning och kan sedan analysera resultatet för samtliga firmwares. I tabell 3.1 kan IP-adressering ses.

Följande kommando användes på SERVER 2 som agerade server:
iperf -s
Detta kommando försätter SERVER 2 i serverläge för iperf. Detta tillåter klienten att få korrekta svar för att sedan presentera resultaten för användaren. Resultaten av varje test kan även ses på server sidan.

Tabell 3.1: IP-adressering vid test av genomströmning

Enhet	IP-adress	Nätmask	Interface
Linksys WRT54GL	192.168.2.1	24	WAN
Linksys WRT54GL	192.168.1.1	24	LAN
SERVER 1	192.168.1.101	24	eth0
SERVER 2	192.168.2.101	24	eth0



Figur 3.1: Topologi av genomströmningstest

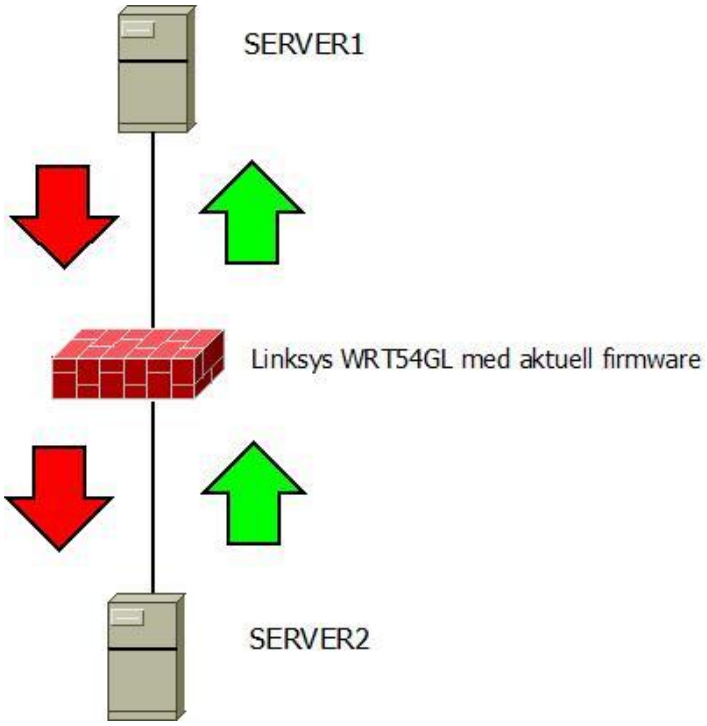
3.3.3 Svarstidstest
Testet för svarstid utfördes genom att SERVER1 initierar ett flertal olika pingmeddelanden till SERVER2. Dessa pingmeddelanden är alla på olika storlekar för att kunna urskilja om någon hantering av datamängd varierar beroende på firmware. Varje test med specifik mängd data pågick i en minut med en hastighet av ett paket per sekund. Efter en minut körs nästa test och mängden data höjs. Denna process genomförs

fyra gånger för varje ökning av datastorleken, medelvärdet för varje test slåss ihop och räknas ut till ett nytt medelvärde. Det är detta värde som presenteras i resultatet. Topologin för testet kan ses i figur 3.2.

Följande kommando kördes på SERVER 1:
ping 192.168.2.101 -s 22 -c 60

Detta kommando kommer skicka ett ICMP-paket på totalt 64 byte med Ethernet II-ram varje sekund tills 60 paket levererats. Första parametern bestämmer hur många byte data som ska skickas, efter att den lagts in i Ethernet-II ram kommer den nå 64 bytes. Denna parameter ändras när paketstorleken ska höjas.

ICMP använder sig av en IP-header på 20 bytes samt en ”ICMP echo request header” på 8 bytes, detta innebär att den totala ICMP-ramen kommer vara 28 bytes + datan man väljer att skicka i varje paket. Detta paket kommer sedan i sin tur att läggas in i en Ethernet II-ram som kommer öka den totala storleken på paketen till 42 bytes utan FCS (Frame Check Sequence). Detta betyder att när parametern ska ändras måste man räkna bort dessa 42 bytes för att de sedan kommer läggas på automatiskt.[36]
Den andra parametern bestämmer hur många paket som ska skickas, den är satt till 60 för alla test. Som standard skickas ett paket i sekunden vilket innebär att varje test håller på i en minut.



