Universitatea POLITEHNICA din București

Facultatea de Automatică și Calculatoare,
Departamentul de Calculatoare

LUCRARE DE DIPLOMĂ

Construind un "Router pe un chip" folosind platforma Freescale T1040

Conducător Științific:
ș.l. dr. ing. Adrian-Răzvan Deaconescu

Autor:
Matei Păvălucă

București, 2014

University POLITEHNICA of Bucharest

Faculty of Automatic Control and Computers,
Computer Science and Engineering Department

BACHELOR THESIS

Building a "Router on a chip" using Freescale's T1040 platform

Scientific Adviser:
ș.l. dr. ing. Adrian-Răzvan Deaconescu

Author:
Matei Păvălucă

Bucharest, 2014

Maecenas elementum venenatis dui, sit amet
vehicula ipsum molestie vitae. Sed porttitor
urna vel ipsum tincidunt venenatis. Aenean
adipiscing porttitor nibh a ultricies. Curabitur
vehicula semper lacus a rutrum.

Quisque ac feugiat libero. Fusce dui tortor,
luctus a convallis sed, lacinia sed ligula.
Integer arcu metus, lacinia vitae posuere ut,
tempor ut ante.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Routers are dedicated netwoking devices, specialized in handling data packets between computer networks. Their main purpose is forwarding packets to their next destinations. When a data packet reaches a router through one of the lines, the destination address is read and then, based upon a routing table or specialised routing policies and algorithms, it is sent toward its next destination.

Since the apparition of routers in the mid '70s, their role has not fundamentally changed, but as the hardware and the software have advanced, routers have become more compact, affordable and the offered functionalities have diversified.

1.1 State of the Art

Early routers were general purpose computers configured to forward packets between networks. With time, they were replaces by specialised hardware, that was more poweful in handling network packets. Nowadays, routers incorporate internal memory, general purpose processors, switches and wireless capabilities.

Advanced routers host tens of network interfaces, Harddisks, multiple cores, proprietary operating systems and range of communication processors for offloading different tasks in hardware (Security, pattern matching etc)

1.2 Context and Motivation

High end routing equipments have a broad range of configuration options available but the price can reach several hundred dolars. At the other end of the spectrum, low end routers offer a reduced number of network interfaces and poor performance.

For casual users, a low end router can fulfill all their needs, but as demands go up, so does the price. Advanced users and small companies are interested in more configuration options but are reluctant to invest in high end routers.

This "Router on a chip" addresses the needs of medium/advanced users and small companies who need more options, decent performance and maybe hosting space without making a pricey aquisition.

In chosing hardware for this router several factors were followed:

- The processor had to be multicore and had to be able to support an Unix based operating sistem
- The router had to have similar networking performance, with it's comercial counterparts
- Power consumption had to be as low as possible
- Price had to be as low, compared to high end devices

As it matched most of the requirements, the T1040 processor provided by Freescale was chosen for building this router.

Chapter 2

The T1040 platform

In order to create a proper router setup one needs to understand all the hardware specifications of available products and select the most suitable hardware.

The decision to use the T1040 platform can be explained by examining the hardware specifications and its general architecture, which is the aim of this chapter.

Previously, certain requirements for the finished router were stated. Proving to be a suitable platform for this router implies catering to all these needs. Simply listing the available hardware is not enough as this chapter needs to explain **why** the hardware caters best to the needs of the router.

The first part presents general hardware specifications, necessary when comparing this platform to other commercial router hardware. In the other sections, advanced construction and architectural features are reviewed, as these provide imporant advantages for the functioning router.

2.1 Hardware specifications

For a complete list of hardware specifications see [[1]].

2.1.1 CPU

One of the necessary requirements for the processor to have multicore architecture and to be strong enough to support a full fledged Unix based operating system.

In terms of CPU processing power, the platform hosts four processing cores running at a frequency of up to 1.4Ghz each. These small yet powerful e5500 [2] are based on the Power architecture are equipped with 256KB L2. The processing power is more than enough in order to run a different operating system on each core with all kinds of servers and services. While it doesn not have graphical memory, the setup can even run graphical servers, although with reduced performance.

