

João Pedro Costa Vieira
Tiago Miguel Rodrigues Gonçalves Limpo

Licenciatura em Engenharia Informática

Implementação IPv6 e DNSSEC

Dissertação para obtenção do Grau de Engenheiro em
Engenharia Informática

Orientador: Prof. Doutor José Faísca, ULHT
Prof. João Ildefonso, ULHT

Júri:

Presidente: Prof. Doutor José Rogado
Vogais: Prof. Doutor Pedro Malta

“Copyright” João Vieira e Tiago Limpo, ULHT

A Universidade Lusófona de Humanidades e Tecnologias tem o direito, perpétuo e sem limites geográficos, de arquivar e publicar esta dissertação através de exemplares impressos reproduzidos em papel ou de forma digital, ou por qualquer outro meio conhecido ou que venha a ser inventado, e de a divulgar através de repositórios científicos e de admitir a sua cópia e distribuição com objectivos educacionais ou de investigação, não comerciais, desde que seja dado crédito ao autor e editor.

AGRADECIMENTOS

Aos meus coordenadores, Professor Doutor José Faísca e ao Professor Doutor João Ildefonso, por me terem proporcionado a oportunidade de realizar este projecto, pela orientação, disponibilidade e ensinamentos prestados, durante a realização deste projecto.

A todos os meus amigos e colegas que ao longo do curso me apoiaram incondicionalmente, nomeadamente, Beatriz Gaspar, Catarina Carneiro, Francisco Guerreiro, Ivan Soares, João Tomás, Mário Caldeano, Manuel Costa, Nuno Maia, João Brito, Markus Wolf, Tiago Paixão, Vítor Lopes, Valter Proença e ao meu colega de grupo João Vieira. Entre outras inúmeras pessoas que foram bastante importantes a nível académico e pessoal.

Por último, aqueles que sempre me acompanharão;
Aos meus pais, irmão e avós, por todo o apoio, carinho e compreensão em todos os aspectos da minha vida.

Tiago Limpo

Aos meus coordenadores, Professor Doutor José Faísca e ao Professor João Ildefonso, por me terem apostado em nós para a realização deste projecto, pela orientação, disponibilidade e ensinamentos prestados durante a duração do mesmo.

A todos os meus amigos e colegas que ao longo do curso me apoiaram incondicionalmente, nomeadamente, Beatriz Gaspar, Catarina Carneiro, Ivan Soares, João Tomás, Mário Caldeano, Manuel Costa, Nuno Maia, João Brito, Tiago Paixão, João Rico e ao meu colega de grupo Tiago Limpo. Entre outras inúmeras pessoas que foram bastante importantes a nível académico e pessoal.

Por último, aqueles que sempre me acompanharão;
Em especial aos meus pais e irmão e a toda a família, que sempre acreditaram em mim e me apoiaram em tudo o que apostei na minha vida até então.

João Vieira

RESUMO

IPv6

A possibilidade de podermos ter a nossa torradeira com IP, assim como o nosso frigorífico ou mesmo o forno estarem acessíveis a partir de qualquer parte da Internet?

O **IPv6** é a nova versão do IP, e foi desenvolvido para suceder à actual versão (o IPv4). O que motivou o desenvolvimento desta nova versão foi a aproximação da exaustão do espaço de endereçamento e a necessidade de resolver algumas das limitações do IPv4, nomeadamente no que toca à segurança, com a ajuda do DNSsec, mobilidade e simplificação de algumas das funcionalidades do protocolo IPv4.

A escassez de endereços, embora manifestando-se globalmente, é particularmente grave em certas zonas do globo onde a Internet não tem tido grande evolução e para as quais foram reservadas pequenas faixas de endereçamento. Na Europa, embora a situação não seja dramática, o problema existe e a Comunidade Europeia está a apostar na evolução para o **IPv6** tendo sido criada uma *Task Force* para o efeito.

DNSSEC

É o nome dado às extensões de segurança ao protocolo DNS e foi criado para proteger e autenticar o tráfego DNS. Estas extensões procuram validar os dados através de assinaturas digitais, fazendo uso de assinaturas criptográficas assimétricas.

Provê segurança para a resolução de endereços. Funciona como um caminho alternativo para a verificação de autenticidade. Por exemplo, no caso de domínios .eu vai ser obrigatório a utilização do **DNSSEC**.

Estas operações ocorrem antes de qualquer verificação de segurança em camadas superiores (SSL, SSH, PGP etc...). A autenticidade e integridade são providas pela assinatura dos Conjuntos de Registos de Recursos (Resource Records Sets - RRset) com uma chave privada. Zonas delegadas (filhas) assinam seus próprios RRsets com sua chave privada. Autenticidade da chave é verificada pela assinatura na zona pai do Recurso DS (Record DS) (hash da chave pública da zona filha).

A chave pública é usada para verificar RRSIGs dos RRsets. Autenticidade da não existência de um nome ou tipo provida por uma cadeia de registos que aponta para o próximo em uma sequência canónica.

ÍNDICE DO TEXTO

GLOSSARIO	12
1. INTRODUÇÃO	16
1.1. Considerações Gerais	16
1.2. IPv4 Vs. IPv6	16
1.3. Data para a mudança	17
2. EXPOSIÇÃO E EXPLICAÇÃO DO PROBLEMA	19
2.1. Introdução	19
2.2. Esquema da rede principal	20
2.3. Software utilizado	21
3. SOLUÇÕES POSSÍVEIS	23
3.1. Introdução	23
3.2. Soluções versus endereçamento	23
3.2.1. Endereçamento Unique-Local	24
3.2.2. Endereçamento Global, Prefixo 2001::/64	24
3.2.2.1.1. Com acesso HSDPA	24
3.2.2.1.2. Prefixo 2001::/64 (ISP)	24
3.2.2.1.3. Tunnel brokers	25
3.3. Túnel Manual	
Vantagens	26
Desvantagens	26
3.4. Túnel 6to4	
Vantagens	27
Desvantagens	27
3.5. Túnel Hexago	
Vantagens	28
Desvantagens	28
4. ARQUITECTURA DA SOLUÇÃO IMPLEMENTADA	30
4.1. Introdução	30
4.2. Configuração da UTM	30
4.3. Configuração de domínio IPV6 (Windows)	30
5. TESTES	31
5.1. Introdução	31
5.2. Conexão IPv6 – IPv6	32
5.3. Conexão IPv6 – IPv4	32
5.4. VPN	32
5.4.1. OpenVPN	32
5.4.2. VPN PPTP conexão IPv4	32
5.5. IPv6 por Wi-Fi	32
6. CONCLUSÕES	33
6.1. O IPv6 no Mundo	33
6.2. Custos de Implementação	34
6.3. Sobre o trabalho	35
7. DNSSEC	36
7.1. Introdução	36
7.2. Porque é o DNSSEC necessário?	36
7.3. Como funciona o DNSSEC?	37

ÍNDICE DE FIGURAS

Fig. 1 – IPv4 Vs. IPv6	16
Fig. 10 – Funcionamento do túnel da Hurricane Electric	25
Fig. 11 – Teste com Visual Route 2008 www.sapo.pt	28
Fig. 12 – Exemplo do encaminhamento com tunnel Hexago	28
Fig. 13 – Tunnel IPv6 a funcionar	30
Fig. 14 – Teste com Visual Route 2008 acesso a um site IPv6	31
Fig. 15 – Ping através de um tunnel Sixxs	31
Fig. 16 – Esquema Open VPN	32
Fig. 17 – Funcionamento do DNSSEC	37
Fig. 2 – Contagem para o esgotamento do IPv4	16
Fig. 3 – Mapa mundial de registos da internet	17
Fig. 4 – Esquema da rede física	19
Fig. 5 – Laboratório virtual	20
Fig. 6 – Switch do laboratório virtual	21
Fig. 7 – Ping a um endereço link-local	22
Fig. 8 – whatismyv6.com via tunnel broker	23
Fig. 9 – Detalhes do tunnel broker	24

GLOSSÁRIO

(por ordem alfabética)