Figur 3.2 Topologi för svarstid

3.3.4 Test för samtidiga sessioner

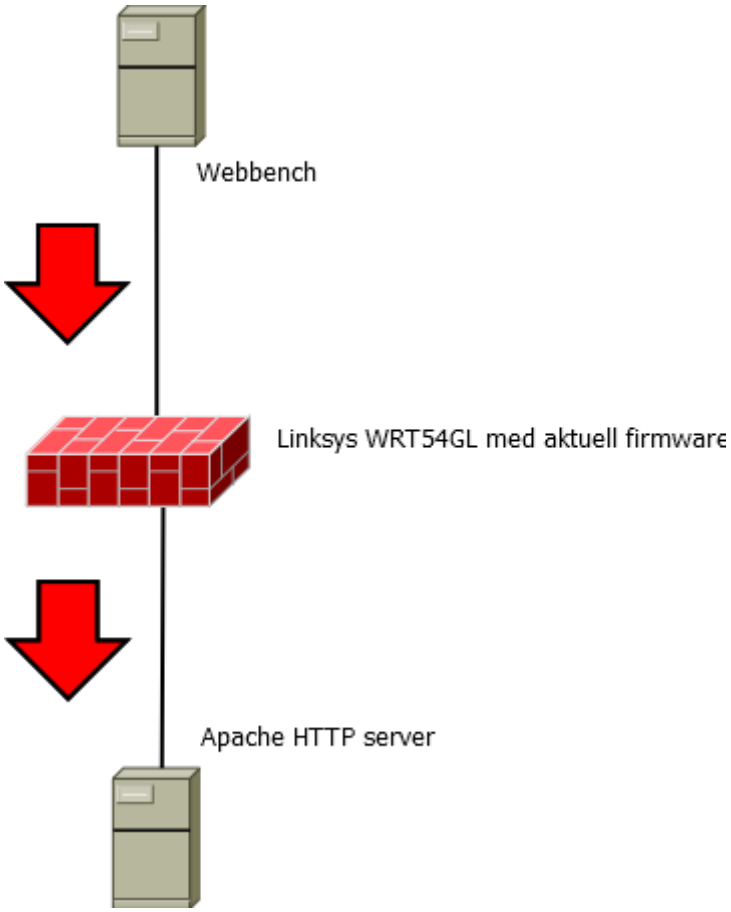
Innan prestandajämförelsen mellan de olika firmwares rapporten behandlar måste man sätta upp ett basundersökningstest. Detta test utförs för att undersöka gränser för att vad hårdvara och mjukvara kan prestera vid optimala förhållanden, man använder detta test för att ha något konkret att jämföra med vid testerna.
För detta scenario gjordes ett test där SERVER1 kör verktyget Web Bench som genererar HTTP-förfrågningar till en Apache HTTP-server som är konfigurerad på SERVER2. Servrarna är direktanslutna för att undvika flaskhalsar, detta test kommer att bestämma gränsen för hårdvaran i servrarna maximalt klarar. I figur 3.3 kan topologin för testet ses.

Det kommando som kördes på Web Bench ser ut som följande:
webbench -c 20000 -t 30 http://192.168.2.101/
Parametern "c" bestämmer hur många klientförfrågningar den ska generera, parametern "t" bestämmer under vilket tidsintervall testet ska köras i sekunder. Med detta test fastställdes det att utan inblandning av routern klarar SERVER 2 att ta emot 20000 HTTP-anslutningar med få fel. I tabell 3.2 kan IP-adresseringen ses.

Resultatet som presenteras kommer vara i form av hur många misslyckade förfrågningar som skedde under varje test. Fyra test per nivå har valts för att utesluta att slumpmässiga resultat uppstår samt för att kunna summera resultaten på ett bra sätt. Efter att fyra test har avslutats för varje nivå kommer ett medelvärde presenteras för att underlätta jämförelser. En omstart av routern sker mellan varje test för att utesluta att förfrågningar ligger kvar och bearbetas av routern.

Tabell 3.2: IP-adressering vid test av samtidiga sessioner.

Enhet	Ip-adress	Nätmask	Interface
Linksys WRT54GL	192.168.2.1	24	WAN
Linksys WRT54GL	192.168.1.1	24	LAN
SERVER 1	192.168.1.101	24	eth0
SERVER 2	192.168.2.101	24	eth0



Figur 3.3: Topologi för test för max antal samtidiga sessioner.

3.4 Analys

De resultat som har framkommit baseras på de tester som gjorts under genomförandet. Den data som samlats in utgör den grund som arbetet bygger på. Resultaten analyserades och jämfördes för att kunna komma fram till vilken firmware som har presterat bäst i de olika testerna som utförts. Alla resultat fördes sedan in i diagram och tabeller för att ge en grafisk bild över resultaten och därmed underlätta urskiljning.

3.5 Tillförlitlighet

För att kunna säkerställa att resultaten är tillförlitliga har undersökningar och åtgärder gjorts på de faktorer som skulle kunna påverka resultaten. Följande faktorer har behandlats under de tester som utförts.