Being powerful enough to run multiple operating systems simlutaneously, not using virtualization would greatly limit the potential of this platform. Running several virtual machines is usefull for this setup, but performance can be hindered if virtualization is handled by software.

[1] T1040 HW specs - http://www.freescale.com/webapp/sps/site/prod_summary.jsp?code=T1040

[2] http://www.freescale.com/webapp/sps/site/overview.jsp?code=64BIT

When virtualization is done in software, virtual machines are treated like normal programs by the operating system. Unfortunately, accessing hardware devices from the virtual machine(VM) implies passing the call from the VM to the operating system, which in turn is able to access the hardware. This creates overhead and the VM performance is rather limited.

Hardware virtualization solutions have increased complexity, but they offer improved performance over software solutions.

An important feature of this platform is the presence of the 3 levels of instructions: user, supervisor and hypervisor. Instruction levels in CPU instruction sets control access of the program currently running on the processor to resources such as I/O ports, special instructions and memory regions. The hypervisor instruction level is used in hardware virtualization by the Virtual Machine Manager(VMM) or hypervisor, that acts as a host for the virtual machines.

All these features allow the platform to run multiple VMs without losing performance, greatly extending application scenarios that can be run.

2.1.2 Memory

Random Access Memory(RAM) is important in every machine, as its speed and quantity shape the overall performance of the machine. Too little RAM and programs running at one time on the machine are limited both in performance and number. Having an outdated type of RAM implies slow access speeds which again, limit the overall performance of running tasks.

In the virtualization environment RAM requierements are even greater, as each machine needs its own dedicated RAM space.

The T1040 platform supports DDR3 type RAM and the maximum throughput is 1600MT/s. For this application only 2GB of RAM were installed, as this is satisfactory for the type of applications running.

As this is a networking application Direct Memory Access(DMA) is one of the critical features used by the system. DMA allows subsystems to access the main system memory independently of the CPU. To address this, the platform hosts dual four channel DMA.

TODO:
reread the above paraghraph

On the connectivity side, included are 2 Serial ATA(SATA 2.0) controllers, enhanced secure digital host controllers (SD/MMC/eMMC), 2 USB2.0 ports with integrated PHYs, 4 PCI-express ports, controllers for NAND and NOR flash memory and 4 UART ports.

TODO:
Poate e mai bine ca lista??

The networking connectivity includes 5 Gbps Ethernet MAC ports (with support for SGMII and QSGMII interfaces) and a hardware Gigabit Ethernet switch with 8 ports.

TODO:
Spune de specificatiile placii wireless

2.2 General arch details

Being a Communications Processor T1040 offers facilities for speeding up packet analysis, clasification and distribution, by offloading them in hardware. Also present are Buffer Managers and Queue Managers for handling frames in hardware, before they get sent for processing.