ACL – *Acces Control List*
AD – *Active Directory*
ADSL – *Asymmetric Digital Subscriber Line*
ALG – *Application Layer Gateways*
APNIC – *Asia Pacific Network Information Center*
APJII – *Asosiasi Penyelenggara Jasa Internet Indonesia*
ARIN – *American Registry for Internet Numbers*
ARP – *Address Resolution Protocol*
ATM – *Asynchronous Transfer Mode*
BGP – *Border Gateway Protocol*
CAR – *Committed Acces Rate*
CGAs – *Cryptographically Generated Addresses*
CNNIC – *China Internet Network Information Center*
CQ – *Custom Queueing*
CRTP – *Compressed Real-Time Protocol*
DA – *Destination Address*
DAD – *Duplicate Address Detection*
DHCP – *Dynamic Host Configuration Protocol*
DHCPv6 – *Dynamic Host Configuration Protocol versão 6*
DNS – *Domain Name System*
DNSSEC – *Domain Name System Security Extensions*
DOS – *Denial of Service*
EIGRP – *Enhanced Interior Gateway Routing Protocol*
ESP – *Encapsulating Security Payload*
FR – *Frame Replay*
FTP – *File Transfer Protocol*
GLBP – *Gateway Load Balancing Protocol*
GPO – *Group Policy*
JPNIC – *Japan Network Information Center*
KRNIC – *National Internet Development Agency of Korea (do Sul)*
HSRP – *Hot Standby Routing Protocol*
HTTP – *Hypertext Transfer Protocol*
HTTPS ou SSL – *Secure Socket Layer*
IANA – *Internet Assigned Numbers Authority*
ICMP – *Internet Control Message Protocol*
IEEE – *Institute of Electrical and Electronics Engineers*
IGMP – *Internet Group Membership Protocol*
IOS – *Internetwork Operating Security*
IPv4 – *Internet Protocol, versão 4*
IIS7 – *Internet Information Service, versão 7*
IPv6 – *Internet Protocol, versão 6*
ISP – *Internet Service Provider*
IS-IS – *Intermediate System to Intermediate System*
LIR – *Local Internet Registries*
MLD – *Multicast Listener Discovery*
MTU – *Maximum Transmit Unit*
NA – *Neighbor Advertisement*
NAP – *Network Architecture Protection*

NAT – *Network Address Translation*
NBAR – *Network-Based Application Recognition*
NBMA – *Non Broadcast Multi-Access*
NEMO – *Network Mobility*
MAC – *Media Access Control*
MIPv4 – *Mobile IPv4*
MIPv6 – *Mobile IPv6*
MLD – *Multicast Listener Discovery*
NLA – *Next-Level Aggregation Identifier*
NS – *Neighbor Solicitation*
NTP – *Network Time Protocol*
PDA – *Personal Digital Assistant*
PAT – *Port Address Translation*
POP3 – *Post Office Protocol*
PPP – *Point-to-Point Protocol*
PPTP – *Point-To-Point Tunneling Protocol*
PQ – *Priority Queuing*
QoS – *Quality of Service*
RA – *Router Advertisements*
RAM – *Random Access Memory*
RFC – *Request for Comments*
RIP – *Routing Information Protocol*
RIRs – *Regional Internet Registries*
RSVP – *Resource Reservation Protocol*
RSVP2 – *Resource Reservation Protocol, versão 2*
SLA – *Site-Level Aggregation*
SIP – *Session Initiation Protocol*
SA – *Source Address*
SO – *Sistema Operativo*
SSM – *Source-Specific Multicast*
TCP – *Transmission Control Protocol*
TLA ID – *Top-Level Aggregation Identifier*
TOS – *Type of Service*
TTL – *Time To Live*
TWNIC – *Taiwan Network Information Center*
UDP – *User Datagram Protocol*
UTM – *Unified Threat Management*
VPN – *Virtual Private Network*

CAPÍTULO 1

1. INTRODUÇÃO

1.1. Considerações Gerais

A necessidade da elaboração deste projecto insere-se com o anunciado esgotamento da arquitectura de IPv4, prevista para dia 1 de Julho de 2012. À data da elaboração deste documento faltavam apenas 17 dias.

Assim sendo o IPv6 surge como sendo o substituto necessário e eminente do IPv4, apesar das enormes vantagens que esta nova arquitectura apresenta existe também um enorme risco, pois o IPv4 levou anos até ficar totalmente afinado. Com esta nova arquitectura muitas questões se colocam em termos de segurança e se não seria preferível uma “reciclagem do IPv4” ao invés da criação de uma nova arquitectura, pois um dos problemas que este apresenta é a sua credibilidade.

1.2. IPv4 Vs. IPv6

O IPv4 apresentava um espaço de endereçamento cerca de 4.3×10^9 disponíveis que no início da década de 80 seriam mais que suficientes, isto porque este protocolo foi concebido numa era em que o computador era um equipamento pouco acessível. Mas com a multiplicação destes equipamentos, associado ao suporte de IP, e com pouca razoabilidade na alocação de endereços, levou a que o esgotamento desta arquitectura se tornaria eminente.

Numa altura de abundancia de endereços empresas como a **IBM, HP**, entre outras puderam adquirir classes completas A e B, quando uma classe C se justificaria por completo (visto estarmos a falar em blocos de 255 endereços).

O IPv6 tornou-se sendo o substituto ideal, visto que a maior vantagem apresentada por este é o facto de o endereçamento ser feito a 128 bits, em contraponto aos 32 bits oferecidos pelo IPv4. Isto resolve grande parte do problema de falta de endereços disponíveis pois, com 128 bits é possível endereçar um total de:

$2^{128} = 340,282,366,920,938,463,374,607,431,768,211,456$ hosts, para ser mais fácil de conseguirmos compreender este numero astronómico é o mesmo de estarmos a falar de 655.570.793.348.866.943.898.599 ($6,5 \times 10^{23}$) endereços por m^2 da superfície terrestre.

O quadro seguinte ajuda-nos a ter uma maior percepção das vantagens que o IPv6 nos oferece em relação ao IPv4

IPv4	IPv6
Endereços de 32 bits	Endereços de 128 bits
Suporte opcional do IPSec	Suporte nativo de IPSec
Nenhuma referência a capacidade de QoS (qualidade de serviço)	Introduz capacidades de QoS utilizando para isso o campo Flow Label
Processo de fragmentação realizado pelo router	A fragmentação deixa de ser realizada pelos routers para passar a ser processada pelos hosts emissores
O cabeçalho inclui os campos de opção	Todos os campos de opção foram mudados para dentro do campo Extension header
O Address Resolution Protocol (ARP), utiliza requisitos do tipo <i>broadcast</i>	O ARP foi abandonado, sendo substituído por mensagens de multicast Neighbor Discovery
Internet Resolution Management Protocol (IGMP) é utilizado para gerir relações locais de sub-redes.	O IGMP foi substituído por mensagens de Multicast Listener Discovery
Os endereços de <i>broadcast</i> são utilizados para enviar tráfego para todos os hosts de uma rede	Deixa de existir endereços do tipo <i>broadcast</i> , para utilizar endereços multicast
O endereço tem de ser configurado manualmente	Adição de funcionalidades de auto configuração
Suporta pacotes de 576 bytes, passíveis de serem fragmentados	Suporta pacotes de 1280 bytes, sem fragmentação

Fig. 1 – IPv4 Vs. IPv6

1.3. Data para a mudança

Aqui surge o primeiro problema a data para prevista para o esgotamento público do IPv4 é pouco consensual inicialmente estaria apontado para 2011, 2012, mas actualmente não se consegue dar ao certo uma data certa.

Existe alguns sites que tentam ser o mais preciso possíveis como é o caso do <http://penrose.uk6x.com/>

RIPE Regional registry IPv4 address exhaustion in...

17 Days, 15 Hours, 23 Minutes, 40 Seconds.

APNIC IPv4 RIR: All Gone! 15th April 2011

IANA Central IPv4 Registry: All Gone! 1st February 2011

Fig. 2 – Contagem para o esgotamento do IPv4

Neste contador indica que estaremos a 17 dias do esgotamento do IPv4 no continente Europeu e Asiático.

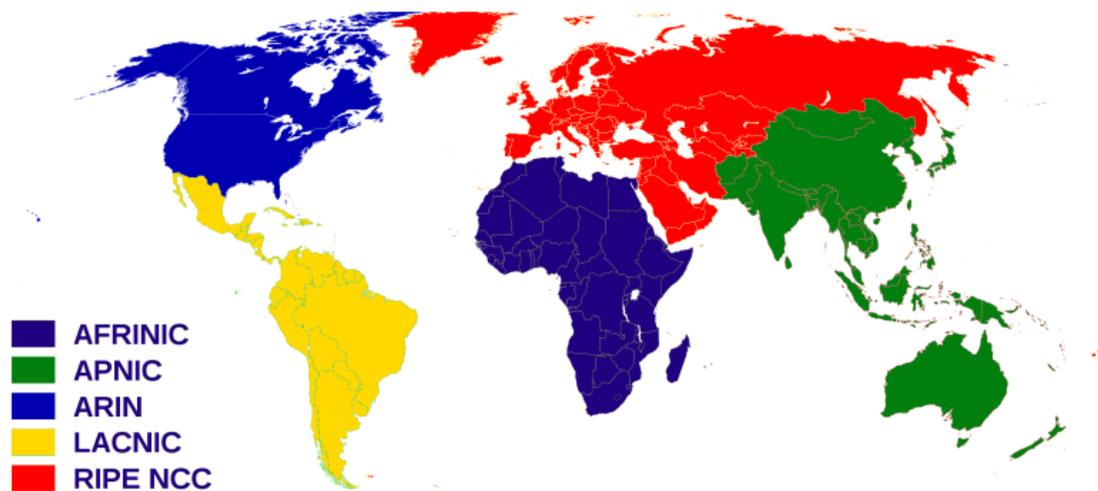


Fig. 3 – Mapa mundial de registos da internet

Com o intuito de acelerar/agilizar o processo de mudança foi definido em que no dia mundial do IPv6 (8 de Julho) de 2011 seria a data escolhida, para que algumas das maiores empresas mundiais, como a *Google, Facebook, Yahoo!, Akamai* entre outras. Disponibilizassem muitos dos seus serviços em IPv6, durante 24 horas.