- Alla maskiner är fysiska för att eliminera eventuell extra last vid virtualisering.
- Basundersökningar har gjorts i alla scenarion utan brandvägg för att eliminera eventuella prestandaförluster orsakade av maskinerna.
- Alla enheter kommer att använda sig av samma hårdvara under alla tester.
- Testerna görs flertalet gånger för att säkerställa att resultat ej uppstår slumpmässigt.
- All kablage är av samma längd och typ för att säkerställa att detta ej påverkar resultat.
- Ingen konfiguration har gjorts på programvarorna innan testerna förutom tilldelning av IP-adresser på nätverksinterfacen.

3.6 Testmiljö

Testmiljön består av tre olika topologier beroende på vilket test som utförs. Antalet enheter är samma i alla topologier.

3.6.1 Hårdvaruspecifikation

I tabell 3.3 kan specifikationerna för de enheter som använts i samtliga tester ses.

Tabell 3.3: Hårdvaruspecifikation för testenheter

Namn	Funktion	Program	OS	Modell	CPU	Minne	Lagring	Nätverk
SERVER 1	Sessions & trafik generator	Webbench & Iperf	Ubuntu 12.04.4 LTS	Dell PowerEdge 2900	Intel Xeon 5000	10 GB	200 GB	100 mbit/s
Router/brandvägg	MIPS Router/brandvägg		OpenWRT, FREE-WRT och Tomato firmware	Linksys WRT54 GL	Broadcom BCM5352 200 MHz	16 MB	4 MB	100 mbit/s
SERVER 2	Monitor för nätverkstrafik & http server	apache HTTP server	Ubuntu 12.04.4 LTS	Dell PowerEdge 2900	Intel Xeon 5000	10 GB	200 GB	100 mbit/s

3.7 Begränsningar

Testmiljön har olika begränsningar beroende på vilket test som utförs. Saker som hårdvara och resurskrävande program kan påverka resultatet vilket gör det mindre trovärdigt. För att undersöka eventuella problem har basundersökningar genomförts för de tester som kräver det.

3.7.1 Begränsningar för test av maximalt antal anslutningar

Programvaran Web Bench klarar att generera upp till 30000 anslutningar, detta har framkommit genom att basundersökningar har gjorts på programmet. Den största begränsningen i det här testet är dock servern som Web Bench körs på. Detta är en Dell PowerEdge 2900 och kan bara generera upp till 20000 sessioner på grund av begränsningar i hårdvaran.

3.7.2 Begränsningar för genomströmningstest

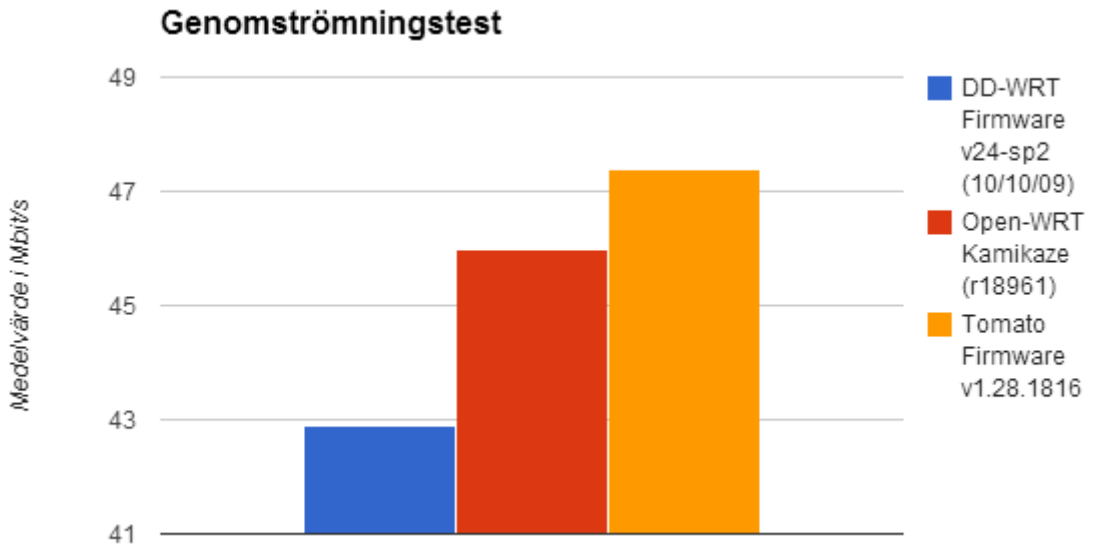
En av begränsningarna i genomströmningstestet är att Linksys WRT54GL är begränsad till 100 Mbit/s bandbredd på alla dess Ethernetportar, detta innebär att vi aldrig får reda på om mjukvaran kan hantera mer än just denna bandbredd. En annan begränsning är att alla portar på routern är bryggade och använder sig av en gemensam MAC-adress vilket gör det svårt att hitta passande program för att generera trafik och omöjligt att köra tester på datalänkskiktet.