TODO:
cred ca e mai bine pe lateral, pusa pe o pagina intreaga

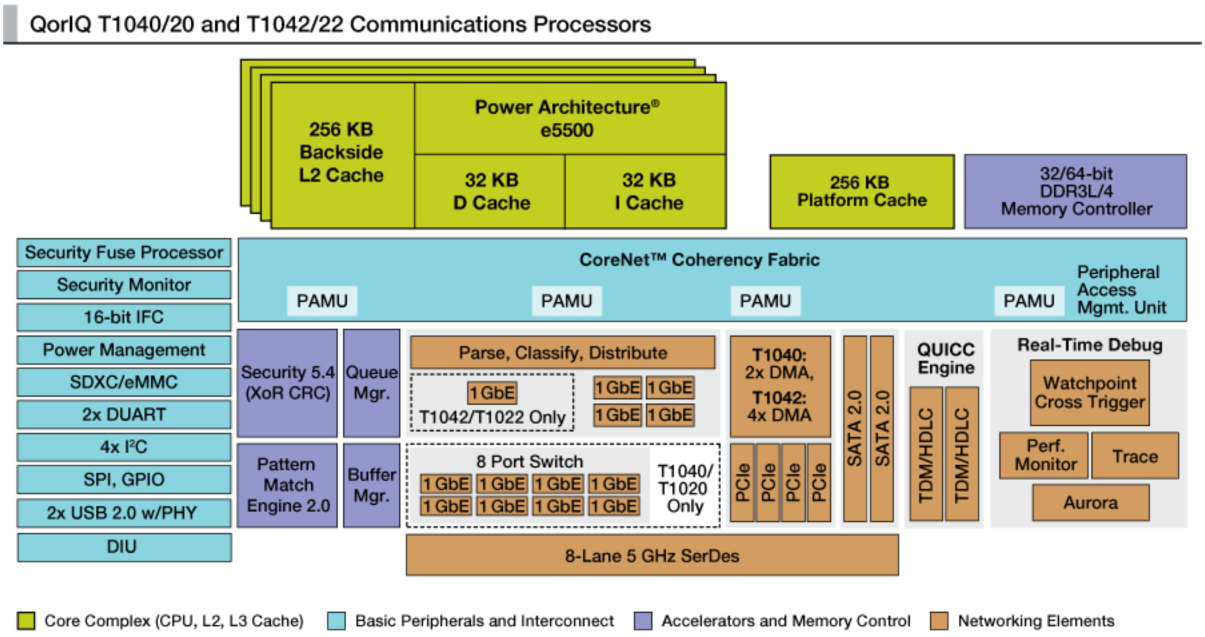

Figure 2.1: T1040 diagram

As soon as a packet enters through the physical interface it gets handled by a Frame Manager. The Frame Manager is responisble for having pre-allocated frames for the incoming packet. This is where the Parse, Classify, Distribute step takes place. The pattern maching is done by a configurable HW engine. Based on the analysis, the packet is then classified and handed to the Queue Manager. The Queue Manager can set affinities for different types of traffic, allowing to send all packets of a type to preset processor

We can also have citations like [1].

2.3 Why is it good for what we need

The presence of a Frame Manager, PCD(Parse, Classify, Distribute) engine and encription/decription engine means that an important part of the operations done by a router, for example static forwarding, blocking ports and filtering traffic can be done by the hardware.

All this hardware offloading capabilities of this platform helps save important CPU cycles allowing it to maintain higher transfer rates with with less CPU load, leaving more capabilities for the applications running on the machine.

These advantages recommend the platform for this type of application.

Chapter 3

Router characteristics

This chapter presents the different functionalities of the router. The features range from basic requirements, needed in order for the setup to function as a minimal router to advanced features, that separate this setup from other comercial routers. All the features presented are for **this** setup. There are other functionalities that can be added, as the hardware and software allows it, but these are just a proof of concept.

3.1 Basic functionality

These functionalities are needed by the application in order to function as a router. They are provided by almost all commercial routers, therefore they can not be absent.

3.1.1 LAN network with switching

One of the basic characteristics of a router is being able to function as a switch. Switching involves passing packets between different LAN segments. This can be done either at Layer 2 of the OSI reference model, using MAC addresses or at Layer 3, using IP addresses. Switches employ a number of protocols in order to determine where to send each incoming packet.

Switching can be done both in hardware and in software. Software solutions, while being cheaper and more versatile in configuring, have a lot to suffer when it comes to intense packet crunching. This is why HW switches are preffered.

This setup integrates a hardware Layer 2 switch with 8 LAN ports and is able to handle the packets at speeds up to 1Gbps.

3.1.2 Wireless network

In recent years, Wireless capabilities have become one of the most used features of routers. With the increase in popularity of mobile devices, laptops, tablets and smartphones which rely almost solely on this technology in order to connect to the internet, not having a wireless network integrated into the router is not an option. Furthemore the adapter needs to be compatible with all kinds of devices, both new and old.

To address this need, this router has a wireless network card that complies with the IEEE 802.11b/g/n standards and has a transfer rate of up to 150Mbps.

3.1.3 Wireless security and authentification

Simply having a wireless connection is not enough for the good functioning of the router. Security is a very important issue. Being able to limit access to the wireless network only to the authorised devices is crucial.

Therefore, the setup has to offer authentification support. Out of several alternatives for an authenthification service, HostAP was chosen as it is easy to use and does not need constant configuration.

Out of the authentification protocols, WEP,WPA and WPA2, the latter was chosen for its improved security over the former two.

3.1.4 Wireless and LAN bridge

On basic routers that feature both LAN and Wireless support, devices connected through different networks need to be able to communicate with each other.