O objectivo desta passagem simbólica do IPv4 para IPv6, deu para que especialistas da área das redes avaliassem o impacto e eventuais problemas assim como a performance do mesmo. O objectivo do dia mundial do IPv6, também baptizado de "*Flight Test Day*", é de motivar as organizações, ISP's, fabricantes de hardware, empresas responsáveis pelo desenvolvimento de sistemas operativos, área da web, entre outros de preparar os seus serviços para o IPv6.

CAPÍTULO 2

2. EXPOSIÇÃO E EXPLICAÇÃO DO PROBLEMA

2.1. Introdução

Depois do que foi falado por nós no capítulo anterior, nada melhor do que passar para a experimentação real e observarmos as vantagens/desvantagens *“in loco”*.

A elaboração deste projecto prende-se também com o que foi decidido pela FCCN, que obriga a que todas as universidades a migrarem para a arquitectura de IPv6, assim sendo nós para além de respondermos ao que foi deliberado pela FCCN, pensamos numa forma de construir um sistema ou appliance que fosse facilmente integrada no mercado.

Foi um processo bastante moroso toda a procura de software e configuração, testamos varias soluções em que por vezes fomos obrigados a voltar ao ponto de partida e começar todo o trabalho desde o início. Os testes efectuados vão ser explicados nos capítulos seguintes.

2.2. Esquema da rede principal

A proxima figura representa o esquema principal da rede.

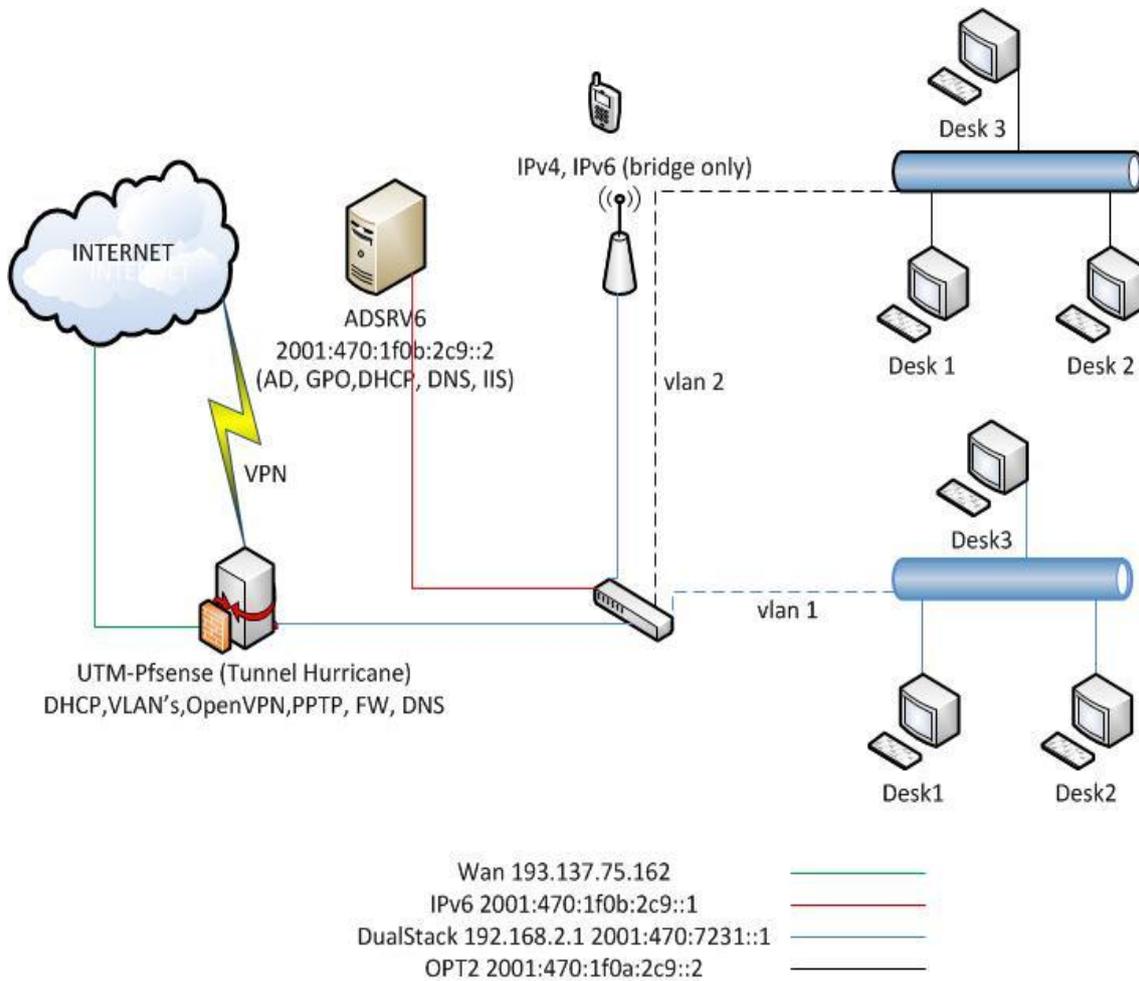


Fig. 4 – Esquema da rede física

A rede foi concebida para testes por isso mesmo escolhemos um ambiente virtual, sujeita aos condicionalismos resultantes do equipamento disponível, que cumpriu na íntegra para o objectivo ao qual se propunha.

O objectivo era implementar uma estrutura que pudesse simular o mais possível as necessidades de comunicação existentes na Universidade Lusófona, onde não falta uma AD com GPO definidas.

2.3. Software utilizado

Para o nosso trabalho, inicialmente optamos pelo Ubuntu Server 10.10 aqui conseguimos colocar tudo o que a DHCPv6 dizia respeito a funcionar. Os problemas vieram a seguir com a pouca documentação existente assim com inúmeros bugs em alguns serviços.

A nossa segunda opção foi o pfsense que se revelou uma agradável surpresa, não só pela sua robustez, mas também pela sua enorme versatilidade. A documentação existente também foi determinante para a nossa escolha.

Este foi um projecto todo ele primeiramente desenhado em ambiente virtual graças as ferramentas disponibilizadas pela VMWare.

The screenshot displays the VMware ESXi 5.0.0 interface for a virtual machine named 'tfcsvr.adminzone.ulusofona.pt'. The interface is divided into several sections:

- General:** Manufacturer: Hewlett-Packard; Model: HP Compaq dc5800 Small F...; CPU Cores: 2 CPUs x 2,992 GHz; Processor Type: Intel(R) Core(TM)2 Duo CPU E6400 @ 3.00GHz; License: VMware vSphere 5 Hypervisor - Licensed for 1 physical CP...; Processor Sockets: 1; Cores per Socket: 2; Logical Processors: 2; Hyperthreading: Inactive; Number of NICs: 1; State: Connected; Virtual Machines and Templates: 7; vMotion Enabled: N/A; VMware EVC Mode: Disabled; vSphere HA State: N/A; Host Configured for FT: N/A.
- Resources:** CPU usage: 101 MHz; Capacity: 2 x 2,992 GHz; Memory usage: 2754,00 MB; Capacity: 4015,23 MB.
- Storage:** datastore1 (Non-SSD, 144,00 GB).
- Network:** DMZ, VM Network, IPv4, IPv6 (all Standard port group).
- Fault Tolerance:** Fault Tolerance Version: 2.0.1-3.0.0-3.0.0; Total Primary VMs: 0; Powered On Primary VMs: 0; Total Secondary VMs: 0; Powered On Secondary VMs: 0.

Fig. 5 – Laboratório virtual

O nosso laboratório virtual foi composto por:

- 2 Desktops em Ubuntu,
- 2 Desktops em Windows 7 (um de 32bits e outro de 64)
- UTM em pfsense
- Domain Controller (Windows Server 2008 R2)

Nota: O CentOS diz respeito ao à segunda parte do trabalho (DNSSEC)

A imagem seguinte diz respeito à configuração do vSwitch, onde estão presentes todas as VLANs por nós utilizadas.