4 Resultat/Empiri

Prestandatesterna som gjorts kommer i detta kapitel redovisas och presenteras. Varje test kommer att redovisas med en kort förklaring. Resultaten kommer att presenteras i tabellform samt i grafer.

4.1 Genomströmning

Figur 4.1 beskriver de resultat som framkommit från testerna av maximal genomströmning i form av en graf. Genomströmningens värden mäts i Mbit/s och här är ett högre värde bättre.
Inga paket förlorades under testerna därför presenteras inte mängd data överförd, utan den firmware med högst medelvärde skickade även mest data i MB.



Figur 4.1: Diagram av medelvärde vid genomströmningstest

Exakta värden för staplarna i figur 4.1 är följande:
DD-WRT: 42.1 Mbit/s
Open-WRT: 45.8 Mbit/s
Tomato Firmware: 46.7 Mbit/s

För komplett tabell och individuella testresultat se Bilaga 2.

4.2 Svarstid

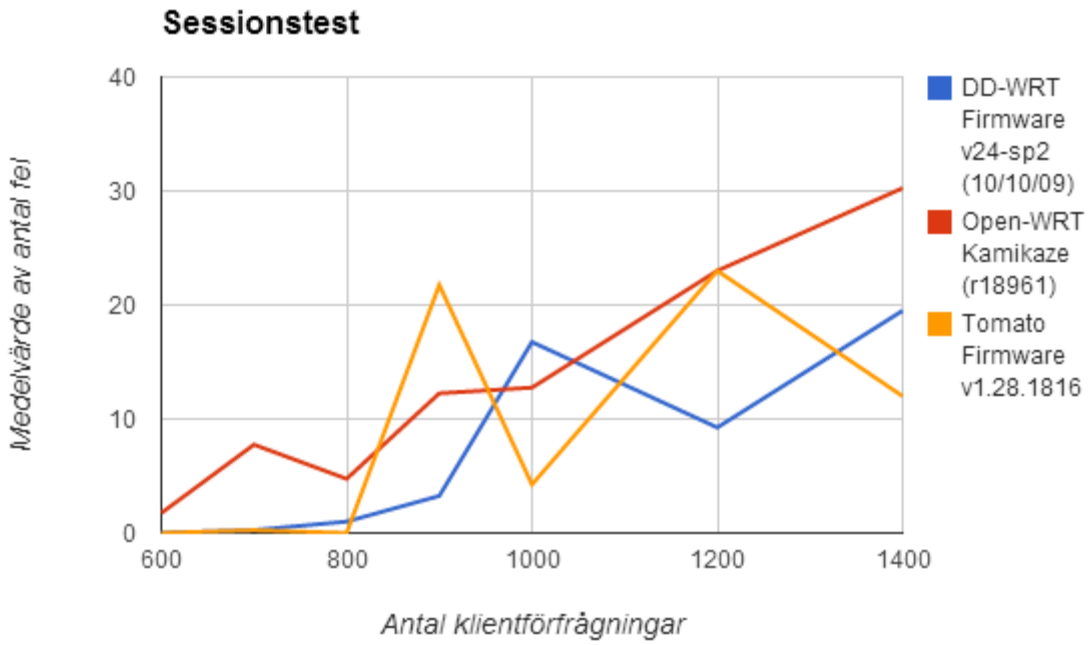
I tabell 4.1 visas resultaten ifrån svarstidstestet. Stapeln längst till vänster representerar de olika paketlängderna som användes i testerna. Resterande staplar representerar de olika firmwaresen och deras resultat. Mätningarna som gjorts presenteras i millisekunder (ms) och är ett medelvärde av de antal tester som utfördes. Det medelvärde som räknas ut av testarna presenteras ihop med den firmware som kördes och ett resultat per paketlängd.
Gällande resultaten är ett lägre värde bättre.

Tabell 4.1: Resultat av svarstidstest.

	Medelvärde av svarstid (ms)		
Paketlängd	Open-WRT	DD-WRT	Tomato Firmware
64	0.767	0.817	0.792
128	0.83	0.877	0.84
256	0.974	1.002	0.923
512	1.162	1.193	1.105
1518	1.897	1.925	1.788

4.3 Samtidiga sessioner

I figur 4.2 presenteras de resultat som framkommit i de olika tester som utförts för att mäta antalet sessioner. Den vänstra vertikala spalten visar medelvärdet av antalet fel som uppstått under testerna. Den högra vertikala axeln visar vilken graf som tillhör en viss firmware genom en viss kulör. Den undre horisontella axeln visar de antalet klientförfrågningar som gjordes.
Ett generellt lägre värde är ett bättre resultat i detta test.