With this in mind, LAN and Wireless are bridged forming a single address space. This choice was made for the sake of simplicity, although it has a downside. Switching between LAN and the Wireless network is limited in speed compared to switching between the LAN ports.

3.1.5 HW/SW routing

Routing, along with switching represents the core of the router's functions. This device currently has capabilities for routing both in software and using the hardware.

Routing in software relies on setting static routes in the operating system. It is easily configurable, but the disadvantage is that all these operations consume precious CPU cycles. Therefore, routing using the hardware is preffered, where possible.

Hardware routing implies configuring the Frame Manager to intercept certain types of traffic / addresses, to bypass verification by the kernel and send them directly to a specified port. While it is a bit rigid and hard to configure, it can provide a very important speed boost over software routing.

3.1.6 Network Address Translation

Because the IPv4 address space is limited, routers usually have just one address, as it seen from the Internet. If each machine serviced by the router would have a different external IP address, the whole IP space would be used up very fast. The problem is that most users want to connect multiple machines to a router and each of them has to have internet access. They each have their own internal IP address but they must share only one external IP address.

In order to solve this problem, the Network Address Translation protocol (NAT) was created. NAT holds mappings between internal IP addresses and external ports. Each device that wants to access the internet will receive its own port on the external interface which will service all traffic directed to that machine. From the internet's point of view, there is only one machine, but multiple ports.

This requirement had to be addressed as well, as the absence of NAT would mean that the internet is accessible only from the router, not from the connected devices. Therefore, NAT is done in software, through **iptables**.

3.1.7 SW services

Modern roters employ a number of software services in order to run efficiently. Amongst these, there are DHCP client and server, PPPoE client and port forwarding.

DHCP (Dynamic Host Configuration Protocol) is a standardized networking protocol used for distributing network configuration parameters such as IP addressesi automatically. When using DHCP, devices request networking parameters from a DHCP server, removing the need for a network administrator to configure these settings by hand.

The router needs both a DHCP client and a server. The client is used in order to request networking paramenters from the Internet Service Provider (ISP) DHCP server. The internal DHCP server is used to service requests coming from the internal network, LAN and Wireless.

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames. It currently is one of the most used methods of connecting a device the ISP network. It's an alternative way of connecting and needs to be offered as an option, in order to cover basic usecases of the router.

The last basic service offered is Port Forwading. Port forwarding binds an external port,located on the router,to a port located on a machine in the internal network. All traffic sent to the specified external port is forwarded to the internal port. As some services are port dependent, NAT can change incoming ports so these services can't function properly. This technique is used to permit communication between external hosts and services provided within the private LAN.

All these protocols and servers are available on the router. DHCP client and server are installed, the PPPoE client is installed and port forwarding is done through **iptables**.

3.1.8 Easy administration using Webmin

Configuring a router can be a confusing task, especially for inexperienced users. Although this router targets medium/advanced users, the problem of easy configuration still remains. Normally, this setup would be configured by connecting through SSH and by changing different options and configuration files directly. However, a more elegant and accesible solution can be found.

Routers usually can be configured through a web interface. There are some clear advantages with this approach. The first one is that one can do the configuration on any device that has a web browser and is connected to the network. The second advantage is that all options are a few clicks away, easy to find and alter.

With this in mind, a router that is not capable of offering easy configuration would have a big dissadvantage over comercial routers. As a solution, a Webmin server has been installed on the router.

Webmin[1] is an open source project that provides a web-based interface for system administration for Unix. Using any modern browser one can setup user accounts, Apache, DNS and change everything you want about the administrated machine.

Using Webmin administrators don't need to connect physically to the machine and manually edit configuration files. It also provides support for scripts, a shell and has a modular construction, making it easy to extend or limit the functionalities of the client.

Webmin is even more powerful than normal web-based router configuration solutions, as it allows its users to change virtually any setting on the router machine.

[1] http://www.webmin.com/

3.2 Advanced functionality

Basic features are the core of the router, but the advanced feature separate this router setup from other commercial solutions and provide powerful aditions to the router capabilities.