View: vSphere Standard Switch

Networking

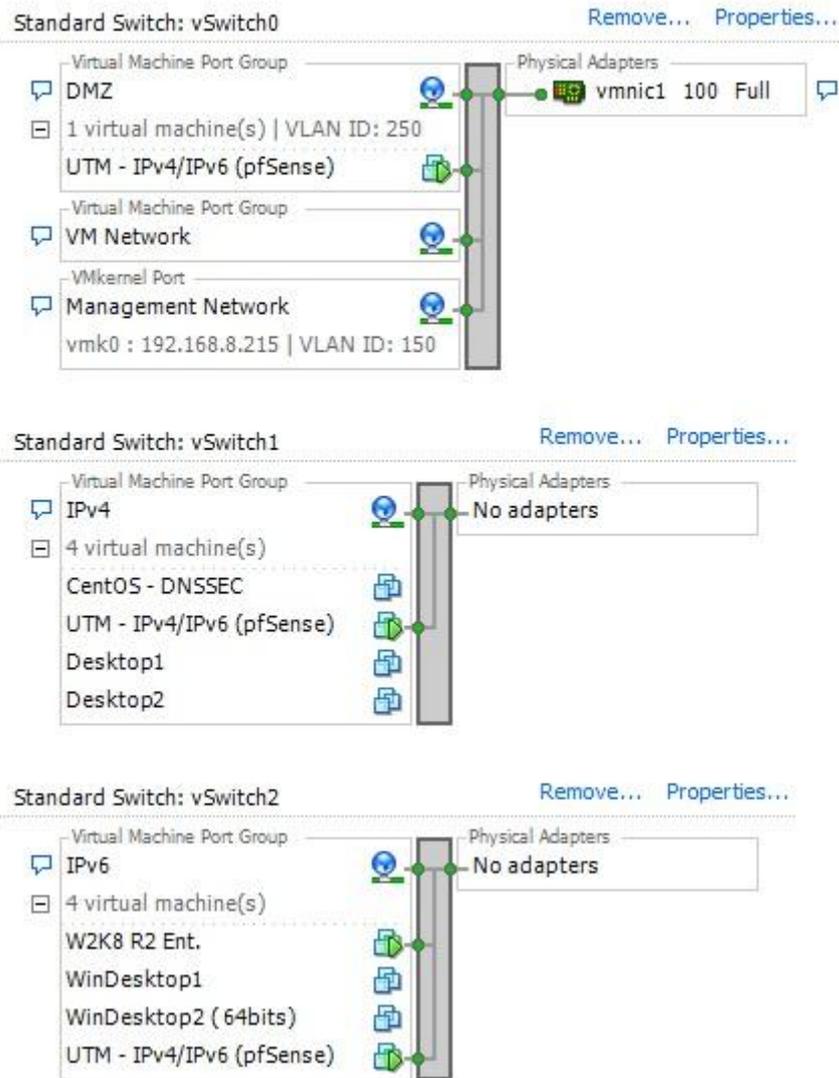


Fig. 6 – Switch do laboratório virtual

CAPÍTULO 3

3. SOLUÇÕES POSSÍVEIS

3.1. Introdução

São três as soluções que propomos, como transição do IPv6 para o IPv4: “Dual Stack”, “Tunneling”, e a tradução de endereços.

Foram assim usados nestes trabalhos vários tipos de endereçamento IPv6 e de conectividade unicast para ligação ao mundo IPv6, existem outras opções.

Neste trabalho apresentamos os resultados das que foram testadas.

3.2. Soluções versus endereçamento

Em IPv6 para cada tipo de domínio de utilização deveremos usar o endereçamento adequado. Nos próximos pontos faremos a apresentação das várias soluções usadas em função do scope do endereçamento.

Endereçamento Link-Local Link-Local é auto-atribuído automaticamente pelos equipamentos (depois de activado o IPv6) na gama FE80::/10, este endereçamento, como o nome indica, apenas permite conectividade local. É o tipo de endereço anunciado pelos routers às máquinas de uma rede, como o peer da rota por omissão.

Este tipo de endereço não pode ser encaminhado, não podemos nunca ultrapassar circuito físico onde pertence (rede de nível 2 OSI).