Figur 4.2: Diagram över resultat av sessionstesten

Exakta värden för graferna i figur 4.2 är följande:
Open-WRT vid 600, 800, 1000, 1200 och 1400 förfrågningar: 1.75, 7.75, 4.75, 12.25, 12.75, 23 och 30.25
DD-WRT vid 600, 800, 1000, 1200 och 1400 förfrågningar: 0, 0.25, 1, 3.25, 16.75, 9.25 och 19.5
Tomato Firmware vid 600, 800, 1000, 1200 och 1400 förfrågningar: 0, 0.25, 0, 21.75, 4.25, 23, 12

För individuella resultat i tabellform se Bilaga 1.

5 Analys

I detta kapitel analyseras resultaten som framkommit i kapitel 4. Genomförande bestod av tre olika tester: genomströmning, svarstid och samtidiga sessioner. De tre olika typer av tester presenteras i var sitt eget avsnitt.

5.1 Genomströmning

De slutsatser som kan dras genom att beskåda resultaten i figur 4.1 från genomströmningstestet är flera.
Tomato firmware var den firmware som klarade att leverera högst genomströmning, detta bidrar även till det faktum att Tomato firmware klarar att transportera mest data under en viss tidsperiod.
Generellt sett så höll sig alla firmwares inom samma spann av hastigheter (40 - 60 Mbit/s) vilket var förväntat innan resultaten framkom. Detta på grund av begränsningarna i hårdvaran.

Vidare enligt figur 4.1 kan vi se att den firmware som hade näst högsta genomströmningshastighet var Open-WRT följt av DD-WRT som var den firmware som presterade sämst.

5.2 Svarstid

Resultaten från testerna av svarstid var rent generellt väldigt lika och hade mycket små marginaler. Eftersom resultaten mäts i millisekunder är skillnaden på resultaten ur ett verklighetsperspektiv obefintligt liten.

När det gäller resultatet från testerna av svarstid kan vi genom att beskåda Tabell 4.1 konstatera att Tomato Firmware är den firmware som generellt hade den lägsta svarstiden oavsett paketlängd.

5.3 Samtidiga sessioner

Resultaten från testet av maximalt antal samtidiga sessioner som kan ses i Figur 4.2 skiljer sig generellt mer än resultaten från testen av svarstid.
Vidare enligt figur 4.2 kan vi se att Tomato Firmware hade minst antalet fel vid 800 samt 1400 klientförfrågningar. Dock genom att titta på hela grafen och tidigare resultat kan vi också konstatera att det är den firmware som varit mest inkonsekvent.

DD-WRT är den firmware som totalt sett fick minst antal fel men även denna precis som Tomato är väldigt inkonsekvent. Open-WRT är den firmware som fick totalt sett mest antal fel men var den firmware som höll sig mest konsekvent genom testerna.

6 Diskussion

Det här kapitlet innehåller diskussioner om de resultat som framkommit samt en reflektion om utförandet och eventuella motgångar.

6.1 Problemlösning

Syftet med detta arbete var att få en insyn i firmwares baserade på öppen källkod och dess kapacitet när det gäller prestanda. Eftersom tiden var begränsad valdes endast en prestandaanalys att utföras mellan dessa firmwares. Andra jämförelser och tester som återstår att göra kommer under rubriken "7.2 Förslag till fortsatt forskning" i avslutningskapitlet.

Överlag anses resultaten vara lyckade och att de fyllt i den kunskapslucka som rapporten belyser. Eftersom ingen tidigare forskning skett på just detta område finns det inget att jämföra med. Detta gör denna rapport till en bra grund för eventuella framtida jämförelser. Slutresultatet anser vi kan hjälpa många att dels bli mer intresserade i ämnet samt att insatta personer kan få ut en konkret prestandajämförelse. Introduktionen fokuserar på att lyfta fram fördelar med firmwares baserad på öppen källkod. Detta för att göra ämnet mer intressant för en som är osäker men även göra en redan insatt person mer intresserad av rapporten. Resultaten är väldigt tilltalande och ihop med andra jämförelser i samma ämne så kan det bli bara bli bättre. Därför uppmanas det att göra fler jämförelser i ämnet.

Resultaten som framkom var över förväntan, någon större skillnad hade inte räknats med på testerna då samma hårdvara användes på alla firmwares. Vi ansåg dock att testerna behövdes göras för att bevisa om en skillnad faktiskt fanns. Resultaten som framkom var dock blandade, vissa tester var mer jämna än andra men det viktigaste var resultaten var varierande beroende på firmware.

Ett dilemma som uppstod efter start av tester var val av program för att utföra själva prestandatesterna. Vi hade sen tidigare en uppfattning om vilka program som skulle användas för alla våra tester. Under arbetets gång stöttes dock det på problem med de program som valt och fick leta efter ersättare. Ett problem som uppstod var att Linksys WRT54GL endast har en gemensam MAC-adress vilket betyder att alla dess portar är bryggade, detta orsakade problem med verktyg som hade planerats att användas. Det blev då väldigt tidskrävande och gjorde att planeringen fick ändras om flertalet gånger.