3.2.1 HW/SW firewall

The firewall is a security system that controlls incoming and outgoing network traffic based on specific rules. The firewall is a barrier between the trusted, internal network and the external network, deemed unsafe.

Software firewalls are very customisable but costly for the CPU and can lead to performance deterioration. On the other hand, hardware firewalls don't put any stress on the CPU, but are harder to configure.

The router has firewalling capabilities both in software and hardware. Software firewalling is done using **iptables**. Hardware firewalling is enabled by configuring the Frame Manager. This HW firewall can drop traffic, block ports and filter traffic based on source and destination.

3.2.2 Demilitarized partition

The feature that makes this setup stand out the most compared to similar performing routers is the presence of the virtualisation environment, and virtual machines.

The Demilitarized Partition(DMZ) is a virtual machine, running on the router that can be used to deploy all sorts of applications, for example web hosting, email servers and FTP servers. It is a full fledged machine, having its own dedicated CPU core, kernel image and filesystem and most importantly it can be restarted without restarting the whole router.

This DMZ partition can be compromised without losing data, or contaminating the entire machine. The root filesystem is loaded from flash, but it can be loaded restored from an virtual machine image as well.

Having such a feature is a powerful bonus of this router as the DMZ cand host almost any application that runs properly on a single core machine. It is secure, completely isolated, easy to setup and restore.

Installed on the DMZ partition is a lighttpd server that serves static content. It is just an example of the applications that can run securely, without impacting the router's overall performance.

3.2.3 Storing space on the HDD

Routers usually feature limited storing space, but in recent years, this feature has become more and more requested. Having a full HDD usually increases the router price beyond mid level but for multiple potential virtual machines and for the type of applications that the router is able to run, not having enough storing space can be detrimental

As a result the router is equipped with a 250GB HDD. All applications benefit from this storing space and it can even save multiple snapshots of the DMZ parition.

Chapter 4

Architecture / Implementation

TODO:
schema cu partitionarea si flow-urile

So far, the HW specifications and features of this router were covered. This chapter provides details in the internal functioning of the machine, how all the services, settings and systems work together in order for it to function as a router.

4.1 Overview

From a top down perspective the router is composed of 2 different virtual machines that run on the hardware, that will pe called partitions:

- The Master partition
- Demilitarised or Slave partition (DMZ)

Each parition runs its own kernel and rootfilesystem and is completely independent of the other partition, meaning it can be shut down or rebooted without impacting the other partitions. In practice, the DMZ is dependent on the Master partition, as all traffic that is destined for the DMZ passes through the Master.

Both Master and DMZ run the same kernel image which is based on the 8.12 linux kernel.The Master partition has its root filesystem loaded from the HDD, while the DMZ has the root filesystem in flash.

4.1.1 Master partition

This partition is responsible for handling most of the HW the machine has. It controls 3 of the 4 cores, the HDD, all the conectivity ports and network interfaces.

It also functions as a gateway, linking the external network (the internet) with the Wireless, LAN and DMZ.

As such, it's natural for all the critical software components and services to be hosted on the Master partition.

4.1.2 DMZ partition

The second partition acts as a deployment space for all the services that need to be accesed from the external network. This partition can be compromised without endangering the router or the internal network.

Because the root filesistem is always loaded from flash memory, the DMZ acts as a frozen machine, any changes made there being non-persistent. In case of a malitious attack, a simple reboot will restore the machine to it's previous state, without endangering the Master partition.

The DMZ hosts a lighttpd server which serves static content, but virtually any service that can run on a single core can be deployed there. In case of more complex servers (which need persistent storage) the DMZ cand act as a frontend, having a backend on the Master partition and exchanging calls.

4.2 Networks

TODO:
schema cu toate retelele

From the networking point of view, the router hosts 4 networks and 3 addres spaces:

- LAN + Wireless are bridged under the same address space
- External network provides the Master partition with a dinamic IP, making it a gateway
- Communication between partition is done through macless ports

4.2.1 The Bridge

TODO:
schema cu bridge-ul si switch-ul

The wireless interface(wlan0) and the LAN interface(eth1) are bridged using OpenVSwitch, an open source solution for software switches. The bridge acts as contact point between LAN, Wireless and the other networks. The bridge interface is configured with a static IP and the DHCP server listens for request on this interface.