Assim o seu uso é muito limitado. Por exemplo no comando ping no Windows (usando o endereçamento link-local é necessário indicar a interface correcta de origem com o sufixo %x, em que “x” é o identificador da interface, de outra forma este não responde.

```
C:\Users\Administrator>ping fe80::eda9:a1bc:4768:1de0%11
Pinging fe80::eda9:a1bc:4768:1de0%11 with 32 bytes of data:
Reply from fe80::eda9:a1bc:4768:1de0%11: time<1ms
Reply from fe80::eda9:a1bc:4768:1de0%11: time<1ms
Reply from fe80::eda9:a1bc:4768:1de0%11: time<1ms
Reply from fe80::eda9:a1bc:4768:1de0%11: time<1ms

Ping statistics for fe80::eda9:a1bc:4768:1de0%11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fig. 7 – Ping a um endereço link-local

3.2.1. Endereçamento Unique-Local

Este tipo de endereçamento foi escolhida para a comunicação interna entre os vários pontos da rede, pois não sendo um endereçamento global (público, com encaminhamento na Internet), permite o encaminhamento na rede privada, e portanto a comunicação interna entre os vários pontos da rede.

Não sendo talvez a opção mais lógica face à abundante disponibilidade de endereçamento global (abordado mais tarde), e do estrito ponto de vista da conectividade IP (bem mais flexível), penso que irá ser esta a opção da maior parte dos gestores de redes, pois irá continuar a permitir o controlo centralizado dos acessos ao mundo exterior a partir da rede interna (por exemplo, usando um proxy para a conectividade para o exterior).

O endereçamento Unique-Local tem o prefixo FC00::/7 (1111 110L), mas como na prática o valor de L é sempre 1, pois indica que tem apenas um valor local (o valor "0" não está em uso), os primeiros 8 bits assumem o valor FD00::/8.

3.2.2. Endereçamento Global, Prefixo 2001::/64

Neste prefixo implementei com dois tipos de túneis: Manual e automático. O conceito do túnel pode ser usado, mas obriga sempre à existência algures na rede de uma máquina com suporte simultâneo de IPv4 e IPv6 (Dual Stack), em função da rede dominante, a solução poderá passar por efectuar túneis IPv6 sobre IPv4 (o mais provável na actual fase de arranque) ou IPv4 sobre IPv6 (quando a migração estiver quase completa e for necessário continuar a assegurar a compatibilidade com SO ou hardware obsoleto).

3.2.2.1. Túnel automático IPv6 sobre IPv4: 6To4

3.2.2.1.1. Com acesso HSDPA

Teoricamente também é possível ter conectividade IPv6 com HSDPA da TMN, o problema é que a resposta a um IP passa por Londres e tem como destino um servidor nos EUA. Enquanto a ligação RCTS responde com um servidor sediado em Portugal (da FCCN).

Consequentemente a resposta por via deste túnel (a ser efectivamente estabelecido) será sempre muito mais lenta do que a resposta obtida na solução ADSL usada.

A resposta com o HSDPA é 13 vezes mais lenta (o RTD é cerca de 150ms contra 11ms do acesso ADSL).

3.2.2.1.2. Prefixo 2001::/64 (ISP)

Este endereçamento é o único que permite verdadeira conectividade global IPv6, ou seja conectividade entre pontos remotos que só usam IPv6 (com o <http://ipv6.google.com/>).

O problema é que o não possui Hardware na faculdade capaz de tratar endereçamento IPv6 nativo. Assim este tipo de conectividade só foi possível na Universidade Lusófona (via FCCN), e com um Tunnel broker.

This page shows your IPv6 and/or IPv4 address

You are connecting with an IPv6 Address of:

2001:470:1f0b:2c9::2

[IPv4 only Test](#)

[Normal Test](#)

[IPv6 only Test](#)

Fig. 8 – whatismyv6.com via tunnel broker

3.2.2.1.3. Tunnel brokers

Na falta de endereçamento nativo IPv6 do prefixo 2001::/64 fornecido pelo meu ISP recorremos aos famosos tunnel brokers. A nossa experiência inicial foi bastante rápida e com sucesso com algumas soluções também bastante amigáveis como a [SixXs](#), também com sucesso com a [Hurricane Electric](#). O túnel [Hurricane Electric](#) foi fácil de estabelecer, após registo no site <http://www.tunnelbroker.net/>, foi atribuído um IPv6 global, e um endereçamento global com um prefixo ::/48 (delegated prefix) para uso outras de máquinas da rede, e ainda um domínio.



Tunnel Details

IPv6 Tunnel | Example Configurations | Advanced

Tunnel ID: 158497 [Delete Tunnel](#)
Creation Date: May 4, 2012
Description:

IPv6 Tunnel Endpoints

Server IPv4 Address: 216.66.80.30
Server IPv6 Address: 2001:470:1f0a:2c9::1/64
Client IPv4 Address: **193.137.75.162**
Client IPv6 Address: 2001:470:1f0a:2c9::2/64

Available DNS Resolvers

Anycasted IPv6 Caching Nameserver: 2001:470:20::2
Anycasted IPv4 Caching Nameserver: 74.82.42.42

Routed IPv6 Prefixes

Routed /64: 2001:470:1f0b:2c9::/64
Routed /48: 2001:470:7231::/48 [X]

rDNS Delegations [Edit](#)

rDNS Delegated NS1:
rDNS Delegated NS2:
rDNS Delegated NS3:
rDNS Delegated NS4:
rDNS Delegated NS5:

Fig. 9 – Detalhes do tunnel broker

A próxima figura representa o funcionamento deste tipo de túnel.

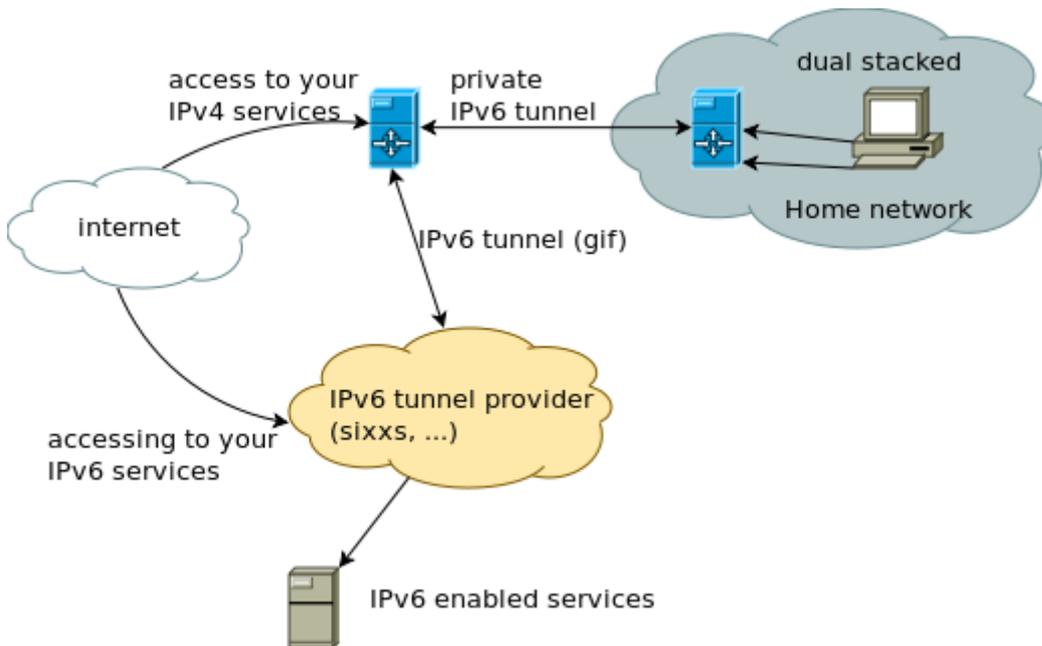


Fig. 10 – Funcionamento do túnel da [Hurricane Electric](#)

3.3. Túnel Manual

Vantagens

- Excelente controlo dos parâmetros da ligação, pois trata-se de uma ligação “ponto-a-ponto” entre dois pontos com IPv4 público. A implementação é muito fácil, e pode ser centralizada num router, tornando a solução “transparente” para os utilizadores das duas redes. Portanto a ligação apenas se estabelece com o ponto definido no router, e pode ser uma boa solução para assegurar ligações (com IP’s públicos ou não) IPv6 sobre estruturas IPv4, às quais se poderá acrescentar segurança definindo o tráfego interessante e encriptando os dados (usando por exemplo IPsec).

- O tráfego segue o caminho directamente estabelecido (dependendo do encaminhamento dos ISP’s envolvidos) para o endereço IPv4 definido pelo túnel (não depende de um ponto central).

Desvantagens

- Tem pouca flexibilidade, terá de existir sempre um túnel por cada conectividade.
- Os IP’s devem ser fixos. De outro modo com IPv4 dinâmico, como era o caso do acesso ADSL do router “AcessoNet”, os túneis e regras de segurança (como ACLs IPv4) terão de ser alterados com mesma frequência com que o ISP alterar o IP, ou sempre que este é renegociado (por exemplo quando um router ADSL é desligado), o que é incomportável numa solução que se queira permanente.
- Nos acessos ADSL o tráfego estará sempre limitado à velocidade de upload (com menor largura de banda) dos acessos envolvidos, em função da direcção do tráfego.

Nota: Foi solicitado ao ISP que suporta a ligação ADSL (PT.COM - Sapo) a atribuição de um IP fixo, mas fui informado que IP fixo só no serviço empresarial (Telepac ADSL) e que tal teria um custo de 29€ por mês. Eis um boa razão para mudar para IPv6, pois nenhum ISP terá a “necessidade” de cobrar por um endereçamento global e abundante, o que se pôde comprovar com os tunnel brokers usados.

3.4. Túnel 6to4

Vantagens

- Proporciona um ponto centralizado de acesso ao mundo IPv6 numa rede, com a hipótese de assim se poderem estabelecer regras de acesso (segurança) centralizadas e controladas pelo administrador da rede.

- O relay 6to4 é sempre o mais próximo do ISP (em termos de métricas de encaminhamento), e não terá de ser o mesmo nos dois sentidos, o que implica menos saltos, maior eficiência e redundância na ligação.

- Um exemplo curioso é a rápida conectividade ao site IPv6 do IPL <http://www.net.ipl.pt/> (resposta ao ping em cerca de entre 11 e 22 ms, e apenas com 5 saltos) por via deste túnel, o que se justifica pelo facto da conectividade global IPv6 (também a IPv4) do IPL ser assegurada pela FCCN.

Nota: Esta solução não se comporta verdadeiramente como um túnel. Isto porque o IPv4 (e o Servidor relay 6to4) para o qual enviamos tráfego IPv6 encapsulado, pode não ser o mesmo que nos devolve resposta.

Desvantagens

- Ligações por um gateway na prática fixo, neste caso da FCCN, constituindo um ponto de falha ou possibilidade de ter de realizar mais saltos do que os necessários, embora neste caso seja preferível a ter um gateway permanentemente mais longe (a exemplo do túnel Hexago6), pelas razões já apresentadas.

- Os túneis não são fáceis de configurar devido a pouca documentação existente. Menos fácil será neste momento se o router não for Cisco.

- A solução "6to4" embora se tenha demonstrado ser executável e com um desempenho razoável, as conclusões poderão ser muito diferentes com outros operadores, em função das soluções implementadas, pelo que o seu real comportamento terá de ser verificado caso a caso.

3.5. Túnel Hexago

Vantagens

- Os túneis são muito fáceis de configurar, e sem muitas perguntas no registo que no entanto é imprescindível uma vantagem.
- Atribuição de recursos é gratuita (conectividade IPv6, um domínio e um prefixo para a rede local), estes serviços são bem pagos ou difíceis de obter em IPv4, mas gratuitos neste operador em IPv6 (para os fins declarados).
- Ponto centralizado de acesso ao mundo IPv6 numa rede, com a hipótese de assim se poderem estabelecer regras de acesso (segurança) centralizadas controladas pelo administrador da rede, embora neste caso num PC e não num router como o túnel 6to4.
- Fornece um IPv6 com um prefixo verdadeiramente global: 2001::/64
- É possível implementar este tipo de solução num router, como a nossa UTM (pfsense).

Desvantagens

- Ligações por meio de um gateway fixo (um ponto de falha e a possibilidade de ter de realizar mais saltos do que os necessários). E neste caso o gateway está distante do meu ISP, o que se nota mais nos sites com sede em Portugal.
 - A ligação por vezes cai ocasionalmente por timeout.
 - Ligação mais lenta (pelas razões apresentadas primeiro ponto). O site <http://ipv6.net.ipl.pt/> não respondeu no browser devido a timeout, Para este site temos conectividade, mas sempre com mais de 550ms de resposta (13ms do túnel 6to4!)
 - O desempenho da solução dependerá directamente da distância do utilizador relativamente ao servidor do túnel (e não tanto do ISP usado, como no túnel “6to4”).
- A figura seguinte e bem elucidativa deste facto: O tráfego vai até a Alemanha e regressa atravessando quase toda a Europa até atingir o www.sapo.pt

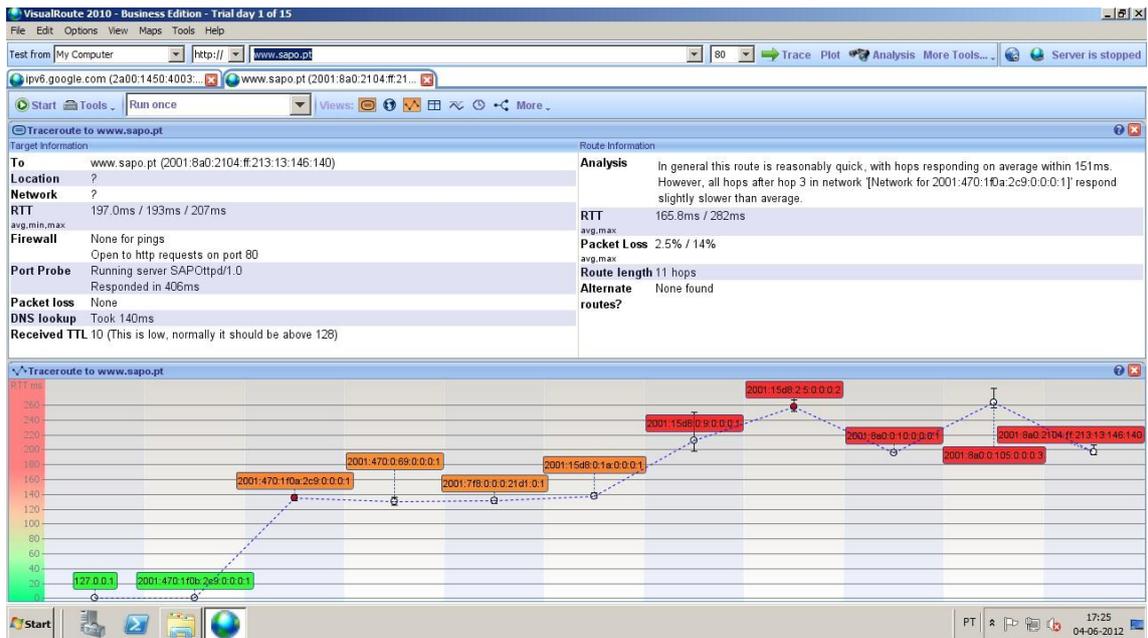


Fig. 11 – Teste com Visual Route 2008 www.sapo.pt

- Tipicamente só funciona com suporte num PC (mas existem soluções para diferentes Sistemas Operativos).
- O túnel da Hexago, quando estabelecido, impede a comunicação por IPv6 fora do túnel devido à introdução de uma rota `::/0` para o túnel, o que impede a comunicação com a restante rede (sites remotos). Será necessário introduzir rotas específicas no PC.