6.2 Metodreflektion

Metoderna som användes bestämdes genom två RFC:er (RFC 1242, RFC 1246) som berör ämnet prestandaanalys. Dessa två RFC:er innehåller båda riktlinjer och termer för utvärdering av brandväggar och nätverkskopplade enheter. Genom att läsa dessa kan man få en uppfattning om vad man skall jämföra. Detta stärker uppsatsens validitet av resultatet då utgivarna bakom metoderna är ”Internet Engineering Task Force”. Verktyg och topologi bestämdes sedan av oss själva för att uppnå önskat resultat.

7 Avslutning

I detta kapitel kommer en slutsats av arbetet presenteras samt ett förslag till fortsatt forskning.

7.1 Slutsats

En direkt frågeställning framkom aldrig från vår introduktion utan syftet var endast att utföra en prestandaanalys mellan tre firmwares, dessa var DD-WRT, Open-WRT och Tomato. Ingen direkt förväntning fanns på resultaten, syftet var mer att ha något att presentera till en intressent av dessa firmwares istället för att bevisa någon förutspådd vinnare. Rapporten lyfter fram resultaten på ett bra sätt och anses vara korrekt genomförd. Vidare anses även att resultaten är presenterade på ett bra och lättförståeligt sätt.

En tydlig vinnare är svårt att utse då det är flera faktorer som spelar in. Detta som till exempel hur konsekventa och hur varierande resultaten har framkommit . Detta hänger även ihop med en möjlig slutsats där firmwaresen presterar olika bra beroende på vilken typ av uppgift det gäller. Dock kan man, baserat på alla resultat, utse en vinnare som har haft generellt bäst resultat genom alla tester. Genom att beskåda resultatsdelen kan man se att den firmware som har generellt presterat bäst är Tomato firmware.

7.2 Förslag till fortsatt forskning

På grund av begränsade resurser finns det mycket som återstår att göra i ämnet. Det som anses vara mest av intresse just nu från vår synvinkel skulle vara en analys av de olika funktioner som dessa firmwares erbjuder. Många av dessa firmwares har olika implementationer av samma tjänster, det skulle vara intressant att utföra en prestandaanalys på dessa tjänster och se vem som står sig bäst.

Även liknande prestandatester med hastigheter på 1 Gbit/s kunde inte göras på grund av begränsad hårdvara. Detta skulle vara en intressant analys för att se vilka hastigheter man skulle kunna komma upp i lokalt med dessa firmwares.

En annan tanke som kom upp under arbetet med rapporten var användargränssnittet som i detta fall var ett webbaserat GUI. Detta kan vara svårt att göra någon direkt analys på eftersom det är en individuell uppfattning om vad som anses fungera bäst. Det borde ändå finnas kriterier och riktlinjer för vad som anses vara ett användarvänligt GUI. Detta skulle man kunna titta djupare på för att sedan kunna presentera en komplett jämförelse mellan dessa firmwares.

Referenser

[1] Eds.b.ebscohost.com, 'Enhance Your Router With Open-Source Firmware: OneSearch', 2014. [Online]. Tillgänglig: http://eds.b.ebscohost.com/eds/detail?sid=13147dc6-09c4-4d4e-b1e4-9de96994f5ad%40sessionmgr113&vid=3&hid=101&bdata=Jmxhbmc9c3Ymc2l0ZT1lZHMtbGl2ZSZzY29wZT1zaXRl#db=buh&AN=82536736. [Kontrollerad: 24- Apr- 2014].

[2] Security.illinois.edu, 'Secure Your Home Wireless Network | CITES Security', 2014. [Online]. Tillgänglig: https://security.illinois.edu/content/secure-your-home-wireless-network. [Kontrollerad: 24- Apr- 2014].

[3] K. Fogarty, 'Home Routers Pose Biggest Consumer Cyberthreat - Dice News', *Dice News*, 2014. [Online]. Tillgänglig: http://news.dice.com/2014/02/18/home-routers-pose-biggest-consumer-cyberthreat/. [Kontrollerad: 24- Apr- 2014].

[4] BBC News, 'Home routers hit by security bugs', 2014. [Online]. Tillgänglig: http://www.bbc.com/news/technology-26287517. [Kontrollerad: 24- Apr- 2014].

[5] M. Brown, 'What Separates Business Routers From Consumer Routers? | PCWorld', *PCWorld*, 2014. [Online]. Tillgänglig: http://www.pcworld.com/article/256683/what_separates_business_routers_from_consumer_routers_.html. [Kontrollerad: 24- Apr- 2014].