Switching inside the LAN network is done at high speed, as the hardware switch handles all the packets sent between the physical switch interfaces, but all traffic that is sent to the Wireless network has to go through the bridge and through one of the CPUs.

The switch has an internal port connected to the machine (controlled by the operating sistem) fig??? which is used as an exit point for all the internal traffic of the switch. The problem is that this port is Gigabit, so it's speed is insufficient in order to service the combined traffic speeds of the external ports simultaneously. This is effectively a bottleneck. Such behavior can occur for example when all the machines connected to the external ports try to transfer data to the internet.

The Wireless Adapter has a maximum speed of 150Mbps so the maximum (theoretical) transfer rate between a machine connected through the Wireless network is limited to that amount. The setup can be upgraded with a more powerful wireless card, but for this type of application the Gigabit Wireless card was considered unnecessary.

4.2.2 Connecting to the Internet

One of the Ethernet ports(eth0) is connected directly to the exterior network. By default this internet receives it's IP dinamically, but it can be configured to have a static IP, or to connect through PPPoE.

Being the only connection with the exterior, this makes the Master Partition the Gateway of all the networks. With this in mind, certain protocols and services such as NAT and firewalling are specific only to this interface.

In a real-life scenario, where several LAN clients are trying to send traffic to the exterior this interface can prove to be a bottleneck, as it's speed is Gigabit(1Gbps), while the combined maximum traffic of all the other networks exceeds the ports capabilities.

4.2.3 Communicating with the DMZ

The communication between the DMZ and the Master partition is done with the help of the hypervisor with a pair of preconfigured macless ports. From the operating sistem point of view, these macless interfaces behave identically with other interfaces, the only difference is in their implementation in the kernel.

The macless ports are configured statically, the Master having the address 1.1.1.1 and the DMZ having 1.1.1.2. Int he current setup, this connection is used mainly for controlling the DMZ, as the Slave partition has no means of connecting to the Master in this way. The motivation behind this design choice was the total isolation of the DMZ in case of an attack.

4.3 Services

TODO:
Spune despre toate serverele instalate si ce fac

The machine needs certain servers and services in order to function as a router. This section provides details on the installed services that are currently available how they are configured.

4.3.1 Master Partition services

The Master partition needs to bridge the LAN with the Wireless network. This is done using OpenVSwitch. Both interfaces are aggregated unde a virtual interface, br0.

Listening on **br0** are certain servers:

- Hostapd server, for authentification on the Wireless network.
- DHCP server, servicing any IP requests. In order fo the DNS to work relaying is configured in the DHCP server, informing any new connected machines of the address of the external DNS server. This is currently done statically, therefore changing the ISP, or connecting the router to a new external network implies changing the mentioned DNS address in the dhcpd configuration file.
- SSH server, for remote connection and configuration
- Webmin server, having increased importance, allowing remote connection and configuration using any web browser in order to provide conveninence in administration.

No specific firewall rules are applied to the **br0** interface, except for a forwading rule, that diverts all incoming traffic on port **8080** to port **80** on the **DMZ**. This is the only way to acces the webserver that is running on the Slave Partition.

The Gateway interface, **eth0** has a limited number of servers servicing it, but it has the most firewall rules.

The only servers listening on this interface are the **SSH** server, for configuration and the **DHCP** client for obtaining the dynamic IP. On demand, a PPoE client can be configured,.

All external traffic for ports greater than **2000** is blocked by the HW firewall, so packets destined for other ports are dropped without reaching the SW. The exception is port **8080**, which is configured to be forwarded to port **80** on the DMZ in a similar way to the **br0** interface.

As for **NAT**, necessary for communicating between the internal and the external network, it is available through **iptables** rules.

4.3.2 DMZ services

The DMZ services are limited compared to the Master Partition. There is a **SSH** server running, for remote administration and a **lighttpd** server that serves static content.

Howerver, almost any server that can be effectively run on a single core machine can be hosted here, for example FTP, streaming and mail servers.

Due to the nature of the root filesistem setup on the DMZ, installing new servers implies making modifications to the rootfs and then writing the new rootfs to the flash memory. Servers also need to be able to recover gracefully in case the DMZ encounters a hard reset.