```

netsh interface ipv6 show route
yes   Manuais  0 2001:470:1f0b:2c9::/64          5 Rede testes IPv6
yes   Manuais  0 ::/0                            4 Hexago Gateway6

```

Fig. 12 – Exemplo do encaminhamento com tunnel Hexago

- Potenciais problemas de segurança (comum a túneis idênticos). A conectividade é indirectamente estabelecida com um ponto IPv4 usando UDP, através de uma máquina que estabeleceu o túnel e que serve de proxy às restantes. Consultar os testes de segurança.
- Por HSDPA não obtive conectividade neste túnel.

CAPÍTULO 4

4. ARQUITECTURA DA SOLUÇÃO IMPLEMENTADA

4.1. Introdução

Tal como já foi estudado nos capitulos anteriores (capítulo 2 e 3) as diferentes soluções possíveis de implementar, bem como toda a configuração necessária para que este projecto se possa integrar na rede da faculdade.

A nossa escolha recaiu pela solução do Tunnel brokers, não só pela nossa limitação em termos de material mas também por ser a solução mais executável no nosso ambiente de teste.

4.2. Configuração da UTM

Assim sendo poderá ser consultado o “Anexo 1” configuração da UTM, para uma futura implementação definitiva na faculdade apenas terá de ser alterada a configuração da porta WAN, não sendo necessário a criação da placa **gif**. Aqui também é apresentado como criar uma ligação de VPN só em IPv6.

4.3. Configuração de domínio IPV6 (Windows)

Neste ponto vamos apresentar no “Anexo 2” a configuração básica de um domínio puro IPv6, serão utilizadas todas as principais tecnologias oferecidas pelo Windows Server 2008 R2. Tais como DHCP, GPO, IIS, AD e DNS.

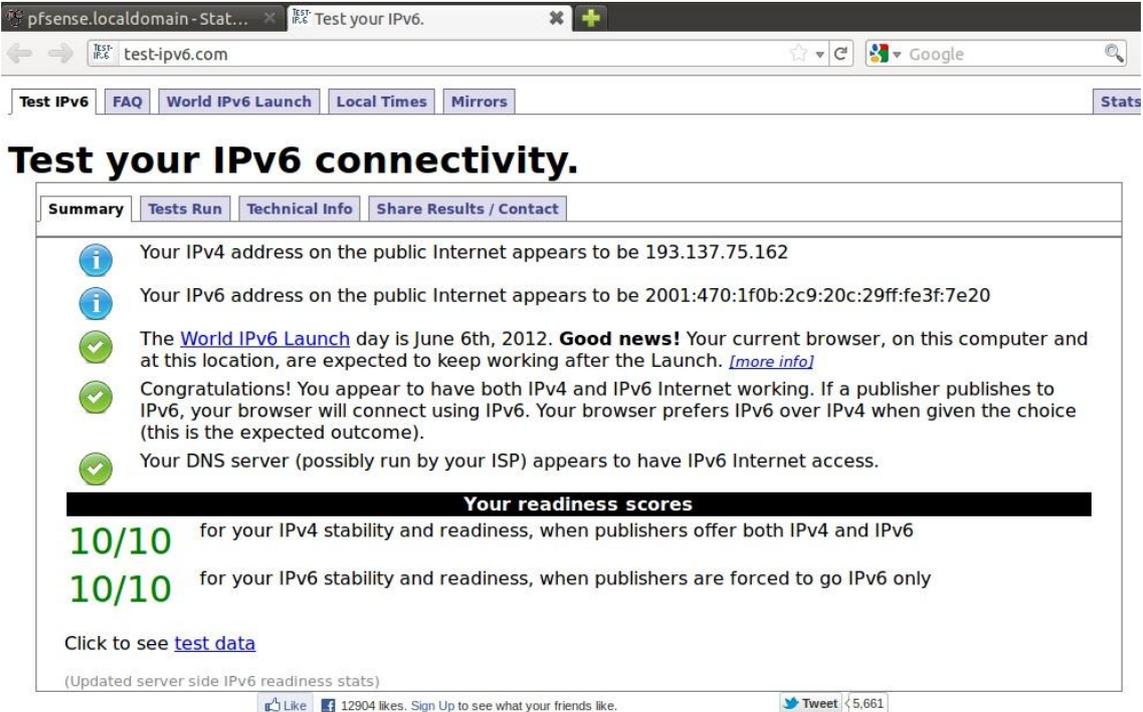
CAPÍTULO 5

5. TESTES

5.1. Introdução

Os testes que podemos efectuar foram apenas de conectividade, pelo projecto ser inicialmente efectuado num ambiente virtual, todos os teste de qualidade que podessemos fazer seriam resultados que não representavam a realidade.

Assim sendo inicialmente tentamos obter conexão pura de IPv6, onde a imagem seguinte pode provar o sucesso desse teste.



The screenshot shows a web browser window with the URL 'test-ipv6.com'. The page title is 'Test your IPv6 connectivity.' and it features a navigation menu with links for 'Test IPv6', 'FAQ', 'World IPv6 Launch', 'Local Times', 'Mirrors', and 'Stats'. The main content area has tabs for 'Summary', 'Tests Run', 'Technical Info', and 'Share Results / Contact'. The 'Summary' tab is active, displaying the following information:

- Your IPv4 address on the public Internet appears to be 193.137.75.162
- Your IPv6 address on the public Internet appears to be 2001:470:1f0b:2c9:20c:29ff:fe3f:7e20
- The [World IPv6 Launch](#) day is June 6th, 2012. **Good news!** Your current browser, on this computer and at this location, are expected to keep working after the Launch. [\[more info\]](#)
- ✓ Congratulations! You appear to have both IPv4 and IPv6 Internet working. If a publisher publishes to IPv6, your browser will connect using IPv6. Your browser prefers IPv6 over IPv4 when given the choice (this is the expected outcome).
- ✓ Your DNS server (possibly run by your ISP) appears to have IPv6 Internet access.

Your readiness scores

- 10/10** for your IPv4 stability and readiness, when publishers offer both IPv4 and IPv6
- 10/10** for your IPv6 stability and readiness, when publishers are forced to go IPv6 only

Click to see [test data](#)

(Updated server side IPv6 readiness stats)

Like 12904 likes. Sign Up to see what your friends like. Tweet 5,661

Fig. 13 – Tunnel IPv6 a funcionar

5.2. Conexão IPv6 – IPv6

Através do Visual Route foi-nos possível fazer um teste de conexão e assim ter uma percepção muito maior do percurso do pedido desde a nossa máquina ate ao servidor em questão. É interessante ver que o pedido segue até à Alemanha (Frankfurt **216.66.80.30**), onde está sediado o nosso tunnel broker, voltando para Portugal.

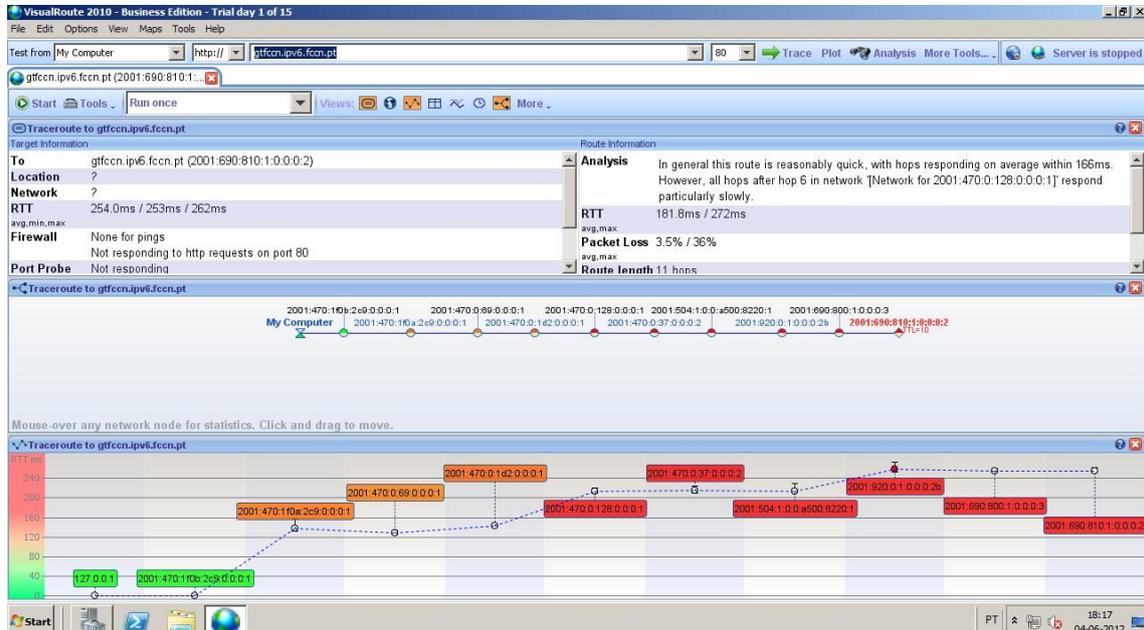


Fig. 14 – Teste com Visual Route 2008 acesso a um site IPv6

5.3. Conexão IPv6 – IPv4

A conversão de IPv6 para IPv4 foi conseguida por intermédio do tunnel Sixxs, este permitiu-nos fazer a conversão e desta forma conseguir chegar a sites de IPv4 puros, a partir de IPv6.

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping www.abola.pt.sixxs.org

Pinging ipv6.nginx.sixxs.net [2001:838:2:1::30:67] with 32 bytes of data:
Reply from 2001:838:2:1::30:67: time=135ms
Reply from 2001:838:2:1::30:67: time=134ms
Reply from 2001:838:2:1::30:67: time=134ms
Reply from 2001:838:2:1::30:67: time=134ms

Ping statistics for 2001:838:2:1::30:67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 134ms, Maximum = 135ms, Average = 134ms

C:\Users\Administrator>ping www.abola.pt
Ping request could not find host www.abola.pt. Please check the name and try again.

C:\Users\Administrator>
```