[6] C. Palazzi, M. Brunati and M. Roccetti, 'An OpenWRT solution for future wireless homes', *Multimedia and Expo (ICME), 2010 IEEE International Conference on*, pp. 1701-1706, 2010.

[7] S. Esnaashari, I. Welch and P. Komisarczuk, 'Determining Home Users' Vulnerability to Universal Plug and Play (UPnP) Attacks', *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on*, pp. 725-729, 2013.

[8] J. Xu and W. Su, 'Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions', *Hh.diva-portal.org*, 2013. [Online]. Tillgänglig: http://hh.diva-portal.org/smash/record.jsf?pid=diva2:622522. [Kontrollerad: 24- Apr- 2014].

[9] J. Edwards, 'Enterprises cut costs with open-source routers', *Computerworld*, 2014. [Online]. Tillgänglig: http://www.computerworld.com/s/article/9133851/Enterprises_cut_costs_with_open_source_routers?taxonomyId=16&pageNumber=1. [Kontrollerad: 24- Apr- 2014].

[10] Wikipedia, 'R2000 (microprocessor)', 2014. [Online]. Tillgänglig: http://en.wikipedia.org/wiki/R2000_(microprocessor). [Kontrollerad: 05- Maj- 2014].

[11] Princeton.edu, 'MIPS architecture', 2014. [Online]. Tillgänglig: http://www.princeton.edu/~achaney/tmve/wiki100k/docs/MIPS_architecture.html. [Kontrollerad: 05- Maj- 2014].

[12] B. Mitchell, 'Firmware - Router Firmware', *About.com Wireless / Networking*, 2014. [Online]. Tillgänglig: http://compnetworking.about.com/od/homenetworkhardware/g/bldef_firmware.htm. [Kontrollerad: 05- Maj- 2014].

[13] Iperf.fr, (2014). *Iperf - The TCP/UDP Bandwidth Measurement Tool*. [Online] Tillgänglig at: http://iperf.fr/ [Kontrollerad 12 Maj. 2014].

[14] Wikipedia, 'DD-WRT', 2014. [Online]. Tillgänglig: http://en.wikipedia.org/wiki/DD-WRT. [Kontrollerad: 05- Maj- 2014].

[15] Polarcloud.com, 'Tomato Firmware | polarcloud.com', 2014. [Online]. Tillgänglig: http://www.polarcloud.com/tomato. [Kontrollerad: 05- Maj- 2014].
[16] Wiki.openwrt.org, 'About OpenWrt - OpenWrt Wiki', 2014. [Online]. Tillgänglig: http://wiki.openwrt.org/about/start. [Kontrollerad: 05- Maj- 2014].
[17] Opensource.com, 'What is open source software? | opensource.com', 2014. [Online]. Tillgänglig: http://opensource.com/resources/what-open-source. [Kontrollerad: 05- Maj- 2014].
[18] InfoSec Institute, 'Packet Filtering - InfoSec Institute', 2012. [Online]. Tillgänglig: http://resources.infosecinstitute.com/packet-filtering. [Kontrollerad: 05- Maj- 2014].
[19] Tech-FAQ, 'Firewalls', 2012. [Online]. Tillgänglig: http://www.tech-faq.com/firewall.html. [Kontrollerad: 05- Maj- 2014].
[20] Linksys.com, 'Linksys Wi-Fi Router WRT54GL', 2014. [Online]. Tillgänglig: http://www.linksys.com/en-eu/products/routers/WRT54GL. [Kontrollerad: 05- Maj- 2014].
[21] Wikipedia, 'Linksys WRT54G series', 2014. [Online]. Tillgänglig: http://en.wikipedia.org/wiki/Linksys_WRT54G_series#WRT54GL. [Kontrollerad: 05- Maj- 2014].
[22] Mrxuri.com, 'Install Web Bench | Ri Xu Online', 2014. [Online]. Tillgänglig: http://www.mrxuri.com/2013/10/27/install-webbench.html. [Kontrollerad: 05- Maj- 2014].
[23] News.netcraft.com, 'June 2013 Web Server Survey | Netcraft', 2014. [Online]. Tillgänglig: http://news.netcraft.com/archives/2013/06/06/june-2013-web-server-survey-3.html. [Kontrollerad: 05- Maj- 2014].
[24] Wiki.apache.org, 'FAQ - Httpd Wiki', 2014. [Online]. Tillgänglig: http://wiki.apache.org/httpd/FAQ#What_is_Apache.3F. [Kontrollerad: 05- Maj- 2014].
[25] Ietf.org, 2014. [Online]. Tillgänglig: http://www.ietf.org/rfc/rfc1242.txt. [Kontrollerad: 05- Maj- 2014].
[26] Tools.ietf.org, 'RFC 2647 - Benchmarking Terminology for Firewall Performance', 2014. [Online]. Tillgänglig: http://tools.ietf.org/html/rfc2647.html. [Kontrollerad: 05- Maj- 2014].
[27] w. Lightmaker, 'What is the difference between Store-and-Forward switching and Cut-Through switching?', *Dlink.com*, 2014. [Online]. Tillgänglig: http://www.dlink.com/uk/en/support/faq/switches/layer-3-gigabit/dgs-series/what-is-the-difference-between-store-and-forward-switching-and-cut-through-switching. [Kontrollerad: 05- Maj- 2014].
[28] R. Bryant and D. O'Hallaron, *Computer systems*, 1st ed. Boston: Prentice Hall, 2011.
[29] Graziani, R. and Johnson, A. (2008). *Routing protocols and concepts*. 1st ed. Indianapolis, Ind.: Cisco Press.
[30] Goodrich, T. M. & Tamassia, R. 2011. Introduction to Computer Security. (2011). internal ed.
[31] Pash, A. (2014). *Turn Your $60 Router into a User-Friendly Super-Router with Tomato*. [Online] Lifehacker. Tillgänglig at: http://lifehacker.com/344765/turn-your-60-router-into-a-user-friendly-super-router-with-tomato [Kontrollerad 13 Maj. 2014].
[32] Ietf.org, (1981). *RFC 792*. [Online] Tillgänglig at: http://tools.ietf.org/html/rfc792 [Kontrollerad 25 Apr. 2014].
[33] Diva Portal, 'Performance Evaluations of Cisco ASA and Linux IPTABLES firewall', 2014. [Online]. Tillgänglig: http://hh.diva-