4.4 Packet flows

Through design, the router has a number of different packet flows. Understanding and separating them can help in a number of applications, for example setting different processor affinities based on the type of incoming traffic.

In figure?? 4 packet flows are identified. Although one can argue that more flows can be isolated, they are, in general, separated by their different source and destination.

The first flow, marked in COLOR1 in diagram??? is the LAN/Wireless flow. Traffic is generated in either Wireless or LAN and it has it's destination in the same network. This includes LAN to LAN, Wireless to Wireless and LAN to Wireless traffic. This traffic is not subject to any artificial limitations or filtering, and the speed is limited by HW.

The typical usecase that generates this kind of traffic is data transfer between computers on the internal network (in the same address space).

The second flow, marked in COLOR2 is between the internal network and the external one. Traffic on this flow is filtered, external ports greater than **2000** being closed, with exceptions. Because the 2 networks are in distinct address spaces, all packets need to pass through NAT.

A tipical usecase that would generate this flow is a computer on the internal network trying to access the internet.

The third and fourth flow are similar, each having one endpoint in the DMZ partition. They are generated when either the external network or the internal one tries to acces resources located on the DMZ. These resources are not accessed directly, as the interface between the two partitions is not directly addressable by the two networks.

For example when a machine on the internal network wants to acces the http server located on the DMZ, it will access port **8080** on its gateway address (in this case, the bridge, **br0**, interface). Incoming connections on port **8080** are routed statically to port **80** on the DMZ machine.

The same principle applies for accesing the DMZ located http server from the external network. A request to port **8080** of the external interface are routed to the DMZ on port **80**.

Any server running on the DMZ that needs to be access receives it's own forwarding rule, statically.

Chapter 5

Usecases

In previous chapters both software and hardware capabilities of this setup were preseted. There were also indications on potential bottlenecks and performance limitations. All these characteristics, combined with the price range of the platform and its power consumption, recommend it for certain applications. The limited number of interfaces makes this router better suited for home / small office use.

The wireless card supports more connections than the physical ones, but perfomance is dictated by the type of the wireless card. The currently instaled one is an entry level card, so performance is rather weak.

Another aspect taken into consideration is that, while easy to configure through the web interface, the setup offers a great range of configuration options that can be hard to understand for the average user. With this in mind, this router is most likely destined for medium and advanced users.

5.1 Simple Router

The first usecase for this setup is a simple router, suited for home or small office use. Basic router features like NAT, DHCP, switching, wireless as well as the configurable firewall are the base of this usecase.

In most cases, performance in this case is not critical, the DMZ is not used and the HDD is not necessary.

While it can function perfectly in this role, other single-core solutions can be found on the market that offer similar perfomance, but feature a lower power consumption, lower price and are easier to configure and maintain.

If performance is critical, the DMZ can be disabled (all 4 cores would be controlled by the Master Partition), the wireless card can be upgraded and certain CPU affinities can be set in order to ballance the load.

The conclusion of this usecase is that if performance is not critical, this is a sub-optimal choice for role of simple router.

5.2 Lightweight hosting service

Another potential usecase of this setup is that of a hosting platform for several webservers. The features that recommends it for such a purpose is the customizable number of virtual machines. If router services are not critical, the master partiton can downgraded and up to 3 virtual machines can function at the same time on the machine, each with its own servers. These machines function independently and can be powerd on/off and reset without disturbing the whole ecosystem.

The usecase is called "lightweight", as this architecture is not the best suited for heavy server-side processing.

In conclusion, this router can offer some powerful customization options for small companies trying to host some of their servers on isolated environments.

5.3 Hybrid router-hosting service

The usecase that is most suitable for this setup is that of a hybrid, deploying full router capabilities while still having one or two virtual machines used of services.

This would be the best use of the router's resources and would prove valuable, cost wise and performance wise. The designation would still be "lightweight" as the hardware isn't best suited for handling CPU intensive tasks.

Chapter 6

Conclusions

Bibliography

[1] International Organization for Standardization. Iso/iec 26300:2006 open document format. http://std.dkuug.dk/keld/iso26300-odf/is26300/iso_iec_26300:2006_e.pdf, December 2006.