Fig. 15 – Ping através de um tunnel Sixxs

5.4. VPN

Achamos interessante integrar uma solução de VPN no nosso projecto, as opções por nós testadas foram então o OpenVPN e PPTP, seguidamente explicaremos qual, para que funções e porque foi escolhida.

5.4.1. OpenVPN

Como já foi por nós abordado no capítulo anterior, o porque da nossa opção ter recaído pela arquitectura do OpenVPN, em termos de segurança pareceu-nos ser a mais fidigna, pois é gerada uma chave para cada utilizador. Em que esta chave fica associada à máquina, sendo assim o OpenVPN é a opção mais segura.

O próximo esquema nos ajuda a entender a arquitectura do OpenVPN.

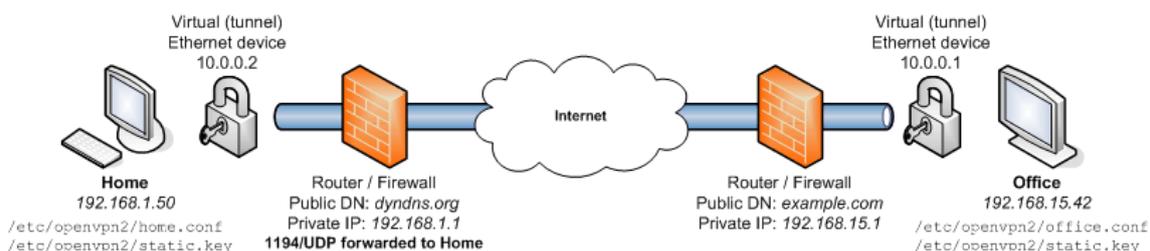


Fig. 16 – Esquema Open VPN

5.4.2. VPN PPTP conexão IPv4

A opção PPTP, foi uma opção gorada para a ligação ao IPv6, pois o protocolo PPTP ainda não suporta IPv6. Mesmo assim optamos por colocar uma VPN PPTP lida à parte da gestão do Pfsenes.

5.5. IPv6 por Wi-Fi

A solução que nós conseguimos arranjar foi um pouco limitada pelo hardware disponível, pois a única antena que possuímos na faculdades e que nos permitia integrar com uma rede de IPv6, apresentou algumas limitações.

Sendo assim o AP que utilizamos para testes entra-se a difundir IPv4 e IPv6 em modo bridge only.

CAPÍTULO 6

6. CONCLUSÕES

6.1. O IPv6 no Mundo

Como já foi utilizado para um anúncio de refrigerantes, podemos dizer o mesmo em relação ao IPv6, “primeiro estranha-se depois entranha-se”, actualmente quase todos os equipamentos vêm com suporte IPv6. Muitos dos administradores de redes acreditam na sua implementação e nas suas vantagens, mas num futuro distante ... É comum ouvir dizer-se que o IPv4 levou muitos anos até ficar completamente “afinado”, daí a desconfiança com que ainda se olha para o IPv6.

Foi decidido que os gigantes da internet (Google, Amazone, Facebook, etc.) iriam fazer a alteração no “dia D”, afim de acelerar o processo de mudança. O problema é que se for efectuado demasiado tarde e sem um adequado planeamento, poderá ser difícil evitar constrangimentos económicos, sociais e políticos. Terá forçosamente de passar por muita formação, levantamento das capacidades dos equipamentos e do software e por fim uma implementação faseada e cautelosa.

Nota: Talvez o problema do ano 2000 e as bases de dados (devido às datas de apenas dois dígitos) seja um bom e um mau exemplo de adaptação: Bom, porque foi atempadamente equacionado e resolvido, mau porque a sua resolução pareceu demasiado fácil.

O importante será saber se as pessoas envolvidas no desenvolvimento de projectos em redes de comunicação, principalmente quem decide quais os investimentos a efectuar (gestores) são capazes de acreditar nas suas vantagens.

A Ásia aparenta ser a mais empenhada em seguir este novo protocolo. Isto porque ficou prejudicada na distribuição de endereçamento, é assim perceptível a importancia do endereçamento IP em economias emergentes como a da Índia ou da China.

Em particular a China que impressionou o mundo com os seus recentes Jogos Olímpicos (2008) e agora em Londres que vai ser os jogos Olímpicos mais tecnológicos, provavelmente aproveitando o facto de estar a construir de raiz novas estruturas de comunicação apostou no IPv6.

6.2. Custos de Implementação

Para podermos fazer propostas empresarias sobre o sistema implementado e com vista a mostrar que as soluções "open source" são opções viáveis, a nível de estabilidade e economicamente uma vantagem, decidimos fazer um relatório de custos para mostrar a possíveis clientes.

Todos este relatório incidirá apenas sobre a UTM Pfsense implementada e o que achamos uma proposta razoável para uma PME detentora de um nível significativo de infraestrutura informática, bem como da dependência dos vários serviços apresentados por esta solução.

Atenção que são apenas custos relacionados com a implementação de Hardware, a nível de configuração tem um custo de implementação de 100€(tendo em conta uma implementação idêntica à nossa, ou seja, até 2 redes), a nível de ISP contamos com a colaboração do nosso cliente e o seu gestor de conta.