portal.org/smash/get/diva2:622522/FULLTEXT01.pdf. [Kontrollerad: 24- Maj- 2014].

[34] Diva Portal, 'Prestandaskillnader mellan IPv4 och IPv6 i Windows 7 och Ubuntu 10.10', 2014. [Online]. Tillgänglig: http://lnu.diva-portal.org/smash/get/diva2:422118/FULLTEXT01.pdf. [Kontrollerad: 17- Maj- 2014].

[35] Diva Portal, 'Migrering från IPv4 och IPv6', 2014. [Online]. Tillgänglig: http://lnu.diva-portal.org/smash/get/diva2:426359/FULLTEXT01.pdf. [Kontrollerad: 23- Maj- 2014].

[36] Technet.microsoft.com, 'Internet Control Message Protocol', 2014. [Online]. Tillgänglig: http://technet.microsoft.com/en-us/library/cc940069.aspx. [Kontrollerad: 24- Maj- 2014].

[37] R. Patel and B. Davidson, Forskningsmetodikens grunder, 1st ed. Lund: Studentlitteratur, 2011.

[38] Linuxjournal.com, 'Linux on Linksys Wi-Fi Routers | Linux Journal', 2014. [Online]. Tillgänglig: http://www.linuxjournal.com/article/7322. [Kontrollerad: 01- Jun- 2014]

Bilagor

Bilaga 1

Sessionstest

Open-WRT Kamikaze (r18961)					
	Antal fel				
Antal klientförfrågningar	**Test 1**	**Test 2**	**Test 3**	**Test 4**	**Medelvärde**
600	0	1	6	0	**1.75**
700	5	7	7	12	**7.75**
800	5	2	5	7	**4.75**
900	2	10	20	17	**12.25**
1000	4	11	13	23	**12.75**
1200	24	18	8	42	**23**
1400	20	40	54	7	**30.25**

DD-WRT Firmware v24-sp2 (10/10/09)					
	Antal fel				
Antal klientförfrågningar	**Test 1**	**Test 2**	**Test 3**	**Test 4**	**Medelvärde**
600	0	0	0	0	**0**
700	1	0	0	0	**0.25**
800	3	0	0	1	**1**
900	1	0	4	8	**3.25**
1000	7	1	8	51	**16.75**
1200	1	14	13	9	**9.25**
1400	11	27	16	24	**19.5**

Tomato Firmware v1.28.1816					
	Antal fel				
Antal klientförfrågningar	**Test 1**	**Test 2**	**Test 3**	**Test 4**	**Medelvärde**
600	0	0	0	0	**0**
700	0	0	0	1	**0.25**
800	0	0	0	0	**0**
900	17	70	0	0	**21.75**
1000	4	7	6	0	**4.25**
1200	19	0	38	35	**23**
1400	0	13	6	29	**12**

Bilaga 2

Genomströmningstest

Test av genomströmning (Mbit/s)					
	Test 1	**Test 2**	**Test 3**	**Test 4**	**Medelvärde i Mbit/s**
DD-WRT	42.9	43	42.9	39.7	**42.1**
Open-WRT	46	45.7	46.4	45.2	**45.8**
Tomato Firmware	47.4	44.3	45.9	49.1	**46.7**