Decidimos assim apresentar 2 soluções, uma "LowCost" e outra "Performance":

- LowCost -> até 10 utilizadores VPN + restantes serviços
- Performance -> até 50 utilizadores VPN + restantes serviços (com raid 1+0, sistema com capacidade de utilização elevada)

UTM Appliance "LowCost"		Quant.	Preço
HDD	Wester Digital 250GB SATA II 16mb Cache	1	66,45
Ram	DDR3 4096MB 1333MHz KINGSTON	1	30,75
MB	ASUS P8H61	1	75,60
Caixa	Cx MidiTow ATX450W Preta	1	40,00
CPU	Intel® Pentium G850, 2,9GHZ, skt 1155, 3M Cache	1	88,20
Placa de Rede	NX1101 Gigabit PCI Card, 10/100/1000 MBPS	2	30,17
Drive	DRW-24B5ST/BLK/B/AS SATA	1	16,00

Total	347,17
--------------	--------

Preços com IVA

Computador Intel Core2Duo		Quant.	Preço
Servidor	HP Proliant DL120 G7 c/Interl QuadCore E3-1220 e 4GB	1	618,20
Ram	HP 4GB 2Rx8 PC3-10600E-9 Kit	1	78,50
HDD	Disco HP 160GB 7.2k HP ETY SATA QR	2	279,26
Placa de Rede	Adaptador de Servidor HP NC360T Gigabit de Porta Dupla PCI-E	1	202,30

Total	1178,26
--------------	---------

Preços com IVA

6.3. Sobre o trabalho

Se um entusiasmo inicial para com o IPv6 pode ser fácil de obter, face às suas muitas promessas, a sua implementação prática ainda levanta muitos problemas:

- O *software* disponível com suporte IPv6 já é frequente, mas ainda existem muitas lacunas.
- O equipamento mais antigo tem dificuldades devido a questões de desempenho ou incapacidade de actualização do *firmware* para o suporte do novo protocolo.
- O *firmware* que aparenta suportar IPv6 mas ao qual faltam características fundamentais (correntes em IPv4).
- Em testes futuros podemos pensar em concretizar uma avaliação ao QoS e principalmente à segurança, onde se levantam os maiores problemas e é necessária muita ponderação, cautela e capacidade de inovação.

No entanto ficamos convencidos de que a transição para o IPv6 é tão desejável. Devido às potencialidades de desenvolvimento económico que promete ao tornar a conectividade verdadeiramente global e sem barreiras, como necessária, devido à exaustão do endereçamento IPv4.

Mas verdades absolutas não existem, e como já foi referido por nós o IPv4 está muito “afinado”, o que pode levar a que seja perpetuado, como muitos parecem acreditar. No entanto não nos parece muito sensato que tal aconteça. Ficar à espera que o IPv4 se esgote e correr o risco de nos envolvermos em soluções de complexidade crescente para o manter, que provocarão constrangimentos que podem abalar as nossas economias (tal como em 2000).

CAPÍTULO 7

7. DNSSEC

7.1. Introdução

DNSSEC é o nome dado às extensões de segurança ao protocolo DNS e foi criado para proteger e autenticar o tráfego DNS. Estas extensões procuram validar os dados através de assinaturas digitais, fazendo uso de assinaturas criptográficas assimétricas. Provê segurança para a resolução de endereços. Funciona como um caminho alternativo para a verificação de autenticidade.

Por exemplo, no caso de domínios .eu vai ser obrigatório a utilização do **DNSSEC**. Estas operações ocorrem antes de qualquer verificação de segurança em camadas superiores (**SSL, SSH, PGP** etc...).

A autenticidade e integridade são providas pela assinatura dos Conjuntos de **Registros de Recursos** (Resource Records Sets - RRset) com uma chave privada. Zonas delegadas (filhas) assinam seus próprios RRsets com sua chave privada.

Autenticidade da chave é verificada pela assinatura na zona pai do Recurso DS (Record DS) (hash da chave pública da zona filha).

A chave pública é usada para verificar RRSIGs dos RRsets.

Autenticidade da não existência de um nome ou tipo provida por uma cadeia de registros que aponta para o próximo em uma sequência canónica.

7.2. Porque é o DNSSEC necessário?

Com a, cada vez maior, dependência do cidadão comum nas tecnologias da comunicação e da informação e da Internet em particular, tem vindo a crescer a preocupação dos utilizadores e o grau de importância das questões relacionadas com a segurança das transacções electrónicas.

Esta preocupação resulta da exposição mediática de ataques feitos a serviços em linha, explorando vulnerabilidades nas aplicações e nos serviços básicos da Internet.

Como consequência diversos países identificaram a segurança informática e a confiança dos utilizadores nos serviços prestados em linha como o principal constrangimento ao crescimento do comércio electrónico. Noutra contexto, as autoridades responsáveis pela protecção de infra-estruturas críticas da informação têm vindo a implementar medidas extraordinárias para reforçar a segurança do ciberespaço, na qual o DNS assume um papel de destaque.

Para responder a estas necessidades for criado, pelas entidades normalizadoras, o DNSSEC, um conjunto de extensões realizadas ao protocolo DNS (Domain Name System) que

vem mitigar uma série de vulnerabilidades e de vectores de ataque bem conhecidos a serviços em linha, melhorando a qualidade e a confiança dos utilizadores nestes.

As extensões DNSSEC visam melhorar a confiabilidade dos utilizadores nos serviços prestados em linha. O DNSSEC vem nomeadamente:

Porquê o DNSSEC?

- Para contribuir para uma Internet Segura.
- Suprimir fragilidades do protocolo DNS;
- Prevenir ataques do tipo man-in-the middle e cache poisoning;
- Reduzir o risco de manipulação de informação;
- Reforçar a fiabilidade do sistema.

7.3. Como funciona o DNSSEC?

O DNSSEC tem por base a utilização de criptografia assimétrica, tecnologia com a qual os dados DNS são assinados. Quando um domínio se encontra “assinado”, um servidor de nomes DNS pode autenticar as respostas que obtém protegendo assim o utilizador de ataques, como por exemplo, de injeção de informação corrupta na memória temporária do servidor.

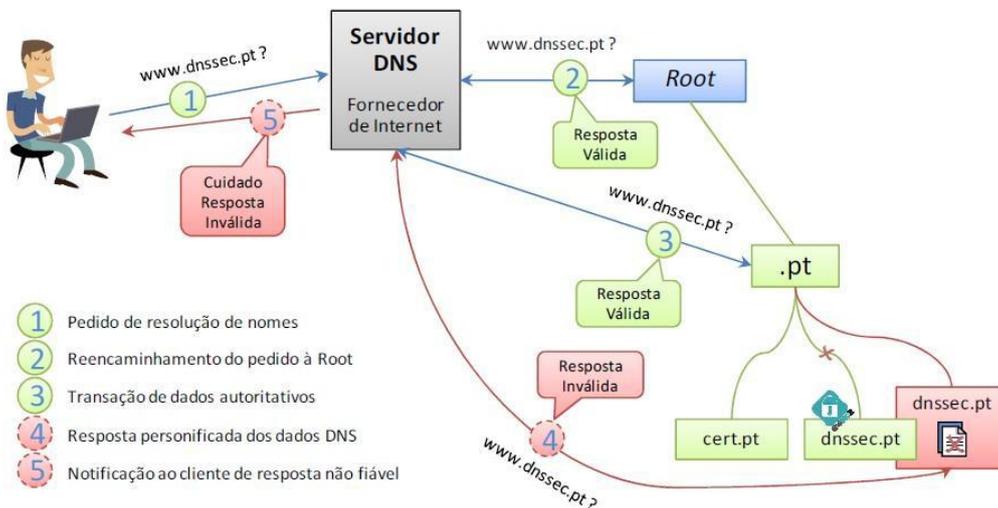


Fig. 17 – Funcionamento do DNSSEC

A criptografia assimétrica utiliza um par de chaves distintas mas relacionadas entre si, são estas:

A chave pública e a chave privada.

Em termos técnicos as principais responsabilidades em relação à utilização de criptografia assimétrica no DNSSEC são:

- Delimitação rigorosa das chaves privadas aos legítimos detentores;
- Distribuição fidedigna de chaves públicas a todos os que delas necessitem;
- Actualização da informação da assinatura da zona com a hierarquia superior;
- Correcta manutenção da zona assinada;
- Gestão do tempo de vida dos pares de chaves.

Em contraponto com a implementação tradicional de DNS, com uma solução DNSSEC e tal como observado na figura consegue-se detectar uma alteração de informação DNS (ponto 4 da figura acima apresentada), e proceder à necessária notificação ao utilizador (ponto 5 da figura) levando a que essa informação seja descartada.